

Manage Fabrics

- Create a Cisco SD-WAN Cloud-Pro fabric, on page 1
- Configure advanced options for a Cisco SD-WAN Cloud-Pro fabric, on page 5
- Hybrid fabrics and on-premises SD-WAN Controllers, on page 10
- Delete a fabric, on page 10
- Specify the allowed list of IP addresses for managing control component access, on page 10

Create a Cisco SD-WAN Cloud-Pro fabric

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

Before you begin

Ensure that you have these items:

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

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

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

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

Create a first Cisco SD-WAN Cloud-Pro fabric

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

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

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



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

4. If your Smart Account has unused SD-WAN control component licenses, you are asked if you want to use them to create your fabric. Select **Yes** or **No** and click **Submit**.
   a. If you selected **Yes**, an option to **Assign SDWAN Fabric License** appears. Click the option to display a list of available licenses.
   b. Enter the quantity of each type of license you want to use and click **Assign**.
5. From the **Virtual Account** drop-down list, choose the name of the Cisco Virtual Account to which you want to associate the fabric.
6. Select a Cisco SD-WAN Cloud or Cisco SD-WAN Cloud-Pro Fabric. If you select Cisco SD-WAN Cloud-Pro, a questionnaire dialog box appears. Provide the required details in the dialog box.



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

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

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

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

Option	Description
Assign (for the **SD-WAN Validator** control component type)	Enter the number of Cisco SD-WAN Validators in your deployment. The minimum value is **2**.
Assign (for the **SD-WAN Controller** control component type)	Enter the number of Cisco SD-WAN control components in your deployment. 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 **Single Tenant Cluster** to enable a single tenant cluster.

b. Click **Assign**.

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

c. Click on the pencil icon to edit.

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

e. Click on the check mark icon to save.

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

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

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

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

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

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

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

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



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

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

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

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

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

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

Custom Subnets

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

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

Option	Description
Primary Subnet	
VPC Subnet	Enter a private IP address block for the VPC for the primary region, For example, 192.168.0.0/24. 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 bits.
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 bits.
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 bits.
Secondary Subnet	
VPC Subnet	Enter a private IP address block for the VPC for the secondary region, for example, 192.168.1.0/24. This IP address block must be reachable from your private network.
Primary Location	Shows the secondary region for the fabric.

Option	Description
Management Subnet	Enter a private IP address block for the management subnet for the secondary region. 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.

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

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

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

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

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

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

Snapshot Settings

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

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

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

Option	Description
Frequency	Choose how often the system takes a snapshot of Cisco SD-WAN Manager instances: • **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 each organization's name is unique, the Cisco Catalyst SD-WAN Portal automatically appends a hyphen and your virtual account ID at the end of the name you enter.

Certification Compliance Modes

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

Table 1: Supported Certifications

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

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

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

Custom Key Management

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

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

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

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

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

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

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

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

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

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

Dual Stack

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

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

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

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

Hybrid fabrics and on-premises SD-WAN Controllers

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

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

Manage on-premises SD-WAN Controllers

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

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

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

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

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

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

Delete a fabric

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

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

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

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

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

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