



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, on page 1](#)
- [Configure Advanced Options for a Cisco Catalyst SD-WAN Cloud Hosted Fabric, on page 5](#)
- [Information About Snapshots, on page 8](#)
- [Take an On-Demand Snapshot, on page 10](#)
- [Delete an Overlay Network, on page 10](#)
- [Specify the Allowed List of IP Addresses for Managing Controller Access, on page 10](#)
- [Create Predefined Inbound Rules, on page 12](#)
- [Create Additional Overlay Networks, on page 13](#)

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: <ul style="list-style-type: none"> • 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 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 of Cisco 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 | <p>Enter a private IP address block for the VPC for the primary region, For example, 192.168.0.0/24.</p> <p>This IP address block must be reachable from your private network.</p> |
| Primary Location | Shows the primary region for the fabric. |
| Management Subnet | <p>Enter a private IP address block for the management subnet for the primary region.</p> <p>This address must be within the IP address block that you enter for the VPC.</p> <p>The minimum size of the IP address block is 16.</p> |
| Control Subnet | <p>Enter a private IP address block for the control subnet for the primary region.</p> <p>This address must be within the IP address block that you entered for the VPC.</p> <p>The minimum size of the IP address block is 16.</p> |
| Cluster Subnet | <p>Enter a private IP address block for the cluster subnet for the primary region.</p> <p>This address must be within the IP address block that you entered for the VPC.</p> <p>The minimum size of the IP address block is 16.</p> |
| Secondary Subnet | |
| VPC Subnet | <p>Enter a private IP address block for the VPC for the secondary region, for example, 192.168.1.0/24.</p> <p>This IP address block must be reachable from your private network.</p> |
| Primary Location | Shows the secondary region for the fabric. |
| Management Subnet | <p>Enter a private IP address block for the management subnet for the secondary region.</p> <p>This address must be within the IP address block that you entered for the VPC.</p> <p>The minimum size of the IP address block is 16.</p> |
| Control Subnet | <p>Enter a private IP address block for the control subnet for the secondary region.</p> <p>This address must be within the IP address block that you entered for the VPC.</p> <p>The minimum size of the IP address block is 16.</p> |

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

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 | <p>Choose how often the system takes a snapshot of Cisco SD-WAN Manager instances. Options are:</p> <ul style="list-style-type: none"> • 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 | <p>Enter a unique name for your organization.</p> <p>You can enter a name of up to 56 characters.</p> <p>To ensure that an organization name is unique, the Cisco Catalyst SD-WAN Portal automatically appends a hyphen (-) followed by your virtual account ID at the end of the name that you enter.</p> |

Compliance Configuration

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

| Option | Description |
|----------------------------|--|
| Security Compliance | <p>Options are:</p> <ul style="list-style-type: none"> • 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 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](#).

