Configure Security Parameters

This section describes how to change security parameters for the control plane and the data plane in the Cisco Catalyst SD-WAN overlay network.

Configure Control Plane Security Parameters

By default, the control plane uses DTLS as the protocol that provides privacy on all its tunnels. DTLS runs over UDP.

You can change the control plane security protocol to TLS, which runs over TCP. The primary reason to use TLS is that, if you consider the Cisco SD-WAN Controller to be a server, firewalls protect TCP servers better than UDP servers.

You configure the control plane tunnel protocol on a Cisco SD-WAN Controller:

```
vSmart(config)# security control protocol tls
```

With this change, all control plane tunnels between the Cisco SD-WAN Controller and the routers and between the Cisco SD-WAN Controller and Cisco SD-WAN Manager use TLS. Control plane tunnels to Cisco Catalyst SD-WAN Validator always use DTLS, because these connections must be handled by UDP.

In a domain with multiple Cisco SD-WAN Controllers, when you configure TLS on one of the Cisco SD-WAN Controllers, all control plane tunnels from that controller to the other controllers use TLS. Said another way, TLS always takes precedence over DTLS. However, from the perspective of the other Cisco SD-WAN Controllers, if you have not configured TLS on them, they use TLS on the control plane tunnel only to that one Cisco SD-WAN Controller, and they use DTLS tunnels to all the other Cisco SD-WAN Controllers and to all their connected routers. To have all Cisco SD-WAN Controllers use TLS, configure it on all of them.

By default, the Cisco SD-WAN Controller listens on port 23456 for TLS requests. To change this:

```
vSmart(config)# security control tls-port number
```

The port can be a number from 1025 through 65535.

To display control plane security information, use the **show control connections** command on the Cisco SD-WAN Controller. For example:

```
vSmart-2# show control connections

                                                                    PEER                  PEER
PEER    PEER     PEER           SITE   DOMAIN  PEER         PEER    PRIVATE  PEER         PUBLIC
TYPE    PROTOCOL SYSTEM IP      ID     ID      PRIVATE IP   PORT    PUBLIC IP    PORT
REMOTE COLOR  STATE  UPTIME
------------------------------------------------------------------------------------------------
vedge   dtls     172.16.255.11  100    1       10.0.5.11    12346   10.0.5.11    12346
lte           up    0:07:48:58
vedge   dtls     172.16.255.21  100    1       10.0.5.21    12346   10.0.5.21    12346
lte           up    0:07:48:51
vedge   dtls     172.16.255.14  400    1       10.1.14.14   12360   10.1.14.14   12360
lte           up    0:07:49:02
vedge   dtls     172.16.255.15  500    1       10.1.15.15   12346   10.1.15.15   12346
default       up    0:07:47:18
vedge   dtls     172.16.255.16  600    1       10.1.16.16   12346   10.1.16.16   12346
default       up    0:07:41:52
vsmart  tls      172.16.255.19  100    1       10.0.5.19    12345   10.0.5.19    12345
default       up    0:00:01:44
vbond   dtls     -              0      0       10.1.14.14   12346   10.1.14.14   12346
default       up    0:07:49:08

vSmart-2# control connections

                                                                    PEER                  PEER
PEER     PEER     PEER           SITE   DOMAIN  PEER         PEER    PRIVATE  PEER         PUBLIC
TYPE     PROTOCOL SYSTEM IP      ID     ID      PRIVATE IP   PORT    PUBLIC IP    PORT
 REMOTE COLOR  STATE   UPTIME
------------------------------------------------------------------------------------------------
vedge    tls      172.16.255.11  100    1       10.0.5.11    12345   10.0.5.11    12345
 lte           up     0:00:01:18
vedge    tls      172.16.255.21  100    1       10.0.5.21    12345   10.0.5.21    12345
 lte           up     0:00:01:18
vedge    tls      172.16.255.14  400    1       10.1.14.14   12345   10.1.14.14   12345
 lte           up     0:00:01:18
vedge    tls      172.16.255.15  500    1       10.1.15.15   12345   10.1.15.15   12345
 default       up     0:00:01:18
vedge    tls      172.16.255.16  600    1       10.1.16.16   12345   10.1.16.16   12345
 default       up     0:00:01:18
vsmart   tls      172.16.255.20  200    1       10.0.12.20   23456   10.0.12.20   23456
 default       up     0:00:01:32
vbond    dtls     -              0      0       10.1.14.14   12346   10.1.14.14   12346
 default       up     0:00:01:33
```

Configure DTLS in Cisco SD-WAN Manager

If you configure the Cisco SD-WAN Manager to use TLS as the control plane security protocol, you must enable port forwarding on your NAT. If you are using DTLS as the control plane security protocol, you do not need to do anything.

The number of ports forwarded depends on the number of vdaemon processes running on the Cisco SD-WAN Manager. To display information about these processes and about and the number of ports that are being forwarded, use the **show control summary** command shows that four vdaemon processes are running:

```
vManage# show control summary
          VBOND     VMANAGE    VSMART    VEDGE
INSTANCE  COUNTS    COUNTS     COUNTS    COUNTS
-------------------------------------------------
0           2           0          2        7
1           2           0          0        5
2           2           0          0        5
3           2           0          0        4
```

To see the listening ports, use the **show control local-properties** command:

```
vManage# show control local-properties

organization-name            Cisco SD-WAN Inc Test
certificate-status           Installed
root-ca-chain-status         Installed

certificate-validity         Valid
certificate-not-valid-before May 20 00:00:00 2015 GMT
certificate-not-valid-after  May 20 23:59:59 2016 GMT

dns-name                     vbond.cisco.com
site-id                      5000
domain-id                    0
protocol                     dtls
tls-port                     23456
...
...
...
number-active-wan-interfaces 1

                PUBLIC       PUBLIC PRIVATE       PRIVATE
  ADMIN  OPERATION LAST
INDEX INTERFACE IP           PORT   IP            PORT    VSMARTS  VMANAGES COLOR  CARRIER
  STATE  STATE     CONNECTION
-------------------------------------------------------------------------------------------------------
0     eth0      72.28.108.37 12361  172.16.98.150 12361   2        0        silver default
  up     up       0:00:00:08
```

This output shows that the listening TCP port is 23456. If you are running Cisco SD-WAN Manager behind a NAT, you should open the following ports on the NAT device:

- 23456 (base - instance 0 port)
- 23456 + 100 (base + 100)
- 23456 + 200 (base + 200)
- 23456 + 300 (base + 300)

Note that the number of instances is the same as the number of cores you have assigned for the Cisco SD-WAN Manager, up to a maximum of 8.

Configure Security Parameters Using the Security Feature Template

Use the Cisco Security feature template for all Cisco IOS XE Catalyst SD-WAN devices. On the edge routers and on Cisco SD-WAN Validator, use this template to configure IPsec for data plane security. On Cisco SD-WAN Manager and Cisco SD-WAN Controller, use the Security feature template to configure DTLS or TLS for control plane security.

Configure Security Parameters

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

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

3. From the Devices list in the left pane, choose a device.

   The templates applicable to the selected device appear in the right pane.
4. Click **Cisco Security** to open the template.
5. In the **Template Name** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
6. In the **Template Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down menu to the left of the parameter field and choose one of the following:

Table 1:

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. You enter the value when you attach a Viptela device to a device template . When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet . To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

Configure Control Plane Security

Note The Configure Control Plane Security section is applicable to Cisco SD-WAN Manager and Cisco SD-WAN Controller only.

To configure the control plane connection protocol on a Cisco SD-WAN Manager instance or a Cisco SD-WAN Controller, choose the **Basic Configuration** area and configure the following parameters:

Table 2:

Parameter Name	Description
Protocol	Choose the protocol to use on control plane connections to a Cisco SD-WAN Controller: • DTLS (Datagram Transport Layer Security). This is the default. • TLS (Transport Layer Security)
Control TLS Port	If you selected TLS, configure the port number to use:*Range:* 1025 through 65535*Default:* 23456

Click **Save**

Configure Data Plane Security

Configure various data plane security parameters under the relevant areas of the template:

Table 3: Basic Configuration

Parameter Name	Description
Rekey Time	Specify how often a device changes the AES key used on its secure DTLS connection to the Cisco SD-WAN Controller. If OMP graceful restart is enabled, the rekeying time must be at least twice the value of the OMP graceful restart timer.*Range:* 10 through 1209600 seconds (14 days) *Default:* 86400 seconds (24 hours)
Replay Window	Specify the size of the sliding replay window. *Values:* 64, 128, 256, 512, 1024, 2048, 4096, 8192 packets. *Default:* 512 packets
Extended Anti Replay	This is turned off by default. Click **On** to turn it on.
IPsec pairwise-keying	This is turned off by default. Click **On** to turn it on.

Table 4: Authentication Type

Parameter Name	Description
Authentication Type	Select the authentication types from the **Authentication List**, and click the arrow pointing right to move the authentication types to the **Selected List** column. Authentication types supported from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a: • **esp**: Enables Encapsulating Security Payload (ESP) encryption and integrity checking on the ESP header. • **ip-udp-esp:** Enables ESP encryption. In addition to the integrity checks on the ESP header and payload, the checks also include the outer IP and UDP headers. • **ip-udp-esp-no-id**: Ignores the ID field in the IP header so that Cisco Catalyst SD-WAN can work in conjunction with the non-Cisco devices. • **none**: Turns integrity checking off on IPSec packets. We don't recommend using this option. Authentication types supported in Cisco IOS XE Catalyst SD-WAN Release 17.5.1a and earlier: • **ah-no-id**: Enable an enhanced version of AH-SHA1 HMAC and ESP HMAC-SHA1 that ignores the ID field in the packet's outer IP header. • **ah-sha1-hmac**: Enable AH-SHA1 HMAC and ESP HMAC-SHA1. • **none**: Select no authentication. • **sha1-hmac**: Enable ESP HMAC-SHA1. **Note** For an edge device running on Cisco IOS XE Catalyst SD-WAN Release 17.5.1a or earlier, you may have configured authentication types using a **Cisco Security** template. When you upgrade the device to Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or later, update the selected authentication types in the **Cisco Security** template to the authentication types supported from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a . To update the authentication types, do the following: 1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**. 2. Click **Feature Templates**. 3. Find the **Cisco Security** template to update and click … and click **Edit**. 4. Click **Update**. Do not modify any configuration. Cisco SD-WAN Manager updates the **Cisco Security** template to display the supported authentication types.

Key Chain and Key ID

To add a new key chain, click **New Key Chain** and specify the following:

Table 5: Key Chain

Parameter Name	Description
Keychain Name	Enter a name for the key chain
Key ID	Specify a key ID

Click **Save**.

Configure Data Plane Security Parameters

In the data plane, IPsec is enabled by default on all routers, and by default IPsec tunnel connections use an enhanced version of the Encapsulating Security Payload (ESP) protocol for authentication on IPsec tunnels. On the routers, you can change the type of authentication, the IPsec rekeying timer, and the size of the IPsec anti-replay window.

Configure Allowed Authentication Types

Authentication Types in Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Later

From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco SD-WAN Release 20.6.1, the following integrity types are supported:

- **esp:** This option enables Encapsulating Security Payload (ESP) encryption and integrity checking on the ESP header.
- **ip-udp-esp:** This option enables ESP encryption. In addition to the integrity checks on the ESP header and the payload, the checks also include the outer IP and UDP headers.
- **ip-udp-esp-no-id:** This option is is similar to ip-udp-esp, however, the ID field of the outer IP header is ignored. Configure this option in the list of integrity types to have the Cisco Catalyst SD-WAN software ignore the ID field in the IP header so that the Cisco Catalyst SD-WAN can work in conjunction with non-Cisco devices.
- **none:** This option turns integrity checking off on IPSec packets. We don't recommend using this option.

By default, IPsec tunnel connections use an enhanced version of the Encapsulating Security Payload (ESP) protocol for authentication. To modify the negotiated interity types, use the following command:

When you change the authentication-type from CLI, the configuration change works well but the new authentication-change doesn't show in the running configuration. We recommend you to change the authentication type to integrity type from Cisco SD-WAN Manager during the template push.

security ipsec integrity-type { **none** | **ip-udp-esp** | **ip-udp-esp-no-id** | **esp** }

Authentication Types Before Cisco IOS XE Catalyst SD-WAN Release 17.6.1a

By default, IPsec tunnel connections use an enhanced version of the Encapsulating Security Payload (ESP) protocol for authentication. To modify the negotiated authentication types, use the following command:

```
Device(config)# security ipsec authentication-type (ah-sha1-hmac | ah-no-id | sha1-hmac |
)
```

By default, IPsec tunnel connections use AES-GCM-256, which provides both encryption and authentication.

Configure each authentication type with a separate **security ipsec authentication-type** command. The command options map to the following authentication types, which are listed in order from most strong to least strong:

Note The `sha1` in the configuration options is used for historical reasons. The authentication options indicate over how much of the packet integrity checking is done. They do not specify the algorithm that checks the integrity. The authentication algorithms supported by Cisco Catalyst SD-WAN do not use SHA1.

- **ah-sha1-hmac** enables encryption and encapsulation using ESP. However, in addition to the integrity checks on the ESP header and payload, the checks also include the outer IP and UDP headers. Hence, this option supports an integrity check of the packet similar to the Authentication Header (AH) protocol. All integrity and encryption is performed using AES-256-GCM.
- **ah-no-id** enables a mode that is similar to **ah-sha1-hmac**, however the ID field of the outer IP header is ignored. This option accommodates some non-Cisco Catalyst SD-WAN devices, including the Apple AirPort Express NAT, that have a bug that causes the ID field in the IP header, a non-mutable field, to be modified. Configure the **ah-no-id** option in the list of authentication types to have the Cisco Catalyst SD-WAN AH software ignore the ID field in the IP header so that the Cisco Catalyst SD-WAN software can work in conjunction with these devices.
- **sha1-hmac** enables ESP encryption and integrity checking.

For information about which data packet fields are affected by these authentication types, see Data Plane Integrity.

Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices advertise their configured authentication types in their TLOC properties. The two routers on either side of an IPsec tunnel connection negotiate the authentication to use on the connection between them, using the strongest authentication type that is configured on both of the routers. For example, if one router advertises the `ah-sha1-hmac` and `ah-no-id` types, and a second router advertises the `ah-no-id` type, the two routers negotiate to use `ah-no-id` on the IPsec tunnel connection between them. If no common authentication types are configured on the two peers, no IPsec tunnel is established between them.

For the unicast traffic, the encryption algorithm on IPSec tunnel connections is AES-256-GCM. From Cisco IOS XE SD-WAN Release 17.2.1r, the multicast traffic also supports AES-256-GCM encryption algorithm. You cannot modify the encryption algorithm choice made by the software.

When the IPsec authentication type is changed, the AES key for the data path is changed.

Change the Rekeying Timer

Before Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices can exchange data traffic, they set up a secure authenticated communications channel between them. The routers use IPSec tunnels between them as the channel, and the AES-256 cipher to perform encryption. Each router generates a new AES key for its data path periodically.

By default, a key is valid for 86400 seconds (24 hours), and the timer range is 10 seconds through 1209600 seconds (14 days). To change the rekey timer value:

```
Device(config)# security ipsec
rekey seconds
```

The configuration looks like this:

```
security
    ipsec
      rekey seconds
    !
```

If you want to generate new IPsec keys immediately, you can do so without modifying the configuration of the router. To do this, issue the **request platform software sdwan security ipsec-rekey** command on the compromised router.

For example, the following output shows that the local SA has a Security Parameter Index (SPI) of 256:

```
Device# show sdwan ipsec local-sa

                                          SOURCE           SOURCE
TLOC ADDRESS     TLOC COLOR       SPI     IP               PORT    KEY HASH
-------------------------------------------------------------------------------
172.16.255.15    lte              256     10.1.15.15       12346   *****b93a
```

A unique key is associated with each SPI. If this key is compromised, use the **request platform software sdwan security ipsec-rekey** command to generate a new key immediately. This command increments the SPI. In our example, the SPI changes to 257 and the key associated with it is now used:

```
Device# request platform software sdwan security ipsec-rekey
Device# show sdwan ipsec local-sa
                                          SOURCE           SOURCE
TLOC ADDRESS     TLOC COLOR       SPI     IP               PORT    KEY HASH
-------------------------------------------------------------------------------
172.16.255.15    lte              257     10.1.15.15       12346   *****b93a
```

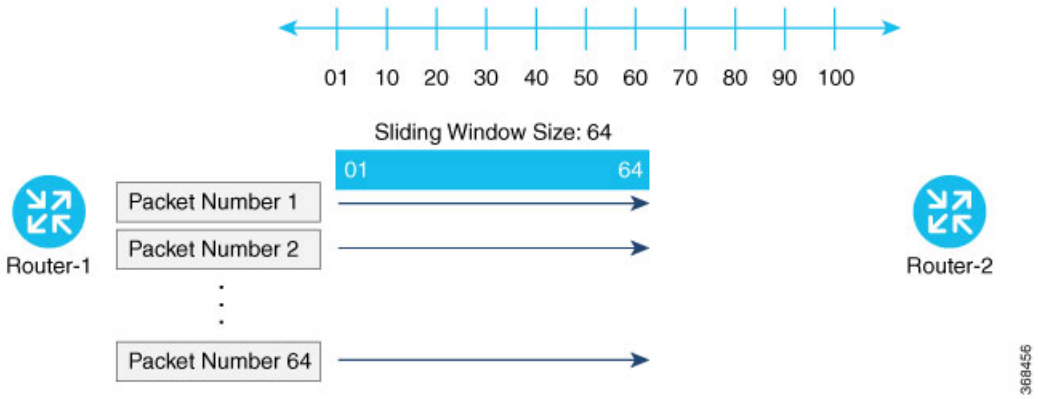
After the new key is generated, the router sends it immediately to the Cisco SD-WAN Controllers using DTLS or TLS. The Cisco SD-WAN Controllers send the key to the peer routers. The routers begin using it as soon as they receive it. Note that the key associated with the old SPI (256) will continue to be used for a short period of time, until it times out.

To stop using the old key immediately, issue the **request platform software sdwan security ipsec-rekey** command twice, in quick succession. This sequence of commands removes both SPI 256 and 257 and sets the SPI to 258. The router then uses the associated key of SPI 258. Note, however, that some packets will be dropped for a short period of time, until all the remote routers learn the new key.

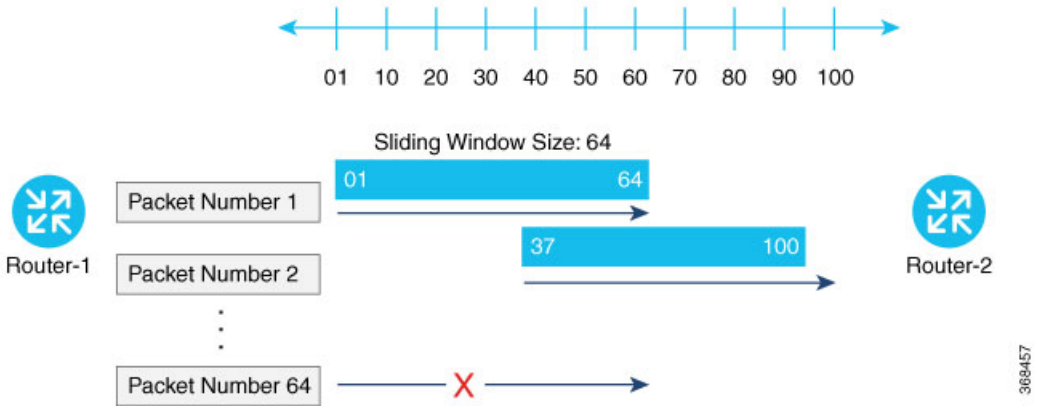
```
Device# request platform software sdwan security ipsec-rekey
Device# request platform software sdwan security ipsec-rekey
Device# show sdwan ipsec local-sa
                                          SOURCE           SOURCE
TLOC ADDRESS     TLOC COLOR       SPI     IP               PORT    KEY HASH
-------------------------------------------------------------------------------
172.16.255.15    lte              258     10.1.15.15       12346   *****b93a
```

Change the Size of the Anti-Replay Window

IPsec authentication provides anti-replay protection by assigning a unique sequence number to each packet in a data stream. This sequence numbering protects against an attacker duplicating data packets. With anti-replay protection, the sender assigns monotonically increasing sequence numbers, and the destination checks these sequence numbers to detect duplicates. Because packets often do not arrive in order, the destination maintains a sliding window of sequence numbers that it will accept.



Packets with sequence numbers that fall to the left of the sliding window range are considered old or duplicates, and the destination drops them. The destination tracks the highest sequence number it has received, and adjusts the sliding window when it receives a packet with a higher value.



By default, the sliding window is set to 512 packets. It can be set to any value between 64 and 4096 that is a power of 2 (that is, 64, 128, 256, 512, 1024, 2048, or 4096). To modify the anti-replay window size, use the **replay-window** command, specifying the size of the window:

```
Device(config)# security ipsec replay-window
number
```

The configuration looks like this:

```
security
   ipsec
     replay-window number
   !
!
```

To help with QoS, separate replay windows are maintained for each of the first eight traffic channels. The configured replay window size is divided by eight for each channel.

If QoS is configured on a router, that router might experience a larger than expected number of packet drops as a result of the IPsec anti-replay mechanism, and many of the packets that are dropped are legitimate ones. This occurs because QoS reorders packets, giving higher-priority packets preferential treatment and delaying lower-priority packets. To minimize or prevent this situation, you can do the following:

- Increase the size of the anti-replay window.
- Engineer traffic onto the first eight traffic channels to ensure that traffic within a channel is not reordered.

VPN Interface IPsec

Use the VPN Interface IPsec feature template to configure IPsec tunnels on Cisco IOS XE service VPNs that are being used for Internet Key Exchange (IKE) sessions. You can configure IPsec on tunnels for VPN 1 through 65530, except for 512.

Cisco Cisco IOS XE Catalyst SD-WAN devices use VRFs in place of VPNs. However, the following steps still apply to configure Cisco IOS XE Catalyst SD-WAN devices through Cisco SD-WAN Manager. In Cisco SD-WAN Manager, the system automatically maps the VPN configurations to VRF configurations.

In controller mode, only Route based IPSec tunnels are supported.

Create VPN IPsec Interface Template

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

Step 2 Click **Feature Templates**.

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

Step 3 Click **Add Template**.

Step 4 Choose a Cisco IOS XE Catalyst SD-WAN device from the list.

Step 5 From the VPN section, click **VPN Interface IPsec**. The Cisco VPN Interface IPsec template displays.

Step 6 In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

Step 7 In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Changing the Scope for a Parameter Value

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (a), and the default setting or value is shown. To change the default or to enter a value, click the **scope** drop-down to the left of the parameter field and choose one of the following:

Parameter Name	Description
 Device Specific	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. Upload the CSV file when you attach a device to a device template. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.
 Global	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

Once you have created and named the template, enter the following values. Parameters marked with an asterisk are required.

Configure IPsec Tunnel Parameters

To configure the IPsec tunnel that carries Internet Key Exchange (IKE) traffic, click IPsec and configure the following parameters:

Parameter Name	Options	Description
IPsec Rekey Interval	3600 - 1209600 seconds	Specify the interval for refreshing IKE keys. Range: 1 hour through 14 days Default: 3600 seconds
IKE Replay Window	64, 128, 256, 512, 1024, 2048, 4096, 8192	Specify the replay window size for the IPsec tunnel. Default: 512
IPsec Cipher Suite	aes256-cbc-sha1 aes256-gcm null-sha1	Specify the authentication and encryption to use on the IPsec tunnel Default: aes256-gcm

Parameter Name	Options	Description
Perfect Forward Secrecy	**2** 1024-bit modulus **14** 2048-bit modulus **15** 3072-bit modulus **16** 4096-bit modulus **none**	Specify the PFS settings to use on the IPsec tunnel. Choose one of the following Diffie-Hellman prime modulus groups: 1024-bit – group-2 2048-bit – group-14 3072-bit – group-15 4096-bit – group-16 none –disable PFS. *Default*: group-16

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, as part of the security hardening, the weaker ciphers are deprecated. As part of this change, the option to configure Diffie-Hellman (DH) groups 1, 2, and 5 is no longer supported. DH groups are used in IKE to establish session keys and are also available in IPsec as support for perfect forward secrecy.

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

CLI Equivalent

```
crypto
   ipsec
      profile ipsec_profile_name
         set ikev2-profile ikev2_profile_name
         set security-association
            lifetime {seconds 120-2592000 | kilobytes disable}
            replay {disable | window-size {64 | 128 | 256 | 512 | 1024 | 4096 | 8192}
         set pfs group {2 | 14 | 15 | 16 | none}
         set transform-set transform_set_name
```

Configure Dead-Peer Detection

To configure Internet key exchange (IKE) dead-peer detection (DPD) to determine whether the connection to an IKE peer is functional and reachable, click DPD and configure the following parameters:

Parameter Name	Description
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. Range: 10 through 3600 seconds Default: Disabled

Parameter Name	Description
DPD Retries	Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then tearing down the tunnel to the peer. Range: 2 through 60 Default: 3

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

CLI Equivalent

```
crypto
   ikev2
      profile ikev2_profile_name
         dpd 10-3600 2-60 {on-demand | periodic}
```

Configure IKE

Table 6: Feature History

Feature Name	Release Information	Description
SHA256 Support for IPSec Tunnels	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature adds support for `HMAC_SHA256` algorithms for enhanced security.

To configure IKE, click **IKE** and configure the following parameters:

Note When you create an IPsec tunnel on a Cisco IOS XE Catalyst SD-WAN device, IKE Version 1 is enabled by default on the tunnel interface.

IKE Version 1 and IKE Version 2

To configure the IPsec tunnel that carries IKEv1 and IKEv2 traffic, click **IPSEC** and configure the following parameters:

Parameter Name	Options	Description
IKE Version	**1** IKEv1 **2** IKEv2	Enter **1** to choose IKEv1. Enter **2** to choose IKEv2. *Default*: IKEv1 **Note** In IKEv2 Preshared Keys (PSK), the '\' character is not supported and should not be used.

Parameter Name	Options	Description
IKE Mode	**Aggressive mode** **Main mode**	For IKEv1 only, specify one of the following modes: • Aggressive mode - Negotiation is quicker, and the initiator and responder ID pass in the clear. • Establishes an IKE SA session before starting IPsec negotiations. **Note** For IKEv2, there is no mode. **Note** IKE aggressive mode with pre-shared keys should be avoided where possible. Otherwise a strong pre-shared key should be chosen. *Default*: Main mode
IPsec Rekey Interval	3600 - 1209600 seconds	Specify the interval for refreshing IKE keys. *Range*: 1 hour through 14 days *Default*: 14400 seconds (4 hours)
IKE Cipher Suite	• AES 256 CBC SHA 256 • AES 256 CBC SHA 384 • AES 256 CBC SHA 512 • AES 256 CBC SHA 1 • AES 256 GCM • Nul SHA 256 • Nul SHA 384 • Nul SHA 512 • Nul SHA 1	Specify the type of authentication and encryption to use during IKE key exchange. *Default*: AES 256 CBC SHA 1

Parameter Name	Options	Description
IKE Diffie-Hellman Group	**2** **14** **15** **16**	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2. • 1024-bit modulus • 2048-bit modulus • 3072-bit modulus • 4096-bit modulus *Default*: 4096-bit modulus
IKE Authentication	Configure IKE authentication.	
	Preshared Key	Enter the password to use with the preshared key.
	IKE ID for Local End Point	If the remote IKE peer requires a local end point identifier, specify it. *Range*: 1 through 64 characters *Default*: Tunnel's source IP address
	IKE ID for Remote End Point	If the remote IKE peer requires a remote end point identifier, specify it. *Range*: 1 through 64 characters *Default*: Tunnel's destination IP address

Note When you are pushing authentication from Cisco SD-WAN Manager, use the authentication string configured for the source and destination stations in double quotes as special characters are not supported. The string can be up to eight characters long.

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

Change the IKE Version from IKEv1 to IKEv2

To change the IKE version, do the following:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**, and then click **Add Template**.

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

3. Choose the device for which you are creating the template.
4. Click **Basic Configuration**.
5. Use the **shutdown** parameter with the **yes** option (**yes shutdown**) to shut down the tunnel.
6. Remove the ISAKMP profile from the IPsec profile.
7. Attach the IKEv2 profile with the IPsec profile.

Note Perform this step if you already have an IKEv2 profile. Otherwise, create an IKEv2 profile first.

8. Use the **shutdown** parameter with the **no** option (**no shutdown**) to start up the tunnel.

Note You must issue the **shutdown** operations in two separate operations.

Note There is no single CLI for changing the IKE version. You need to follow the sequence of steps listed in the Change the IKE Version from IKEv1 to IKEv2 section.

CLI Equivalents for IKEv1

ISAKMP CLI Configuration for IKEv1

```
crypto
   isakmp
      keepalive 60-86400 2-60 {on-demand | periodic}
      policy policy_num
         encryption {AES128-CBC-SHA1 | AES256-CBC-SHA1}
         hash {sha384 | sha256 | sha}
         authentication pre-share
         group {2 | 14 | 16 | 19 | 20 | 21}
         lifetime 60-86400
      profile ikev1_profile_name
         match identity address ip_address [mask]
         keyring keyring_name
```

IPsec CLI Configuration for IKEv1

```
profile ipsec_profile_name
         set transform-set transform_set_name
         set isakmp-profile ikev1_profile_name
         set security-association
            lifetime {kilobytes disable | seconds 120-2592000}
            replay {disable | window-size [64 | 128 | 256 | 512 | 1024]}
         set pfs group {14 | 16 | 19 | 20 | 21}
   keyring keyring_name
      pre-shared-key address ip_address [mask] key key_string
   ipsec transform-set transform_set_name {esp-gcm 256 | esp-aes 256 [esp-sha384-hmac |
esp-sha256-hmac] mode tunnel
```

Summary Steps

1. enable
2. configure terminal
3. crypto isakmp policy *priority*
4. encryption {des | 3des | aes | aes 192 | aes 256 }
5. hash {sha | sha256 | sha384 | md5 }
6. authentication {rsa-sig | rsa-encr | pre-share }
7. group {1 | 2 | 5 | 14 | 15 | 16 | 19 | 20 | 24 }
8. lifetime *seconds*
9. exit
10. exit

CLI Equivalent for IKE2

```
crypto
   ikev2
      proposal proposal_name
         encryption {3des | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | des}
         integrity {sha256 | sha384 | sha512}
         group {2 | 14 | 15 | 16}
      keyring idev2_keyring_name
         peer peer_name
         address tunnel_dest_ip [mask]
         pre-shared-key key_string
      profile ikev2_profile_name
         match identity remote address ip_address
         authentication {remote | local} pre-share
         keyring local ikev2_keyring_name
         lifetime 120-86400
```

Disable Weak SSH Encryption Algorithms on Cisco SD-WAN Manager

Table 7: Feature History Table

Feature Name	Release Information	Feature Description
Disable Weak SSH Encryption Algorithms on Cisco SD-WAN Manager	Cisco vManage Release 20.9.1	This feature allows you to disable weaker SSH algorithms on Cisco SD-WAN Manager that may not comply with certain data security standards.

Information About Disabling Weak SSH Encryption Algorithms on Cisco SD-WAN Manager

Cisco SD-WAN Manager provides an SSH client for communication with components in the network, including controllers and edge devices. The SSH client provides an encrypted connection for secure data transfer, based on a variety of encryption algorithms. Many organizations require stronger encryption than that provided by SHA-1, AES-128, and AES-192.

From Cisco vManage Release 20.9.1, you can disable the following weaker encryption algorithms so that an SSH client does not use these algorithms:

- SHA-1
- AES-128
- AES-192

Before disabling these encryption algorithms, ensure that Cisco vEdge devices, if any, in the network, are using a software release later than Cisco SD-WAN Release 18.4.6.

Note You cannot change the SSH KEX and cipher algorithms on the Cisco SD-WAN Controller and the Cisco Catalyst SD-WAN Validator through the CLI. It is only supported on Cisco SD-WAN Manager.

Benefits of Disabling Weak SSH Encryption Algorithms on Cisco SD-WAN Manager

Disabling weaker SSH encryption algorithms improves the security of SSH communication, and ensures that organizations using Cisco Catalyst SD-WAN are compliant with strict security regulations.

Disable Weak SSH Encryption Algorithms on Cisco SD-WAN Manager Using CLI

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **SSH Terminal**.
2. Choose the Cisco SD-WAN Manager device on which you wish to disable weaker SSH algorithms.
3. Enter the username and password to log in to the device.
4. Enter SSH server mode.

   ```
   vmanage# config terminal
   vmanage(config)# system
   vmanage(config-system)# ssh-server
   ```

5. Do one of the following to disable an SSH encryption algorithm:
   - Disable SHA-1:
     a. `vmanage(config-ssh-server)# no kex-algo sha1`
     b. `vmanage(config-ssh-server)# commit`

        The following warning message is displayed:

```
The following warnings were generated:
'system ssh-server kex-algo sha1': WARNING: Please ensure all your edges run code
 version > 18.4.6 which negotiates better than SHA1 with vManage. Otherwise those
 edges may become offline.
Proceed? [yes,no] yes
```

c. Ensure that any Cisco vEdge devices in the network are running Cisco SD-WAN Release 18.4.6 or later and enter **yes**.

- Disable AES-128 and AES-192:

a. `vmanage(config-ssh-server)# no cipher aes-128-192`

b. `vmanage(config-ssh-server)# commit`

The following warning message is displayed:

```
The following warnings were generated:
'system ssh-server cipher aes-128-192': WARNING: Please ensure all your edges
run code version > 18.4.6 which negotiates better than AES-128-192 with vManage.
 Otherwise those edges may become offline.
Proceed? [yes,no] yes
```

c. Ensure that any Cisco vEdge devices in the network are running Cisco SD-WAN Release 18.4.6 or later and enter **yes**.

Verify that Weak SSH Encryption Algorithms Are Disabled on Cisco SD-WAN Manager Using the CLI

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **SSH Terminal**.
2. Select the Cisco SD-WAN Manager device you wish to verify.
3. Enter the username and password to log in to the device.
4. Run the following command:

   ```
   show running-config system ssh-server
   ```

5. Confirm that the output shows one or more of the commands that disable weaker encryption algorithms:
   - no cipher aes-128-192
   - no kex-algo sha1