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 Controller**. 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.

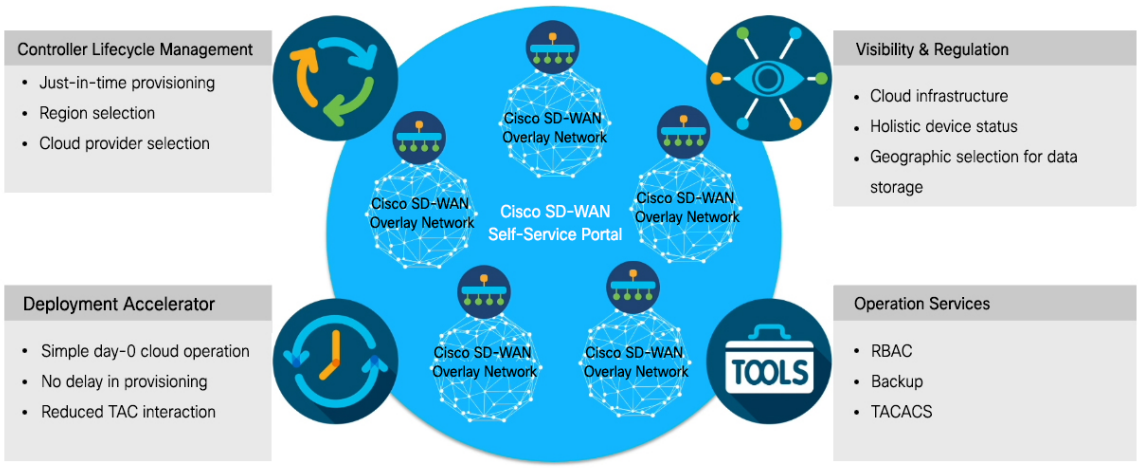
Overview of the Cisco Catalyst SD-WAN Portal

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



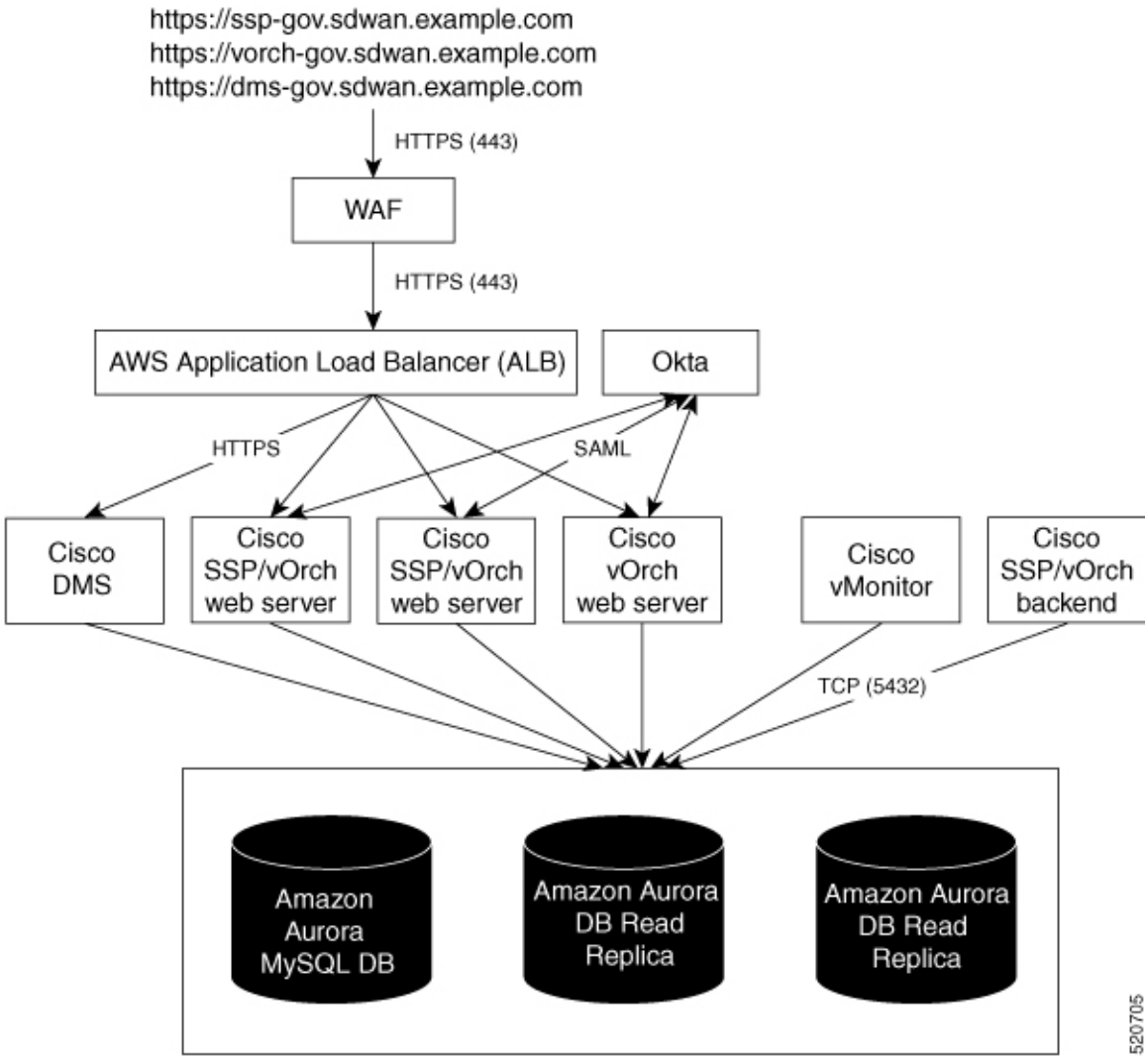
The Cisco Catalyst SD-WAN Portal can be configured to use an identity provider (IdP) to enable multi-factor authentication (MFA) for the portal access. You can configure the Cisco Catalyst SD-WAN Portal to use an IdP that lets you connect any user with any application on any device, using single sign-on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

Cisco vMonitor monitors the cloud infrastructure and updates health notifications regarding a customer's overlay infrastructure to 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.

A common global database with multiple read replicas for high availability and disaster recovery is used by all the three applications, and the applications connect to the database using a Transport Layer Security (TLS) or a Secure Socket Layer (SSL) connection.

Figure 2: Cisco Catalyst SD-WAN Portal Architecture



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 Federal Operations (FedOps): A Cisco team that maintains and monitors Cisco Catalyst SD-WAN for government.

Note Cisco FedOps cannot access the customers' Amazon VPCs.

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 Access the Cisco Catalyst SD-WAN Portal, on page 5.

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 Access the Cisco Catalyst SD-WAN Portal, on page 5.

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.

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 Controller**. 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 Access the Cisco Catalyst SD-WAN Portal, on page 5.
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 Access the Cisco Catalyst SD-WAN Portal, on page 5.

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.

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 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 Controller**. 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. (Applicable only for federal environments), check the **I acknowledge that this is a Federal IDP** check box.
3. Click **Submit Request**.
4. On your IdP site, confirm the IdP creation.

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 Controller**. 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.

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 Controller**. 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**.
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

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	
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	

Option	Description
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.
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.

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 1: 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.

Monitor Overlay Networks

You can monitor the Cisco Catalyst SD-WAN controllers and devices in the overlay networks. You can also view the Plan of Actions and Milestones report.

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.

View Plan of Action and Milestones

To view the POA&M report, do the following:

1. From the Cisco Catalyst SD-WAN Portal dashboard, click **Regulated**.

   The **POAM** window, which provides a vulnerability feed of your overlay networks, is displayed. Using sources such as Qualys, Wazuh, and so on, the **POAM** window lists a variety of issues. You can search,

categorize, and download the reports. You can feed the downloaded reports to a security information and event management (SIEM) software such as Splunk.

2. Perform the following tasks in the **POAM** window:
   - Use the search bar to filter and search for issues. You can filter by various parameters, such as POAM status, risk rating, custom date ranges for detection of issues, and so on.
   - To view information about a specific issue, click **Details**.

     A dialog box, which lists additional information about the alert, including a description of the issue, appears.
   - To filter by a specific column, click the textbox under the column. For example, you can click under the **Adjusted Risk** column, and enter **high** to list all the high-risk issues.

Troubleshooting

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 Access the Cisco Catalyst SD-WAN Portal, on page 5.

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 Cisco Catalyst SD-WAN Portal, on page 1.

For more information, see Access the Cisco Catalyst SD-WAN Portal, on page 5.

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.