Cisco Catalyst SD-WAN Cloud Guide

Cisco SD-WAN
Updated November 18, 2026

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

Full Cisco Trademarks with Software License

Full Cisco Trademarks with Software License

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)

Topics included

1 Read Me First....5

2 Getting Started With Cisco SD-WAN Cloud....7
The Cisco SD-WAN Cloud platform....8
SD-WAN Cloud platform feature differences....8
Prerequisites for Cloud platform implementation....9
Create a Cloud fabric in the SD-WAN Portal....9
Add users and assign roles....10
Access SD-WAN Manager from the SD-WAN Portal....11
Add devices from your Smart Account to SD-WAN Manager....12
Access SD-WAN Analytics for your Cloud fabric....12

3 Upgrade and Update Devices in a Cloud Fabric....15
Device software image installation and update information....16

4 Migration from Cisco SD-WAN Cloud-Pro to Cisco SD-WAN Cloud....17
Migration requirements and compatibility for Cloud-Pro to Cloud....18
Key information about migration to a Cloud fabric....19

5 Use APIs in Cisco SD-WAN Cloud....23
API keys for Cisco SD-WAN Cloud....24
Restrictions for Cisco SD-WAN Cloud API key usage....24
Obtain a Cisco API key....25
Examples of authenticated API requests with cURL....26

6 Integrate Cisco Identity Services Engine....29
Cisco ISE features....30
Prerequisites for Cisco ISE integration....30
Configure Cisco ISE integration in SD-WAN Manager....30
Enable Cisco ISE integration for a fabric....31

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

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.

2 Getting Started With Cisco SD-WAN Cloud

Topics:

- The Cisco SD-WAN Cloud platform
- SD-WAN Cloud platform feature differences
- Prerequisites for Cloud platform implementation
- Create a Cloud fabric in the SD-WAN Portal
- Add users and assign roles
- Access SD-WAN Manager from the SD-WAN Portal
- Add devices from your Smart Account to SD-WAN Manager
- Access SD-WAN Analytics for your Cloud fabric

The Cisco SD-WAN Cloud platform

Explains the essential features and architectural principles of the Cisco SD-WAN Cloud platform, enabling you to understand its core capabilities and operational overview.

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

- reduces and simplifies operational tasks for a Cisco Catalyst SD-WAN fabric,
- provides cloud consumption flexibility, operational simplicity, and analytics features as part of Cisco Catalyst SD-WAN, and
- only requires you to manage edge devices and the edge network while Cisco handles almost all operational responsibilities for the fabric.

The SD-WAN Cloud platform is ideal if you have limited network resources and want to reduce the operational workload of running your 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.

SD-WAN Cloud platform feature differences

Provides the distinguishing feature set and operational differences of the SD-WAN Cloud platform compared to other deployment models, highlighting unique functions and limitations.

The Cisco SD-WAN Cloud platform is a simplified, cloud-delivered SD-WAN operating model. Some capabilities differ from traditional customer-managed Cisco SD-WAN deployments. Key differences include these areas:

- **Device support**: 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**: Uses CCO as the identity provider. Bring Your Own Identity Provider (BYOIdP) is available only for the Cisco SD-WAN Cloud-Pro platform.
- **Multi-Region Fabric (MRF)**: Not supported on the Cisco SD-WAN Cloud platform to keep operations simple and standardized.
- **Integration with customer-managed on-premises services**: Integration with customer-managed on-premises services such as AAA, TACACS, and Syslog servers is not supported. The platform offers a cloud-delivered experience with simplified operations and reduced reliance on customer-hosted infrastructure.
- **Cloud controller location and data sovereignty**: You cannot select specific cloud controller deployment locations. We plan to expand regional deployment options to address data sovereignty and residency requirements.
- **Statistics collection**: The platform always uses the cloud-based Analytics engine. Single Analytics Ingest Engine (SAIE) and Aggregated SAIE statistics are configured exclusively through Cisco SD-WAN Analytics. In Cloud-Pro deployments, Analytics is enabled by default and can be disabled if required.
- **On-Demand Troubleshooting**: Available in dedicated and multitenant Cisco SD-WAN Manager deployments, but not on the Cisco SD-WAN Cloud platform. If UI options and APIs for this feature appear in the Cloud interface, leave the feature disabled.

For features not supported in the Cisco SD-WAN Cloud platform, see the instructions for creating a dedicated Cisco SD-WAN Cloud-Pro fabric in the *Cisco Catalyst SD-WAN Portal Configuration Guide*.

Prerequisites for Cloud platform implementation

Lists the requirements and access roles you need for a successful SD-WAN Cloud implementation, including network credentials and active Cisco subscriptions.

To implement the Cisco SD-WAN Cloud platform, you must meet these requirements:

- An active Cisco Smart Account.
- An active Cisco Virtual Account.
- The Smart Account (SA) Administrator role for your Cisco Smart Account. This role is required for inital access to the Catalyst SD-WAN Manager to create a fabric, but is not required thereafter.
- A valid order for a Cisco DNA Cloud subscription or paid SD-WAN Control Component SKUs on the Cisco Commerce site (formerly named Cisco Commerce Workspace).

Create a Cloud fabric in the SD-WAN Portal

Configure a Cloud fabric in the SD-WAN Portal by following step-by-step instructions for essential initial deployment.

Set up a Cloud fabric in your Cisco Catalyst SD-WAN environment for network management and deployment.

Use this task to deploy a new Cloud fabric using Cisco Catalyst SD-WAN Portal. Only Cloud fabrics (not dedicated fabrics) are supported in these steps. A valid Smart Account and Virtual Account are required.

Before you begin

- Log in to Cisco Catalyst SD-WAN Portal.
- Confirm you have a valid Smart Account and Virtual Account.

> **Note**
>
> The Cisco SD-WAN Cloud fabric is only available in limited locations in the United States, European Union, and Asia-Pacific regions. For other locations, use a dedicated Cisco SD-WAN Cloud-Pro fabric.

Follow these steps to create a Cisco SD-WAN Cloud fabric in the SD-WAN Portal.

Procedure

1. Log in to the Cisco Catalyst SD-WAN Portal at https://ssp.sdwan.cisco.com using your account username and password.
2. Select the **SD-WAN Customer** role.
3. In the Portal dashboard, choose **Create Fabric** and select the **SD-WAN Cloud** fabric type.
4. Choose your **Smart Account** and **Virtual Account**.
5. If you have unused SD-WAN control component licenses, decide whether to use them to create your fabric. Select **Yes** to assign the licenses, specify the quantity for each type and confirm the assignment. Otherwise, select**No** and continue.
6. Enter or select the **Fabric Name**, **Fabric Location**, and **Fabric Admin(s)**.
7. Select a **Release Category**:

- **Recommended**: Preferred for most deployments; emphasizes stability and reliability. The releases in this category are 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.
- **Early Adopter**: The newest software versions available; required to access the latest features and platform updates. Required for support of Cisco 8000 Series Secure Routers. You cannot downgrade from Early Adopter to Recommended. When an Early Adopter version is reclassified as Recommended, your system will be upgraded accordingly.

  Early Adopter releases are ideal for deployments that require capabilities not yet available in the Recommended release. They continue to receive patches and bug fixes as they mature. Over time, they may be reclassified as Recommended releases.

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

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

   For more information on ISE, refer to Cisco ISE features on page 30.

9. Review all entered information in the preview section. Accept the Terms and Conditions, then select **Create Fabric**.

An email notification confirms the fabric has been created.

What to do next

Log in to the Cisco Catalyst SD-WAN Portal again to access the new fabric.

Add users and assign roles

Outlines the process of onboarding users to the SD-WAN Cloud platform, including adding user accounts and managing role-based access assignments to ensure proper authorization.

User roles define which access permissions users have within a fabric.

Roles, also known as user groups, are configured in Cisco Catalyst SD-WAN Manager. Each user group determines which features users can access with read-only permissions and which features they can access with both read and write permissions.

When you create a fabric, you are automatically assigned the Admin user role for that fabric. You can then 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 user's email address.
6. From the **Role** drop-down list, choose the user group for the user.
7. Click **Add**.

The user becomes a member of the fabric with the assigned role.

Access SD-WAN Manager from the SD-WAN Portal

Access SD-WAN Manager through the SD-WAN Portal to configure, manage, and monitor your cloud environment.

Enable seamless management of your SD-WAN fabric and cloud deployments using SD-WAN Manager.

The SD-WAN portal provides centralized access and single sign-on authentication for SD-WAN Manager and related services.

Before you begin

- Confirm you have a user role assigned in the SD-WAN portal.
- Obtain access credentials (Cisco.com email address and password).

Procedure

1. Log into the Cisco Catalyst SD-WAN Portal.

   This login grants single sign-on access to the Cisco Catalyst SD-WAN Portal, Cisco SD-WAN Manager, and other services.

2. Choose **Manage Fabric** for the desired fabric.

   Cisco SD-WAN Manager launches for that fabric.

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

You can now configure, manage, and monitor your SD-WAN fabric and cloud deployments using SD-WAN Manager.

> **Note**
>
> You can also bookmark the SD-WAN Manager URL, which allows you to directly access it with your Cisco.com email address and password after you have logged into the Cisco Catalyst SD-WAN Portal at least once. Ensure you keep your login credentials secure for direct access.

Add devices from your Smart Account to SD-WAN Manager

Configure and synchronize devices from your Smart Account so they can be integrated and managed within your SD-WAN Cloud environment.

Integrate devices registered in your Smart Account with SD-WAN Manager for centralized management and configuration.

Use this process whenever you need to onboard new devices from your Software Assurance-enabled Smart Account to SD-WAN Manager, ensuring they can be managed as part of your SD-WAN fabric.

Before you begin

- Ensure you have access credentials for both the SD-WAN Manager and your Smart Account.
- Confirm the SD-WAN Manager instance is online and connected to the SD-WAN Cloud environment.

Procedure

1. Log in to the Cisco Catalyst SD-WAN Portal.
2. Select the appropriate fabric where you want to onboard devices. Then, click **Manage Fabric**.
3. From the Cisco SD-WAN Manager menu, select **Configuration** > **Devices**.
4. Click **Sync Smart Account**.
5. In the Sync Smart Account pane, click **Sync**to initiate synchronization with your Smart Account.

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

What to do next

Review the imported devices, assign configurations or templates as needed, and verify device connectivity and status within your SD-WAN environment.

Access SD-WAN Analytics for your Cloud fabric

Access SD-WAN Analytics tools for your Cloud fabric to monitor device behavior, traffic, and related activities, enabling you to view performance metrics and generate actionable insights.

Use SD-WAN Analytics to view and analyze information about device behavior, traffic, and activities in your cloud fabric.

This task allows administrators to utilize SD-WAN Analytics tools for monitoring and analyzing their network fabric's performance and activity.

Before you begin

- Ensure you have the Admin role for the target cloud fabric.

- Verify access to the SD-WAN Analytics platform.

Procedure

1. Log in to the Cisco Catalyst SD-WAN Portal as a user with the Admin role for your Cloud fabric.
2. Navigate to the main page for your Cloud fabric.
3. From the menu, choose **Analytics** > **Overview**.

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

For more information, consult the Cisco Catalyst SD-WAN Analytics documentation.

3 Upgrade and Update Devices in a Cloud Fabric

Topics:

- Device software image installation and update information

Device software image installation and update information

Provides instructions for acquiring, staging, and activating device software images to ensure devices remain up to date with the latest features and security enhancements.

Device software updates from a remote repository server

Update device software by using images stored on the Cisco remote repository server (cloudopsremoterepo.sdwan.cisco.com).

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

The minimum supported release for edge devices is 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, or if edge devices in your network use a release earlier than Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, open a support case to request the image.

When submitting a request, provide this information:

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

Following these guidelines ensures that your devices are consistently updated with supported software versions and remain able to leverage new features and security enhancements.

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

Topics:

- Migration requirements and compatibility for Cloud-Pro to Cloud
- Key information about migration to a Cloud fabric

Migration requirements and compatibility for Cloud-Pro to Cloud

Provides reference information on migration prerequisites, compatibility, feature changes, and best practices for moving from Cloud-Pro to Cloud.

Overview

For organizations using Cisco SD-WAN Cloud-Pro with a dedicated fabric and fewer than 800 devices, migrating to Cisco SD-WAN Cloud simplifies operations, reduces daily network management workloads, and ensures compliance with Cisco Catalyst SD-WAN controller policy.

If you do not choose to migrate, the purchase of control component SKUs or a management add-on is required for a dedicated Cisco SD-WAN Cloud-Pro fabric.

Migration process

Eligible customers are contacted to confirm eligibility and provide the necessary information to complete the migration.

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

After you provide the required information, a maintenance window is scheduled within 48 hours. Migration duration depends on the fabric device count and can take up to 6 hours (360 minutes).

The Cloud Operations team performs the migration remotely. Any issues that prevent successful migration are resolved and you are contacted as needed.

The network's data plane remains minimally affected because the control connection automatically re-establishes after migration.

Key feature and compatibility changes

- Enterprise certificates are not supported in Cisco SD-WAN Cloud.
- Custom subnets are not supported. Any custom subnets configured for your Cisco SD-WAN Cloud-Pro dedicated fabric are removed during migration.
- A new URL is generated for accessing Cisco Catalyst SD-WAN Manager.
  - This URL is accessed via the Cisco Catalyst SD-WAN Portal.
  - Previous URLs for Cisco Catalyst SD-WAN Manager are not retained.
- Proxy settings from the Cisco SD-WAN Cloud-Pro dedicated fabric are disabled.
- Statistics and analytics data from your Cisco SD-WAN Cloud-Pro dedicated fabric are not retained.
- Identity provider information from your Cisco SD-WAN Cloud-Pro dedicated fabric is not retained.
- Configuring customer identity provider information is not supported.
- No inbound rules setting is required in Cisco SD-WAN Cloud.

Migration prerequisites

Before migrating from Cisco SD-WAN Cloud-Pro to Cisco SD-WAN Cloud:

- Valid Cisco SD-WAN Cloud licenses must be available in the Cisco Smart Account and Virtual Account for the current dedicated fabric. Contact your Cisco representative for licensing details.
- Upgrade the Cisco SD-WAN Cloud-Pro fabric to match the current Cisco SD-WAN Cloud version. The required version will be provided.

For upgrade instructions, refer to the *Upgrade SD-WAN Controllers with the Use of vManage GUI or CLI* documentation.

- Provide netadmin credentials for the existing Cisco SD-WAN Cloud-Pro fabric upon request.
- Verify that all edge devices run on IOS XE SD-WAN ("cEdge"). Viptela OS ("vEdge") devices are not supported for Cisco SD-WAN Cloud fabrics.
- Cisco Catalyst 8000 Edge Platforms used as cloud gateways for TACACS can be deleted. The system does not support cloud gateways for TACACS. If retained, these platforms remain after migration but are non-functional.

After migration

Once migration completes, the old Cisco SD-WAN Cloud-Pro fabric is no longer operational. Access the new Cisco SD-WAN Cloud fabric using the Cisco Catalyst SD-WAN Portal. For more information, refer to the *Cisco Catalyst SD-WAN Portal Configuration Guide* document.

Key information about migration to a Cloud fabric

Provides answers to frequently asked questions about SD-WAN migration, clarifying common concerns, troubleshooting issues, and offering solutions to support users throughout the migration process.

The 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, access to the latest features, and simplified management and analytics.

Operational benefits

- Cisco SD-WAN Cloud simplifies operations: network administrators manage edge devices, while we handle operational responsibilities for SD-WAN Control Components.
- The solution offers flexible cloud consumption, operational simplicity, and comprehensive analytics.

Migration preparation steps

- Ask your Cisco representative about the required software version for your Cisco SD-WAN Cloud-Pro Control Components and upgrade them as specified.
- Ask your Cisco representative about the required software version for your edge devices and upgrade them. Check device compatibility using the Cisco SD-WAN Control Components Compatibility Matrix.
- Remove unreachable or unused edge device serial numbers from your current SD-WAN Manager.
- Ensure all edge devices are configured with working NTP and DNS servers.
- Do not configure static hostname-to-IP mapping for the SD-WAN Validator. Use the SD-WAN Validator fully-qualified domain name (FQDN) value in System Configuration.
- Ensure you have out-of-band (OOB) direct access to edge devices, especially software-based devices, to address any connectivity issues during migration.

Frequently asked questions

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

The migration is performed in a single maintenance window, which includes migration, post-migration checks, and recovery if needed.

How long does the migration process take?

Plan for at least 8 hours, but the exact time depends on the fabric size.

What are the communication channels during migration?

The primary channel is through a Technical Assistance Center (TAC) support case for coordination and support.

Who is responsible for upgrading Cloud-Pro Control Components and edge devices?

You are responsible for upgrades as part of preparation. Contact CloudOps for assistance if needed. After migration, we will handle future software upgrades for SD-WAN Control Components.

What information must I provide for the migration request?

- Sales or Web Order details for the SD-WAN subscriptions
- Name of the SD-WAN Control Component fabric and target region
- Contact email address
- SD-WAN Manager admin credentials for the existing environment

What precautions should be taken during migration?

Maintain OOB access to edge devices for troubleshooting. Update edge site firewall rules as needed to allow edge devices to communicate with the new public IP addresses of the Control Components.

What steps are required if I am using Enterprise certificates?

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

How is configuration data transferred to the Cloud fabric?

Migration scripts extract all configuration data (policies, templates, and edge device serials) from your current SD-WAN Manager and restore it to the new environment.

Will edge devices automatically connect to the Cloud fabric after migration?

After the configuration is pushed, edge devices will authenticate and connect using previously configured policies.

Is SD-WAN Analytics onboarded during migration?

Analytics is automatically enabled during migration.

Will the controller profile from the Plug and Play (PnP) portal be created in the Cloud environment?

Organization names are used to create controller profiles and link your Smart Account and Virtual Account (SA and VA) using PnP external management features.

Will the data plane be affected during the change window?

Plan for downtime during the change window. Usually, the data plane remains unaffected, but unforeseen events may cause disruption.

Where do I log in after migration?

Continue using the Cisco Catalyst SD-WAN Portal and SD-WAN Manager dashboard via single sign-on (SSO).

How do I verify migration success?

You will receive notification from support. Log in to the Cisco Catalyst SD-WAN Portal, open Cisco SD-WAN Manager, and review your devices and configurations.

What should I do if edge device issues occur after migration?

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

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

Review role assignments in the Cisco Catalyst SD-WAN portal by navigating to **Overlay Details** > **User** as needed. Support can assist.

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

Maintain OOB access to edge devices to update the SD-WAN Validator DNS and organization (sp-org-name) values for fallback to the source Cisco SD-WAN Manager.

What risks are involved with this migration?

Risks include temporary loss of connectivity, device control issues, or incomplete migration. Strict procedures minimize these risks.

What features are enabled by default in a new Cloud fabric?

SD-WAN Analytics and Cloud OnRamp for SaaS are enabled by default, even if previously disabled. Software-Defined Application Visibility and Control (SD-AVC), SSO, and the Remote Software Upgrade Image Repository are also enabled.

Will my existing SD-WAN Analytics and reporting continue post-migration?

SD-WAN Analytics and reporting capabilities will remain intact.

What happens to my Cloud-Pro Control Components after migration?

After migration, the system deletes the Cisco SD-WAN Cloud-Pro Control Components.

Will CLI access to Control Components be available after migration?

CLI access is not available after migration.

What do I do when public IP addresses of Control Components change?

If public IP addresses of the SD-WAN Control Components change, update your firewall rules. You can request the public IP addresses of the SD-WAN Control Components from the SD-WAN Cloud Infra team via a TAC support case.

5 Use APIs in Cisco SD-WAN Cloud

Topics:

- API keys for Cisco SD-WAN Cloud
- Restrictions for Cisco SD-WAN Cloud API key usage
- Obtain a Cisco API key
- Examples of authenticated API requests with cURL

API keys for Cisco SD-WAN Cloud

Explains the role of API keys in Cisco SD-WAN Cloud and describes how API keys facilitate secure authentication for API access.

An API key, also known as a JSON web tokens (JWT), is a unique code that:

- grants client access to an application programming interface (API),
- serves as a password to prevent unauthorized access, and
- is required for Cisco SD-WAN Cloud customer access to APIs.

A specified fabric user employs an API key to make API calls. The key remains valid until the user is deleted or the user role changes.

API keys in Cisco SD-WAN Cloud Release 20.15 and higher are used for secure API authentication. To access APIs on a Cisco SD-WAN Cloud fabric, you must acquire an API key through the designated process, ensuring proper management for secure operations.

Restrictions for Cisco SD-WAN Cloud API key usage

Lists operational and security restrictions related to Cisco API key usage, emphasizing considerations and limitations that apply when accessing Cisco SD-WAN Cloud APIs.

You can access APIs from Cisco SD-WAN Cloud using your SSO login, but you must follow certain operational and security restrictions. For additional details and documentation, refer to Cisco DevNet.

- **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 or 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 are subject to a rate limit of 10 per second. Cisco SD-WAN Manager enforces an API rate limit of 5 per second.

- **No continuous monitoring**

  Use this feature only for occasional access. For information about API rate limits, see the *Cisco Catalyst SD-WAN Getting Started Guide*.

- **Supported categories**

  API calls are provided only for these categories of operations:

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

- Troubleshooting tools

- **No NAT configuration**

  Cisco SD-WAN Cloud does not support NAT configuration using REST APIs.

Obtain a Cisco API key

Provides step-by-step instructions for obtaining a Cisco API key, outlining the required procedures and prerequisites to enable authorized access to Cisco SD-WAN Cloud APIs.

Enable authorized access to Cisco SD-WAN Cloud APIs by generating and collecting all necessary credentials and endpoint details.

The Cisco SD-WAN Cloud Release 20.15 (and later) lets you generate a personal API key, find your API gateway URL, organization name, and obtain a cross-site request forgery (CSRF) token–all prerequisites for making secure authorized API calls.

Before you begin

- Ensure you have access to your Cisco SD-WAN Cloud fabric with an account for which you can view My Profile.
- Make sure you have administrative privileges, if required, to generate API tokens or view organizational settings.

Follow these steps to obtain your Cisco API key and all related authentication values:

Procedure

1. Log in to your SD-WAN Cloud fabric.
2. Select **My Profile** from the drop-down menu under your user ID.
3. Obtain your API key (also called 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**.

      The system generates and displays the API key.

   c) Copy the API key, or download it.
4. Obtain your organization name.
   a) Open **Administration** > **Settings** > **Organization name**.
   b) Copy the name from the **Organization name** field.
5. Obtain your API gateway URL.

   Use the endpoint information provided. In the payload, use the organization name for 'org' and the API key for 'apikey'.

   #### 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, a new API gateway might have been provisioned near your location. Start a new process to connect to the newly provisioned gateway for your overlay.

You receive the API Gateway URL in the response.

6. Obtain your 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.

   Example
   Based on the returned gateway URL, use the full pathname https://apigw1clouduswest2-1024.viptela.info/dataservice/client/token in your GET request.
   You receive the CSRF token in the response.

You have collected your API key, organization name, gateway URL, and CSRF token—everything needed to authenticate and make secure API calls.

What to do next

Use the information you have obtained to make API calls. Note that some API calls, such as PUT and POST, require the CSRF token.

Examples of authenticated API requests with cURL

Provides practical examples of executing authenticated API calls using API keys, gateway URLs, and CSRF/XSRF tokens with cURL commands for GET, PUT, and POST requests.

This section demonstrates how to use API keys, gateway URLs, and CSRF/XSRF tokens to execute authenticated API requests with cURL.

GET API request example using cURL

You can retrieve the resource specified by the location parameter using cURL and the required headers for authentication:

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

```
...
a_fcNoeAlVYvrXzDXA'
```

PUT or POST API request example using cURL

You can send data to the resource specified by the location parameter using a PUT request with cURL, including the necessary headers and data payload:

```
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"}'
```

These examples show how to include authentication headers and data payloads to interact securely with the API endpoints.

6 Integrate Cisco Identity Services Engine

Topics:

- Cisco ISE features
- Prerequisites for Cisco ISE integration
- Configure Cisco ISE integration in SD-WAN Manager

Cisco ISE features

Explains the fundamental concepts and features of Cisco ISE, providing an overview of its role in secure identity management and network access control.

The Cisco Identity Services Engine (Cisco ISE) feature is a capability of a centralized policy engine that:

- simplifies identity management by providing a single point of control for authentication, authorization, and accounting (AAA),
- integrates with network infrastructure to enable context-aware access, and
- enforces security policies using identity, location, and device information for granular access permissions.

Cisco ISE integrates with your Cisco SD-WAN Cloud environment to enable centralized authentication, authorization, and policy management, enhancing visibility, control, compliance, and security across the network infrastructure.

Integrating Cisco ISE with Cisco SD-WAN Cloud enhances identity-based policies and visibility across your network fabric.

Using standalone authentication solutions without Cisco ISE does not enable centralized management, context-aware access, or granular security policies.

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

Prerequisites for Cisco ISE integration

Details the requirements and dependencies necessary for successful Cisco ISE integration, including software, hardware, and configuration prerequisites.

To integrate the Cisco Identity Services Engine (Cisco ISE), gather these items and files:

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

Configure Cisco ISE integration in SD-WAN Manager

Configure Cisco Identity Services Engine (ISE) integration within SD-WAN Manager to enable secure access and seamless policy management for your SD-WAN fabric.

Integrate Cisco ISE with SD-WAN Manager to centrally manage identity services, enforce policies, and improve security in your SD-WAN environment.

Use this task when you need to enable Cisco ISE integration for a fabric in SD-WAN Manager, which allows for unified access control and policy enforcement across your SD-WAN deployment.

Before you begin

- Ensure you have administrative access to SD-WAN Manager.

- Obtain the Cisco ISE server IP address, username, and password.
- Verify that required CA certificates are available in the correct format (`.cer`).
- Confirm that VPN and firewall rules allow communication between SD-WAN Manager and the Cisco ISE server, including necessary ports (HTTPS/443 and pxGrid).

Procedure

1. Log in to your SD-WAN Manager dashboard.
2. Go to **Administration** > **Integration Management**.
3. Select the **Identity Services Engine** tab.
4. Click **Add Connection**.
5. In the **Add ISE Server** panel, enter this required information:
   - ISE Server IP Address: Enter your Cisco ISE server's IP address.
   - Username: Enter the administrative username for ISE.
   - Password: Enter the corresponding password.
   - VPN: Select the appropriate VPN to ensure network connectivity between SD-WAN Manager and Cisco ISE server.
6. Upload the trusted CA certificates to establish a secure connection:
   a) Under the **ISE Server CA** section. upload the Cisco ISE Server CA certificate.
   b) Under the **pxGrid Server CA** section, upload the pxGrid Server CA certificate for pxGrid communication.
7. Review all entered information for accuracy, then click **Submit**.

SD-WAN Manager attempts to authenticate and establish a connection with the Cisco ISE server. If successful, the server status updates to “Connected” or “Active” in the Integration Management list.

If you encounter errors:

- Field Required Errors: Ensure all required fields are completed.
- Certificate Errors: Check certificate formats and expiry dates.
- Connectivity Issues: Confirm VPN routing and firewall rules are correctly configured.

What to do next

Ensure Cisco ISE integration is enabled for the SD-WAN fabric in the SD-WAN Portal. If not done during fabric creation, follow the steps in Enable Cisco ISE integration for a fabric on page 31 to enable ISE integration for the fabric.

Enable Cisco ISE integration for a fabric

Provides instructions for enabling Cisco ISE integration within a fabric through the SD-WAN Portal, including selecting the fabric, activating integration, and entering VPN identification.

Note

You can enable ISE Integration when creating a fabric. For more information, refer to Create a Cloud fabric in the SD-WAN Portal on page 9.

Procedure

1. Log in to your SD-WAN Portal.
2. Select the desired fabric.
3. From the **Actions** menu, select **Enable ISE Integration**.
4. Enter the VPN ID and click **OK**.