Configure System Logging for Cisco IOS XE SD-WAN Devices

Table 1: Feature History

Feature Name	Release Information	Description
Ability to Send Syslog Messages over TLS	Cisco IOS XE Release Amsterdam 17.2.1r	This feature allows you to transport syslog messages to external configured hosts by establishing a Transport Layer Security (TLS) connection. Using the TLS protocol enables the content of syslog messages to remain confidential, secure, and untampered or unaltered during each hop.

System Logging

System logging operations use a mechanism similar to the UNIX syslog command to record system-wide, high-level operations that occur on Cisco SD-WAN devices in the overlay network. The log levels (priorities) of the messages are the same as standard UNIX commands, and you can configure the priority of syslog messages. Cisco SD-WAN devices can send log messages to a UNIX-style syslog service.

Cisco IOS XE SD-WAN devices and Cisco vEdge devices send syslog messages to syslog servers on configured external hosts using TCP and UDP. When these devices are sending the syslog messages, the messages might transit several hops to reach the output destination. The intermediate networks during the hops might not be trustworthy, be in a different domain, or have a different security level. Therefore, Cisco IOS XE SD-WAN devices now support sending secure syslog messages over the Transport Layer Security (TLS) as per RFC5425. To secure the syslog message content from potential tampering, the TLS protocol is used for certificate exchange, mutual authentication, and ciphers negotiation.

Cisco IOS XE SD-WAN devices supports both mutual and server authentication for sending syslog messages over TLS.

Benefits of Using TLS for Sending Syslog Messages

The benefits of using TLS for sending syslog messages are:

- Confidentiality of message content where each TLS session begins with a handshake between the Cisco IOS XE SD-WAN device and the syslog server. The Cisco IOS XE SD-WAN device and syslog server agree on the specific security key and the encryption algorithms to be used for that session. The TLS session opposes any disclosure of the contents of the syslog message.
- Integrity-checking of the content of each message to disable modifications to a message during transit on a hop-by-hop basis.
- Mutual authentication between the Cisco IOS XE SD-WAN device and syslog server ensures that the syslog server accepts log messages only from authorized clients through certificate exchange.

Configure Logging in Server Authentication for TLS

In server authentication, Cisco IOS XE SD-WAN devices verify the identity of the syslog server. If the syslog server and the certificate are legitimate entities, the device establishes a TLS connection with the server. For implementing server authentication, the syslog server shares the public certificate with the Cisco IOS XE SD-WAN devices.

Prerequisite

Ensure that Cisco IOS XE SD-WAN devices have preinstalled Root Certificate Authority (CA), which you configure using cryptographic module CLIs. See Install Root Certificate Authority on Cisco IOS XE SD-WAN Device for Server Authentication .

To configure TLS profile for syslog server, perform the following steps:

1. Configure Logging Feature Template Using Cisco vManage.
    a. Configure Logging Attributes to Local Disk.
    b. Configure TLS Profile for Server Authentication.
    c. Configure Syslog Servers for TLS.
2. Create a device template from logging feature template.

Configure Logging in Mutual Authentication for TLS

In mutual authentication, both the syslog server and Cisco IOS XE SD-WAN device authenticate each other at the same time. Cisco IOS XE SD-WAN devices must have root or identity certificates for mutual authentication of the TLS session. To configure TLS profile for syslog server, perform the following steps:

1. Install Syslog Root Certificate on Cisco IOS XE SD-WAN Device for Mutual Authentication.
2. Configure Logging Feature Template Using Cisco vManage.
   a. Configure Logging Attributes to Local Disk.
   b. Generate Feature Certificate Signing Request and Install Feature Certificates, on page 16
   c. Configure TLS Profile for Mutual Authentication.
   d. Configure Syslog Servers for TLS.
3. Create a device template from logging feature template.
4. Generate Feature Certificate Signing Request and Install Feature Certificates, on page 16.
5. Verify Trustpoint Configuration on Cisco IOS XE SD-WAN Device.

Syslog Message Format and System Log Files

Syslog messages begin with a percent sign (%) and the two syslog message formats are structured as follows:

- Syslog message format

  seq no:timestamp: %facility-severity-MENEMONIC:description (hostname-n)
- Syslog message format based on RFC5424

  <pri>ver timestamp hostname appname procid msgid structured data description/msg

Note In the syslog message format based on RFC5424, the optional fields such as, hostname, appname, procId, msgId, structured data are specified with a **-**.

The field descriptions of syslog messages are as follows:

Table 2: Field Descriptions of Syslog Message Format

Field	Description
facility	Sets the logging facility to a value other than 20, which UNIX systems expect.

Field	Description
severity	The importance or severity of the message is categorized by the numerical code from 0 through 7. A lower number in this range indicates greater severity of the system condition.
msg or description	A text string that describes the condition of syslog server. This portion of the syslog message sometimes includes IP addresses, interface names, port numbers, or usernames. In syslog message formats based on RFC5424, the description represents: *%facility-severity-MENEMONIC:description*

Usually, the syslog messages are preceded by extra text.

- The following is an example of a system logging message preceded by a priority value, sequence number, and time stamp:

  *<45>10: polaris-user1: *Jun 21 10:76:84.100: %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down*
- Based on RFC5424, the following is an example of a system logging message preceded by a priority value, version of syslog protocol specification, and time stamp:

  <45>1 2003-10-11T22:14:15.003Z 10.64.48.125 polaris-user1 - - - %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down

Note The time stamp formats are not the same in both the syslog message formats. In the message format based on RFC5424, T and Z are mandatory where T represents a separator and Z represents zero timezone.

System Log Files

Syslog messages are recorded on the local device of the syslog server in the `/var/log` directory.

Install Root Certificate Authority on Cisco IOS XE SD-WAN Device for Server Authentication

Before you begin

Ensure that you generate the encoded CA certificate on the syslog server. See Install Root Certificate Authority on Syslog Server for Server Authentication, on page 6.

Step 1 To configure PKI trustpoint for Certificate Authority, use these commands for authorizing and revocation of certificates in PKI.

a) **enable**

Enables privileged EXEC mode.

Example:

```
Cisco XE SD-WAN> enable
```

b) **config-transaction**

Enters the configuration mode.

Example:

```
Cisco XE SD-WAN# config-transaction
```

c) **crypto pki trustpoint** *name*

Declares the trustpoint and a given name and enters CA-trustpoint configuration mode.

Example:

```
Cisco XE SD-WAN  (config)# crypto pki trustpoint Syslog-signing-CA
```

d) **enrollment [mode] [retry period** *minutes*] [**retry count** *number*] **url** url [**pem**]

Specifies the enrollment parameters of the CA.

Example:

```
Cisco XE SD-WAN(ca-trustpoint)# enrollment terminal
```

e) **chain-validation [{stop | continue}[parent-trustpoint]]**

Configures the level to which a certificate chain is processed on all certificates.

Example:

```
Cisco XE SD-WAN(ca-trustpoint)# chain-validation stop
```

f) **revocation-check method**

(Optional) Checks the revocation status of a certificate.

Example:

```
Cisco XE SD-WAN(ca-trustpoint)# revocation-check none
```

g) **exit**

Returns to global configuration mode.

Example:

```
Cisco XE SD-WAN(ca-trustpoint)# exit
```

Step 2 Retrieve and authenticate the Root CA before the Cisco IOS XE SD-WAN device can be issued a certificate and certificate enrollment occurs.

To authenticate the CA, use the **crypto pki authenticate** command.

Example:

```
Cisco XE SD-WAN(config)# crypto pki authenticate root
```

Step 3 Copy the block of text containing the base 64 encoded CA certificate and paste it at the prompt.

To generate and copy the text containing the encoded CA certificate, see Install Root Certificate Authority on Syslog Server for Server Authentication, on page 6.

Example:

A sample base 64 encoded CA certificate:

```
-----BEGIN CERTIFICATE-----
MIID9jCCAt6gAwIBAgIJAM5b3nyjDAKIMA0GCSqGSIb3DQEBCwUAMIGPMQswCQYD
VQQGEwJJTjESMBAGA1UECAwJS2FybmF0YWthMRIwEAYDVQQHDAlCYW5nYWxvcmUx
DjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQLDANDU0cxGzAZBgNVBAMMEmVtYmQtbG54
LmNpc2NvLmNvbTEdMBsGCSqGSIb3DQEJARYOYW5idkBjaXNjby5jb20wHhcNMTkw
OTIwMTQ1NjAxWhcNMjIwOTE5MTQ1NjAxWjCBjzELMAkGA1UEBhMCSU4xEjAQBgNV
BAgMCUthcm5hdGFrYTESMBAGA1UEBwwJQmFuZ2Fsb3JlMQ4wDAYDVQQKDAVDaXNj
bzEMMAoGA1UECwwDQ1NHMRswGQYDVQQDDBJlbWJkLWxueC5jaXNjby5jb20xHTAb
BgkqhkiG9w0BCQEWDmFuYnZAY2lzY28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAuof+Dh8EdAQ7bHJPdnXhy9ibTLAQ+OpQrMBoOqeAsU/Jru8y
3ht2Eqci35aNjlDcsTUlZyUHBNAMtL69t1HxTRVCOghOZmipzOS+q8rFykHa+bcA
FqmHyqxNwdQcW3cQFZ6rvWTFD9O46ONX3xewpdCR+s+0KFOHDd+RxpAb2NyDWIvn
/1/xwq2a4ZlwgM2d0G8sit0i0D/+6FbZuJjAf+PRTypo4IJyQjcOHpZuslLzPztM
HxLI7pOmR+8+WcInT0l0dyGdpKKHXi6lEbeiyubIym0z0Des5OckDYFejXgXpJDx
9jCVkz+r0bijqbT5PMpSAYYcjdnQ0kdH43sykwIDAQABo1MwUTAdBgNVHQ4EFgQU
OcOmN72TyBqD/Ud2qBLUwId1Yv0wHwYDVR0jBBgwFoAUOcOmN72TyBqD/Ud2qBLU
wId1Yv0wDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAUVVWJHWo
rKxfFV2w7jR7mLZSlVtEvZueMXWPvyYP+Qt09MrRqwNDUJEvggTxU7lvLwtnITPM
l/dOmpoer8GhDtnxUnjsVeVWGIR74SJCS0GU/03bEJ2sto/eAJEOzI7wDg7Fubgy
Pc3RHbk4JWTWs4JF8+E64p2UzJMuu0eLDPQWxl7p2wd3sr4DBHB3qlfbg31T3VHr
PCcuzJmOEdeZYGL1/LFvPx7NZS8lwFAohe6h8ptm3ENg7dzIeyZFZVfcq11Q1rer
+3RcM0VqjScIOZhp97dqfBlHEdqUE/QfKlBt12KU+0sj8yJJC+cuKlHQj5JGmGLI
Y6r7bMcn99Y6Rw==
-----END CERTIFICATE-----
```

Step 4 Type **yes** to confirm the acceptance of the certificate.

The Root CA certificate is successfully imported.

What to do next

Configure Logging Feature Template Using Cisco vManage, on page 8

Install Root Certificate Authority on Syslog Server for Server Authentication

In this document, the following steps describe the procedure to set up syslog-ng server that supports TLS.

Step 1 To install syslog-ng on the server, use the following command:

Example:

```
# apt-get install syslog-ng openssl
```

Step 2 To change the directory to syslog-ng folder and create folders to store the root certificates, use the following commands:

Example:

```
# cd /etc/syslog-ng
# mkdir cert.d
# mkdir key.d
# mkdir ca.d
# cd cert.d
# openssl req -new -x509 -out cacert.pem -days 1095 -nodes
# mv privkey.pem ../key.d
```

After using the **openssl** command, an encoded root certificate is available in `cacert.pem` file. The file is located in the `cd/etc/syslog-ng/cert.d` directory.

Step 3 Copy the content from the `cacert.pem` file when installing root certificate on Cisco IOS XE SD-WAN Device. See Step 3 of Install Root Certificate Authority on Cisco IOS XE SD-WAN Device for Server Authentication , on page 4.

What to do next

Install Root Certificate Authority on Cisco IOS XE SD-WAN Device for Server Authentication , on page 4

Install Syslog Root Certificate on Cisco IOS XE SD-WAN Device for Mutual Authentication

To configure Cisco IOS XE SD-WAN devices with Transport Layer Security (TLS) syslog protocol, the devices must have root or identity certificates for mutual authentication of TLS session. You can either use a third-party Certificate Authority (CA) to get public key infrastructure (PKI) services, or Microsoft Active Directory Certificate Services (AD CS). AD CS allows you to build a PKI and provide public key cryptography, digital certificates, and digital signature capabilities for your requirement.

Step 1 Generate the enterprise root certificate using a third party CA or Microsoft Active Directory Certificate Services.

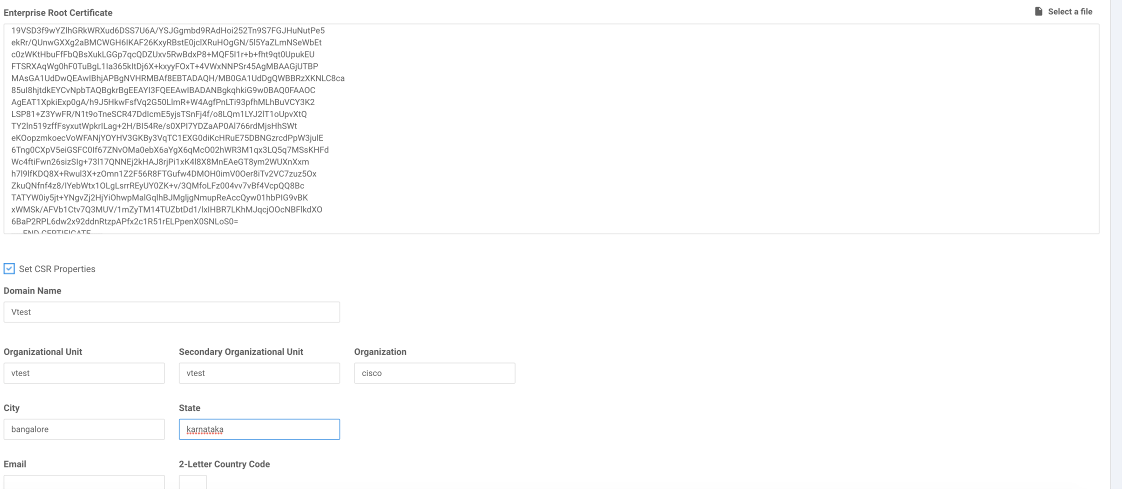
Step 2 Download the root CA in base 64 format, select and copy the content of root CA.

Step 3 In Cisco vManage, click **Administration** > **Settings**.

Step 4 In the **Settings** screen, click **Edit** to the right of the **Enterprise Feature Certificate Authorization**.

Step 5 Paste the root CA content in the **Enterprise Root Certificate** box.

Step 6 (Optional) Check **Set CSR Properties** if you want to generate a Certificate Signing Request (CSR).



Enterprise Root Certificate

```
19VSD3f9wYZlhGRkWRXud6DSS7U6A/YSJGgmbd9RAdHoi252Tn9S7FGJHuNutPe5
ekRr/QUnwGXXg2aBMCWGH6IKAF26KxyRBstE0jclXRuHOgGN/5l5YaZLmNSeWbEt
c0zWKtHbuFfFbQBsXukLGGp7qcQDZUxv5RwBdxP8+MQF5I1r+b+fht9qt0UpukEU
FTSRXAqWg0hF0TuBgL1Ia365kItDj6X+kxyyFOxT+4VWxNNPSr45AgMBAAGjUTBP
MAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBRzXKNLC8ca
85uI8hjtdkEYCvNpbTAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQ0FAAOC
AgEAT1XpkiExp0gA/h9J5HkwFsfVq2G50LlmR+W4AgfPnLTi93pfhMLhBuVCY3K2
LSP81+Z3YwFR/N1t9oTneSCR47DdIcmE5yjsTSnFj4f/o8LQm1LYJ2lT1oUpvXtQ
TY2ln519zffFsyxutWpkrILag+2H/BI54Re/s0XPI7YDZaAP0Al766rdMjsHhSWt
eKOopzmkoecVoWFANjYOYHV3GKBy3VqTC1EXG0diKcHRuE75DBNGzrcdPpW3julE
6Tng0CXpV5eiGSFC0If67ZNvOMa0ebX6aYgX6qMcO02hWR3M1qx3LQ5q7MSsKHFd
Wc4ftiFwn26sizSIg+73l17QNNEj2kHAJ8rjPi1xK4l8X8MnEAeGT8ym2WUXnXxm
h7l9IfKDQ8X+Rwul3X+zOmn1Z2F56R8FTGufw4DMOH0imV0Oer8iTv2VC7zuz5Ox
ZkuQNfnf4z8/IYebWtx1OLgLsrrREyUY0ZK+v/3QMfoLFz004vv7vBf4VcpQQ8Bc
TATYW0iy5jt+YNgvZj2HjYiOhwpMalGqlhBJMgljgNmupReAccQyw01hbPIG9vBK
xWMSk/AFVb1Ctv7Q3MUV/1mZyTM14TUZbtDd1/lxIHBR7LKhMJqcjOOcNBFlkdXO
6BaP2RPL6dw2x92ddnRtzpAPfx2c1R51rELPpenX0SNLoS0=
-----END CERTIFICATE-----
```

☑ Set CSR Properties

Domain Name		
Vtest		
Organizational Unit	Secondary Organizational Unit	Organization
vtest	vtest	cisco
City	State	
bangalore	karnataka	
Email	2-Letter Country Code	

Step 7 Click **Close**.

The root CA is uploaded to Cisco vManage, and Cisco vManage saves the root certificate to the Cisco IOS XE SD-WAN device.

What to do next

Configure Logging Feature Template Using Cisco vManage, on page 8

Configure Logging Feature Template Using Cisco vManage

Step 1 In Cisco vManage, click **Configuration** > **Templates**.

Step 2 In the **Feature** tab, click **Add Template**.

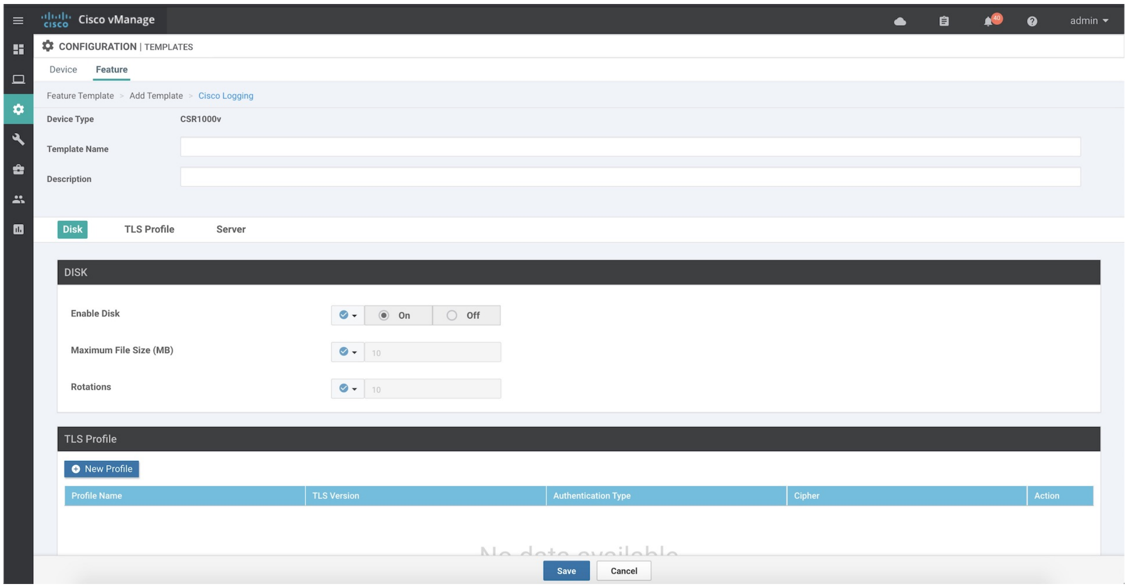
Step 3 From the **Select Devices** drop-down, choose the type of device for which you are creating a template.

Step 4 To create a template for logging, select **Cisco Logging**.

The Cisco Logging template form appears. The top of the form contains fields for naming the template, and the bottom contains fields for defining Logging parameters. Click a tab or the plus sign (+) to display other fields.

When you first open a feature template, the scope is set to **Default** for those parameters that have a default value. The default setting or value appears next to a parameter. To change the default or to enter a value, click the **Scope** drop-down to the left of the parameter field.

Figure 1: Configure Logging Feature Template



Device Type CSR1000v

Template Name

Description

DISK

Enable Disk ● On ○ Off

Maximum File Size (MB) 10

Rotations 10

TLS Profile

Profile Name	TLS Version	Authentication Type	Cipher	Action

No data available

Step 5 In the **Template Name** field, enter a name for the template.

The name may contain up to 128 alphanumeric characters.

Step 6 In the **Template Description** field, enter a description of the template.

The description may contain up to 2048 alphanumeric characters.

What to do next

Configure Logging Attributes to Local Disk, on page 9

Configure Logging Attributes to Local Disk

1. Click **Disk** and configure the following parameters:

Table 3: Parameter Information

Parameter	Description
Enable Disk	To save syslog messages in a file on the local hard disk, click **On**, or click **Off** to disallow saving. By default, logging to a local disk file is enabled on all devices.
Maximum File Size	Enter the maximum size of syslog files. The syslog files are rotated on an hourly basis based on the file size. When the file size exceeds configured value, the file is rotated and the *syslogd* process is notified. Range: 1-20 MB Default: 10 MB
Rotations	Enter the number of syslog files to create before discarding the earliest created files. Range: 1-10 MB Default: 10 MB

2. To save the feature template, click **Save**.
3. To associate the feature template with a device template, see the chapter, Create a Device Template from Feature Templates.

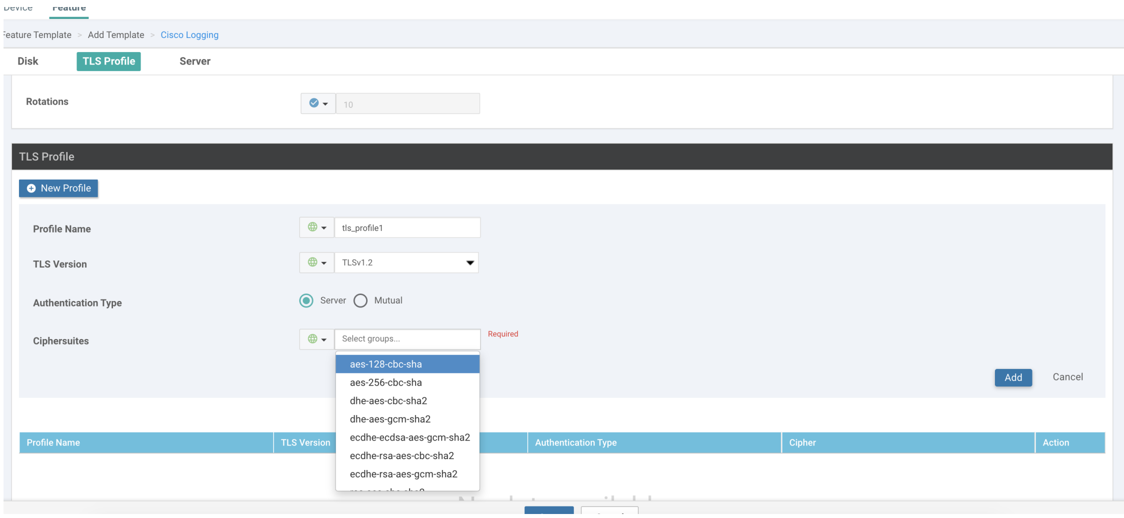
What to Do Next

Configure TLS Profile for Server Authentication, on page 9 or Configure TLS Profile for Mutual Authentication, on page 12

Configure TLS Profile for Server Authentication

1. Click **TLS Profile**.
2. Click **New Profile** and configure the following parameters:

Figure 2: TLS Profile for Server Authentication



Rotations: 10

Profile Name: tls_profile1

TLS Version: TLSv1.2

Authentication Type: ● Server ○ Mutual

Ciphersuites: Select groups... Required

Profile Name	TLS Version	Authentication Type	Cipher	Action

Table 4: Parameter Information

Parameter Name	Description
Profile Name	Enter the TLS profile name
TLS Version	Choose TLS versions v1.1 or v1.2
Authentication Type	Choose authentication types as **Server**.

Parameter Name	Description
Ciphersuites	Choose groups of cipher suites (encryption algorithm) based on the TLS version. The following are the list of cipher suites. • aes-128-cbc-sha Encryption type tls_rsa_with_aes_cbc_128_sha • aes-256-cbc-sha Encryption type tls_rsa_with_aes_cbc_256_sha • dhe-aes-128-cbc-sha Encryption type tls_dhe_rsa_with_aes_128_cbc_sha • dhe-aes-cbc-sha2 Encryption typetls_dhe_rsa_with_aes_cbc_sha2(TLS1.2 & above) • dhe-aes-gcm-sha2 Encryption typetls_dhe_rsa_with_aes_gcm_sha2(TLS1.2 & above) • ecdhe-ecdsa-aes-gcm-sha2 Encryption type tls_ecdhe_ecdsa_aes_gcm_sha2(TLS1.2 & above) SuiteB • ecdhe-rsa-aes-128-cbc-sha Encryption type tls_ecdhe_rsa_with_aes_128_cbc_sha • ecdhe-rsa-aes-cbc-sha2 Encryption type tls_ecdhe_rsa_aes_cbc_sha2(TLS1.2& above) • ecdhe-rsa-aes-gcm-sha2 Encryption type tls_ecdhe_rsa_aes_gcm_sha2(TLS1.2& above) • rsa-aes-cbc-sha2 Encryption type tls_rsa_with_aes_cbc_sha2(TLS1.2 & above) • rsa-aes-gcm-sha2 Encryption type tls_rsa_with_aes_gcm_sha2(TLS1.2 & above)

You can use the following cipher suites for each TLS version:

TLS v1.1

```
aes-128-cbc-sha Encryption type tls_rsa_with_aes_cbc_128_sha
aes-256-cbc-sha Encryption type tls_rsa_with_aes_cbc_256_sha
```

TLS v1.2 and later

```
dhe-aes-cbc-sha2 Encryption type tls_dhe_rsa_with_aes_cbc_sha2(TLS1.2 & above)
dhe-aes-gcm-sha2 Encryption type tls_dhe_rsa_with_aes_gcm_sha2(TLS1.2 & above)

ecdhe-ecdsa-aes-gcm-sha2 Encryption type tls_ecdhe_ecdsa_aes_gcm_sha2 (TLS1.2 & above)
ecdhe-rsa-aes-cbc-sha2 Encryption type tls_ecdhe_rsa_aes_cbc_sha2(TLS1.2 & above)
```

```
ecdhe-rsa-aes-gcm-sha2 Encryption type tls_ecdhe_rsa_aes_gcm_sha2(TLS1.2 & above)

rsa-aes-cbc-sha2 Encryption type tls_rsa_with_aes_cbc_sha2(TLS1.2 & above)
rsa-aes-gcm-sha2 Encryption type tls_rsa_with_aes_gcm_sha2(TLS1.2 & above)
```

The TLS profiles appear in a table.

3. Click **Add** to create another profile.
4. To edit or delete a TLS profile information, click ✎ or 🗑 under **Action**.
5. To save the feature template, click **Save**.
6. To associate the feature template with a device template, see the chapter, Create a Device Template from Feature Templates.

When you choose the authentication type as **Server**, all information about TLS profiles, except the trustpoint information, is saved.

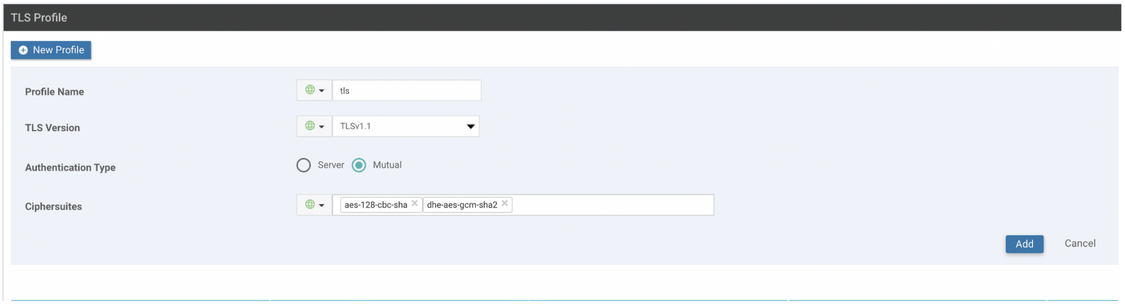
What to Do Next

Configure Syslog Servers for TLS, on page 14

Configure TLS Profile for Mutual Authentication

1. Click **TLS Profile**.
2. Click **New Profile** and configure the following parameters:

Figure 3: Logging Through TLS Profile



Profile Name: tls
TLS Version: TLSv1.1
Authentication Type: ○ Server ● Mutual
Ciphersuites: aes-128-cbc-sha × dhe-aes-gcm-sha2 ×

Table 5: Parameter Information

Parameter Name	Description
Profile Name	Enter the TLS profile name
TLS Version	Choose TLS versions v1.1 or v1.2
Authentication Type	Choose authentication types as **Mutual**.

Parameter Name	Description
Ciphersuites	Choose groups of cipher suites (encryption algorithm) based on the TLS version that must be used for encryption. The following are the list of cipher suites. • aes-128-cbc-sha Encryption type tls_rsa_with_aes_cbc_128_sha • aes-256-cbc-sha Encryption type tls_rsa_with_aes_cbc_256_sha • dhe-aes-128-cbc-sha Encryption type tls_dhe_rsa_with_aes_128_cbc_sha • dhe-aes-cbc-sha2 Encryption typetls_dhe_rsa_with_aes_cbc_sha2(TLS1.2 & above) • dhe-aes-gcm-sha2 Encryption typetls_dhe_rsa_with_aes_gcm_sha2(TLS1.2 & above) • ecdhe-ecdsa-aes-gcm-sha2 Encryption type tls_ecdhe_ecdsa_aes_gcm_sha2(TLS1.2 & above) SuiteB • ecdhe-rsa-aes-128-cbc-sha Encryption type tls_ecdhe_rsa_with_aes_128_cbc_sha • ecdhe-rsa-aes-cbc-sha2 Encryption type tls_ecdhe_rsa_aes_cbc_sha2(TLS1.2& above) • ecdhe-rsa-aes-gcm-sha2 Encryption type tls_ecdhe_rsa_aes_gcm_sha2(TLS1.2& above) • rsa-aes-cbc-sha2 Encryption type tls_rsa_with_aes_cbc_sha2(TLS1.2 & above) • rsa-aes-gcm-sha2 Encryption type tls_rsa_with_aes_gcm_sha2(TLS1.2 & above)

You can use the following cipher suites for each TLS version:

TLS v1.1

```
aes-128-cbc-sha Encryption type tls_rsa_with_aes_cbc_128_sha
aes-256-cbc-sha Encryption type tls_rsa_with_aes_cbc_256_sha
```

TLS v1.2 and later

```
dhe-aes-cbc-sha2 Encryption type tls_dhe_rsa_with_aes_cbc_sha2(TLS1.2 & above)
dhe-aes-gcm-sha2 Encryption type tls_dhe_rsa_with_aes_gcm_sha2(TLS1.2 & above)
```

```
ecdhe-ecdsa-aes-gcm-sha2 Encryption type tls_ecdhe_ecdsa_aes_gcm_sha2 (TLS1.2 & above)
ecdhe-rsa-aes-cbc-sha2 Encryption type tls_ecdhe_rsa_aes_cbc_sha2(TLS1.2 & above)
ecdhe-rsa-aes-gcm-sha2 Encryption type tls_ecdhe_rsa_aes_gcm_sha2(TLS1.2 & above)

rsa-aes-cbc-sha2 Encryption type tls_rsa_with_aes_cbc_sha2(TLS1.2 & above)
rsa-aes-gcm-sha2 Encryption type tls_rsa_with_aes_gcm_sha2(TLS1.2 & above)
```

The TLS profiles appear in a table.

3. Click **Add** to create another profile.
4. To edit or delete a TLS profile information, click ✎ or 🗑 under **Action**.
5. To save the feature template, click **Save**.
6. Associate the feature template with a device template. See the chapter, Create a Device Template from Feature Templates.

The mutually authenticated feature template is saved on the Cisco IOS XE SD-WAN devices, and trustpoint such as, SYSLOG-SIGNING-CA certificate is saved on the device. Cisco vManage can now install the certificate from Cisco IOS XE SD-WAN devices.

What to Do Next

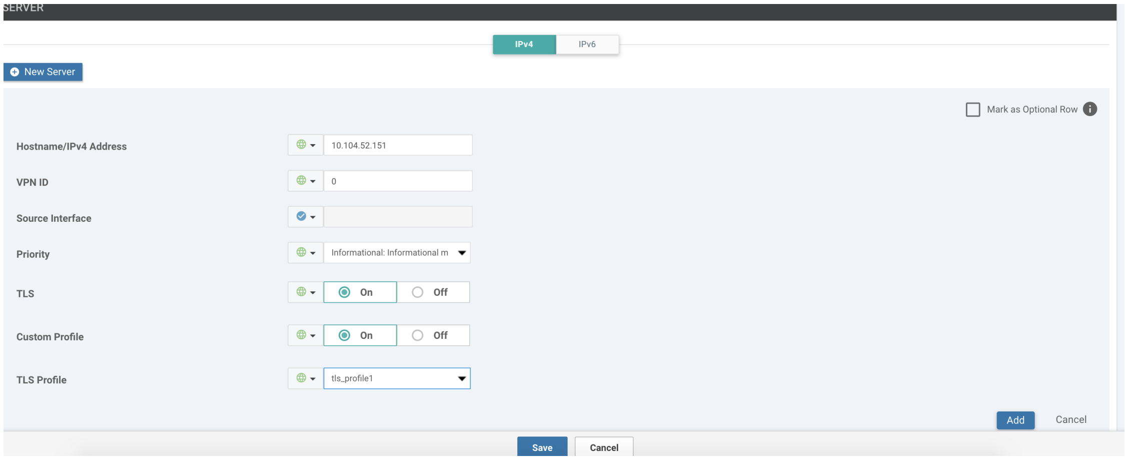
Configure Syslog Servers for TLS, on page 14

Configure Syslog Servers for TLS

To include the TLS profile in IPV6 or IPV4 server configuration,

1. Click the **Server** tab.
2. Click **Add New Server** and configure the following parameters for IPv4 or IPv6:

Figure 4: Logging Through Remote Server



Hostname/IPv4 Address	10.104.52.151
VPN ID	0
Source Interface	
Priority	Informational: Informational m
TLS	● On ○ Off
Custom Profile	● On ○ Off
TLS Profile	tls_profile1

Table 6: Parameter Information

Parameter Name	Description
Hostname/IP Address	Enter the DNS name, hostname, or IPv4, IPv6 address of the system on which to store syslog messages. To add another syslog server, click **+**. To delete a syslog server, click 🗑.
VPN ID	Enter the identifier of the VPN in which the syslog server is located or through which the syslog server can be reached. VPN ID Range: 0-65530
Source Interface	Enter the specific interface to use for outgoing system log messages. The interface must be located in the same VPN as the syslog server. Otherwise, the configuration of syslog servers is ignored. If you configure multiple syslog servers, the source interface must be same for all of them.
Priority	Choose a severity of the syslog message to be saved. The severity indicates the seriousness of the event that generated the syslog message. The priority can be one of the following: • **Emergency**: System is unusable (corresponds to syslog severity 0). • **Alert**: Ensure that you act immediately. (corresponds to syslog severity 1). • **Critical**: A serious condition (corresponds to syslog severity 2). • **Error**: An error condition that doesn’t fully impair system usability (corresponds to syslog severity 3). • **Warning**: A minor error condition (corresponds to syslog severity 4). • **Notice**: A normal, but significant condition (corresponds to syslog severity 5). • **Informational**: Routine condition or the default condition (corresponds to syslog severity 6). • **Debug**: Issues debug messages that correspond to syslog severity 7.

Parameter Name	Description
TLS	Click **On** to enable syslog over TLS.
Custom Profile	Click **On** to enable choosing a TLS profile, or click **Off** to disable choosing a TLS profile.
TLS Profile	Choose a TLS profile that you have created for server or mutual authentication in IPv4 or IPv6 server configuration.

The server entries appear in a table.

3. Click **Add** to create another entry for a server.
4. To edit a logging server, click ✎.
5. To remove a logging server, click 🗑.
6. To save the feature template, click **Save**.
7. To associate the feature template with a device template, see the chapter, Create a Device Template from Feature Templates.

Generate Feature Certificate Signing Request and Install Feature Certificates

To validate and authenticate Cisco IOS XE SD-WAN devices and syslog server, perform the following operation on the Cisco vManage Certificates screen. See the Cisco SD-WAN Getting Started Guide for information about enterprise certificates.

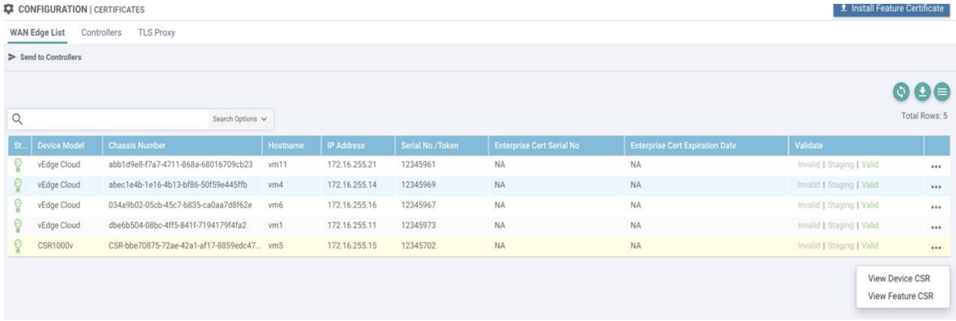
Step 1 In Cisco vManage, click **Configuration** > **Certificates**.

Step 2 On the Certificates page, click a Cisco IOS XE SD-WAN device.

a) Generate Feature Certificate Signing Request (CSR).

After you generate the Feature CSR, the **View Feature CSR** and **Install Feature certificate** options are available.

Figure 5: Generate Feature CSR



St...	Device Model	Chassis Number	Hostname	IP Address	Serial No./Token	Enterprise Cert Serial No	Enterprise Cert Expiration Date	Validate	
	vEdge Cloud	abb1d9e8-f7a7-4711-868a-68016709cb23	vm11	172.16.255.21	12345961	NA	NA	Invalid | Staging | Valid	•••
	vEdge Cloud	abec1e4b-1e16-4b13-bf86-50f59e445ffb	vm4	172.16.255.14	12345969	NA	NA	Invalid | Staging | Valid	•••
	vEdge Cloud	034a9b02-05cb-45c7-b835-ca0aa7d8f62e	vm6	172.16.255.16	12345967	NA	NA	Invalid | Staging | Valid	•••
	vEdge Cloud	dbe6b504-08bc-4ff5-841f-7194179f4fa2	vm1	172.16.255.11	12345973	NA	NA	Invalid | Staging | Valid	•••
	CSR1000v	CSR-bbe70875-72ae-42a1-af17-8859edc47...	vm5	172.16.255.15	12345702	NA	NA	Invalid | Staging | Valid	•••

b) View Feature CSR.

c) To download the feature CSR, click **Download**.

Step 3 To sign the certificate, send the certificate to a third-party signing authority.

Step 4 To import the certificate into Cisco IOS XE SD-WAN devices, Install feature certificate.

The Install Feature Certificate screen uses the signed certificate and installs it on Cisco IOS XE SD-WAN devices.

After the feature certificate installation is successful, the Revoke Feature Certificate and View Feature Certificate options are available on Cisco vManage.

What to do next

Verify Trustpoint Configuration on Cisco IOS XE SD-WAN Device, on page 17

Verify Trustpoint Configuration on Cisco IOS XE SD-WAN Device

To display the contents of syslog file with trustpoint information for Cisco IOS XE SD-WAN device, use the **show crypto pki trustpoints status** command.

Examples

Server authentication

```
Cisco XE SD-WAN# show crypto pki trustpoints status

crypto pki trustpoint SYSLOG-SIGNING-CA
  enrollment url bootflash:vmanage-admin/
  fqdn none
  fingerprint xxxxxx
  revocation-check none
  subject-name CN=CSR-cbc47d9d-45bf-433a-9816-1f12a8b48223_vManage Root CA
```

Mutual authentication

```
Cisco XE SD-WAN# show crypto pki trustpoints status

crypto pki trustpoint SYSLOG-SIGNING-CA
  enrollment url bootflash:vmanage-admin/
  fqdn none
  fingerprint xxxxxx
  revocation-check none
  rsakeypair SYSLOG-SIGNING-CA 2048
  subject-name CN=CSR-cbc47d9d-45bf-433a-9816-1f12a8b48223_vManage Root CA
```

Verify trustpoints on a device for a Syslog-signing-CA certificate

```
Cisco XE SD-WAN# show crypto pki trustpoints SYSLOG-SIGNING-CA status

Trustpoint SYSLOG-SIGNING-CA:

 Issuing CA certificate not configured.

State:

Keys generated ............ No

 Issuing CA authenticated ....... No

  Certificate request(s) ..... None
```