Cisco Cloud-delivered Catalyst SD-WAN Guide

First Published: 2023-05-03

Last Modified: 2025-07-25

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

Read Me First

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.

Related References

- Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations
- Cisco Catalyst SD-WAN Device Compatibility

User Documentation

- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17
- User Documentation for Cisco SD-WAN Release 20

Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.

- To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.

CHAPTER 2

Getting Started

Information about Cloud-delivered Catalyst SD-WAN

Cisco Cloud-delivered Catalyst SD-WAN (CDCS) is a platform for Cisco Catalyst SD-WAN services that reduces and simplifies operational tasks for your Cisco Catalyst SD-WAN fabric. With this platform, you can deploy the Cisco Catalyst SD-WAN fabric, managing only edge devices and the edge network, while Cisco manages almost all the operational responsibilities for the fabric. Cloud-delivered Catalyst SD-WAN provides flexible cloud consumption, operational simplicity, and the comprehensive analytics features that are part of Cisco Catalyst SD-WAN.

Cloud-delivered Catalyst SD-WAN is ideal for small-sized or medium-sized businesses and enterprises that have limited network resources and want to limit the operational burdens of running the Cisco Catalyst SD-WAN fabric.

This document describes the initial setup and configuration procedures for Cloud-delivered Catalyst SD-WAN. Perform these procedures from the Cisco Catalyst SD-WAN Portal, which provides options for creating and accessing management tools for fabrics in Cloud-delivered Catalyst SD-WAN.

Limitations of Cloud-delivered Catalyst SD-WAN

Cloud-delivered Catalyst SD-WAN may not fully meet your unique needs if the following features are required:

- BYO-IDP (Bring Your Own IDP)
- SD-WAN Manager API
- Identity Services Engine (ISE) Integrations (such as SD-WAN/SDA, Trustsec, ACI)
- Multi-Region Fabric (MRF)
- Cloud gateways for AAA/TACACS/SYSLOG

- Specific requirements for control component locations (such as data sovereignty)
- 800+ edge devices in an SD-WAN fabric

For these cases, refer to the instructions for creating a dedicated fabric in the *Cisco Catalyst SD-WAN Portal Configuration Guide*.

Prerequisites for Cloud-delivered Catalyst SD-WAN

- Active Cisco Smart Account.
- Active Cisco Virtual Account.
- SA-Admin role for your Cisco Smart Account. This is required to access the Cisco Catalyst SD-WAN Portal for the first time to create a fabric. It is not required thereafter.
- Valid order for a Cisco DNA Cloud subscription or paid SD-WAN Control Component SKUs, on the Cisco Commerce site (formerly Cisco Commerce Workspace).

Create a fabric in the Cisco Catalyst SD-WAN Portal

After logging into Cisco Catalyst SD-WAN Portal, you can:

- by default, create a Cloud-delivered Catalyst SD-WAN fabric, or
- find information about requesting a Cisco hosted dedicated SD-WAN fabric.

Create a Cloud-delivered Catalyst SD-WAN fabric

A valid Smart Account is required to add a Cloud-delivered Catalyst SD-WAN fabric. No Smart Account license is required to create a Cloud-delivered Catalyst SD-WAN fabric.

Note Cloud-delivered Catalyst SD-WAN is only available in limited locations in the US/EU/APAC regions. If you require a Cisco Catalyst SD-WAN fabric to be hosted in a specific location apart from the available locations for cloud-delivered fabrics, you need to provision a Cisco hosted dedicated fabric.

Note The **Create Catalyst SD-WAN Fabric** section displays a banner to describe the steps required to create dedicated fabrics. See *Cisco Catalyst SD-WAN Portal Configuration Guide* for more information.

Procedure

Step 1 Enter https://ssp.sdwan.cisco.com to log in to the Cisco Catalyst SD-WAN Portal.

Step 2 Enter your Cisco Connection Online (CCO) **user name**.

Step 3 Enter your Cisco Connection Online (CCO) **password**.
The **Cisco Catalyst SD-WAN Portal Dashboard** opens.

Step 4 In the dashboard, click **Create Fabric**.

Step 5 On the **Create Fabric** page, do the following:

a) From the **Smart Account** drop-down list, choose the name of your Cisco Smart Account.
b) From the **Virtual Account** drop-down list, choose the name of your Cisco Virtual Account.
c) Enter the **Fabric Name**.
d) Choose the **Fabric Location**.
e) Enter the **Fabric Admin(s)**.
f) Select the **Release Category**.

The **Recommended** release category provides new features and new platform support in addition to bug fixes. It delivers maximum stability and reliability, making it ideal for most production environments.

The **Early Adopter** release category, if available in your location, delivers new features and expanded platform support compared to the Recommended category, but may require more frequent maintenance and updates for bug fixes.

Note
All the information selected and entered is listed in the **Preview** section located on the right side of the page.

Step 6 Accept the Terms and Conditions in the **Preview** section.

Step 7 Click **Create Fabric** from the dashboard.

You are notified by email that the fabric has been created.

What to do next

You can begin to access the fabric by logging back into the Cisco Catalyst SD-WAN Portal.

Add a user

When you create a fabric, you are automatically given the Admin role for that fabric. You can then configure roles for other users.

A role defines which Cisco Catalyst SD-WAN Manager features a user has read-only access to, and which features they have read and write access to.

Note Before you can add a role for a user, the user must have an account in Cisco Connection Online.

1. Log in to the Cisco Catalyst SD-WAN Portal with the Admin role for the fabric.
2. Click **View Details**.
3. On the **Fabric Details** page, click **User Role**.
4. Click **Add User**.

5. In the **User Email ID** field, enter the Cisco Connection Online email address for whom you are adding a role.
6. From the **Role** drop-down list, choose the user group to belong to.

   User groups are configured in Cisco Catalyst SD-WAN Manager. A user group specifies which features the users in the group have read-only access to, and which features the users have read and write access to.
7. Click **Add**.

Access Cisco Catalyst SD-WAN Manager

Cisco SD-WAN Manager provides options for configuring, managing, and monitoring a fabric. Any user with a user role that has been added to the Cisco Catalyst SD-WAN Portal can access Cisco SD-WAN Manager.

1. Log in to the Cisco Catalyst SD-WAN Portal: https://ssp.sdwan.cisco.com

   This login provides single sign-on authentication for the Cisco Catalyst SD-WAN Portal and Cisco SD-WAN Manager.
2. Click **Manage Fabric** for the fabric you want to access.

To exit the Cisco SD-WAN Manager and return to the Cisco Catalyst SD-WAN Portal, choose **SD-WAN Portal** from the Cisco SD-WAN Manager menu.

Add devices from a Smart Account to the Cisco SD-WAN Manager instance for a fabric

Procedure

Step 1 Log in to the Cisco Catalyst SD-WAN Portal.

Step 2 From the list of available fabrics, select a fabric to add devices to and click **Manage Fabric**.
The Cisco SD-WAN Manager instance for the selected fabric opens.

Step 3 From the Cisco SD-WAN Manager menu, select **Configuration** > **Devices**.

Step 4 Click **Sync Smart Account**.
The Sync Smart Account pane opens.

Step 5 Click **Sync**.

After synchronization, the devices in your Smart Account appear in the list of edge devices in the Cisco SD-WAN Manager instance for the selected fabric.

Access Cisco Catalyst SD-WAN Analytics for a fabric

Cisco SD-WAN Analytics provides information about device behavior, traffic, and related activities in your fabric.

1. Log in to the Cisco Catalyst SD-WAN Portal as a user with the Admin role for the fabric and navigate to the Cisco Catalyst SD-WAN for that fabric.
2. From the Cisco Catalyst SD-WAN menu, choose **Analytics** > **Overview**.

For more information, see Cisco Catalyst SD-WAN Analytics.

CHAPTER 3

Upgrading and Updating Devices

Installing new device software

Updating software using a remote repository server

Minimum supported release for edge devices: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

You can update the software on devices in the network using software images stored on a remote repository server (cloudopsremoterepo.sdwan.cisco.com) maintained by Cisco.

To enable devices in the network to receive the software updates from the remote server, see Enable Software Updates by a Remote Repository Server.

Requesting an image

If you need a software image and it is not available in the remote repository, open a TAC case to request an image. Similarly, open a TAC case to request an image if edge devices in the network are using a release earlier than Cisco IOS XE Catalyst SD-WAN Release 17.9.1a.

Provide these details about the image you need:

- Image version
- Link to the image on the Software Download portal
- Link that you use to connect to Cisco SD-WAN Manager
- Organization name

CHAPTER 4

Migrating from Cisco Hosted Catalyst SD-WAN to Cloud-delivered Catalyst SD-WAN

Migrate from Cisco Hosted Catalyst SD-WAN to Cloud-delivered Catalyst SD-WAN

Overview

If you are using Cisco Hosted Catalyst SD-WAN with a dedicated fabric and fewer than 800 devices, we recommend that you migrate to Cloud-delivered Catalyst SD-WAN to simplify your operations, reduce your daily networking management tasks, and bring your fabric into compliance with the Cisco Catalyst SD-WAN controller policy.

If you choose not to migrate, you need to purchase controllers for a dedicated Cisco Catalyst SD-WAN fabric.

Migration process

If you are entitled to migrate from Cisco Hosted Catalyst SD-WAN to Cloud-delivered Catalyst SD-WAN, we’ll contact you. We’ll let you know that you are entitled to the migration, and we’ll request the information that we need from you for the migration process.

Alternatively, you can open a case with the Cisco Technical Assistance Center (TAC) and request that the Cisco Cloud Operations team perform a migration.

After you provide the information that is required for a migration, we’ll contact you within 48 hours to schedule a maintenance window during which to perform the migration. This migration can take up to approximately 6 hours, depending on the number of devices in your fabric.

The Cisco Cloud Operations team performs the migration remotely. If any issues prevent a successful migration, we’ll resolve the issues and contact you as needed.

A migration has a minimal effect on the data plane because the control connection is automatically reestablished after the migration completes.

What to expect from the migration

- Enterprise certificates are not supported in Cloud-delivered Catalyst SD-WAN.
- Custom subnets are not supported in Cloud-delivered Catalyst SD-WAN. Custom subnets that were configured in your Cisco Hosted Cisco Catalyst SD-WAN for a dedicated fabric are removed during the migration.
- A new URL is generated for accessing Cisco Catalyst SD-WAN Manager. You can access this URL from the Cisco Catalyst SD-WAN Portal. Your old URL for accessing Cisco Catalyst SD-WAN Manager is not retained.
- Proxy settings from your Cisco Hosted Catalyst SD-WAN for a dedicated fabric are disabled.
- Statistics data from your Cisco Hosted Catalyst SD-WAN for a dedicated fabric are not retained.
- Analytics data from your Cisco Hosted Catalyst SD-WAN for a dedicated fabric data is not retained.
- Identity provider information Cisco Hosted Catalyst SD-WAN for a dedicated fabric is not retained.
- Configuring your own identity provider information is not supported in Cloud-delivered Catalyst SD-WAN.
- No inbound rules setting is required in Cloud-delivered Catalyst SD-WAN.

Migration prerequisites

Before we perform your migration from Cisco Hosted Catalyst SD-WAN to Cloud-delivered Catalyst SD-WAN:

- Ensure that you have valid Cloud-delivered Catalyst SD-WAN licenses in the Cisco Smart Account and Virtual Account for your current dedicated fabric.

  For information about obtaining these licenses, contact your Cisco representative.
- Upgrade your Cisco Hosted Catalyst SD-WAN fabric to match the current Cloud-delivered Catalyst SD-WAN version. We’ll let you know what this version is.

  For upgrade instructions, see *Upgrade SD-WAN Controllers with the Use of vManage GUI or CLI*.
- When requested, provide us with the netadmin credentials for your existing Cisco Hosted Catalyst SD-WAN fabric.
- Optionally, delete all Cisco Catalyst 8000 Edge Platforms that you are using as cloud gateways for TACACS. Cloud-delivered Catalyst SD-WAN currently does not support cloud gateways for TACACS. If you do not delete these platforms, they exist after the migration but are not functional.

After migration

After the migration completes, your old Cisco Hosted Catalyst SD-WAN fabric is no longer operational. You can access your new Cloud-delivered Catalyst SD-WAN fabric using the Cisco Catalyst SD-WAN Portal. For more information, see *Cisco Catalyst SD-WAN Portal Configuration Guide*.

Migration FAQ

Cisco Cloud-delivered SD-WAN fabric migration moves your existing Cisco Hosted SD-WAN environment to the Cisco Cloud-delivered SD-WAN environment, providing enhanced scalability, the latest features, and simplified management and analytics.

Cisco Cloud-delivered SD-WAN simplifies operations by having a network administrator manage network edge devices while Cisco handles operational responsibilities for SD-WAN Control Components. It offers flexible cloud consumption, operational simplicity, and comprehensive analytics.

Q. What preparation steps do I need to complete before the migration starts?

A. Before the migration, you need to:

- Ask your Cisco representative about the required software version for your Cisco Hosted SD-WAN Control Components. Upgrade accordingly
- Ask your Cisco representative about the required software version for your edge devices. Upgrade accordingly

  Use the Cisco SD-WAN Control Components Compatibility Matrix to check device compatibility with the SD-WAN Control Components.
- Remove unreachable or unused edge device serial numbers from your current SD-WAN Manager.
- Ensure that all edge devices are configured with working NTP and DNS servers.
- Ensure that none of the edge devices are configured with static hostname to IP mapping for the SD-WAN Validator (formerly vBond) fully qualified domain name (FQDN). Ensure that the edge devices are configured with the SD-WAN Validator FQDN value in System Configuration and not the exact IPs of the SD-WAN Validator.
- Ensure that you have out-of-band (OOB) direct access to the edge devices, especially the software-based devices. This may be required to address any connectivity issues during migration from Cisco Hosted SD-WAN to the Cisco Cloud-delivered SD-WAN fabric.

Q. Is an all-at-once migration required, or can the migration be performed in phases?

A. The actual migration of the Cisco Hosted SD-WAN fabric to a Cisco Cloud-delivered SD-WAN fabric is done in a single maintenance window, which includes the migration, post-migration checks, and recovery in case of a migration failure.

Q. How long does the migration process take?

A. The migration typically requires an 8-hour change window, but this depends on the size of the fabric.

Q. What are the communication channels between parties during the migration?

A. The primary means of communication during the migration is through a TAC (Technical Assistance Center) support case to ensure smooth coordination and support throughout the migration process.

Q. Who is responsible for upgrading the Cisco Hosted SD-WAN Control Components and edge devices?

A. You are responsible for upgrading both the Cisco Hosted SD-WAN Control Components and the edge devices as part of migration preparation. Cisco CloudOps can assist, if needed. When you have migrated to the Cisco Cloud-delivered SD-WAN, future software version upgrades of SD-WAN Control Components will be completed by Cisco.

Q. What information must I provide during the migration request?

A. You need to provide:

- Sales/Web Order details for the SD-WAN subscriptions
- SD-WAN Control Component fabric name and region of deployment
- Contact email address
- SD-WAN Manager admin credentials for the existing Cisco Hosted SD-WAN Control Component fabric

Q. What precautions should be taken during migration?

A. Ensure that you have out-of-band (OOB) access to edge devices for troubleshooting. If you have a firewall at your edge sites, it may need to be updated during the migration to allow the edge devices to communicate with the new Cisco Cloud-delivered SD-WAN Control Components' public IPs.

Q. What steps are required if I am using Enterprise certificates on the current Cisco Hosted SD-WAN Control Components?

A. Perform these steps:

1. Renew the certificates and migrate to Cisco PKI-based certificates on all SD-WAN Control Components.
2. Ensure the Cisco root CA bundle is installed on all edge devices.

Q. What steps are required if I am using Enterprise certificates on the current Cisco Hosted SD-WAN Control Components?

A. Perform these steps:

1. Renew the certificates and migrate to Cisco PKI-based certificates on all SD-WAN Control Components.

2. Ensure the Cisco root CA bundle is installed on all edge devices.

Q. How is configuration data transferred to the Cisco Cloud-delivered SD-WAN fabric?

A. All configuration data, including policies, templates, and edge device serial numbers, is extracted from your current SD-WAN Manager and restored to the new SD-WAN Manager using migration scripts.

Q. Will my edge devices automatically connect to the Cisco Cloud-delivered SD-WAN fabric after migration?

A. After the migration scripts push the new configuration, the edge devices will authenticate and connect to the Cisco Cloud-delivered SD-WAN fabric, using the policies configured previously.

Q. Is SD-WAN Analytics onboarded during migration?

A. SD-WAN Analytics is automatically enabled for your Cisco Cloud-delivered SD-WAN fabric during the migration process.

Q. Will the controller profile configured on the Plug-n-Play (PnP) portal be created in the Cisco Cloud-delivered SD-WAN environment?

A. The controller profile will be created in the Cisco Cloud-delivered SD-WAN Smart Account/Virtual Account (SA/VA) with your organization and service provider organization names. Also, your enterprise

SA/VA will be linked to the Cisco Cloud-delivered SD-WAN SA/VA using the external management feature in PnP.

Q. Will the data plane be affected during the change window?

A. Ideally, the data plane should remain unaffected during this change. However, due to unforeseen events that may arise, we recommend scheduling downtime as a precautionary measure during the change window. This ensures minimal disruption and allows for any necessary adjustments if issues occur.

Q. Where do I log in to access my new environment after migration?

A. You will continue using the Cisco Catalyst SD-WAN portal to access your Cisco Cloud-delivered SD-WAN fabric and SD-WAN Manager dashboard, using single sign-on (SSO).

Q. How do I verify that the migration was successful?

A. You will receive notice of migration completion from the Cisco support team. You can then log in to the Cisco Catalyst SD-WAN portal, open Cisco SD-WAN Manager, and review your devices and configurations to ensure everything is present and operating as expected.

Q. What should I do if there are issues with edge devices after migration?

A. Provide out-of-band (OOB) access to your edge devices so that Cisco Support can assist in re-establishing control connections.

Q. How can I ensure my user permissions and roles are correctly set up after migration?

A. Review your user role assignments in the Cisco Catalyst SD-WAN portal by selecting **Overlay Details** > **User** and update as needed. Cisco Support can assist if issues arise.

Q. What preparation do I need to make in case of a rollback?

A. You must have out-of-band (OOB) access to edge devices to update the SD-WAN Validator DNS and organization (sp-org-name) values for the devices to fall back to the source Cisco Hosted SD-WAN Manager.

Q. What are the risks involved with this migration?

A. Risks include potential temporary loss of connectivity, device control issues, or incomplete migration. Cisco follows very strict procedures to effectively minimize these risks.

Q. What features are enabled by default in a new Cisco Cloud-delivered SD-WAN fabric?

A. SD-WAN Analytics and Cloud OnRamp for SaaS are enabled by default, even if they were not previously enabled in your existing Cisco Hosted SD-WAN Control Components.

Software-Defined Application Visibility and Control (SD-AVC), Cisco SSO, and Remote Software Upgrade Image Repository are also enabled.

Q. Will my existing SD-WAN Analytics and reporting continue post-migration?
A. SD-WAN Analytics will continue to function, and your reporting capabilities will remain intact.

Q. What happens to my Cisco Hosted SD-WAN Control Components after migration?
A. The current Cisco Hosted SD-WAN Control Components are deleted after all devices and data are migrated to the Cisco Cloud-delivered SD-WAN fabric.

Q. Will CLI access to SD-WAN Control Components be available after migration?
A. CLI access to SD-WAN Control Components is not available after migration.

Q. Will the SD-WAN Control Components' public IPs change?
A. The SD-WAN Control Components' public IPs will change, and you may need to update your firewall rules to accommodate the new IP addresses. Cisco Cloud-delivered SD-WAN customers can request the public IP addresses of the SD-WAN Control Components at any time from the SD-WAN Cloud Infra team, using a Cisco TAC support case.