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.