

# Cisco Catalyst SD-WAN Portal Configuration Guide

**First Published:** 2022-12-01

**Last Modified:** 2026-08-05

**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 **Cisco Catalyst SD-WAN Portal Feature History** 3

Cisco Catalyst SD-WAN Portal Feature History 3

CHAPTER 3 **Cisco Catalyst SD-WAN Portal** 7

Overview of the Cisco Catalyst SD-WAN Portal 7

Prerequisites for the Cisco Catalyst SD-WAN Portal 10

Benefits of the Cisco Catalyst SD-WAN Portal 10

Smart Accounts and Virtual Accounts 10

CHAPTER 4 **Access the Cisco Catalyst SD-WAN Portal** 13

Workflow for Smart Account and Virtual Accounts for provisioning control components 13

Create a Virtual Account associated with your Smart Account 14

Workflow for certified overlays 15

Access the Cisco Catalyst SD-WAN Portal for the first time 15

Log in to the Cisco Catalyst SD-WAN Portal 16

Access the SD-WAN Manager from the SD-WAN Portal 16

Reset the Cisco Catalyst SD-WAN Manager Admin password 16

Configure additional MFA options or update an existing MFA option 17

CHAPTER 5 **Configure an Identity Provider for the Cisco Catalyst SD-WAN Portal** 19

Configure an identity provider for the Cisco Catalyst SD-WAN Portal 19

CHAPTER 6 **Manage Role-based Access** 21

Configure Cisco Catalyst SD-WAN Portal roles for IdP users 21

Create additional roles 21

CHAPTER 7 Manage Fabrics 23

Create a Cisco SD-WAN Cloud-Pro fabric 23

Configure advanced options for a Cisco SD-WAN Cloud-Pro fabric 27

Hybrid fabrics and on-premises SD-WAN Controllers 32

Delete a fabric 32

Specify the allowed list of IP addresses for managing control component access 32

CHAPTER 8 Use Cisco Catalyst 8000V as a Cloud Gateway for a fabric 35

Information about Cisco Catalyst 8000V as a cloud gateway for a fabric 35

Use cases for Cisco Catalyst 8000V as a cloud gateway for a fabric 36

Prerequisites for Cisco Catalyst 8000V as a cloud gateway for a fabric 36

Restrictions for Cisco Catalyst 8000V as a cloud gateway for a fabric 36

Configure Cisco Catalyst 8000V as a cloud gateway for a fabric 37

CHAPTER 9 Monitor Fabrics 41

Monitor control components and devices in fabrics 41

View fabric and control component details 41

View change window notifications 42

CHAPTER 10 Manage Predefined Inbound Routes 45

Information about predefined inbound rules 45

Configure predefined inbound rules 46

CHAPTER 11 Configure Certification Compliance 49

Cisco Catalyst SD-WAN compliance and certification 49

Benefits of a certified environment 50

Enable compliance with industry certifications for a new fabric 50

Enable compliance with industry certifications for an existing fabric 51

View certification compliance 51

CHAPTER 12 Configure System Snapshots 53

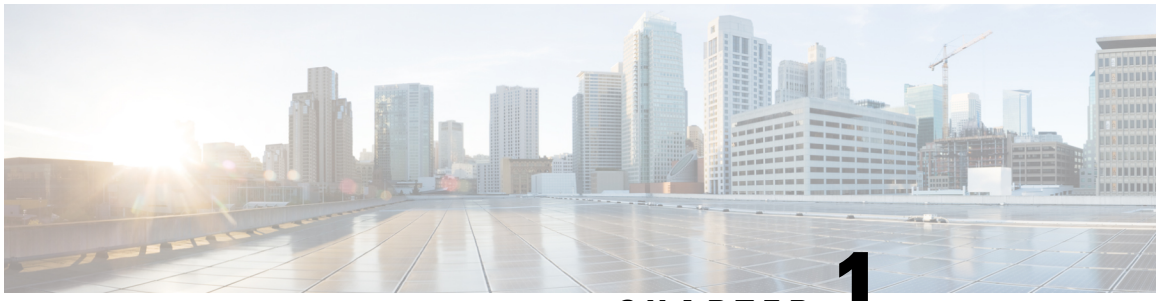
Information about system snapshots 53
Take an on-demand snapshot 54
View snapshots 55

CHAPTER 13 Configure Webhooks 59
Information about webhooks 59
Configure a webhook 59
Send a webhook notification 60

CHAPTER 14 Configuration Conversion Tool 61
Configuration Conversion Tool feature history 61
Information about the Configuration Conversion Tool 61
Restrictions for the Configuration Conversion Tool 62
Prerequisites for the Configuration Conversion Tool 62
Use the Configuration Conversion Tool 62

CHAPTER 15 Frequently Asked Questions 65
Frequently Asked Questions 65
How to 66
Troubleshooting 66

CHAPTER 16 Troubleshoot the Cisco Catalyst SD-WAN Portal 69
Update an expired IdP certificate 69
Reset a Misconfigured IdP 69
Troubleshoot Smart Account issues 70
Troubleshoot Virtual Account issues 70
Troubleshoot browser security issues 71



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

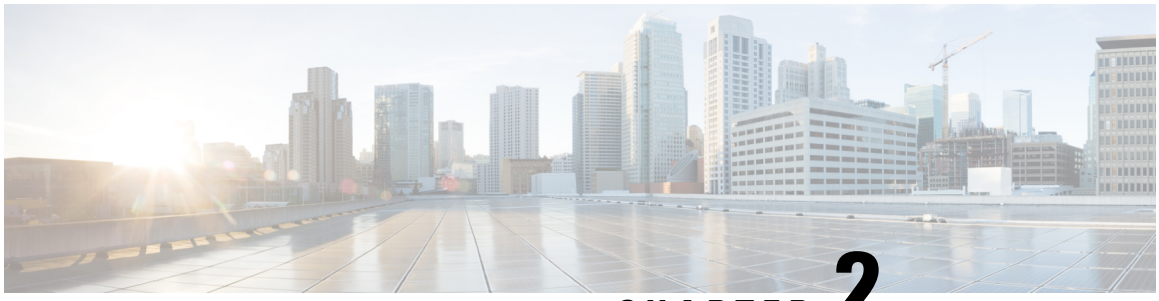
- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17

### 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

# Cisco Catalyst SD-WAN Portal Feature History


• Cisco Catalyst SD-WAN Portal Feature History, on page 3


## Cisco Catalyst SD-WAN Portal Feature History

*Table 1: Feature History*

| Release date | Feature name | Description |
|---|---|---|
| July 2026 | Support for on-premises SD-WAN Controllers in Cloud-Pro fabrics. | You can manage your own on-premises SD-WAN Controllers in a hybrid Cloud-Pro fabric. |
| April 2026 | Software Release Category default selection changes. | If you have UNX licenses, the default software release category when creating a new fabric is Early Adopter. |
| April 2026 | Customer email alert for CMK key failures | If you are using Customer Managed Keys with your AWS-hosted fabric, they are monitored, and you will receive an email alert if any irregularity is detected. |
| March 2026 | Fabric creation process updates | Fabric creation includes a check for paid licenses and option to use them. The Cloud-Pro-A fabric type is supported on AWS for customers with UNX licenses. |
| March 2026 | WAF/ALB enabled on-demand for AWS MT fabrics. | AWS Application Load Balancer (ALB) and Web Application Firewall (WAF) can be enabled on demand for empty Cloud-Pro MT fabrics. |
| March 2026 | MLSA license information captured by SD-WAN Portal. | The SD-WAN Portal receives Managed Services License Agreement (MSLA) license information and manages fabric expiration at the SA level. |
| March 2026 | Customer-provided CMK encryption keys are supported for SD-WAN Cloud-Pro AWS-hosted fabrics. | Customer Managed KMS (CMK) encryption keys can be provided and managed for new or existing AWS-hosted fabrics. |
| March 2026 | Open Cisco SD-WAN Manager directly from the SD-WAN Portal | The Fabric Details page includes a browser link to launch the SD-WAN Manager without re-entering credentials. |

Cisco Catalyst SD-WAN Portal Feature History

| Release date | Feature name | Description |
|---|---|---|
| February 2026 | Reset SD-WAN Manager Admin password from non-Cisco-hosted fabric | You can reset the SD-WAN Manager Administrator password for a non-Cisco-hosted fabric in the SD-WAN Portal. |
| January 2026 | Cisco ISE integration | Cisco SD-WAN Cloud customers can use Cisco Identity Services Engine (ISE) for enhanced identity-based policies and visibility across the network fabric. |
| December 2025 | Reset SD-WAN Manager Admin password from Cisco-hosted fabric | You can reset the SD-WAN Manager Administrator password for a Cisco-hosted fabric in the SD-WAN Portal. |
| December 2025 | Non-Cisco hosted overlays created by easy onboarding service displayed for internal users. | Internal Cisco Catalyst SD-WAN Portal users can view non-Cisco hosted overlays created by the easy onboarding service. |
| November 2025 | Non-Cisco hosted overlays created in SD-WAN Manager displayed for users with Customer role | You can view non-Cisco hosted overlays created in SD-WAN Manager in Cisco Catalyst SD-WAN Portal. |
| October 2025 | Automatic email confirmation after Cisco SD-WAN Cloud and Cloud-Pro purchases | After you purchase Cisco SD-WAN Cloud or Cloud-Pro subscriptions, the Cisco Catalyst SD-WAN Portal sends you confirmation emails and guidances for next steps. |
| October 2025 | TAC case hyperlink available when creating fabric | If you need assistance when selecting a fabric type for a new fabric, you can open a TAC case directly from the window. |
| October 2025 | Customer Name field added to fabric overview | You can view and search on the customer name in the Overview page for Cisco SD-WAN Cloud-Pro fabrics. |
| September 2025 | Release Notes and FAQ support links in Resources area | The Resources area for Cisco SD-WAN Cloud-Pro fabrics in the Cisco Catalyst SD-WAN Portal display includes links for Release Notes and FAQ documentation. |
| August 2025 | Enhanced Proof of Concept (POC) workflow | The POC workflow has been improved to simplify onboarding and other POC operations.<br>**Note**<br>The Cisco Catalyst SD-WAN Portal provides access to both production and POC workflows. If you need to execute a POC project before purchasing a Cisco SD-WAN offering, contact your account team to discuss details. |

Cisco Catalyst SD-WAN Portal Feature History

| Release date | Feature name | Description |
|---|---|---|
| August 2025 | SD-WAN Manager session management and bookmarking | After you successfully log in to Cisco Catalyst SD-WAN Portal and access your fabric for the first time, you can bookmark the SD-WAN Manager URL and then directly access SD-WAN Manager there with your CCO email and password.<br>The Cisco Catalyst SD-WAN Portal and SD-WAN Manager share the same session timer and active or idle status. |
| August 2025 | Display **Snapshot Frequency** and **Max Snapshot** in Cisco Catalyst SD-WAN Portal | The **Snapshot Frequency** and **Max Snapshot** counts are displayed on the **Overlay Details** and **Snapshot** pages. |
| July 2025 | New fabric creation workflow | There is a new workflow for fabric creation. The process is customized for your site needs and automated to improve response time. |
| June 2025 | Improved fabric creation load time | Virtual Accounts are retrieved directly from the Cisco Catalyst SD-WAN Portal database, so they load much faster. |
| May 2025 | **Software Release Category** field in **Create Fabric** page for Cloud fabrics. | You can choose between Recommended and Early Adopter software release when creating a Cisco SD-WAN Cloud fabric. |
| April 2025 | Improved loading time for Cisco Catalyst SD-WAN Portal | The Cisco Catalyst SD-WAN Portal loading time is significantly improved. |
| April 2025 | Snapshot retention changes | Retention time for a golden snapshot changed from 180 days to 90 days. Retention time for an on-demand snapshot changed from 90 days to 10 days.<br>The number of retained regular snapshots, taken automatically, changed from 10 to 7.<br>Snapshots are retained only in the Primary region. |
| March 2025 | Configuration Conversion Tool | A configuration conversion tool available through the Cisco Catalyst SD-WAN Portal enables you to convert device templates into configuration groups, and traditionally configured policies into policy groups. The policy conversion is considered to operate at a beta level in this release, performing a best-effort conversion.<br>Converting configurations to configuration groups enables all of the benefits of the newer device-agnostic configuration model. |

Cisco Catalyst SD-WAN Portal Feature History

| Release date | Feature name | Description |
|---|---|---|
| February 2025 | Additional network compliance certification support | The Cisco Catalyst SD-WAN solution supports these network compliance certifications: SOC2 Type2, ISO 27001, ISO 27701, ISO 27017, ISO 27018, C5, and ENS<br>These compliance certifications are supported on all long-lived releases. |
| October 2024 | Webhook notification support | Support for sending notifications based on network events in the SD-WAN fabric. |
| August 2024 | Use of any email account for a support ticket | On the **Dashboard** > **Overlays** > **Details** page, you can open a support ticket for the SD-WAN fabric. When opening a support ticket, you can specify any email address for contact information. |
| August 2024 | Fabric details page shows Cisco support case information | In the SD-WAN Portal, the **Service Requests** section of the **Fabric Details** page shows Cisco Support cases related to the fabric. |



CHAPTER 3

# Cisco Catalyst SD-WAN Portal


- Overview of the Cisco Catalyst SD-WAN Portal, on page 7
- Prerequisites for the Cisco Catalyst SD-WAN Portal, on page 10
- Benefits of the Cisco Catalyst SD-WAN Portal, on page 10
- Smart Accounts and Virtual Accounts, on page 10


## Overview of the Cisco Catalyst SD-WAN Portal

The Cisco Catalyst SD-WAN Portal is a cloud-infrastructure automation tool that:

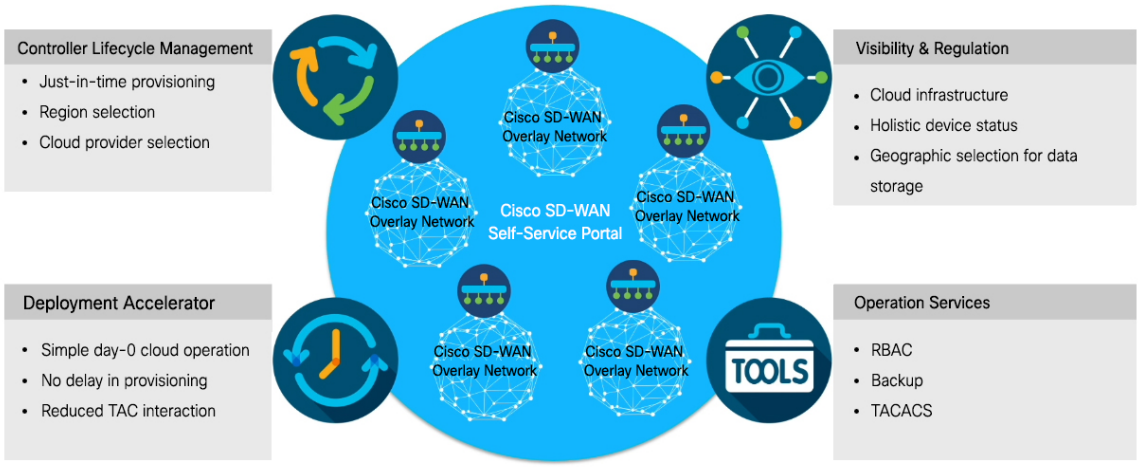
- is tailored for Cisco Catalyst SD-WAN,
- provides a quick way to provision, monitor, and maintain Cisco Catalyst SD-WAN control components on public cloud providers, and
- supports user authentication and granular access management for high security.

You can provision these control components using the Cisco Catalyst SD-WAN Portal:

- Cisco SD-WAN Manager
- Cisco SD-WAN Validator
- Cisco SD-WAN Controller
- Optional virtual devices such as the Cisco Catalyst 8000v

## Benefits and Functions

***Figure 1: Cisco Catalyst SD-WAN Portal Benefits and Operations***




The Cisco Catalyst SD-WAN Portal enforces multi-factor authentication (MFA) by default for the portal access. You can configure the Cisco Catalyst SD-WAN Portal to use an identity provider (IdP) that lets you connect any user with any application on any device, using single sign-on (SSO). The Cisco Catalyst SD-WAN Portal is modularized into separate web servers, backend servers, and database clusters to achieve software scalability.

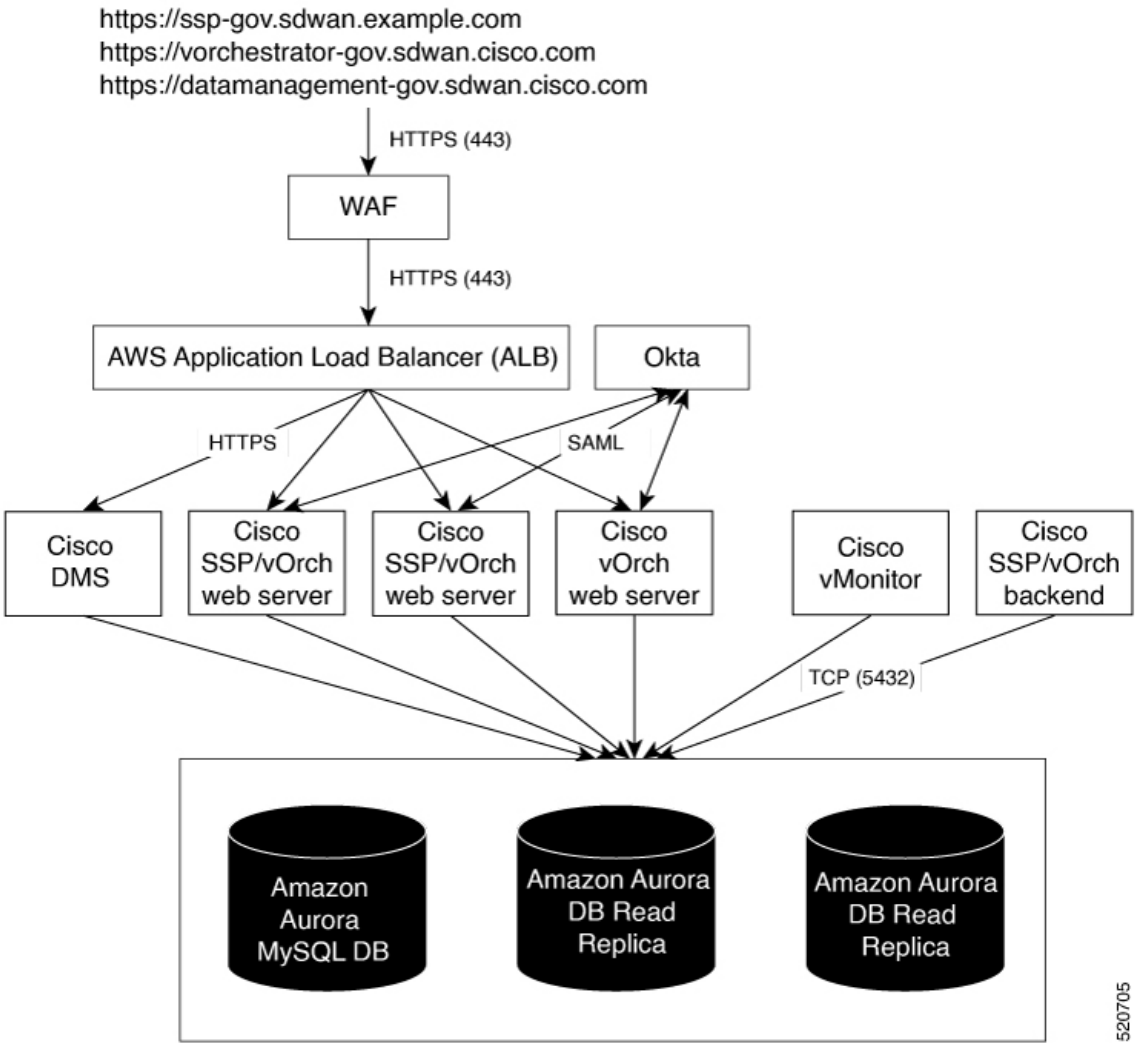
Cisco vMonitor collects data on the cloud infrastructure and generates health notifications about the overlay infrastructure for the customer in a common database. The Cisco vOrchestrator web server is also accessible for advanced features and existing infrastructure-tier customizations, if any, that you use. The Cisco Catalyst SD-WAN Portal uses Cisco vMonitor and Cisco vOrchestrator by way of API calls to orchestrate actions and monitor the overlay.

**Note** Cisco vMonitor and Cisco vOrchestrator can be accessed by Cisco FedOps only.

All three applications use a common global database that includes multiple read replicas for high availability and disaster recovery. The applications connect to the database using either Transport Layer Security (TLS) or Secure Sockets Layer (SSL).

## Architecture (Government)

*Figure 2: Cisco Catalyst SD-WAN Portal Architecture*




## Audience

This document is intended for customers such as service providers, partners, and other end users.

There are two types of users for Cisco Catalyst SD-WAN Portal for Government:

- Customers, such as service providers, partners, and other end users.
- Cisco Catalyst SD-WAN Federal Operations (FedOps): A Cisco team that maintains and monitors Cisco Catalyst SD-WAN for Government.

# Prerequisites for the Cisco Catalyst SD-WAN Portal

- Purchase a Cisco DNA subscription from the Commerce Workspace.
- Create or open an existing Smart Account.
- Create a Virtual Account that is associated with your Smart Account.
- Add the device serial numbers on the Plug and Play Connect (PnP) portal.

  For more information, see the Network Plug and Play Connect Capability Overview.

# Benefits of the Cisco Catalyst SD-WAN Portal

The Cisco Catalyst SD-WAN Portal:

- enables visibility into critical statistics like instance CPU utilization,
- provides a centralized dashboard for real-time monitoring of your Cisco Catalyst SD-WAN overlay networks,
- includes a wizard-driven interface that helps you easily navigate to tasks within the workflow,
- lets you select cloud providers and specify geographic locations for primary and secondary data storage,
- supports secure login using an identity provider (IdP) for single sign-on (SSO) with multi-factor authentication (MFA),
- supports role-based access control (RBAC),
- and supports provisioning new overlay networks with custom subnets that enable on-premises TACACS+ server connections.

# Smart Accounts and Virtual Accounts

For more information, see Workflow for Smart Account and Virtual Accounts for Provisioning the Controllers.

### Smart Accounts

Smart Accounts are centralized, cloud-based data repositories that:

- contain the software licenses purchased by an organization,
- serve as a central hub for license management, and
- enable real-time enterprise-wide license management and compliance.

Use the Smart Account as a central repository to view software assets you have purchased, register and report software use, and manage licenses for your organization.

Using the Cisco Catalyst SD-WAN Portal, the Smart Account administrator can view and manage your control component infrastructure. Management tasks include viewing IP addresses for control components and

changing the control component IP access lists. To restrict access for other users, go to the Manage Smart Account section on Cisco Software Central and remove those users as Smart Account administrators. Alternatively, use the identity provider (IdP) onboarding feature to grant access to the Cisco Catalyst SD-WAN Portal based on trusted users in the IdP.

### Virtual Accounts

Virtual Accounts are subaccounts within your Smart Account that:

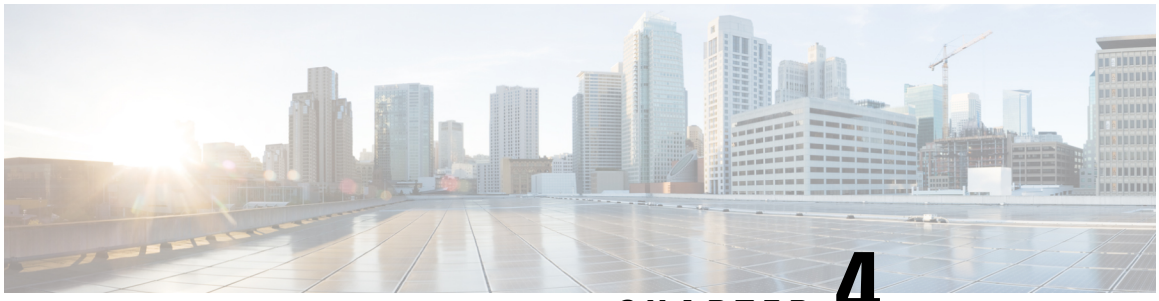
- help you organize your Cisco assets in a way that aligns with your business,
- can be set up by department, product, geography, or another designation that suits your business model, and
- allow you to organize and manage your software licenses, devices, and users more granularly.

The system creates a default Virtual Account for you. Create an additional dedicated Virtual Account for Cisco Catalyst SD-WAN fabrics.

For more information, see Create a Virtual Account Associated with Your Smart Account.

To provision a Cisco Catalyst SD-WAN control component, associate a Virtual Account with an offer attribute that is Cisco Catalyst SD-WAN-capable. An Cisco Catalyst SD-WAN-capable attribute is associated with a Virtual Account when ordering your Cisco DNA cloud license.

**Note** When you order DNA licenses using the enterprise agreement, the system does not automatically associate Virtual Accounts to an SD-WAN-capable attribute. Submit a cloud control component provisioning request form through the Enterprise Agreement Workspace for the CloudOps team to provision the control components. Contact Cisco Catalyst SD-WAN Technical Support to request access to the desired Virtual Account on the Cisco Catalyst SD-WAN Portal. After receiving access, you can provision the control components by providing the necessary enterprise agreement contract information.



CHAPTER 4

# Access the Cisco Catalyst SD-WAN Portal


- Workflow for Smart Account and Virtual Accounts for provisioning control components, on page 13
- Create a Virtual Account associated with your Smart Account, on page 14
- Workflow for certified overlays, on page 15
- Access the Cisco Catalyst SD-WAN Portal for the first time, on page 15
- Log in to the Cisco Catalyst SD-WAN Portal, on page 16
- Access the SD-WAN Manager from the SD-WAN Portal, on page 16
- Reset the Cisco Catalyst SD-WAN Manager Admin password, on page 16
- Configure additional MFA options or update an existing MFA option, on page 17


## Workflow for Smart Account and Virtual Accounts for provisioning control components

This workflow describes how to create a Smart Account, create a Virtual Account, and associate the Cisco DNA subscription with your Virtual Account.

1. Open Cisco Software Central and create a Smart Account for your organization.
2. Create a Virtual Account associated with your Smart Account.

   For instructions on how to create a Virtual Account, review Create a Virtual Account Associated with Your Smart Account.
3. At the Cisco Commerce Workspace, purchase a Cisco DNA subscription.

**Note** You must associate the Cisco DNA subscription with one Virtual Account within the respective Smart Account.

   An account manager or sales representative usually places the order for the customer.
4. Choose the DNA cloud subscription product identification (PID) for your license.

   Selecting the DNA cloud subscription PID automatically associates your Virtual Account with the SD-WAN-capable attribute for control component provisioning.
5. When the order is complete, the Virtual Account is available on the Cisco Catalyst SD-WAN Portal for control component provisioning.

**Note** The Virtual Account must include the device serial numbers that were added on the Cisco Plug and Play (PnP) portal. AFter creating the overlay through the Cisco Catalyst SD-WAN Portal, see the **Control Component Profile** tab on the Cisco PnP portal to view the mapping of the device serial numbers with their respective control components. This mapping provides the necessary information to add the devices to Cisco SD-WAN Manager or to perform zero-touch provisioning (ZTP). To confirm control component provisioning as part of the overlay creation process using the Cisco Catalyst SD-WAN Portal, view the **Control Component Profile** tab in the Cisco PnP portal.

For additional details, refer to Cisco Network Plug and Play Connect Capability Overview.

# Create a Virtual Account associated with your Smart Account

### Before You Begin

Create a Smart Account for your organization using Cisco Software Central.

For information on creating a Smart Account, refer to the Workflow for Smart Account and Virtual Accounts for Provisioning the Controllers documentation.

### Create a Virtual Account

1. In Cisco Software Central, choose **Manage account** under **Manage Smart Account**.
2. Click **Virtual Accounts**.
3. Click **Create Virtual Account**.
4. Click **Review Notice**, and after reviewing the notice, click **I Have Reviewed the Notice**.
5. Enter the required information in each field.

**Note** The **Parent Account** field is autopopulated with **At Top Level**. You may retain this selection.

6. Click **Next**.
7. (Optional) Assign users to the Virtual Account.
8. Click **Next**.
9. Click **Create Virtual Account**.

   The newly created Virtual Account is listed in Virtual Accounts.

# Workflow for certified overlays

### Workflow for certified overlays for new customers

1. If you are a new Cisco Catalyst SD-WAN customer or partner, place an order on the Cisco Commerce Workspace.
2. Choose the **Certified Hosting Infra for vManage PID** subscription option.
3. Follow the same steps as for any other order.

**Note** Ensure that you select the correct PID that corresponds to the certified overlay.

### Workflow for certified overlays for existing customers

1. If you are an existing Cisco Catalyst SD-WAN customer or partner, place an order on the Cisco Commerce Workspace with an existing Virtual Account.
2. Select the **Certified Hosting Infra for vManage PID** subscription option.
3. Create a ticket in Cisco One.

   Include this information in the ticket:

   - Virtual Account
   - Organization Name
   - Order Number
   - Region

4. The CloudOps team confirms the order. Then, they upgrade an existing overlay to a certified overlay.

# Access the Cisco Catalyst SD-WAN Portal for the first time

When you log in to the Cisco Catalyst SD-WAN Portal for the first time, you see a guided workflow. You can use this workflow to configure selected features and to create your first Cisco Catalyst SD-WAN overlay network.

Log in to the Cisco Catalyst SD-WAN Portal for the first time as a Smart Account administrator. If you do not use an identity provider (IdP), you must have Smart Account administrator privileges each time you log in.

If you use an IdP, you can access the Cisco Catalyst SD-WAN Portal with the permissions provided by the IdP.

**Note** You cannot use Virtual Account administrator-level access to log in to the Cisco Catalyst SD-WAN Portal, but you can use it with other portals, such as software.cisco.com. The Cisco Catalyst SD-WAN Portal does not accept Virtual Account administrator-level access.

# Log in to the Cisco Catalyst SD-WAN Portal

1. For the commercial version of the Cisco Catalyst SD-WAN Portal, navigate to: https://ssp.sdwan.cisco.com/

   For the government version, log in at: https://ssp-gov.sdwangov.fedramp.cisco
2. Enter your appropriate login credentials.
3. When prompted, set up or enter your multi-factor authentication (MFA) credentials. MFA is required for all users.

# Access the SD-WAN Manager from the SD-WAN Portal

From the **Fabric Details** page in the SD-WAN Portal, you can log in to SD-WAN Manager by clicking the **SD-WAN Manager** browser link in the **Description** pane. You can bookmark this link for later use. You do not need to re-enter your credentials while your session is active.

**Note** The SD-WAN Portal and SD-WAN Manager share the same session timer and active or idle status. If your login session is about to time out, you will be requested to extend it, whether you are using SD-WAN Portal or SD-WAN Manager.

# Reset the Cisco Catalyst SD-WAN Manager Admin password

If you forget the Administrator password to access SD-WAN Manager from a fabric, you can change it from the SD-WAN Portal.

### Cisco-Hosted Fabrics

1. Select **Cisco-Hosted Overlays** from the SD-WAN Portal Dashboard.
2. Choose a fabric and click **Details**.
3. From the **Actions** menu on the Fabric Details page, select **SD-WAN Manager Password Reset**.
4. Enter the new password, following the displayed rules.
5. Re-enter the new password and click **Confirm**.

### Non-Hosted Fabrics

Before proceeding, verify your organization's whitelist and firewall settings and ensure that your SD-WAN Manager is reachable from ssp.sdwan.cisco.com.

1. Select **Non-Cisco Hosted Overlays** from the SD-WAN Portal Dashboard.
2. Choose a fabric and click **Details**.
3. From the **Actions** menu on the Fabric Details page, select **SD-WAN Manager Password Reset**.
4. Enter the IP address or DNS address of the SD-WAN Manager.
5. Enter the new password, following the displayed rules.
6. Re-enter the new password and click **Confirm**.

# Configure additional MFA options or update an existing MFA option

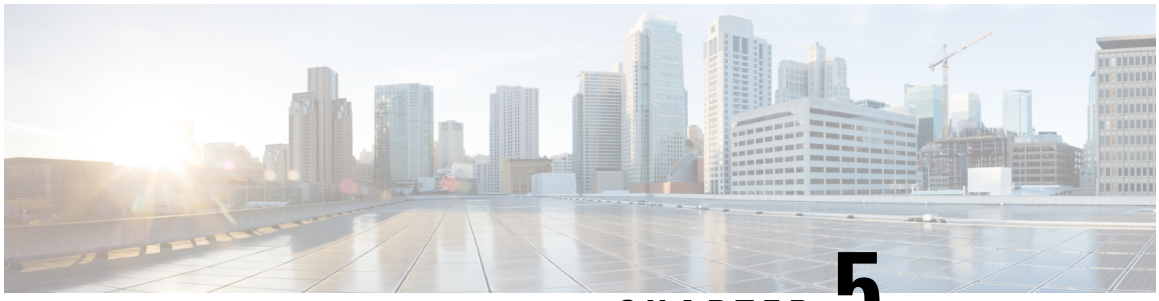
You can add an additional MFA option or update an existing MFA option using the Cisco SD-WAN portal.

### Before You Begin

Ensure that you can log in successfully to the Cisco Catalyst SD-WAN Portal.

### Add or Update an MFA Option

1. After you successfully log in to the Cisco SD-WAN Self-Service Portal, go to Cisco SD-WAN SSO.
2. On the SSO page, you will see Cisco Catalyst SD-WAN Portal under the **Work** tab.
3. From the drop-down list by your name in the top right corner of the page, click **Settings**.
4. In the **Extra Verification** section, add an MFA option or update an existing MFA option.



CHAPTER 5

# Configure an Identity Provider for the Cisco Catalyst SD-WAN Portal


• Configure an identity provider for the Cisco Catalyst SD-WAN Portal, on page 19


## Configure an identity provider for the Cisco Catalyst SD-WAN Portal

When you log in to the Cisco Catalyst SD-WAN Portal for the first time, you have the option to configure the Cisco Catalyst SD-WAN Portal to use the identity provider (IdP) of your organization, such as Okta Identity Management.

**Note** Configuring an IdP for the Cisco Catalyst SD-WAN Portal is optional.

After you configure your IdP and assign roles, you can log in using your organization's IdP instead of your account credentials on Cisco.com. For details on role configuration, refer to Configure Cisco Catalyst SD-WAN Portal Roles for IdP Users.

**Note** Even if you configure your own IdP to allow Portal logins, you must still authenticate with the Cisco IdP using MFA.

**Note** When you set up an IdP in the Cisco Catalyst SD-WAN Portal, the issuer, login URL, and privacy-enhanced mail (PEM) key are not available from the IdP of your organization. This information is available after you set up the Assertion Consumer Service (ACS) URL and audience in your organization's IdP. When setting up your organization's IdP, we recommend that you add placeholder values for the ACS URL and audience. Later, you can configure the IdP on the Cisco Catalyst SD-WAN Portal and update your organization's IdP with the correct value of the ACS URL and audience Uniform Resource Identifier (URI) that is editable in the Cisco Catalyst SD-WAN Portal.

### Before you begin

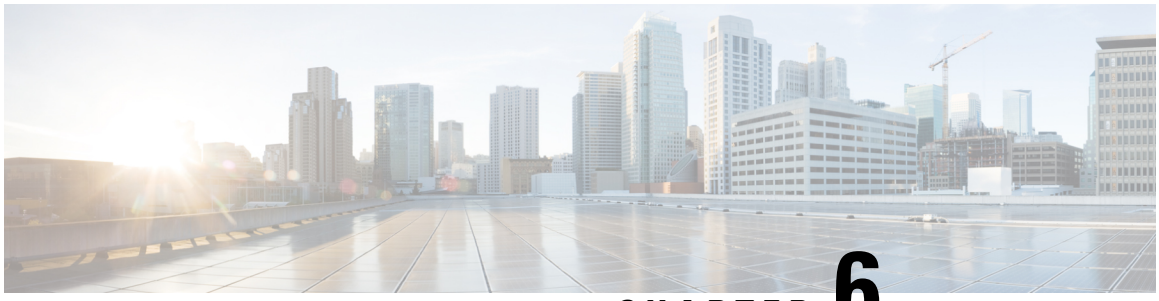
Before you configure an IdP in Cisco Catalyst SD-WAN Portal, create these variables on your organization's IdP. These variables are required for each user who logs in.

- `firstName`
- `lastName`
- `email`
- `SSP_User_Role`

For more information on roles, refer to Configure Cisco Catalyst SD-WAN Portal Roles for IdP Users.

### Configure an IdP for the Cisco Catalyst SD-WAN Portal

1. Specify the following information for your IdP.
   - Domain Name
   - IdP Issuer URL
   - IdP SSO URL
   - IdP Signature Certificate in PEM format
2. In federal environments only, check the **I acknowledge that this is a Federal IDP** check box.
3. To submit your IdP details, click **Submit Request**.
4. On your IdP site, confirm the IdP creation.



CHAPTER 6

# Manage Role-based Access


- Configure Cisco Catalyst SD-WAN Portal roles for IdP users, on page 21
- Create additional roles, on page 21


# Configure Cisco Catalyst SD-WAN Portal roles for IdP users

### Before you begin

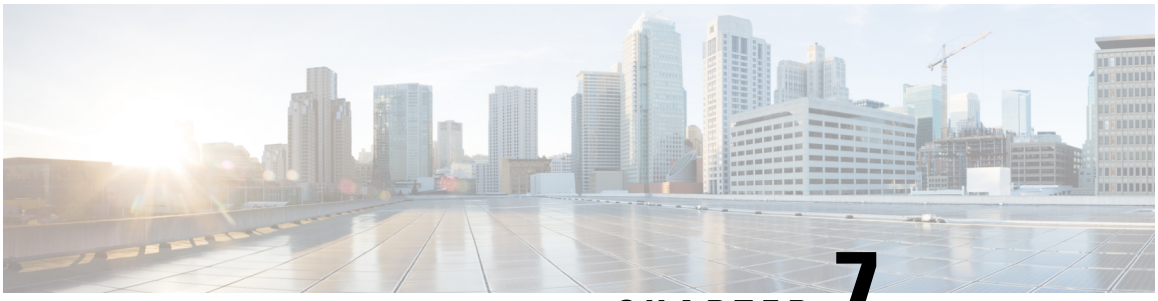
**Note** Configuring Cisco Catalyst SD-WAN Portal roles for an identity provider (IdP) is optional.

### Configure roles for IdP users

1. From the Cisco Catalyst SD-WAN Portal menu, choose **Manage Roles**.
2. Enter a name for the role.
3. For each of your virtual accounts, assign a role from this list:
   - **Monitor**: You can view and monitor all the overlay options in the Cisco Catalyst SD-WAN Portal.
   - **Overlay Management**: You can create, change, and monitor overlay networks.
   - **Administration**: You can perform the tasks defined by the monitor and overlay network roles, and onboard a secondary IdP.
4. Click **Add Role**.
5. After adding all the roles, click **Done**.
6. Log in to the Cisco Catalyst SD-WAN Portal again using your IdP credentials.

# Create additional roles

To create an additional role, repeat the procedure described in the Configure Cisco Catalyst SD-WAN Portal roles for IdP users section.



CHAPTER 7

# Manage Fabrics


- Create a Cisco SD-WAN Cloud-Pro fabric, on page 23
- Configure advanced options for a Cisco SD-WAN Cloud-Pro fabric, on page 27
- Hybrid fabrics and on-premises SD-WAN Controllers, on page 32
- Delete a fabric, on page 32
- Specify the allowed list of IP addresses for managing control component access, on page 32


# Create a Cisco SD-WAN Cloud-Pro fabric

The Cisco Catalyst SD-WAN Portal provisions Cisco Catalyst SD-WAN fabrics using the information you provide during this procedure.

### Before you begin

Ensure that you have these items:

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

**Note** For Cisco SD-WAN Cloud-Pro fabrics, only SA-Admin users can access the Cisco Catalyst SD-WAN Portal and create fabrics.

For Cisco SD-WAN Cloud fabrics, an SA-Admin user must create the fabric, but they can then authorize other users without SA-Admin privileges to access the Cisco Catalyst SD-WAN Portal.

- A valid order for control components on Cisco Commerce (formerly CCW).

### Create a first Cisco SD-WAN Cloud-Pro fabric

1. Go to the URL that you received in the email from Cisco to access the Cisco Catalyst SD-WAN Portal, and log in.
2. From the Cisco Catalyst SD-WAN Portal menu, choose **Create Fabric**.

The **Create Cisco SD-WAN Fabric** page appears.

3. From the **Smart Account** drop-down list, choose the name of the Cisco Smart Account to which you want to associate the fabric.



**Note** If your Cisco Smart Account is not listed in the drop-down, refresh the list and search for your account by its domain ID.

4. 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**.
5. From the **Virtual Account** drop-down list, choose the name of the Cisco Virtual Account to which you want to associate the fabric.
6. Select a Cisco SD-WAN Cloud or Cisco SD-WAN Cloud-Pro Fabric. If you select Cisco SD-WAN Cloud-Pro, a questionnaire dialog box appears. Provide the required details in the dialog box.



**Note** If your site has the appropriate licenses, an option for **Cloud-Pro-A Fabric** will appear. This fabric type functions identically to Cloud-Pro, but uses a pre-selected Cloud Provider.

7. Check the appropriate boxes if you intend to use any of the listed features on the fabric. Select "None of the options" if you do not use any additional features. (required)
8. Enter the number of devices you plan to add to the fabric (required).
9. Enter the sales order number for any SD-WAN subscriptions you have (optional).
10. Click **Next**.

    Based on your responses, you are directed to the Cisco SD-WAN Cloud or Cisco SD-WAN Cloud-Pro fabric creation workflow. Consult the *Cisco SD-WAN Cloud Guide* to create a Cisco SD-WAN Cloud fabric. The remaining instructions apply to creating a Cisco SD-WAN Cloud-Pro fabric.
11. Click **Assign Control Components** and perform these actions in the **Assign Control Components** area:
    a. Configure the options for the number of control component types in a Cisco SD-WAN Cloud-Pro fabric.

| Option | Description |
|---|---|
| **Assign** (for the **SD-WAN Manager** control component type) | Enter the number of Cisco SD-WAN Manager control components in your deployment.<br>Valid values are **1**, **3**, or **6**. |

| Option | Description |
|---|---|
| **Assign** (for the **SD-WAN Validator** control component type) | Enter the number of Cisco SD-WAN Validators in your deployment.<br>The minimum value is **2**. |
| **Assign** (for the **SD-WAN Controller** control component type) | Enter the number of Cisco SD-WAN control components in your deployment.<br>The minimum value is **2**. |
| **Enable Cluster** | Applies only if you choose a value of **3** or **6** for the number of Cisco SD-WAN Manager controllers.<br>Turn on this option to create a Cisco SD-WAN Manager cluster. |
| **Cluster Type** | Applies only if you turn on the **Enable Cluster** option.<br>Choose **Single Tenant Cluster** to enable a single tenant cluster. |

**b.** Click **Assign**.

**12.** In the **Fabric** field, enter a name for your fabric.

**13.** Under **Cloud Provider**, choose **AWS** or **Azure** as the cloud provider at which you want the control components for your fabric to be hosted. Government sites use only Amazon Web Services (AWS).



**Note** IPv6 provisioning is only supported for Single Tenant fabrics hosted on AWS.

**14.** From the **SD-WAN Version** drop-down list, choose the version of Cisco Catalyst SD-WAN that you want to use on your control components.

Use the recommended version unless you require features that are offered only in another version. To see recommended versions, visit Cisco Software Central.

Cisco Catalyst SD-WAN releases are described in the Cisco Catalyst SD-WAN Release Notes in the **Release Information** area in User Documentation for Cisco IOS XE (SD-WAN) Release 17.

**15.** Under **Locations**, perform these actions:

**a.** From the **Primary Location** drop-down list, choose the geographical location where the Cisco SD-WAN Manager is provisioned.

We recommend that you choose a location that is relatively close to your network.

**b.** From the **Secondary Location** drop-down list, choose the geographical location for backed up data storage and load balancing. If you choose the same region for both primary and secondary, then the Cisco Catalyst SD-WAN Portal automatically places the instances in two different Zones within the same region.

We recommend that you choose the location that is closest to the primary location.

c. From the **Data Location** drop-down list, choose the geographical location for Cisco SD-WAN Analytics data storage.

We recommend that you choose the location that is closest to the primary location.

16. Enter this information under **Contacts**:

- In the **Fabric Admins** field, enter one or more comma-separated email addresses or mailing list names to which the Cisco Catalyst SD-WAN Portal sends notifications about the fabric.
- In the **Cisco Contact Email** field, enter the email address of a contact at Cisco that can be reached if there is an urgent issue and the administrator of the fabric cannot be reached.
- In the **Enter Contract Number of Service** field, enter the number of your Cisco Catalyst SD-WAN Portal service contract.
- In the **Enter CCO ID of Service Requester** field, enter the Cisco Connection Online (CCO) ID of the person who created the ticket for your Cisco Catalyst SD-WAN Portal.

Alert Notifications: The Cisco Catalyst SD-WAN Portal generates alert notifications for various events, such as expiring subscriptions, maintenance windows, and feature changes. Notifications are sent to the registered Overlay Admin contact email addresses configured under Overlay Details. Keep your email addresses updated. You can register multiple email addresses. To update your registered email addresses, perform these steps:

a. Log in to Cisco Catalyst SD-WAN Portal at https://ssp.sdwan.cisco.com for commercial sites or https://ssp-gov.sdwangov.fedramp.cisco/ for government sites. You must have PNP Smart Account Administrator role to be able to log in.

Alternatively, if your Smart Account Administrator has already set up an identity provider (IdP) on the Cisco Catalyst SD-WAN Portal, then you can log in with the role provided by your Administrator.

b. Go to **Overlay Details** > **Description** > **Overlay Admin**

c. Click on the pencil icon to edit.

d. Type in your email address and hit **Tab**.

e. Click on the check mark icon to save.

17. Configure the **Advanced Options** as needed.

For detailed information about these options, refer to Configure Advanced Options for a Cisco SD-WAN Cloud-Pro Fabric.

- **Custom Subnets**: Configure private IP addresses for control component interfaces.
- **Custom Domain Settings**: Configure custom domains for accessing Cisco SD-WAN Validator and Cisco SD-WAN Manager.
- **Snapshot Settings**: Configure how often the system takes a snapshot of Cisco SD-WAN Manager instances in your deployment.
- **Custom Organization Name**: Configure a unique organization name to identify your network.
- **Certification Compliance**: Select certification compliances for the fabric. Compliance is on by default in the government version of the Cisco Catalyst SD-WAN Portal.

- **Custom Key Management**: Provide Customer Managed Keys (CMKs) for AWS-hosted fabrics.
- **Dual Stack**: Enable IPv6 dual stack.

18. Click **Click here to review and agree to Terms and Conditions before proceeding**. In the **Terms and Conditions** dialog box, review the displayed information and click **I Agree**.
19. Click **Create Fabric**.

    Your request is submitted. Manual approval for a Cisco SD-WAN Cloud-Pro fabric can take up to 24 hours (1 day). You can view the progress of your request in the **Requests** area.

    In addition, a password appears in the Cisco Catalyst SD-WAN Portal **Notification** page. Use this password to access the fabric for the first time.

    After logging in, change this password immediately to secure your environment.



**Note** The system-provided control component password is no longer visible in the Cisco Catalyst SD-WAN Portal after seven days. We recommend that you keep a copy of the password if you want to retain it.

20. Once you receive a notification that your fabric is ready, follow these steps:
    - Install control component certificates on your devices. For more details about certificate installation, refer to Use Case: Cisco-Hosted Cloud Overlays with Software Version 19.x and Above.
    - Install web server certificates. For information about installing web server certificates, refer to Web Server Certificates.

# Configure advanced options for a Cisco SD-WAN Cloud-Pro fabric

Advanced options allow you to configure various settings for your fabric if the default settings are not what you need.

To configure advanced options for your fabric, click **Advanced Options** on the Cisco Catalyst SD-WAN Portal, then configure options as described in these sections:

- Custom Subnets
- Custom Domain Settings
- Snapshot Settings
- Custom Organization Name
- Compliance Configuration
- Custom Key Management
- Dual Stack

### Custom Subnets

The **Custom Subnets** area includes options for configuring private IP addresses to be used for control component interface IP addresses.

For use cases such as connecting to an enterprise TACACS+, connecting to an authentication, authorization, and accounting (AAA) server, sending messages to a syslog server, or enabling management access to instances over the fabric, you may want to deploy the control components with private IP addresses in specific prefixes which are unique and are not used elsewhere within your fabric.

| Option | Description |
|---|---|
| **Primary Subnet** | |
| **VPC Subnet** | Enter a private IP address block for the VPC for the primary region, For example, 192.168.0.0/24.<br>This IP address block must be reachable from your private network. |
| **Primary Location** | Shows the primary region for the fabric. |
| **Management Subnet** | Enter a private IP address block for the management subnet for the primary region.<br>This address must be within the IP address block that you enter for the VPC.<br>The minimum size of the IP address block is 16 bits. |
| **Control Subnet** | Enter a private IP address block for the control subnet for the primary region.<br>This address must be within the IP address block that you entered for the VPC.<br>The minimum size of the IP address block is 16 bits. |
| **Cluster Subnet** | Enter a private IP address block for the cluster subnet for the primary region.<br>This address must be within the IP address block that you entered for the VPC.<br>The minimum size of the IP address block is 16 bits. |
| **Secondary Subnet** | |
| **VPC Subnet** | Enter a private IP address block for the VPC for the secondary region, for example, 192.168.1.0/24.<br>This IP address block must be reachable from your private network. |
| **Primary Location** | Shows the secondary region for the fabric. |

| Option | Description |
|---|---|
| **Management Subnet** | Enter a private IP address block for the management subnet for the secondary region.<br>This address must be within the IP address block that you entered for the VPC.<br>The minimum size of the IP address block is 16. |
| **Control Subnet** | Enter a private IP address block for the control subnet for the secondary region.<br>This address must be within the IP address block that you entered for the VPC.<br>The minimum size of the IP address block is 16. |
| **Cluster Subnet** | Enter a private IP address block for the cluster subnet for the secondary region.<br>This address must be within the IP address block that you entered for the VPC.<br>The minimum size of the IP address block is 16. |

### Custom Domain Settings

The **Custom Domain Settings** area includes options for configuring custom domains for accessing Cisco SD-WAN Validator and Cisco SD-WAN Manager.

**Note** For government deployments, the default domain is sdwangov.fedramp.cisco and cannot be changed.

By default, the domain name for commercial deployments is cisco.com. You can specify another domain, if needed.

If you specify a custom domain, you must create your own domain name systems for the Cisco SD-WAN Validator and Cisco SD-WAN Manager because we do not have access to your domains.

After you configure a custom domain, make these mappings to allow control component certificates to come up:

- Map the Cisco SD-WAN Validator DNS to all VPN 0 IP addresses.
- Map the Cisco SD-WAN Manager DNS to all VPN 512 IP addresses.

| Option | Description |
|---|---|
| **SD-WAN Validator** | Enter the name of the DNS for the Cisco SD-WAN Validator. |
| **SD-WAN Manager** | Enter the name of the DNS for the Cisco SD-WAN Manager. |

### Snapshot Settings

The **Snapshot Settings** area includes an option for configuring how often the system takes a snapshot of Cisco SD-WAN Manager instances in your deployment.

By default, the network overlay configuration is backed up once a day and seven snapshots are stored.

For more detailed information about snapshots, see Information About Snapshots.

| Option | Description |
|---|---|
| **Frequency** | Choose how often the system takes a snapshot of Cisco SD-WAN Manager instances:<br>• **Once a day**<br>• **Once in 2 days**<br>• **Once in 3 days**<br>• **Once in 4 days** |

### Custom Organization Name

The **Custom Organization Name** area includes an option for configuring a unique organization name to identify your network.

| Option | Description |
|---|---|
| **Custom Organization Name** | Enter a unique name for your organization.<br>You can enter a name of up to 56 characters.<br>To ensure that each organization's name is unique, the Cisco Catalyst SD-WAN Portal automatically appends a hyphen and your virtual account ID at the end of the name you enter. |

### Certification Compliance Modes

The **Compliance Configuration** area includes certification compliance options for the fabric in commercial deployments only. These compliance modes are available:

***Table 2: Supported Certifications***

| Option | Description |
|---|---|
| **PCI-DSS** | Payment Card Industry Data Security Standard, Service Provider, Level 1 |
| **SOC2** | System and Organization Controls |
| **ISO27001, ISO27017, ISO27018, ISO27701** | International Organization for Standardization |
| **C5** | Cloud Computing Compliance Controls Catalog (Germany) |
| **ENS** | Esquema Nacional de Seguridad (Spain) |

| Option | Description |
|---|---|
| **Tx-RAMP** | Texas Risk and Authorization Management Program Level 2 |

For more detailed information about certification compliance, see Cisco Catalyst SD-WAN compliance and certification.

### Custom Key Management

Customer Managed Keys (CMKs) are supported for AWS-hosted, Cisco-provisioned fabrics.

CMKs are encryption keys created, owned, and managed by you within the KMS (Key Management Service) of your own AWS account, as an alternative to using Cisco-managed keys. An AWS KMS key is a logical, secure cryptographic key used to encrypt, decrypt, and protect data across AWS services.

Enter your CMKs for an AWS-hosted fabric in this section during fabric creation. You need distinct CMKs for your primary and secondary locations. For each CMK, include the full ARN (Amazon Resource Name) assigned by AWS at CMK creation.

The ARN is the fully-qualified identifier for the key, constructed from the Key ID and other metadata in the format `arn:aws:kms:region:account-id:key/key-id`. A complete CMK ARN would look like this example:

```
arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

| Option | Description |
|---|---|
| **CMK ID** | CMK ARNs for your primary and secondary locations. |

You can manage your CMKs on the **Customer managed keys** page of the AWS Management Console. Contact Cisco Support for the credentials needed to access the Cisco AWS account.

The system will monitor your CMK values, and you will receive an email alert if any irregularity is detected, such as accidental modification or deletion.

For more information on AWS KMS keys, refer to AWS KMS keys on the Amazon AWS website.

**Note** Existing fabrics can be migrated to use CMK keys. This requires a migration change window. Open a service request with the Cisco Support SD-WAN CloudInfra team.

### Dual Stack

The **Dual Stack** area includes an option for enabling IPv6 for control components on AWS hosted fabrics. IPv6 provisioning is only supported for Single Tenant fabrics hosted on AWS.

Enabling this option is required if your enterprise network is configured with IPv6. After this option is enabled, the fabric subnets are configured with both IPv4 and IPv6. IPv6 addresses are assigned by your cloud service provider.

**Note** After this option is enabled for a fabric, it cannot be disabled.

| Option | Description |
|---|---|
| **IPv6 Dual Stack** | Select the checkbox to enable IPv6 dual stack for control components. |

# Hybrid fabrics and on-premises SD-WAN Controllers

If you need to supplement your cloud-hosted control components with additional on-premises self-hosted control components, you can configure a hybrid fabric, which allows you to manage on-premises SD-WAN Controllers.

You can manually add and delete on-premises SD-WAN Controllers in a Cloud-Pro fabric using SD-WAN Portal.

### Manage on-premises SD-WAN Controllers

To add an on-premises SD-WAN Controller to your fabric, select **Add On-Prem Controller** from the **Actions** menu in the **Overlay Details** window and provide a public IP address and a UUID for the SD-WAN Controller.

The new SD-WAN Controller appears in the control components list as "Customer-Hosted," with no state information. It is automatically added to the allowed list.

You can onboard the new SD-WAN Controller in SD-WAN Manager. If you do not onboard it within 24 hours, you receive an email alert.

You are responsible for managing the on-premises SD-WAN Controller's infrastructure, including its sizing specifications. You have certain limited monitoring capabilities for on-premises SD-WAN Controllers.

The Cloud Infra team handles certificate renewal (if you are using Cisco PKI certificates) and software upgrades for all controllers, as defined in the "Cisco CloudOps responsibilities in cloud management" section of the *Cisco Catalyst SD-WAN CloudOps Guide*.

You can delete an on-premises SD-WAN Controller manually, without needing to make a deletion request.

# Delete a fabric

You cannot delete a fabric. If you need assistance, contact Cisco Catalyst SD-WAN Technical Support.

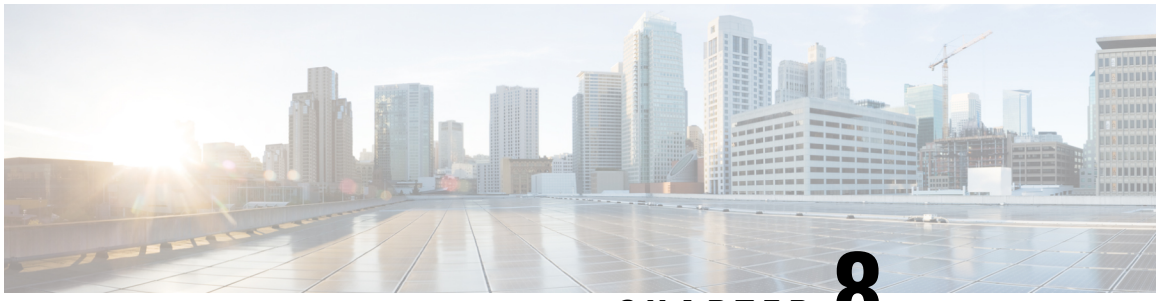
# Specify the allowed list of IP addresses for managing control component access

For Cisco SD-WAN Cloud-Pro fabrics, you can specify trusted IP addresses, including prefixes, from which you can manage access to control components. To enable management access, specify a rule type, protocol, port range, and the source IP (IP addresses and prefixes) for which you require access.

**Note** You do not need to add the IP addresses of WAN edge devices for them to join the fabric. Devices with any IP address can join the fabric, using Datagram Transport Layer Security (DTLS) or Transport Layer Security (TLS) tunnels, as long as Cisco SD-WAN Manager allows the device serial numbers.

- You can add up to 200 rules per fabric.
- Each rule is uniformly applied to all Cisco SD-WAN Cloud-Pro control components within the fabric.
- The same rules are automatically applied when new Cisco SD-WAN Cloud-Pro instances are added, or when existing instances are replaced. Each rule can specify either a single IP address or a larger IP prefix.

1. From the Cisco Catalyst SD-WAN Portal dashboard, navigate to your fabric.
2. In the **List View** tab, click the name of your fabric.
3. Click **Inbound Rules**.
4. Click **Add Inbound Rule**.
5. Specify the following parameters for your IP address or prefix:
   - **Rule type**: Choose a rule type: **All**, **SSH**, **HTTPS**, **Custom TCP rule**, or **Custom UDP rule**.
   - **Port range**: For custom TCP and UDP rules, specify a port range.
   - **Source**: Specify one or more IP addresses or IP address prefixes. For multiple entries, press tab to enter the next IP address or prefix.
   - **Descriptions**: Enter a description of the inbound rule.
6. Click **Add Rule**.
7. Click **Add New Inbound Rule** and add other IP addresses or IP address prefixes that you want to allow. (Optional)



CHAPTER 8

# Use Cisco Catalyst 8000V as a Cloud Gateway for a fabric


- Information about Cisco Catalyst 8000V as a cloud gateway for a fabric, on page 35
- Use cases for Cisco Catalyst 8000V as a cloud gateway for a fabric, on page 36
- Prerequisites for Cisco Catalyst 8000V as a cloud gateway for a fabric, on page 36
- Restrictions for Cisco Catalyst 8000V as a cloud gateway for a fabric, on page 36
- Configure Cisco Catalyst 8000V as a cloud gateway for a fabric, on page 37


## Information about Cisco Catalyst 8000V as a cloud gateway for a fabric

***Table 3: Feature History***

| Feature Name | Release Information | Description |
|---|---|---|
| Cisco Catalyst 8000V as a cloud gateway for a fabric | SD-WAN Portal: 2023-05<br>Cisco Catalyst SD-WAN Control Components Release 20.6.1 | This feature lets you configure a Cisco Catalyst 8000V device as the cloud gateway for connecting a virtual private cloud with a private data center. |

The Cisco Catalyst 8000V serves as the cloud gateway for connecting a virtual private cloud (VPC) with a private data center.

You can configure a Cisco Catalyst 8000V device as a cloud gateway in these ways, depending on your requirements:

- Create a new fabric and add a Cisco Catalyst 8000V device as the cloud gateway for each region in the fabric.
- Add a Cisco Catalyst 8000V device to each region in an existing fabric.
- Replace Cisco vEdge Cloud in an existing fabric with a Cisco Catalyst 8000V device.

# Use cases for Cisco Catalyst 8000V as a cloud gateway for a fabric

You can use Cisco Catalyst 8000V as a cloud gateway in these scenarios:

- Integrating your fabric with a TACACS or RADIUS server for AAA (authentication, authorization, and accounting) when the server resides in a private data center that you access through a VPN.
- Sending syslog information to a private data center that you access through a VPN.

# Prerequisites for Cisco Catalyst 8000V as a cloud gateway for a fabric

Before deploying the 8000V as a gateway, confirm these requirements:

- You must have a Cisco SD-WAN Manager administrator username and password.
- You must have a Smart Account administrator username and password.
- You must know the serial number of the 8000V that you are adding to a fabric.



**Note** As of Cisco Catalyst SD-WAN Control Components Release 20.15.5, no license is required for up to two Cisco 8000V devices if:

- they are operating as cloud gateway routers for a Cisco SD-WAN Cloud-Pro environment, and
- they provide a gateway for a TACACS or syslog server located outside the Catalyst SD-WAN fabric.

The license exemption requires tagging the devices with the Connector tag. After tagging the devices, the license compliance check will not flag them as requiring a license, and SD-WAN Manager will not show an out-of-compliance message for the devices.

For more information on tagging devices, refer to Device Tagging in the *Cisco Catalyst SD-WAN Control Components and Device Management Guide*.

# Restrictions for Cisco Catalyst 8000V as a cloud gateway for a fabric

You can use the 8000V as a cloud gateway only in Cisco SD-WAN Cloud-Pro environments.

# Configure Cisco Catalyst 8000V as a cloud gateway for a fabric

### Before you begin

Obtain the serial number of each 8000V device that you are configuring. Go to Cisco Software Central. In the **Smart Licensing** area, click **Manage Devices** under **Network Plug and Play**.

### Configuration procedures

Use this table to find the steps for configuring an 8000V device as a cloud gateway in various scenarios. Choose the scenario that corresponds to your requirements. For each scenario, the table provides the general steps and links to more detailed information.

| Scenario | General Steps | Reference |
|---|---|---|
| Create a new fabric and add an 8000V device as the cloud gateway for every region in the fabric. | **Step 1:** In the Cisco Catalyst SD-WAN Portal, create a new fabric. | See Create a Cisco Catalyst SD-WAN Cloud Hosted Fabric. |
| | **Step 2:** In the Cisco Catalyst SD-WAN Portal, configure a cloud gateway. | See Configure a cloud gateway in the Cisco Catalyst SD-WAN Portal, on page 37. |
| Add an 8000V device to every region in an existing fabric. | In the Cisco Catalyst SD-WAN Portal, configure a cloud gateway. | See Configure a cloud gateway in the Cisco Catalyst SD-WAN Portal, on page 37. |
| Replace Cisco vEdge Cloud with an 8000V device in an existing fabric. | **Step 1:** In the Cisco Catalyst SD-WAN Portal, configure a cloud gateway. | See Configure a cloud gateway in the Cisco Catalyst SD-WAN Portal, on page 37. |
| | **Step 2:**You can open a support case to request that the existing vEdge Cloud be removed. | See Open a support case for a fabric update, on page 39. |

### Configure a cloud gateway in the Cisco Catalyst SD-WAN Portal

1. Log in to the Cisco Catalyst SD-WAN Portal with administrator credentials.
2. Click the fabric for which you want to configure a cloud gateway.
3. From the **Actions** drop-down menu, choose **Add Cloud Gateways**.
4. Configure the fields listed in this table.

**Note** The Cisco Catalyst SD-WAN Portal does not save the usernames and passwords that you enter in these fields.

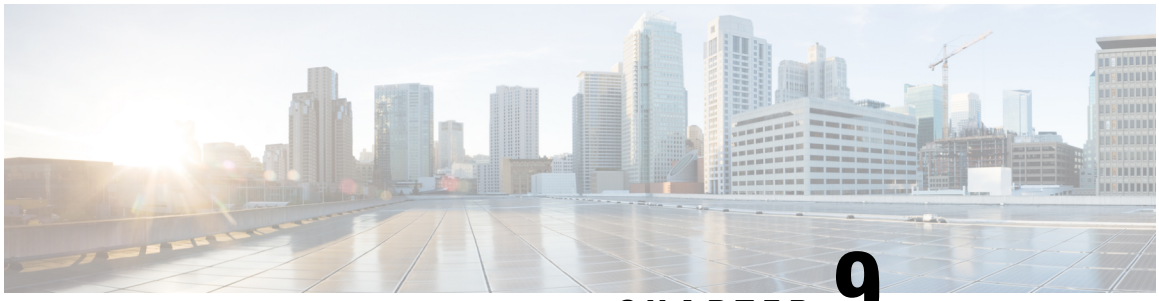
| Field | Description |
|---|---|
| **vManage Admin Credentials** | |

| Field | Description |
|---|---|
| **Username** | Enter your Cisco SD-WAN Manager administrator username. |
| **Password** | Enter your Cisco SD-WAN Manager administrator password. |
| **Smart Account Admin Credentials** | |
| **Username** | Enter your Cisco Smart Account administrator username. |
| **Password** | Enter your Cisco Smart Account administrator password. |
| **Cloud Gateway Serials** | |
| **Serial** | The number of fields that appear equals the number of regions in your fabric.<br>Enter the serial number of the Cisco 8000V in each **Serial** field to designate it as a cloud gateway for each region.<br>Ensure that each serial number you enter is unique. |
| **Custom IPs** | |
| **System IPs** | The number of **System IPs** fields equals the number of regions in your fabric.<br>Optionally, enter an IP address in each field to configure a system interface for the cloud gateway that you are adding.<br>A system interface IP address is persistent and identifies the device. It works like a router ID, which identifies the router from which packets originate.<br>Specify a system IP address using decimal four-part dotted notation as an IPv4 address. Enter only the address because the prefix length (/32) is implicit.<br>Select any IPv4 address except for 0.0.0.0/8, 127.0.0.0/8, and 224.0.0.0/4, or 240.0.0.0/4 and later.<br>If you do not specify a system IP address, the Cisco Catalyst SD-WAN Portal assigns a random IP address. This address might duplicate the IP address of another device.<br>Ensure that the IP address you enter is unused in the existing fabric. This prevents conflicts when provisioning the cloud gateway. |

5. Click **Submit**.

### Open a support case for a fabric update

To open a support case for a fabric update, go to Cisco Support Case Manager, log in with your Cisco credentials, and click **Open New Case**.



CHAPTER 9

# Monitor Fabrics


- Monitor control components and devices in fabrics, on page 41
- View fabric and control component details, on page 41
- View change window notifications, on page 42


## Monitor control components and devices in fabrics

1. From the Cisco Catalyst SD-WAN Portal dashboard, click the **List View** tab.

   The list of fabrics appears.

2. Select your fabric.
3. In the **Controller View** area, click the control component that you want to monitor—**SD-WAN Manager**, **SD-WAN Validator**, **SD-WAN Controller**, **Cloud Gateways**, or **vEdge**.
4. In the **Control Components** window, you can filter by network usage, CPU usage, or duration. Filter by state, type, version, or region to further narrow the list.

**Note** To align with Cisco Catalyst SD-WAN rebranding, the **Controllers** tab is renamed as the **Control Components** tab from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a.

## View fabric and control component details

1. From the Cisco Catalyst SD-WAN Portal dashboard, click the **List View** tab.

   The list of fabrics appears.

2. Click the name of the fabric.

   The **Dashboard** > **Overlays** > **Details** page displays detailed information for your fabric.

# View change window notifications

*Table 4: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Change Window Notifications | 2021-02 Release | Change window notifications let you view when your Cisco Catalyst SD-WAN fabric maintenance events start or end. You can also access details about the scheduled change notification and the planned maintenance operation.<br>Cisco Catalyst SD-WAN Portal customers can only view change window notifications. A CloudOps user needs to schedule or start a change window notification. |

Change window notifications let you view the start and end times of your Cisco Catalyst SD-WAN fabric maintenance events. You can also access details about the scheduled change notification and the planned maintenance operation.

Banner alerts are displayed for notifications scheduled to start or that begin within 10 days. If a notification is completed or scheduled to start in more than 10 days, banner alerts are not displayed on the Cisco Catalyst SD-WAN Portal dashboard.

If a change notification has started, it shows as ongoing in the banner alert.

If a change notification is scheduled, it shows as started in the banner alert.

### Before you begin

Cisco Catalyst SD-WAN Portal customers can only view change window notifications.

Only a CloudOps user can schedule or start a change window notification.

### View change window notifications for all fabrics

1. From the Cisco Catalyst SD-WAN Portal dashboard, under **Change Window Notifications**, click a fabric that is scheduled or started.

   The **Dashboard** > **Change Window Notifications** page is displayed with the list of fabrics.

   A banner alert is displayed for every change window notification.

   View all change window notifications for your fabrics on this page.

2. Optionally, filter by status to change the number of fabrics displayed.

3. Click **Change Window Notifications** to display all change window notifications and view their descriptions in the details column.

   The **Dashboard** > **Overlays** > **Details** > **Change Window Notifications** page displays.

### View change window notifications for specific fabrics

1. To view a change notification for a specific fabric, from the Cisco Catalyst SD-WAN Portal dashboard, click a fabric that has a scheduled or started change notification.

   The **Dashboard** > **Overlays** > **Details** page is displayed.

2. Click an overlay that has a scheduled or started change window notification.

   For change window notifications specific to a fabric, the banner alert is displayed without the fabric name because you are already viewing it.

   On this page, view change window notifications for the selected fabric.

### View the list of change window notifications

1. From the Cisco Catalyst SD-WAN Portal dashboard, click the fabric for which you have a scheduled or started change window notification.

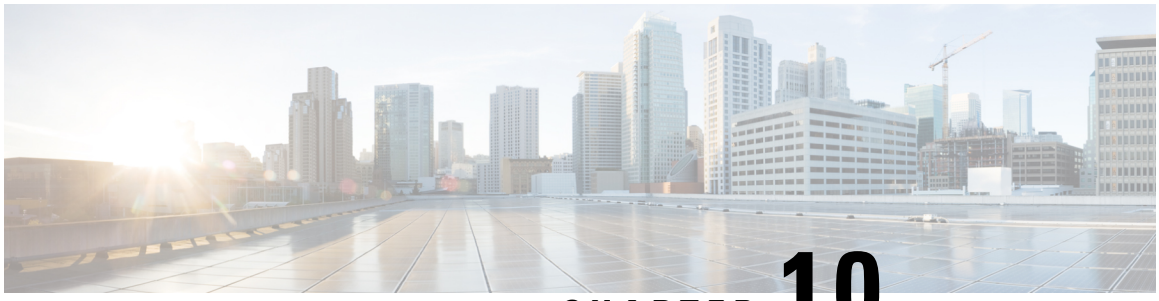
   The **Dashboard** > **Overlays** page displays.

2. Click the fabric name.

   The **Dashboard** > **Overlays** > **Details** page displays.

3. In **Change Window Notifications**, choose the scheduled or started change window notification.

   The **Dashboard** > **Overlays** > **Details** > **Change Window Notifications**page displays where you can view detailed information about your change notification event.



CHAPTER 10

# Manage Predefined Inbound Routes

The table lists the feature history for managing predefined inbound routes.

***Table 5: Feature History***

| Feature Name | Release Information | Description |
|---|---|---|
| Predefined Inbound Rules | March 2023 Release | With this feature you can specify trusted IP addresses. These IP addresses are applied to any new overlay that you create under the Smart Account for which you configure this feature. These IP addresses can also be applied to existing overlays under the Smart Account for which you configure this feature. |


- Information about predefined inbound rules, on page 45
- Configure predefined inbound rules, on page 46


# Information about predefined inbound rules

Predefined inbound rules allow you to manage control component access by automatically applying trusted IP addresses and prefixes to all existing and new overlays within a Smart Account. This feature eliminates the need for manual configuration per overlay and includes support for audit log entries for all allowed IP addresses.

An inbound rule includes the rule name, protocol and port range to which the rule applies, and source IP address or prefix information. You can create up to 200 inbound rules per fabric and up to 5 allowed list entries.

**Note** If you have dynamic IP requirements for an existing multitenant Cloud-Pro fabric hosted on AWS, you can request activation of Application Load Balancing (ALB) and Web Application Firewall (WAF) for the fabric. This option replaces the static IP allow list with WAF-based access control, removing the 200-rule limit and enabling scalable, flexible, and secure ingress management.

To enable ALB and WAF, you must file a CSOne ticket and include a mandatory justification.

Normal inbound rule management will not be available when ALB/WAF has been enabled on a fabric. This feature is irreversible once enabled.

# Configure predefined inbound rules

### Before you begin

1. Create a Smart Account.

   For more information on creating a Smart Account, see Workflow for Smart Account and Virtual Accounts for Provisioning the Controllers.

2. Create a fabric.

   For more information on creating a Cisco SD-WAN Cloud-Pro fabric, see Create a Cisco SD-WAN Cloud-Pro Overlay Network.

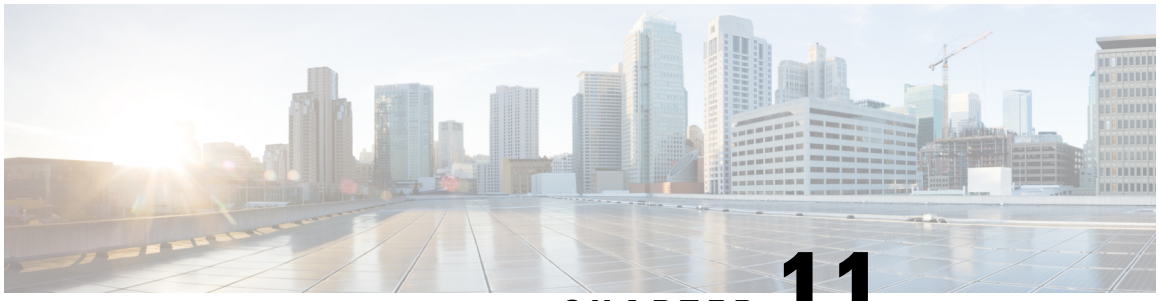
### Manage predefined inbound rules

1. From the Cisco Catalyst SD-WAN Portal menu, choose **Admin Settings**.
2. Under **Actions**, click **. . .** adjacent to the appropriate Smart Account and choose **Manage Predefined Inbound Rules** from the drop-down list.
3. Click **Add Predefined Inbound Rules** to add a predefined inbound rule.
4. Configure the following fields:

| Field | Description |
|---|---|
| **Name** | Enter a name for the predefined inbound rule. |
| **Rule Type** | Select the protocol to which the rule applies from the drop-down list.<br>• **All** (rule applies to all protocols)<br>• **SSH**<br>• **HTTPS**<br>• **Custom TCP rule**<br>• **Custom UDP rule** |

| Field | Description |
|---|---|
| **Protocol** | **Protocol** is automatically populated depending on which **Rule Type** you choose. |
| **Port Range** | If you chose **Custom TCP rule** or **Custom UDP rule** for **Rule Type**, enter the port range to which the rule applies. |
| **Source** | Enter an IP address or an IP address prefix. |
| **Description** | Enter a description for the predefined inbound rule. |
| **Automatically add this rule to ALL fabrics** | Select this option to apply the predefined rules to all the existing fabrics associated with your Smart Account, as well as any new fabrics.<br>If you do not select this option, the rule is not added to your existing fabrics. |

5. Click **Add**.



CHAPTER 11

# Configure Certification Compliance


- Cisco Catalyst SD-WAN compliance and certification, on page 49
- Benefits of a certified environment, on page 50
- Enable compliance with industry certifications for a new fabric, on page 50
- Enable compliance with industry certifications for an existing fabric, on page 51
- View certification compliance, on page 51


## Cisco Catalyst SD-WAN compliance and certification

Commercial certification and compliance help your business meet customer requirements in many industries. You may need commercial certification for cloud services due to issues such as:

- regulatory compliance,
- data security and privacy,
- reduced risk based on audits and assessments,
- trust and credibility,
- disaster recovery and business continuity,
- improved service quality,
- competitive advantage,
- interoperability, and
- easier audits,

Your organization can obtain these internationally recognized certifications with Cisco Catalyst SD-WAN for regulated industries:

- Payment Card Industry Data Security Standard (PCI DSS)
- System and Organization Controls (SOC) 2 Type 2 and SOC 3
- International Organization for Standardization (ISO) 27001, ISO 27701, ISO 27017, and ISO 27018
- Cloud Computing Compliance Criteria Catalogue (C5)
- Esquema Nacional de Seguridad (ENS)

- Texas Risk and Authorization Management Program (Tx-RAMP)

Contact your channel partner for a report on Cisco Catalyst SD-WAN certifications.

# Benefits of a certified environment

Configure a certified environment to gain these benefits.

- Maintain a secure network with centralized configuration management using secure configuration baseline standards from Center for Internet Security (CIS) or Security Technical Implementation Guide (STIG).
- Protect data in transit and at rest across networks using encryption.
- Use centralized user account management to identify, access, and authenticate with unique credentials and strict role-based access control.
- Ensure Cisco Catalyst SD-WAN Control Components are subject to ongoing penetration testing and vulnerability scans.

# Enable compliance with industry certifications for a new fabric

You can benefit from a certified environment by purchasing a DNA subscription, using a certified release version, and selecting the certifications options in Cisco Catalyst SD-WAN Portal before creating a fabric.

**Note** All commercial certifications are managed through the shared Cisco SD-WAN Cloud.

**Procedure**

**Step 1** Open https://ssp.sdwan.cisco.com to access the Cisco Catalyst SD-WAN Portal.
**Step 2** Sign in to the Cisco Catalyst SD-WAN Portal using your credentials.
**Step 3** From the **Create Cisco SD-WAN Cloud-Pro Fabric** page, enter your Smart Account and Virtual Account.
**Step 4** In the **Fabric Name** field, enter a fabric name.
**Step 5** Select **Assign Control Components**.
**Step 6** In **Advanced Options**, select the **Compliance Configuration** option and then choose the required industry certifications.
**Step 7** Click **Create Fabric**.

# Enable compliance with industry certifications for an existing fabric

### Before you begin

You can enable compliance with industry certifications only if your Cisco SD-WAN Cloud-Pro fabric is encrypted. If your fabric is not encrypted, encryption is required to enable compliance.

### Procedure

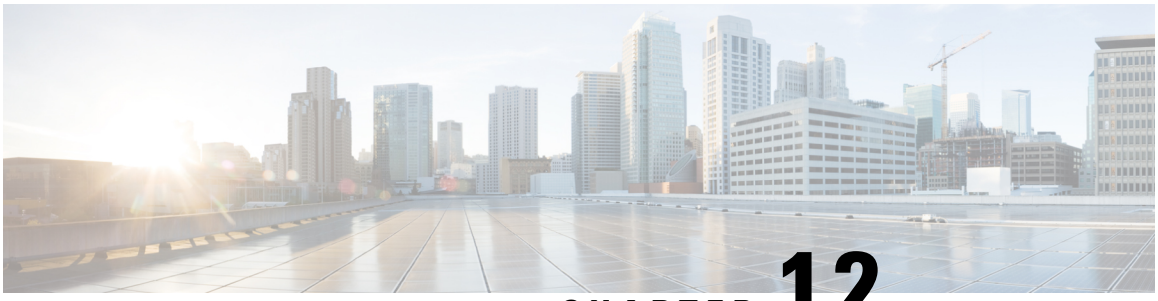
**Step 1** Sign in to the Cisco Catalyst SD-WAN Portal.
**Step 2** Click **Fabric** to find your fabric.
**Step 3** In the **Actions** drop-down list choose **Compliance Mode**.
**Step 4** In the **Compliance** panel, select the required industry certifications.
**Step 5** Click **Apply**.

# View certification compliance

### Procedure

**Step 1** Open https://ssp.sdwan.cisco.com to access the Cisco Catalyst SD-WAN Portal.
**Step 2** Log in to the Cisco Catalyst SD-WAN Portal using your credentials.
**Step 3** Select the desired fabric and click **View Details**.

You can view the active compliances for the fabric in the **Description** pane.



CHAPTER 12

# Configure System Snapshots


- Information about system snapshots, on page 53
- Take an on-demand snapshot, on page 54
- View snapshots, on page 55


# Information about system snapshots

A Cisco SD-WAN Manager snapshot is a saved state of a Cisco SD-WAN Manager instance. Snapshots provide recovery points that the CloudOps team can use to restore your system. The SD-WAN Portal automatically saves the snapshots.

By contrast, you do not need to create snapshots for SD-WAN Controllers or SD-WAN Validators because they are stateless.

### Which Cisco Catalyst SD-WAN installations store snapshots?

In Cisco SD-WAN Cloud and Cisco SD-WAN Cloud-Pro environments, the SD-WAN Portal manages saving snapshots of SD-WAN Manager, which are saved to cloud storage managed by Cisco. The system stores snapshots in the primary region that you select when you set up the SD-WAN fabric.

### Viewing snapshot details

You can view details of the saved snapshots in the SD-WAN Portal. You cannot download the snapshots themselves.

### Snapshot types

This table describes the available snapshot types.

*Table 6: Snapshot types*

| Snapshot type | Description | When they are taken | How many are retained | How long they are retained |
|---|---|---|---|---|
| On-demand | You can take an on-demand snapshot at any time, such as before a major change to your Cisco SD-WAN Manager configuration. Before the change window, freeze configuration changes and allocate up to eight hours (480 minutes) to create and save the on-demand snapshot.<br>See Take an On-Demand Snapshot. | On-demand | 1 | 15 days. If you take another on-demand snapshot, retention ends sooner. |
| Regular | Regular snapshots are saved at a configurable interval of one to four days. The snapshot typically occurs at midnight in the region of SD-WAN Manager.<br>Set the interval during fabric creation:<br>**Advanced Options** > **Edit** > **Snapshot Settings**<br>See Create a Cisco SD-WAN Cloud-Pro Overlay Network.<br>For an existing fabric, you can edit the snapshot interval in the SD-WAN Portal:<br>**View details** > **Snapshots** > **Actions** > **Edit snapshot frequency** | Interval you define: one to four days. | 7 | The oldest of seven is discarded when a new snapshot is created.<br>The retention duration is:<br>(7 * *user-configured-interval*), which is seven to 28 days. |
| Golden | You can mark a single regular or on-demand snapshot as Golden to save it for a longer period. Use this when SD-WAN Manager is in an ideal state for a long-term recovery point.<br>Marking a new snapshot as Golden removes the Golden designation from the previous Golden snapshot. The previous Golden snapshot is then subject to removal according to its expiration schedule. | This is an existing regular or on-demand snapshot manually marked as Golden. | 1 | 90 days |

# Take an on-demand snapshot

You can take an on-demand snapshot of Cisco SD-WAN Manager configuration when needed. We recommend that you take a snapshot before any major change window.

When you take an on-demand snapshot, freeze configuration changes. Allocate up to 8 hours before the change window to ensure the snapshot is completed.

An on-demand snapshot is stored for 15 days after its creation, then it is deleted automatically. Only one on-demand snapshot is retained at any given time, as a new on-demand snapshot replaces the existing stored snapshot.

**Note** On-demand snapshots are not available for shared tenants.

1. From the Cisco Catalyst SD-WAN Portal, navigate to the list of available overlays.

   The **Dashboard** > **Overlays** page appears.
2. Click the name of the fabric for which you want to take a snapshot.
3. From the **Dashboard** > **Cisco Hosted Overlays** > **Details** page, click the **Snapshot** tile.
4. From the **Actions** drop-down menu, choose **On-Demand Snapshot**.
5. In the **On-Demand Snapshot** area, turn on the switch for the Cisco SD-WAN Manager instance for which you want to take the snapshot.

   For a Cisco SD-WAN Manager cluster, turn on the switches for each Cisco SD-WAN Manager instance in the cluster.
6. Click **Submit**.

   Snapshot creation starts. Completing the snapshot can take up to 8 hours to complete, depending on the amount of data in Cisco SD-WAN Manager.

# View snapshots

### Before you begin

To view snapshot details, ensure that your overlay is associated with a Cisco SD-WAN Cloud-Pro controller.

For more information, see Create a Cisco SD-WAN Cloud-Pro Overlay Network.

For more information on snapshots, see Information About Snapshots.

### View snapshots

1. From the Cisco Catalyst SD-WAN Portal dashboard, navigate to the list of available overlays.

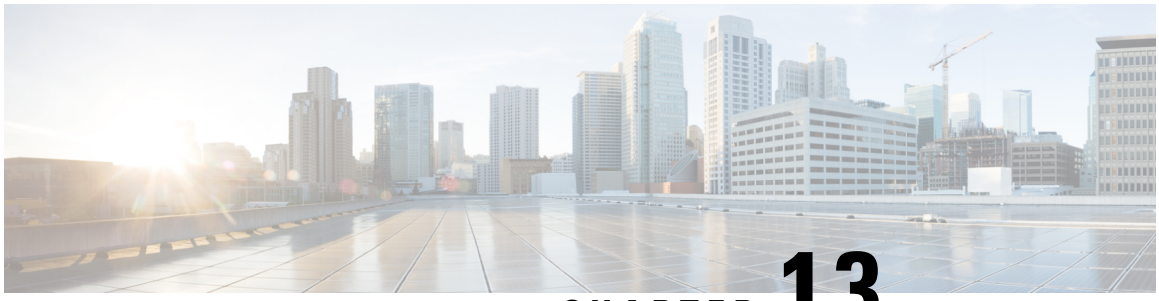
   The **Dashboard** > **Overlays** page displays.
2. Click the name of an overlay for which you want to view a snapshot.
3. From the **Dashboard** > **Cisco Hosted Overlays** > **Details** page, click on the tile for **Snapshot**.

   The **Dashboard** > **Cisco Hosted Overlays** > **Details** > **Snapshots** page displays.

*Table 7: Snapshot Fields*

| Field | Description |
|---|---|
| **Snapshot ID (*denotes golden snapshot)** | Specifies the snapshot ID.<br>If a snapshot is a golden snapshot, it is denoted by an asterisk. |
| **Name** | Specifies the name of the snapshot. |
| **Version** | Specifies the version number of the Cisco SD-WAN Manager software. |
| **Progress** | Specifies the progress of the snapshot creation process. |
| **Duration** | Specifies the duration of the snapshot creation process. |
| **State** | Specifies the state of the snapshot creation process. |
| **Device** | Specifies the disk on Cisco SD-WAN Manager for which the snapshot was taken. There are either two or three disks on the Cisco SD-WAN Manager instance, depending on which version the device was originally provisioned on.<br>Snapshots of all disks, taken at the same time, enable recovery and reconstruction of theCisco SD-WAN Manager instance during disaster recovery. |
| **Golden** | Specifies if the snapshot is a golden snapshot.<br>Available values are as follows:<br>• **false**<br>• **true** |
| **Region** | Specifies the region where this snapshot is stored. |
| **Type** | Specifies the type of snapshot.<br>Available values include:<br>• **REGULAR**,<br>• **ON-DEMAND**, and<br>• **GOLDEN**. |
| **Overlay ID** | Specifies the overlay ID. |
| **Overlay** | Specifies the overlay name and an ID. |

| Field | Description |
|---|---|
| **Instance ID** | Specifies the Cisco SD-WAN Manager instance ID. |
| **Instance** | Specifies the Cisco SD-WAN Manager instance name and ID. |
| **Actions** | To mark a specific date snapshot as golden, click **Make Golden Snapshot**. |



CHAPTER 13

# Configure Webhooks


- Information about webhooks, on page 59
- Configure a webhook, on page 59
- Send a webhook notification, on page 60


## Information about webhooks

A webhook is a method that enables HTTP communication between two systems and is initiated by a specified event. The SD-WAN Portal uses webhooks to send event notifications about the fabric. You can configure and manage webhooks through a tab in the **Administration Settings** area of the SD-WAN Portal.

## Configure a webhook

**Procedure**

**Step 1** From the SD-WAN Portal menu, click **Administration** and select **Admin Settings**.

**Step 2** Select the **Webhooks** tab.

**Step 3** Click **Configure Webhook**.

**Step 4** Enter or select this information:

- Smart Account name
- Virtual Account name
- URL of webhook endpoint
- Authorization type (choose Basic [username/password] or None).

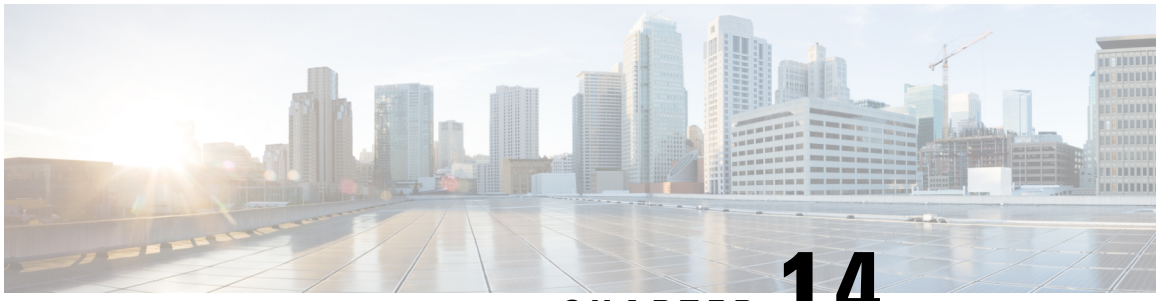
**Step 5** Click **Add**.
The system displays a table of defined webhooks.

# Send a webhook notification

### Procedure

**Step 1** Right-click the webhook you want to edit in the table of defined webhooks, then choose **Send**.

**Step 2** Enter the plaintext notification for the webhook. Click **Send** to send the notification to the webhook server.



CHAPTER 14

# Configuration Conversion Tool


- Configuration Conversion Tool feature history, on page 61
- Information about the Configuration Conversion Tool, on page 61
- Restrictions for the Configuration Conversion Tool, on page 62
- Prerequisites for the Configuration Conversion Tool, on page 62
- Use the Configuration Conversion Tool, on page 62


## Configuration Conversion Tool feature history

*Table 8: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Configuration Conversion Tool | SD-WAN Manager 20.12.1 | The Configuration Conversion Tool converts templates and policies to configuration groups, policy groups, and topology groups. |
| Export option for Configuration Conversion | SD-WAN Manager 20.18.2 | You can export the converted template files from the Configuration Conversion Tool. |

## Information about the Configuration Conversion Tool

Use the Catalyst SD-WAN Configuration Conversion Tool to collect templates and policies from your SD-WAN Manager instance, convert them, and create new configuration groups, policy groups, and topology groups in a new SD-WAN Manager instance.

### Conversion details

The Configuration Conversion Tool:

- converts device templates to configuration groups,
- converts policies into policy groups and topology groups where applicable, and
- transfers global device values and variable names.

# Restrictions for the Configuration Conversion Tool

- The Configuration Conversion Tool is considered to be in beta.
- The Configuration Conversion Tool does not convert features that do not have a configuration group or policy group equivalent.

# Prerequisites for the Configuration Conversion Tool

- Your site must be using Cisco Catalyst SD-WAN Manager Release 20.12.x or later.
- Your SD-WAN Manager hostname must be resolvable.
- Your network firewall must accept incoming traffic from 74.207.103.254 and `*-apigw.sdwan.cisco.com`.

# Use the Configuration Conversion Tool

You can use the configuration conversion tool from Cisco Catalyst SD-WAN Portal or from **Classic Templates** menu.

### Procedure

**Step 1** Sign in to the SD-WAN Portal using your CCO credentials. If you are a Smart Account administrator, you are logged into the SD-WAN Portal as normal. Choose **Configuration Conversion** from the menu in order to enter the workflow. If your are not a Smart Account administrator, you get a 403 Forbidden page with a link to the tool.

**Step 2** Launch the **Configuration Conversion Tool**.

**Step 3** You can select the flows from SD-WAN Manager or upload the templates that are exported from SD-WAN Manager.

| Choice | Description |
|---|---|
| Connect to SD-WAN Manager | Enter username, password, and the SD-WAN Manager port. The default port for HTTPS is 443. |
| Upload templates exported from SD-WAN Manager. | Follow the instructions to upload a file. |

**Step 4** Click **Collect** to retrieve all legacy constructs, including device templates, feature templates, policies, and associated constructs, from SD-WAN Manager.

When the collection is complete, download the JSON file containing all configurations. Use this file to repeat the process later without collecting the data again from SD-WAN Manager.

**Step 5** If you are using from SD-WAN Manager, click **Configuration** > **Templates**.

**Step 6** In the **Device Templates** pane, select the device template you want to convert to their new equivalents.

**Step 7** Click **Configure conversion**. The Configuration conversion wizard opens.

The tool converts the device templates and associated feature templates.

**Step 8** Click **Go to SD-WAN Portal** to open SD-WAN Portal.

If cloud services is enabled - it will stat interactive workflow on the portal automatically.

**Step 9** From SD-WAN Manager 20.18.2, you can export files. Click **Export file** to export the templates to your local. The templates are in the JSON format.

It produces a tarball for off-line conversion. You can start air-gap workflow using provided tarball in the portal.

**Step 10** Click **Convert** to convert the selected items.
The **Converted Configurations** page displays all the newly converted constructs. Review the items created and their statuses.

**Step 11** Confirm the list and click **Upload** to add the configurations to SD-WAN Manager.

You can cancel an upload in progress.

After the upload is complete, a summary of the configurations that were uploaded appears.

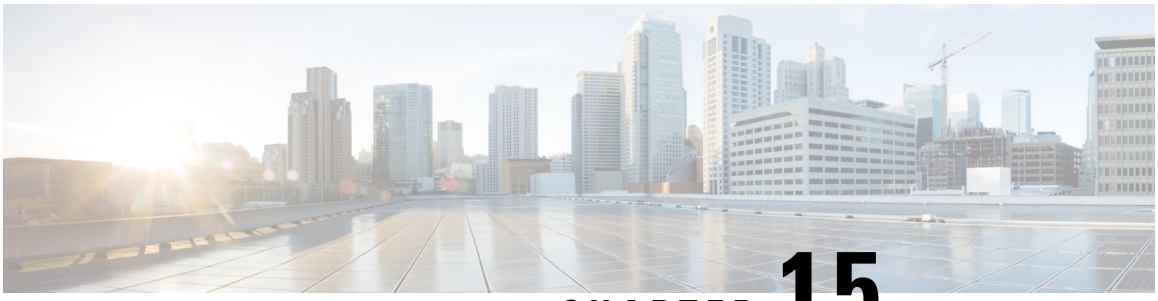
If needed, you can click **Rollback** to remove all the constructs added to SD-WAN Manager during this session.

---

The new constructs are now ready to use.

### What to do next

To migrate your devices to the newly converted configuration groups, complete the steps in the Existing Deployments section of the *Quick Start Guide - Catalyst SD-WAN Simplified Configuration and Policies*.



CHAPTER 15

# Frequently Asked Questions


- Frequently Asked Questions, on page 65
- How to, on page 66
- Troubleshooting, on page 66


## Frequently Asked Questions

**What types of Cisco Catalyst SD-WAN deployments are supported on the Cisco Catalyst SD-WAN Portal?**

You can deploy the following types of Cisco Catalyst SD-WAN on the Cisco Catalyst SD-WAN Portal:

- Cisco SD-WAN Cloud
- Cisco SD-WAN Cloud-Pro

See more details in Types of Fabric Network in Cisco Catalyst SD-WAN.

**What cloud providers are supported to provision SD-WAN control components in the Cisco Catalyst SD-WAN Portal?**

The supported cloud providers for provisioning SD-WAN Control Components in the Cisco Catalyst SD-WAN Portal are Amazon Web Services (AWS) and Microsoft Azure.

**What is the role of a Virtual Account in Cisco Catalyst SD-WAN Portal controller provisioning?**

The Cisco Catalyst SD-WAN Portal uses SD-WAN subscriptions linked to a Virtual Account to determine which cloud SD-WAN Control Component entitlements are available and to facilitate SD-WAN Control Component provisioning. This information shows whether your Virtual Account supports SD-WAN. Provide a Virtual Account when you order an SD-WAN license to ensure successful provisioning through the Catalyst SD-WAN Portal.

# How to

### How do I access the Cisco Catalyst SD-WAN Portal?

Use the instructions in Access the Cisco Catalyst SD-WAN Portal for the First Time to access the Cisco Catalyst SD-WAN Portal.

If you want to use an identity provider (IdP) to access the portal, refer to Configure an IdP for the Cisco Catalyst SD-WAN Portal.

### How do I configure role-based access in the Cisco Catalyst SD-WAN Portal?

The role-based access control feature in the Cisco Catalyst SD-WAN Portal allows users to be assigned specific roles (Monitor, Overlay Management, or Administration) within designated virtual accounts. This process ensures granular visibility and streamlines provisioning and monitoring of new overlays. To configure role-based access, refer to the instructions provided in Manage role-based access.

### How do I set up multifactor authentication (MFA)?

The Cisco Catalyst SD-WAN Portal supports MFA by default, and it is mandatory for users. These one-time password generation options are available:

- Google Authenticator
- Email Authenticator
- Fingerprint sensor on supported computers (such as Apple MacBook)

For more information, refer to Configure Additional MFA Options or Update an Existing MFA Option.

### How do I move SD-WAN Control Component SKUs from one Virtual Account to another Virtual Account?

To reassign an order containing SD-WAN Control Component SKUs to a different Virtual Account, open a support case as described in Troubleshooting, on page 66.

### How do I add IP addresses to an allow list for managing fabric access through the Cisco Catalyst SD-WAN Portal?

To add IP addresses to an allow list through the Cisco Catalyst SD-WAN Portal, refer to the instructions in Specify the Allowed List of IP Addresses for Managing Controller Access.

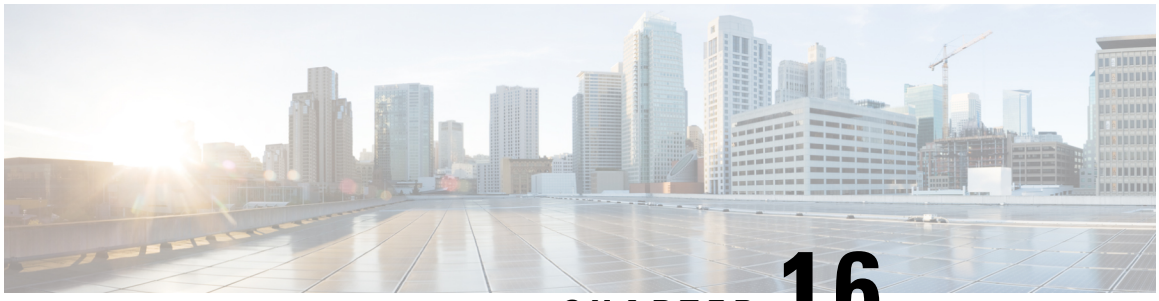
# Troubleshooting

### How do I get support for Cisco Catalyst SD-WAN Portal?

Follow these steps to open a Cisco support case for Catalyst SD-WAN Portal.

1. Go to https://mycase.cloudapps.cisco.com/case.
2. Select **Open New Case** > **Products & Services** > **Open Case**.

3. Enter the appropriate entitlement information. You typically need to include the serial number of a WAN edge device.
4. Click **Next**.
5. Enter your case details.
6. Select **Technology** and search for the appropriate Sub Tech keyword. For Cisco Catalyst SD-WAN Portal issues, select these keywords:
    - Technology: SDWAN - Cisco-Hosted
    - SubTechnology: SDWAN Cloud Infra



CHAPTER 16

# Troubleshoot the Cisco Catalyst SD-WAN Portal


- Update an expired IdP certificate, on page 69
- Reset a Misconfigured IdP, on page 69
- Troubleshoot Smart Account issues, on page 70
- Troubleshoot Virtual Account issues, on page 70
- Troubleshoot browser security issues, on page 71


## Update an expired IdP certificate

To update an expired identity provider (IdP) certificate, use the **Need help signing in** link in the Cisco Catalyst SD-WAN Portal **Sign In** window.

1. Navigate to the Cisco Catalyst SD-WAN Portal URL.
2. Click the **Need help signing in** link.
3. Click the **Need to reset IdP** link.

   You are redirected to your Cisco account.
4. Enter your Cisco login credentials.
5. When prompted, set up or enter your MFA credentials.

## Reset a Misconfigured IdP

If your identity provider (IdP) is misconfigured and you cannot log in, you can configure a new IdP.

1. Go to the Cisco Catalyst SD-WAN Portal URL.
2. Click **Need help signing in**.
3. Click **Need to reset IdP**.

   You are redirected to your account.
4. Enter your login credentials.
5. When prompted, set up or enter your multifactor authentication (MFA) credentials.

### Delete an IdP

1. Go to the Cisco Catalyst SD-WAN Portal URL.
2. Click **Need help signing in**.
3. Click the **Need to reset IdP**.
4. You are redirected to your account.
5. Enter your login credentials.
6. When prompted, set up or enter your MFA credentials.
7. Select **IdP details** > **Actions** and delete the IDP.

**Note** Only the IdP administrator is able to delete an IdP from Cisco Catalyst SD-WAN Portal. If you are not the IdP administrator or the administrator is no longer active, open a TAC case.

# Troubleshoot Smart Account issues

### Problem

A Smart Account is not visible in the **Smart Account** drop-down list after logging in to the Cisco Catalyst SD-WAN Portal. This can occur when there is no SD-WAN-capable attribute associated with the Smart Account.

### Solution

Associate your DNA subscription with your Smart Account and Virtual Account.

For more information, see Workflow for Smart Account and Virtual Accounts for Provisioning the Controllers.

Contact Technical Support to have your Smart Account associated with your DNA cloud subscription.

# Troubleshoot Virtual Account issues

### Problem

The Cisco Catalyst SD-WAN Portal displays an error that the Virtual Account is not SD-WAN capable.

This error indicates that a DNA subscription is not associated with the Virtual Account.

### Solution

If you have an enterprise agreement, you cannot automatically associate Virtual Accounts to an SD-WAN-capable attribute.

As an enterprise customer, complete these steps to associate a Virtual Account with your DNA subscription:

1. Submit a cloud-controller provisioning request form through the Enterprise Agreement Workspace for the CloudOps team to provision the controllers.
2. Contact Cisco Catalyst SD-WAN Technical Support to request that the desired Virtual Account become available on the Cisco Catalyst SD-WAN Portal.
3. After the desired Virtual Account is available on the Cisco Catalyst SD-WAN Portal, provide the necessary enterprise agreement contract information to provision the controllers.

For more information, see Smart Account and Virtual Accounts.

For more information, see Workflow for Smart Account and Virtual Accounts for Provisioning the Controllers.

If you are unable to associate your Virtual Account with your DNA subscription, contact Technical Support to associate the Virtual Account with your DNA cloud subscription.

# Troubleshoot browser security issues

### Problem

You see this error:

```
CSRF Failed: CSRF token missing or incorrect
```

You see a cross-site request forgery (CSRF) token mismatch when the browser is unable to create a secure cookie or to access the cookie required for you to log in.

### Solution

This error appears because of certain security settings in your web browser.

Clear the cache on your browser, or try another browser.