Integrate Your Devices with Secure Service Edge

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.

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.

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.

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 is not reflected in Cisco SD-WAN Manager.

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

Workflow for Cisco Secure Access 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.

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

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

Create Cisco Secure Access Credentials

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 Tunnels to Cisco Secure Access Using Policy Groups

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

Redirect Traffic to Cisco Secure Access

You can redirect traffic to a Cisco Secure Access 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
****************************************
```

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
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.

Field	Description
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.
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**.