

Integrate Your Devices with Secure Service Edge

Table 1: Feature History

Feature	Release Information	Description
Cisco Secure Access Integration	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a 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). This feature supports Cisco Secure Access integration through policy groups in Cisco SD-WAN Manager.
Zscaler Integration	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature adds Zscaler integration with Cisco Catalyst SD-WAN as part of a simplified Security Service Edge (SSE) automation solution. You can provision both IPSec and GRE tunnels to Scaler using policy groups in Cisco SD-WAN Manager.
Zscaler Sub-Locations	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	With this feature you can configure one or more Zscaler sub-locations for a given location.

- Information About Cisco Secure Access Integration, on page 2
- Information About Zscaler Integration, on page 2
- Restrictions for Cisco Secure Access Integration, on page 3
- Configure Tunnels to Cisco Secure Access or Zscaler Using Cisco SD-WAN Manager, on page 3
- Monitor Security Service Edge Tunnels using CLI, on page 6
- Monitor SIG/SSE Tunnels, on page 8
- Troubleshooting Using Cisco SD-WAN Manager, on page 11

Information About Cisco Secure Access Integration

Cisco Secure Access is a cloud-based platform that provides multiple levels of defense against internet-based threats. From Cisco Catalyst SD-WAN Manager Release 20.13.1 Cisco Secure Access is integrated with Cisco Catalyst SD-WAN.

To configure Secure Service Edge (SSE), choose 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 setup IPSec tunnels. For more information on network tunnel groups, see Manage Network Tunnel Groups.

Information About Zscaler Integration

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

You can integrate Cisco Catalyst SD-WAN edge devices with Zscaler by provisioning automatic IPsec or GRE tunnels between the edge devices and the Security Service Edge (SSE) solution. Zscaler Internet Access (ZIA) inspects and secures traffic from Cisco Catalyst SD-WAN devices. The Cisco SD-WAN Manager uses Zscaler APIs to create the IPSec or GRE tunnels.

In the Zscaler integration the data center selection is based on the public IP address of the device. In the SSE configurations in Cisco SD-WAN Manager, if you enable the **Country** flag, the Zscaler APIs calls return the closest data centers within the country of the device. If there are no data centers in the country, Cisco SD-WAN Manager reports an error.

Information About Zscaler Sub-Locations

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Manager Release 20.15.1

For a given Zscaler location, Cisco SD-WAN Manager supports one or more Zscaler sub-locations and their corresponding subnets. Using the IP addresses encapsulated within a GRE or IPSec tunnel of the sublocations, you can create new locations.

When you add a sub-location in Cisco SD-WAN Manager, the service automatically creates a default **Other** sub-location. You cannot rename the **Other** sub-location. The **Other** sub-location includes IP addresses that aren't already defined in any other sub-location.

Bandwidth Control

With the bandwidth control functionality, you can control bandwidth usage between a location and its sub-locations. You can provide a different bandwidth for sub-locations or use the parent locations settings. You can specify the upload and download bandwidths while creating a location. Any unused bandwidth from sub-locations remain available to the parent location.

Restrictions for Cisco Secure Access Integration

- Cisco SD-WAN Manager does not support API throttling to Cisco Secure Access.
- This feature cannot be configured through a CLI template. This feature can be configured using policy groups on Cisco SD-WAN Manager.
- 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.
- 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.
- 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.
- When the provider and tunnel type are changed or updated, perform the change in two separate deployment steps:
  1. Delete the existing provider or tunnel type template or config group feature and deploy that removal.
  2. Add the new provider or tunnel type configurations and deploy the new provider or tunnel type in a separate subsequent deployment.

Restrictions for Zscaler Sub-Locations

- IP Addresses

  The sub-locations cannot have overlapping IP addresses within a location.

  The Sub-locations should support an individual IP address or a range of IP addresses. For example 10.0.0.2-10.0.0.25.

- Name

  The sub-location name should be unique.

Configure Tunnels to Cisco Secure Access or Zscaler Using Cisco SD-WAN Manager

Workflow for Cisco Secure Access or Zscaler Integration with Cisco Catalyst SD-WAN

Before You Begin

- 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 or Zscaler.
- Add, modify or delete Zscaler sub-locations only from Cisco SD-WAN Manager and not from Zscaler portal. This ensures that the sub-location configurations between Cisco SD-WAN Manager and Zscaler are in sync.

Workflow for Cisco Secure Access or Zscaler Integration with Cisco Catalyst SD-WAN:

1. Create Cisco Secure Access or Zscaler credentials on the **Administrator** > **Settings** page.
2. Create automatic tunnels to Cisco Secure Access or Zscaler using **Configuration** > **Policy Groups**.
3. Redirect traffic to Cisco Secure Access or Zscaler using service routes or policy groups.

Create Cisco Secure Access Credentials

Ensure that 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. We recommend that you 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.

1. From **Configuration** > **Policy Groups** > **Add Secure Service Edge (SSE)** in Cisco SD-WAN Manager, select Cisco Secure Access as the provider.
2. 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. 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.

   Click **Add**.

Create Zscaler Credentials

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups**.
2. Click **Add Secure Service Edge (SSE)** and select **Zscaler** as the provider.
3. Add the Zscaler credentials.
   a. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

b. Click **Click here to add Zscaler Credentials** to create the Zscaler credentials.

c. Enter the following information:

Table 2: Zscaler Credentials

Field	Description
Organization ID	Name of the organization in Zscaler cloud. For more information, see *ZIA Help > Getting Started > Admin Portal > About the Company Profile*.
Partner base URI	This is the base URI that Cisco SD-WAN Manager uses in REST API calls. To find this information on the Zscaler portal, see *ZIA Help > ZIA API > API Developer & Reference Guide > Getting Started*.
Partner API key	Partner API key. To find the key in Zscaler, see *ZIA Help > Partner Integrations > Managing SD-WAN Partner Keys*.
Username	Username of the Cisco Catalyst SD-WAN partner account.
Password	Password of the Cisco Catalyst SD-WAN partner account.

d. Click **Add**.

Create Tunnels to Cisco Secure Access or Zscaler Using Policy Groups

You can create automatic tunnels to Cisco Secure Access or Zscaler using **Configuration > Policy Groups > Secure Service Edge**. For more information see, Configure Secure Service Edge.

When ...	Then for Cisco Secure Access ...	And for Zscaler ...
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.	If the location is not deleted, you must search for the given location in Zscaler and delete it.

Redirect Traffic to Cisco Secure Access or Zscaler

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

- Using policy groups:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **Application Priority & SLA**.

2. 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*.

- Using service route:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups** > **Service Profile**.
2. 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 Configuration Guide*.

Monitor Security Service Edge Tunnels using CLI

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
****************************************
```

To view information about the GRE tunnels configured using Zscaler SSE provider on a Cisco Catalyst SD-WAN device, use the **show sse all** command.

```
Device# show sse all

**************************************
   SSE  Instance zScaler
**************************************
Tunnel name : Tunnel16000512
Site id: 2447182820
Tunnel id: 1299582
SSE tunnel name: site2447182820sys172x16x255x15Tunnel16000512
HA role: Active
Local state: Up
Tracker state: Up
Destination Data Center: 165.225.50.20
Tunnel type: GRE
Provider name: zScaler
Context sharing:  NA

Tunnel name : Tunnel16000513
Site id: 2447182820
Tunnel id: 1299582
SSE tunnel name: site2447182820sys172x16x255x15Tunnel16000513
HA role: Backup
Local state: Up
Tracker state: Up
Destination Data Center: 104.129.198.174

Tunnel type: GRE
Provider name: zScaler
Context sharing:  NA



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

 Tun:Tunnel16000512 Instance:zScaler (Id:2)
 Tun:Tunnel16000513 Instance:zScaler (Id:2)
```

To view information about the IPsec tunnels configured using Zscaler SSE provider on a Cisco Catalyst SD-WAN device, use the **show sse all** command.

```
Device# show sse all

**************************************
   SSE  Instance zScaler
**************************************

Tunnel name : Tunnel16000001
Site id: 2480190864
Tunnel id: 101989981
SSE tunnel name: site2480190864sys172x16x255x15Tunnel16000001
HA role: Active
Local state: Up
Tracker state: Up
Destination Data Center: 165.225.242.40
Tunnel type: IPSEC
```

```
Provider name: zScaler
Context sharing:  NA

Tunnel name : Tunnel16000002
Site id: 2480190864
Tunnel id: 101990028
SSE tunnel name: site2480190864sys172x16x255x15Tunnel16000002
HA role: Backup
Local state: Up
Tracker state: Up
Destination Data Center: 104.129.198.179
Tunnel type: IPSEC
Provider name: zScaler
Context sharing:  NA



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

 Tun:Tunnel16000001 Instance:zScaler (Id:2)
 Tun:Tunnel16000002 Instance:zScaler (Id:2)

****************************************
   SERVICE ROUTE LIST ALL
****************************************
Service Route    : 0.0.0.0/0 vrf_name:2
sse_list:
 Name:global

Service Route    : 0.0.0.0/0 vrf_name:3
sse_list:
 Name:global

Service Route    : 10.0.0.2/32 vrf_name:65528
sse_list:
 Name:zScaler

Service Route    : 0.0.0.0/0 vrf_name:1
sse_list:
 Name:zScaler
```

Monitor SIG/SSE Tunnels

Minimum supported releases for SIG: Cisco IOS XE Release 17.9.1a and Cisco vManage 20.9.1

Minimum supported releases for SSE: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1

Monitor the status of automatic SIG/SSE tunnels using the following Cisco SD-WAN Manager GUI components:

- **SIG/SSE Tunnel Status** pane on the **Monitor** > **Security** page
- **SIG/SSE Tunnels** dashboard on the **Monitor** > **Tunnels** page

SIG/SSE Tunnel Status

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

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

- total number of SIG/SSE tunnels that are configured
- the number of SIG/SSE tunnels that are up
- the number of SIG/SSE tunnels that are down
- the number of SIG/SSE tunnels that are in a degraded state (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. Therefore, the traffic is not routed through the tunnel.)

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.

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

SIG/SSE Tunnels Dashboard

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Tunnels**.
2. Click **SIG/SSE Tunnels**.

   Cisco SD-WAN Manager displays a table that provides the following details about each automatic tunnel created to a Cisco Umbrella, Zscaler SIG or Cisco Secure Access:

Field	Description
Host Name	Host name of the Cisco IOS XE Catalyst SD-WAN device or edge device.
Site ID	ID of the site where the WAN edge device is deployed.
Tunnel ID	Unique ID for the tunnel defined by the SIG/SSE provider.
Transport Type	IPSec or GRE
Tunnel Name	Unique name for the tunnel that can be used to identify the tunnel at both the local and remote ends. On the SIG provider portal, you can use the tunnel name to find details about a particular tunnel.
HA Pair	Active or Backup
Provider	Cisco Umbrella or Zscaler or Cisco Secure Access

Field	Description
Destination Data Center	SIG/SSE provider data center to which the tunnel is connected. **Note** This feature is supported for Cisco Umbrella SIG endpoints and it is yet to be supported for Zscaler ZIA Public Service Edges.
Tunnel Status (Local)	Tunnel status as perceived by the device.
Tunnel Status (Remote)	Tunnel status as perceived by the SIG/SSE endpoint. **Note** This feature is supported for Cisco Umbrella SIG endpoints and it is yet to be supported for Zscaler ZIA Public Service Edges.
Events	Number of events related to the tunnel set up, interface state change, and tracker notifications. Click on the number to display an Events slide-in pane. The slide-in pane lists all the relevant events for the particular tunnel. **Note** If you delete an automatic SIG tunnel from a GRE or IPSec interface and later configure an automatic SIG tunnel from the same interface, the newly configured SIG tunnel has the same name as the tunnel that you deleted earlier. As a result, when you configure the new tunnel, you may see SIG-tunnel-related events that were historically reported for the tunnel that was deleted earlier, if these events are not yet purged. Before deleting a tunnel using a CLI template, remove any static route pointing to the tunnel. Add the static route after creating the tunnel again.
Tracker	Enabled or disabled during tunnel configuration.

3. (Optional) By default, the table displays information for the past 24 hours. To modify the time period, hover the mouse pointer over **24 Hours** and choose a desired time period from the drop-down list.
4. (Optional) To download a CSV file containing the table data, click **Export**.

   The file is downloaded to your browser's default download location.
5. (Optional) Hide or display table columns: Click on the gear icon adjacent to **Export** to display the **Table Settings** slide-in pane. Toggle the columns that you wish to display or hide and click **Apply**.

Troubleshooting Using Cisco SD-WAN Manager

You can troubleshoot provisioning errors or view the remote tunnel status using the audit logs. For more information, see View Audit Log Information.