Revised: July 2, 2026

Zscaler for Cisco Catalyst SD-WAN Devices

Feature history for Zscaler integration

Table 1: Feature history

Feature	Release information	Description
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.

What is Zscaler integration

A Cisco Catalyst SD-WAN and Zscaler integration is a security solution that

- provisions automatic IPsec or GRE tunnels between edge devices and the Zscaler Security Service Edge (SSE) solution,
- uses Zscaler Internet Access (ZIA) to inspect and secure traffic from Cisco Catalyst SD-WAN devices, and
- utilizes Zscaler APIs to automate the creation of IPSec or GRE tunnels.

Zscaler data center selection

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.

Zscaler sub-locations

A Zscaler sub-location configuration is a Cisco SD-WAN Manager capability that

- supports one or more Zscaler sub-locations and their corresponding subnets for a given Zscaler location, and
- uses the IP addresses encapsulated within a GRE or IPSec tunnel of the sub-locations to create new locations.

Bandwidth control settings

Bandwidth control allows you to manage bandwidth usage between a location and its sub-locations.

- You can provide different bandwidth for sub-locations or use the parent location's settings.

- Upload and download bandwidths can be specified while creating a location.
- Any unused bandwidth from sub-locations remains available to the parent location.

Restrictions for Zscaler sub-locations

IP address restrictions

The sub-locations cannot have overlapping IP addresses within a location. Each sub-location must support an individual IP address or a range of IP addresses, such as 10.0.0.2-10.0.0.25.

Name restrictions

The sub-location name should be unique within the location.

Workflow to set up Zscaler

Follow these steps to integrate Zscaler 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 Zscaler.

Step 1 Create Zscaler credentials on the **Administrator** > **Settings** page.

Step 2 Create automatic tunnels to Zscaler using **Configuration** > **Policy Groups**.

Step 3 Redirect traffic to Zscaler using service routes or policy groups.

Create Zscaler credentials

Follow these steps to create Zscaler credentials:

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups**.

Step 2 Click **Add Secure Service Edge (SSE)** and select **Zscaler** as the provider.

Step 3 Add the Zscaler credentials as follows:

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 Zscaler using policy groups

Follow these steps to create tunnels to Zscaler using policy groups:

Table 3: Actions for tunnel deletion in Cisco Secure Access

When ...	Then for Zscaler ...	
The deletion is initiated from Cisco SD-WAN Manager , the SSE Tunnel is not removed from the SSE dashboard.	If the location is not deleted, you must search for the given location in Zscaler and delete it.	

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 4: 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. Default: service.sig.umbrella.com

Field	Description
Threshold	Enter the wait time for the probe to return a response before declaring that the configured endpoint is down. Range: 100 to 1000 milliseconds Default: 300 milliseconds
Probe Interval	Enter the time interval between probes to determine the status of the configured endpoint. Range: 20 to 600 seconds Default: 60 seconds
Multiplier	Enter the number of times to resend probes before determining that a tunnel is up or down. Range: 1 to 10 Default: 3

Step 3 Configure tunnel parameters.

Table 5: Basic Settings

Field	Description
Tunnel Type	• Cisco Secure Access: (Read only) **ipsec** • (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) Public IP address of the tunnel source interface that is required to create the GRE tunnel to Zscaler. Default: Auto. 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.

Field	Description
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)	
Shutdown	Click the radio button to enable this option. Default: Disabled
Enable Tracker	Click the radio button to enable this option.
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 to 2000 bytes 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. Range: 500 to 1460 bytes Default: None
DPD Interval	Specify the interval for Internet Key Exchange (IKE) to send Hello packets on the connection. Range: 10 to 3600 seconds 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. 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. Range: 2 to 60 seconds Default: 3
IKE	
IKE Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 to 1209600 seconds (1 hour to 14 days) Default: 14400 seconds

Field	Description
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Choose one of the following: • AES 256 CBC SHA1 • AES 256 CBC SHA2 • AES 128 CBC SHA1 • AES 128 CBC SHA2 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. Range: 3600 to 1209600 seconds (1 hour to 14 days) Default: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. Options: 64, 128, 256, 512, 1024, 2048, or 4096 packets. Default: 512
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Options: • AES 256 CBC SHA1 • AES 256 CBC SHA 384 • AES 256 CBC SHA 256 • AES 256 CBC SHA 512 • AES 256 GCM 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: • Group-2 1024-bit modulus • Group-14 2048-bit modulus • Group-15 3072-bit modulus • Group-16 4096-bit modulus • 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 6: 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. 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. 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. To omit designating a back-up tunnel, choose **None**.

Field	Description
Backup Interface Weight	Enter weight (weight range 1 to 255) for load balancing. 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. 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 Configure advanced settings.

Field	Description
Primary Datacenter	Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. To route traffic to a specific Zscaler data center, choose the data center from the drop-down list.
Secondary Datacenter	Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. To route traffic to a specific Zscaler data center, choose the data center from the drop-down list.

Table 7: Zscaler location

Field	Description
Zscaler Location	Enter the name of a location that is configured on the ZIA Admin Portal. If you do not enter a location name, the Zscaler service detects the location based on the received traffic. From Cisco Catalyst SD-WAN Manager Release 20.18.1, enter unique location name for primary and secondary routers. For more information about locations, see *ZIA Help > Traffic Forwarding > Location Management > About Locations*.
Country	You can enable or disable this option only if either primary or secondary data center is set to Auto. When you choose Auto, the data center selected is within the country of the device.

Table 8: Gateway options

Field	Description
Authentication Required	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. Default: Off
Enable Caution	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. Default: Off
Enable AUP	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. Default: Off
XFF Forwarding	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. Default: Off
Enable IPS Control	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. Default: Off
Enable Firewall	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. Default: Off

Table 9: Bandwidth control

Field	Description
Enforce Bandwidth Control	Enable to enforce bandwidth control on the location. • **Download (Mbps)**: Specify the maximum bandwidth limits for download. • **Upload (Mbps)**: Specify the maximum bandwidth limits for upload. For more information about locations, see *ZIA Help > Traffic Forwarding > Location Management > About Locations*.

Table 10: Sub-locations

Field	Description
Name	Enter a name for the sub-location.

Field	Description
Service VPN	Select a service VPN from the drop-down menu.
IP Address	Enter an IP address or a range of IP addresses for the service VPN.
Authentication Required	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. Default: Off
Enable Caution	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. Default: Off
Enable AUP	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. Default: Off
XFF Forwarding	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. Default: Off
Enable IPS Control	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. Default: Off
Enable Firewall	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. Default: Off
Enforce Bandwidth Control	Choose one of the following: • **Location Bandwidth**: Uses bandwidth of the parent location on the sub-location. The download and upload maximum bandwidth limits are the same as specified for the parent location. A percentage of the parent location bandwidth is allocated to the sub-location based on the allocations of other sub-locations. For more information, see *Secure Internet and SaaS Access (ZIA) Help > Traffic Forwarding > Location Management > Configuring Sub-Locations*. • **Override**: Overrides the bandwidth of the parent location. Specify the maximum bandwidth limits for **Download (Mbps)** and **Upload (Mbps)**. This bandwidth is dedicated to the sub-location and not shared with other sub-locations. • **Disable**: Disables the sub-location traffic from any bandwidth management

Step 7 Click **Add**.

Redirect traffic to Zscaler

Follow these steps to redirect traffic to Zscaler:

You can redirect traffic to Zscaler in two ways:

Option	Description
Redirect traffic using policy groups	• From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **Application Priority & SLA**. • 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**. • 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 Zscaler

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

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

Follow these steps to monitor SIG/SSE tunnels:

Before you begin

Ensure that your deployment meets the minimum supported release requirements for SIG or SSE as applicable.

Step 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.)

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.

Step 4 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Tunnels**.

Step 5 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.

Field	Description
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.
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.

Step 6 (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.

Step 7 (Optional) To download a CSV file containing the table data, click **Export**.

The file is downloaded to your browser's default download location.

Step 8 (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

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.