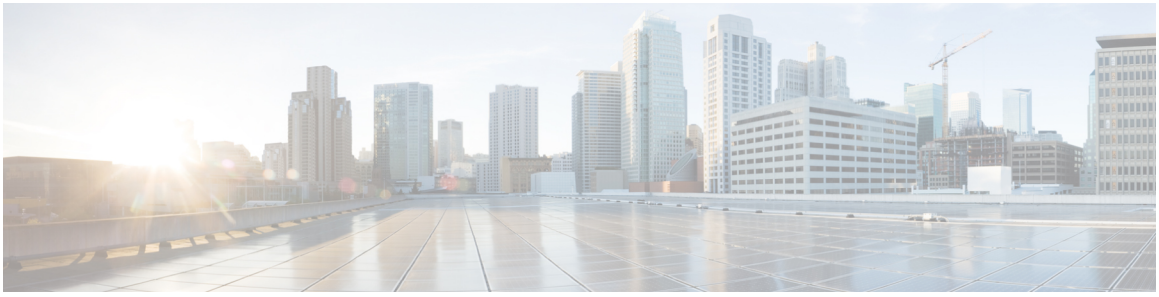
Security Configuration Guide for SD-Routing Devices

First Published: 2024-04-30

Last Modified: 2024-04-30

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

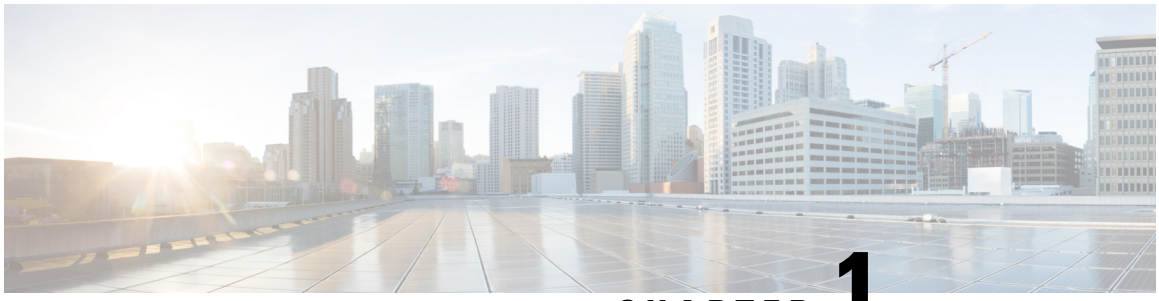
Preface

This preface describes the audience, organization, and conventions of this document. It also provides information on how to obtain other documentation.

This preface includes the following sections:

Reference Preface Map here

Preface



CHAPTER 1

What is Cisco Secure Access

Cisco Secure Access is a cloud Security Service Edge (SSE) solution that is a convergence of network security services delivered from the cloud to connect a hybrid workforce. This solution provides seamless, transparent, and secure Direct Internet Access (DIA) to users helping them connect from anything to anywhere.

In Cisco IOS XE 17.14.1a, Cisco SSE provides the capability for SD-Routing devices to connect with SSE providers using IPSec tunnels.

Feature	Release Information	Description
Configure Cisco Secure Access	Cisco IOS XE Release 17.14.1a	Cisco Secure Access Edge (SSE) solution transparent, and secu (DIA). This solution can be groups in Cisco SD-

Restrictions

- Cisco Secure Access does not support API Throttling
- After integrating CiscoSecure Access with Cisco SD-Routing, any changes made to the network tunnel group name in Cisco Secure Access dashboard is not reflected in Cisco SD-WAN Manager

Workflow to Set Up Cisco Secure Access

This workflow outlines the high-level steps required to set up Cisco Secure Access. The detailed instructions are covered in the following sections.

Task	Description
Preliminary configurations on Cisco Secure Access Portal	

Task	Description
Check credentials on the portal and ensure that the API credentials have write access.	Go to **Admin** > **Management** > **API Keys** and generate and manage API keys. Ensure that you have write access to Tunnel Group and tunnel creation. Having this ensures seamless connection between Cisco Secure Access and the SD-Routing device, after tunnels have been set up and deployed using the SD-WAN Manager.
Preliminary configurations on Cisco SD-WAN Manager	
Ensure that you have created a Configuration Group and assigned it to the SD-Routing device.	Go to Configuration Groups
Configure the following using the CLI template available on the SD -WAN Manager.	Go to Configuration Groups select any SD-Routing config group, click Edit and select the corresponding CLI Profile dialog box. In the **Add Feature Profile** window, select **Create New** and enter a name and description followed by the command in the **CLI Configuration** section. Save it to add this feature parcel.
• Ensure DNS configuration for the sd-routing device.	By doing this you are allowing the device to interact with DNS servers. You can configure any DNS server on the device which connects to HTTPS to get the public IP address. To configure a source interface for HTTPS, use the **ip http client source-interface** *name and number of the interface* command on Cisco SD-WAN Manager.

• Ensure NAT is enabled on WAN and LAN interface (outside/inside)	By doing this you are ensuring that multiple private addresses inside a local network get mapped to a public IP address before transferring the information onto the internet. For example, all source addresses of the packets that match *access-list nat acl1* will be converted to *Loopback 1* IP address when exiting the router.
	`ip nat inside source list wan-acl1 interface GigabitEthernet2 overload`
	OR
	`ip nat inside source list nat_acl1 interface Loopback1 overload`

Enable domain look up for the device	Go to **Configuration Groups** > **System Profile** > **Global** and enable **Global Lookup**
SSE related configurations on Cisco SD-WAN Manager	
Set up Cloud Provider credentials	Go to **Administration** > **Settings** > **Cloud Provider Credentials** > **Cisco SSE**

Task	Description
Configure source interface address	Go to **Configuration** > **Configuration Groups**
Create SSE Policy using Policy Groups	Go to **Configuration** > **Policy Groups** > **Secure Internet Gateway/Secure Service Edge**
Configure Traffic Redirection	By configuring this, you are creating a service route to redirect traffic through the SSE tunnels Go to **Configuration Groups** select any SD-Routing config group, click Edit and select the corresponding CLI Profile dialog box. In the **Add Feature Profile** window, select **Create New** and enter a name and description followed by the command in the **CLI Configuration** section. Save it to add this feature parcel.
Associate the SSE Policy with Policy Group	Go to **Configuration** > **Policy Groups** > **Add Policy Group** , select the SSE policy created earlier and click **Save** to associate the SSE Policy with the Policy Group. Next associate this policy group with the device and deploy.
Verify the SSE Configuration	Verify the configuration.
Monitor the SSE Tunnels	**Monitor** > **Audit Logs** **Monitor** > **Security** for SSE Tunnels **Monitor** > **Tunnels** > **SSE Tunnels**

Set up Cloud Provider Credentials

Configure credentials to enable Cisco SD-WAN Manager for automated tunnel provisioning to Cisco SSE.

Step 1 Click **Administration** > **Settings** > **Cloud Credentials** > **Cloud Provider Credentials** enable **Cisco Secure Access** and enter the following details. These credentials are used to initiate authentication for a session and are later used in subsequent sessions.

Field	Description
Organization ID	Cisco Secure Access organization ID for your organization.
API Key	Cisco Secure Access API Key.
Secret	Cisco Secure Access API Secret.

Step 2 Save these details.

Configure Loopback Interface as the Source Interface

Configure a loopback interface as source. As this loopback interface is not tied to any interface, there is no risk of interruptions in connections.

Add the following command to the CLI template:

```
interface loopback1
no shutdown
ip nat inside
ip address 1.1.1.1 255.255.255.255
```

Create an SSE Policy Using Policy Group

Before you begin

Ensure that you have created the SSE credentials.You can do this on the SD-WAN Manager by going to **Administration** > **Settings** > **Cloud Provider Credentials** > **Cisco SSE** and enter the details.

Step 1 On the SD-WAN Manager go to **Configuration** > **Policy Groups** > **Secure Internet Gateway/Secure Service Edge**. Click on **Add Secure Service Edge (SSE)**.

Step 2 Enter a name for the SSE policy and specify the solution type as **sd-routing** and click **Create**.

Step 3 Create a tracker. While creating automatic tunnels, Cisco SD-WAN Manager creates and attaches a default tracker endpoint with default values for failover parameters. However, you can also create customized trackers with failover parameters that suit your requirements.

a) In the **Source IP Address** field, enter a source IP address without a subnet mask. This is used for sending http probes to tracker endpoint to detect if there is a unexpected network drops or any latency and is used under the vrf id 65330.

b) Click **Add Tracker**. In the **Add Tracker** window, configure the following and click **Add**.

Table 1: Tracker Parameters

Field	Description
Name	Name of the tracker. The name can be up to 128 alphanumeric characters.
API URL of Endpoint	Specify the API URL for the Secure Service Edge endpoint of the tunnel. Default: service.sig.umbrella.com
Threshold	Enter the wait time for the probe to return a response before declaring that the configured endpoint is down. The range is 100 to 1000 milliseconds, the default is 300 milliseconds.
Probe Interval	Enter the time interval between probes to determine the status of the configured endpoint. The range is 20 to 600 seconds, the default is 60 seconds.
Multiplier	Enter the number of times to resend probes before determining that a tunnel is up or down. The range is 1 to 10, the default is 3.

Step 4 Create a Tunnel. Click **Configuration**.

a) Click **Add Tunnel**.

b) In the **Add Tunnel** pop-up window, under **Basic Settings**, configure the following and click **Add** .

Table 2: Basic Settings

Field	Description
Tunnel Type	Cisco Secure Access: (Read only) **ipsec**
Interface Name (1..255)	Name of the interface.
Description	Enter a description for the interface.
Tracker	By default, a tracker is attached to monitor the health of tunnels.
Tunnel Source Interface	Name of the source interface of the tunnel. This interface should be an egress interface and is typically the internet-facing interface. The tunnel source interface supports loopback. Depending on your intent you can configure up to 16 tunnels (8 Active/8 Backup).
Data-Center	For a primary data center, click **Primary**, or for a secondary data center, click **Secondary**. Tunnels to the primary data center serve as active tunnels, and tunnels to the secondary data center serve as back-up tunnels.
Advanced Options (Optional)	
Shutdown	Click the radio button to enable this option. Default: Disabled
Enable Tracker	Click the radio button to enable this option.
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 to 2000 bytes Default: 1400 bytes
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 500 to 1460 bytes Default: None
DPD Interval	Specify the interval for Internet Key Exchange (IKE) to send Hello packets on the connection. Range: 10 to 3600 seconds Default: 10

Field	Description
DPD Retries	Specify the number of seconds between Dead Peer Detection (DPD) retry messages if the DPD retry message is missed by the peer. If a peer misses a DPD message, the router changes the state and sends a DPD retry message. The message is sent at a faster retry interval, which is the number of seconds between DPD retries. The default DPD retry message is sent every 2 seconds. The tunnel is marked as down after five DPD retry messages are missed. Range: 2 to 60 seconds Default: 3
IKE	
IKE Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 to 1209600 seconds (1 hour to 14 days) Default: 14400 seconds
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Choose one of the following: • AES 256 CBC SHA1 • AES 256 CBC SHA2 • AES 128 CBC SHA1 • AES 128 CBC SHA2 Default: AES 256 CBC SHA1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2.
IPSec	
IPsec Rekey Interval	Specify the interval for refreshing IPsec keys. Range: 3600 to 1209600 seconds (1 hour to 14 days) Default: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. Options: 64, 128, 256, 512, 1024, 2048, or 4096 packets. Default: 512

Field	Description
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Options: • AES 256 CBC SHA1 • AES 256 CBC SHA 384 • AES 256 CBC SHA 256 • AES 256 CBC SHA 512 • AES 256 GCM Default: AEM 256 GCM
Perfect Forward Secrecy	Specify the Perfect Forward Secrecy (PFS) settings to use on the IPsec tunnel. Choose one of the following Diffie-Hellman prime modulus groups: • Group-2 1024-bit modulus • Group-14 2048-bit modulus • Group-15 3072-bit modulus • Group-16 4096-bit modulus • None: disable PFS

Step 5 Configure High Availability. To designate active and back-up tunnels and distribute traffic among tunnels, click **High Availability** and do the following:

a) Click **Add Interface Pair**. In the **Add Interface Pair** pop-up window, configure the following

b) Click Add to save these configurations.

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

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

Step 6 Select the **Region**: When you choose the region, a pair of primary and secondary region is selected. Choose the primary region that Cisco Secure Service Edge provides from the drop-down list and the secondary region is auto-selected in Cisco SD-WAN Manager. If the primary region with a unicast IP address is not reachable then the secondary region with a unicast IP address is reachable and vice versa. Cisco Secure Access ensures that both the regions are reachable at all times.

What to do next

Create Route-Based Traffic Forwarding

After the tunnels are established, relevant traffic should be forwarded to the tunnels. In Cisco IOS XE 17.14.1a, configure traffic forwarding by using the CLI template to add the following command:

ip sdwan route vrf <*network*> <*subnetmask*> **service sse Cisco-Secure-Access**

Example: **ip sdwan route vrf 2 0.0.0.0/0 service sse Cisco-Secure-Access**

Associate the SSE Policy with a Policy Group and Deploy the Policy Group to a Device

The SSE policy created earlier needs to be associated with a Policy Group and later associated with a device for the policy to work on that device.

Step 1 On the SD-WAN Manager go to **Configuration** > **Policy Groups** > **Add Policy Group** to create a new policy group for sd-routing devices.

Step 2 Select the **Action** button and under **Policy** select the **SSE Policy** created earlier from the available policies.

Step 3 Click **Save** to create an association between the SSE Policy and the Policy Group. This association ensures that the SSE policy is now part of the Policy Group.

Step 4 Associate the Policy Group to the device. This association ensures that when you deploy this Policy group to a device, the device inherits all the policies associated with this Policy Group.

Step 5 Deploy the Policy Group to the device. Your device is now ready to use the SSE tunnels.

What to do next

Verify Cisco Secure Access Tunnels

To view information about the Cisco Secure Access tunnels that you have configured for the SD-Routing device, use the **show sse all** command.

```
Device# show sse all

************************************
   SSE  Instance Cisco-Secure-Access
************************************
Tunnel name : Tunnel15000001
Site id: 2678135102
Tunnel id: 617865691
SSE tunnel name: C8K-63a9b72b-f1fa-4973-a323-c36861cf59ee
HA role: Active
Local state: Up
Tracker state: Up
Destination Data Center: 52.42.220.205
Tunnel type: IPSEC
Provider name: Cisco Secure Access
```

Monitor and Troubleshoot Cisco Secure Access Tunnels from SD-WAN Manager

The following sections show how to identify issues with the SSE tunnels and take corrective measures.

Monitoring SSE Tunnel State Using Cisco SD-WAN Manager

Monitor the state of the SSE tunnels using the following options in Cisco SD-WAN Manager:

- **Monitor** > **Security** > **SIG/SSE Tunnel** dashboard to view information about:
  - Down Tunnels
  - Degraded Tunnels: Degraded state indicates that the SSE 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.
  - Up Tunnels

- **Monitor** > **Tunnels** > **SIG/SSE Tunnel** to view information about :

  Data plane tunnels, tunnel end points, and health of the tunnel

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

Field	Description
Host Name	Host name of the SD-Routing device.

Field	Description
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
Tunnel Name	Unique name for the tunnel that can be used to identify the tunnel at both the local and remote ends. On the SSE provider portal, you can use the tunnel name to find details about a particular tunnel.
HA Pair	Active or Backup
Provider	Cisco Secure Access
Destination Data Center	SIG/SSE provider data center to which the tunnel is connected.
Tunnel Status (Local)	Tunnel status as perceived by the device.
Tunnel Status (Remote)	Tunnel status as perceived by the SIG/SSE endpoint.
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.
Tracker	Enabled or disabled during tunnel configuration.

Monitoring and Troubleshooting Using Commands

This section provides details on how to identify and troubleshoot SSE tunnel issues from device commands.

Troubleshooting Using Device Notifications

Note Accessing the device shell needs a consent token. Consent Token is a security feature that is used to authenticate the network administrator of an organization to access system shell with mutual consent from the network administrator and Cisco Technical Assistance Centre (Cisco TAC).

To view information about a device on which an event was generated use the following steps:

1. Execute the **/opt/confd/bin/confd_cli -C -P 3010 -noaaa -g sdwan-oper** command. This command gives you access to the shell to run commands to view device notifications.
2. Execute **show notification stream viptela** command to view the device notifications

Device**#show notification stream viptela**

```
notification
 eventTime 2023-11-09T06:21:19.95062+00:00
 sse-tunnel-params-absent
  severity major
  host-name vm6
  if-name TunnelSSE
  wan-if-ip 192.1.2.8
```

Troubleshooting Using Crypto Session Details

Execute **show crypto session** command to view the crypto session details

Device**#show crypto session**

```
Interface: Tunnel15000010
Profile: if-ipsec10-ikev2-profile
Session status: UP-ACTIVE
Peer: 3.76.88.203 port 4500
  Session ID: 7
  IKEv2 SA: local 10.1.15.15/4500 remote 3.76.88.203/4500 Active
  IPSEC FLOW: permit ip   0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
```

Troubleshooting Using Interface Details

Execute the **show interface brief** command. This command displays the interface details.

Device**#show interface brief**

```
Tunnel15000010         10.1.15.15      YES TFTP   up    up
```

Troubleshooting Using Endpoint Tracker Details

Execute the **show endpoint tracker** command. This command displays all the endpoint tracker details.

Device**#show endpoint-tracker**

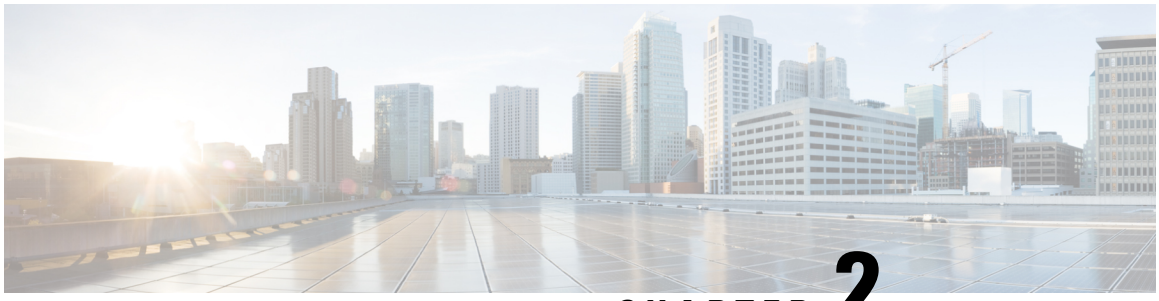
```
Interface                       Record Name            Status        Address Family   RTT
 in msecs    Probe ID   Next Hop
Tunnel16000002                  DefaultTracker         Up            IPv4             22
             20         None
```

Troubleshooting Using Tunnel Details

Execute the **show running config|sec sse** command. This command displays the tunnel and vrf details.

Device**#show running config|sec sse**

```
sse instance Cisco-Secure-Access
  ha-pairs
   interface-pair Tunnel15000010 active-interface-weight 1 None backup-interface-weight 1
!
ip sdwan route vrf 2 0.0.0.0/0 service sse Cisco-Secure-Access
```



CHAPTER 2

Overview of SSL/TLS Proxy

Today more and more apps and data reside in the cloud. As a result, majority of internet traffic is encrypted. This may lead to malware remaining hidden and lack of control over security. The TLS proxy feature allows you to configure edge devices as transparent TLS proxy. This allows the devices to identify risks that are otherwise hidden by end-to-end encrypted TLS channel. The data is re-encrypted post inspection before being sent to its destination.

Feature Name	Release Information	Description
Configure an SD-Routing Device as an SSL/TLS Proxy	Cisco IOS XE 17.14.1a	This feature allows you to configure an autonomous device as a transparent SSL/TLS proxy. These proxy devices can then decrypt incoming and outgoing TLS traffic to enable their inspection and identify risks that are hidden by end-to-end encryption.

Traffic Flow with TLS Proxy

A typical TLS handshake involves authentication using certificates signed by trusted, third-party Certificate Authorities (CAs). The clients and servers must trust these CAs in order to establish trust. TLS Proxy acts as MitM and runs a CA to issue proxy certificates for the connection dynamically.

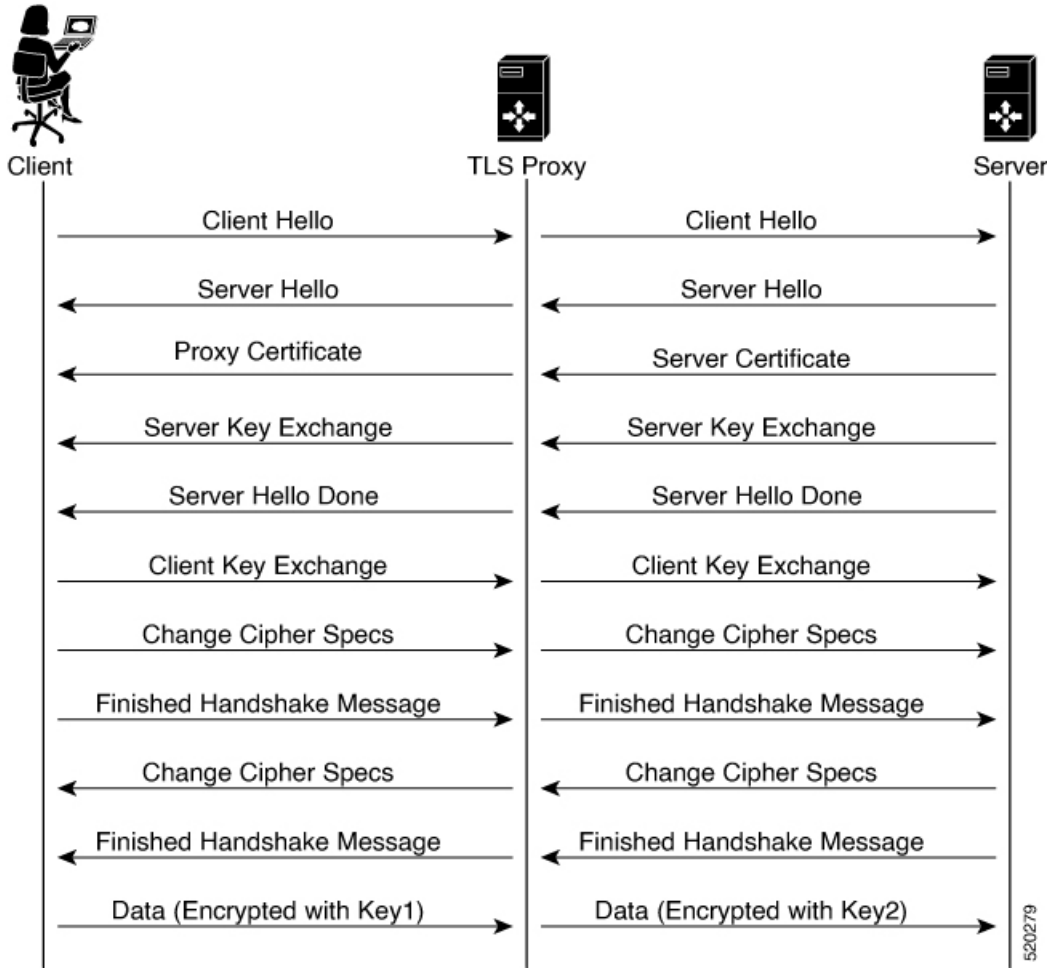
This is how traffic flows when TLS proxy is enabled:

1. A TCP connection is established between the client and the proxy, and the proxy and the server.
2. If a decryption policy is enabled for the flow, a client Hello packet is sent to the server to determine the decryption action.
3. Based on the decryption policy, one of the following actions takes place:
   - **drop:** If the verdict is drop, the hello packet from the client is dropped and the connection is reset.
   - **do-not-decrypt:** If the verdict is do-not-decrypt, the hello packet bypasses TLS proxy.

- **decrypt:** If the verdict is decrypt, the packet is forwarded to the client and goes through the following:
  a. TCP optimization for optimization of traffic
  b. Decryption of encrypted traffic through TLS proxy
  c. Re-encryption of decrypted traffic through TLS proxy

The following image shows the TLS handshake process

Figure 1: The Process of TLS Handshake



Supported Cipher Suites

The TLS Proxy feature supports the following cipher suites.

Table 3: Ciphers Supported for TLS Proxy

TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256	TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_SEED_CBC_SHA	TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_RSA_WITH_AES_128_GCM_SHA256	TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	

Benefits of TLS Proxy

- Monitoring of TLS traffic for any threats through transparent inspection
- Enforcement of security polices based on the inspection of the decrypted traffic
- Threat and malware protection for TLS traffic

Limitations TLS Proxy

- Only RSA and its variant cipher suites are supported.
- Certificate Revocation List (CRL) check is not supported for server certificate validation. However, you can enable OCSP from Advanced Settings in SSL Decryption policy.
- OCSP stapling is not supported and must be explicitly disabled on the browser for the TLS session to be established.
- IPv6 traffic is not supported.
- TLS session resumption, renegotiation and client certificate authentication are not supported.
- If TLS proxy crashes, it takes up to two minutes for it to be ready to serve as proxy for TLS flows again. During this time, depending upon your security settings, the flows are either bypassed or dropped.

Supported Devices and Device Requirements

The following devices support the SSL/TLS Proxy feature.

Table 4: Supported Devices and Releases

Release	Supported Devices
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	• Cisco Catalyst 8000V Edge Software • Cisco Catalyst 8300 Series Edge Platforms

Minimum Device Requirements

- The device must have a minimum of 8 GB of DRAM; 16 GB for Cisco Catalyst 8300 Series Edge Platforms.
- The device must have a minimum of 8 vCPUs.

Workflow to Set Up TLS Proxy for SD-Routing Devices

This workflow outlines the high-level steps required to set up TLS Proxy for SD-Routing devices using SD-WAN Manager. The detailed instructions are covered in the following sections.

Task	Description
Set up Time Synchronization	
Set up time synchronization between the Certificate Authority (CA) server and the device seeking the certificate.	Go to **Configuration** > **Configuration Groups** Select **System Profile** in SD-WAN Manager. Enter details to configure NTP.
Set up Certificate Authority	
Determine how to configure the CA server.	A CA issues SSL certificates to verify the authenticity and establish trust between a client and server. You can configure a CA using one of the following options: • Enterprise CA • Enterprise CA with SCEP • Cisco SD-WAN Manager as CA • Cisco SD-WAN Manager as Intermediate CA
Select devices to be configured as TLS Proxy	
Create a Configuration Group in Cisco SD-WAN Manager and associate it to the WAN edge device.	Helps to form a logical grouping of features or configurations that can be applied to one or more devices in the network.
Configure Security Policies	

Task	Description
Configure an embedded firewall security policy for inspection, prevention and decryption.	Go to **Configuration** > **Policy Groups** > **Embedded Security** > **Add Security Policy** and follow the steps to configure the security policy.
Configure additional parameters for TLS traffic decryption.	**Create an inline TLS Decryption Security Policy** Add additional parameters to the Embedded Security policy created above. To do that, select the Embedded Policy created above, go to **Additional Settings** and create a TLS/SSL Decryption policy and associate this with the Embedded Security Policy that you created above. OR **Create a Security Policy using Group of Interest** Go to **Configuration** > **Policy Groups** > **Group of Interest** > **Security**, add **TLS/SSL Decryption Policy** and follow the steps to configure the security policy. Next associate this with the Embedded Security Policy created above.
Associate the TLS Decryption Policy with a Device	
1. Associate the Embedded Security Policy (has the associated TLS/SSL Decryption Policy) to a Policy Group **2.** Associate the Policy Group with the device **3.** Deploy the device	Go to **Configuration** > **Policy Group** > **Add Policy Group**. Select the Embedded Security policy (has the associated TLS/SSL Decryption policy) and click **Save** to associate the policy with the Policy Group. Next, associate the policy group to a device and delpoy the device.
Verify the TLS Proxy Configuration	Use the following commands to verify the configuration of SSL/TLS Proxy: • **show sd-routing running** • **show sd-routing running-config** • **show crypto pki status** • **show sslproxy statistics** • **show sslproxy status** • **show platform hardware qfp active feature utd config** • **show sd-routing running-configuration|section utd-tls-decrypt** • **show utd engine standard config** • **show utd engine standard status**

Configure Time Synchronization

Set up time synchronization between the CA server and the device seeking the certificate.

Step 1 Click **Configuration** > **Configuration Groups** . Select **System Profile** and enter the following details.

Field	Description
Add Server	
Hostname/IP address	Enter the IP address of an NTP server, or a DNS server that knows how to reach the NTP server.
VRF to reach NTP Server*	Enter the VRF name used to reach the NTP server, can be up to 32 alphanumeric characters
Set authentication key for the server	Specify the MD5 key associated with the NTP server, to enable MD5 authentication. For the key to work, you must mark it as trusted in the **Trusted Key** field under **Authentication**.
Set NTP version	Enter the version number of the NTP protocol software. Range: 1 to 4 Default: 4
Set interface to use to reach NTP server	Enter the name of a specific interface to use for outgoing NTP packets. The interface must be located in the same VPN as the NTP server. If it is not, the configuration is ignored.
Prefer this NTP server*	Enable this option if multiple NTP servers are at the same stratum level and you want one to be preferred. For servers at different stratum levels, Cisco SD-Routing chooses the one at the highest stratum level.

Step 2 Save these details.

Configure Certificate Authority

The following CA options are supported for configuring TLS proxy :

- Enterprise CA, on page 19
- Enterprise CA with SCEP, on page 19
- Cisco SD-WAN Manager as CA, on page 20
- Cisco SD-WAN Manager as Intermediate CA, on page 21

The following sections cover the benefits and limitations of each of the supported CA options to help you make an informed decision about choosing the CA for TLS proxy.

Enterprise CA

Use this option to manage issuing certificates through an Enterprise CA or your own internal CA. For Enterprise CA that does not support Simple Certificate Enrollment Protocol (SCEP), manual enrollment is required.

Manual enrollment involves downloading a Certificate Signing Request (CSR) for your device, getting it signed by your CA, and then uploading the signed certificate to the device through Cisco SD-WAN Manager

Table 5: Enterprise CA: Benefits and Limitations

Benefits	Limitations
• Can use your existing enterprise CA and certificate management infrastructure for monitoring the usage, expiry, and validity of certificates • The client trust-store need not be updated • Provides a single location for managing all certificates issued • Certificates can be revoked and tracked through your own CA	• Maintenance creates an administrative overload. • Manual certificate deployment is required for TLS proxy • Out-of-band management is required for tracking the usage and expiry of certificates • Requires manual re-issuance of expired proxy certificates • If an enterprise CA certificate is revoked or compromised, all certificates it issued are invalidated

Configure Enterprise CA

Note When configuring TLS/SSL proxy feature, trust point allows only two certificates; root certificate and certificate signed by root certificate. You cannot upload cert chain.

1. Download a CA certificate from your CA server in PEM or Base 64 format.
2. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificate Authority**.
3. Choose **Enterprise CA.**
4. To upload your PEM-encoded CA certificate. click **Select a file**.

   OR

   Paste the CA certificate in the Root Certificates box.
5. Verify that the fingerprint, which auto-populates after you upload the certificate, matches your CA.
6. Click **Save Certificate Authority**.
7. Configure a Firewall Policy to Inspect and Decrypt TLS Traffic , on page 23.

Enterprise CA with SCEP

Simple Certificate Enrollment Protocol (SCEP) is an open source protocol that is widely used to make digital certificate issuance easier, more secure, and scalable. Use this option to manage issuing certificates through

an Enterprise CA or your own internal CA. If your CA supports SCEP, you can configure it to automate the certificate management process.

Table 6: Enterprise CA with SCEP: Benefits and Limitations

Benefits	Limitations
• Can use your existing enterprise CA and certificate management infrastructure for monitoring the usage, expiry, and validity of certificates • The client trust-store need not be updated • Provides a single location for managing all certificates issued • Certificates can be revoked and tracked through your own CA • Certificate deployment to TLS Proxy can be automated	• Maintenance creates an administrative overload. • If an enterprise CA certificate is revoked or compromised, all certificates it issued are invalidated • Offers limited visibility through Cisco SD-WAN Manager • Enterprise CA have limited support for SCEP

Configure Enterprise CA with SCEP

1. Download a CA certificate from your CA server in PEM or Base 64 format.
2. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificate Authority**.
3. Choose **Enterprise CA.**
4. [Optional,but recommended] Check the **Simple Certificate Enrollment Protocol (SCEP)** check box.
5. Enter the SCEP server URL in the **URL Base** field.
6. [Optional] Enter the **Challenge Password/Phrase** if you have one configured.

Note If Enterprise CA is configured with SCEP, the Enterprise SCEP CA server should be reachable from the VRF.

7. To upload your PEM-encoded CA certificate. click **Select a file**

   OR

   Paste the CA certificate in the **Root Certificates** box.
8. Click **Save Certificate Authority**.
9. Configure a Firewall Policy to Inspect and Decrypt TLS Traffic , on page 23

Cisco SD-WAN Manager as CA

Use this option to manage issuing certificates through an Enterprise CA or your own internal CA. For Enterprise CA that does not support Simple Certificate Enrollment Protocol (SCEP), manual enrollment is required.

Table 7: Cisco SD-WAN Manager as CA: Benefits and Limitations

Benefits	Limitations
• Certificate deployment to proxy devices is automated • Certificates are reissued and revalidated before they expire • Certificates can be monitored, tracked, and validated through Cisco SD-WAN Manager	• Cisco SD-WAN Manager certificate needs to be pushed to the client trust store

Configure Cisco SD-WAN Manager as CA

Use **SD-WAN Manager as CA** if your enterprise does not have an internal CA. With this option, Cisco SD-WAN is used as a root CA and is authorized to issue subordinate CAs to the proxy devices at the edge of the network. The certificates issued by the CA can be managed through Cisco SD-WAN Manager .

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificate Authority**.
2. Choose **SD-WAN as CA**

Note Leave the **Set SD-WAN as Intermediate CA** check box not checked if you want to set SD-WAN Manager as CA.

3. Enter the requested details: Common Name, Organization, Organizational Unit, Locality, State/Province, Country Code, and Email.
4. Choose the certificate validity period from the drop-down list.
5. Click **Save Certificate Authority**.
6. Configure a Firewall Policy to Inspect and Decrypt TLS Traffic , on page 23.

Cisco SD-WAN Manager as Intermediate CA

Use this option if you have an internal enterprise CA, but would like to use Cisco SD-WAN Manager as intermediate CA to issue and manage subordinate CA certificates.

Table 8: CiscoSD-WAN Manager as Intermediate CA: Benefits and Limitations

Benefits	Limitations

• Certificate deployment to proxy devices is automated • Certificate sare reissued and revalidated before they expire • The risk associated with certificates being compromised is limited as compromised proxy certificates are revoked • Certificates can be monitored, tracked, and validated through Cisco SD-WAN Manager • No other certificates, besides your enterprise CA certificate, need to be pushed to your client trust-store	• Requires manual deployment • Maintaining two CAs causes administrative overload • Cisco SD-WAN Manager certificate usage is tracked through the enterprise CA • Deployment can be complex if your network has multiple Cisco SD-WAN Manager controllers for clusteringor redundancy

Configure SD-WAN Manager as Intermediate CA

Configure Cisco SD-WAN Manager as Intermediate CA to enable a TLS proxy device to use subordinate CA certificates issued by the Cisco SD-WAN Manager .

When Cisco SD-WAN Manager is set as intermediate CA, your enterprise CA acts as the root CA and is designated as the preferred intermediate CA to issue and manage subordinate CA certificates for a proxy device. This option is suitable for enterprises that have their own internal CA but would like to use Cisco SD-WAN Manager to automate and manage certificate issuance and renewal.

1. From the menu, choose **Configuration** > **Certificate Authority**.
2. Choose **SD-WAN Manager as CA.**
3. Check the **Set SD-WAN as Intermediate CA** check box.
4. Upload the CA certificate using the **Select a file** option.

   OR

   Paste the content of the PEM-encoded CA certificate file in the Root Certificate text box.
5. Click **Next**.
6. Under the Generate CSR area, enter the requested details, and click **Generate CSR**.

   The CSR field on the screen populates with the Certificate Signing Request (CSR).
7. Copy or download the CSR and upload it to the enterprise CA server to get it signed by the CA server as the subordinate CA certificate.

Note The process to get a CSR signed by a CA server may differ from one CA to another. Follow your standard procedure to get a CSR signed by your CA.

8. Click **Save Certificate Authority**.

9. Configure a Firewall Policy to Inspect and Decrypt TLS Traffic , on page 23.

Upload a Subordinate CA Certificate to TLS Proxy

When Cisco SD-WAN Manager is set as intermediate CA, your enterprise CA acts as the root CA and Cisco SD-WAN Manager is designated as the preferred intermediate CA to issue and manage subordinate CA certificates for a proxy device. This option is suitable for enterprises that have their own internal CA but would like to use Cisco SD-WAN Manager to automate and manage certificate issuance and renewal.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificate Authority**.
2. Check the **Set vManage as Intermediate CA**checkbox.
3. To upload your PEM-encoded CA certificate. click **Select a file**

   OR

   Paste the CA certificate in the **Root Certificates** box.

   Click **Next**.
4. In the **Intermediate Certificate** text box, paste the content of the signed Cisco SD-WAN Manager certificate, and click **Upload**.

   OR

   Click **Select a file** and upload the CSR generated in the previous step, and click **Upload**
5. Verify that the **Finger Print**, which auto-populates after you upload the CSR, matches your CA certificate.
6. Click **Save Certificate Authority.**

Note When a Cisco public key (PKI) certificate is installed on a device, and you want to make changes to the certificate, detach the embedded security policy from the policy group and push the policy group to the device. This will remove the existing PKI certificate and configuration. After you have made changes to the PKI certificate, re-attach the embedded security policy and then push the policy group to the device. This process updates the device for any the changes to the Cisco PKI certificate

Add Devices to a Configuration Group

Add devices to a Configuration Group.

Step 1 Click **...** adjacent to the configuration group name and choose **Edit** >

Step 2 Click **Associated Devices** and then click **Add Devices**

Step 3 Follow the instructions. The selected devices are listed in the **Devices** table.

Configure a Firewall Policy to Inspect and Decrypt TLS Traffic

Configure a firewall policy that defines the conditions to be met for traffic to flow between zones.

Step 1 From the Cisco SD-WAN Manager menu, go to **Configuration** > **Policy Groups** > **Embedded Security** > **Add Security Policy** and follow the steps to configure the firewall policy.

Step 2 **Create a sub-policy for source and destination zone**:

Zones establish the security borders of your network. A zone defines a boundary where traffic is subjected to policy restrictions as it crosses to another region of your network.

Step 3 Create a security policy for inspection, decryption and prevention:

a) **Advanced Inspection Profile:**

An advanced inspection profile is a security inspection profile that includes Cisco UTD security features such as IPS, URLF, AMP, TLS Action, and TLS/SSL Decryption.

b) **Intrusion Prevention:**

This profile when configured detects or stops threats and attacks by flagging suspicious activities.

c) **URL Filtering:**

The URL Filtering profile enables the user to provide controlled access to Internet websites or Intranet sites by configuring the URL-based policies and filters on the device. The user can configure the URL Filtering profiles to manage the web access.

d) **Advanced Malware Protection:**

The AMP profile equips SD-Routing devices to provide protection and visibility to cover all stages of the malware lifecycle.

e) **TLS/SSL Profile:**

This profile lets your configure the action based on the kind of TLS traffic.

f) **TLS/SSL Decryption:**

A decryption policy determines how the system handles encrypted traffic on your network.

The TLS/SSL Decryption Policy can be configured in two ways. You can either configure it from the Embedded Security policy creation page or through the Group of Interest Policy creation page.

Step 4 Click on **Additional Settings** in the Security Policy creation page, to add specific parameters for TLS/SSL decryption.

Step 5 Click **Create New** from the **TLS/SSL Decryption Policy** drop-down to define the decryption policy.

Field Name	Description
Policy Name	Name of the policy. The name can contain a maximum of 32 characters.
Server Certificate Checks	
Expired Certificate	Defines what the policy should do if the server certificate has expired. The options are: • **Drop**: Drop traffic • **Decrypt**: Decrypt traffic

Field Name	Description
Untrusted Certificate	Defines what the policy should do if the server certificate is not trusted. The options are: • **Drop**: Drop traffic • **Decrypt**: Decrypt traffic
Certificate Revocation Status	Defines whether the Online Certificate Status Protocol (OCSP) should be used to check the revocation status of the server certificate. The options are **Enabled** or **Disabled**.
Unknown Revocation Status	Defines what the policy does, if the OCSP revocation status is **unknown**. • **Drop**: Drop traffic • **Decrypt**: Decrypt traffic
Unsupported Mode Checks	
Unsupported Protocol Versions	Defines the unsupported protocol versions. • **Drop**: Drop the unsupported protocol versions. • **Decrypt**: Decrypt the unsupported protocol versions.
Unsupported Cipher Suites	Defines the unsupported cipher suites. • **Drop**: Drop the unsupported cipher suites. • **Decrypt**: Decrypt the unsupported cipher suites.
Failure Mode	Defines the failure mode. The options are close and open.
Certificate Bundle	Check the **Use default CA certificate bundle** checkbox to use the default CA.
Minimum TLS Version	Sets the minimum version of TLS that the proxy should support. The options are: • **TLS 1.0** • **TLS 1.1** • **TLS 1.2**
Proxy Certificate Attributes	

Field Name	Description
RSA Keypair Modules	Defines the Proxy Certificate RSA Key modules. The options are: • **1024 bit RSA** • **2048 bit RSA** • **4096 bit RSA**
Ec Key Type	Defines the key type. The options are: • **P256** • **P384** • **P521**
Certificate Lifetime (in Days)	Sets the lifetime of the proxy certificate, in days.

Alternatively, you can also configure a TLS/SSL Decryption Policy using **Policy Group** > **Group of Interest** and add TLS/SSL Decryption Policy. Ensure that you add this policy to the Embedded policy as indicated in Step 4 above.

Step 6 Save the decryption policy.

Add Security Policy to Policy Group

Associate the Embeded Security Policy created above to the Policy Group. To do so:

Step 1 Click **Policy Group** to create a new policy group. A policy group logically groups policies that can be applied to one or more sites or devices at the site in the network

Step 2 Specify **Policy Group Name** and select solution type as **SD-Routing**. Enter a description for the Policy Group. Click **Create**.

Step 3 Select an embedded security policy from the drop-down list. The embedded security policy includes policies for encryption, firewall, intrusion prevention, URL filtering, and malware.

Step 4 Click **Save** to save your configuration.

Step 5 Click the pencil icon to select a device to associate with the policy group. This association ensures that when you deploy this Policy group to a device, the device inherits all the policies associated with this Policy Group.

Step 6 Click **Deploy** to select sites and deploy the policy group.

Verify TLS Proxy Configuration

Use the following commands to verify the configuration for TLS proxy.

show sd-routing running	In Cisco SD-WAN Manager, run this command in C verify if your configuration is applied.

show sd-routing running-config	In Cisco SD-WAN Manager, run this command the device CLI through SSH
show crypto pki status	On your device CLI, run this command to verify PROXY-SIGNING-CA is present and configure device.
show sslproxy statistics	On your device CLI, run this command to view T
show sslproxy status	On your device CLI, run this command to verify was successfully configured and is enabled on C Manager. In the output , Clear Mode: FALSE denotes that successfully configured and enabled on Cisco S
show platform hardware qfp active feature utd config	On your device CLI, run this command to verify
show sd-routing running-configuration|section utd-tls-decrypt	On your device CLI, run this command to verify
show utd engine standard config	On your device CLI, run this command to verify
show utd engine standard status	On your device CLI, run this command to verify

INDEX