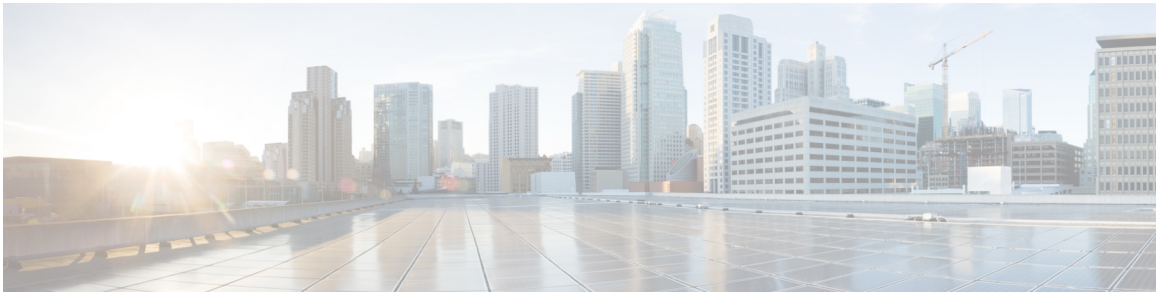
Cisco Catalyst SD-WAN CloudOps

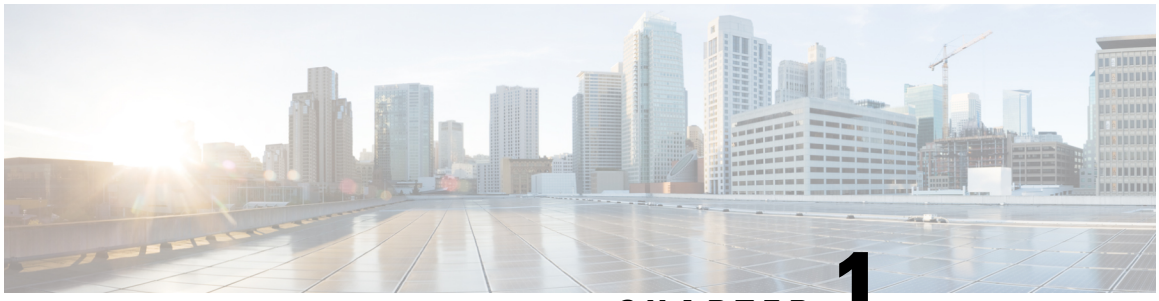
First Published: 2019-04-30

Last Modified: 2024-09-17

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS



CHAPTER 1

Cisco CloudOps Overview

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.

Cisco offers a cloud-hosting subscription for Cisco Catalyst SD-WAN Controllers such as Cisco SD-WAN Manager, Cisco SD-WAN Validator, and Cisco SD-WAN Controller that simplifies and accelerates Cisco Catalyst SD-WAN deployment, while reducing the cost of running these controllers on their own. The cloud deployment model also includes monitoring services for the instances and advanced analytics.

About This Guide

This guide describes the Cisco-managed, cloud-hosted Cisco Catalyst SD-WAN Controller, as well as its capabilities and services. This guide details the cloud infrastructure hosting processes, responsibilities, and recommendations.

Audience

The audience for this document includes network design engineers and network operators who want to purchase or deploy the cloud-based subscription options for Cisco Catalyst SD-WAN.

Types of Fabric Network in Cisco Catalyst SD-WAN

- **Dedicated Fabric**: In dedicated fabric, also known as single tenant fabric, the hosting of Cisco Catalyst SD-WAN controllers such as Cisco SD-WAN Manager, Cisco SD-WAN Validator, and Cisco SD-WAN Controller is dedicated only to the customer.
- **Shared Fabric**: In shared fabric, the hosting of Cisco Catalyst SD-WAN controllers such as Cisco SD-WAN Manager, Cisco SD-WAN Validator, and Cisco SD-WAN Controller is shared across multiple customers.

  Some of the salient features of this fabric are:

  - The data plane, the control plane, and the management plane traffic for each customer are isolated.
  - All fabric remain on the same long-lived release. Shared fabric always run on the latest long-lived star-marked release.
  - Customer agrees to external management of their Virtual Account (VA).
  - Cisco Software-Defined AVC (SD-AVC) and web certificates are available and managed by Cisco CloudOps.
  - The only limitation with this type of fabric is that TrustSec, Lawful Intercept, and RADIUS/TACACS are not supported at present.

- **Dedicated Multitenant (MT) Fabric**: In this type of fabric, the hosting of Cisco Catalyst SD-WAN Controllers such as Cisco SD-WAN Manager, Cisco SD-WAN Validator, and Cisco SD-WAN Controller is dedicated to the customer. A managed service provider hosts shared fabric for its end-customers.

Note A dedicated multitenant fabric can be hosted only on AWS cloud.

Coverage Summary

Task	Single-Tenant	Multitenant (MT)	Shared (Cisco Hosted Cloud SD-WAN)	Cloud-delivered Cisco Catalyst SD-WAN	Comments
Fabric provisioning					
Provisioning from Cisco Catalyst SD-WAN Portal	Customer	Cisco CloudOps	Customer	Customer	
Monitoring and troubleshooting of Cisco Catalyst SD-WAN Cloud controller infrastructure					
CPU and data disk utilization	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	

Task	Single-Tenant	Multitenant (MT)	Shared (Cisco Hosted Cloud SD-WAN)	Cloud-delivered Cisco Catalyst SD-WAN	Comments
Loss of connectivity to network interfaces	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	
Failure to reach instances	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	
Monitoring of Cisco Catalyst SD-WAN services					
Expiry notification of controller SSL certificates	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	
Availability of the Cisco SD-WAN Manager web server	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	
Loss of control connection to the controllers	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	
Capacity management of Cisco Catalyst SD-WAN Controllers	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps monitors and upgrades the instance capacity and expansion to clusters based on the number of devices on the fabric.
Disaster recovery					
Take periodic volume-based snapshots	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	Note that in multitenancy, the volume-based and config-based snapshot is for the entire multitenancy Cisco SD-WAN Manager cluster, not for a particular tenant.
Take periodic configuration-based backups	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	
On-demand snapshots	Customer	Customer	Not Applicable	Not Applicable	
Restore fabric based on volume or configurations	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	
Onboard to Cisco SD-WAN Analytics	Customer	Customer	Customer	Not Applicable	Cisco SD-WAN Analytics is by default onboarded for cloud-delivered Cisco Catalyst SD-WAN customers

Task	Single-Tenant	Multitenant (MT)	Shared (Cisco Hosted Cloud SD-WAN)	Cloud-delivered Cisco Catalyst SD-WAN	Comments
On-premises to cloud migration assistance	Cisco CloudOps	Not Applicable	Not Applicable	Not Applicable	Limited support - For more details on the On-prem to cloud migration, see On-Premises to Cloud Migration Process Details.
Custom subnets and TACACS	Customer	Not Applicable	Not Applicable	Not Applicable	For customers, setting up custom subnets and TACACS is only possible during Day-0 provisioning. For Day-N, customers can open TAC with Cisco CloudOps. TACACS is not available for multitenant fabric at present.
Renew controller certificates (before expiration)	Customer	Customer	Cisco CloudOps	Cisco CloudOps	
Upgrade software					
Controller software upgrade	Customer	Customer	Cisco CloudOps	Cisco CloudOps	
Edge device/node software upgrade	Customer	Customer	Customer	Customer	
Upload and manage Edge images in Cisco SD-WAN Manager Software Repository	Customer	Customer	Cisco CloudOps	Cisco CloudOps	
Respond to Cisco CloudOps notifications to authorize the service window, instance reboot, review, or verify changes carried out by Cisco CloudOps	Customer	Customer	Customer	Customer	

Task	Single-Tenant	Multitenant (MT)	Shared (Cisco Hosted Cloud SD-WAN)	Cloud-delivered Cisco Catalyst SD-WAN	Comments
Create Smart Accounts (SA) or Virtual Accounts (VA) on `software.cisco.com` and attach Cisco Catalyst SD-WAN subscribed devices to the SA/VA	Customer	Customer	Customer	Customer	
Allow external management of SA/VA on PNP Connect	Not Applicable	Not Applicable	Cisco CloudOps	Cisco CloudOps	Do Not allow external management of SA/VA on PNP Connect before provisioning fabric in Cisco Catalyst SD-WAN Portal. The provisioning workflow automatically enables the external management.
Accept external management of SA/VA and map tenant VA to customer SA/VA	Not Applicable	Not Applicable	Cisco CloudOps	Cisco CloudOps	
Define device configuration templates and policies through Cisco SD-WAN Manager	Customer	Customer	Customer	Customer	
Perform other activities that require logging in to Cisco SD-WAN Manager. For example, template and policy configuration, and edge device management	Customer	Customer	Customer	Customer	
Web server certificates	Customer	Customer	Cisco CloudOps	Cisco CloudOps	This is not applicable for multi-tenant fabric with custom domain option.

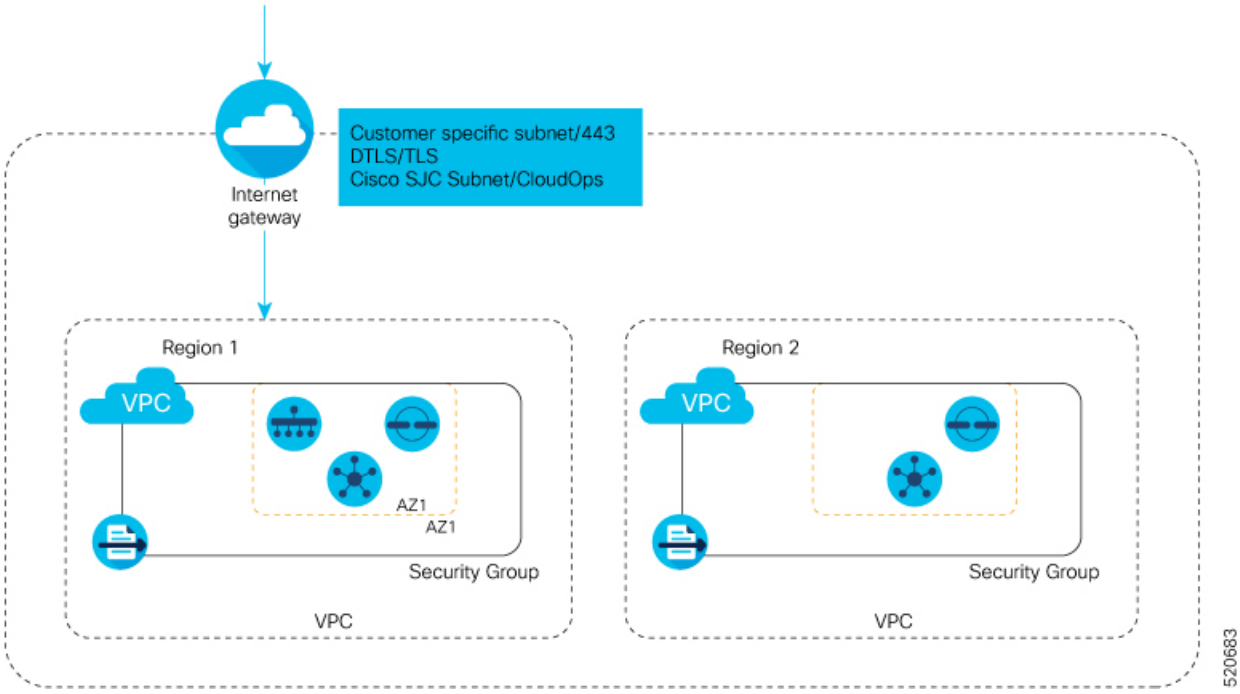
Task	Single-Tenant	Multitenant (MT)	Shared (Cisco Hosted Cloud SD-WAN)	Cloud-delivered Cisco Catalyst SD-WAN	Comments
Edge serial sync with credentials	Customer	Customer	Customer	Not Applicable	Cloud-delivered Cisco Catalyst SD-WAN customers can use their Cisco Connection On-line (CCO) login credentials for Single-Sign-On and sync edge serials.
Managed Allowed IP access list	Customer	Customer	Customer	Not Applicable	
Custom Identity Provider (IdP) Configuration	Customer	Customer	Customer	Not Applicable	Cloud-delivered Cisco Catalyst SD-WAN only supports Cisco Connection On-line (CCO) as identity provider. Customers can use Single-Sign-On feature to navigate among Catalyst SD-WAN applications such as Cisco SD-WAN Manager, Cisco SD-WAN Analytics, and Cisco Catalyst SD-WAN Portal.

Solution Design

About This Solution

When you choose a cloud-based subscription for your Cisco Catalyst SD-WAN Controllers, Cisco deploys Cisco SD-WAN Manager, Cisco SD-WAN Validator, and Cisco SD-WAN Controller on the public cloud. Cisco then provides you with administrator access. By default, a single Cisco SD-WAN Manager, Cisco SD-WAN Validator, and Cisco SD-WAN Controller are deployed in the primary cloud region and an additional Cisco SD-WAN Validator and Cisco SD-WAN Controller are deployed in the secondary or backup region.

Figure 1: Solution Architecture



Supported Clouds and Cloud Regions

The following clouds and cloud regions are supported for Cisco Catalyst SD-WAN Controller deployments:

Amazon Web Services	Microsoft Azure
Asia Pacific—Jakarta | Indonesia	Asia Pacific | Australia East—Sydney | New South Wales
Asia Pacific—Mumbai | India	Asia Pacific | Australia Southeast—Melbourne | Victoria
Asia Pacific – Hyderabad | India	Asia Pacific | Japan East—Tokyo
Asia Pacific—Seoul | South Korea	Asia Pacific | Southeast Asia—Singapore
Asia Pacific—Singapore | Singapore	Asia Pacific | West India—Mumbai Asia Pacific | South India
Asia Pacific—Sydney | Australia	UAE North—Dubai
Asia Pacific – Melbourne | Australia	Asia Pacific | Australia Central—Canberra
Asia Pacific—Tokyo | Japan	South Africa—North
Africa—Cape Town	
Canada Central—Montreal | Canada	Canada Central—Montreal | Canada Canada East

Amazon Web Services	Microsoft Azure
EU—Frankfurt | Germany	Americas | Brazil South—Sao Paulo State
EU—Ireland | Dublin	Europe | France Central—Paris
EU—London | UK	Europe | North Europe—Ireland
EU—Stockholm | Sweden	Europe | UK South—London
South America—Sao Paulo | Brazil	Europe | West Europe—Netherlands
US East—Northern Virginia | USA	Americas | East US—Virginia
US West—Northern California | USA	Americas | West US—California
US West—Oregon | USA	Americas | West US 2—Washington

Cisco Catalyst SD-WAN Cloud Provisioning

Note By default, Cisco provisions one Cisco SD-WAN Manager, two Cisco SD-WAN Validators and two Cisco SD-WAN Controllers for a fabric of size <1500.

For information on recommended computing resources, see Recommended Computing Resources for Cisco Catalyst SD-WAN Control Components.

Customer Responsibilities

- Manage allowed access-list with customer's source public IP ranges for management access of controllers.
- Renew controller certificates on time.
- Before making any changes in the Cisco Catalyst SD-WAN Portal, take the on-demand snapshot using the procedure, Take an On-Demand Snapshot and configuration backup using Back Up the Active Cisco SD-WAN Manager procedure.
- Upgrade the software.
  - You can open a TAC case for the following:
    - If you face any issues with software upgrade.
    - If you want any rollback.
  - The Cisco SD-WAN Validator and Cisco SD-WAN Controller are stateless services. Therefore, you do not need to take backups for these services. Cisco SD-WAN Manager automatically pushes the configurations once they are attached to templates.

We recommend that customers create and attach templates to the Cisco SD-WAN Validators and Cisco SD-WAN Controller instead, so the Cisco SD-WAN Manager backups automatically include the configuration backup of the controllers.

- The Cisco Catalyst SD-WAN support teams may cover the software upgrade for complex deployments such as clusters and multitenant tenant fabric. However, this support is not available for single-tenant single-node fabric.
- It is the responsibility of a customer to upgrade the software version of an edge device. For the compatible versions of edge devices based on controller versions, see Cisco SD-WAN Controller Compatibility Matrix.

- Respond to the notifications sent by Cisco CloudOps to authorize the service window, instance reboot, review, or verify changes carried out by Cisco CloudOps.
- In case of dedicated fabric, configure the third interface on Cisco SD-WAN Manager with static IP or DHCP based IP to use it for SD-AVC feature. By default the third interface is in shut state.
- Open a TAC case to arrange a service window when you receive a notification from Cisco CloudOps. Some operations can be performed only with the consent of the customer.
- Create Smart Accounts (SA) or Virtual Accounts (VA) on `software.cisco.com` and attach Cisco Catalyst SD-WAN subscribed devices to the SA or VA.
- Define device configuration templates and policies through Cisco SD-WAN Manager.
- Perform other activities that require logging in to Cisco SD-WAN Manager.
- For shared-tenant fabric, open a Cisco TAC support case if you need specific software versions to be added in the Cisco SD-WAN Manager software repository.

Your failure to meet the responsibilities outlined in this section will invalidate the SD-WAN Cloud SLA, including any guaranteed service uptimes.

Responsibilities of Cisco CloudOps

Fabric Provisioning

- Provision cloud-hosted controllers for your Cisco Catalyst SD-WAN fabric, configure a unique admin password with an expiry time of a week, and hand over Cisco SD-WAN Manager to the customer.
- Configure Cisco SD-WAN Manager with a default template and policy, when customers choose the default template and policy push option on the sales order.
- Create and manage single-tenant and multitenant clusters as needed.
- Manage tenants on multitenant fabric (direct enterprise customers).

Monitor and Troubleshoot

Cisco CloudOps monitors the health of cloud-hosted fabric and troubleshoots if there are any issues.

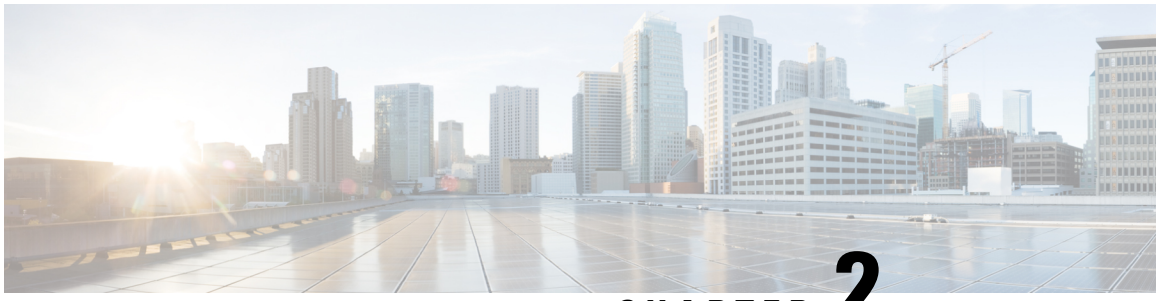
- Cisco CloudOps is backed by a real-time monitoring system that checks the health of Cisco Catalyst SD-WAN controllers and generates alerts. The check includes the health of Cisco SD-WAN Manager, application or web server, other micro services, and configuration or statistics databases.
- Take proactive action for cloud infrastructure issues, which are beyond the control of the users. Else, notify the customer about the potential issues and request the customer to open a Cisco TAC support case for further investigation.
- Manage alerts based on notifications from the cloud provider environments on instance up or down states and CPU, network inactivity status.
- Resolve the alerts proactively if it doesn't require a down time of the services. Notify the customer when services flap.
- Send 30-, 15-, and 5-day notices to the customers to renew expiring certificates on Cisco SD-WAN Manager. Cisco Catalyst SD-WAN controller certificates have a validity of one year.

Cloud Infrastructure Support

- Carry out disaster recovery workflows, including snapshot volumes or configurations. Restore Cisco SD-WAN Manager clusters based on volumes or configurations.
- Provision custom subnetting to extend customer premises network into cloud-hosted fabric network.
- Manage on-premises to cloud migrations.

Capacity Management

- Monitor the growth of devices per fabric along with the controller instance capacity parameters such as CPU, disk, and memory utilizations. Follow a pre-set guideline to increase the capacity of the service instances as needed.



CHAPTER 2

Ordering, Validation, and Account Management

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.

Role of Cisco Plug and Play

Cisco Plug and Play replaces the legacy process of Cisco Catalyst SD-WAN Salesforce (SFDC).

Refer to the following guide for information about Cisco Catalyst SD-WAN Plug and Play:

- Cisco Plug and Play Support Guide
- FAQs

Provisioning of Cisco Catalyst SD-WAN Cloud-Hosted Controllers

The Cisco CloudOps system allows creation of the Cisco Catalyst SD-WAN cloud-hosted controllers for a sales order after the following conditions are met:

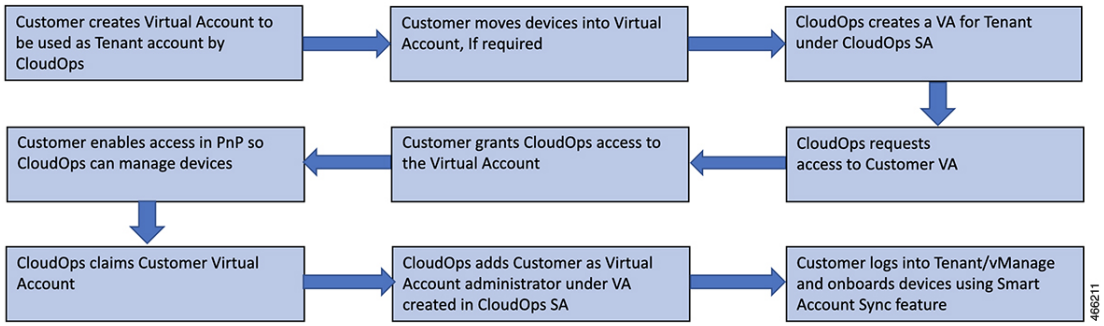
1. The sales order that has the cloud subscription licenses for edge nodes and the controller SKU for the controller provisioning.
2. Cisco Catalyst SD-WAN items in the sales order are marked as **Shipped**.

3. The sales order is assigned to an active Smart Account (SA), and, within that SA, to a Virtual Account (VA).

Cisco PNP Configuration for Shared Overlay Deployments

The customer allows external management of their virtual account (VA). Cisco CloudOps accepts virtual account management to keep Cisco Digital Network Architecture (DNA) subscriptions still in the customer VA. It creates the overlay based on this mapping.

Figure 2: Customer Virtual Account Management



Ordering

License Types and Ordering Information

There are three types of licenses and contracts.

- **A La Carte**: Customer purchases each Cisco Catalyst SD-WAN Controller stock keeping unit (SKU) separately.
- **Enterprise Agreement (EA)**: Customer purchases an EA bundle that includes Cisco Catalyst SD-WAN Controller SKUs. However, it is not available at present. A la carte license for controllers must be used for cloud controller provisioning along with an EA contract.
- **Managed Services License Agreement (MSLA)**: Customer purchases an MSLA contract that includes Cisco Catalyst SD-WAN Controller SKUs. However, it is not available at present.

A La Carte Ordering

For customers who prefer to purchase a la carte licenses for Cisco Catalyst SD-WAN Controller, see Cisco Catalyst SD-WAN Controller Ordering Guide.

EA Ordering

For provisioning a Cisco Catalyst SD-WAN cloud-hosted controller for an Enterprise Agreement (EA) customer, do the following:

1. Place a request on the EA Workspace (EAWS).
2. Place a separate order for Cisco SD-WAN Controller stock keeping units (SKUs) using a la carte SKUs. See Cisco SD-WAN Controllers Ordering Guide for ordering details.
3. The Cisco CloudOps team validates the order details and provisions the overlay or directs you to Cisco Catalyst SD-WAN Portal for overlay provisioning.

Validation

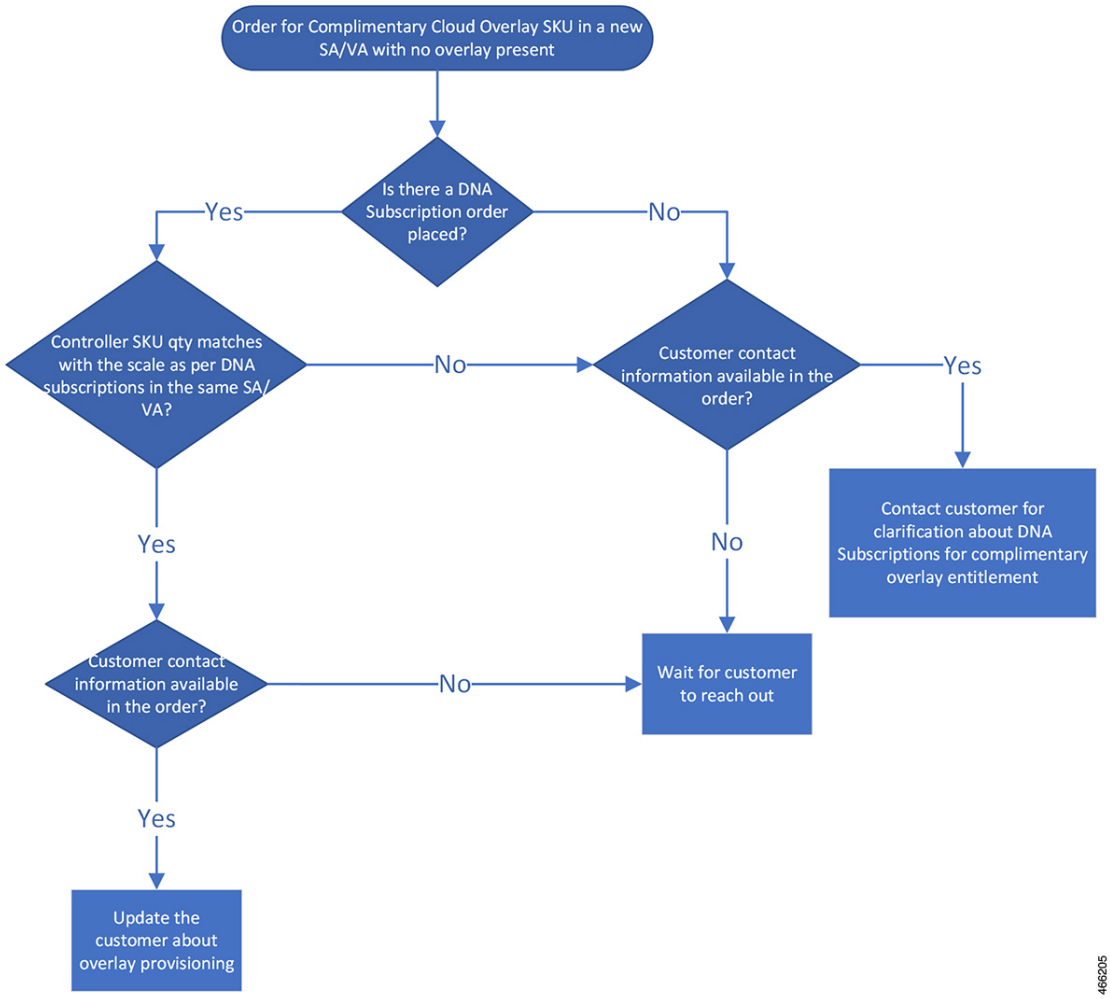
Complimentary Cisco Catalyst SD-WAN Cloud Controller SKU

Cisco CloudOps validates complimentary controller provisioning based on controller stock keeping units (SKUs) by checking the following items:

- Number of Cisco Digital Network Architecture (Cisco DNA) subscriptions that support the corresponding network scale (mandatory Cisco Catalyst SD-WAN subscription)
- Correct selection of controller SKUs for the corresponding network scale (number of devices)

If both the items are available and if they are compatible, Cisco CloudOps contacts the customer to gather more details required for controller provisioning. For this, the Cisco CloudOps team uses the contact information provided in the new order. When the required information is received from the customer, Cisco CloudOps proceeds with provisioning the cloud controllers.

Figure 3: Complimentary Cisco Catalyst SD-WAN Cloud Controller SKU Workflow



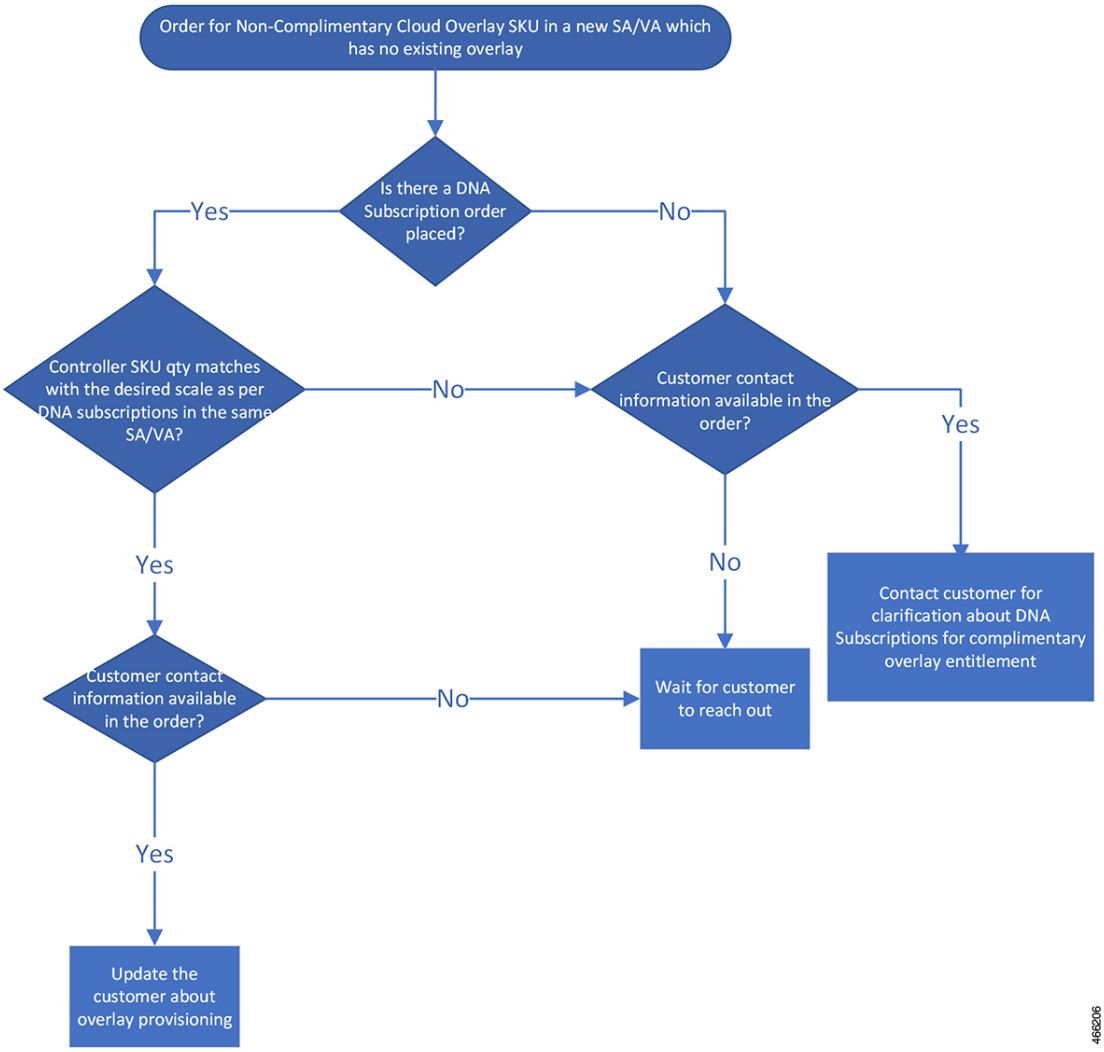
Non-Complimentary Cisco Catalyst SD-WAN Controller SKU

Cisco CloudOps validates non-complimentary controller provisioning based on controller stock keeping units (SKUs) by checking the following item:

- Correct selection of controller SKUs for the corresponding network scale (number of devices)

If the selected controller SKUs are compatible with the corresponding network scale, Cisco CloudOps contacts the customer to gather more details required for controller provisioning. For this, the Cisco CloudOps team uses the contact information provided in the new order. When the required information is received from the customer, Cisco CloudOps proceeds with provisioning the cloud controllers.

Figure 4: Non-Complimentary Cisco Catalyst SD-WAN Controller SKU Workflow

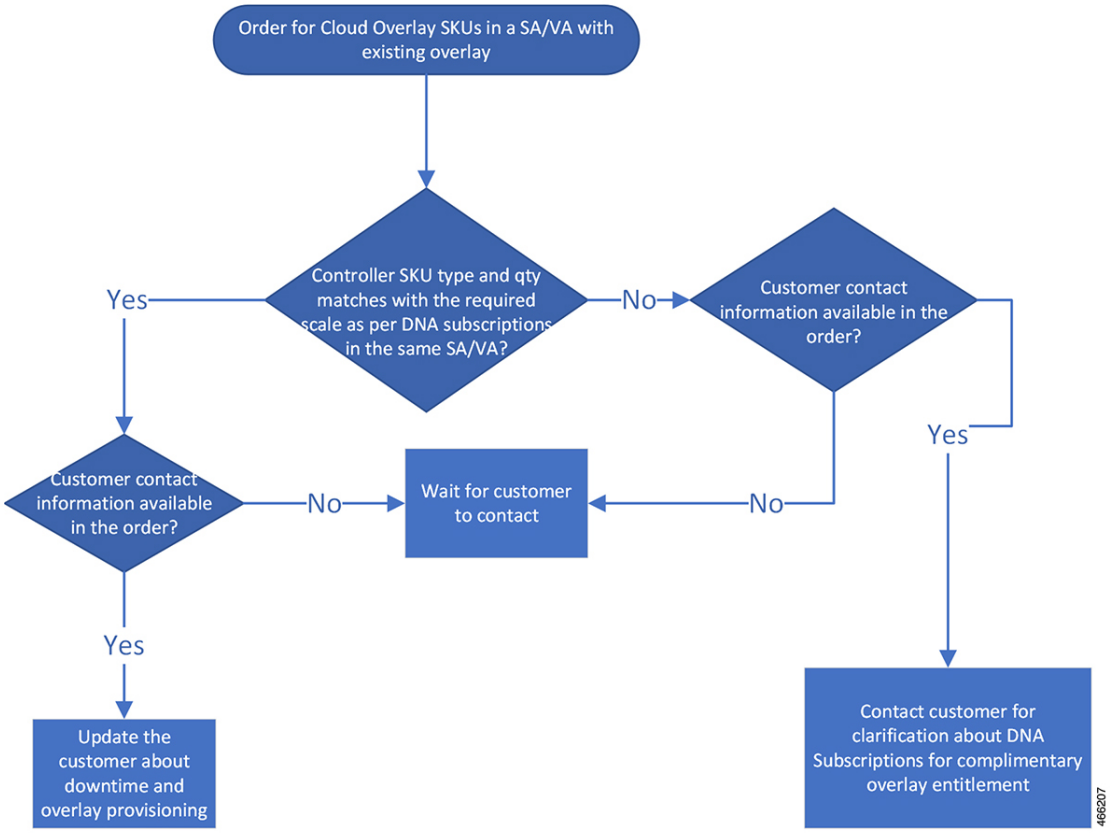


New Controllers in an Existing Overlay

Cisco CloudOps validates adding more computing resources (scale horizontally or vertically) based on controller stock keeping units (SKUs) by checking the following items:

- Correct selection of controller SKUs for the corresponding network scale (number of devices)
- Number of Cisco Digital Network Architecture (Cisco DNA) subscription that supports the corresponding network scale (mandatory Cisco Catalyst SD-WAN subscription for complimentary SKUs)
- The maintenance window because it requires downtime

Figure 5: New Controllers in an Existing Overlay Workflow



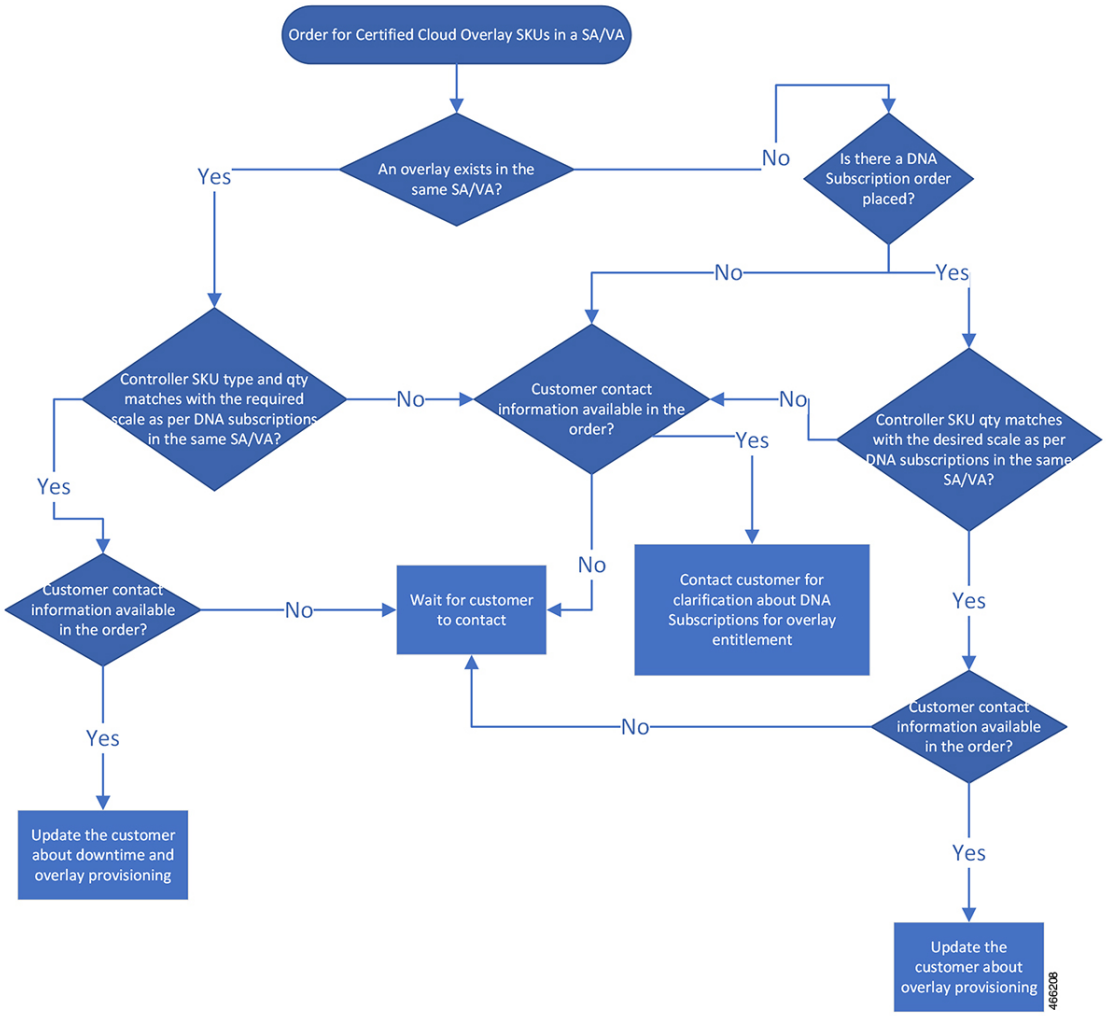
Controller in Certified Environment

Cisco CloudOps validates certified controller provisioning based on controller stock keeping units (SKUs) by checking the following items: :

- Correct selection of certified controller SKUs for the corresponding network scale (number of devices).
- CloudOps cross-checks for an order based on controller SKUs or existing controllers.
- The maintenance window because it requires downtime.

If the selected certified controller SKUs are compatible with both the selected controller SKUs or the existing controller and the network scale, Cisco CloudOps contacts the customer to gather more details required for controller provisioning. For this, the Cisco CloudOps team uses the contact information provided in the new order. When the required information is received from the customer, Cisco CloudOps proceeds with provisioning the cloud controllers.

Figure 6: Controller in Certified Environment Workflow



Account Management

Transfer Overlay to Another Account

To move an overlay from one Smart Account (SA) or Virtual Account (VA) to another SA or VA:

- Open a Cisco TAC support case for the migration request.
- Specify the SA and VA details for both the source and destination in the Cisco TAC case.

There is no downtime expected for this migration.

You can move the device serial numbers to the new SA or VA using the PNP **Transfer Selected** button, or you can open a Cisco TAC support case for assistance.

The functionality and the following details of the overlay do not change during this migration:

1. Organization name
2. Cisco SD-WAN Validator, Cisco SD-WAN Manager, or Cisco SD-WAN Controller DNS name
3. All current IPs assigned to all controllers
4. The entire Cisco SD-WAN Manager configuration, including certificates
5. Current allowed list of IP addresses

After the overlay migration, you may need to update the SA credentials configured in the Cisco SD-WAN Manager settings.

On-Premises to Cloud Migration Process Details

In the case, where an existing on-premise Cisco Catalyst SD-WAN overlay needs to be migrated to Cisco-provisioned cloud-hosted controllers, the process is outlined below:

Note This migration process is only supported for on-premise single tenant overlays to a cloud-hosted single tenant overlay controller set. This migration is not supported for shared tenant or multi-tenant overlays.

Overall Process

- Purchase Cisco DNA subscriptions for cloud and controller SKUs for cloud.
- You must open a Cisco TAC support case with the Cisco CloudOps team and request for the on-premises to cloud migration.
- You must provide details about the following:
  - Existing Smart Account (SA) and Virtual Account (VA) where the on-premises overlay controller profile is created.
  - The sales order number where cloud subscriptions were purchased.
  - Current on-premises configured organization name of overlay.
  - Choice of the required cloud type.
  - Choice of the required primary and secondary region of provisioning.
  - Single email address as contact for receiving alert notifications and other communications from the Cisco CloudOps team (team email address is preferred).
  - Optional choice of hostname for the FQDN of the Cisco SD-WAN Manager and the Cisco SD-WAN Validator to be provisioned.
  - Optional choice of custom private IP subnets required for TACACS/AAA/Syslog or other such use cases (provide a /24 IP prefix for each of the two regions of provisioning).
  - Current on-premises overlay fabric size in terms of number of edges deployed.

- Current on-premises overlay Cisco SD-WAN Manager, Cisco SD-WAN Validator, and Cisco SD-WAN Controller instances running software versions.
- Current on-premises overlay controller certificate source (Cisco/Symantec/Enterprise) root CA.
- Configuration database backup copy from the current on-premises overlay Cisco SD-WAN Manager.

Note You can either reset the Cisco SD-WAN Manager configuration database password to the default and then take the backup, or take the backup with your configured password and share that password on the Cisco TAC case.

- Copy of the running configuration from the current on-premises overlay Cisco SD-WAN Manager

  .
- Range of system-IP addresses to be used for cloud-hosted controllers (should be an unused range within the current on-premises Cisco Catalyst SD-WAN fabric).

- The Cisco CloudOps team provisions the cloud-hosted controller set, installs controller certificates, and shares details.
- The Cisco CloudOps team applies the configuration database backup and the running configuration provided from the on-premises Cisco SD-WAN Manager to the new cloud-hosted Cisco SD-WAN Manager instance.
- You may need to update your enterprise firewalls as required, with the new IPs of the cloud-hosted controllers.
- Set up and execute a pilot change window to migrate one or more test edge nodes to the cloud-hosted controllers and then roll back to the on-premises Cisco SD-WAN Manager.
- Migration is triggered by configuring the new Cisco SD-WAN Validator FQDN on the edge node.
- Take necessary measures to prepare for the final change window.
- Set up and execute a final change window to migrate all edge nodes from on-premises to cloud-hosted controller set.
- If templates were created and applied for the on-premises Cisco SD-WAN Manager, Cisco SD-WAN Validators, and Cisco SD-WAN Controllers, then they must be reviewed and corrected, before applying them to the cloud-hosted controllers, post migration. Special care must be taken with respect to the interface configuration.

Prerequisites

- Before opening a case, you must upgrade all your existing controllers and edge nodes to one of the latest Cisco-suggested release versions and verify that your data plane is stable.
- You must have all edge nodes attached to a template or agree to reconfigure the edge nodes manually for the migration.
- You must have all edge nodes with working NTP and DNS.
- You must provide the root CA to Cisco if in case you are using enterprise certificates on the on-premises controllers.

- You must have out-of-band access to edge nodes via console or an alternate way in case the edge nodes need manual configuration for recovery.

Considerations and Impact

- You must work with your Cisco Account Team or Cisco support to procure Cisco Catalyst SD-WAN cloud subscriptions and add them to the existing Smart Account (SA) and Virtual Account (VA) where the on-premises overlay controller profile is created.
- The Cisco CloudOps team provisions Cisco SD-WAN Manager only in the primary region.

  There is a Cisco SD-WAN Validator and Cisco SD-WAN Controller instance provisioned in both the primary and the secondary regions.
- The Cisco CloudOps team creates a new controller profile in the same SA/VA as the existing on-premises overlay.

  This allows the cloud-hosted controller set to have the same organization name as the existing on-premises overlay. This in turn makes it possible to transfer the configuration database from on-premises Cisco SD-WAN Manager to the cloud-hosted Cisco SD-WAN Manager.

  The configuration database restore method, otherwise, can't be used if the source and destination Cisco SD-WAN Manager instances have different organization name configured. Organization name on a cloud-hosted Cisco SD-WAN Manager instance can't be changed once provisioned.
- As the new Cisco SD-WAN Manager is configured using the configuration database restore method, the statistics database from the on-premises Cisco SD-WAN Manager will not be migrated.
- If Cisco SD-WAN Analytics is in use on the on-premises overlay, it continues to work.

  There may be some data loss when the migration happens, as the new cloud Cisco SD-WAN Manager starts fresh data collection and sends it to the Cisco SD-WAN Analytics servers.
- As the Cisco SD-WAN Validator FQDN changes, the configuration on the edge nodes requires to be updated for the migration.

  This can be done via CLI templates from Cisco SD-WAN Manager applied to all the edge nodes. If no CLI templates exist on the on-premises Cisco SD-WAN Manager, you must create and apply them before starting the migration. If you do not prefer CLI templates, then you would need to manually reconfigure all the edge nodes individually via console or ssh.
- If any issue occurs during the edge node migration, you may need to have an out-of-band management access to the edge nodes to make changes manually to switch over to new Cisco SD-WAN Validators.
- At the time of migration, the control and data plane flaps for each edge node as it is pointed to the new Cisco SD-WAN Validator DNS and reconnects to the new cloud-hosted controllers.
- It is mandatory that all edge nodes be configured with working NTP and DNS before the migration.
- Rollback plan would involve Cisco SD-WAN Validator configuration to be changed back on the edge nodes to the on-premises Cisco SD-WAN Validator.
- After successful migration, the controller profile that you hosted can be deleted from Cisco PNP SA/VA.

Cloud-Hosted Controller Deletion Policy

Cisco can delete a customer cloud-hosted controller overlay based on the following conditions:

Certificate Expiration

- **Identification Stage**: If your controller certificates have expired for 15 days or more, and if you have not renewed the certificates, Cisco can move your cloud-hosted controller to a shutdown state. The expired controller certificates indicate that the cloud-hosted controller overlay and the connected devices are not being used.
- **Final Termination**: If your overlay remains in the shutdown state for a period of at least three months, and if you have not made any communication to Cisco to recover the controllers, Cisco deletes the controllers. As a result, the customer data cannot be recovered.
- **Reprovisioning**: Once an overlay is deleted, it needs to be reprovisioned. If you have an active Cisco Digital Network Architecture (Cisco DNA) license, you can request a new cloud-hosted controller overlay.

Abandoned Overlays

- **Identification Stage**: If the cloud-hosted controllers are provisioned for six months or more and:

  1. if there are no active edge devices
  2. OR if the overlays are in the shutdown state for 30 days or more for reasons other than those set forth in this Cloud-Hosted Controller Policy

  then Cisco can deem your cloud-hosted controller as abandoned. Please note that no active edge devices or shutdown overlays indicate that the Cisco Catalyst SD-WAN overlay and the cloud-hosted controller devices are not being used.
- **Notification Stage**: Cisco sends notifications to you communicating the overlay abandoned state along with a target shutdown date.
- **Shutdown Stage**: If the customer overlay continues to remain unused even after the notifications, Cisco shuts down the overlay on the specified date.
- **Final Termination**: If you have not communicated to Cisco to recover Cisco Catalyst SD-WAN cloud-hosted controllers within 30 days of the overlay shutdown, Cisco deletes the controllers. As a result, the customer data cannot be recovered.
- **Reprovisioning**: Once an overlay is deleted, it needs to be reprovisioned. If you have an active Cisco Digital Network Architecture (Cisco DNA) license, you can request a new cloud-hosted controller overlay.

DNA Subscription Expired

This policy applies to Cisco Digital Network Architecture (Cisco DNA) subscriptions for the devices licensed before Cisco made the cloud controller subscription separately available. It is also known as Pre-Controller Subscription Offering.

- **Identification Stage**: If all the Cisco DNA subscriptions for your devices connected to the cloud-hosted controller have expired, Cisco can deem your corresponding cloud-hosted controller as subscription expired.

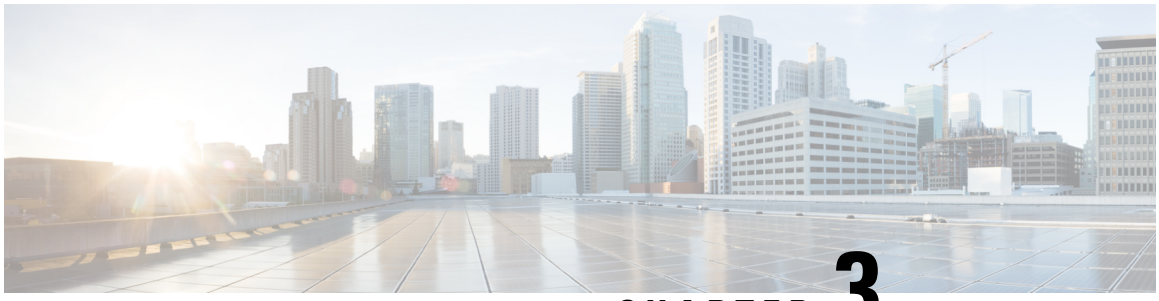
- **Notification Stage**: Cisco sends notifications to you communicating the overlay abandoned state along with a target shutdown date. Ensure that you keep your contact information up-to-date to receive timely notifications.
- **Shutdown Stage**: If the customer overlay continues to run with the expired DNA subscriptions even after the notifications, Cisco shuts down the overlay on the specified date.
- **Final Termination**: If you have not communicated to Cisco to recover your Cisco Catalyst SD-WAN cloud-hosted controllers within 30 days of the overlay shutdown, Cisco deletes the controllers. As a result, the customer data cannot be recovered.
- **Reprovisioning**: Once an overlay is deleted, it needs to be reprovisioned. You can purchase a new cloud-hosted controller overlay by purchasing the required stock keeping units (SKUs).

Controller Subscription Expired

A controller subscription is licensed separately from the Cisco Digital Network Architecture (Cisco DNA) subscriptions for devices.

- **Identification Stage**: If the subscription of your cloud-hosted controllers has expired, and if you have not renewed it, Cisco can deem your corresponding cloud-hosted controller as subscription expired.
- **Notification Stage**: Cisco sends notifications to you communicating the overlay abandoned state along with a target shutdown date. Ensure that you keep your contact information up-to-date to receive timely notifications.
- **Shutdown Stage**: If the controller subscription continues to remain unrenewed even after the notifications, Cisco shuts down the overlay on the specified date.
- **Final Termination**: If you have not communicated to Cisco to recover your Cisco Catalyst SD-WAN cloud-hosted controllers within 30 days of the overlay shutdown, Cisco deletes the controllers. As a result, the customer data cannot be recovered.
- **Reprovisioning**: Once an overlay is deleted, it needs to be reprovisioned. You can purchase a new cloud-hosted controller overlay by purchasing the required stock keeping units (SKUs).

Note Failure to renew your DNA subscription for the Cisco cloud-hosted controllers may impact the functionality of the Cisco Catalyst SD-WAN features that are part of the Cisco DNA subscription for your devices. It is because these features are dependent on Cisco SD-WAN Controllers.



CHAPTER 3

Certificate Management

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.

Web Server Certificates

Cisco does not issue web certificates for Cisco SD-WAN Manager. We recommend that you generate the Certificate Signing Request (CSR) and get it signed by your Certificate Authority (CA) for your Domain Name System (DNS) name. Then, you may either add an A entry in your DNS server for the IP, or a CNAME to the `.viptela.net / .sdwan.cisco.com` Cisco SD-WAN Manager DNS name.

Note The controller certificates issued by Cisco are for the controllers to use internally. You cannot use these certificates to issue web server certificates.

For more information, see the Web Server Certificates section in the Cisco Catalyst SD-WAN Getting Started Guide.

Renew Cisco Catalyst SD-WAN SSL Certificates for Controllers

Signed certificates are used to authenticate devices in the overlay network. After being authenticated, devices can establish secure sessions between each other.

Note The certificate renewal process is applicable only if you have a dedicated single tenant or multi-tenant controller overlay. This process is not applicable if you have a shared tenant overlay.

You can generate the Certificate Signing Request (CSR) as well as install the signed certificates, using Cisco SD-WAN Manager. There are 3 options for Certificate Root CA:

1. Cisco Root CA bundle (already present on controllers with software version 19.2.3 and above, Cisco Catalyst SD-WAN devices with software version 19.2.3 and above, Cisco IOS XE Catalyst SD-WAN devices with software versions 16.12.3+ or 16.10.4+ or 17.x+.
2. Symantec/Digicert Root CA (already present on all controllers, Cisco Catalyst SD-WAN devices and Cisco IOS XE Catalyst SD-WAN devices).
3. Your own Enterprise Root CA.

Note Select the certificate-generation method only once. The method you select is automatically applied each time you add a device to the overlay network.

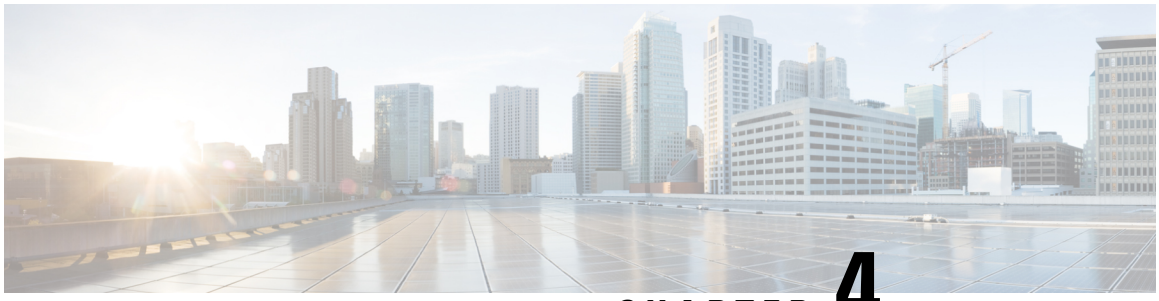
To renew the controller certificates, you need to follow the appropriate process based on your deployment type and certificate type:

- The controller certification authorization settings configure the certification- generation process for all controller devices. For more information, see Cisco Catalyst SD-WAN Controller Certificates.
- Note that since the certificate renewal involves an entire control plane flap, you are required to follow the instructions as per above, to renew the certificates, even for cloud hosted Cisco provisioned controllers.
- The Cisco CloudOps team does not automatically renew the certificates for the customers.
- On the Cisco SD-WAN Manager **Settings** page, there is an option for **Symantec Automated** or **Cisco Automated** where automated refers to automatic submission of CSRs and retrieval of certificates. The option does include automation of certain steps of the process, compared to the manual option. However, the step to trigger the generation of CSRs for each controller is still manual, to be done by you, to initiate the renewal process.
- Note that the Cisco SD-WAN Manager Dashboard shows a warning 6 months in advance that the certificates are about to expire.
- You can view the expiry date at any time at by choosing **Configuration** > **Certificates** > **Controllers** from the Cisco SD-WAN Manager menu.

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

- The Cisco CloudOps team sends email notifications 30/15/5 day prior to expiry, to the registered email address contact for the overlay in your system as well.

- You can open a case with us anytime to request the current registered email address or change it. We recommend that customers help keep the owner email address updated for all Cisco CloudOps notifications. We recommend keeping us updated with the customer contact email address for alert notifications, preferably a team mailer address instead of an individual user email address.
- Also, we recommend being aware of the controller certificate expiry dates and plan for renewal atleast a 1 month before expiry.



CHAPTER 4

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.

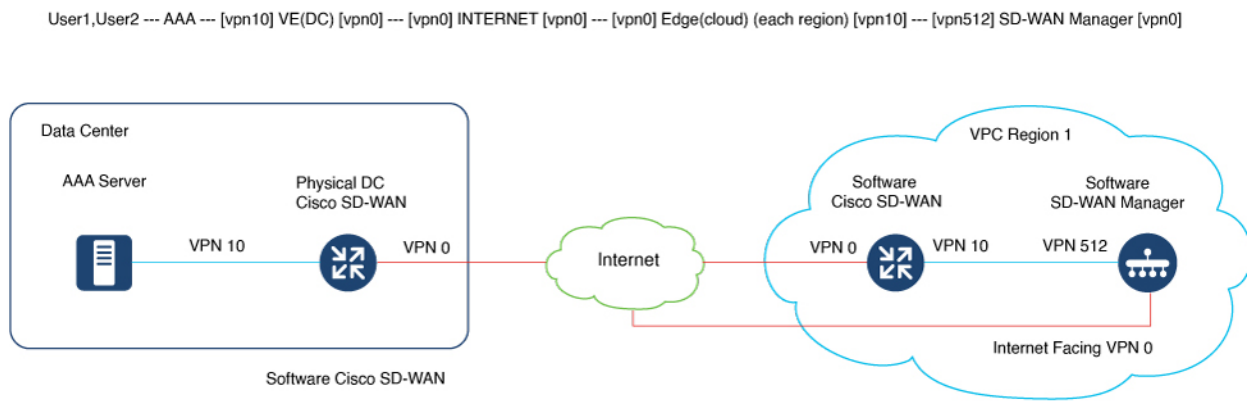
Custom IP Prefixes for Cloud Hosted Controllers

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 7: 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.

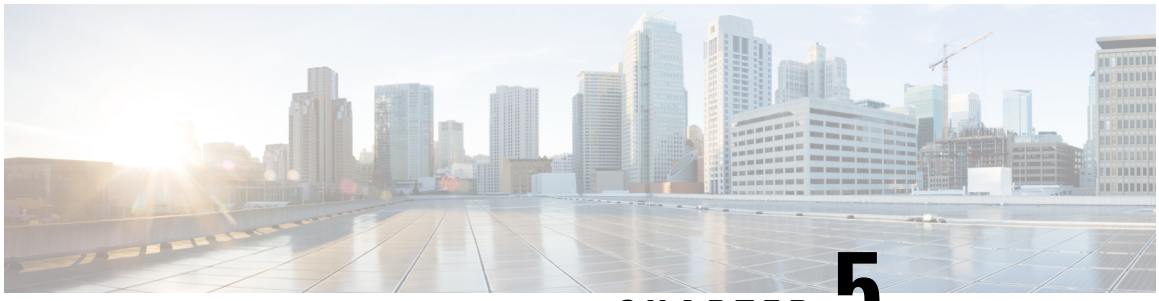
   If you don't have any cloud gateway UUID available in the WAN Edge Device list on your Cisco SD-WAN Manager, then you may need to login into the Cisco PNP portal, on the overlay's associated Smart Account and Virtual Account, and Add Software Devices (VEDGE-CLOUD-DNA) and then Sync Smart Account on the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



CHAPTER 5

Monitoring

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.

Monitor the Cisco Catalyst SD-WAN Cloud-Hosted Controllers

Cloud hosted controller monitoring covers the following:

- Infrastructure monitoring of the following:
  - CPU and data disk utilization.
  - Loss of connectivity to network interfaces.
  - Failure to reach instances.
- Service monitoring of the following:
  - Expiration of controller SSL certificates.
  - Availability of the Cisco SD-WAN Manager web server.
  - Loss of control connection to the controllers.

Health Monitoring of Overlays with Cisco SD-WAN Manager Version below 20.3.x

The cloud monitoring is performed as a part of the Cisco Catalyst SD-WAN cloud-hosting services to ensure the availability of the Cisco SD-WAN Controllers. By default, Cisco SD-WAN Manager is configured with a user called `viptelatac` with `operator` privileges. Cisco uses this user to login to Cisco SD-WAN Manager and to collect and monitor the health of Cisco Catalyst SD-WAN.

The Cisco SD-WAN Manager audit log displays periodic logins from the monitoring system using the `viptelatac` user. The monitoring service uses RestAPIs to collect health information from Cisco SD-WAN Manager.

In case you want to disable the Cisco cloud monitoring system, you can open a Cisco TAC case with the Cisco Catalyst SD-WAN Cloud Infra team, requesting to disable the cloud monitoring. Once the monitoring is disabled, you can also remove the configured `viptelatac` user from the Cisco SD-WAN Manager.

Cisco Cloud Infra team will also use the `viptelatac` user to login to the Cisco SD-WAN Manager to do additional health checks, triage issues in response to internally generated alerts, as well as to assist with customer opened TAC cases.

Health Monitoring of Overlays with Cisco SD-WAN Manager Version Running at or above 20.3.x

From Cisco SD-WAN Release 20.3.1 release onwards, push based model is used.

In this model, the monitoring architecture uses Cisco SD-WAN Manager to authenticate with the system to send the health data. Cisco SD-WAN Manager pushes the data instead of monitoring system logging into the Cisco SD-WAN Manager with the `viptelatac` user. In order for this to work, you need to explicitly provide consent on the Cisco SD-WAN Manager settings page, as well as configure a One Time Password (OTP). The `viptelatac` user is not needed once Cisco SD-WAN Manager is upgraded to 20.3.1 or above.

You can login to Cisco SD-WAN Manager and perform the follwing steps:

1. Go to **Settings** > **Cloud Services** > **Enable**
2. Enter the OTP value. You can request the token from the Cisco CloudOps team by opening a Cisco TAC Support case.
3. Leave the Cloud Gateway URL blank.
4. Check the **vMonitoring** to enable monitoring.
5. Approve permission to collect the data regarding health status of the overlay from Cisco SD-WAN Manager.

For version 20.3.x and above, Cisco Cloud Infra team will use the `ciscotacro` and `ciscotacrw` user to login to the Cisco SD-WAN Manager to do additional health checks, triage issues in response to internally generated alerts, as well as to assist with the customer opened TAC cases. The same user will also be used to perform automated infrastructure upgrades and certain software updates based on pre-notified changes to the customer contacts for the overlay.

The `ciscotacro` user has read-only *operator* group privilege while `ciscotacrw` has read-write *netadmin* group privilege. For certain enhanced debugging, cloud infrastructure upgrades and management, Cisco Cloud Infra team needs to use the `ciscotacrw` user.

Only specific Cisco support teams have the ability to login via these users and they are based on a token challenge and token response based password mechanism i.e., the two users are not based on static passwords.

In case, you want to disable this access on any of the Cisco Catalyst SD-WAN fabric controllers, you can remove the user from the configuration at any time. However, this will limit Cisco ability to triage the issues.

Alert Notifications by CloudOps

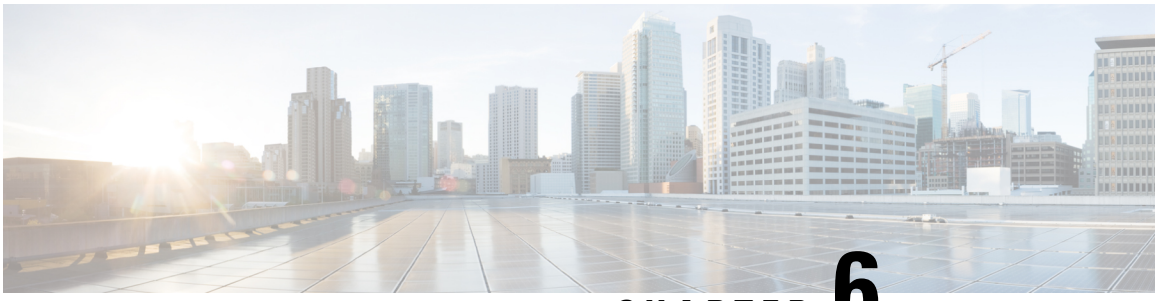
CloudOps team manages the infrastructure of the cloud hosted instances and help with the monitoring and backend infrastructure maintenance. However, CloudOps team does not make changes or manage the running software version or configuration of the instances.

CloudOps team may send alert notifications to customers, based on any issues seen, which may indicate either software issue or misconfiguration or some features overutilizing the capacity, which CloudOps team is not aware of. Customers may be running their own tests, changes, or configuration updates, that the team is not aware of.

CloudOps team will therefore, only notify the customers instead of taking direct action on the hosted controller instances, and request customer to open a Cisco TAC support case for assistance and evaluation as needed. Once the customer has a TAC case open, Cisco TAC and thereafter, CloudOps team, can work together with the customer, to resolve the issue as needed.

Update Overlay Contact for Receiving Alert Notifications

- Every Cisco provisioned cloud-hosted overlay has a single customer contact email address registered as the owner, to receive CloudOps Alert notifications.
- By default, the contact email address provided on the Cisco Sales Order's End Customer details has been used as the owner contact.
- Customers can open a Cisco TAC case to review or update the contact at any time.
- For Cisco-hosted, cloud-based, dedicated, single tenant controllers, you can directly update the owner contact email address through the Cisco Catalyst SD-WAN Portal.
- We support only one email address contact as the owner contact and hence it is recommended that you provide a group mailing list email address.



CHAPTER 6

Cloud Infrastructure

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.

Cisco Cloud-Hosted Controller Snapshots

Cisco takes regular snapshots of the cloud hosted Cisco SD-WAN Manager controller managed by Cisco, based on the snapshot frequency. The snapshot frequency is set by default to once every day, typically midnight of the region of deployment, and the last 10 snapshots are retained. The snapshot frequency can be configured from once a day, to upto once in 4 days. For more information on Snapshots, see Information About Snapshots.

You can open a Cisco TAC support case with the Cisco CloudOps team to review the current snapshot setting or change it on the Cisco Catalyst SD-WAN Portal. You can retain only a maximum of last 10 periodic snapshots. The Cisco Catalyst SD-WAN Controller and Cisco SD-WAN Validator are stateless and therefore snapshots are not taken. It is recommended that their configurations can be done via templates on Cisco SD-WAN Manager for disaster recovery.

You cannot download the snapshots as snapshots are stored within the Cisco cloud account. However, you can download the config-db backup file from Cisco SD-WAN Manager and save the configurations including templates using command request nms configuration-db backup path.

Note Since, Cisco SD-WAN Validator and Cisco Catalyst SD-WAN Controller are stateless, snapshots are not captured. Use Cisco SD-WAN Manager template to configure and save Cisco SD-WAN Validator and Cisco Catalyst SD-WAN Controller Configuration settings.

Take an On-demand Snapshot

Note The on-demand snapshot process is applicable only for overlays with Cisco-hosted, cloud-based, dedicated, single tenant controllers. This is not applicable if you have a shared tenant overlay.

For any major planned change windows for Cisco SD-WAN Manager, You can take on-demand snapshot using Cisco Catalyst SD-WAN Portal. This can be requested via opening a Cisco TAC support case with the Cisco CloudOps team. You need to freeze the configuration changes and allocate up to eight hours prior to the change window to allow the on-demand snapshot to be taken and completed. We can store up to one on-demand snapshot. We can store this on-demand snapshot for a period of 3 months from the date of creation of the snapshot. Also, each time a new on-demand snapshot is taken, the previous one, if present, is automatically removed and replaced with the new one.

Cisco Catalyst SD-WAN Analytics

Refer to Cisco Catalyst SD-WAN Analytics.

Pen Test

Customers with overlay controllers in AWS can conduct their own pen tests for the Cisco Catalyst SD-WAN solution without approval using:

- https://aws.amazon.com/security/penetration-testing/

Customers with overlay controllers in Azure can conduct their own pen tests for the Cisco Catalyst SD-WAN solution without approval using:

- https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement

Mandatory Maintenance of Cloud-Hosted Controllers

The Cisco CloudOps team sends email notices to customers for mandatory reboot of a specific cloud-hosted controller managed by Cisco, only when hosted in AWS. Sometimes, maintenance is required on the instances and rebooting the instances prior to the cloud provider's maintenance window. It allows you to move them from the current hardware node requiring maintenance, to a new healthy hardware node, to avoid disruption of service.

The Cisco CloudOps team then sends notifications to the registered email address of the customer, which is a single email address registered for an overlay within the Cisco CloudOps system. Note that this registered

email address is configured initially using the original Sales Order's **End Customer Email Address** field and can be updated anytime by logging into the Cisco Catalyst SD-WAN Portal (link to https://ssp.sdwan.cisco.com). This registered email address is not derived from Cisco SD-WAN Manager Settings page.

You can reschedule to update the change window, as long as the requested date and time is before the cloud provider's maintenance window time. The amount of advance notice is not guaranteed and depends on the severity of the issue on the hardware node on cloud provider side.

Cisco Catalyst SD-WAN Disaster Recovery Guidelines

- Cisco Catalyst SD-WAN disaster recovery is based on Cisco SD-WAN Manager disk volume snapshots or configuration database backups.
- These configuration database backups and volume snapshots are taken each daily, typically around midnight time of the location of the Cisco SD-WAN Manager instance and securely stored on cloud.
- For Cisco SD-WAN Release 20.3.x and later, you can turn off configuration database backup feature, if desired, and take own backups and make them available to CloudOps when needed for recovery of the service.
- Cisco SD-WAN Manager disk volume snapshots are taken every night and sometimes on-demand for customer request or at start of major change windows. Each Cisco SD-WAN Manager has two or more disks and a snapshot of each of the volumes is taken at the exact same time to form an overall backup of the Cisco SD-WAN Manager instance. The snapshots, once completed, in the region where the Cisco SD-WAN Manager is running, are then copied over to the designated backup region, usually a different geographic region.

  For example, Cisco SD-WAN Manager may be running in US-East and backup region may be designated as US-West. The backup region is essentially the same region, where the second Cisco Catalyst SD-WAN Validator and Cisco Catalyst SD-WAN Controller are already running.
- Cisco Catalyst SD-WAN Validator and Cisco Catalyst SD-WAN Controller are stateless services and have a CLI-managed configuration or Cisco SD-WAN Manager provide configuration and hence they aren't backed up.
- There's no standby or active Cisco SD-WAN Manager service in a backup region. Three or six node cluster offers high availability of Cisco SD-WAN Manager, running within the same availability zone and region.
- Cisco Catalyst SD-WAN Validator and Cisco Catalyst SD-WAN Controller services are deployed in primary and backup regions. Both Cisco Catalyst SD-WAN Validator and Cisco Catalyst SD-WAN Controller work in active mode. The device and policy information is pushed to both the instances from Cisco SD-WAN Manager. When one region fails, Cisco Catalyst SD-WAN Controller and Cisco Catalyst SD-WAN Validator continue to function fine in the backup region.
- Cisco Catalyst SD-WAN is designed for the data plane to continue to function even if all the controllers fail. GR (Graceful Restart) timer configuration enables the high availability of the data plane. GR timer is configured to hold on to the routes advertised by Cisco Catalyst SD-WAN Controllers, by default for 12hrs. We recommend Cisco Catalyst SD-WAN customers to choose GR timer value judiciously to allow controllers to be back up in case of failures, and at the same time be able to learn the new routes from changed network configurations.
- Configuration database-based recovery method when used, allows only templates and policies to be restored. Volume-based recovery is used to include the stats data collected as well.

Volume Snapshot based Recovery Process

- Once determined that the Cisco SD-WAN Manager instance needs to be replaced with a backup, we can initiate the Disaster Recovery (DR) process.
- For DR at same region, Cisco pick the same region and same datacenter as the existing Cisco SD-WAN Manager instance location.

  We also specify the time/date of the snapshot set to use, based on requirement and availability.
- Once DR triggers, the system first shuts down the existing Cisco SD-WAN Manager instance.
- System then uses the volume snapshots to create a new cloud instance with the same set of disks, same instance size specifications, same private subnets, same security access-list, same isolated environment as that of the original Cisco SD-WAN Manager. Once the instance is up, the system swaps the public IPs from the old shutdown Cisco SD-WAN Manager instance to the new Cisco SD-WAN Manager instance.
- Overall, the new running Cisco SD-WAN Manager instance has the same public IPs, but new private IPs and have the same software version, same configuration, same data, as that present at the time when snapshot is taken.
- Cisco SD-WAN Manager has the necessary information to join the fabric. You can use the same FQDN/URL to log in into the Cisco SD-WAN Manager instance as before.
- For DR to the backup region, in the unlikely case where the primary region of Cisco SD-WAN Manager has failed and unavailable, we use the exact same process, except that the backup cloud region is selected.
- The difference with DR to backup region is that, once the new Cisco SD-WAN Manager instance is running in backup region, there's no swapping of public IPs from old region to new region. Cloud regions have a specific public IP pool per region and can't be assigned to instances across regions.

  Therefore, the new DR Cisco SD-WAN Manager instance in backup region, has new public IPs. The system updates the FQDN/DNS with the new public IP of the Cisco SD-WAN Manager.

  In this case, you may need to update the enterprise end firewall with the new public IP of the Cisco SD-WAN Manager.

Configuration Database backup by Cisco CloudInfra System

- Prior to Cisco vManage Release 20.3.1, the configuration database was backed up only if:
  - Monitoring is enabled in Cisco CloudInfra system. If 'viptelatac' user is unusable on the Cisco SD-WAN Manager for any reason, monitoring gets disabled, and customers are notified with request for correction.
  - The 'viptelatac' user must be usable on the Cisco SD-WAN Manager.
  - The configuration database size is lesser than 4GB.
- Cisco vManage Release 20.3.1 and later, the configuration database is backed up only if:
  - Monitoring is enabled in Cisco CloudInfra system.

Note In Cisco SD-WAN Manager, if the cloud service is disabled for any reasons, then monitoring gets disabled on Cisco CloudInfra system and customers are notified with request for correction.

- From the Cisco SD-WAN Manager menu, choose **Adminstration** > **Settings**, and enable Cloud Services and vMonitoring along with OTP added in the same section.
- In the Cisco SD-WAN Manager CLI, the **`nms configuration-db daily-backup`** service is enabled.
- The configuration database size is lesser than 4GB.

Configuration Database based Recovery Process

- If volume snapshot is not viable for DR for any reasons, then Cisco uses the configuration database recovery process. Cisco creates a brand new Cisco SD-WAN Manager instance and use the configuration database backup to restore the original configuration files. With this method, the statistics database of the original Cisco SD-WAN Manager instance is not restored. This method restores your templates and policies configuration. The new Cisco SD-WAN Manager instance in this case has both new public IPs and new private IPs.
- We update the FQDN/DNS of the Cisco SD-WAN Manager to use the new public IP of the new instance.
- In this case, you may need to update the enterprise end firewall with the new public IP of the Cisco SD-WAN Manager.
- The process for using disaster recovery method using configuration database backup remains same for both same region and backup region recovery.
- For process details, see Troubleshooting TechNotes.