Cisco Catalyst SD-WAN CloudOps Guide

Cisco SD-WAN
Updated September 3, 2026

Topics included

1 Cisco CloudOps Overview

Topics:

About Cisco CloudOps

Explains how Cisco cloud services and the CloudOps team streamline cloud-hosted network operations and enhance deployment and management for Cisco Catalyst SD-WAN control components.

Cisco provides a cloud-hosted subscription service for its Cisco Catalyst SD-WAN control components. This service streamlines and speeds up deployment. It also lowers operational costs and includes instance monitoring and advanced analytics capabilities.

Cisco CloudOps is the support team and automated framework that manages the "underlying fabric" of the cloud service. Their primary goal is to ensure that the cloud infrastructure is always on, secure, and up-to-date.

About This Guide

Network design engineers and network operators interested in purchasing or deploying Cisco Catalyst SD-WAN cloud-based subscription options can use this guide to learn about the capabilities and services of the cloud-hosted Cisco Catalyst SD-WAN control components managed by Cisco. It covers the hosting processes for the cloud infrastructure, assigned responsibilities, and pertinent recommendations.

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.

Types of fabric network in Cisco Catalyst SD-WAN

Lists and describes the available fabric network types in Cisco Catalyst SD-WAN, including Cloud, Cloud-Pro, and Cloud-MSP, noting key features and distinctions.

Cisco Catalyst SD-WAN supports several fabric network types. Each fabric type offers specific capabilities and deployment options:

Cisco SD-WAN Cloud fabric

In a Cisco SD-WAN Cloud fabric, the control components are hosted and managed by Cisco. This fabric type is best for customers who prefer to focus on their edge device networking instead of cloud control component infrastructure operations.

Cisco SD-WAN Cloud fabrics always run on the long-lived recommended software releases, providing reliability and stability.

The Cloud fabric is mapped to the customer's Smart Account and Virtual Account for easier device onboarding, utilizing the external management capabilities of their Virtual Account.

Cisco SD-WAN Cloud-Pro fabric

In addition to the capabilities of a Cisco SD-WAN Cloud fabric, a Cisco SD-WAN Cloud-Pro fabric allows you to access these options:

- Isolated/Private instance of SD-WAN control components.
- Specific software versions.
- AWS or Azure for a Cloud provider and specific location from available Cloud provider regions for deployment of Control Components.
- Ability to choose your control component software upgrade schedule.
- Commercial certifications, such as PCI DSS, C5, ENS, CC, and TxRAMP.

Cisco SD-WAN Cloud-MSP fabric

In this type of fabric, the hosting of control components (Cisco SD-WAN Manager, Cisco SD-WAN Validator, and Cisco SD-WAN Controller) is dedicated to Managed Service Providers (MSPs). The MSP hosts and manages tenants within this multitenant environment for their end-customers.

> **Note**
>
> A Cisco SD-WAN Cloud-MSP fabric can be hosted only on the AWS cloud provider.

Coverage and responsibilities in cloud management

Provides a comparison of tasks and the parties responsible for cloud management, including Cisco SD-WAN Cloud, Cloud-Pro, and Cloud-MSP services. Any functions not listed here are not monitored by Cisco. In this table, "CloudOps" refers to the Cisco SD-WAN CloudOps team.

Table 1: Coverage and responsibilities in cloud management

This table summarizes which parties are responsible for key tasks in Cisco SD-WAN Cloud management across different service models.

Task	Cisco SD-WAN Cloud	Cisco SD-WAN Cloud-Pro	Cisco SD-WAN Cloud-MSP	Comments
Provision fabrics				
Provision fabrics from Cisco Catalyst SD-WAN Portal	Customer	Customer	CloudOps	-
Monitor and troubleshoot cloud control components infrastructure				
Monitor CPU and data disk utilization	CloudOps			-
Troubleshoot loss of connectivity to network interfaces	CloudOps			-

Task	Cisco SD-WAN Cloud	Cisco SD-WAN Cloud-Pro	Cisco SD-WAN Cloud-MSP	Comments
Troubleshoot failure to reach instances	CloudOps			-
Monitor Cisco Catalyst SD-WAN services				
Provide expiration notification of control component SSL certificates	CloudOps			-
Monitor availability of the Cisco SD-WAN Manager web server	CloudOps			-
Troubleshoot loss of control connection to the control components	CloudOps			-
Manage capacity of Cisco Catalyst SD-WAN control components	CloudOps			CloudOps monitors and upgrades the instance capacity according to the number of devices on the fabric. Cluster expansion may occur.
Disaster Recovery				
Capture periodic volume snapshots	CloudOps			In multitenancy, volume snapshots apply to the entire multitenant Cisco SD-WAN Manager cluster, not to individual tenants.
Capture periodic configuration backups	CloudOps			In multitenancy, configuration backups apply to the entire multitenant Cisco SD-WAN Manager cluster, not to individual tenants.
Capture on-demand snapshots	-	Customer	Customer	-
Restore fabric based on volume or configuration	CloudOps			-
Upgrade software				
Upgrade control component software	CloudOps	CloudOps *	CloudOps *	* We perform upgrades only to recommended releases.
Upgrade edge device or node software	Customer			-

Task	Cisco SD-WAN Cloud	Cisco SD-WAN Cloud-Pro	Cisco SD-WAN Cloud-MSP	Comments
Upload and manage edge images in Cisco SD-WAN Manager Software Repository	CloudOps	Customer	Customer	-
Other tasks				
Onboard Cisco SD-WAN Analytics	Not applicable *	Customer	Customer	* Cisco SD-WAN Analytics is onboarded by default for all Cisco Catalyst SD-WAN deployments.
Assist with on-premises to cloud migration	CloudOps			For more details on the on-premises to cloud migration, refer to On-Premises to Cloud Migration Process Details on the Cisco website.
Configure custom subnets and TACACS	-	Customer	Customer	Set up custom subnets and TACACS during Day-0 provisioning. For Day-N, you can open a TAC case with CloudOps. TACACS is available for Cisco SD-WAN Cloud-MSP fabrics via MT-Edge. Refer to the Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide for more information.
Renew control component certificates	CloudOps	Customer *	Customer *	* CloudOps can help renew certificates when requested.
Create Smart Accounts (SA) or Virtual Accounts (VA) on `software.cisco.com` and attach Cisco Catalyst SD-WAN subscribed devices to the SA and VA	Customer			-
Allow external management of SA and VA on PNP Connect	Customer	-	-	Do not allow external management of SA and VA on PNP Connect before provisioning a fabric in Cisco Catalyst SD-WAN Portal. The provisioning workflow automatically enables the external management.

Task	Cisco SD-WAN Cloud	Cisco SD-WAN Cloud-Pro	Cisco SD-WAN Cloud-MSP	Comments
Accept external management of SA and VA and map tenant VA to your SA and VA	CloudOps	–	–	–
Define device configuration templates and policies through Cisco SD-WAN Manager	Customer			–
Manage certificates for web servers	CloudOps	Customer *	Customer **	* CloudOps can help renew certificates when requested. ** CloudOps can renew web certificates if the Cisco SD-WAN Cloud-MSP fabric is deployed in the cisco.com domain.
Sync edge serials with credentials	Not applicable *	Customer	Customer	* Cisco SD-WAN Cloud customers can use their Cisco Connection Online (CCO) login credentials for SSO and syncing edge serials.
Manage the allowed IP access list	–	Customer	Customer	
Configure a custom identity provider (IdP)	–	Customer	Customer	Cisco SD-WAN Cloud fabrics only support CCO as an identity provider. You can use SSO to navigate among Catalyst SD-WAN applications such as Cisco SD-WAN Manager, Cisco SD-WAN Analytics, and Cisco Catalyst SD-WAN Portal.

Cloud solution architectures

Explains how Cisco Catalyst SD-WAN Control Components are deployed and organized in a cloud solution for fabrics with fewer than 1,500 devices.

A cloud solution architecture is a deployment model that

- automatically provisions key SD-WAN control components in the public cloud,
- separates resources across primary and backup regions for resilience, and
- provides administrator access to manage and maintain the environment.

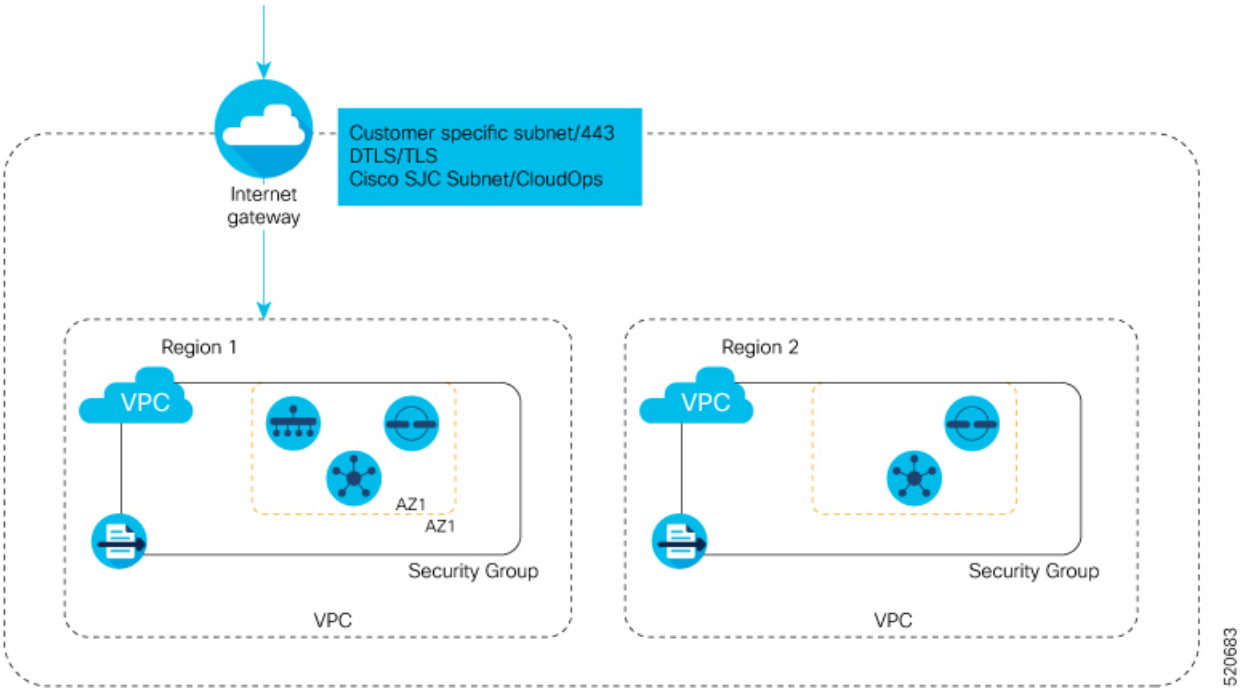
Cloud deployment details

When you choose a cloud-based subscription for your Cisco Catalyst SD-WAN Control Components, we deploy, by default, one Cisco SD-WAN Manager, two Cisco SD-WAN Validators, and two Cisco SD-WAN Controllers on the public cloud, for a fabric with fewer than 1,500 devices. We then provide 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. An additional Cisco SD-WAN Validator and Cisco SD-WAN Controller are deployed in the secondary or backup region.

Note

For recommended computing resources, refer to Recommended Computing Resources for Cisco Catalyst SD-WAN Control Components on the Cisco website.

Figure 1: Cloud solution architecture



Supported clouds and cloud regions in AWS and Azure

Lists the supported clouds and cloud regions in AWS and Azure for Cisco Catalyst SD-WAN control component deployments.

These clouds and cloud regions are supported for Cisco Catalyst SD-WAN control component deployments:

Table 2: Supported clouds and cloud regions for Cisco SD-WAN Cloud fabrics

Amazon Web Services (AWS)
Asia Pacific (APAC)
Europe (EU)
United States (US)

Amazon Web Services (AWS)
Africa

Table 3: Supported clouds and cloud regions for Cisco SD-WAN Cloud-Pro fabrics

Amazon Web Services (AWS)	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–Sydney | Australia	Asia Pacific | South India
Asia Pacific–Melbourne | Australia	UAE North–Dubai
Asia Pacific–Tokyo | Japan	Asia Pacific | Australia Central–Canberra
Africa–Cape Town	South Africa–North
Canada Central–Montreal | Canada	Canada Central–Montreal | Canada
Canada West–Calgary | Canada	Canada East
EU–Frankfurt | Germany	Americas | Brazil South–Sao Paulo State
EU–Ireland | Dublin	Europe | France Central–Paris
EU–London | United Kingdom	Europe | North Europe–Ireland
EU–Stockholm | Sweden	Europe | UK South–London
South America–São Paulo | Brazil	Europe | West Europe–Netherlands
US East–Northern Virginia | United States	Americas | East US–Virginia
US West–Northern California | United States	Americas | West US–California
US West–Oregon | United States	Americas | West US 2–Washington

> **Note**
>
> The listing reflects current support as verified. Regions awaiting support verification are not included.

Customer responsibilities in Cisco SD-WAN cloud management

Lists the key customer responsibilities required for maintaining Cisco SD-WAN cloud services, which affect the validity of the SD-WAN Cloud SLA and service uptime.

You must fulfill specific responsibilities to maintain guaranteed SLA and service uptime for cloud management. Failure to meet these requirements will invalidate the SD-WAN Cloud SLA, including any service uptime guarantees.

Your main responsibilities include:

- Manage the allowed access-list with your source public IP ranges for management access of control components.
- Renew control component certificates on time.
- Before you make any changes in the Cisco Catalyst SD-WAN Portal, capture an on-demand snapshot by using the Take an On-Demand Snapshot procedure. Then, back up the configuration using the Back Up the Active Cisco SD-WAN Manager procedure.
- Upgrade the software.

  Open a Cisco Technical Assistance Center (TAC) case if you face any issues with software upgrade, or want a version 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 you create and attach templates to the Cisco SD-WAN Validator and Cisco SD-WAN Controller instead, so that the Cisco SD-WAN Manager backups automatically include the configuration backup of the control components.

  The Cisco Catalyst SD-WAN support teams can assist with the control component software upgrade for all deployment types.

  It is your responsibility to upgrade the software version of an edge device. For the compatible versions of edge devices based on control component versions, refer to Cisco SD-WAN Control Components Compatibility Matrix.
- Respond to notifications sent by the CloudOps team to authorize the service window, approve an instance reboot, review changes, or verify changes carried out by the CloudOps team.
- For a Cisco SD-WAN Cloud-Pro fabric, configure the third interface on Cisco SD-WAN Manager with a static IP or a DHCP-based IP to use it for Software Defined Application Visibility and Control (SD-AVC). By default, the third interface is in the shutdown state.
- Open a TAC case to arrange a service window when you receive a notification from the CloudOps team. Some operations require your consent before they can be performed.
- Create Smart Accounts or Virtual Accounts on `software.cisco.com` and attach Cisco Catalyst SD-WAN subscribed devices to them.
- Define device configuration templates and policies, and perform other activities that require logging into Cisco SD-WAN Manager.

- For a Cisco SD-WAN Cloud fabric, open a Cisco TAC support case if you need specific software versions to be added in the Cisco SD-WAN Manager software repository.

Meeting these responsibilities ensures compliance with the SD-WAN Cloud SLA and maintains all associated service guarantees.

Cisco CloudOps cloud management responsibilities

Lists Cisco CloudOps responsibilities for fabric provisioning, monitoring, troubleshooting, capacity management, and cloud infrastructure support in Cisco SD-WAN cloud environments.

Cisco CloudOps provides a structured approach to managing and supporting cloud-hosted SD-WAN infrastructures. Their responsibilities cover fabric provisioning, real-time monitoring, troubleshooting, disaster recovery, capacity management, and cloud infrastructure support. These help ensure reliable network operation and optimal cloud service performance.

Fabric provisioning responsibilities

- Provision cloud-hosted control components for your Cisco Catalyst SD-WAN fabric, configure a unique admin password with an expiration time of one week, and hand over Cisco SD-WAN Manager to you.
- Configure Cisco SD-WAN Manager with a default template and policy when you choose the default template and policy push option on the sales order.
- Create and manage Cisco SD-WAN Cloud, Cisco SD-WAN Cloud-Pro, and Cisco SD-WAN Cloud-MSP clusters as needed.
- For direct enterprise customers, manage tenants on Cisco SD-WAN Cloud-MSP fabrics.

Monitoring and troubleshooting responsibilities

- Use a real-time monitoring system to check the health of Cisco Catalyst SD-WAN control components and generates alerts. The check includes the health of Cisco SD-WAN Manager, application servers, web servers, other microservices, and configuration or statistics databases.
- Take proactive action for cloud infrastructure issues, which are beyond your control. Otherwise, notify you about the potential issues and request that you open a Technical Assistance Center (TAC) support case for further investigation.
- Manage alerts based on notifications from the cloud provider environments on instance status, CPU inactivity status, or network inactivity status.
- Resolve the alerts proactively if it doesn't require a down time of the services and notify you when services experience intermittent disruptions.
- Send renewal notices to you thirty, fifteen, and five days before certificate expiration on Cisco SD-WAN Manager. Your Cisco Catalyst SD-WAN control component certificates remain valid for one year.

Cloud infrastructure support responsibilities

- Carry out disaster recovery workflows, such as creating snapshots of volumes or configurations. Restore Cisco SD-WAN Manager clusters based on these snapshots.
- Provision custom subnetting to extend your on-premises network into the cloud-hosted fabric's network.
- Manage on-premises-to-cloud migrations.

Capacity management responsibilities

- Monitor the growth of devices per fabric and control component instance capacity parameters such as CPU, disk, and memory utilization.
- Increase the capacity of the service instances according to a preset guideline when needed.

This reference enables quick understanding of the specific operational and support activities that Cisco CloudOps undertakes to maintain, supervise, and enhance Cisco SD-WAN cloud environments.

2 Order, License, and Manage Fabrics

Topics:

Fabric ordering, licensing, and management

Describes the process of ordering, licensing, and managing network fabrics, including procurement procedures, license activation requirements, and ongoing fabric administration tasks.

Fabric ordering, licensing, and management is a comprehensive process that involves procurement procedures, license activation requirements, and ongoing fabric administration tasks.

Order Cisco Catalyst SD-WAN cloud-hosted controllers

Provides the conditions for creating Cisco Catalyst SD-WAN cloud-hosted control components for a sales order.

The Cisco SD-WAN Portal allows you to create the Cisco Catalyst SD-WAN cloud-hosted control components for a sales order when all of these conditions are met:

- The sales order includes cloud subscription licenses for edge nodes and Cisco SD-WAN Control Components. SKUs are required for additional paid control components.
- Cisco Catalyst SD-WAN items in the sales order are marked as **Shipped**.
- The sales order is assigned to an active Smart Account (SA). Within that SA, it is assigned to a Virtual Account (VA).

> **Note**
>
> Plug and Play replaces the legacy Salesforce (SFDC) process for ordering Cisco Catalyst SD-WAN.
>
> Refer to the Cisco Plug and Play Support Guide and Cisco Catalyst Software-Defined WAN (SD-WAN) FAQ on the Cisco website for information about Cisco Catalyst SD-WAN Plug and Play.

License types and ordering information

Lists the types of licenses and contracts used with Cisco Catalyst SD-WAN fabrics and explains how to order them.

There are two types of licenses and contracts:

- **A la carte:** Purchase DNA Cloud (DNA-C) licenses and SD-WAN Control Component stock-keeping units (SKUs), if required.
- **Enterprise Agreement (EA):** Purchase an EA bundle that includes SD-WAN Control Component SKUs (if required).

If you prefer to purchase a la carte licenses for SD-WAN Control Components, refer to the Cisco Catalyst SD-WAN Controller Ordering Guide.

To provision a Cisco Catalyst SD-WAN cloud-hosted control component for an Enterprise Agreement (EA) customer, place a request on the EA Workspace (EAWS).

License requirements for various Cisco Catalyst SD-WAN fabric configurations

Lists the license requirements for different Cisco Catalyst SD-WAN fabric types in certified and non-certified environments.

This reference provides license requirements for different Cisco Catalyst SD-WAN fabric types in certified and non-certified environments, covering both the first fabric associated with the Smart Account and additional fabrics.

First fabric

Table 4: License requirements for the first fabric associated with the smart account

For these requirements...		Here's what you need...		
SD-WAN fabric type	**Certified environment?**	**SD-WAN Control Components SKUs** [1]	**Device licenses** [2]	**Comments**
Cisco SD-WAN Cloud	No	No SKU requirements	Each device requires a DNA-C license.	
Cisco SD-WAN Cloud-Pro [3]	No	Contact your Cisco Sales representative or channel partner for assistance.	Each device requires a DNA-C license.	Contact your Cisco Sales representative to determine if your network specifications require a Cisco SD-WAN Cloud-Pro fabric.
	Yes	Contact your Cisco Sales representative or channel partner for assistance.	Each device requires a DNA-C license.	In a certified environment, a Cisco SD-WAN Cloud-Pro fabric is required.

Additional fabrics

Table 5: License requirements for the second or subsequent fabrics associated with the Smart Account

For these requirements...		Here's what you need...		
SD-WAN fabric type	**Certified environment?**	**SD-WAN Control Components SKUs** [4]	**Device licenses** [5]	**Comments**
Cisco SD-WAN Cloud	No	No SKU requirements	Each device requires a DNA-C license.	

[2] Refer to the Cisco DNA Software for SD-WAN and Routing Ordering Guide for information about ordering DNA-C licenses.
[1] Refer to the Cisco Catalyst SD-WAN Control Components Ordering Guide.
[3] Setting up a Cisco SD-WAN Cloud-Pro fabric requires opening a TAC case with the Cloud Infra Team.
[5] Refer to the Cisco DNA Software for SD-WAN and Routing Ordering Guide for information about ordering DNA-C licenses.
[4] Refer to the Cisco Catalyst SD-WAN Control Components Ordering Guide.

For these requirements...		Here's what you need...		
SD-WAN fabric type	**Certified environment?**	**SD-WAN Control Components SKUs**[4]	**Device licenses**[5]	**Comments**
Cisco SD-WAN Cloud-Pro[6]	No	Contact your Cisco Sales representative or channel partner for assistance.	Each device requires a DNA-C license.	Contact your Cisco Sales representative to determine if your network specifications require a Cisco SD-WAN Cloud-Pro fabric.
	Yes	An SD-WAN Control Components license is required.	Each device requires a DNA-C license.	In a certified environment, a Cisco SD-WAN Cloud-Pro fabric is required.

Transfer a fabric to another account

Configure migration of an SD-WAN fabric between Smart Account and Virtual Account instances.

Move an SD-WAN fabric and associated devices to a different Smart Account or Virtual Account.

Use this task when organizational changes require transferring fabrics between accounts to maintain accurate record-keeping and access control.

Procedure

1. Open a Technical Assistance Center (TAC) case to request the migration.
2. Specify the SA and VA details for both the source and destination in your TAC case.

This migration does not cause downtime.

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

The function of the fabric and these configuration details do not change after the migration:

- Organization name
- Cisco SD-WAN Validator, Cisco SD-WAN Manager, or Cisco SD-WAN Controller DNS name
- All current IPs assigned to all control components
- The entire Cisco SD-WAN Manager configuration, including certificates
- The current list of allowed IP addresses

[5] Refer to the Cisco DNA Software for SD-WAN and Routing Ordering Guide for information about ordering DNA-C licenses.
[4] Refer to the Cisco Catalyst SD-WAN Control Components Ordering Guide.
[6] Setting up a Cisco SD-WAN Cloud-Pro fabric requires opening a TAC case with the Cloud Infra Team.

What to do next

After the fabric migration, update the SA credentials configured in the Cisco SD-WAN Manager settings as needed.

Migrate an on-premises fabric to the cloud

Configure the migration of an SD-WAN fabric from on-premises deployment to Cisco Catalyst SD-WAN Cloud, including licensing, account settings, and device templates.

Move an existing SD-WAN fabric from on-premises to cloud-hosted control components for improved scalability and manageability.

Use this migration when upgrading infrastructure, consolidating management, or aligning licensing with cloud services.

Before you begin

- Before opening a case, upgrade all your existing control components and edge nodes to one of the latest Cisco-suggested release versions.
- Verify that your data plane is stable.
- Attach all edge nodes to a template or agree to manually reconfigure the edge nodes for the migration.
- Make sure that all edge nodes have working NTP and DNS.
- If you are using enterprise certificates on the on-premises control components, provide the root certificate authority (CA).
- Ensure you have out-of-band access to edge nodes via console or an alternate way, in case the edge nodes need manual configuration for recovery.

Procedure

1. Purchase a DNA subscription and control component SKUs for cloud.
2. Open a TAC support case with the CloudOps team and request the on-premises to cloud migration. Provide these details in the case:
   - The existing Smart Account (SA) and Virtual Account (VA) where the on-premises fabric control component profile is created.
   - The sales order number where the cloud subscriptions were purchased.
   - The current on-premises configured organization name of the fabric.
   - Your desired cloud type and primary and secondary region of provisioning.
   - A single email address to receive alert notifications and other communications from the CloudOps team. Provide a team email address if possible.
   - An optional hostname for the FQDN of the Cisco SD-WAN Manager and the Cisco SD-WAN Validator to be provisioned.
   - Optional custom private IP subnets for TACACS, AAA, Syslog, or other such use cases. Provide a block of 256 IP addresses (a /24 prefix) for each region.
   - The current on-premises fabric size expressed as the number of edge devices deployed.
   - The software versions of the Cisco SD-WAN Manager, Cisco SD-WAN Validator, and Cisco SD-WAN Controller instances running on the current on-premises fabric.

- The control component certificate source (Cisco, Symantec, or Enterprise) root CA of the current on-premises fabric.
- A configuration database backup copy from Cisco SD-WAN Manager of the current on-premises fabric.

  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 in the TAC case.

- A copy of the running configuration from the current on-premises fabric Cisco SD-WAN Manager
- A range of system-IP addresses to be used for cloud-hosted control components. This should be an unused range within the current on-premises Cisco Catalyst SD-WAN fabric.

When you have provided the necessary details, the CloudOps team provisions the cloud-hosted control component set, installs control component certificates, and shares details.

The CloudOps team applies the configuration database backup and the running configuration you provided from the on-premises Cisco SD-WAN Manager to the new cloud-hosted Cisco SD-WAN Manager instance.

3. You may need to update your enterprise firewalls with the new IPs of the cloud-hosted control components.
4. Set up and execute a pilot change window to migrate one or more test edge nodes to the cloud-hosted control components. Then roll back to the on-premises Cisco SD-WAN Manager.
5. Configure the new Cisco SD-WAN Validator FQDN on the edge node to begin the migration.
6. Prepare for the final change window as necessary.
7. Set up and execute a final change window to migrate all edge nodes from on-premises to cloud-hosted control component set.
8. If templates were created and applied for the on-premises Cisco SD-WAN Manager, Cisco SD-WAN Validators, and Cisco SD-WAN Controllers, review and correct them before applying them to the cloud-hosted control components after migration, with special attention to the interface configuration.
9. The edge templates created and applied for the on-premises Cisco SD-WAN Manager contain the pre-migration orchestrator FQDN when the database is restored to the new Cisco SD-WAN Manager. Update the target Cisco SD-WAN Manager to reflect the post-migration orchestrator FQDN.

What to do next

Work with your Account Team or 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 fabric control component profile is created.

The Cisco SD-WAN Manager is provisioned only in the primary region. The Cisco SD-WAN Validator and Cisco SD-WAN Controller instances are provisioned in both the primary and the secondary regions.

The CloudOps team creates a new control component profile in the same SA/VA as the existing on-premises fabric. This allows the cloud-hosted control component set to have the same organization name as the existing on-premises fabric, which makes it possible to transfer the configuration database from on-premises Cisco SD-WAN Manager to the cloud-hosted Cisco SD-WAN Manager.

You cannot use the configuration database restore method if the source and destination Cisco SD-WAN Manager instances have different organization names configured. You cannot change the organization name on a cloud-hosted Cisco SD-WAN Manager instance once it is provisioned.

Since 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 fabric, it will continue to work after the migration.

Some data loss may occur when the migration happens because the new cloud Cisco SD-WAN Manager starts a 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 must be updated for the migration.

You can do this using command-line interface (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 must manually reconfigure all the edge nodes individually via console or Secure Shell (ssh).

If an issue occurs during the edge node migration, you may need to use out-of-band management access to manually update the edge nodes so they can 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 control components.

Configure all edge nodes with functioning NTP and DNS before the migration.

Rolling back requires changing the Cisco SD-WAN Validator configuration on the edge nodes back to the on-premises Cisco SD-WAN Validator.

After a successful migration, you can delete the control component profile that you hosted from the PNP SA/VA.

Cloud-hosted control component deletion conditions

Lists the scenarios and criteria under which cloud-hosted SD-WAN control component fabrics are deleted, as well as the recovery or reprovisioning steps.

Your cloud-hosted control component fabric may be automatically deleted under one of these conditions:

Control component certificates have expired

- Identification Stage: If your control component certificates have been expired for 15 days or more, and you have not renewed them, your cloud-hosted control component may be moved to a shutdown state. The expired control component certificates indicate that the cloud-hosted control component fabric and the connected devices are not being used.
- Final Termination: If your fabric stays in the shutdown state for at least 30 days, and you do not request to recover the control components, the control components are deleted, and your data cannot be recovered.
- Reprovisioning: After a fabric is removed, you must reprovision it. If you have an active Cisco Digital Network Architecture (Cisco DNA) license, you can request a new fabric.

Fabrics are abandoned

- Identification stage: If you have cloud-hosted control components that have been provisioned for six months or more without active edge devices, or if fabrics remain in the shutdown state for 30 days or more for reasons other than those described in the Cloud-Hosted Control Component Policy, your control components may be considered abandoned.

  If you do not have active edge devices or your fabrics are shut down, your Cisco Catalyst SD-WAN fabric and cloud-hosted control component devices are considered to be unused.
- Notification stage: We will send notifications to you communicating the fabric abandoned state along with a target shutdown date.
- Shutdown stage: If your fabric continues to remain unused even after the notifications, we will shut down the fabric on the specified date.

- Final termination: If you have not requested to recover Cisco Catalyst SD-WAN cloud-hosted control components within 30 days of the fabric shutdown, we will delete the control components, and your data cannot be recovered.
- Reprovisioning: Once an fabric has been deleted, it must be reprovisioned. You can request a new cloud-hosted control component fabric if you have an active Cisco Digital Network Architecture (Cisco DNA) license.

The Cisco DNA subscription has expired

This policy applies to Cisco Digital Network Architecture (Cisco DNA) subscriptions for devices that were licensed before we made cloud control component subscriptions available separately. This is known as Pre-Controller Subscription Offering.

- Identification Stage: If all Cisco DNA subscriptions for your devices connected to the cloud-hosted control component have expired, your cloud-hosted control component is considered to have an expired subscription.
- Notification Stage: We will notify you about the expired subscription and provide a target shutdown date. Keep your contact information current to receive timely notifications.
- Shutdown Stage: If your fabric continues to run with the expired subscription after you receive notifications, your network fabric will be shut down on the specified date.
- Final Termination: If you do not recover your Cisco Catalyst SD-WAN cloud-hosted control components within 30 days after network fabric shutdown, we will delete the control components. Your data will not be recoverable.
- Reprovisioning: Once a fabric is deleted, you must reprovision it. To obtain a new cloud-hosted control component fabric, purchase the required stock-keeping units (SKUs).

A control component subscriptions has expired

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

- Identification Stage: If your cloud-hosted control component subscription has expired and you have not renewed it, your control component is considered subscription expired.
- Notification Stage: We will send notifications that communicate the expired subscription and specify a shutdown date. Keep your contact information current to receive timely notifications.
- Shutdown Stage: If you do not renew the control component subscription after the notifications, your network fabric will be shut down on the specified date.
- Final Termination: If you do not recover your Cisco Catalyst SD-WAN cloud-hosted control components within 30 days of the fabric shutdown, we will delete the control components. Your data will not be recoverable.
- Reprovisioning: Once a network fabric is deleted, you must reprovision it. You can purchase a new cloud-hosted control component fabric by purchasing the required stock-keeping units (SKUs).

Note

Failure to renew your DNA subscription for cloud-hosted control components may impact the functionality of the Cisco Catalyst SD-WAN features that are part of the Cisco DNA subscription for your devices, because these features depend on Cisco SD-WAN control components.

3 Certificates

Topics:

About Certificates

Explains what certificates are and their role in fabric networks, including authentication and security.

A certificate is a digital security credential that

- enables authentication between devices in a fabric network,
- establishes secure communication sessions, and
- ensures compliance with certificate management policies.

Certificate management in fabric networks

Certificates are key to device authentication in Cisco SD-WAN fabric networks. Once authenticated, devices can safely exchange information. Certificate management involves generating Certificate Signing Requests (CSRs), obtaining signatures from Certificate Authorities (CAs), and installing the certificates per deployment requirements.

In commercial deployments, create a DNS A entry or CNAME for the .viptela.net or .sdwan.cisco.com DNS name. In government deployments, use the sdwangov.fedramp.cisco DNS name.

Control component certificates are used internally and should not be used for web server authentication. Only web server certificates are used for web server authentication.

Web server certificates

Explains the purpose, issuance, and management of web server certificates in Cisco SD-WAN environments.

A web server certificate is a digital authentication credential that

- ensures secure access to the web server,
- is issued via a Certificate Signing Request (CSR) signed by a trusted Certificate Authority (CA), and
- is associated with a specific DNS name for the deployment environment.

Certificate generation and deployment requirements

Web server certificates are not automatically issued for Cisco SD-WAN Manager. Generate the Certificate Signing Request (CSR) and get it signed by your Certificate Authority (CA) for your Domain Name System (DNS) name. For commercial deployments, add an A entry in your DNS server for the IP address, or add a CNAME to the `.viptela.net` or `.sdwan.cisco.com` Cisco SD-WAN Manager DNS name. For government deployments, use `sdwangov.fedramp.cisco`.

> **Note**
>
> Control component certificates are for internal control component use only. Use web server certificates for web server authentication.

Refer to "Web Server Certificates" in the *Cisco Catalyst SD-WAN Getting Started Guide* for more information.

Cisco Catalyst SD-WAN SSL certificates for control components

Explains how Cisco SD-WAN SSL certificates are used for authenticating and securing control components within SD-WAN fabric.

A Cisco Catalyst SD-WAN SSL certificate is a device authentication credential that

- verifies the identity of control components in the SD-WAN fabric,
- enables secure sessions between devices, and
- is managed via automated, manual, or enterprise root CA processes.

Certificate authentication and management

Signed certificates authenticate devices in the fabric network. After devices are authenticated, they can establish secure sessions with each other.

> **Note**
>
> If you have a Cisco SD-WAN Cloud-Pro single tenant or multi-tenant control component fabric, use this certificate renewal process. Do not use this process for a shared-tenant fabric.

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

- The Cisco Root CA bundle is present on control components with software version 19.2.3 and above, Cisco Catalyst SD-WAN devices with software version 19.2.3 and above, and Cisco IOS XE Catalyst SD-WAN devices with software versions 16.12.3+ or 16.10.4+ or 17.x+.
- The Symantec/Digicert Root CA is present on all control components, Cisco Catalyst SD-WAN devices and Cisco IOS XE Catalyst SD-WAN devices.
- Your own Enterprise Root CA.

> **Note**
>
> You select the certificate-generation method only once. The method you select is automatically applied each time you add a device to the fabric network.

To renew the control component certificates, use the appropriate process for your deployment type and certificate type.

The control component certification authorization settings determine how certificates are generated for control component devices. For more information, refer to Cisco Catalyst SD-WAN Control Component Certificates.

Because certificate renewal causes a control plane flap, always follow these certificate renewal instructions, even if you are using Cisco SD-WAN Cloud-Pro control components.

You must renew your certificates; the CloudOps team does not renew them for you. On the Cisco SD-WAN Manager **Settings** page, you can choose **Symantec Automated** or **Cisco Automated**. "Automated" refers to automatic submission of CSRs and retrieval of certificates. The option automates certain steps of the process, compared to the

manual option. However, you must manually trigger the generation of CSRs for each control component to initiate the renewal process.

The Cisco SD-WAN Manager Dashboard displays a certificate expiration warning 6 months in advance. You can view the expiration date at any time at by choosing **Configuration** > **Certificates** > **Controllers** from the Cisco SD-WAN Manager menu.

> **Note**
>
> As of 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 CloudOps team sends email notifications to the registered contact for your fabric 30 days, 15 days, and 5 days prior to expiration.

You can open a case to request or change the current registered email addresses. Keep the owner email address current for all CloudOps notifications, and keep the customer contact email address current for alerts. Use team addresses rather than individual user addresses if possible.

Check the control component certificate expiration dates and schedule the renewal at least one month before expiration.

4 Provision Control Components

Topics:

Access permissions for cloud-hosted control components

Provides the requirements and options for granting management access to Cisco-managed cloud-hosted control components.

Cisco-managed cloud-hosted control components are, by default, closed for management access. To permit access, configure specific public IP prefixes within your enterprise VPN. The universal IP address range (0.0.0.0/0) is not permitted for security reasons. Only those IP prefixes that are specifically listed in the allow list can access management interfaces; you may also specify that only HTTPS and SSH protocols are permitted for your source IP prefixes.

Key facts about allow lists:

- The allow list applies to all network interfaces with public IP addresses on control components.
- Cisco SD-WAN Cloud-Pro control components have private IP addresses mapped one-to-one to public IP addresses in the cloud.
- IP addresses assigned to the control components remain the same unless the instance is recovered or replaced.
- Smart Account administrators can view and modify control component IP access lists via the SD-WAN Service Portal.

To remove Smart Account administrator privileges, use the Manage Smart Account section in Cisco Software Central. Trusted users may be added using the identity provider (IDP) onboarding feature for access to the Cisco Catalyst SD-WAN Portal.

Update allow lists

For shared tenant fabrics, open a TAC support case to update or view the allow list for your control component set. Support can permit up to five IP prefixes or restrict HTTP access for web login.

For single-tenant dedicated fabric control components:

- Log in to the Cisco Catalyst SD-WAN Portal at https://ssp.sdwan.cisco.com to manage the access list. You must be the Cisco PNP Smart Account administrator for the Smart Account where the fabric control component profile resides.
- Provide up to 200 IP prefixes for inclusion in the allow list.
- Alternatively, contact TAC and supply information including Fabric and VA name, Cisco SD-WAN Manager IP address or FQDN, specific IP address, and desired protocol restrictions.

Cloud-hosted SD-WAN control component interfaces

Lists the network interface allocations, IP address assignments, and recommended configurations for cloud-hosted SD-WAN control components.

Network interface allocation for SD-WAN control components

For SD-WAN Manager instances, we allocate three network interfaces: eth0, eth1, and eth2.

For SD-WAN Validator and SD-WAN Controller instances, we allocate two network interfaces: eth0 and eth1.

Public and private IP addresses assigned to the network interfaces remain static. If you replace or move an SD-WAN control component instance to a new region, these addresses may change.

You can view the static IP address using the Catalyst SD-WAN Portal, from **Overlay Details** > **Controller view** > **Private IP**.

Recommended interface configurations
Table 6: Interface configuration

Control Component	Network interface 1 (eth0) Management access	Network interface 2 (eth1) Control access by nodes in fabric	Network interface 3 (eth2) Communication among SD-WAN Manager instances in a cluster; SD-AVC component functionality
SD-WAN Manager	**Private IP** Static pre-assigned address (Refer to Note 1.) **Public IP** Static pre-assigned address One-to-one NAT mapping to private IP address **Configuration requirements** ▪ VPN 512 ▪ Non-tunnel interface ▪ Configure the interface to act as a DHCP client. (Refer to Note 2.)	**Private IP** Static pre-assigned address **Public IP** Static pre-assigned address One-to-one NAT mapping to private IP address **Configuration requirements** ▪ VPN 0 ▪ Tunnel interface ▪ Configure the interface to act as a DHCP client. (Refer to Note 2.)	**Private IP** Static pre-assigned address **Public IP** None assigned **Configuration requirements** ▪ VPN 0 ▪ Non-tunnel interface ▪ Configure with a static IP. Use the assigned private IP address. View the static IP address using the Catalyst SD-WAN Portal, from **Overlay Details** > **Controller view** > **Private IP**.
SD-WAN Validator	Use the same configuration as for SD-WAN Manager.	Use the same configuration as for SD-WAN Manager.	Not applicable.
SD-WAN Controller	Use the same configuration as for SD-WAN Manager.	Use the same configuration as for SD-WAN Manager.	Not applicable.

Note

1: A cloud gateway deployed using the Catalyst SD-WAN Portal can access this address. For details, refer to the Custom IP prefixes for cloud-hosted SD-WAN control components section in this guide.

2: The interface always receives the same private IP on every DHCP renewal, even when DHCP is used for IP assignment.

Cloud-hosted SD-WAN control component access

Provides guidelines for edge device and management access to cloud-hosted SD-WAN control components, including VPN interface configuration and domain name usage.

Edge device access to SD-WAN control components

Use the VPN 0 tunnel interface to connect edge devices to SD-WAN control components.

Configure edge devices to communicate with SD-WAN control components using Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS) ports.

Firewall configuration

If your deployment includes an on-premises firewall, enable traffic on any safe IP address range, such as 0.0.0.0, for these TLS or DTLS ports. Alternatively, enable traffic to the current public IP addresses of the cloud-based SD-WAN control components.

> **Note**
>
> To find the assigned public IP address, log in to the Catalyst SD-WAN Portal and navigate to: **Overlay Details** > **Controller view** > **Public IP**.

For more information about TLS and DTLS ports, refer to the "Ports Used by Cisco Catalyst SD-WAN Devices Running Multiple vCPUs" section in the *Cisco Catalyst SD-WAN Getting Started Guide*.

Management access to SD-WAN Manager

Connect to SD-WAN Manager for management access using fully qualified domain names (FQDNs) mapped to the VPN 512 public IP.

If the fabric is provisioned with a three-node or six-node SD-WAN Manager cluster, then the FQDN resolves to the public IP addresses of all of the SD-WAN Manager instances.

HTTPS access for SD-WAN Manager

You can access SD-WAN Manager using HTTP or HTTPS. You cannot access other SD-WAN control components by HTTP or HTTPS.

Domain names for SD-WAN Manager and SD-WAN Validator

In a Cloud-hosted SD-WAN environment, domain names are assigned only to SD-WAN Manager and SD-WAN Validator for cloud hosting.

Access SD-WAN Validator by domain name

When you configure nodes in the SD-WAN fabric, use the FQDN of the SD-WAN Validator. Do not use the IP address. Using the domain name ensures continued reliable operation in case the SD-WAN Validator IP addresses change or more SD-WAN Validators are added to the fabric.

DNS server recommendation

Configure a DNS server accessible in VPN 0 for all nodes in the SD-WAN fabric, including hardware and software edge devices and control components.

Example DNS configuration:

```
vpn 0
   dns 208.67.222.222 primary
   dns 208.67.220.220 secondary
```

Configure access to SD-WAN Validator

Provides the command formats and best practices for configuring access to SD-WAN Validator nodes on SD-WAN components and edge devices.

To configure access to SD-WAN Validator on other nodes in the network, such as SD-WAN Manager, SD-WAN Controller, and edge devices, use this command format:

```
system
   vbond validator-domain-name
```

Include your SD-WAN Validator domain name. Do not use a static IP address.

For VPN 0, specify a DNS server IP that can resolve the SD-WAN Validator domain name:

```
vpn 0
   dns dns-server-ip primary
```

Do not assign a static host IP to the SD-WAN Validator with the `ip host` command.

Note

To view the FQDN of the SD-WAN Validator for your fabric using the Catalyst SD-WAN Portal, open **Overlay Details** > **Description** > **vBond DNS**. Note that **vBond** may be replaced by **SD-WAN Validator**.

Custom IP prefixes for cloud-hosted control components

Explains how to assign custom IP prefixes to cloud-hosted control component interfaces and the implications for management access and service configuration.

A custom IP prefix is a network allocation that

- enables tailored management and control access for cloud-hosted control component interfaces,
- allows secure configuration of AAA (Authentication, Authorization, and Accounting) and TACACS authentication, and
- must be specified to avoid conflicts with existing fabric subnets.

Custom IP prefix configuration requirements

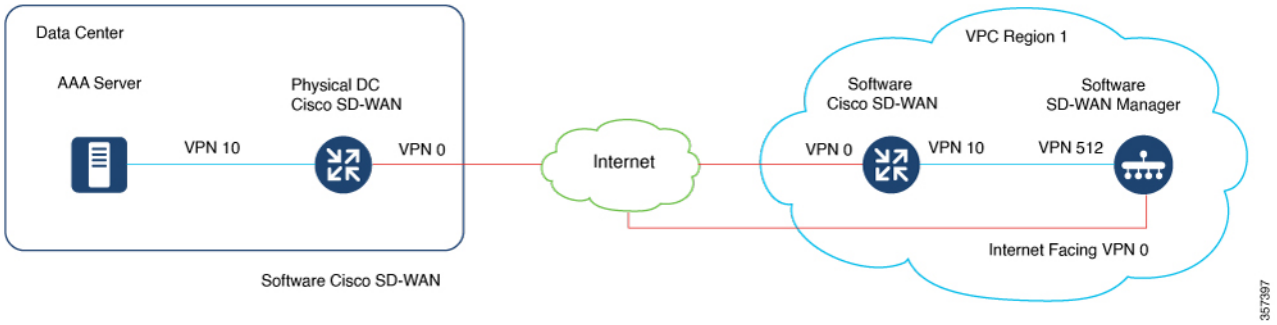
Custom IP prefixes apply only to Cisco-managed, cloud-based, dedicated single tenant control components. They are not used for shared tenant fabrics.

Assign custom network prefix-based IPs to the cloud control component interfaces for management access and control if necessary. For example:

- accessing the management VPN 512 of Cisco SD-WAN Manager and Cisco SD-WAN Validator or Cisco SD-WAN Controller devices over a Cisco Catalyst SD-WAN tunnel with Authentication, Authorization, and Accounting (AAA) or Terminal Access Controller Access-Control System (TACACS) based authentication, or
- sending syslog data from Cisco SD-WAN Manager on VPN 512 to a syslog server over a Cisco Catalyst SD-WAN tunnel.

Figure 2: AAA TACACS

User1,User2 --- AAA --- [vpn10] VE(DC) [vpn0] --- [vpn0] INTERNET [vpn0] --- [vpn0] Edge(cloud) (each region) [vpn10] --- [vpn512] SD-WAN Manager [vpn0]



By default, Cisco-managed cloud-hosted control components use 10.0.0.0/16-based subnets, including for VPN 512.

If you add the cloud Cisco Catalyst SD-WAN and make the VPN 512 subnet reachable within your fabric, you might encounter a conflict with an existing subnet.

If this occurs, you must share a /24 prefix for each of the two control component deployment regions. Use these IP prefixes to create control components. You can then use the subnets within the Cisco Catalyst SD-WAN fabric.

Request cloud gateways after fabric provisioning:

1. For a fabric that we host on Azure, open a TAC case and provide this information::
   - The specific enterprise subnet prefixes from which the connectivity to the VPN 512 of the control components is required.
   - To enable AAA or TACACS, provide IP prefixes that are unused within your existing fabric. These prefixes are used to create the control components. The original control components are shut down, then snapshotted, and finally cloned back.
   - Each region with control components uses one /24 unique custom subnet across the Cisco Catalyst SD-WAN fabric. Since each fabric includes two regions, you need two subnets.
   - Admin credentials to the Cisco SD-WAN Validator, Cisco SD-WAN Controller and Cisco SD-WAN Manager devices are required. You can provide credentials at the start of the change window.
2. Schedule an eight-hour maintenance window after the pre-approval and pre-checks are completed by the CloudOps engineer.
3. Before starting the process, enable DNS for Cisco SD-WAN Validator and configure all control components.
4. Ensure that GR is set to a default of twelve hours or higher on Cisco Catalyst SD-WAN or Cisco SD-WAN Controller devices.
5. Reserve two available Cloud Cisco Catalyst SD-WAN UUIDs through Plug and Play (PNP) and attach them to Cisco SD-WAN Manager.
6. We recommend attaching Cisco SD-WAN Manager templates to Cisco SD-WAN Validator, Cisco SD-WAN Controller, and any existing cloud Cisco Catalyst SD-WAN devices from Cisco.

You can use this feature only with single-tenant single-node Cisco SD-WAN Manager fabrics, single-tenant cluster-node Cisco SD-WAN Manager fabrics for provisioned control components, and all new control component sets to be provisioned. You cannot use this feature with multitenant Cisco SD-WAN Manager cluster fabrics.

Configure cloud gateways after provisioning:

Once CloudOps has completed the provisioning of the cloud gateways next to the cloud-hosted control components, they provide the public and private IP assignments for each cloud gateway. These are in the format (VPN 512, VPN 0, and VPN X).

CloudOps also provides the credentials for the newly provisioned cloud gateways. The cloud gateways have VPN 512 and VPN X interfaces in the same subnet as the VPN 512 of the control components in that region. CloudOps sets up the cloud gateways for AAA TACACS in this network layout.

Table 7: VPN interface mappings on cloud gateway

Interface	Description	Configuration
GigabitEthernet1	VPN 512 (Management)	DCHP-assigned
GigabitEthernet2	VPN 0 (Transport)	DHCP-assigned
GigabitEthernet3	VPN X (Service)	Static IP

If you encounter reachability issues with the cloud gateway, they usually result from problems with the interface IP address or route configurations.

Public and private IPs are assigned one-to-one to the cloud gateway interfaces using NAT. Although the gateway interface uses DHCP, it receives the same IP address from the cloud each time.

For VPN X interfaces, configure the static IP identical to the one shared by CloudOps. Do not use random IP addresses within the subnet.

The cloud gateways are subject to the same Inbound access list as the control components, since they are provisioned in the same unique environment per fabric.

Perform these steps to complete the configuration:

1. Log in via SSH to the gateway public IPs using the provided credentials.
2. 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.
3. If you are using Enterprise root-ca, also upload and install the same on the cloud gateways.
4. You may configure AAA or TACACS on the Cisco SD-WAN Manager with authentication fallback to local mode. The local mode must have the viptelatac, ciscotacro, or ciscotacrw users enabled. This configuration allows support teams to log in and resolve issues when necessary.
5. Acquire one unused cloud gateway UUID from the device list of the Cisco SD-WAN Manager per cloud gateway provisioned.

   If you do not have any cloud gateway UUID available in the WAN Edge Device list on your Cisco SD-WAN Manager, log in to the Cisco PNP portal on the fabric's associated Smart Account and Virtual Account. Perform **Add Software Devices** (C8000V), then **Sync Smart Account** on the Cisco SD-WAN Manager.
6. Activate the UUID on the cloud gateways so they can be authenticated by the Cisco SD-WAN Manager and join the Cisco Catalyst SD-WAN fabric.
7. The Azure subnet default gateway is your default gateway, even if you configure the gateway service VPN IP to be the gateway for your enterprise subnets. Therefore, in addition to your configuration on VPN 512 on the control components, there is additional configuration needed on the Azure side.

   Important

   We 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.

Note

Additional actions are needed to configure enterprise prefixes.

5 Monitor Control Components

Topics:

Cisco Catalyst SD-WAN cloud-hosted control components monitoring areas

Lists the key areas monitored for Cisco Catalyst SD-WAN cloud-hosted control components.

- Infrastructure monitoring, including:
  - CPU and data disk utilization,
  - loss of connectivity to network interfaces, and
  - failure to reach instances.
- Service monitoring, including:
  - expiration of control component SSL certificates,
  - availability of the Cisco SD-WAN Manager web server,
  - and loss of control connection to the control components.

Health monitoring for fabrics with Cisco SD-WAN Manager version earlier than 20.3.x

Provides information about cloud monitoring and the use of system users for health checks in Cisco SD-WAN Manager version earlier than 20.3.x.

Cloud monitoring helps ensure the availability of SD-WAN Control Components as part of the Cisco Catalyst SD-WAN cloud hosting services. By default, Cisco SD-WAN Manager has a user named `viptelatac` with `operator` privileges. We use this user to log in to Cisco SD-WAN Manager to collect and monitor the health of Cisco Catalyst SD-WAN.

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

The Cloud Infra team uses the `viptelatac` user to log in to Cisco SD-WAN Manager for additional health checks. The team also uses this account to triage issues in response to internal alerts and to assist with your Technical Assistance Center (TAC) cases.

To disable the cloud monitoring system, open a TAC case with the Cisco Catalyst SD-WAN Cloud Infra team and request to disable the cloud monitoring. After monitoring is disabled, remove the configured `viptelatac` user from Cisco SD-WAN Manager.

Enable health monitoring for fabrics with Cisco SD-WAN Manager version 20.3.x or later

Configure Cisco SD-WAN Manager to use push-based health monitoring for fabrics beginning with version 20.3.x.

Set up health monitoring using push-based architecture in Cisco SD-WAN Manager version 20.3.x or later.

Beginning with Cisco SD-WAN Release 20.3.1, the system uses a push-based monitoring model. In this model, the monitoring architecture uses Cisco SD-WAN Manager to authenticate with the system and send the health data. Cisco SD-WAN Manager pushes the data rather than the monitoring system logging into the Cisco SD-WAN Manager with the `viptelatac` user.

For version 20.3.x and later, the Cloud Infra team uses the `ciscotacro` and `ciscotacrw` users to log in to the Cisco SD-WAN Manager for additional health checks, to triage issues in response to internally generated alerts, and to assist

with your Technical Assistance Center (TAC) cases. The same user also performs automated infrastructure upgrades and certain software updates when prenotified changes are communicated to customer contacts for the fabric.

The `ciscotacro` user has read-only operator group privilege, while `ciscotacrw` has read-write netadmin group privilege. The Cloud Infra team uses the `ciscotacrw` user for certain enhanced debugging functions, cloud infrastructure upgrades, and management.

Before you begin

- Ensure that vManage is upgraded to version 20.3.1 or later. After Cisco SD-WAN Manager is upgraded to 20.3.1 or later, the `viptelatac` user is no longer required.
- Be prepared to provide consent on the Cisco SD-WAN Manager settings page and configure a one-time password (OTP).
- Obtain the OTP from the CloudOps team by opening a TAC Support case.

To enable this feature, you must provide consent and configure a one-time password (OTP).

To enable monitoring, log in to Cisco SD-WAN Manager and perform these steps:

Procedure

1. Go to **Settings** > **Cloud Services** > **Enable** in Cisco SD-WAN Manager.
2. Enter the OTP value provided by the CloudOps team.
3. Leave the Cloud Gateway URL blank.
4. Check the **vMonitoring** option.
5. Approve permission to collect fabric health status data from Cisco SD-WAN Manager.

Health monitoring is enabled for fabrics, and data is pushed from vManage to the monitoring system.

What to do next

To disable this access on any of the Cisco Catalyst SD-WAN fabric control components, remove the user from the configuration. Note that removing any of these users limits the ability of the support team to triage issues.

Alert notifications sent by CloudOps

Lists how alert notifications are managed and received for Cisco SD-WAN cloud-hosted fabric control components.

The CloudOps team manages the infrastructure of cloud-hosted instances. The team also helps with monitoring and back-end infrastructure maintenance. However, the team does not change or manage the running software version or configuration of the instances.

The CloudOps team may send alert notifications to indicate software issues, misconfiguration, or features that are overusing capacity. You may also be running your own tests, changes, or configuration updates that the team is not aware of.

The CloudOps team will notify you instead of taking direct action on the hosted control component instances. The team will ask you to open a Technical Assistance Center (TAC) support case for assistance and evaluation as needed. After you open a TAC case, TAC and the CloudOps team will work with you to resolve the issue.

Updating your fabric contact for receiving alert notifications

Each cloud-hosted fabric has one customer contact email address defined as the owner to receive CloudOps Alert notifications. Your fabric uses the contact email address from the End Customer details in the Sales Order as the owner contact by default.

You can open a Technical Assistance Center (TAC) case to review or update the contact information.

If you have cloud-based dedicated single-tenant control components, you can directly update the owner contact email address through the Cisco Catalyst SD-WAN Portal.

Only one email address contact can be defined as the owner. Use a group mailing list email address.

6 Cloud Infrastructure Operations

Topics:

Cloud-hosted control component snapshots

Provides information about how the system manages snapshots for cloud-hosted control components, retention periods, on-demand snapshots, and limitations.

The system takes regular snapshots of cloud-hosted Cisco SD-WAN Manager control components that we manage, based on the snapshot frequency. By default, the snapshot frequency is once every day, typically at midnight of the region of deployment, and the system retains the last seven snapshots. You can set the snapshot frequency to values between once a day to once every four days. To learn more about snapshots, refer to Information About Snapshots in the *Cisco Catalyst SD-WAN Portal Configuration Guide*.

Open a Technical Assistance Center (TAC) support case to review the current snapshot setting, or use the Cisco Catalyst SD-WAN Portal to change it. You can retain a maximum of seven periodic snapshots.

Snapshots are stored in your cloud account and cannot be downloaded. However, you can download the `config-db` backup file from Cisco SD-WAN Manager and save the configurations, including the templates, with the 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 a Cisco SD-WAN Manager template to configure and save Cisco SD-WAN Validator and Cisco Catalyst SD-WAN Controller configuration settings.

On-demand snapshots

Note

You can only use the on-demand snapshot process for fabrics with Cisco-hosted, cloud-based, dedicated, single-tenant control components. This is not applicable if you have a shared tenant fabric.

For any major planned change windows for Cisco SD-WAN Manager, you can take on-demand snapshot using Cisco Catalyst SD-WAN Portal. You can request this by opening a TAC support case with the CloudOps team. Freeze configuration changes and allocate up to eight hours prior to the change window to allow the on-demand snapshot to be taken and completed. You can store only one on-demand snapshot at a time for up to ten days from the creation date. If you create a new on-demand snapshot, the system removes and replaces the previous snapshot.

Penetration testing requirements for overlay control components

Provides the rules and resources for conducting penetration tests on SD-WAN overlay control components.

You can conduct your own penetration tests for Cisco Catalyst SD-WAN overlay control components without approval. Visit these websites for instructions:

- Amazon Web Services (AWS): https://aws.amazon.com/security/penetration-testing/
- Microsoft Azure: https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement

Mandatory maintenance of cloud-hosted control components

Lists the procedures and notifications related to mandatory maintenance of cloud-hosted control components.

The CloudOps team may at times need to perform maintenance on your instances. The instances are then rebooted before the cloud provider's maintenance window. This process allows you to move the instances from a hardware node that requires maintenance to a new and healthy hardware node. This approach prevents disruption of service.

You receive notifications at your registered email address for your fabric in the CloudOps system. The registered email address is initially configured using your original Sales Order's **End Customer Email Address** field. You can update it by logging into the Cisco Catalyst SD-WAN Portal at https://ssp.sdwan.cisco.com. The registered email address is not derived from the Cisco SD-WAN Manager Settings page.

> **Note**
>
> You receive email notices about mandatory reboots of cloud-hosted control components hosted in Amazon Web Services (AWS) only.

You can reschedule the change window, as long as the requested date and time is before the cloud provider's maintenance window time.You may not always receive advance notice, as the timing depends on the severity of the issue on the cloud provider's hardware node.

Cisco Catalyst SD-WAN disaster recovery guidelines

Cisco Catalyst SD-WAN disaster recovery (DR) is based on Cisco SD-WAN Manager disk volume snapshots and configuration database backups.

About backups and snapshots

- The system takes configuration database backups and disk volume snapshots daily (typically around midnight where vManage is located), securely storing them in the cloud.
- Starting with vEdge release 20.3.x and later, you can disable the configuration database backup feature, make your own backups, and provide them to CloudOps when needed.
- Disk volume snapshots are taken nightly, on-demand for your requests, or at major change windows. Snapshots cover all volumes of the vManage instance.
- Completed snapshots are copied to a designated backup region (usually a different geographic area). For example, if Cisco SD-WAN Manager runs in US-East, backups may go to US-West. The backup region is an identically configured 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; their configuration is managed through Cisco SD-WAN Manager or CLI, so backups are not taken for them.
- High availability for Cisco SD-WAN Manager is managed by a cluster (three or six nodes) within the same availability zone and region. The backup region does not include a standby or active Cisco SD-WAN Manager service.
- Cisco Catalyst SD-WAN Validator and Cisco Catalyst SD-WAN Controller services are deployed in both primary and backup regions; both operate actively, and device and policy information is pushed from Cisco SD-WAN Manager to both. When one region fails, Cisco Catalyst SD-WAN Controller and Cisco Catalyst SD-WAN Validator continue to function in the backup region.

- The configuration database-based recovery method allows the restoration of templates and policies only. In contrast, volume-based recovery includes collected statistics data.

> **Note**
>
> The data plane is designed to continue functioning even if all control components fail, via the Graceful Restart (GR) timer. The GR timer holds routes from vSmart for 12 hours by default. Choose the GR timer value carefully for backup and route learning.

Configuration database backup conditions

Prior to Cisco vManage Release 20.3.1, the configuration database is backed up only if all these conditions are met:

- Monitoring is enabled in the CloudInfra system. If the `viptelatac` user is unusable on the Cisco SD-WAN Manager for any reason, monitoring is disabled and you are notified with a request for correction.
- The `viptelatac` user is usable on the Cisco SD-WAN Manager.
- The configuration database size is less than 4 GB.

In Cisco vManage Release 20.3.1 and later, the configuration database is backed up only if all these conditions are met:

- Monitoring is enabled in the CloudInfra system.

  > **Note**
  >
  > In Cisco SD-WAN Manager, if the cloud service is disabled for any reason, monitoring is disabled on the CloudInfra system and you are notified with a request for correction.

- The `nms configuration-db daily-backup` service is enabled in the Cisco SD-WAN Manager CLI.
- Cloud Services, vMonitoring, and OTP are enabled in Cisco SD-WAN Manager Settings.
- The configuration database size is less than 4 GB.

Volume snapshot-based recovery

After the CloudOps team determines that the Cisco SD-WAN Manager instance needs to be replaced with a backup, we can initiate the DR process.

For DR in the same region, we select the same region and datacenter as the current Cisco SD-WAN Manager instance location. We specify the snapshot date and time of the snapshot based on requirements and availability.

Once DR triggers, the system first shuts down the existing Cisco SD-WAN Manager instance.

The system then uses the volume snapshots to create a new cloud instance with the same set of disks, instance size specifications, private subnets, security access list, and isolated environment that the original Cisco SD-WAN Manager had. Once the instance is up, the system swaps the public IPs from the old Cisco SD-WAN Manager instance to the new Cisco SD-WAN Manager instance.

The new running Cisco SD-WAN Manager instance has new private IPs but the same public IPs, software version, configuration, and data as when the snapshot was taken.

Cisco SD-WAN Manager is configured with the information necessary to join the fabric. You can use the same FQDN or URL to log in to the Cisco SD-WAN Manager instance as before.

In the unlikely case where the primary region of Cisco SD-WAN Manager has failed and is unavailable, we use the exact same process for DR to the backup region, except that the backup cloud region is selected.

When the new Cisco SD-WAN Manager instance runs in the backup region, the system does not swap public IPs between regions. Cloud regions have a specific public IP pool per region and cannot be assigned to instances across regions.

Thus, the new DR Cisco SD-WAN Manager instance in the backup region has new public IPs. The system updates the FQDN or 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-based recovery

If we cannot take a volume snapshot, we use the configuration database recovery process. We create a 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 or 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 a configuration database backup for DR is identical for both same region and backup region recovery.

For process details, refer to the section Restore a Cisco SD-WAN Manager Instance from Backup in the *Recover Cisco Catalyst SD-WAN Manager* Troubleshooting TechNote.

7 CloudOps Frequently Asked Questions

Topics:

Describes common questions and answers about CloudOps operations, troubleshooting, and best practices to help users effectively manage and optimize their cloud infrastructure deployments.

CloudOps security FAQs

Provides frequently asked questions and answers about security measures, access control, and monitoring for Cisco SD-WAN cloud environments.

What are the standard cloud security measures implemented to protect both Cisco and its customers within the AWS cloud environment?

You are protected by AWS network-level features, such as DDoS protection shields, which are active on all SD-WAN production fabrics. These protections reduce the risk of volumetric and application-layer attacks. AWS security groups control your access to cloud resources.

What happens if someone tries to brute force the SD-WAN Manager infrastructure?

If someone tries to brute force SD-WAN Manager from an unathorized IP, the cloud provider's security monitoring systems alert the SD-WAN CloudOps team so they can act immediately. This proactive monitoring prevents unauthorized access and protects your SD-WAN Manager control components.

How does Cisco view the risk of customers accessing SD-WAN Manager without Single Sign-On (SSO), and what mitigations exist?

While many customers globally access SD-WAN Manager without SSO, we have not observed security issues to date. We encourage you to adopt SSO, which is supported in all models except SD-WAN Cloud (formerly CDCS), to enhance security. If you do not use SSO, Cisco offers a custom VPC option that places private IP interfaces of cloud-hosted control components within your on-premises network. This allows secure access using TACACS, RADIUS, or AAA servers and avoids exposing public IP addresses.

What security measures does Cisco use beyond AWS security groups to protect Internet-facing SD-WAN control components?

Multiple layers of security protect your data, including Web Application Firewalls (WAF) and application-level DDoS protection. Your data is protected both in transit and at rest. WAF and integrated DDoS protections safeguard the publicly accessible SD-WAN models, preventing attacks and unauthorized access.

Is there security monitoring to detect brute force or other attacks?

Cloud providers monitor for security breaches and suspicious activities at all times to help keep your SD-WAN environment secure. If a compromise or brute force attempt is detected, SD-WAN CloudOps responds immediately, according to incident management protocols. The Security and Trust Organization (STO) regularly scans production deployments for vulnerabilities, and you can review reports on the Cisco Trust Portal. Basic DDoS protection and WAF are enabled by default for both cloud deployments and publicly accessible portals. For more information, refer to the SD-WAN Security At-a-Glance guide on the Cisco website.

How is access controlled for Cloud and Cloud-Pro environments?

You can only access the environment if you are an authorized customer or part of the SD-WAN support team. Authenticate through Day Zero Servers, SD-WAN Validator, or SD-WAN Manager. The system enforces role-based access control and Access Control Lists (ACLs) on SD-WAN Manager and in the cloud environment to keep your access secure.

How can customers request penetration testing (pen test) for Cisco SD-WAN cloud control components?

- For SD-WAN fabric control components hosted in AWS, conduct your own penetration tests in accordance with the AWS penetration testing policy at https://AWS.amazon.com/security/penetration-testing/
- For Azure-hosted SD-WAN fabric control components, perform penetration testing adhering to the Microsoft rules of engagement at https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement

Can the SD-WAN CloudOps team provide security certifications or audit reports?

We provide direct access to the Cisco Trust Portal, which contains security compliance documents, industry certifications (such as SOC, ISO, FedRAMP, and PCI DSS), privacy data sheets, penetration test confirmations, and whitepapers. You can register to access content protected by a Non-Disclosure Agreement (NDA). If your questions are not covered by the Trust Portal, the Customer Information Clearinghouse (CIC) team can provide vetted responses. Engage CIC through the CIC Request Tool on Salesforce.

A Open a TAC support case for the Cloud Infra team

Provides instructions on how to effectively open and manage a Technical Assistance Center (TAC) case to ensure timely support and resolution for Cisco SD-WAN operational issues.

Before you begin

Procedure

1. Log in to the Support Case Manager on the Cisco website.
2. Select **New Case** > **Products & Services** > **Open Case**.
3. Enter the appropriate entitlement information. You can use the serial number of a WAN Edge device for entitlement information.
4. Select **Next** and enter your case details.
5. Select **Technology** > **Search** and enter the appropriate Tech and Sub Tech keywords:
   - Technology: SDWAN - Cisco-Hosted
   - SubTechnology: SDWAN Cloud Infra

What to do next

Notices