

Migration from Cisco SD-WAN Cloud-Pro to Cisco SD-WAN Cloud

- Migration from Cisco SD-WAN Cloud-Pro to Cisco SD-WAN Cloud, on page 1
- Cisco SD-WAN Cloud migration FAQs, on page 3

Migration from Cisco SD-WAN Cloud-Pro to Cisco SD-WAN Cloud

Overview

If you are using Cisco SD-WAN Cloud-Pro with a dedicated fabric and fewer than 800 devices, we recommend that you migrate to Cisco SD-WAN Cloud 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 control component SKUs or management add-on for a dedicated Cisco SD-WAN Cloud-Pro fabric.

Migration process

If you are eligible to migrate from Cisco SD-WAN Cloud-Pro to Cisco SD-WAN Cloud, we will contact you. We will confirm your eligibility and request the necessary information from you to complete the migration.

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

After you provide the information that is required for a migration, we will contact you within 48 hours to schedule a maintenance window during which to perform the migration. The migration may take as long as 6 hours, depending on how many devices are in your fabric.

The Cloud Operations team performs the migration remotely. If any issues prevent a successful migration, we will 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 Cisco SD-WAN Cloud.

Migration from Cisco SD-WAN Cloud-Pro to Cisco SD-WAN Cloud

- Custom subnets are not supported in Cisco SD-WAN Cloud. Custom subnets that were configured for your Cisco SD-WAN Cloud-Pro 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 SD-WAN Cloud-Pro dedicated fabric are disabled.
- Statistics data from your Cisco SD-WAN Cloud-Pro dedicated fabric are not retained.
- Analytics data from your Cisco SD-WAN Cloud-Pro dedicated fabric is not retained.
- Identity provider information from your Cisco SD-WAN Cloud-Pro dedicated fabric is not retained.
- Configuring your own identity provider information is not supported in Cisco SD-WAN Cloud.
- No inbound rules setting is required in Cisco SD-WAN Cloud.

Migration prerequisites

Before we perform your migration from Cisco SD-WAN Cloud-Pro to Cisco SD-WAN Cloud:

- Ensure that you have valid Cisco SD-WAN Cloud 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 SD-WAN Cloud-Pro fabric to match the current Cisco SD-WAN Cloud 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 SD-WAN Cloud-Pro fabric.
- Verify that your edge devices all run on Cisco IOS XE SD-WAN (often referred to as "cEdge" devices). Viptela OS ("vEdge") devices are not supported for Cisco SD-WAN Cloud fabrics.
- Optionally, delete all Cisco Catalyst 8000 Edge Platforms that you are using as cloud gateways for TACACS. Cisco SD-WAN Cloud 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 SD-WAN Cloud-Pro fabric is no longer operational. You can access your new Cisco SD-WAN Cloud fabric using the Cisco Catalyst SD-WAN Portal. For more information, see *Cisco Catalyst SD-WAN Portal Configuration Guide*.

Cisco SD-WAN Cloud migration FAQs

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

Cisco SD-WAN Cloud simplifies operations by having a network administrator manage network edge devices while we handle 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 SD-WAN Cloud-Pro Control Components and upgrade them to the specified version.
- Ask your Cisco representative about the required software version for your edge devices and upgrade them to the specified version.

  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) and 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, which may be necessary to address any connectivity issues during migration from Cisco SD-WAN Cloud-Pro to the Cisco SD-WAN Cloud fabric.

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

A. The actual migration of the Cisco SD-WAN Cloud-Pro fabric to a Cisco SD-WAN Cloud 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 eight-hour (8 hours) change window, but this depends on the fabric size.

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

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

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

A. You are responsible for upgrading both the Cisco SD-WAN Cloud-Pro Control Components and the edge devices as part of migration preparation. Contact CloudOps for assistance if you need help with

upgrades. Once you have migrated to the Cisco SD-WAN Cloud, we will complete future software version upgrades of SD-WAN Control Components.

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

A. You need to provide:

- Your Sales/Web Order details for the SD-WAN subscriptions
- The SD-WAN Control Component fabric name and region of deployment
- Your contact email address
- The SD-WAN Manager admin credentials for the existing Cisco SD-WAN Cloud-Pro 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 public IP addresses of the Cisco SD-WAN Cloud Control Components.

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

A. Perform these steps:

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

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

A. Perform these steps:

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

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

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

Q. Is SD-WAN Analytics onboarded during migration?

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

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

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

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

Q. Will the data plane be affected during the change window?
A. Plan for downtime during the change window to ensure minimal disruption. Unforeseen events may occur, but the data plane usually remains unaffected during this change.

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 SD-WAN Cloud 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 that migration is complete from the 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 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. 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 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. We follow very strict procedures to minimize these risks.

Q. What features are enabled by default in a new Cisco SD-WAN Cloud 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 SD-WAN Cloud-Pro Control Components. The system also enables

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

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 SD-WAN Cloud-Pro Control Components after migration?
A. After all devices and data are migrated to the new Cisco SD-WAN Cloud fabric, the current Cisco SD-WAN Cloud-Pro Control Components are deleted.

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 public IP addresses of the SD-WAN Control Components change?
A. When the public IP addresses of the SD-WAN Control Components change, update your firewall rules to allow the new IP addresses. Cisco SD-WAN Cloud 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 TAC support case.