

Cisco SD-WAN Cloud Guide

First Published: 2023-05-03

Last Modified: 2026-06-22

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023–2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Read Me First** 1

CHAPTER 2 **Getting Started With Cisco SD-WAN Cloud** 3

- The Cisco SD-WAN Cloud platform 3
- Feature differences of the Cisco SD-WAN Cloud platform 3
- Prerequisites for Cisco SD-WAN Cloud implementation 4
- Create a Cisco SD-WAN Cloud fabric in Cisco Catalyst SD-WAN Portal 4
- Add a user to a fabric and assign a role 6
- Access Cisco Catalyst SD-WAN Manager from the Cisco Catalyst SD-WAN Portal 6
- Add devices from a Smart Account to Cisco SD-WAN Manager 7
- Access Cisco Catalyst SD-WAN Analytics for a Cisco SD-WAN Cloud 7

CHAPTER 3 **Upgrade and Update Devices in a Cisco SD-WAN Cloud Fabric** 9

- Cisco SD-WAN Cloud device software updates 9

CHAPTER 4 **Migration from Cisco SD-WAN Cloud-Pro to Cisco SD-WAN Cloud** 11

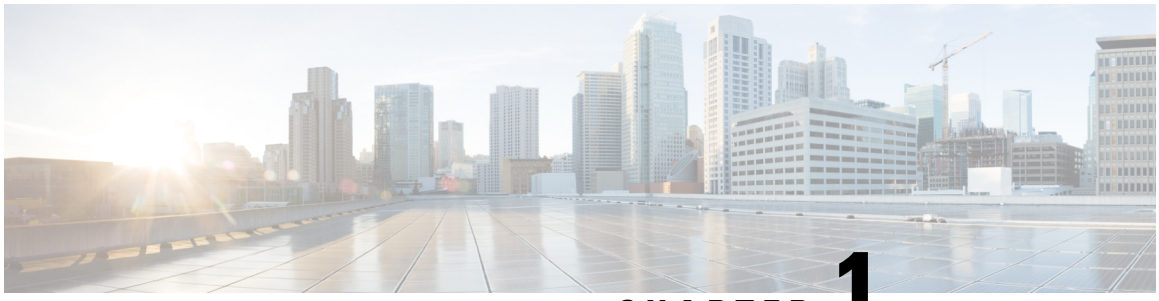
- Migration from Cisco SD-WAN Cloud-Pro to Cisco SD-WAN Cloud 11
- Cisco SD-WAN Cloud migration FAQs 13

CHAPTER 5 **Use Cisco APIs in Cisco SD-WAN Cloud** 17

- API keys for Cisco SD-WAN Cloud 17
- Restrictions for using a Cisco API key 17
- Obtain a Cisco API key 18
- Cisco API request examples 19

CHAPTER 6 **Integrate Cisco Identity Services Engine** 21

About Cisco ISE 21
Prerequisites for Cisco ISE Integration 21
Configure Cisco ISE Integration 21
Enable Cisco ISE Integration for a fabric 22



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

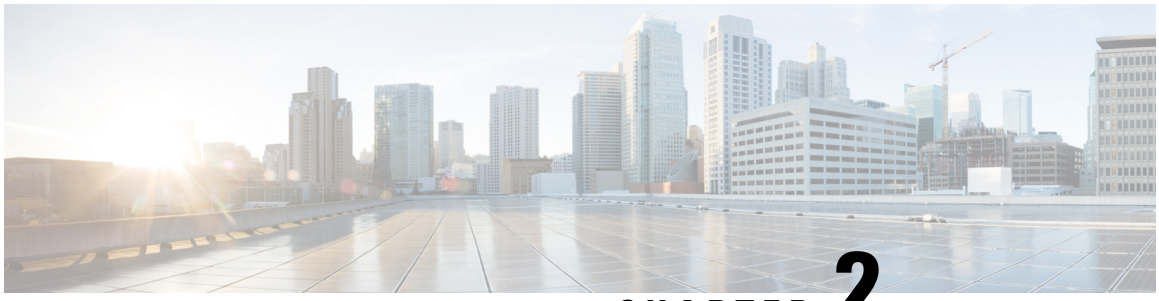
Communications, Services, and Additional Information

- 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 With Cisco SD-WAN Cloud

- The Cisco SD-WAN Cloud platform, on page 3
- Feature differences of the Cisco SD-WAN Cloud platform, on page 3
- Prerequisites for Cisco SD-WAN Cloud implementation, on page 4
- Create a Cisco SD-WAN Cloud fabric in Cisco Catalyst SD-WAN Portal, on page 4
- Add a user to a fabric and assign a role, on page 6
- Access Cisco Catalyst SD-WAN Manager from the Cisco Catalyst SD-WAN Portal, on page 6
- Add devices from a Smart Account to Cisco SD-WAN Manager , on page 7
- Access Cisco Catalyst SD-WAN Analytics for a Cisco SD-WAN Cloud, on page 7

The Cisco SD-WAN Cloud platform

The Cisco SD-WAN Cloud networking solution (formerly referred to as "Cloud-delivered Catalyst SD-WAN") is a platform for Cisco Catalyst SD-WAN services that:

- reduces and simplifies operational tasks for your Cisco Catalyst SD-WAN fabric,
- provides flexible cloud consumption, operational simplicity, and the comprehensive analytics features that are part of Cisco Catalyst SD-WAN,
- requires you to manage only edge devices and the edge network while Cisco handles almost all the operational responsibilities for the fabric, and
- is ideal for small 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 Cisco SD-WAN Cloud. Perform these procedures from the Cisco Catalyst SD-WAN Portal, which provides options for creating and accessing management tools for fabrics in Cisco SD-WAN Cloud.

Feature differences of the Cisco SD-WAN Cloud platform

The Cisco SD-WAN Cloud platform is designed as a simplified, cloud-delivered SD-WAN operating model. As a result, some capabilities differ from traditional customer-managed Cisco SD-WAN deployments.

- **Device support**: The Cisco SD-WAN Cloud platform supports Cisco IOS XE SD-WAN edge devices. Legacy edge devices running Viptela OS, commonly referred to as vEdge devices, are not supported.

- **Identity provider integration**: At this time, the Cisco SD-WAN Cloud platform uses Cisco CCO as the identity provider. Bring Your Own Identity Provider (BYOIdP) capabilities are planned for a future release through integration with Cisco's centralized identity platform.
- **Multi-Region Fabric**: Multi-Region Fabric (MRF) is a highly customizable deployment capability used in traditional SD-WAN environments. To keep the Cisco SD-WAN Cloud platform simple, standardized, and easy to operate, MRF is not currently supported.
- **Integration with customer-managed on-premises services**: Direct integration with customer-managed on-premises services such as AAA, TACACS, and Syslog servers is not supported in the current SaaS operating model. The Cisco SD-WAN Cloud platform is designed to provide a cloud-delivered experience with simplified operations and reduced dependency on customer-hosted infrastructure.
- **Cloud controller location and data sovereignty**: Customer selection of specific cloud controller deployment locations is limited at this time. Future roadmap plans include expanding regional deployment options to support broader data sovereignty and residency requirements.

If you require any of these features, see the instructions for creating a Cisco SD-WAN Cloud-Pro dedicated fabric in the *Cisco Catalyst SD-WAN Portal Configuration Guide*.

Prerequisites for Cisco SD-WAN Cloud implementation

These requirements must be met to implement the Cisco SD-WAN Cloud platform:

- An active Cisco Smart Account.
- An active Cisco Virtual Account.
- The SA-Admin role for your Cisco Smart Account.

  This is required to access the Catalyst SD-WAN Manager for the first time to create a fabric. It is not required thereafter.
- A valid order for a Cisco DNA Cloud subscription or for a paid SD-WAN Control Component SKUs on the Cisco Commerce site (formerly called Cisco Commerce Workspace).

Create a Cisco SD-WAN Cloud fabric in Cisco Catalyst SD-WAN Portal

Note Cisco SD-WAN Cloud is only available in limited locations in the US, EU, and APAC regions. To host a Cisco Catalyst SD-WAN fabric in a specific location apart from the available locations for Cisco SD-WAN Cloud fabrics, provision a Cisco SD-WAN Cloud-Pro dedicated fabric instead.

Before you begin

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

- create a Cisco SD-WAN Cloud fabric by default, or

- find information about requesting a Cisco SD-WAN Cloud-Pro dedicated fabric.

These instructions apply to creating Cisco SD-WAN Cloud fabrics only.

A valid Smart Account and Virtual Account are required to create a Cisco SD-WAN Cloud fabric.

Procedure

Step 1 Log in to the Cisco Catalyst SD-WAN Portal at https://ssp.sdwan.cisco.com with your CCO username and password.

Step 2 Select the **SD-WAN Customer** role.

Step 3 In the **Cisco Catalyst SD-WAN Portal Dashboard**, select **Create Fabric**.

Step 4 Select the **SD-WAN Cloud** fabric type.

Step 5 Select your **Smart Account** and **Virtual Account**.

Step 6 If your Smart Account has unused SD-WAN control component licenses, you are asked if you want to use them to create your fabric. Select **Yes** or **No** and click **Submit**.

a) If you selected **Yes**, an option to **Assign SDWAN Fabric License** appears. Click the option to display a list of available licenses.

b) Enter the quantity of each type of license you want to use and click **Assign**.

Step 7 Enter or select the **Fabric Name**, **Fabric Location**, and **Fabric Admin(s)**.

Step 8 Select the **Release Category**:

- The **Recommended** release category is the preferred option for most customers. It is selected based on rigorous quality and stability standards and supported by metrics, customer feedback, and extensive testing. Recommended releases are classified as long-lived and are widely adopted across the customer base. They offer maximum stability and reliability for most production environments.
- The **Early Adopter** release category, if available in your location, is required to access the latest features, platform enhancements, and bug fixes. This release is ideal for deployments that require capabilities not yet available in the Recommended release. Early Adopter versions continue to receive patches and bug fixes as they mature and may be reclassified as Recommended over time.

  You must select the Early Adopter category if you plan to add Cisco 8000 Series Secure Routers to your Cisco SD-WAN Cloud fabric.

  Early Adopter releases are the newest software versions available.

  Note
  Early Adopter is the default Release Category option for sites with UNX licenses.

  You cannot downgrade from an Early Adopter release to an older Recommended release.

  When an Early Adopter version newer than your current version is reclassified as Recommended, you will be upgraded to this Recommended release.

a) If your selected Release Category supports Cisco Identity Services Engine (ISE), an option appears to enable it. To enable ISE for the new fabric, select the option and enter the VPN ID.

Refer to Cisco Identity Services Engine for more information on ISE.

Step 9 All the information you provide is listed in the **Preview** section on the right panel of the page. Accept the Terms and Conditions.

Step 10 Select **Create Fabric**.

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

What to do next

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

Add a user to a fabric and assign a role

User roles assign specific access permissions to users for a fabric.

Roles, or 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.

When you create a fabric, you are automatically assigned the Admin user role for that fabric and you can configure roles for other users.



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 CCO email address of the user.
6. From the **Role** drop-down list, choose the user group the user should belong to.
7. Click **Add**.

The user is added to the fabric with the assigned role.

Access Cisco Catalyst SD-WAN Manager from the Cisco Catalyst SD-WAN Portal

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 into the Cisco Catalyst SD-WAN Portal.

   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.

The Cisco SD-WAN Manager opens.

3. 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.



Note You can also bookmark the SD-WAN Manager URL, which allows you to directly access it with your CCO email address and password after you have logged into the Cisco Catalyst SD-WAN Portal at least once.

Add devices from a Smart Account to Cisco SD-WAN Manager

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**.

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

Step 4 Click **Sync Smart Account**.

Step 5 In the Sync Smart Account pane, 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 Cisco SD-WAN Cloud

Use Cisco SD-WAN Analytics to view 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.
2. Navigate to the Cisco Catalyst SD-WAN page for the fabric.
3. From the Cisco Catalyst SD-WAN menu, choose **Analytics** > **Overview**.

Cisco SD-WAN Analytics opens, displaying device behavior, traffic, and related activities for your fabric.

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



CHAPTER 3

Upgrade and Update Devices in a Cisco SD-WAN Cloud Fabric

• Cisco SD-WAN Cloud device software updates, on page 9

Cisco SD-WAN Cloud device software updates

Device software updates from a remote repository server

You can update the software on devices in the network using software images stored on a remote repository server (cloudopsremoterepo.sdwan.cisco.com) that we maintain.

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

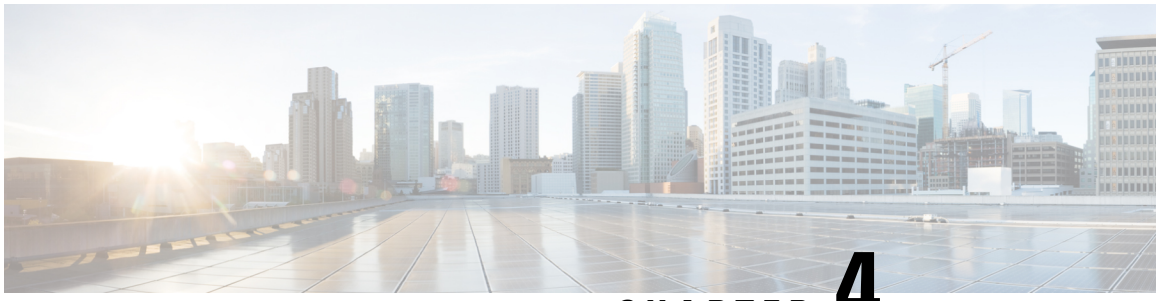
Minimum supported release for edge devices: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

Device software image requests

If the required software image is not available in the remote repository, open a TAC case to request it. Also, if edge devices in the network use a release earlier than Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, open a TAC case to request the software image.

Provide these details about the image you need:

- Desired image version
- The link to the image on the Software Download portal
- The link that you use to connect to Cisco SD-WAN Manager
- Your organization name



CHAPTER 4

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 11
- Cisco SD-WAN Cloud migration FAQs, on page 13

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.

- 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

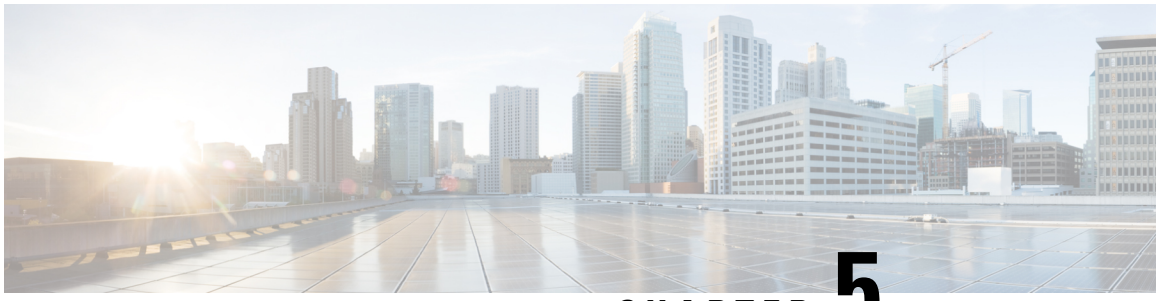
Software-Defined Application Visibility and Control (SD-AVC), SSO, and Remote Software Upgrade Image Repository.

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.



CHAPTER 5

Use Cisco APIs in Cisco SD-WAN Cloud

- API keys for Cisco SD-WAN Cloud, on page 17
- Restrictions for using a Cisco API key, on page 17
- Obtain a Cisco API key, on page 18
- Cisco API request examples, on page 19

API keys for Cisco SD-WAN Cloud

API key, or JSON web tokens (JWT), are unique codes that:

- grant client access to an application programming interface (API),
- serve as a password preventing unauthorized access, and
- are required for Cisco SD-WAN Cloud customer access to Cisco APIs.

A Cisco API key is to be used for Cisco API calls by a specified fabric user. It remains valid until the user is deleted or the user role is changed.

This chapter describes how to acquire a Cisco API key and use Cisco APIs on a Cisco SD-WAN Cloud fabric in Cisco SD-WAN Cloud Release 20.15 and higher.

Restrictions for using a Cisco API key

Use the Cisco API key to access all Cisco APIs from Cisco SD-WAN Cloud through your SSO login, subject to certain restrictions. Refer to Cisco DevNet for more information on Cisco APIs.

- Authentication method

  You must specify the Bearer token authentication method in a header field. Use the value you received from your GET request.

- Cross-site request forgery protection (CSRF/XSRF)

  Your API request header must include an X-XSRF-Token header field to protect against cross-site request forgery. Use the value you received from your GET request.

- API body use

  You can include an API body as needed, based on the API call you are making.

- Rate limit

  Real time APIs and bulk APIs are not available. All other APIs can be used, subject to a rate limit of 10 per second. Cisco SD-WAN Manager imposes an API rate limit of 5 per second.

- No continuous monitoring

  Do not use this feature for continuous monitoring. Refer to the Cisco Catalyst SD-WAN Getting Started Guide for more information on API rate limits.

- Supported categories

  API calls are provided for only these categories of operations:

  - Certificate management
  - Configuration
  - Device and device inventory
  - Monitoring
  - Troubleshooting tools

- No NAT configuration

  NAT configuration using REST APIs is not supported.

Obtain a Cisco API key

Cisco SD-WAN Cloud Release 20.15 provides a mechanism to generate an API key directly. Follow these steps to generate an API key and find the gateway URL and Cross-site request forgery protection (CSRF) token values:

Procedure

Step 1 Log in to the fabric.

Step 2 Select **My Profile** from the drop-down menu under your user ID.

Step 3 Obtain the API key (also called the API token).

a) In Cisco SD-WAN Manager click your user name at the top of the page, and choose **My profile**.

b) In the **API token** area, click **Generate**.

SD-WAN Manager generates and displays the API key.

c) Copy or download the API key.

Step 4 Obtain the organization name.

a) Open **Administration** > **Settings** > **Organization name**.

b) Copy the name from the **Organization name** field.

Step 5 Obtain the API gateway URL.

Use the endpoint information provided in the example here. In the payload, use the organization name in "org" and the API key in "apikey". The response provides the API gateway URL.

Example:

Post

```
https://ssp.sdwan.cisco.com/ssp/api/v6/apigw/info/
```

Payload

```
{
"org": "kdk...",
"apikey": "eyJ0eX...",
"is_redirect": false
}
```

Response

```
{
"gateway_url": "apigw1clouduswest2-1024.viptela.info",
"org": "kdk..."
}
```

Note
If the response is not successful, it might be that a new API gateway was provisioned near your location. Repeat this process to connect to the new gateway serving your overlay.

Step 6 Obtain the cross-site request forgery (CSRF) token.

Using the API key and gateway URL hostname values you received, make a GET request to the endpoint "/dataservice/client/token" to obtain the CSRF token. The response provides the CSRF token.

Example:

Based on the gateway URL returned in this example, the full pathname would be https://apigw1clouduswest2-1024.viptela.info/dataservice/client/token.

What to do next

Use the information you've obtained to make API calls. Some PUT and POST calls require the CSRF token.

Cisco API request examples

The examples in this section demonstrate how to use the API key, gateway URL, and CSRF/XSRF token to execute API calls.

GET API request example using Curl

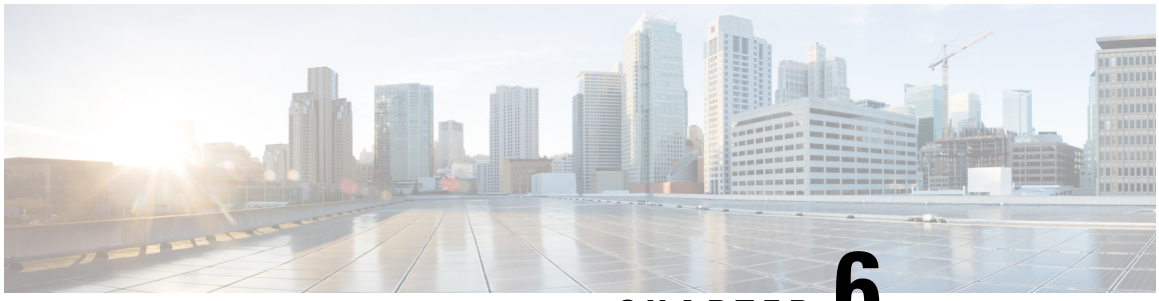
This GET request retrieves the page at the URL specified in the location parameter.

```
curl --location
apigw1clouduswest2-1024.viptela.info/dataservice/settings/configuration/banner'
--header 'X-XSRF-Token: AB0E71CAE...'
--header 'Authorization: Bearer
eyJ0eXAiOiJqd3QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJ2bGluZ2FtcEBjaXNjby5jb20iLCJpc3MiOiJiOGVkYW
...
a_fcNoeAlVYvrXzDXA'
```

PUT/POST API request example using Curl

This PUT request sends the data in the data parameter to the page URL specified in the location parameter.

```
curl --location --request PUT
apigw1clouduswest2-1024.viptela.info/dataservice/settings/configuration/banner'
--header 'X-XSRF-Token: AB0E71CAE72C6D...'
--header 'Content-Type: application/json'
--header 'Authorization: Bearer
eyJ0eXAiOiJqd3QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJ2bGluZ2FtcEBjaXNjby5jb20iLCJpc3MiOiJiOGVkYW
...
a_fcNoeAlVYvrXzDXA'
--data '{"mode":"on","bannerDetail":"check"}'
```



CHAPTER 6

Integrate Cisco Identity Services Engine

- About Cisco ISE, on page 21
- Prerequisites for Cisco ISE Integration, on page 21
- Configure Cisco ISE Integration, on page 21

About Cisco ISE

Cisco ISE Integration enables you to leverage the Cisco Identity Services Engine (ISE) for centralized authentication, authorization, and policy management in your Cisco SD-WAN Cloud environment. Gain greater visibility, control, and compliance while ensuring a secure and scalable network infrastructure.

Integrating Cisco ISE with Cisco SD-WAN Cloud allows for enhanced identity-based policies and visibility across your network fabric. This chapter provides step-by-step instructions for configuring the integration.

Note This feature is currently supported only on Early Adopter Cisco SD-WAN Cloud software releases.

Prerequisites for Cisco ISE Integration

Before you begin the Cisco ISE Integration, ensure you have these items and files ready:

- The reachable IP address of your Cisco ISE primary server node.
- A valid username and password with sufficient privileges on the Cisco ISE server.
- The VPN ID through which Cisco Catalyst SD-WAN Manager can communicate with the Cisco ISE server, typically VPN 0.
- The Root CA certificate files for the Cisco ISE Server and the pxGrid Server, in .cer format.

Configure Cisco ISE Integration

Perform these steps on the Cisco Catalyst SD-WAN Manager to enable Cisco Identity Service Engine (ISE) Integrationon your system:

Procedure

Step 1 Log in to your SD-WAN Manager dashboard.

Step 2 On the navigation pane, select **Administration**.

Step 3 From the sub-menu, select **Integration Management**.

Step 4 In the main window, select the **Identity Services Engine** tab.

Step 5 Click **Add Connection**.

Step 6 In the **Add ISE Server** panel, complete these required fields:

- ISE Server IP Address - Enter the IP address of your Cisco ISE server.
- Username - Enter the administrative username for ISE.
- Password - Enter the corresponding password.
- VPN - Select the appropriate VPN from the drop-down menu to ensure the Manager can route traffic to the Cisco ISE server.

Step 7 Upload the trusted CA certificates to establish a secure connection:

a) Locate the **ISE Server CA** section.
b) Click **Choose a file** or drag and drop your Cisco ISE Server CA certificate file into the box.
c) Locate the **pxGrid Server CA** section.
d) Upload the pxGrid Server CA certificate file for pxGrid communication in the same manner.

Step 8 Review all entered information for accuracy and click **Submit**.

The system attempts to authenticate and establish a connection with the Cisco ISE server. Once successful, the server status should update to “Connected” or “Active” in the Integration Management list.

If you encounter any errors, check these conditions:

- Field Required Errors - Ensure all fields marked with a red asterisk (*) are filled.
- Certificate Errors - Ensure the certificates are in the correct .cer format and have not expired.
- Connectivity Issues - Verify that the selected VPN has a valid route to the Cisco ISE Server IP address and that firewall rules allow traffic on the necessary ports, such as HTTPS/443 and pxGrid ports.

What to do next

Cisco Identity Services Engine (ISE) Integration must also be enabled for the fabric in SD-WAN Portal. If this was not done during fabric creation, follow the steps in Enable Cisco ISE Integration for a fabric, on page 22.

Enable Cisco ISE Integration for a fabric

Perform these steps to enable Cisco Identity Service Engine (ISE) Integration for an existing fabric.

Note ISE Integration can also be enabled at the time of fabric creation. See Create a Cisco SD-WAN Cloud fabric in Cisco Catalyst SD-WAN Portal, on page 4 for more information.

Procedure

Step 1 Log in to your SD-WAN Portal.

Step 2 Select the desired fabric.

Step 3 From the **Actions** menu, select **Enable ISE Integration**.

Step 4 Enter the VPN ID and click **OK**.