Integrate Your Devices With Secure Internet Gateways

Table 1: Feature History

Feature	Release Information	Description
IPSEC/GRE Tunnel Routing and Load-Balancing Using ECMP	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	This feature allows you to use the SIG template to steer application traffic to Cisco Umbrella or a Third party SIG Provider. The application traffic is steered to a SIG based on a defined data policy and other match criteria. This feature also allows you to configure weights for multiple GRE/IPSEC tunnels for distribution of traffic among multiple tunnels. The traffic distribution enables you to balance the load among the tunnels. You can also configure the weights to achieve Equal-cost multi-path (ECMP) routing.
Support for Zscaler Automatic IPSec Tunnel Provisioning	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature automates the provisioning of tunnels from Cisco Catalyst SD-WAN routers to Zscaler. Using your Zscaler partner API credentials, you can automatically provisions tunnels to Zscaler Internet Access (ZIA) Public Service Edges. You can choose **Zscaler** in the Cisco Security Internet Gateway (SIG) and SIG credentials feature templates to automate tunnel provisioning.

Feature	Release Information	Description
SIG Integration Improvements	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	

Feature	Release Information	Description
		Source-Only Load Sharing: When you configure two or more active tunnels to a Secure Internet Gateway (SIG), different traffic flows from the same source IP address, with different destination public IP addresses, may be mapped to use different tunnels. With this feature, you can configure all traffic flows from a particular source IP address, irrespective of the destination IP address, to be routed to the SIG through only one of the active tunnels. **IPSec Tunnel Creation Improvements in an Active-Active Setup**: This feature ensures that when you provision an IPSec tunnel, the control and data traffic are sent through the same the physical interface toward the SIG endpoint. Pinning the control and data packets to the same physical interface removes a limitation that exists in previous releases. In previous releases, in certain situations, the control and data packets may be routed to the SIG endpoint through different physical interfaces. When the packets are routed in this way, one of the following scenarios occurs: • If the source is a physical interface, tunnel creation fails because the source IP address of the negotiation packets differs from the source IP address of the keepalive control packet. • If the source is a loopback interface, the source IP address of the data packets differs from the source IP address of the IPSec SA negotiated through the control packets. This difference causes the SIG endpoint to

Feature	Release Information	Description
		drop the data packets.
Layer 7 Health Check for Manual Tunnels	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	You can create and attach trackers to manually created GRE or IPSec tunnels to a SIG endpoint. Trackers help failover traffic when a SIG tunnel is down.
Automatic GRE Tunnels to Zscaler	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	With this feature, use the Secure Internet Gateway (SIG) feature template to provision automatic GRE tunnels to Zscaler SIGs. In earlier releases, the SIG template only supported the provisioning of automatic IPSec tunnels to Zscaler SIGs.
Global SIG Credentials Template	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	With this feature, create a single global Cisco SIG Credentials template for each SIG provider (Cisco Umbrella or Zscaler). When you attach a Cisco SIG template to a device template, Cisco SD-WAN Manager automatically attaches the applicable global Cisco SIG Credentials template to the device template.
Monitor Automatic SIG Tunnel Status and Events	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	Monitor security events related to automatic SIG tunnels using the **Security Events** pane on the **Monitor** > **Security** page, and the **Events** dashboard on the **Monitor** > **Logs** page. Monitor automatic SIG tunnel status using the **SIG Tunnel Status** pane on the **Monitor** > **Security** page, and the **SIG Tunnels** dashboard on the **Monitor** > **Tunnels** page.

Feature	Release Information	Description
Configure SIG Tunnels in a Security Feature Profile	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	With this feature, create a Security feature profile and associate it with one or more configuration groups. In the Security feature profile, configure the Secure Internet Gateway feature to create automatic or manual SIG tunnels. After configuring the feature, deploy the configuration group on the desired WAN edge devices to create SIG tunnels from the devices to the configured SIG endpoints.
Cisco Umbrella Multi-Org Support	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature supports management of multiple organizations through a single parent organization. With this feature, Cisco Catalyst SD-WAN Umbrella for SIG support security policy requirements for different regions of the SD-WAN network.
SLA Profile Support for Layer 7 Health Check	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	This feature uses jitter and packet loss, in addition to latency in SLA metrics to determine the health of the tunnel.
Share Traffic Information with Cisco Security Service Edge	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	Cisco SD-WAN Manager can share VPN and security group tag (SGT) information with Cisco Security Service Edge (SSE). This is called context information. SSE can apply different policies to traffic based on the context information of the traffic.

Cisco Catalyst SD-WAN edge devices support SD-WAN, routing, security, and other LAN access features that can be managed centrally. On high-end devices, you can enable all these features while providing the scale and performance required by large enterprises. However, on lower-end devices, enabling all the security features simultaneously can degrade performance. To avoid the performance degradation, integrate lower-end devices with Secure Internet Gateways (SIG) that do most of the processing to secure enterprise traffic. When you integrate a Cisco Catalyst SD-WAN edge device with a SIG, all client internet traffic, based on routing or policy, is forwarded to the SIG. In addition, the SIG can also protect roaming users, mobile users, and BYOD users. The Multi-security association (SA) Virtual Tunnel Interface (VTI) is not supported on Cisco Catalyst SD-WAN devices.

- Options to Integrate Your Devices with Secure Internet Gateways, on page 6
- Restrictions for Devices With Secure Internet Gateways , on page 12
- Configure Tunnels, on page 12
- Configure SIG Tunnels in a Security Feature Profile, on page 46

Options to Integrate Your Devices with Secure Internet Gateways

To integrate Cisco Catalyst SD-WAN edge devices with a SIG, you can use:

- Automatic tunnels
- Manual tunnels

Automatic Tunnels

Using the Cisco Secure Internet Gateway (SIG) feature template, you can provision automatic IPSec tunnels to Cisco Umbrella SIGs, or automatic IPSec or GRE tunnels to Zscaler SIGs.

Provision an automatic tunnel as follows:

1. Complete the following prerequisites for the SIG:
   a. Specify the address of one or more DNS servers.
   b. Enable the DNS lookup feature by using the **ip domain lookup** command on the Cisco IOS XE Catalyst SD-WAN device. For more information, see ip domain lookup.
   c. Ping the configured DNS name server. The DNS must be reachable using the VRF 65528.
   d. Automatic SIG tunnels use the first NAT outside WAN interface to connect to Umbrella or Zscaler. The DNS and the internet must be accessible through the same interface.
2. Specify Cisco Umbrella or Zscaler credentials using the Cisco SIG Credentials feature template.
3. Specify the details for the tunnel to the SIGs using the Cisco Security Internet Gateway (SIG) feature template.

   In the template, define the parameters for the tunnels such as the interface name, the source interface, the SIG provider, and so on.
4. Edit the Cisco VPN feature template that provides the service route for the devices to the internet. Add a service route to the SIG in the Cisco VPN feature template.
5. Add feature templates to the device templates of the devices that should route traffic to the SIG.
6. Attach the device templates to the devices.

When you attach the device template, the device sets up tunnels to the SIGs and redirects traffic to it.

Note When a SIG Zscaler template is removed from a device template, the corresponding tunnel entry sometimes fails to be deleted from Zscaler's cloud services. As a result, attempting to establish a new tunnel may result in a DUPLICATE_ITEM error due to the presence of the existing entry. To resolve this issue, manually delete the stale tunnel entry from the Zscaler cloud whenever the SIG template is removed from a device template.

Cisco Umbrella Integration

From Cisco IOS XE Catalyst SD-WAN Release 17.2.1r and Cisco vManage Release 20.2.1, use Cisco Umbrella as a SIG by choosing Umbrella as the SIG provider in the Cisco Security Internet Gateway (SIG) feature template, and then define IPSec tunnels, and tunnel parameters. Use the SIG credentials feature template to specify the Umbrella Organization ID, Registration Key, and Secret. For information on configuring automatic tunnelling, see Configure Automatic Tunnels Using Cisco SD-WAN Manager, on page 12.

Cisco Umbrella Multi-Org Support

Minimum releases: Cisco IOS XE Release 17.11.1a and Cisco vManage Release 20.11.1

The Cisco Catalyst SD-WAN Umbrella for SIG support security policy requirements for different sub-regions of their SD-WAN network. This feature is supported for both DNS security policy and SIG templates.

Although Cisco Umbrella's individual dashboards can only support a single domain, the multi-org feature allows you to view and manage multiple domains or logically separate network segments from a particular dashboard. The multi-org setup is suitable for organizations that are highly distributed across different locations where networks are all connected, but where different regions require different security policies. The multi-org feature is also helpful for networks with more than one Active Directory (AD) domain, whether within an AD or logically separate domains.

Zscaler Integration

You can integrate Cisco Catalyst SD-WAN edge devices to Zscaler SIGs by provisioning automatic IPsec or GRE tunnels between the edge devices and the SIGs.

Automatic IPSec Tunnels: From Cisco IOS XE Catalyst SD-WAN Release 17.5.1a and Cisco vManage Release 20.5.1, you can provision automatic IPSec tunnels to Zscaler Internet Access (ZIA) Public Service Edges using the Cisco Security Internet Gateway (SIG) feature template. ZIA Public Service Edges are secure internet gateways that can inspect and secure traffic from Cisco Catalyst SD-WAN devices. The devices use Zscaler APIs to create IPSec tunnels by doing the following:

1. Establish an authenticated session with ZIA.
2. Based on the IP address of the device, obtain a list of nearby data centres.
3. Provision the VPN credentials and location using ZIA APIs.
4. Using the VPN credentials and location, create an IPSec tunnel between the ZIA Public Service Edges and the device.

Automatic GRE Tunnels: From Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and Cisco vManage Release 20.9.1, you can provision automatic GRE tunnels to Zscaler Internet Access (ZIA) Public Service Edges using the Cisco Security Internet Gateway (SIG) feature template. The devices use Zscaler APIs to create the GRE tunnels.

For information on configuring automatic tunnelling, see Configure Automatic Tunnels Using Cisco SD-WAN Manager, on page 12.

Manual Tunnels

You can create a GRE or IPSec tunnel to a third-party SIG or a GRE tunnel to a Zscaler SIG by defining the tunnel properties in the Cisco Secure Internet Gateway (SIG) feature template.

Provision manual tunnels as follows:

1. Specify the details for the tunnel to the SIG by using the Cisco Security Internet Gateway (SIG) feature template.

   In the template, define the parameters for the tunnels such as the interface name, the source interface, the SIG provider, and so on.

2. Edit the Cisco VPN feature template that provides the service route for the devices to the internet. Add a service route to the SIG in the Cisco VPN feature template.

3. Add feature templates to the device templates of the devices that should route traffic to the SIG.

4. Attach the device templates to the devices.

When you attach the device template, the device sets up the defined IPSec or GRE tunnels to the SIG and redirects traffic to it.

Note When a SIG Zscaler template is removed from a device template, the corresponding tunnel entry sometimes fails to be deleted from Zscaler's cloud services. As a result, attempting to establish a new tunnel may result in a DUPLICATE_ITEM error due to the presence of the existing entry. To resolve this issue, manually delete the stale tunnel entry from the Zscaler cloud whenever the SIG template is removed from a device template.

High Availability and Load Balancing

When you connect a Cisco Catalyst SD-WAN edge device to Cisco Umbrella, Zscaler, or a third-party SIG, you can connect the device to a primary data center and a secondary data center. Also, you can provision more than one tunnel to each data center.

Active Tunnels: You can provision up to four IPSec tunnels to the primary data center. These tunnels serve as active tunnels, and when two or more active tunnels are provisioned, the traffic toward the SIG is distributed among these tunnels, increasing the available bandwidth toward the SIG. From Cisco IOS XE Release 17.4.1 and Cisco vManage Release 20.4.1, you can distribute the traffic equally among the active tunnels to achieve an equal-cost multi-path (ECMP) distribution, or assign different weights to the active tunnels so that some tunnels carry more traffic toward the SIG than the others.

Back-up Tunnels: You can provision up to four IPSec tunnels to the secondary data center, one for each active tunnel that you have provisioned to the primary data center. These tunnels to the secondary data center serve as back-up tunnels. When an active tunnel fails, the traffic toward the SIG is sent through the corresponding back-up tunnel. When you provision two or more back-up tunnels, the traffic toward the SIG is distributed among these tunnels, increasing the available bandwidth toward the SIG. From Cisco IOS XE Release 17.4.1 and Cisco vManage Release 20.4.1, you can distribute the traffic equally among the back-up

tunnels to achieve an ECMP distribution, or assign different weights to the back-up tunnels so that some tunnels carry more traffic toward the SIG than the others.

By provisioning two or more active tunnels and distributing the traffic among them, while not provisioning any back-up tunnels, you can create an active-active setup. By provisioning a back-up tunnel for each active tunnel, you can create an active-back-up setup.

Load Sharing Among Tunnels

When you connect a Cisco Catalyst SD-WAN edge device to a SIG and redirect internet-bound traffic to the SIG, any traffic from the branch that is destined for a public IP address passes through the SIG. If you have provisioned more than one tunnel to carry traffic to the SIG, Cisco Express Forwarding (CEF) may map different traffic flows from the same source IP address, and with different public IP address destinations, to different SIG tunnels.

Source-Only Load Sharing: From Cisco IOS XE Release 17.8.1a and Cisco vManage Release 20.8.1, you can configure the traffic from a particular source IP address to be sent to the SIG over only one of the tunnels, irrespective of the destination public IP address. Cisco Express Forwarding (CEF) maps each source IP address to one of the tunnels, distributing traffic from different source IP addresses among the tunnels. For more information, see Configure Source-Only Load Sharing, on page 42.

Note This configuration does not create a sticky mapping between source IP addresses and tunnels to the SIG. If one or more of the tunnels are down, CEF maps source IP addresses to the remaining tunnels. During this mapping, traffic from a particular source IP address may be sent to the SIG over a tunnel that is different from the tunnel that was previously assigned.

Support for Layer 7 Health Check

You can monitor the health of tunnels towards the SIG using trackers attached to the tunnels. These trackers are used to automatically fail over to backup tunnels based on the health of the tunnel.

While creating automatic tunnels, Cisco SD-WAN Manager creates and attaches a default tracker with default values for failover parameters. However, you can also create customized trackers with failover parameter values that suit your SLA requirements.

In the case of manually created tunnels, create and attach the tracker.

Note From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, SIG trackers calculate latency using only the HTTP transaction threshold, rather than the total Round-Trip Time (RTT), which includes TCP, DNS, and HTTP components.

From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, the tracker also uses jitter and packet loss in the calculation of tunnel health.

The following table summarizes tracker support for automatic and manual tunnels:

Tunnel Type	Default Tracker	Customized Tracker
Automatic IPSec Tunnels	Yes	Yes Minimum releases: Cisco IOS XE Release 17.6.2 and Cisco vManage Release 20.6.2
Automatic GRE Tunnels	Yes	Yes Minimum releases: Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1
Manual	No	Yes Minimum releases: Cisco IOS XE Release 17.8.1a and Cisco vManage Release 20.8.1

The tunnel health is monitored as follows:

1. Based on the configuration in the System feature template, Cisco SD-WAN Manager creates a tracker according to the default or customized failover parameters that you define in the SIG template. This tracker uses VPN 65530. Cisco SD-WAN Manager reserves VPN 65530 for tracker VPNs.
2. The tracker resolves the IP address of the SIG service using VPN 0.

   For automatic tunnels to Cisco Umbrella or Zscaler, the tracker uses the following URLs to connect to the SIG:

   - Cisco Umbrella: http://service.sig.umbrella.com
   - Zscaler: http://gateway.*zscaler-cloud-url*/vpntest
3. The device sets up tunnels to the SIG.
4. For each tunnel, the device creates a named TCP socket that it uses to identify the tunnels.
5. The tracker monitors the health of the tunnel using HTTP probes. The tracker calculates the round-trip time (RTT) and compares it to the configured SLA parameters.

   From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, the tracker also uses jitter and packet loss in the calculation of tunnel health.
6. For any tunnels that fail to receive a response within the interval and retransmit timers, or for any tunnels that exceed the latency threshold, the tunnel tracker status is marked down and the VPN routes pointing to this tunnel is marked standby. Crypto IKE stays up for the tunnel but the routes are withdrawn.
7. The device updates the routes for any service VPNs that are connected to the tunnel.

Related Topics

Create Automatic Tunnels Using a Cisco SIG Feature Template, on page 17
Create Manual Tunnels Using Cisco SIG Feature Template, on page 32

Global SIG Credentials Template

Minimum supported release: Cisco vManage Release 20.9.1

In Cisco vManage Release 20.8.x and earlier releases, you must create a Cisco SIG Credentials template for a SIG provider (Cisco Umbrella or Zscaler) for each Cisco IOS XE Catalyst SD-WAN device model that you wish to connect to the SIG.

From Cisco vManage Release 20.9.1, create a single global Cisco SIG Credentials template for a SIG provider (Cisco Umbrella or Zscaler) and attach the template to the required Cisco IOS XE Catalyst SD-WAN device s, irrespective of the device model. When you attach a Cisco SIG feature template that configures automatic SIG tunnels to a device template, Cisco SD-WAN Manager automatically attaches the applicable global SIG Credentials template to the device template.

The Cisco IOS XE Catalyst SD-WAN devices of your organization connect to Cisco Umbrella or Zscaler using a common organization account with the SIG provider. As such, it is beneficial to configure the organization account credentials on the devices through a global template. When you modify the Cisco Umbrella or Zscaler credentials, update only one global template for the modified credentials to take effect on the attached Cisco IOS XE Catalyst SD-WAN devices.

Note After you upgrade Cisco SD-WAN Manager software from Cisco vManage Release 20.8.x or earlier to Cisco vManage Release 20.9.1 or later, the device-model-specific Cisco SIG Credentials templates created in Cisco vManage Release 20.8.x or earlier become read-only. The read-only status allows you to only view the configured credentials. To update the credentials configured in Cisco vManage Release 20.8.x or an earlier release, create a Cisco SIG Credentials template for the SIG provider.

If you try to create or modify a Cisco SIG feature template, Cisco SD-WAN Manager prompts you to create a global Cisco SIG Credentials template for the SIG provider.

Related Topics

Create Cisco Umbrella SIG Credentials Template, on page 13
Create Zscaler SIG Credentials Template, on page 14

Information About Cisco Umbrella Scope Credentials

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

You can generate new Cisco Umbrella credentials, also called as scope credentials, and use the same credentials for both Cisco Umbrella SIG and Cisco Umbrella DNS security configurations. The Cisco Umbrella scope credentials provide flexibility with the ability to customize API keys. You can create multiple API keys with tailored access control for each API key. For more information, see Cisco Umbrella SIG User Guide.

Use the **no use-v2-api** command to continue using legacy credentials while configuring Cisco Umbrella DNS Security.

Upgrade Scenarios

When you ...	And you ...	Then the result is ...
upgrade to Cisco Catalyst SD-WAN Manager Release 20.15.1	• upgrade edge devices to Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, and • configure Cisco Umbrella scope API keys	Cisco SD-WAN Manager automatically discovers and upgrades the Cisco Umbrella DNS and SIG configurations with the Cisco Umbrella scope API credentials.
upgrade to Cisco Catalyst SD-WAN Manager Release 20.15.1	have edge devices in the network running various releases of Cisco IOS XE	Cisco SD-WAN Manager uses both the Cisco Umbrella legacy and scope API credentials for Cisco Umbrella DNS and SIG configurations.

Restrictions for Devices With Secure Internet Gateways

- For Zscaler, GRE tunnel over TLOC extension is not supported.
- In IKEv2 Preshared Keys (PSK), the '\' character is not supported and should not be used.

Configure Tunnels

Configure Automatic Tunnels Using Cisco SD-WAN Manager

Prerequisites

To configure automatic tunneling to a SIG, complete the following requisites:

- Cisco Umbrella: To configure automatic tunnels to Cisco Umbrella, you can do one of the following
  - For Cisco SD-WAN Manager to fetch the API keys, specify Smart Account credentials here: **Administration** > **Settings** > **Smart Account Credentials**. Your Cisco Smart Account is the account that you use to log in to the Cisco Smart Software Manager (CSSM) portal.
  - To manually specify the API keys, generate Umbrella Management API keys. See *Management and Provisioning* > *Getting Started* > *Overview* in the *Cloud Security API* documentation on the Cisco DevNet portal.

    Specify the generated keys in the Cisco SIG Credentials template.

- Zscaler Internet Access (ZIA): To configure automatic tunnels to Zscaler, do the following:
  1. Create partner API keys on the ZIA Partner Integrations page.
  2. Add the Partner Administrator role to the partner API keys.
  3. Create a Partner Administrator.

4. Activate the changes.

For more information, see *Managing SD-WAN Partner Keys* on the Zscaler Help Center.

Specify the generated keys in the Cisco SIG Credentials template.

Create Cisco Umbrella SIG Credentials Template

Minimum supported release: Cisco vManage Release 20.9.1

When you Create Automatic Tunnels Using a Cisco SIG Feature Template, on page 17, on selecting Umbrella as the SIG provider, Cisco SD-WAN Manager prompts you to create the global SIG credentials template, if you haven't yet created the template. Click **Click here to create - Cisco SIG Credentials template** to create the Cisco Umbrella SIG credentials template.

Template Name and **Description** fields are prefilled:

Table 2: Cisco SIG Credentials Template Name and Description

Field	Description
Template Name	(Read only) Umbrella Global Credentials
Description	(Read only) Global credentials for Umbrella

Configure Cisco Umbrella Credentials

1. In the **Basic Details** section, do one of the following:
   - Enable Cisco SD-WAN Manager to fetch credentials from the Cisco Umbrella portal:
     a. Ensure that you have added your Cisco Smart Account credentials here: **Administration** > **Settings** > **Smart Account Credentials**.

        Cisco SD-WAN Manager uses the Cisco Smart Account credentials to connect to the Cisco Umbrella portal.

     b. Click **Get Keys**.

   - Enter Cisco Umbrella credentials:

Field	Description
SIG Provider	(Read only) Umbrella
Organization ID	Enter the Cisco Umbrella parent organization ID for your organization. For more information, see *Find Your Organization ID* in the Cisco Umbrella SIG User Guide.

Field	Description
Registration Key	Enter the Umbrella Management API Key. It is part of DNS security policy under unified security policy. For more information, see *Management and Provisioning* > *Getting Started* > *Overview* in the Cloud Security API documentation on the Cisco DevNet portal.
Secret	Enter the Umbrella Management API Secret.

2. To save the template, click **Save**.

Create Cisco Umbrella Scope Credentials

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Cloud Credentials** and select **Umbrella** as the provider.
3. Enter the following information, which is applicable to both Cisco Umbrella SIG and Cisco Umbrella DNS security:

Field	Description
Organization ID	Enter the Cisco Umbrella organization ID (Org ID) for your organization. For more information, see *Find Your Organization ID* in the *Cisco Umbrella SIG User Guide*.
Scope Credentials	
API Key	Enter the Umbrella management API key.
Secret	Enter the Umbrella management API secret.

4. Click **Save**.

Create Zscaler SIG Credentials Template

Minimum release: Cisco vManage Release 20.9.1

When you Create Automatic Tunnels Using a Cisco SIG Feature Template, on page 17, on selecting Zscaler as the SIG provider, Cisco SD-WAN Manager prompts you to create the global SIG credentials template, if you haven't yet created the template. Click **Click here to create - Cisco SIG Credentials template** to create the Zscaler SIG credentials template.

Template Name and **Description** fields are prefilled:

Table 3: Cisco SIG Credentials Template Name and Description

Field	Description
Template Name	(Read only) Zscaler-Global-Credentials

Field	Description
Description	(Read only) Global credentials for Zscaler

1. In the **Basic Details** section, enter the Zscaler credentials:

   Table 4: Zscaler Credentials

Field	Description
SIG Provider	(Read only) Zscaler
Organization	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*.
Username	Username of the SD-WAN partner account.
Password	Password of the SD-WAN partner account.
Partner API key	Partner API key. To find the key in Zscaler, see *ZIA Help* > *Partner Integrations* > *Managing SD-WAN Partner Keys*.

2. To save the template, click **Save**.

Create Cisco SIG Credentials Template

Applicable releases: Cisco vManage Release 20.8.x and earlier releases.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Click **Add Template**.
4. Choose the device for which you are creating the template.
5. Under **Other Templates**, click **Cisco SIG Credentials**.
6. In the **Template Name** field, enter a name for the feature template.

   This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

7. In the **Description** field, enter a description for the feature template.
8. In **Basic Details** section, do the following:
   a. **SIG Provider**: Click **Umbrella** or **Zscaler**.
   b. For Cisco Umbrella, enter the following registration parameters or click **Get Keys** to have Cisco SD-WAN Manager fetch these parameters from the Cisco Umbrella portal.
      - **Organization ID**
      - **Child Org**
      - **Child Org List**
      - **Registration Key**
      - **Secret**

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can select Child Org ID from the dropdown when a parent Org ID of a multi-org tenant is added to the SIG Credentials.

To fetch the parameters, Cisco SD-WAN Manager uses your Smart Account credentials to connect to the Cisco Umbrella portal. To manually enter the parameters, generate the values in your Umbrella account as described here.

   c. For Zscaler, enter the following details:

Field	Description
Organization	The name of the organization in Zscaler cloud. To find this information in Zscaler, see **Administration** > **Company Profile**.
Child Org	Minimum releases: Cisco IOS XE Release 17.11.1a and Cisco vManage Release 20.11.1 Enter the child organization information in the SIG template.
Child Org List	Minimum releases: Cisco IOS XE Release 17.11.1a and Cisco vManage Release 20.11.1 Select the child org from the **Child Org List** drop-down list.
Partner base URI	This is the Zscaler Cloud API that Cisco SD-WAN Manager uses to connect to Zscaler. To find this information in Zscaler, see **Administration** > **API Key Management**.
Username	Username of the SD-WAN partner account.
Password	Password of the SD-WAN partner account.
Partner API key	The partner API key. To find the key in Zscaler, see **Zscaler Cloud Administration** > **Partner Integrations** > **SD-WAN**.

9. Click **Save**.

Create Automatic Tunnels Using a Cisco SIG Feature Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Click **Add Template**.
4. Choose the device for which you are creating the template.
5. Under **VPN**, click **Cisco Secure Internet Gateway (SIG)**.
6. In the **Template Name** field, enter a name for the feature template.

   This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 to 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
7. In the **Description** field, enter a description for the feature template.
8. (From Cisco vManage Release 20.9.1) **SIG Provider**: Click **Umbrella** or **Zscaler**.

   From Cisco vManage Release 20.9.1, on selecting **Umbrella** or **Zscaler** as the SIG provider, Cisco SD-WAN Manager prompts you to create the corresponding global SIG credentials template if you haven't yet created the template. Click **Click here to create - Cisco SIG Credentials template** to create the Cisco Umbrella or Zscaler SIG credentials template.

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can select Child Org ID from the dropdown when a parent Org ID of a multi-org tenant is added to the SIG Credentials.

9. To create one or more trackers to monitor tunnel health, do the following in the **Tracker** section:

Note From Cisco IOS XE Release 17.6.2 and Cisco vManage Relase 20.6.2 , you can create customized trackers to monitor the health of automatic tunnels. If you do not customize the SLA parameters, Cisco SD-WAN Manager creates a default tracker for the tunnel.

   a. **Source IP Address**: Enter a source IP address for the probe packets.
   b. Click **New Tracker**.
   c. Configure the following:

Table 5: Tracker Parameters

Field	Description
Name	Enter a name for the tracker. The name can be up to 128 alphanumeric characters.

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.
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 the probes are resent before determining that a tunnel is down. **Note** When tunnel status changes continuously within a short period of time, the tunnel goes to the flapping state. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, to avoid flapping of tunnels, the tracker waits for the duration equal to the product of multiplier * interval to declare the status of the tunnel. **Range**: 1 to 10 **Default**: 3
API url of endpoint	Specify the API URL for the SIG endpoint of the tunnel. **Note** The URL value passed to the endpoint-api-url configuration must resolve through DNS to an IPv4 address. Domains which resolve to an IPv6 address are currently not supported for the endpoint-api-url configuration.

d. Click **Add**.

e. To add more trackers, repeat sub-step **b** to sub-step **d**.

10. To create tunnels, do the following in the **Configuration** section:

a. (Cisco 20.8.x and earlier releases) **SIG Provider**: Click **Umbrella** or **Zscaler**.

b. Click **Add Tunnel**.

c. Under **Basic Settings**, configure the following:

Table 6: Basic Settings

Field	Description
Tunnel Type	Click **ipsec** or **gre**. **Note** Automatic GRE tunnels are supported from Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1 and only to Zscaler ZIA.
Interface Name (0..255)	Enter the interface name. **Note** If you have attached the Cisco VPN Interface IPSec feature template to the same device, ensure that the interface number you enter is different from what you have entered in the IPSec template.
Description	Enter a description for the interface.
Tracker	By default, a tracker is attached to monitor the health of automatic tunnels to Cisco Umbrella or Zscaler. If you configured a customized tracker in step **8**, choose the tracker. **Note** From Cisco IOS XE Release 17.6.2 and Cisco vManage Relase 20.6.2, you can create customized trackers to monitor the health of automatic tunnels.

Field	Description

Tunnel Source Interface	Enter the name of the source interface of the tunnel. This interface should be the egress interface and is typically the internet-facing interface.
	
	Note
	From Cisco vManage Release 20.9.1 and later, the selection for this field determines the availability of the **Tunnel Route-via Interface** field:
	
	• Loopback: If a loopback interface name is used, the **Tunnel Route-via Interface** field appears and must be configured to specify the physical egress path.
	
	• Physical/Non-loopback: If a physical interface name is used, the system does not prompt for a **Tunnel Route-via Interface** value. The CLI for the tunnel route-via property is automatically populated with the same interface selected as the tunnel source.
	
	• Device Specific: If set to **Device Specific**, the **Tunnel Route-via Interface** field is displayed and required, as a loopback interface may be assigned at the device level. The value for the **Tunnel Route-via Interface** must be entered on the **Variables** page.
	
	For releases before Cisco IOS XE Catalyst SD-WAN Release 17.13.1aCisco Catalyst SD-WAN Manager Release 20.13.1 and, and you have a Cellular or Dialer interface as the tunnel's source interface, the following workaround must be implemented.
	
	If you use a cellular interface as a tunnel source interface, you must modify your existing tunnel source interface configuration with the following configuration:
	
	`interface <interface name>`
	`no tunnel route-via <Interface> mandatory`
	
	Use the CLI add-on feature template to modify the tunnel configuration on the device. For more information on how to use a CLI add-on feature template, see , Create a CLI Add-On Feature Template.
	
	After you have modified the tunnel configuration, select the device template for which you want to apply the CLI add-on feature template, and push the configuration to the devices. For more information about attaching a device template to one or more devices, see Attach Template to Devices
	
	Note
	A SIG tunnel will be created for cellular interfaces only if a global VRF has only one transport interface. A SIG tunnel is not be created if a global VRF has multiple transport interfaces.

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.
Source Public IP	Minimum supported releases: Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1 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.

d. (Optional) Under **Advanced Options**, configure the following:

Table 7: General

Field	Description
Shutdown	Click **No** to enable the interface; click **Yes** to disable. **Default**: **No**.
Track this interface for SIG	Enable or disable tracker for the tunnel. By default, Cisco SD-WAN Manager enables a tracker for automatic tunnels. **Default**: **On**.
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 IKE to send Hello packets on the connection. **Range**: 10 to 3600 seconds **Default**: 10

Field	Description
DPD Retries	Specify the number of seconds between DPD retry messages if the DPD retry message is missed by the peer. Once 1 DPD message is missed by the peer, the router moves to a more aggressive state and sends the DPD retry message at the faster retry interval, which is the number of seconds between DPD retries if the DPD message is missed by the peer. The default DPD retry message is sent every 2 seconds. Five aggressive DPD retry messages can be missed before the tunnel is marked as down. **Range**: 2 to 60 seconds **Default**: 3

Table 8: IKE

Field Name	Description
IKE Rekey Interval	Specify the interval for refreshing IKE keys. **Range:** 300 to 1209600 seconds (1 hour to 14 days) **Default**: 14400 seconds
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. • 2 1024-bit modulus • 14 2048-bit modulus • 15 3072-bit modulus • 16 4096-bit modulus **Default**: 14 2048-bit modulus

Table 9: IPSEC

Field	Description
IPsec Rekey Interval	Specify the interval for refreshing IPSec keys. **Range**: 300 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, 4096. **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 • NULL SHA1 • NULL SHA 384 • NULL SHA 256 • NULL SHA 512 **Default**: AES 256 GCM
Perfect Forward Secrecy	• Specify the 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. **Default**: None

e. Click **Add**.

f. To create more tunnels, repeat sub-step **b** to sub-step **e**.

11. To designate active and back-up tunnels and distribute traffic among tunnels, configure the following in the **High Availability** section:

Table 10: High Availability

Field	Description
Active	Choose a tunnel that connects to the primary data center.
Active Weight	Enter a 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 active tunnels, where the first tunnel is configured with a 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	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**.
Backup Weight	Enter a 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 a 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.

12. (Optional) Modify the default configuration in the **Advanced Settings** section:

Table 11: Umbrella

Field	Description
Umbrella Primary Data-Center	Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. If you wish to route traffic to a specific Cisco Umbrella data center, choose the data center from the drop-down list.
Umbrella Secondary Data-Center	Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. If you wish to route traffic to a specific Cisco Umbrella data center, choose the data center from the drop-down list.

Table 12: Zscaler

Field	Description
Primary Data-Center	Automatic IPSec tunnels: Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. If you wish to route traffic to a specific Zscaler data center, choose the data center from the drop-down list. Automatic GRE tunnels (Minimum supported releases: Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1): Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. If you wish to route traffic to specific Zscaler data center, ensure that you choose a Zscaler data center that is recommended by Zscaler based on geographical proximity to the device. Obtain the recommend list of Zscaler data centers through a GET API request for `/vips/recommendedList`. In the API request, specify the public IP of your device as the value of the `sourceIp` query parameter. For more information on `/vips/recommendedList`, see *ZIA API Developer & Reference Guide*. If you choose a data center that is not in the recommended list, the Cisco IOS XE Catalyst SD-WAN device reverts to the automatically selected data center.
Secondary Data-Center	Automatic IPSec tunnels: Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. If you wish to route traffic to a specific Zscaler data center, choose the data center from the drop-down list. Automatic GRE tunnels (Minimum supported releases: Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1): Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. If you wish to route traffic to specific Zscaler data center, ensure that you choose a Zscaler data center that is recommended by Zscaler based on geographical proximity to the device. Obtain the recommend list of Zscaler data centers through a GET API request for `/vips/recommendedList`. In the API request, specify the public IP of your device as the value of the `sourceIp` query parameter. For more information on `/vips/recommendedList`, see *ZIA API Developer & Reference Guide*. If you choose a data center that is not in the recommended list, the Cisco IOS XE Catalyst SD-WAN device reverts to the automatically selected data center.

Field	Description
Zscaler Location Name	Minimum supported releases: Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1 (Optional) 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. For more information about locations, see *ZIA Help > Traffic Forwarding > Location Management > About Locations*.
Authentication Required	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 Firewall	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 Caution	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Enable Surrogate IP	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Display Time Unit	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Minute
Idle Time to Disassociation	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: 0
Enforce Surrogate IP for known browsers	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off

Field	Description
Refresh Time Unit	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Minute
Refresh Time	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: 0
Enable AUP	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
First Time AUP Block Internet Access	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Force SSL Inspection	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
AUP Frequency	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: 0

13. Click **Save**.

Create Automatic Tunnels to Cisco Umbrella or Zscaler Using Policy Groups

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1

You can create automatic tunnels to Cisco Umbrella or Zscaler using **Configuration > Policy Groups > Secure Internet Gateway**. For more information see, Configure a Secure Internet Gateway.

Configure Automatic Tunnels Using a CLI Add-On Template

We recommend the use of feature templates to configure automatic tunnels.

Configure a Tracker Using a CLI Add-On Template

For more information about using CLI add-on templates, see CLI Add-On Feature Templates.

Before You Begin

- A default tracker is available if the tunnel is created in Cisco Umbrella or Zscaler. You do not have to configure an endpoint tracker in this scenario.
- You can configure more than one endpoint tracker using the same CLI Add-On template.

Note By default, CLI templates execute commands in global config mode.

1. Configure the tracker name.

   endpoint-tracker *tracker name*

2. Configure the endpoint tracker using an API URL.

   endpoint-api-url *url-address*

3. Set an interval to determine the period between tracker probes.

   interval *interval-value*

4. Set a multiplier value.

   multiplier *multiplier-value*

5. Configure the tracker type.

   tracker-type interface

The following is a sample configuration example for configuring a tracker:

```
endpoint-tracker netflix
 endpoint-api-url http://www.netflix.com
 interval 20
 multiplier 1
 tracker-type interface
endpoint-tracker youtube
 endpoint-api-url http://www.youtube.com
 interval 20
 multiplier 1
 tracker-type interface
```

Configure a Tunnel Using CLI Add-On Template

Note By default, CLI templates execute commands in global config mode.

1. Enter the tunnel interface mode.

   interface Tunnel *interface-number*

2. Configure an IP unnumbered interface.

   ip unnumbered *source-interface-name*

3. Configure the endpoint tracker for tracking the status of an endpoint.

endpoint-tracker *tracker-name*

4. Configure the SLA profile for the tunnel interface.

   endpoint-tracker-sla-profile *profile-name*

5. Set the source address for the tunnel interface.

   tunnel source *source-interface-name*

6. Set the destination address for the tunnel interface.

   tunnel destination *interface-ip-address*

7. Specify the outgoing interface type for the tunnel transport.

   tunnel route-via *interface-type* **mandatory**

8. Enable path MTU discovery on the tunnel interface.

   tunnel path-mtu-discovery

9. Configure **tunnel vrf multiplexing**.

   This configuration allows multiple service VPNs to use the tunnel.

   tunnel vrf multiplexing

The following is a sample configuration example for configuring the tunnel:

```
interface Tunnel601
 ip unnumbered GigabitEthernet1
 endpoint-tracker youtube
 endpoint-tracker-sla-profile sla_mod
 tunnel source GigabitEthernet1
 tunnel destination 10.1.17.14
 tunnel route-via GigabitEthernet1 mandatory
 tunnel path-mtu-discovery
 tunnel vrf multiplexing
```

Note SIG doesnot support outbound traffic. That is, traffic has to be initialed from the service side only, it does not support traffic initiated from the outside side to router service VPN side.

Configure an Endpoint Tracker SLA Profile for Layer 7 Health Check, Using a CLI Add-On Template

Note By default, CLI templates execute commands in global config mode.

1. Configure an SLA profile name.

endpoint-tracker-sla-profile *profile-name*

2. Set the packet loss value as a percentage.

   The value can range from 0-100, with 10 being the default value.

   loss *value*

3. Set the latency value as milliseconds.

   The value can range from 1-10000, with 300 being the default value.

   latency *value*

4. Set the jitter value as milliseconds.

   The value can range from 1-10000, with 20 being the default value.

   jitter *value*

5. Set the SLA mode. You can choose one of the following modes:

   - Aggressive
   - Moderate
   - Conservative

   sla-mode *mode*

Note When SLA profile is configured in a manual tracker, the threshold from the endpoint tracker is used as the timeout value for HTTP probes.

The following is a sample configuration example for configuring an endpoint-tracker SLA profile with an aggressive sla-mode:

```
endpoint-tracker-sla-profile sla_agg
 loss 10
 latency 300
 jitter 80
 sla-mode aggressive
```

Configure a Service Route for SIG Using a CLI Add-On Template

Note By default, CLI templates execute commands in global config mode.

Configure a service route to the SIG Tunnel.

ip sdwan route vrf *vrf-range* **service sig**

The following is a sample configuration for configuring a service route for SIG:

```
ip sdwan route vrf 1 0.0.0.0/0 service sig
```

Configure High Availability Using a CLI Add-On Template

Note By default, CLI templates execute commands in global config mode.

1. Enter the HA pair mode.

   sdwan service sig vrf global
   ha-pairs

2. Define two tunnel interfaces for a high availability configuration.

   interface-pair *active-tunnel* [**active-interface-weight** *active-weight*] *backup-tunnel* [**backup-interface-weight** *backup-weight*]

3. Enter tunnel interface mode for the active tunnel.

   interface *active-tunnel*

4. Configure the tunnel options for the active tunnel.

   tunnel-options tunnel-set secure-internet-gateway-other source-interface *interface-name*

5. Enter tunnel interface mode for the backup tunnel.

   interface *backup-tunnel*

6. Exit tunnel interface mode.

   exit

7. Configure the tunnel options for the backup tunnel.

   tunnel-options tunnel-set secure-internet-gateway-other source-interface *interface-name*

8. Exit tunnel interface mode.

   exit

The following is a sample configuration for configuring high availability:

```
sdwan
 service sig vrf global
  ha-pairs
   interface-pair Tunnel601 active-interface-weight 1 Tunnel602 backup-interface-weight 1
 interface Tunnel601
  tunnel-options tunnel-set secure-internet-gateway-other source-interface GigabitEthernet1

 exit
 interface Tunnel602
  tunnel-options tunnel-set secure-internet-gateway-other source-interface GigabitEthernet2

 exit
```

Create Manual Tunnels Using Cisco SIG Feature Template

From Cisco IOS XE Release 17.4.1 and Cisco vManage Release 20.4.1, all SIG related workflows for automatic and manual tunnels have been consolidated into the Cisco SIG template. If you are using Cisco IOS XE Release 17.4.1 and Cisco vManage Release 20.4.1, or later, use the Cisco SIG template to configure GRE or IPSec tunnels to a third-party SIG, or GRE tunnels to a Zscaler SIG.

For a software release earlier than Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1, see *Configuring a GRE Tunnel or IPsec Tunnel from Cisco SD-WAN Manager.*

Layer 7 Health Check: The option to create trackers and monitor the health of manually created tunnels is available from Cisco IOS XE Release 17.8.1a, Cisco vManage Relase 20.8.1. In earlier releases, the Layer 7 Health Check feature is only available if you use VPN Interface GRE/IPSEC templates, and not with Cisco SIG templates.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Click **Add Template**.
4. Choose the device for which you are creating the template.
5. Under **VPN**, click **Cisco Secure Internet Gateway (SIG)**.
6. In the **Template Name** field, enter a name for the feature template.

   This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 to 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
7. In the **Description** field, enter a description for the feature template.
8. To create one or more trackers to monitor tunnel health, do the following in the Tracker section:

Note The option to create trackers and monitor tunnel health is available from Cisco IOS XE Release 17.8.1a, Cisco vManage Relase 20.8.1.

   a. **Source IP Address**: Enter a source IP address for the probe packets.
   b. (Optional) Click **New Tracker**.
   c. Configure the following:

Field	Description
Name	Enter a name for the tracker. The name can be up to 128 alphanumeric characters.

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
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 down. **Range**: 1 to 10 **Default**: 3
API url of endpoint	Specify the API URL for the SIG endpoint of the tunnel. **Note** Both HTTP and HTTPS API URLs are supported. SIG tunnel tracker configuration only supports HTTP even though the HTTPS option is available.

d. Click **Add**.

e. To add more trackers, repeat sub-step **b** to sub-step **d**.

9. To create tunnels, do the following in the **Configuration** section:

a. **SIG** Provider: Click **Generic**.

Cisco vManage Release 20.4.x and earlier: Click **Third Party**.

b. Click **Add Tunnel**.

c. Under **Basic Settings**, configure the following:

Field	Description
Tunnel Type	Based on the type of tunnel you wish to create, click **ipsec** or **gre**.
Interface Name (0..255)	Enter the interface name. **Note** If you have attached the Cisco VPN Interface IPSec feature template or the Cisco VPN Interface GRE feature template to the same device, ensure that the interface number you enter is different from what you have entered in the IPSec or GRE templates.
Description	(Optional) Enter a description for the interface.

Field	Description
Source Type	Click **INTERFACE**. Cisco IOS XE Catalyst SD-WAN devices, **INTERFACE** is the only supported **Source Type**.
Tracker	(Optional) Choose a tracker to monitor tunnel health. **Note** From Cisco IOS XE Release 17.8.1a and Cisco vManage Relase 20.8.1, you can create trackers to monitor tunnel health.
Track this interface for SIG	Enable or disable tracker for the tunnel. By default, Cisco SD-WAN Manager enables a tracker for automatic tunnels. **Default**: **On**.

Field	Description

Tunnel Source Interface	Enter the name of the source interface of the tunnel. This interface should be the egress interface and is typically the internet-facing interface.
	
	Note
	From Cisco vManage Release 20.9.1 and later, the selection for this field determines the availability of the **Tunnel Route-via Interface** field:
	
	• Loopback: If a loopback interface name is used, the **Tunnel Route-via Interface** field appears and must be configured to specify the physical egress path.
	
	• Physical/Non-loopback: If a physical interface name is used, the system does not prompt for a **Tunnel Route-via Interface** value. The CLI for the tunnel route-via property is automatically populated with the same interface selected as the tunnel source.
	
	• Device Specific: If set to **Device Specific**, the **Tunnel Route-via Interface** field is displayed and required, as a loopback interface may be assigned at the device level. The value for the **Tunnel Route-via Interface** must be entered on the **Variables** page.
	
	For releases before Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1, and you have a Cellular or Dialer interface as the tunnel's source interface, the following workaround must be implemented.
	
	If you use a cellular interface as a tunnel source interface, you must modify your existing tunnel source interface configuration with the following configuration:
	
	`interface <interface name>`
	`no tunnel route-via <Interface> mandatory`
	
	Use the CLI add-on feature template to modify the tunnel configuration on the device. For more information on how to use a CLI add-on feature template, see , Create a CLI Add-On Feature Template.
	
	After you have modified the tunnel configuration, select the device template for which you want to apply the CLI add-on feature template, and push the configuration to the devices. For more information about attaching a device template to one or more devices, see Attach Template to Devices
	
	Note
	A SIG tunnel will be created for cellular interfaces only if a global VRF has only one transport interface. A SIG tunnel is not be created if a global VRF has multiple transport interfaces.

Field	Description
Tunnel Destination IP Address/FQDN	Enter the IP address of the SIG provider endpoint.
Preshared Key	This field is displayed only if you choose **ipsec** as the **Tunnel Type**. Enter the password to use with the preshared key.

d. (Optional) Under **Advanced Options**, configure the following:

Table 13: (Tunnel Type: gre) General

Field	Description
Shutdown	Click **No** to enable the interface; click **Yes** to disable. **Default**: No.
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

Table 14: (Tunnel Type: ipsec) General

Field	Description
Shutdown	Click **No** to enable the interface; click **Yes** to disable. **Default**: No.
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

Field	Description
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. **Range**: 0 to 65535 seconds **Default**: 10
DPD Retries	Specify how many unacknowledged packets to send before declaring an IKE peer to be dead and then removing the tunnel to the peer. **Range**: 0 to 255 **Default**:3

Table 15: (Tunnel Type: ipsec) IKE

Field	Description
IKE Rekey Interval	Specify the interval for refreshing IKE keys **Range:** 300 to 1209600 seconds (1 hour to 14 days) **Default**: 14400 seconds
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. Choose one of the following: • 2 1024-bit modulus • 14 2048-bit modulus • 15 3072-bit modulus • 16 4096-bit modulus **Default**: 16 4096-bit modulus

Field	Description
IKE ID for Local Endpoint	If the remote IKE peer requires a local end point identifier, specify the same. **Range**: 1 to 64 characters **Default**: Tunnel's source IP address
IKE ID for Remote Endpoint	If the remote IKE peer requires a remote end point identifier, specify the same. **Range**: 1 to 64 characters **Default**: Tunnel's destination IP address

Table 16: (Tunnel Type: ipsec) IPSEC

Field	Description
IPsec Rekey Interval	Specify the interval for refreshing IPSec keys. **Range**: 300 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, 4096. **Default**: 512
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Choose one of the following: • AES 256 CBC SHA1 • AES 256 CBC SHA 384 • AES 256 CBC SHA 256 • AES 256 CBC SHA 512 • AES 256 GCM • NULL SHA 384 • NULL SHA 256 • NULL SHA 512 **Default**: NULL SHA 512

Field	Description
Perfect Forward Secrecy	Specify the 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. **Default**: Group-16 4096-bit modulus

e. Click **Add**.

f. To create more tunnels, repeat sub-step **b** to sub-step **e**.

10. To designate active and back-up tunnels and distribute traffic among tunnels, configure the following in the **High Availability** section:

Table 17: High Availability

Field	Description
Active	Choose a tunnel that connects to the primary data center.
Active Weight	Enter a 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 active tunnels, where the first tunnel is configured with a 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	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 Weight	Enter a 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 a 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.

11. Click **Save**.

Redirect Traffic to a SIG

You can redirect traffic to a SIG in two ways:

- Using Data Policy. For more information, see Action Parameters in the Policies Configuration Guide.
- Using the Service route to SIG. For more information, see Modify Service VPN Template, on page 40

Modify Service VPN Template

To ensure that the device connects to the SIG, you must modify the Cisco VPN template to include a service route to the SIG.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. For the Cisco VPN template of the device, click **Edit**.
4. Click **IPv4 Route**.
5. Click the delete icon on any existing IPv4 route to the internet.
6. Click **Service Route**.
7. Click **New Service Route**.
8. Enter a Prefix (for example, 10.0.0.0/8). For Umbrella SIG, use any RFC 1918 subnet for Service IP addresses.
9. For the service route, ensure that **SIG** is chosen.
10. Click **Add**.
11. Click **Update**.

Create Device Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device** .

3. Click **Create Template** and click **From Feature Template**.
4. From the **Device Model** drop-down list, choose the device model for which you are creating the template.

   Cisco SD-WAN Manager displays all the feature templates for that device type. The required feature templates are indicated with an asterisk (*), and the remaining templates are optional. The factory-default template for each feature is chosen by default.
5. From the **Device Role** drop-down list, choose **SDWAN Edge**.
6. In the **Template Name** field, enter a name for the device template.

   This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
7. In the **Description** field, enter a description for the device template.

   This field is mandatory, and it can contain any characters and spaces.
8. Click **Transport & Management VPN**.
9. In the **Transport & Management VPN** section, under **Additional Cisco VPN 0 Templates**, click **Cisco Secure Internet Gateway**.
10. From the **Cisco Secure Internet Gateway** drop-down list, choose the Cisco SIG feature template that you created earlier.
11. Click **Additional Templates**.
12. In the **Additional Templates** section,
    a. Automatic tunneling:

       (Cisco vManage Release 20.8.x and earlier) From the **Cisco SIG Credentials** drop-down list, choose the relevant Cisco SIG Credentials feature template.

       (From Cisco vManage Release 20.9.1) Cisco SD-WAN Manager automatically chooses the applicable global Cisco SIG Credentials feature template based on the Cisco SIG feature template configuration.

Note If there are any changes to the SIG credentials, for these changes to take effect, you must first remove the SIG feature template from the device template and push the device template. Thereafter, re-attach the SIG feature template and then push the template to the device. For information on pushing the device template, see Attach the SIG Template to Devices.

    b. Manual tunneling: No need to attach a **Cisco SIG Credentials** template.

13. Click **Create**.

    The new configuration template is displayed in the **Device Template** table. The **Feature Templates** column shows the number of feature templates that are included in the device template, and the **Type** column shows **Feature** to indicate that the device template was created from a collection of feature templates.

Attach Template to Devices

To attach one or more devices to the device template:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and choose the template that you created.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is called **Device**.

3. For the desired template, click **...** and click **Attach Devices**.

   The Attach Devices dialog box displays.
4. In the **Available Devices** column, choose a group and search for one or more devices, choose a device from the list, or click **Select All**.
5. Click the arrow pointing right to move the device to the **Selected Devices** column.
6. Click **Attach**.
7. If the template contains variables, enter the missing variable values for each device in one of the following ways:
   - Enter the values manually for each device either in the table column or by clicking **...** in the row and clicking **Edit Device Template**. When you are using optional rows, if you do not want to include the parameter for the specific device, do not specify a value.
   - Click **Import File** to upload a CSV file that lists all the variables and defines each variable value for each device.
8. Click **Update**.

Configure Source-Only Load Sharing

Minimum supported releases: Cisco IOS XE Release 17.8.1a and Cisco vManage Release 20.8.1.

Create CLI Add-On Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Click **Add Template**.
4. Under **Select Devices**, choose the devices for which you are creating the template.

5. Under **Select Template**, scroll down to the **OTHER TEMPLATES** section.
6. Click **CLI Add-On Template**.
7. **Template Name**: Enter a name for the feature template.This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
8. **Description**: Enter a description for the device template.

   This field is mandatory, and it can contain any characters and spaces.
9. Under **CLI CONFIGURATION**, enter the following command: **ip cef load-sharing algorithm src-only**
10. Click **Save**.

Add CLI Add-On Template to Device Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration > Templates**.
2. Click **Device Templates**.
3. Find the device template to which you wish to add the CLI add-on feature template.
4. For the device template, click **...** and click **Edit**.
5. Scroll down to **Additional Templates**.
6. From the **CLI Add-On Template** drop-down list, choose the CLI add-on feature template that you created earlier.
7. Click **Update**.

Configuring a GRE Tunnel or IPsec Tunnel from Cisco SD-WAN Manager

Table 18: Feature History

Feature Name	Release Information	Description
Manual Configuration for GRE Tunnels and IPsec Tunnels	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature lets you manually configure a GRE tunnel by using the Cisco VPN Interface GRE template or an IPSec tunnel by using the Cisco VPN Interface IPSec template. For example, use this feature to manually configure a tunnel to a SIG.

Note From Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1, all SIG related workflows for Automatic and Manual Tunnels have been consolidated into the SIG template. If you are using Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1, or later, configure GRE or IPSec tunnels to a generic SIG, or GRE tunnels to a Zscaler SIG, using the SIG template.

Configure a GRE Tunnel from Cisco SD-WAN Manager

This section describes how to manually create a GRE tunnel from Cisco SD-WAN Manager. This procedure lets you configure a GRE tunnel to a third-party vendor.

Note To configure a GRE tunnel from Cisco SD-WAN Manager, use the SIG Feature Template. For more information, see Create Manual Tunnels Using Cisco SIG Feature Template. The Cisco VPN Interface GRE template is no longer used to configure a tunnel to a SIG.

For releases prior to Cisco vManage Release 20.8.1, use the Cisco VPN Interface GRE template.

1. Perform these actions to create a GRE template:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Feature Templates**, and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

   c. Choose the type of device for which you are creating the template.
   d. Choose the Cisco VPN Interface GRE template from the group of VPN templates.
   e. In **Basic Configuration**, configure parameters as desired and then click **Save**.

2. Perform these actions to create a GRE route:
   a. Click **Feature Templates**, and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

   b. Choose the type of device for which you are creating the template.
   c. Choose the Cisco VPN template in the group of VPN templates.
   d. Click **GRE Route**.
   e. Click **New GRE Route**.
   f. Configure parameters as desired, and then click **Add**.

3. Perform these actions to configure a device template for the GRE interface.
   a. Click **Device**, and then click **...**and click **Edit** for the device template that you want to configure.
   b. Click **Transport & Management VPN**.
   c. From the Additional Cisco VPN 0 Templates list, choose the Cisco VPN Interface GRE template.
   d. From the Cisco VPN Interface GRE drop-down menu, click **Create Template**.

e. Configure the templates as desired, and then click **Save**.

Configure an IPsec Tunnel from Cisco SD-WAN Manager

This section describes how to manually create an IPsec tunnel from Cisco SD-WAN Manager. This procedure lets you configure an IPsec tunnel to a third-party vendor.

Note To configure a IPSec tunnel from Cisco SD-WAN Manager, use the SIG Feature Template. For more information, see Create Automatic Tunnels Using Cisco SIG Feature Template. The Cisco VPN Interface IPSec template is no longer used to configure a tunnel to a SIG.

For releases prior to Cisco vManage Release 20.8.1, use the Cisco VPN Interface IPsec template.

1. Perform these actions to create an IPsec template:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Feature Templates**, and click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

   c. Choose the type of device for which you are creating the template.
   d. Choose the Cisco VPN Interface IPsec template from the group of VPN templates.
   e. In **Basic Configuration**, configure parameters as desired,
   f. In **Advanced**, specify a name for your **Tracker**.
   g. Click **Save**.

2. Perform these actions to create an IPSec route:
   a. Click **Feature Templates**, and, click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

   b. Choose the type of device for which you are creating the template.
   c. Choose the Cisco VPN template in the group of VPN templates.
   d. Click **IPSEC Route**.
   e. Click **New IPSEC Route**.
   f. Configure parameters as desired, and then click **Add**.

3. Perform these actions to configure a device template for the IPsec interface.
   a. Click **Device**, and click **…** and choose **Edit** for the device template that you want to configure.

b. Click **Transport & Management VPN**.

c. From the Additional Cisco VPN 0 Templates list, choose the Cisco VPN Interface IPsec template.

d. From the Cisco VPN Interface IPsec drop-down menu, click **Create Template**.

e. Configure the templates as desired, and then click **Save**.

Configure SIG Tunnels in a Security Feature Profile

From Cisco vManage Release 20.10.1 and Cisco IOS XE SD-WAN Release 17.10.1, configure SIG tunnels in a configuration group and deploy the configuration to redirect traffic to SIG endpoints.

To configure SIG tunnels and redirect traffic to SIG endpoints, do the following:

1. For automatic tunnels, configure SIG provider credentials.
2. Create a Security feature profile or choose an exiting Security feature profile and associate it with the configuration group.
3. In the Security feature profile, configure the Secure Internet Gateway feature to create automatic or manual SIG tunnels.

   For automatic tunnels, if you've not configured the SIG provider credentials, you are prompted to do so when you configure the Secure Internet Gateway feature.
4. For desired service VPNs, redirect traffic to SIG using data policies or by adding service routes in the service VPN feature configuration.
5. Deploy the configuration group on the desired WAN edge devices to create SIG tunnels from the devices to the configured SIG endpoints and redirect traffic to the SIG.

Configure SIG Credentials

Before you create automatic SIG tunnels, configure Cisco Umbrella or Zscaler credentials to enable Cisco SD-WAN Manager to create the tunnels to Cisco Umbrella or Zscaler endpoints. If you do not configure the SIG credentials on the **Administration** > **Settings** page before you configure the Secure Internet Gateway feature in the Security feature profile, Cisco SD-WAN Manager prompts you to enter the credentials when you configure the the Secure Internet Gateway feature. After you have configured the SIG credentials, you can modify the credentials on the **Administration** > **Settings** page.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. For the **Secure Internet Gateyway (SIG) Credentials** setting, click **Edit**.
3. Choose **Umbrella** or **Zscaler**.
4. For **Umbrella**, do one of the following:
   - Enable Cisco SD-WAN Manager to fetch credentials from the Cisco Umbrella portal:
     a. Ensure that you have added your Cisco Smart Account credentials here: **Administration** > **Settings** > **Smart Account Credentials**.

Cisco SD-WAN Manager uses the Cisco Smart Account credentials to connect to the Cisco Umbrella portal.

b. Click **Get Keys**.

Cisco SD-WAN Manager obtains the following details:

- Organization ID
- Registration Key
- Secret

- Enter Cisco Umbrella credentials:

Table 19: Cisco Umbrella Credentials

Field	Description
Organization ID	Enter the Cisco Umbrella organization ID (Org ID) for your organization. For more information, see *Find Your Organization ID* in the *Cisco Umbrella SIG User Guide*.
Registration Key	Enter the Umbrella Management API Key. For more information, see *Management and Provisioning > Getting Started > Overview* in the *Cloud Security API* documentation on the Cisco DevNet portal.
Secret	Enter the Umbrella Management API Secret. For more information, see *Management and Provisioning > Getting Started > Overview* in the *Cloud Security API* documentation on the Cisco DevNet portal.

5. For **Zscaler**, configure the following:

Table 20: Zscaler Credentials

Field	Description
Organization	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*.
Username	Username of the SD-WAN partner account.
Password	Password of the SD-WAN partner account.

Field	Description
Partner API key	Partner API key. To find the key in Zscaler, see *ZIA Help* > *Partner Integrations* > *Managing SD-WAN Partner Keys*.

6. Click **Save**.

Associate Security Feature Profile with a Configuration Group

Before you begin: Create a configuration group if you haven't already done so. For more information on creating a configuration group, see Run the Create Configuration Group Workflow.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Configuration Groups**.
2. For the desired configuration group, click **…** adjacent to the configuration group name and choose **Edit**.
3. In the **Feature Profiles - Unconfigured** area, find the **Security Profile** and click **Start Configuration**.
4. In the **Add Profile** slide-in pane, do one of the following:
   - Create a new Security feature profile:
     a. Click **Create new**.
     b. Enter a unique **Name** and an optional **Description** for the profile.
     c. Click **Save**.
   - Choose an existing Security feature profile:
     a. Click **Choose existing**.
     b. Select an existing Security feature profile. Click the radio button adjacent to the profile name.
     c. Click **Save**.

   The Security feature profile is listed under **Associated Profiles**.

Configure Secure Internet Gateway Feature

Before you begin: Create or edit a configuration group and associate the Security feature profile with it.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Configuration Groups**.
2. For the desired configuration group, click **…** adjacent to the configuration group name and choose **Edit**.
3. Under **Associated Profiles**, find the Security feature profile and expand the profile.
4. Click **Add Feature**.
5. In the **Add Feature** slide-in pane, from the drop-down list, choose the **Secure Internet Gateway** feature.
6. Configure the following details:

Table 21: Name, Description, and SIG Provider

Field	Description
Feature Name	Enter a name for the feature. The name can be up to 128 characters and can contain only alphanumeric characters.
Description	(Optional) Enter a description of the feature. The description can be up to 2048 characters and can contain only alphanumeric characters.
SIG Provider	Click one of the following: • **Umbrella**: Configure automatic tunnel to Cisco Umbrella SIG. If you've not configured Umbrella credentials, Cisco SD-WAN Manager prompts you to configure the credentials: **Click here to add Umbrella credentials**. Click, and in the **Add Umbrella Credentials** dialog box, enter the details mentioned in Table 22: Cisco Umbrella Credentials, on page 49 and click **Add**. • **Zscaler**: Configure automatic tunnel to Zscaler SIG. If you've not configured Zscaler credentials, Cisco SD-WAN Manager prompts you to configure the credentials: **Click here to add Zscaler credentials**. Click, and in the **Add Zscaler Credentials** dialog box, enter the details mentioned in Table 23: Zscaler Credentials, on page 50 click **Add**. • **Generic**: Configure manual tunnel to a SIG endpoint.

Table 22: Cisco Umbrella Credentials

Field	Description
Organization ID	Enter the Cisco Umbrella organization ID (Org ID) for your organization. For more information, see *Find Your Organization ID* in the *Cisco Umbrella SIG User Guide*.
Registration Key	Enter the Umbrella Management API Key. For more information, see *Management and Provisioning > Getting Started > Overview* in the *Cloud Security API* documentation on the Cisco DevNet portal.
Secret	Enter the Umbrella Management API Secret. For more information, see *Management and Provisioning > Getting Started > Overview* in the *Cloud Security API* documentation on the Cisco DevNet portal.

Table 23: Zscaler Credentials

Field	Description
Organization	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*.
Username	Username of the SD-WAN partner account.
Password	Password of the SD-WAN partner account.
Partner API key	Partner API key. To find the key in Zscaler, see *ZIA Help > Partner Integrations > Managing SD-WAN Partner Keys*.

7. To create tunnels, click **Configuration** and do the following:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. Enter the value when you add a device to the configuration group. To change the default key, type a new string and move the cursor out of the **Enter Key** box.
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices.

   a. Click **Add Tunnel**.

   b. In the **Add Tunnel** dialog box, under **Basic Settings** configure the following:

Table 24: Basic Settings

Field	Description
Tunnel Type	Umbrella: (Read only) **ipsec** Zscaler: Click **ipsec** or **gre**. Generic: Click **ipsec** or **gre**.
Interface Name (1..255)	Enter the interface name.
Description	Enter a description for the interface.

Field	Description
Tracker	By default, a tracker is attached to monitor the health of tunnels. Alternatively, you can create a customized tracker as described in step **7** and choose the tracker.

Tunnel Source Interface	Enter the name of the source interface of the tunnel. This interface should be the egress interface and is typically the internet-facing interface.
	
	For releases before Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1, and you have a Cellular or Dialer interface as the tunnel's source interface, the following workaround must be implemented.
	
	If you use a cellular interface as a tunnel source interface, you must modify your existing tunnel source interface configuration with the following configuration:
	
	`interface <interface name>`
	`no tunnel route-via <Interface> mandatory`
	
	Use the CLI add-on feature template to modify the tunnel configuration on the device. For more information on how to use a CLI add-on feature template, see , Create a CLI Add-On Feature Template.
	
	After you have modified the tunnel configuration, select the device template for which you want to apply the CLI add-on feature template, and push the configuration to the devices. For more information about attaching a device template to one or more devices, see Attach Template to Devices.
	
	Note
	A SIG tunnel will be created for cellular interfaces only if a global VRF has only one transport interface. A SIG tunnel is not be created if a global VRF has multiple transport interfaces.

Source Public IP	(Automatic GRE tunnels to Zscaler only) 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.
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.

Field	Description
Tunnel Destination IP Address/FQDN	(Manual tunnels only) Enter the IP address of the SIG provider endpoint.
Preshared Key	(Manual tunnels only) This field is displayed only if you choose **ipsec** as the **Tunnel Type**. Enter the password to use with the preshared key.

c. (Optional) Under **Advanced Options**, configure the following:

Table 25: (Tunnel Type: gre) General

Field	Description
Shutdown	Click **No** to enable the interface; click **Yes** to disable. **Default**: No.
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

Table 26: (Tunnel Type: ipsec) General

Field	Description
Shutdown	Click **No** to enable the interface; click **Yes** to disable. **Default**: **No**.
Track this interface for SIG	Enable or disable tracker for the tunnel. By default, Cisco SD-WAN Manager enables a tracker for automatic tunnels. **Default**: **On**.
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

Field	Description
IP MTU	Specify the maximum MTU size of packets on the interface. **Range**: 576 to 2000 bytes **Default**: 1400 bytes
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. **Range**: 10 to 3600 seconds **Default**: 10
DPD Retries	Specify the number of seconds between DPD retry messages if the DPD retry message is missed by the peer. Once 1 DPD message is missed by the peer, the router moves to a more aggressive state and sends the DPD retry message at the faster retry interval, which is the number of seconds between DPD retries if the DPD message is missed by the peer. The default DPD retry message is sent every 2 seconds. Five aggressive DPD retry messages can be missed before the tunnel is marked as down. **Range**: 2 to 60 seconds **Default**: 3

Table 27: (Tunnel Type: ipsec) IKE

Field Name	Description
IKE Rekey Interval	Specify the interval for refreshing IKE keys. **Range:** 300 to 86400 seconds (1 hour to 14 days) **Default**: 14400 seconds
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

Field Name	Description
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2. • 2 1024-bit modulus • 14 2048-bit modulus • 15 3072-bit modulus • 16 4096-bit modulus **Default**: 14 2048-bit modulus

Table 28: (Tunnel Type: ipsec) IPSEC

Field	Description
IPsec Rekey Interval	Specify the interval for refreshing IPSec keys. **Range**: 300 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, 4096. **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 • NULL SHA1 • NULL SHA 384 • NULL SHA 256 • NULL SHA 512 **Default**: AES 256 GCM

Field	Description
Perfect Forward Secrecy	• Specify the 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. **Default**: None

d. Click **Add**.

8. To create one or more trackers to monitor tunnel health, click **Tracker** and do the following:

a. **Source IP Address**: Enter a source IP address for the probe packets.

b. Click **Add Tracker**.

c. In the **Add Tracker** dialog box, configure the following:

Table 29: Tracker Parameters

Field	Description
Name	Enter a name for the tracker. The name can be up to 128 alphanumeric characters.
API url of endpoint	Specify the API URL for the SIG endpoint of the tunnel.
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 down. **Range**: 1 to 10 **Default**: 3

d. Click **Add**.

e. To add more trackers, repeat sub-step **b** to sub-step **d**.

9. To designate active and back-up tunnels and distribute traffic among tunnels, click **High Availability** and do the following:

a. Click **Add Interface Pair**.

b. In the **Add Interface Pair** dialog box, configure the following:

Table 30: High Availability Parameters

Field	Description
Active	Choose a tunnel that connects to the primary data center.
Active Weight	Enter a 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 active tunnels, where the first tunnel is configured with a 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	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**.
Backup Weight	Enter a 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 a 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.

c. Click **Add**.

d. To add more active and back-up tunnel pairs, repeat sub-step **a** to sub-step **c**.

10. (Optional) To configure advanced settings for Cisco Umbrella or Zscaler, click **Advanced Settings** and configure the following:

Table 31: Umbrella

Field	Description
Umbrella Primary Data-Center	Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. If you wish to route traffic to a specific Cisco Umbrella data center, choose the data center from the drop-down list.
Umbrella Secondary Data-Center	Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. If you wish to route traffic to a specific Cisco Umbrella data center, choose the data center from the drop-down list.

Table 32: Zscaler

Field	Description
Primary Datacenter	Automatic IPSec tunnels: Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. If you wish to route traffic to a specific Zscaler data center, choose the data center from the drop-down list. Automatic GRE tunnels: Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. If you wish to route traffic to specific Zscaler data center, ensure that you choose a Zscaler data center that is recommended by Zscaler based on geographical proximity to the device. Obtain the recommend list of Zscaler data centers through a GET API request for `/vips/recommendedList`. In the API request, specify the public IP of your device as the value of the `sourceIp` query parameter. For more information on `/vips/recommendedList`, see *ZIA API Developer & Reference Guide*. If you choose a data center that is not in the recommended list, the Cisco IOS XE Catalyst SD-WAN device reverts to the automatically selected data center.

Field	Description
Secondary Datacenter	Automatic IPSec tunnels: Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. If you wish to route traffic to a specific Zscaler data center, choose the data center from the drop-down list. Automatic GRE tunnels: Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. If you wish to route traffic to specific Zscaler data center, ensure that you choose a Zscaler data center that is recommended by Zscaler based on geographical proximity to the device. Obtain the recommend list of Zscaler data centers through a GET API request for `/vips/recommendedList`. In the API request, specify the public IP of your device as the value of the `sourceIp` query parameter. For more information on `/vips/recommendedList`, see *ZIA API Developer & Reference Guide*. If you choose a data center that is not in the recommended list, the Cisco IOS XE Catalyst SD-WAN device reverts to the automatically selected data center.
Zscaler Location	(Optional) 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. For more information about locations, see *ZIA Help > Traffic Forwarding > Location Management > About Locations*.
Authentication Required	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 Firewall	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 Surrogate IP	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off

Field	Description
Display Time Unit	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Minute
Idle Time to Disassociation	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: 0
Enforce Surrogate IP for known browsers	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Refresh Time Unit	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Minute
Refresh Time	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: 0

11. Click **Save**.

Redirect Traffic to SIG Using Service VPN Feature

Configure a SIG service route for a service VPN to direct the VPN traffic to SIG.

Note Alternatively, you can also redirect traffic to SIG using Data Policy. For more information, see Action Parameters in the *Policies Configuration Guide*.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Configuration Groups**.
2. For the desired configuration group, click **…** adjacent to the configuration group name and choose **Edit**.
3. Expand the **Service Profile**, and for the service VPN whose traffic you want to redirect traffic to SIG, click **...** and click **Edit Parcel**.
4. Remove any existing static IPv4 routes to the internet:
   a. Click **Route**.
   b. Under **IPv4 Static Route**, find any routes to the internet and click the delete icon to remove it.
5. Add SIG service route:
   a. Click **Service Route**.
   b. Click **Add Service Route**.

c. In the **Add Service Route** dialog box, configure the following:

Table 33: Service Route Parameters

Field	Description
Network Address	Enter the public IPv4 address.
Subnet Mask	Enter the subnet for the IPv4 address.
Service	Choose **SIG** from the drop-down list.
VPN	Enter the VPN over which to direct the traffic. Default: VPN 0

d. Click **Add**.

6. Click **Save**.

Next steps: Add Devices to Configuration Group and Deploy Devices.

Monitor SIG Events

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

Monitor security events related automatic SIG tunnels using the following Cisco SD-WAN Manager GUI components:

- **Security Events** pane on the **Monitor** > **Security** page
- **Events** dashboard on the **Monitor** > **Logs** page

Security Events

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

   The **Security Events** pane shows how many critical, major, and minor security events Cisco IOS XE Catalyst SD-WAN devices have reported to Cisco SD-WAN Manager during a specified time period. The information is displayed in a bar chart.

   Cisco IOS XE Catalyst SD-WAN devices notify security events to Cisco SD-WAN Manager using NETCONF. The security events include events related to automatic SIG tunnel creation.

2. (Optional) By default, the pane displays security event 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.

3. (Optional) **View Details**: Click **View Details** to display the **Monitor** > **Logs** > **Events** page, with information filtered for the **Security** component.

Events Dashboard

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

2. Click **Events**.

   Cisco SD-WAN Manager displays any events that WAN edge devices and controllers have notified in the past three hours.

3. Click **Filter** and configure the following:

Field	Description
Component	Choose the **Security** component.
Severity	Choose one or more of **Critical**, **Major**, and **Minor**. If you do not select specific severities, events of all three severites are displayed.
System IP	To view events notified by specific WAN edge devices, choose the system IP of the devices.
Event name	To view information about one or more specific SIG tunnel events, choose the corresponding event names. **Tip** To view Cisco Umbrella SIG tunnel events, search for events that have `ftm-tunnel` in the event name. To view Zscaler SIG tunnel events, search for events that have `ftm-zia` in the event name.

   Click **Apply**.

   If the target devices or controllers notified any of the chosen events, Cisco SD-WAN Manager displays information about the same.

4. (Optional) To modify the time range, click **3 hours**, select a time range, and click **Apply.**

   Cisco SD-WAN Manager displays event information for the modified time range.

5. (Optional) Click **Export** to download a CSV file containing the table data.

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

6. (Optional) 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**.

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**.

Monitor Automatic SIG Tunnels Using CLI

Automatic SIG Tunnels to Cisco Umbrella

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.5.1a

To view information about the automatic SIG tunnels that you have configured from a Cisco IOS XE Catalyst SD-WAN device to Cisco Umbrella, use the **show sdwan secure-internet-gateway umbrella tunnels** command.

The following is a sample output of the **show sdwan secure-internet-gateway umbrella tunnels** command:

```
Device# show sdwan secure-internet-gateway umbrella tunnels
                                                                                                                API
 LAST
TUNNEL IF                                                                                                       HTTP
 SUCCESSFUL    TUNNEL
NAME          TUNNEL ID  TUNNEL NAME                                 FSM STATE             CODE
 REQ           STATE
-------------------------------------------------------------------------------------------------------------------
Tunnel17447  527398582  SITE10005SYS172x16x255x88IFTunnel17447  st-tun-create-notif  200
 rekey-tunnel  -
Tunnel22427  527398577  SITE10005SYS172x16x255x88IFTunnel22427  st-tun-create-notif  200
 rekey-tunnel  -
Tunnel22457  527398373  SITE10005SYS172x16x255x88IFTunnel22457  st-tun-create-notif  200
 rekey-tunnel  -
```

Automatic SIG Tunnels to Zscaler

To view information about the automatic SIG tunnels that you have configured from a Cisco IOS XE Catalyst SD-WAN device to Zscaler SIG, use the **show sdwan secure-internet-gateway zscaler tunnels** command.

The following is a sample output of the **show sdwan secure-internet-gateway zscaler tunnels** command for automatic IPSec tunnels:

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.5.1a

```
Device# show sdwan secure-internet-gateway zscaler tunnels


                        HTTP
TUNNEL IF                                                TUNNEL
                                                              LOCATION
                        RESP
NAME          TUNNEL NAME                                ID        FQDN
                                        TUNNEL FSM STATE          ID        LOCATION FSM
STATE   LAST HTTP REQ     CODE
-------------------------------------------------------------------------------------------------------------------
Tunnel100001  site1820851800sys172x16x255x15ifTunnel100001  52615809
site1820851800sys172x16x255x15iftunnel100001@example.com  add-vpn-credential-info  52615819
  location-init-state  get-data-centers  200
Tunnel100002  site1820851800sys172x16x255x15ifTunnel100002  52615814
site1820851800sys172x16x255x15iftunnel100002@example.com  add-vpn-credential-info  52615819
  location-init-state  get-data-centers  200
```

The following is a sample output of the **show sdwan secure-internet-gateway zscaler tunnels** command for automatic GRE tunnels:

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

```
Device# show sdwan secure-internet-gateway zscaler tunnels

                      HTTP
TUNNEL IF                              TUNNEL        TUNNEL FSM      LOCATION
         LAST HTTP     RESP
NAME           TUNNEL NAME             ID      FQDN  STATE           ID        LOCATION FSM
 STATE   REQ           CODE
-------------------------------------------------------------------------------------------------------
Tunnel100512  192.0.2.2_Tunnel100512  102489  n/a   gre-add-tunnel  46206485
location-init-state  activate-req  200
Tunnel100513  192.0.2.2_Tunnel100513  102489  n/a   gre-add-tunnel  46206485
location-init-state  activate-req  200
```

Automatic SIG Tunnels

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

To view information about the automatic SIG tunnels that you have configured from a Cisco IOS XE Catalyst SD-WAN device, use the **show sdwan secure-internet-gateway tunnels** command.

The following is a sample output of the **show sdwan secure-internet-gateway tunnels** command:

```
Device# show sdwan secure-internet-gateway tunnels
TUNNEL IF     TUNNEL                                                    HA      DEVICE  SIG
   TRACKER              DESTINATION            TUNNEL
NAME          ID        TUNNEL NAME                                    PAIR    STATE   STATE
  STATE    SITE ID     DATA CENTER  PROVIDER  TYPE    TIMESTAMP
-------------------------------------------------------------------------------------------------------
Tunnel100001  52615809  site1820851800sys172x16x255x15ifTunnel100001  Active  Up      NA
   Enabled  1820851800  NA           zScaler   IPsec   NA
Tunnel100002  52615814  site1820851800sys172x16x255x15ifTunnel100002  Backup  Up      NA
   Enabled  1820851800  NA           zScaler   IPsec   NA
```

Monitor Layer 7 Health Check SLA Metrics Using the CLI

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a

SLA Profile

To view information about the SLA profile that you have configured, from Cisco SD-WAN Manager use the **show endpoint-tracker sla-profile** command.

The following is a sample output of the **show endpoint-tracker sla-profile** command:

```
Device# show endpoint-tracker sla-profile

SLA Profile     SLA mode            cfg loss(%)     cfg latency(ms)  cfg jitter(ms)
sla_agg                 aggressive          10              300              80

sla_con                 conservative        10              300              80

sla_mod                 moderate            10              300              30
```

SLA Mode

To view information about the SLA mode that you have configured from Cisco SD-WAN Manager use the **show endpoint-tracker sla-mode** command.

The following is a sample output of the **show endpoint-tracker sla-mode** command:

```
Device# show endpoint-tracker sla-mode
SLA mode         Poll Interval(Secs)  Poll multiplier(buckets)     Dampening multiplier
   Dampening window(Secs)

==========================================================================================

Aggressive   60             1                            1                          60

Moderate  120               1                            2                          240

Conservative   300          1                            3                          900
```

The command output shows the following:

- **Poll Interval**: Time period in seconds which defines a bucket of sample data.
- **Poll Multiplier**: Number of buckets to wait before checking the SLA status (Met or Violated).
- **Dampening Multiplier**: Number of extra buckets to wait before allowing an SLA status to change from Violated to Met, to avoid flapping conditions.

SLA Status

To view information about the SLA status use the **show endpoint-tracker sla-status** command.

The following is a sample output of the **show endpoint-tracker sla-status** command:

```
Device# show endpoint-tracker sla-status
Interface   Record name  SLA Profile    SLA Status   Loss(%) Latency(ms)  Jitter(ms)
Tunnel601            youtbue      sla_agg         Met          0       32          46

Tunnel602            netflix      sla_agg         Met          0       4           1
```

SLA Statistics

To view information about the SLA statistics use the **show endpoint-tracker sla-statistics** command.

The following is a sample output of the **show endpoint-tracker sla-statistics** command:

```
Device# show endpoint-tracker sla-statistics
Interface     Index    Loss(%)    Latency(ms)  Jitter(ms)
Tunnel602            0          0           3           0
```

Troubleshoot Integrating Your Devices With Secure Internet Gateways

This section describes how to troubleshoot integrating your devices with Secure Internet Gateways.

Missing Tunnel Route-via Field After Upgrade

Problem

SIG feature templates created in software versions earlier than Cisco vManage Release 20.9.x may not display the **Tunnel Route-via Interface** field or include the property in the configuration payload after an upgrade.

Possible Causes

The SIG template may be using an older configuration that does not include the latest properties and field requirements of the current software release.

Solution

Edit the affected SIG feature template and click Update. This action synchronizes the template with the current software version and restores availability of the **Tunnel Route-via Interface** field.

After Upgrading Cisco SD-WAN Manager Tunnels Fail

After upgrading from Cisco vManage Release 20.3.1 to Cisco vManage Release 20.3.2, you may see failures when connecting from your devices to SIG services or when connecting standard IPSec tunnels to cloud security services.

Affected Feature Templates

- Cisco Secure Internet Gateway (SIG)
- Cisco VPN Interface IPSec (WAN)
- Cisco VPN Interface GRE

Description

By default, a tunnel created using the SIG template pushes the **tunnel vrf multiplexing** command. For VPN Interface IPSec templates, from the **Application** drop-down list, if you choose **Secure Internet Gateway**, the command is pushed. However, after you upgrade to Cisco vManage Release 20.3.2, your feature templates may remove the **tunnel vrf multiplexing** configuration. This causes your feature templates to fail when connecting to SIG services or other external services such as cloud security services.

Workaround

Depending on which feature template you want to update, do one of the following:

Cisco VPN Interface Feature Templates

1. In Cisco SD-WAN Manager, edit the template.
2. From the **Application** drop-down menu, choose **Secure Internet Gateway**.
3. Save the template.

All Affected Feature Templates

You can do one of the following:

- Manually add **tunnel vrf multiplexing** to the tunnel configuration using a CLI add-on feature template.
- In Cisco SD-WAN Manager, edit the existing template as follows:
  1. Modify a field, such as the description, that does not affect the configuration.
  2. Save the template.
  3. Push the template to the device.

Verification

You can run the following command to verify that **tunnel vrf multiplexing** was added to your templates:

```
show sdwan running-config interface tunnel Number
```

Example:

```
Device#sh sdwan running-config interface | begin Tunnel100001
interface Tunnel100001
 ip unnumbered GigabitEthernet1
 ip mtu 1400
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel route-via GigabitEthernet1 mandatory
 tunnel vrf multiplexing
 tunnel protection ipsec profile if-ipsec2-ipsec-profile
exit
```

GRE Tunnel Creation Fails After You Restore Device Operation

Problem

If you have created an automatic GRE tunnel to a Zscaler SIG endpoint with a source public IP address, the device becomes inoperative due to an event such as a power outage or a maintenance activity. This issue is seen in Cisco IOS XE Catalyst SD-WAN Release 17.9.1a or Cisco IOS XE Catalyst SD-WAN Release 17.9.2a. When you make the device operational again and attempt to create an automatic GRE tunnel to the Zscaler with the same source public IP address, the tunnel creation fails. One of the following failure notifications appears in the **Events** dashboard on the **Monitor** > **Logs** page in the Cisco SD-WAN Manager menu:

- **add-static-ip-failure**
- **add-gre-tunnel-failure**

Alternatively, you can use the **show sdwan secure-internet-gateway zscaler tunnels** command to view the status of the tunnel along with an error code which indicates the reason for the failure of the tunnel creation.

Possible Causes

Tunnel creation fails because the source public IP address may exist on the Zscaler portal. This event occurs because the device didn't clear the previous tunnels after becoming operational again.

Solution

Delete the existing source public IP address on the Zscaler portal by doing the following:

1. Remove the SIG feature template from the device in Cisco SD-WAN Manager.
2. From the Zscaler portal, choose **Administration** > **Location Management** and search for the location that is associated with the tunnel in the **Location** tab.
3. Click the **Edit** icon and delete the entry.
4. From the Zscaler portal, choose **Administration** > **Static IPs & GRE Tunnels** and locate the static IP address in the **Static IP** tab.
5. Click the **Edit** icon and delete the entry.

6. Attach the SIG template that you removed in the first step, back to the device. For more information about attaching the SIG template, see the section Attach the SIG Template to Devices.

IKE/IPsec Tunnel Failure with Cellular Interface

Note: This problem and solution applies for releases Cisco IOS XE Catalyst SD-WAN Release 17.13.1a or before.

Problem

An IKE/IPsec tunnel cannot be established when a cellular interface is used as the source interface.

Possible Causes

IKE/IPsec packets may be routed through the incorrect source interface.

Solution

When configuring SIG tunnels, especially over cellular interfaces, it's recommended to set the tunnel routing option to **preferred** rather than **mandatory**. Utilizing **preferred** avoids packet loss issues that have been observed when **mandatory** is selected as the routing option for cellular interface-based tunnels.

Here are a few example scenarios to consider when setting up SIG tunnels, particularly with cellular interfaces in the configuration:

1. Cisco IOS XE Catalyst SD-WAN Device with Single Cellular Interface.

   When a cellular interface is active, SIG tunnels will be established as soon as the cellular interface is up.

2. Cisco IOS XE Catalyst SD-WAN Device with Both Broadband and Cellular Interfaces.
   - If both Broadband and Cellular interfaces are active:
     - SIG tunnels will be active for the broadband interface.
     - SIG tunnels will also be active for the cellular interface; however, the cellular interface's IKE/IPsec packets will be routed through the broadband interface.
   - If the broadband interface is down but the cellular interface is up:
     - SIG tunnels for the broadband interface will not be active.
     - SIG tunnels for the cellular interface will remain active, and IKE/IPsec negotiation will occur over the cellular link, as expected.

3. Cisco IOS XE Catalyst SD-WAN Device with Dual Cellular Interfaces.
   - When both cellular interfaces (cellular interface 1 and cellular interface 2) are active:
     - SIG tunnels will be active for both interfaces.
   - When cellular interface 1 is down and cellular interface 2 interface is active:
     - SIG tunnels for cellular interface 1 will not be active, but its IKE/IPsec packets will be rerouted via cellular interface 2.

- SIG tunnels for cellular interface 2 will continue to remain active.

Here is a sample configuration to address the issue with the IKE/IPsec tunnel not establishing when using the cellular interface as the source interface.

```
interface Tunnel16000001
 no shutdown
 ip unnumbered Cellular0/1/0
 ip mtu 1400
 tunnel source Cellular0/1/0
 tunnel destination dynamic
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile if-ipsec1-ipsec-profile
 tunnel vrf multiplexing
 tunnel route-via Cellular0/1/0 preferred
```

Share Traffic Information with Cisco Security Service Edge

Information About Sharing Traffic Information with Cisco Security Service Edge

Minimum Supported Releases: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Manager Release 20.15.1

Information Sharing

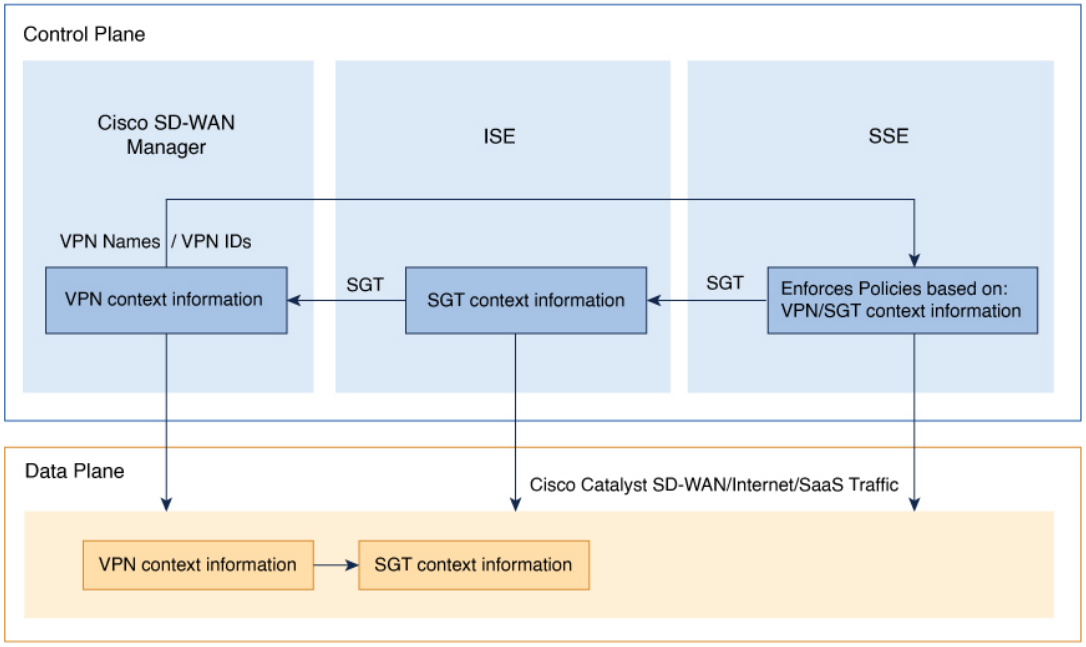
Cisco SD-WAN Manager shares VPN context information with Secure Service Edge (SSE). It provides SSE with VPN details, including VPN names and IDs. ISE shares SGT information with both Cisco SD-WAN Manager and SSE. SSE uses the VPN and SGT information to enforce specific security policies on traffic from Cisco Catalyst SD-WAN to internet and SaaS applications. These policies match source objects based on SGT or VPN for internet- and SaaS-bound traffic.

In the control plane, Cisco SD-WAN Manager shares VPN information with SSE but does not share SGT information. In the data plane, both VPN and SGT information are included in the traffic directed towards Cisco SSE.

Integration Requirements

Integrating ISE with the Cisco SD-WAN Manager is optional, but it is mandatory to configure the integration of ISE with SSE.

Figure 1: Cisco SD-WAN, SSE, and ISE Information Sharing



Prerequisites for Sharing Traffic Information with Cisco Security Service Edge

- **SSE Integration**

  Ensure SSE is integrated with both Cisco SD-WAN Manager and ISE. For more information, see Integrate Your Devices with Secure Service Edge.

- **API Credentials for SSE**

  Ensure that the API credentials for SSE has the necessary permissions, specifically write access, to manage identity-related information and enable context sharing.

- **Configure DNS on VPN0 Interface**

  Ensure DNS is configured on the VPN0 interface of the device for seamless connectivity between Cisco SD-WAN Manager and Cisco Secure Access.

- **Enable NAT on WAN and LAN Interfaces**

  Enable NAT on the WAN and LAN interfaces of the device to ensure proper address translation for both outbound and inbound traffic. This is crucial for maintaining seamless connectivity and proper routing of traffic through the network.

- **CLI Commands for SGT Sharing with SSE**

  To share SGT with SSE, use the following CLI commands as part of the CLI add-on template to fetch the SGT value:

```
policy
 app-visibility
 flow-visibility
```

```
ip visibility features
ulogging enable
```

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Restrictions for Sharing Traffic Information with Cisco Security Service Edge

You cannot use CLI profiles to configure this feature.

Configure Sharing Traffic Information with Cisco Security Service Edge

Enable Context Sharing

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Cloud Credentials**.
2. Click **Context Sharing** to enable the context sharing in Cisco SD-WAN Manager.

Note Context sharing cannot be disabled after it is enabled.

Enable Context Sharing for VPN and SGT

Enable context sharing for VPN and SGT to allow Cisco IOS XE Catalyst SD-WAN devices to share context information with SSE.

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

Field	Description
VPN	Enable sharing of VPN information with SSE.
SGT	Enable sharing of SGT information with SSE.

Create SSE Policy Using Policy Group

For more information, see Configure a Secure Service Edge.

Verify Traffic Information Sharing with Cisco Security Service Edge

To check whether context sharing is active on a Cisco IOS XE Catalyst SD-WAN device, use the **show sse all** command.

In the following command, context sharing is enabled, and it is shown in bold.

```
Device# show sse all

************************************
SSE Instance Cisco-Secure-Access
************************************
Tunnel name : Tunnel16000001
```

```
Site id: 2432287619
Tunnel id: 634930903
SSE tunnel name: C8K-e28146f8-e524-46ff-a799-a95fc1a086da
HA role: Active
Local state: Up
Tracker state: Up
Destination Data Center: 52.42.220.205
Tunnel type: IPSEC
Provider name: Cisco Secure Access
Context sharing: CONTEXT_SHARING_SRC_VPN | CONTEXT_SHARING_SGT
```

Monitor Traffic Information Sharing with Cisco Security Service Edge

Monitor SIG/SSE Tunnels

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

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 and 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. 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.

View SSE Tunnels

View SSE tunnels to obtain granular information about each tunnel.

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: For more information, see the section **SIG/SSE Tunnels Dashboard** in Monitor SIG/SSE Tunnels.

View Context-Sharing Data

View context-sharing data by enabling context-sharing filters. These filters can help identify whether the context-sharing data (VPN and SGT) is enabled or disabled.

To enable context-sharing filters:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Tunnels** > **SIG/SSE Tunnels**.
2. Click on the gear icon to display the table settings slide-in pane.
3. Click to enable the context sharing filters to display detailed information about VPN and SGT context sharing in the table.