Revised: July 22, 2026

# Cisco Secure Access for Cisco Catalyst SD-WAN Devices

## Feature history for Cisco Secure Access integration

*Table 1: Feature history*

| Feature | Release information | Description |
|---|---|---|
| Cisco Secure Access Integration | Cisco IOS XE Catalyst SD-WAN Release 17.13.1a<br>Cisco Catalyst SD-WAN Manager Release 20.13.1 | Cisco Secure Access is a cloud Security Service Edge (SSE) solution, that provides seamless, transparent, and secure Direct Internet Access (DIA).<br>This feature supports Cisco Secure Access integration through policy groups in Cisco SD-WAN Manager. |
| Cisco Secure Access integration extended to Cisco Catalyst SD-WAN for Government | Cisco Catalyst SD-WAN Manager Release 26.1.1.1 | Cisco Catalyst SD-WAN for Government can integrate with a federally authorized Cisco Security Service Edge (SSE) server to enable Cisco Secure Access integration. |

## What is Cisco Secure Access integration

A Cisco Secure Access integration is a cloud security solution that

- provides multiple levels of defense against internet-based threats, and
- integrates with Cisco SD-WAN Manager via REST APIs to share policy information with SD-WAN devices, and
- provides seamless, transparent, and secure Direct Internet Access (DIA) to help users connect from anything to anywhere.

#### Secure Service Edge policy configuration

To configure Secure Service Edge (SSE), select Cisco Secure Access as the provider in the SSE policy group in Cisco SD-WAN Manager.

The SSE policy group defines IPSec tunnels and tunnel parameters. You can provision network tunnel groups in Cisco Secure Access and provide attributes to the edge devices that are needed to set up IPSec tunnels.

For more information on network tunnel groups, see Manage Network Tunnel Groups.

## Restrictions for Cisco Secure Access integration

### Configuration and capabilities

- This feature cannot be configured through a CLI template. This feature can be configured using policy groups on Cisco SD-WAN Manager.

### Operational limitations

- Cisco SD-WAN Manager does not support API throttling to Cisco Secure Access.
- After Cisco Secure Access integration with Cisco Catalyst SD-WAN, any changes made to the network tunnel group name in Cisco Secure Access dashboard are not reflected in Cisco SD-WAN Manager.

## FedRAMP Compliance

- For Cisco Catalyst SD-WAN for Government, the connection between Cisco SD-WAN and Cisco Secure Service Edge has not been assessed for FedRAMP compliance by third-party auditors.

## DNS and HTTPS inspection for SSE API communication

If NGFW is enabled on the router and the Self-Zone is configured with active security rules, ensure that DNS and HTTPS traffic are inspected. This configuration is required for the router to complete the SSE API communication workflow successfully.

# Workflow to set up Cisco Secure Access

Follow these steps to integrate Cisco Secure Access with Cisco Catalyst SD-WAN:

**Before you begin**

Before you begin, ensure the following prerequisites are met:

- Ensure that a configuration group is associated to the selected WAN edge devices and deployed.
- Configure the **IP domain lookup** command on the device.
- Configure the DNS server on Cisco SD-WAN Manager to connect to Cisco Secure Access.

**Step 1** Create Cisco Secure Access credentials on the **Administrator** > **Settings** page.

**Step 2** Create automatic tunnels to Cisco Secure Access using **Configuration** > **Policy Groups**.

**Step 3** Redirect traffic to Cisco Secure Access using service routes or policy groups.

## Create Cisco Secure Access credentials

Follow these steps to create Cisco Secure Access credentials:

**Before you begin**

Ensure you use the same Cisco SSE credentials that you originally used to create the SSE tunnels when you remove any tunnel configurations. Changing or updating these credentials before clearing existing Cisco SSE configurations can result in issues. Change the credentials only if absolutely necessary.

If there are two Cisco SD-WAN Manager instances in the SD-WAN overlay, each Cisco SD-WAN Manager instance has its own SSE credentials and the tunnel is unique to that instance. The SSE tunnels cannot be shared across Cisco SD-WAN Manager instances.

**Step 1** From **Configuration** > **Policy Groups** > **Add Secure Service Edge (SSE)** in Cisco SD-WAN Manager, select Cisco Secure Access as the provider.

**Step 2** From Cisco SD-WAN Manager 26.1.1, choose between **Commercial** or **GovCloud**. Choose **GovCloud** only if you are using Cisco Catalyst SD-WAN for Government.

When changing, SD-WAN Manager prompts you to enter your Cisco SSE credentials.

Before changing this option, remove any configured Cisco SSE features.

**Step 3** Create the credentials in the **Administration > Settings** page. Click **Click here to add Cisco Secure Access Credentials** to create the Cisco Secure Access credentials.

Enter Cisco Secure Access credentials:

| Field | Description |
|---|---|
| **Organization ID** | Cisco Secure Access organization ID for your organization.<br>For more information, see *Find Your Organization ID* in the Cisco Secure Access User Guide. |
| **API Key** | Cisco Secure Access API Key. |
| **Secret** | Cisco Secure Access API Secret. |

**Step 4** Click **Add**.

## Create tunnels to Cisco Secure Access using policy groups

Follow these steps to create tunnels to Cisco Secure Access using policy groups:

***Table 2: Actions for tunnel deletion in Cisco Secure Access***

| When ... | Then for Cisco Secure Access ... | |
|---|---|---|
| The deletion is initiated from Cisco SD-WAN Manager , the SSE Tunnel is not removed from the SSE dashboard. | You must manually delete the Remote Tunnel Group, which is the device Chassis ID (specific to Cisco Secure Access), from the SSE dashboard before provisioning it again from Cisco SD-WAN Manager . | |

**Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **Add Secure Service Edge (SSE)**.

**Step 2** Configure a tracker.

a) **Source IP Address**: Enter a source IP address without a subnet mask.

b) Configure the following parameters for tracker configurations:

***Table 3: Tracker Parameters***

| Field | Description |
|---|---|
| **Name** | Name of the tracker. The name can be up to 128 alphanumeric characters. |
| **API url of endpoint** | Specify the API URL for the Secure Service Edge endpoint of the tunnel.<br>Default: service.sig.umbrella.com |
| **Threshold** | Enter the wait time for the probe to return a response before declaring that the configured endpoint is down.<br>Range: 100 to 1000 milliseconds<br>Default: 300 milliseconds |

| Field | Description |
|---|---|
| **Probe Interval** | Enter the time interval between probes to determine the status of the configured endpoint.<br>Range: 20 to 600 seconds<br>Default: 60 seconds |
| **Multiplier** | Enter the number of times to resend probes before determining that a tunnel is up or down.<br>Range: 1 to 10<br>Default: 3 |

**Step 3** Configure tunnel parameters.

***Table 4: Basic Settings***

| Field | Description |
|---|---|
| **Tunnel Type** | • Cisco Secure Access: (Read only) **ipsec**<br>• (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1) Zscaler: **ipsec** or **gre** |
| **Interface Name (1..255)** | Name of the interface. |
| **Description** | Enter a description for the interface. |
| **Tracker** | By default, a tracker is attached to monitor the health of tunnels. |
| **Tunnel Source Interface** | Name of the source interface of the tunnel. This interface should be an egress interface and is typically the internet-facing interface. The tunnel source interface supports loopback. |
| **Source Public IP** | (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1)<br>Public IP address of the tunnel source interface that is required to create the GRE tunnel to Zscaler.<br>Default: Auto.<br>We recommend that you use the default configuration. With the default configuration, the Cisco IOS XE Catalyst SD-WAN device finds the public IP address assigned to the tunnel source interface using a DNS query. If the DNS query fails, the device notifies Cisco SD-WAN Manager of the failure. Enter the public IP address only if the DNS query fails. |
| **Data-Center** | For a primary data center, click **Primary**, or for a secondary data center, click **Secondary**. Tunnels to the primary data center serve as active tunnels, and tunnels to the secondary data center serve as back-up tunnels. |
| **Advanced Options** (Optional) | |

| Field | Description |
|---|---|
| **Shutdown** | Click the radio button to enable this option.<br>Default: Disabled |
| **Enable Tracker** | Click the radio button to enable this option. |
| **IP MTU** | Specify the maximum MTU size of packets on the interface.<br>Range: 576 to 2000 bytes<br>Default: 1400 bytes |
| **TCP MSS** | Specify the maximum segment size (MSS) of TPC SYN packets. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.<br>Range: 500 to 1460 bytes<br>Default: None |
| **DPD Interval** | Specify the interval for Internet Key Exchange (IKE) to send Hello packets on the connection.<br>Range: 10 to 3600 seconds<br>Default: 10 |
| **DPD Retries** | Specify the number of seconds between Dead Peer Detection (DPD) retry messages if the DPD retry message is missed by the peer.<br>If a peer misses a DPD message, the router changes the state and sends a DPD retry message. The message is sent at a faster retry interval, which is the number of seconds between DPD retries. The default DPD retry message is sent every 2 seconds. The tunnel is marked as down after five DPD retry messages are missed.<br>Range: 2 to 60 seconds<br>Default: 3 |
| **IKE** | |
| **IKE Rekey Interval** | Specify the interval for refreshing IKE keys.<br>Range: 3600 to 1209600 seconds (1 hour to 14 days)<br>Default: 14400 seconds |

| Field | Description |
|---|---|
| **IKE Cipher Suite** | Specify the type of authentication and encryption to use during IKE key exchange.<br>Choose one of the following:<br>• AES 256 CBC SHA1<br>• AES 256 CBC SHA2<br>• AES 128 CBC SHA1<br>• AES 128 CBC SHA2<br>Default: AES 256 CBC SHA1 |
| **IKE Diffie-Hellman Group** | Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2. |
| **IPSec** | |
| **IPsec Rekey Interval** | Specify the interval for refreshing IPsec keys.<br>Range: 3600 to 1209600 seconds (1 hour to 14 days)<br>Default: 3600 seconds |
| **IPsec Replay Window** | Specify the replay window size for the IPsec tunnel.<br>Options: 64, 128, 256, 512, 1024, 2048, or 4096 packets.<br>Default: 512 |
| **IPsec Cipher Suite** | Specify the authentication and encryption to use on the IPsec tunnel.<br>Options:<br>• AES 256 CBC SHA1<br>• AES 256 CBC SHA 384<br>• AES 256 CBC SHA 256<br>• AES 256 CBC SHA 512<br>• AES 256 GCM<br>Default: AEM 256 GCM |

| Field | Description |
|---|---|
| **Perfect Forward Secrecy** | Specify the Perfect Forward Secrecy (PFS) settings to use on the IPsec tunnel. Choose one of the following Diffie-Hellman prime modulus groups:<br>• Group-2 1024-bit modulus<br>• Group-14 2048-bit modulus<br>• Group-15 3072-bit modulus<br>• Group-16 4096-bit modulus<br>• None: disable PFS |

**Step 4** Choose a **Region** from the drop-down list.

When you choose the region, a pair of primary and secondary region is selected. Choose the primary region that Cisco Secure Service Edge provides from the drop-down list and the secondary region is auto-selected in Cisco SD-WAN Manager. If the primary region with a unicast IP address is not reachable then the secondary region with a unicast IP address is reachable and vice versa. Cisco Secure Access ensures that both the regions are reachable at all times.



**Note** You can configure any DNS server on the device which connects to HTTPS to get the public IP address. To configure a source interface for HTTPS, use the **ip http client source-interface** command on Cisco SD-WAN Manager.

**Step 5** To designate active and back-up tunnels and distribute traffic among tunnels configure HA.

***Table 5: Add interface pair***

| Field | Description |
|---|---|
| **Active Interface** | Choose a tunnel that connects to the primary data center. |
| **Active Interface Weight** | Enter weight (weight range 1 to 255) for load balancing.<br>Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights to both the tunnels, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow.<br>For example, if you set up two active tunnels, where the first tunnel is configured with weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio. |
| **Backup Interface** | To designate a back-up tunnel, choose a tunnel that connects to the secondary data center.<br>To omit designating a back-up tunnel, choose **None**. |

| Field | Description |
|---|---|
| **Backup Interface Weight** | Enter weight (weight range 1 to 255) for load balancing.<br><br>Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow.<br><br>For example, if you set up two back-up tunnels, where the first tunnel is configured with weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio. |

**Step 6** Click **Add**.

## Redirect traffic to Cisco Secure Access

Follow these steps to redirect traffic to Cisco Secure Access:

You can redirect traffic to a Cisco Secure Access in two ways:

| Option | Description |
|---|---|
| Redirect traffic using policy groups | • From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **Application Priority & SLA**.<br><br>• Add rules and set the action parameters to the policy to redirect traffic to the SSE instance. For more information, see Action Parameters in the *Policy Groups Configuration Guide*. |
| Redirect traffic using service route | • From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups** > **Service Profile**.<br><br>• Modify the service VPN parameters to ensure that the device connects to the SSE instance to include a service route to the SSE. For more information, see Service VPN in *Configuration Groups Reference Guide*. |

# Monitor tunnels to Cisco Secure Access

To view information about the Cisco Secure Access tunnels on a Cisco Catalyst SD-WAN device, use the **show SSE all** command.

To view information about the Cisco Secure Access tunnels that you have configured from a Cisco Catalyst SD-WAN device, use the **show SSE all** command.

```
Device# show sse all

************************************
   SSE  Instance Cisco-Secure-Access
************************************
Tunnel name : Tunnel15000001
Site id: 2678135102
Tunnel id: 617865691
```

```
SSE tunnel name: C8K-63a9b72b-f1fa-4973-a323-c36861cf59ee
HA role: Active
Local state: Up
Tracker state: Up
Destination Data Center: 52.42.220.205
Tunnel type: IPSEC
Provider name: Cisco Secure Access

Tunnel name : Tunnel15000002
Site id: 2678135102
Tunnel id: 617865691
SSE tunnel name: C8K-63a9b72b-f1fa-4973-a323-c36861cf59ee
HA role: Backup
Local state: Up
Tracker state: Up
Destination Data Center: 44.241.136.173
Tunnel type: IPSEC
Provider name: Cisco Secure Access



****************************************
   TUNNEL DB ALL
****************************************

 Tun:Tunnel15000001 Instance:Cisco-Secure-Access (Id:2)
 Tun:Tunnel15000002 Instance:Cisco-Secure-Access (Id:2)

****************************************
   SERVICE ROUTE LIST ALL
****************************************
```

# Monitor SIG/SSE tunnels

Use the security operations dashboard to monitor the status and performance of SSE tunnels.

**Step 1** From the Cisco SD-WAN Manager menu, choose **Monitor** > **Security**.

The **SIG/SSE Tunnel Status** pane shows tunnel information using a donut chart:

- Total number of SIG/SSE tunnels that are configured.
- The number of SIG/SSE tunnels that are up and down.
- The number of SIG/SSE tunnels that are in a degraded state.

**Note** Degraded state indicates that the SIG tunnel is up but the Layer 7 health of the tunnel as detected by the tracker does not meet the configured SLA parameters. Traffic is not routed through the tunnel.

**Step 2** (Optional) Click a section of the donut chart to view detailed information about tunnels having a particular status.

Cisco SD-WAN Manager displays detailed information about the tunnels in the **SIG/SSE Tunnels** dashboard.

**Step 3** (Optional) Click **All SIG/SSE Tunnels** to view the **SIG/SSE Tunnels** dashboard.

# Troubleshooting using Cisco SD-WAN Manager

Follow these steps to view the audit logs:

You can troubleshoot provisioning errors or view the remote tunnel status using the audit logs.

**Step 1** From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Audit Log** .

**Note** Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Audit Log** .

Cisco SD-WAN Manager displays a log of activities both in table and graphical format.

**Step 2** Click **Filter** and choose one or more modules to filter the view.

You can choose more than one **Module** type.

**Step 3** To export data for all audit logs to a file in CSV format, click **Export** .

Cisco SD-WAN Manager downloads all data from the audit logs table to an Excel file to a CSV format. The file is downloaded to your browser's default download location and is named Audit_Logs.csv.

**Step 4** To view detailed information about any audit log, for the desired row in the table, click **...** and choose **Audit Log Details** .

The **Audit Log Details** dialog box opens, displaying details of the audit log.

**Step 5** To view configuration changes made to a **Template** type **Module** , for the desired row in the table, click **...** adjacent to a log row for a template module, and choose **Config Diff** .

The **Config Difference** pane displays a side-by-side view of the differences between the configuration that was originally in the template and the changes made to the configuration. To view the changes inline, click **Inline Diff** .

**Note** You can view changes to previous and current configurations made only where the module type is template.

**Step 6** To view the updated configuration on the device, click **Configuration** .

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco SD-WAN Release 20.6.1 , for template and policy configuration changes, the **Audit Logs** option displays the action performed. To view the previous and current configuration for any action, click **Audit Log Details**. Audit logs are collected when you create, update, or delete device or feature templates, and localized or centralized, and security policies. Audit logs shows the changes in API payloads when templates or policies are attached or not attached.