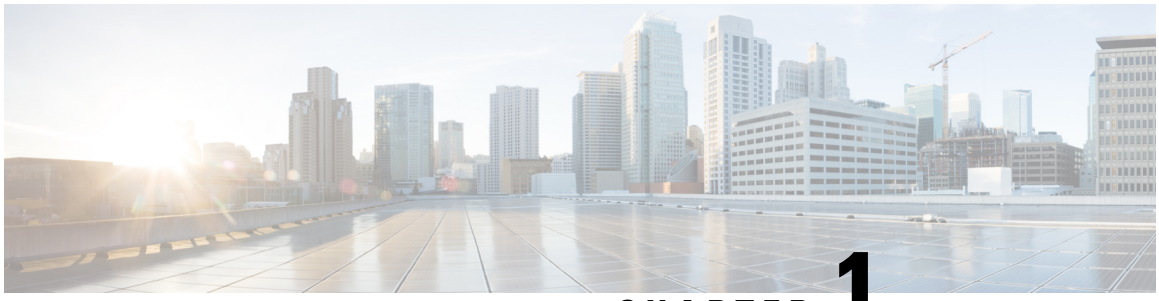
Cisco Catalyst SD-WAN Portal Configuration Guide

First Published: 2022-12-01

Last Modified: 2023-12-19

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

CONTENTS



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

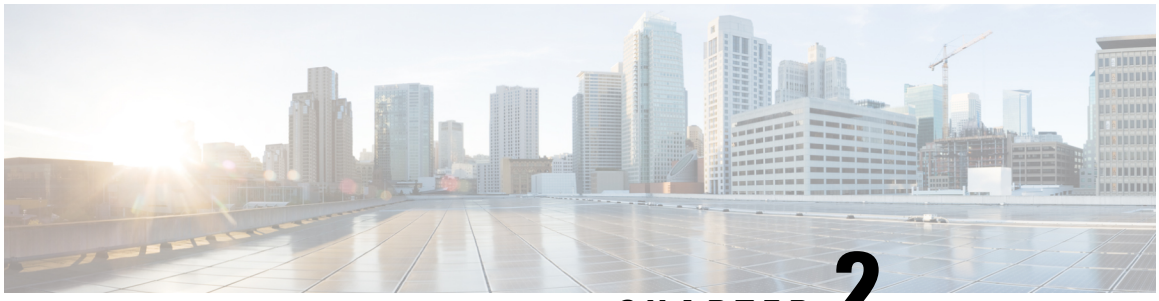
- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17

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

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.

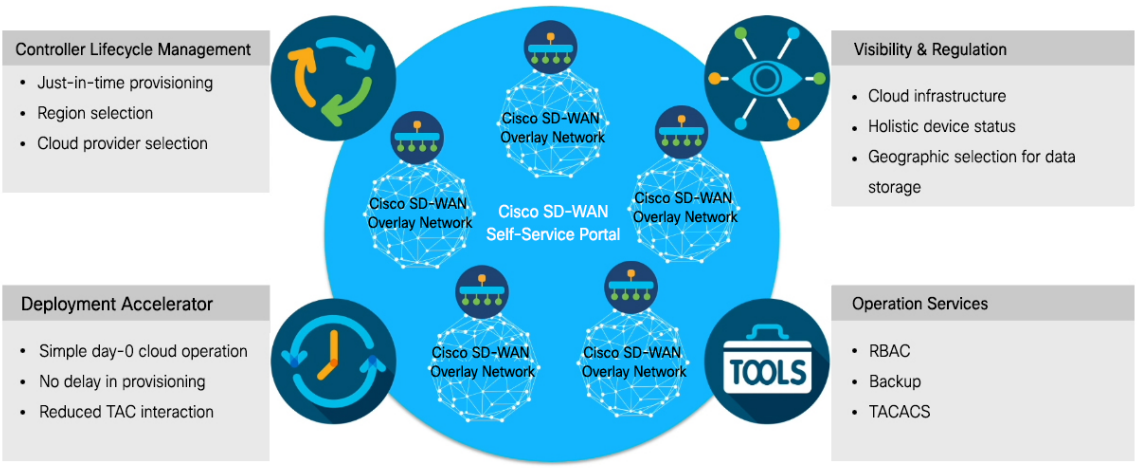
Overview of the Cisco Catalyst SD-WAN Portal

The Cisco Catalyst SD-WAN Portal is a cloud-infrastructure automation tool tailored for Cisco Catalyst SD-WAN, which provides a quick way to provision, monitor, and maintain Cisco Catalyst SD-WAN controllers on public cloud providers.

You can provision the following controllers using the Cisco Catalyst SD-WAN Portal:

- Cisco SD-WAN Manager
- Cisco SD-WAN Validator
- Cisco SD-WAN Controller

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



The Cisco Catalyst SD-WAN Portal can be configured to use an identity provider (IdP) to enable multi-factor authentication (MFA) for the portal access. You can configure the Cisco Catalyst SD-WAN Portal to use an IdP that lets you connect any user with any application on any device, using single sign-on (SSO).

Audience

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

Prerequisites for the Cisco Catalyst SD-WAN Portal

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

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

Benefits of 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 user interface for easy navigation to the appropriate task in the workflow
- Provides selection of cloud providers with options for specifying geographic locations for primary and secondary data storage
- Supports secure log in using an IdP for SSO with multi-factor authentication (MFA)

- Supports role-based access control (RBAC)
- Supports provisioning of new overlay networks with custom subnets for on-premises TACACS server connections to overlays

Smart Account and Virtual Accounts

A Smart Account contains the licenses purchased by your organization. A Smart Account is a central repository where you can view purchased software assets, register, and report software use, and manage licenses across the entire organization.

For the Cisco Catalyst SD-WAN Portal, Cisco has granted the right to access the Cisco Catalyst SD-WAN Portal to the Smart Account administrator. A Smart Account administrator can now view and perform operational tasks related to a customer's hosted controller infrastructure, such as viewing the controllers' IP addresses and modifying the controllers' IP access lists. If you do not wish for certain users to receive such access, go to the Manage Smart Account section of Cisco Software Central, and remove those users as Smart Account administrators, or use the IDP (identity provider) onboarding feature to grant access to the Cisco Catalyst SD-WAN Portal based on the trusted users in the IDP.

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

Virtual Accounts are subaccounts within your Smart Account. Virtual Accounts help you organize your Cisco assets in a way that is logical for your business. You can set up Virtual Accounts by department, product, geography, or other designation that best fits your company's business model.

A default Virtual Account is created for you. We recommend that you create a dedicated Virtual Account for creating Cisco Catalyst SD-WAN overlays.

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

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

Note When you order Cisco DNA licenses using the enterprise agreement, automatic association of Virtual Accounts to an SD-WAN-capable attribute is not available. You need to submit a cloud-controller provisioning request form through the Enterprise Agreement Workspace for the Cisco CloudOps team to provision the controllers. Contact Cisco Catalyst SD-WAN Technical Support to request that the desired Virtual Account become available on the Cisco Catalyst SD-WAN Portal. After the desired Virtual Account is available on the Cisco Catalyst SD-WAN Portal, you can provision the controllers after providing the necessary enterprise agreement contract information.

PCI DSS Certification

Table 1: Feature History

Feature Name	Release Information	Description
Support for PCI DSS Level 1 Certification for Cisco Catalyst SD-WAN Overlay Networks	February 2022 Release	This feature provides Payment Card Industry Data Security Standard (PCI DSS) level 1 certification for Cisco Catalyst SD-WAN overlay networks. Payment Card Industry (PCI)-compliance protects Cisco Catalyst SD-WAN overlay networks against data breaches of cardholder data.

Information About PCI DSS Certification

PCI DSS is an industry information security standard designed to ensure that all companies that accept, process, store, or transmit credit card information, maintain a secure environment. For more information, see the PCI Security Standards Council's website.

Companies handling credit card information are required to maintain data in a secure manner that reduces the likelihood of sensitive financial data from being stolen. If merchants fail to securely handle credit card information, that data can become compromised and used to make fraudulent purchases. Additionally, sensitive information about the cardholder can be used in identity fraud.

While Cisco Catalyst SD-WAN does not directly store or process any cardholder data, Cisco Catalyst SD-WAN is considered a Cloud Service Provider (CSP).

With Cisco Catalyst SD-WAN software controller version 20.6.1, the Cisco Catalyst SD-WAN solution is certified as a PCI DSS level 1 service provider.

Note An upgrade to Cisco Catalyst SD-WAN software controller version 20.6.1 does not mean you are PCI-certified. You must purchase the Cisco Catalyst SD-WAN certified software controller version 20.6.1. Only the certified Cisco Catalyst SD-WAN software controller released with Cisco vManage Release 20.6.1 has the PCI certification.

PCI DDS certification of Cisco Catalyst SD-WAN controller software version 20.6.1 should not impact existing customers whose networks include the Cisco Catalyst SD-WAN solution and were previously certified as PCI DDS compliant. For new customers who wish to obtain PCI DDS certification for their networks, we recommend purchasing the Cisco Catalyst SD-WAN certified software controller version 20.6.1.

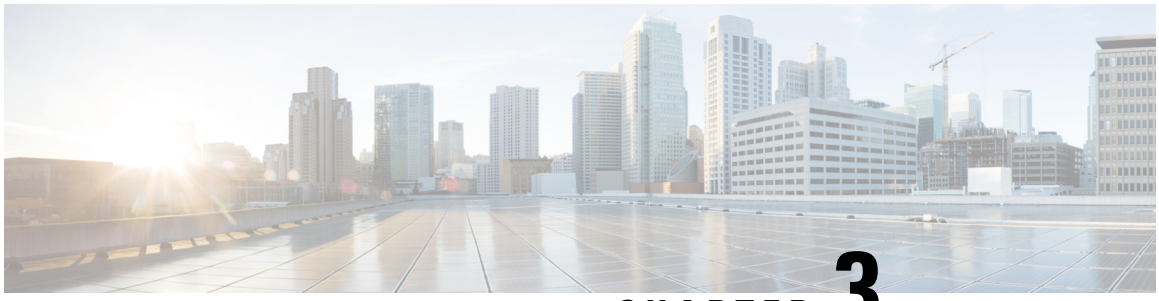
The Cisco Catalyst SD-WAN solution includes security controls aligned with PCI DSS requirements. Many of Cisco’s customers have successfully attained PCI DSS certification, version 3.2.1, with Cisco Catalyst SD-WAN as an integral part of their network.

Contact Cisco Catalyst SD-WAN Technical Support if you have any questions regarding PCI DSS certification of your cloud controllers.

Prerequisites for PCI DSS Certification

- PCI-certified overlay are applicable to cloud deployments only.
- Ensure that you are using Amazon Web Services (AWS) as the cloud provider.
- Ensure that you are using Cisco vManage Release 20.6.1 or other subsequent extended-support releases. Any other release versions, including standard-support releases, are not PCI DSS certified.

  For more information on extended-support releases, see Cisco IOS XE Software Support Timeline for Cisco IOS XE Software Release Starting with 16.x.x.



CHAPTER 3

Access the Cisco Catalyst SD-WAN Portal

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.

Workflow for Smart Account and Virtual Accounts for Provisioning the Controllers

The following is the workflow for creating a Smart Account, a Virtual Account, and associating the Cisco DNA subscription with your Virtual Account.

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

   For information on how to create a Virtual Account, see Create a Virtual Account Associated with Your Smart Account.
3. Purchase a Cisco DNA subscription on the Cisco Commerce Workspace.

Note A Cisco DNA subscription should be associated with one of the Virtual Accounts under the respective Smart Account.

Typically, an account manager or a Cisco sales representative places the order on the behalf of the customer.

4. Choose the DNA cloud subscription product identification (PID) as the license.

   The selection of the DNA cloud subscription PID triggers the automatic association of the Virtual Account with the SD-WAN-capable attribute for provisioning of the controllers.

5. When the order is complete, the Virtual Account is available on the Cisco Catalyst SD-WAN Portal for controller provisioning.

Note The Virtual Account should contain the device serial numbers that were added on the Cisco Plug and Play (PnP) portal. Once the overlay is created through the Cisco Catalyst SD-WAN Portal, see the **Controller Profile** tab on the Cisco PnP portal to view the mapping of the device serial numbers with their respective controllers. The mapping of device serial numbers to the controllers provides the necessary information for adding the devices to Cisco SD-WAN Manager or performing zero-touch provisioning (ZTP). View the **Controller Profile** tab in the Cisco PnP portal to confirm that the controllers were provisioned as part of the Cisco Catalyst SD-WAN overlay creation process using the Cisco Catalyst SD-WAN Portal.

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

Create a Virtual Account

1. In Cisco Software Central, choose **Manage Smart Account** and click **Manage 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 requested information for the required fields.

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 **Create Virtual Account**.

   Your newly created Virtual Account appears in the list of Virtual Accounts.

Workflow for PCI-Certified Overlays

Workflow for PCI-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 PCI-certified overlay.

Workflow for PCI-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. Choose the **Certified Hosting Infra for vManage PID** subscription option.
3. Create a ticket in Cisco One.

   Include the following information in the ticket:

   - Virtual Account
   - Organization Name
   - Order Number
   - Region

4. The Cisco CloudOps team confirms the order number and upgrades an existing overlay as a PCI-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, a guided workflow is presented. This workflow provides you the option to configure some features and create your first Cisco Catalyst SD-WAN overlay network.

You must be a Smart Account administrator to log in to the Cisco Catalyst SD-WAN Portal for the first time and for subsequent log-ins if you are not using an identity provider (IdP).

If you are using an IdP, access to the Cisco Catalyst SD-WAN Portal is based on user access provided by the IdP.

Note You cannot log in to the Cisco Catalyst SD-WAN Portal using Virtual Account administrator-level access as you can with other Cisco 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

When you log in to the Cisco Catalyst SD-WAN Portal, you must use your Cisco credentials.

1. Navigate to the Cisco Catalyst SD-WAN Portal URL.
2. Enter your Cisco login credentials.
3. When prompted, set up or enter your MFA credentials.

Configure Additional MFA Options or Update an Existing MFA Option

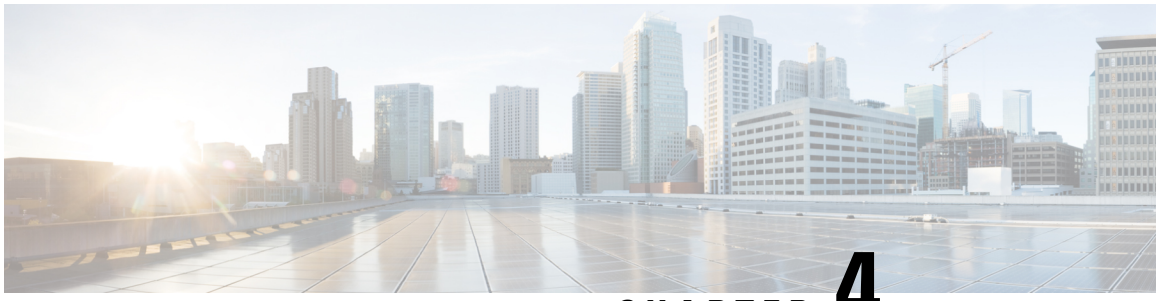
You can add an additional MFA option or update an existing MFA option using the Cisco SD-WAN portal.

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 having successfully logged in to the Cisco SD-WAN Self-Service Portal, navigate 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 right-hand corner of the page, click **Settings**.
4. In the **Extra Verification** section, add an MFA option or update an existing MFA option.



CHAPTER 4

Configure an Identity Provider

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.

Configure an IdP 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 roles (as described in Configure Cisco SD-WAN Self-Service Portal Roles for IdP Users, you can log in using your own IdP instead of your Cisco.com account credentials.

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

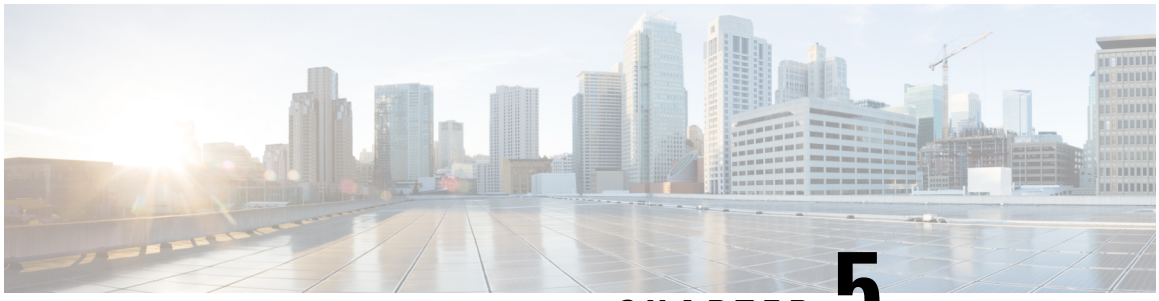
Before you configure an IdP in Cisco Catalyst SD-WAN Portal, you should create the following variables on your organization's IdP. Cisco Catalyst SD-WAN Portal requires these variables for each user that logs in.

- firstName
- lastName
- email
- SSP_User_Role

  For more information on roles, see Configure Cisco SD-WAN Self-Service Portal Roles for IdP Users.

Configure an IdP for the Cisco Catalyst SD-WAN Portal

1. Specify the following information for your IdP. You can find this information in your IdP.
   - Domain Name
   - IdP Issuer URL
   - IdP SSO URL
   - IdP Signature Certificate in .pem format.
2. Click **Submit Request**.
3. On your IdP site, confirm the IdP creation.



CHAPTER 5

Manage Role-Based Access

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.

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.

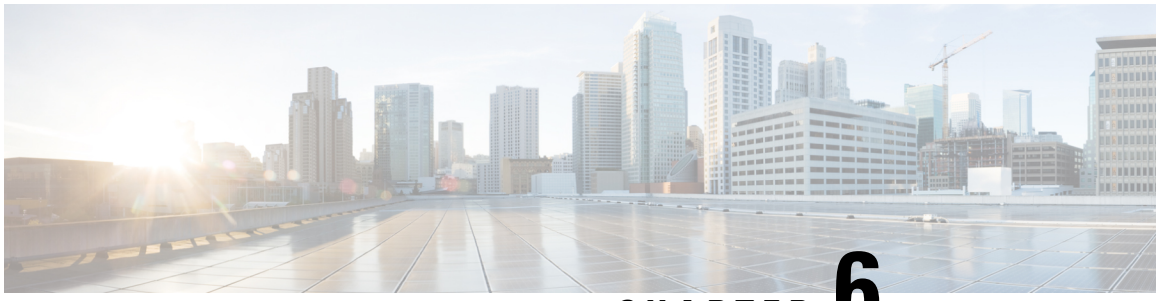
Configure Roles for IdP Users

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 the following list:
   - **Monitor**: Allows you to view and monitor all the overlay options in the Cisco Catalyst SD-WAN Portal.
   - **Overlay Management**: Allows you to create, modify, and monitor overlay networks.
   - **Administration**: Allows you to perform all the tasks defined by the monitor and overlay network roles, and to 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, the Smart Account administrator should follow the same procedure as described in the Configure Cisco SD-WAN Self-Service Portal Roles for IdP Users section.



CHAPTER 6

Manage Overlay Networks

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.

Create a Cisco Catalyst SD-WAN Cloud Hosted Fabric

The Cisco Catalyst SD-WAN Portal provisions Cisco Catalyst SD-WAN fabrics according to the information that you provide as part of the following procedure.

Before You Begin

Ensure that you have the following:

- An active Cisco Smart Account.
- An active Cisco Virtual Account.
- The SA-Admin role for your Cisco Smart Account. (Required to access the Cisco Catalyst SD-WAN Portal for the first time and to create a fabric. Not required thereafter.)
- A valid order for controllers on Cisco Commerce (formerly CCW).

Procedure

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 Overlay** > **Cisco Hosted**.

   The **Create Cisco Hosted Overlay** 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.
4. From the **Virtual Account** drop-down list, choose the name of the Cisco Virtual Account to which you want to associate the fabric.
5. Click **Assign Controllers** and perform the following actions in the **Assign Controllers** area:
   a. From the **Fabric Choice** drop-down list, choose one of the following options:
      - **Shared**: Choose this option if you ordered an SKU for a Shared controller.
      - **Dedicated**: Choose this option if you ordered an SKU for a Dedicated controller (Complimentary or Paid).

   b. If you choose the **Dedicated** fabric option, configure the options for the number of controller types, as described in following table.

      These options do not apply to the **Shared** fabric option. The **Shared** fabric supports only one Cisco SD-WAN Manager, and settings are configured automatically in the background.

Option for Dedicated Fabric	Description
Size (for the **vManage** controller type)	Choose **Small**, **Medium**, or **Large**, depending on the controller SKU that you ordered. For detailed information about these options, see Recommended Computing Resources for Cisco SD-WAN Controller Release 20.11.x.
Assign (for the **vManage** controller type)	Enter the number of Cisco SD-WAN Manager controllers in your deployment. Valid values are **1**, **3**, or **6**.
Size (for the **vBond** controller type)	Enter the number of Cisco SD-WAN Validator in your deployment. The minimum value is **2**.
Size (for the **vSmart** controller type)	Enter the number of Cisco SD-WAN Controllers in your deployment. The minimum value is **2**.

Option for Dedicated Fabric	Description
Enable Cluster	Applies only if you choose a value of **3** or **6** for the number of Cisco SD-WAN Manager controllers. Turn on this option to create a Cisco SD-WAN Manager cluster.
Cluster Type	Applies only if you turn on the **Enable Cluster** option. Choose one of these options: • **Single Tenant Cluster**: Enables a single tenant cluster. • **Multi Tenant Cluster**: Enables a multitenant cluster.

6. In the **Fabric** field, enter a name for your fabric.
7. (Applies to the **Dedicated** fabric option only) Under **Cloud Provider**, choose the cloud provider at which you want Cisco to host the controllers for your fabric (**AWS** or **Azure**).
8. (Applies to the **Dedicated** fabric option only) From the **SD-WAN Version** drop-down list, choose the version of Cisco Catalyst SD-WAN that you want to use on your controllers.

   Choose the recommended version unless there are specific features that you need and these features are available only in another version. For information about recommended versions, go to Cisco Software Central. For information about Cisco Catalyst SD-WAN releases, see the Cisco Catalyst SD-WAN Release Notes in the **Release Information** area in User Documentation for Cisco IOS XE (SD-WAN) Release 17.
9. Turn on the **Enable Analytics** option to enable all the Cisco Catalyst SD-WAN Analytics features for the fabric.

   Cisco Catalyst SD-WAN Analytics is a cloud-based analytics service that offers comprehensive insights into application and network performance, providing information about device and network health, behavior, traffic, and related activities in your fabric.

   If you chose the **Dedicated** fabric option, but do not turn on this **Enable AnalyticsEnable Analytics** option, the system collects Cisco Catalyst SD-WAN Analytics data, but does not provide reports.

   For more information, see Cisco vAnalytics.
10. Under **Locations**, perform these actions:

    a. From the **Primary Location** drop-down list:

       • If you configured the **Shared** fabric option, choose the geographical location where the fabric will be spun up.

       • If you configured the **Dedicated** fabric option, choose the geographical location where the Cisco SD-WAN Manager controllers are provisioned.

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

b. (Applies to the **Dedicated** fabric option only) From the **Secondary Location** drop-down list, choose the geographical location for backed up data storage and load balancing.

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

c. (Applies to the **Dedicated** fabric option only) From the **Data Location** drop-down list, choose the geographical location for Cisco Catalyst SD-WAN Analytics data storage.

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

11. Enter the following information under **Contacts**:

    - In the **Fabric Admin** field, enter the email address or mailer list name 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 ID of the person who created the ticket for your Cisco Catalyst SD-WAN Portal.

12. (Optional, applies to the **Dedicated** fabric option only) Configure the following **Advanced Options**, as needed.

    For detailed information about these options, see Configure Advanced Options for a Cisco Catalyst SD-WAN Cloud Hosted Fabric.

    - **Custom Subnets**: Options for configuring private IP addresses to be used for controller interface IP addresses.
    - **Custom Domain Settings**: Options for configuring custom domains for accessing Cisco SD-WAN Validator and Cisco SD-WAN Manager controllers.
    - **Snapshot Settings**: Option for configuring how often the system takes a snapshot ofCisco SD-WAN Manager instances in your deployment.
    - **Custom Organization Name**: Option for configuring a unique organization name to identify your network.
    - **Compliance Configuration**: Option for selecting a compliance type for a fabric.
    - **Dual Stack**: Option for enabling IPv6 dual stack.

13. Click **Click here to review and agree to Terms & Conditions before proceeding**, and in the **Terms and Conditions** dialog box, review the information that is shown and click **I Agree**.

14. Click **Create Fabric**.

    The system creates the fabric. This process can take up to 60 minutes. Information about the progress of this process appears in the **Create Fabric Progress** area.

    After the fabric is created, you receive an email message notifying you that the fabric is ready.

    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.

To secure your environment, we recommend that you immediately change this password after logging in.

Note The system-provided controller 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.

15. After you receive a notification that your fabric is ready:
    - Install the controller certificates on your devices. For information about installing controller certificates, see Use Case: Cisco-Hosted Cloud Overlays with Software Version 19.x and Above.
    - Install web server certificates. For information about installing web server certificates, see Web Server Certificates.

Configure Advanced Options for a Cisco Catalyst SD-WAN Cloud Hosted 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 that the following sections describe:

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

Custom Subnets

The **Custom Subnets** area includes options for configuring private IP addresses to be used for controller 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 management access to instances over the fabric, you may want to deploy the controllers with their private IP addresses in specific prefixes. These prefixes are unique and unused elsewhere within your fabric.

Option	Description
Primary Subnet	

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

Option	Description
Cluster Subnet	Enter a private IP address block for the cluster subnet for the secondary region. This address must be within the IP address block that you entered for the VPC. 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 controllers.

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

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 Cisco does not have access to your domains.

After you configure a custom domain, make the following mappings to allow controller 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
vBond	Enter the name of the DNS for the Cisco SD-WAN Validator.
vManage	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 ten 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. Options are: • **Once a day** • **Once in 2 days** • **Once in 3 days** • **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. You can enter a name of up to 56 characters. To ensure that an organization name is unique, theCisco Catalyst SD-WAN Portal automatically appends a hyphen (-) followed by your virtual account ID at the end of the name that you enter.

Compliance Configuration

The **Compliance Configuration** area includes an option for selecting a compliance type for a fabric.

Option	Description
Security Compliance	Options are: • **Base**: No compliance type. This setting is the default. • **PCI-DSS**: PCI compliance.

Dual Stack

The **Dual Stack** area includes an option for enabling IPv6 for controllers.

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	Check this check box to enable IPv6 dual stack for controllers.

Information About Snapshots

The Cisco Catalyst SD-WAN cloud-hosted service includes taking regular snapshots of the Cisco SD-WAN Manager instances.

- On-Demand Snapshots

For any major planned change window for your Cisco SD-WAN Manager software, you can take an on-demand snapshot of Cisco SD-WAN Manager. You need to freeze the configuration changes and allocate up to 8 hours before the change window to allow the on-demand snapshot to be taken and completed.

Starting April 2023, you trigger an on-demand snapshot from the Cisco Catalyst SD-WAN Portal. See Take an On-Demand Snapshot.

- Daily Snapshots

  These snapshots are taken automatically each night, around midnight, based on the location of the specified Cisco SD-WAN Manager region. Daily snapshots are taken in accordance with the frequency chosen when creating an overlay network. The snapshot frequency is set by default to once every day, typically midnight of the region of deployment, and the last ten snapshots are retained. You can retain only a maximum of the last ten periodic snapshots. Older snapshots beyond the set frequency are automatically discarded daily.

  Configure the snapshot frequency as part of the Cisco Catalyst SD-WAN Portal overlay creation process by clicking **Advanced Options** > **Edit** and then by clicking **Snapshot Settings**.

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

  You can configure only the frequency of Cisco Catalyst SD-WAN Portal snapshots.

  You can view the snapshot details for your overlays by clicking on the name of the overlay for which a snapshot has been created.

  For more information, see View Snapshots.

Note The Cisco SD-WAN Controller and the Cisco SD-WAN Validator are stateless and therefore snapshots are not taken. Use a Cisco SD-WAN Manager template to configure and save the Cisco SD-WAN Controller and Cisco SD-WAN Validator settings.

Note You cannot download the Cisco Catalyst SD-WAN Portal snapshots, as the snapshots are stored within the Cisco Catalyst SD-WAN Portal cloud account. The Cisco Catalyst SD-WAN Portal snapshot details are provided for read-only purposes. The Cisco CloudOps team uses the snapshots for disaster recovery.

- Golden Snapshots

  Marking an existing daily snapshot or an on-demand snapshot as golden prevents it from getting automatically removed. We can store up to one golden snapshot. If a new daily snapshot or an on-demand snapshot is marked golden, then the golden tag is automatically removed from a previous snapshot, and that old snapshot may be subject to removal, as per the snapshot type expiration process.

  You should mark a snapshot as golden, if the state of Cisco SD-WAN Manager is thought to be in the ideal state at the snapshot time and could serve as a good recovery point later.

Take an On-Demand Snapshot

You can take an on-demand snapshot of Cisco SD-WAN Manager configuration when needed. In general, take a snapshot before any major change window.

When you take an on-demand snapshot, freeze configuration changes and allocate up to 8 hours before the change window to allow the snapshot to be completed.

An on-demand snapshot is stored for 3 months from the date of its creation, then it is deleted automatically. A new on-demand snapshot replaces a stored existing one, so only one on-demand snapshot is stored at a time.

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 overlay 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**.

   The snapshot is created. The creation process can take up 8 hours to complete, depending on the amount of data in Cisco SD-WAN Manager.

Delete an Overlay Network

To delete an overlay network, contact Cisco Catalyst SD-WAN Technical Support. You cannot delete an overlay network.

Specify the Allowed List of IP Addresses for Managing Controller Access

For Cisco-hosted overlay networks, you can specify trusted IP addresses, including prefixes, from which you can manage controller access. To enable management access, specify a rule type, protocol, port range, and 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 overlay. Devices with any IP address can join the overlay, 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 overlay.
- Each rule is uniformly applied to all cloud-hosted controllers within the overlay.
- The same rules are automatically applied when new cloud-hosted instances are added, or existing instances are replaced. The rule can be either a single IP address or a larger IP prefix.

1. From the Cisco Catalyst SD-WAN Portal dashboard, navigate to your overlay network.
2. From the drop-down list, click **Cisco Hosted Overlays**.

   The list of overlay networks appears.
3. Click the name of your overlay network.
4. Click **Inbound Rules**.
5. Specify the following parameters for your IP address or prefix:
   - **Rule type**: Choose one of the following: **All**, **SSH**, **HTTPS**, **Custom TCP rule**, or **Custom UDP rule**.
   - **Port range**: For custom TCP and UDP rules, specify a port range.
   - **Source**: Specify an IP address or IP address prefix.
6. Press **Enter** to add the source IP address or IP address prefix.
7. Click **Add**.
8. (Optional) Add any additional IP addresses or IP address prefixes that you want to allow.
9. Click **Save**.

Create Predefined Inbound Rules

Table 2: 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

With this feature you can create inbound rules, each of which specifies 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.

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.

Use Cases for Predefined Inbound Rules

Predefined inbound rules provide a convenient way to add the same group of trusted IP addresses to existing and new overlays. By creating predefined inbound rules, you avoid having to configure trusted IP address for each overlay manually.

Configure Predefined Inbound Rules

1. From the Cisco Catalyst SD-WAN Portal menu, choose **Admin Settings**.
2. Click **…** adjacent to the Smart Account for which you want to configure a predefined inbound rule and click **Manage Predefined Inbound Rules**.

   A list of the inbound rules that have been configured appears.
3. Click **Add Predefined Inbound Rules**.
4. In the **Add Inbound Rule** area, perform these actions:
   a. In the **Name** field, enter a unique name for the rule.
   b. From the **Rule Type** drop-down list, choose the type of protocol to which the rule applies (**All**, **SSH**, **HTTPS**, **Custom TCP rule**, or **Custom UDP rule**).
   c. If you choose a rule type of **Custom TCP rule** or **Custom UDP rule**, in the **Port Range** field, enter a port range to which the rule applies.

d. In the **Source** field, enter an IP address or IP address prefix.

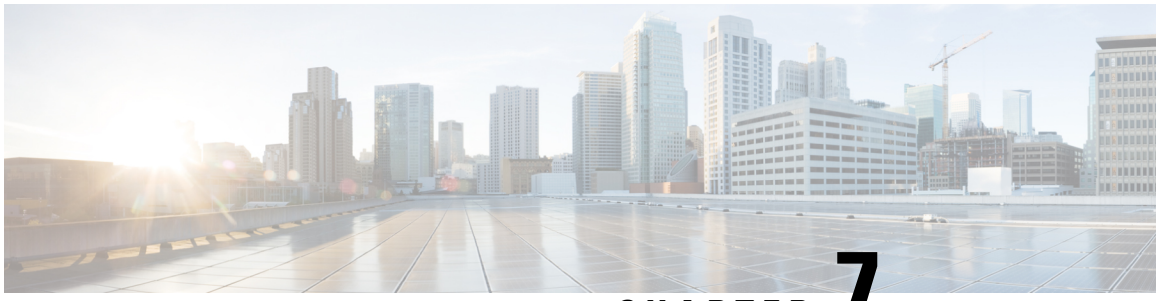
e. (Optional) Click **Automatically add this rule to ALL overlays** to add this new rule to existing overlays under this Smart Account, in addition to future overlays that are created under this Smart Account.

   If you do not click this option, this rule is added to future overlays only.

f. Click **Add**.

Create Additional Overlay Networks

To create additional Cisco Catalyst SD-WAN cloud-hosted overlay networks, follow the same procedure as documented in Create a Cisco SD-WAN Cloud-Hosted Overlay Network.



CHAPTER 7

Cisco Catalyst 8000V as a Cloud Gateway for a Fabric

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.

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	May 2023	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 the following 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

- Integrating your fabric with a TACACS or RADIUS server for authentication, authorization, and accounting (AAA) 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

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

Restrictions for Cisco Catalyst 8000V as a Cloud Gateway for a Fabric

- You must be using a fabric version that is later than Version 20.6.

Configure Cisco Catalyst 8000V as a Cloud Gateway for a Fabric

Before You Begin

Obtain the serial number of each Cisco Catalyst 8000V device that you are configuring. To do so, go to Cisco Software Central and click **Manage Devices** under **Network Plug and Play** in the **Smart Licensing** area.

Configuration Procedures

The following table describes the procedures for configuring a Cisco Catalyst 8000V device as a cloud gateway in various scenarios. For each scenario, the table provides the general steps, and references to more detailed information. See the scenario that applies to your requirements.

Scenario	General Steps	Reference
Create a new fabric and add a Cisco Catalyst 8000V device as the cloud gateway for each 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 33.
Add a Cisco Catalyst 8000V device to each 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 33.
Replace Cisco vEdge Cloud with a Cisco Catalyst 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 33.
	Step 2: (Optional) Open a support case with Cisco to request that the existing Cisco vEdge Cloud be removed.	See Open a Support Case for a Fabric Update, on page 35.

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 that the following table describes.

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	
Username	Enter your Cisco SD-WAN Manager administrator username.
Password	Enter your Cisco SD-WAN Manager administrator password.
Smart Account Admin Credentials	

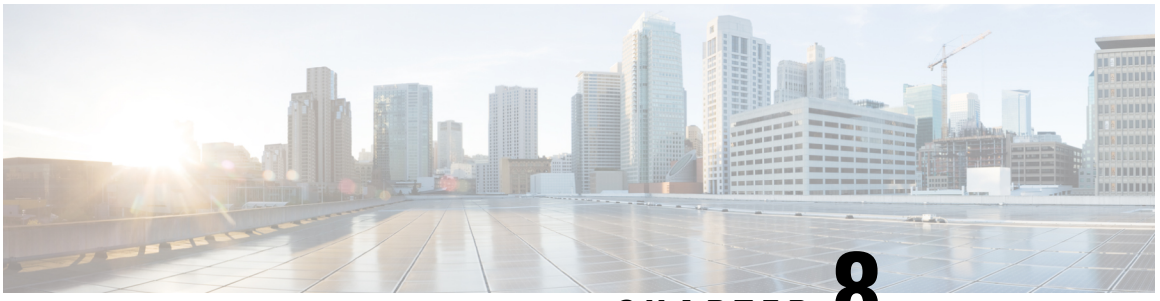
Field	Description
Username	Enter your Cisco Smart Account administrator username.
Password	Enter your Cisco Smart Account administrator password.
Cloud Gateway Serials	
Serial	The number of **Serial** fields that appear matches the number of regions in your fabric. In each field, enter the serial number of the Cisco 8000V to serve as a cloud gateway. Each serial number must be unique.
Custom IPs	
System IPs	The number of **System IPs** fields that appear matches the number of regions in your fabric. (Optional) In each field, enter an IP address to configure a system interface for the cloud gateway that you are adding. A system interface IP address is a persistent address that identifies the device. It is similar to a router ID on a regular router, which is the address that is used to identify the router from which packets originated. Specify a system IP address as an IPv4 address in decimal four-part dotted notation. Specify just the address; the prefix length (/32) is implicit. A system IP address can be any IPv4 address except for 0.0.0.0/8, 127.0.0.0/8, and 224.0.0.0/4, and 240.0.0.0/4 and later. If you do not specify a system IP address, the Cisco Catalyst SD-WAN Portal assigns a system random IP address, which may be a duplicate of the IP address of another device. To ensure that a cloud gateway is provisioned without creating a conflict in the fabric, ensure that an IP address that you enter is unused in the existing fabric.

Field	Description
Enable Webhook via Cloud Gateway	This option applies only to a Dedicated fabric for which AWS is the cloud provider. Check this check box to enable Cisco SD-WAN Manager to route webhook messages from CCisco SD-WAN Manager through a cloud gateway Enabling this option is useful when your webhook server is hosted in your private network and no internet traffic is forwarded to this server. When this option is enabled, a connection is provisioned between your SD-WAN fabric and your private network. After enabling this option, add an entry to the routing table on the Cisco SD-WAN Manager server to forward network traffic to the webhook server through the cloud gateway. For instructions, see the email that you receive after the cloud gateway is provisioned.

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 8

Monitor Overlay Networks

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.

Monitor Cisco Catalyst SD-WAN Controllers and Devices in Overlay Networks

1. From the Cisco Catalyst SD-WAN Portal dashboard, click an overlay.

   The list of overlays appears.

2. Click the name of your overlay.
3. In the **Controller View** tab, click the controller that you want to monitor, such as **Cisco vManage**, **Cisco vBond Orchestrator**, **Cisco vSmart Controller**, or **Cisco vEdge Cloud**.
4. On the **Controllers** window, you can filter by network usage, CPU usage, or duration. In the window, you can also filter by state, type, or the IP address of the controller.

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

View Overlay and Controller Details

1. From the Cisco Catalyst SD-WAN Portal dashboard, click the overlay for which you want to view the details.

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

2. Click the name of the overlay.

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

View Change Window Notifications

Table 4: Feature History

Feature Name	Release Information	Description
Change Window Notifications	February 2021 Release	This feature lets you see when your Cisco Catalyst SD-WAN overlay maintenance event starts or ends, including detailed information about when the change notification is scheduled, and the planned operation for maintenance. 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 allow you to see when your Cisco Catalyst SD-WAN overlay maintenance event starts or ends, including detailed information about when the change notification is scheduled, and the planned operation for maintenance.

Change window notification alerts display for notifications started or scheduled within the next 10 days. If a notification is in a completed state 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 displays as ongoing in the banner alert.

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

Before You Begin

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

A CloudOps user needs to schedule or start a change window notification.

View Change Window Notifications for All Overlays

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

   The **Dashboard** > **Change Window Notifications** page appears with the list of overlays.

Banner alerts display for all of the change window notifications.

This is the global view for viewing all change window notifications for all of your overlays.

2. (Optional) You can filter the overlay by status to limit or expand the list of overlays.
3. Click on **Change Window Notifications** to see the list of change window notifications, including the details column for the description of the change notification.

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

View Change Window Notifications for Specific Overlays

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

   The **Dashboard** > **Overlays** > **Details** page appears.
2. Click an overlay that has a scheduled or started change window notification.

   Banner alerts display for the change window notifications specific to the overlay. The banner alert does not include the name of the overlay because you are already within the overlay.

   This is the individual view for viewing change window notifications for a specific overlay.

View the List of Change Window Notifications

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

   The **Dashboard** > **Overlays** page displays.
2. Click on the overlay 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.

View Snapshots

Before You Begin

You need to have a Cisco-provisioned cloud-hosted controller set for your overlay to view the snapshot details.

For more information, see Create a Cisco SD-WAN Cloud-Hosted 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.

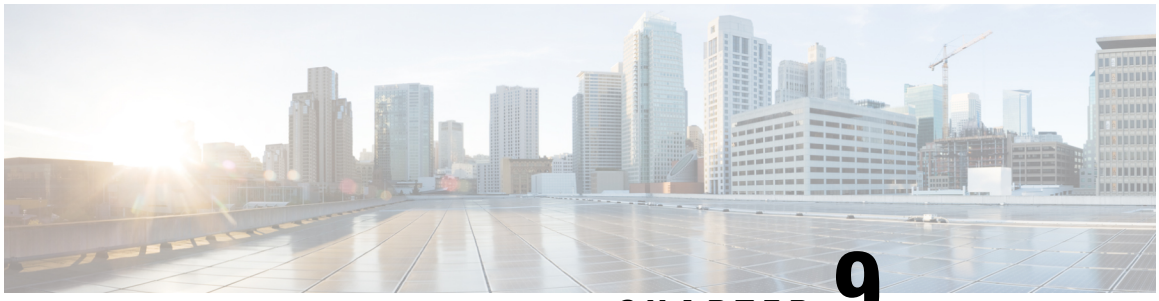
2. Click the name of an overlay for which you want to view a snapshot.
3. From the **Dashboard** > **Cisco Hosted Overlays** > **Details** page, click on the tile for **Snapshot**.

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

Table 5: Snapshot Fields

Field	Description
Snapshot ID (*denotes golden snapshot)	Specifies the snapshot ID. 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. For successful disaster recovery, snapshots of all the disks, taken at the same time, are used to recover and build the Cisco SD-WAN Manager instance.
Golden	Specifies if the snapshot is a golden snapshot. Available values are as follows: • **false** • **true**
Region	Specifies the region where this snapshot is stored.
Type	Specifies the type of snapshot. Available values are as follows: • **REGULAR** • **ON-DEMAND** • **GOLDEN**

Field	Description
Overlay ID	Specifies the overlay ID.
Overlay	Specifies the overlay name and an ID.
Instance ID	Specifies the Cisco SD-WAN Manager instance ID.
Instance	Specifies the Cisco SD-WAN Manager instance name and ID.
Actions	Click **Make Golden Snapshot** to mark a specific date snapshot as golden.



CHAPTER 9

Manage Account Settings

Table 6: Feature History

Feature Name	Release Information	Description
Support for Managing Predefined Inbound Rules	November 2022 Release	With this feature, you can specify trusted IP addresses, including prefixes, from which you can manage controller access. You can apply the predefined inbound rules to all of your overlays.

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.

Information About Predefined Inbound Rules

You can specify predefined inbound rules for allowing trusted IP addresses, including prefixes, for managing controller access. The predefined rules apply to any existing or new overlay network created with the associated Smart Account.

You can add up to 200 rules per overlay network.

Benefits of Predefined Inbound Rules

- Applies predefined inbound rules automatically to any overlay created with the associated Smart Account

- Supports equivalent audit log entries for the allowed IP addresses

Use Case for Predefined Inbound Rules

Manage 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 an overlay.

   For more information on creating a Cisco Catalyst SD-WAN cloud-hosted overlay network, see Create a Cisco Catalyst SD-WAN Cloud-Hosted Overlay Network.

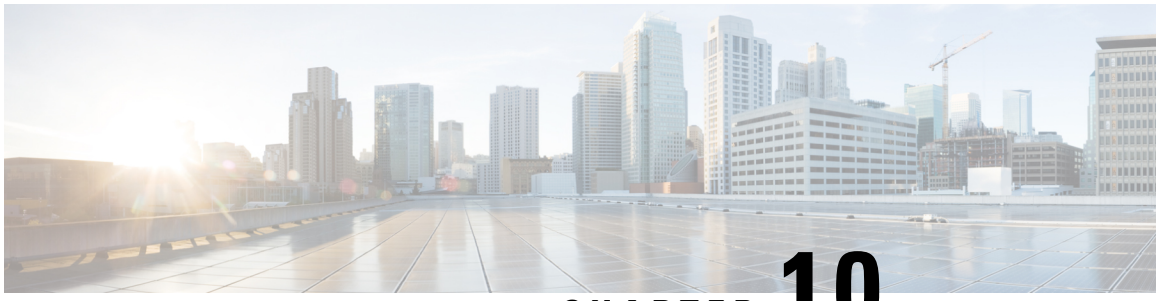
Manage Predefined Inbound Rules

1. From the Cisco Catalyst SD-WAN Portal menu, choose **Admin Settings**.
2. Under **Actions**, click **. . .** 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	Choose one of the available options from the drop-down list. • **All** • **SSH** • **HTTPS** • **Custom TCP rule** • **Custom UDP rule**
Protocol	**Protocol** is automatically populated depending on which **Rule Type** you choose.
Port Range	Enter a port range. If you chose **Custom TCP rule** or **Custom UDP rule**, port range is automatically populated.

Field	Description
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 overlays	Check the **Automatically add this rule to ALL overlays** check box if you want to apply the predefined rules to all the overlays associated with your Smart Account. If you do not check **Automatically add this rule to ALL overlays**, the rule does not get added to your existing overlays.

5. Click **Add**.



CHAPTER 10

Troubleshooting

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.

Update an Expired IdP Certificate

To update an expired identity provider (IdP) certificate, use the **Need help signing in** link at the bottom of 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 IdP is misconfigured, and you are not able to log in, you can configure a new IdP.

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.

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 usually happens when there is no SD-WAN-capable attribute associated with the Smart Account.

Solution

Associate your Cisco 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 Cisco Catalyst SD-WAN Technical Support to associate the Smart Account with your Cisco 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 Cisco DNA subscription is not associated with the Virtual Account.

Solution

For customers with an enterprise agreement, automatic association of Virtual Accounts to an SD-WAN-capable attribute is not available.

To associate a Virtual Account with your Cisco DNA subscription as an enterprise customer, do the following:

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, you can provision the controllers after providing the necessary enterprise agreement contract information.

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 Cisco DNA subscription, contact Cisco Catalyst SD-WAN Technical Support to associate the Virtual Account with your Cisco DNA cloud subscription.

Troubleshoot Browser Security Issues

Problem

You receive the following error:

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

A cross-site request forgery (CSRF) token mismatch is an error whereby the browser is not able to create a secure cookie, or the browser is not able to access the cookie for you to log in.

Solution

This error occurs due to certain security settings on your web browser.

Clear the cache on your browser or try another browser.