



Configure System Logging

Table 1: Feature History

Feature Name	Release Information	Description
Ability to Send Syslog Messages over TLS	Cisco IOS XE Catalyst SD-WAN Release 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.
Remote Logging Over TCP and TLS in Cisco Catalyst SD-WAN Control Components	Cisco Catalyst SD-WAN Control Components Release 20.13.1	The feature allows remote logging of syslog messages through TCP and TLS. This feature is now available on Cisco Catalyst SD-WAN Control Components (Cisco Catalyst SD-WAN Controller, Cisco Catalyst SD-WAN Validator, and Cisco Catalyst SD-WAN Manager) in addition to Cisco IOS XE Catalyst SD-WAN devices.

- [System Logging, on page 2](#)
- [Syslog Message Format, Syslog Message Levels, and System Log Files, on page 2](#)
- [Benefits of Using TLS for Sending Syslog Messages, on page 5](#)
- [Configure Logging in Server Authentication for TLS, on page 6](#)
- [Configure Logging in Mutual Authentication for TLS, on page 6](#)
- [Install Root Certificate Authority on Cisco IOS XE Catalyst SD-WAN Device for Server Authentication, on page 7](#)
- [Install Root Certificate Authority on Syslog Server for Server Authentication, on page 8](#)
- [Install Syslog Root Certificate on Cisco IOS XE Catalyst SD-WAN Device for Mutual Authentication, on page 9](#)
- [Configure Logging Feature Template Using Cisco SD-WAN Manager, on page 10](#)
- [Generate Feature Certificate Signing Request and Install Feature Certificates, on page 16](#)
- [Verify Trustpoint Configuration on Cisco IOS XE Catalyst SD-WAN Device, on page 17](#)
- [Export Cisco SD-WAN Manager NMS Audit Log to Syslog Server, on page 18](#)
- [Remote Logging Over TCP and TLS in Cisco Catalyst SD-WAN Control Components, on page 20](#)

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 Catalyst 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 Catalyst SD-WAN devices can send log messages to a UNIX-style syslog service.

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



Note Disabling system logging to disk (`no system logging disk enable`) does not disable `vsyslog`.

Syslog Message Format, Syslog Message Levels, and System Log Files

Syslog Message Format

Syslog messages begin with a percent sign (%) and following are the syslog message formats:

- 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:

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: <i>%facility-severity-MENEMONIC:description</i>

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.

Syslog Message Levels

All syslog messages are associated with priority levels that indicate the severity of syslog messages to save. The default priority value is "informational", so by default, all syslog messages are recorded. The priority level can be one of the following in order of decreasing severity:

- 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 does not 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 (the default) (corresponds to syslog severity 6).
- Debug—Issues debug messages that correspond to syslog severity 7.

System Log Files

All syslog messages that are at or above the default or configured priority value are recorded in a number of files in the `/var/log` directory on the local device of the syslog server. The following are the contents of the log files:

- `auth.log`—Login, logout, and superuser access events, and usage of authorization systems
- `kern.log`—Kernel messages
- `messages.log`—Consolidated log file that contains syslog messages from all sources.
- `vconfd.log`—All configuration-related syslog messages
- `vdebug.log`—All debug messages for modules whose debugging is turned on and all syslog messages that are above the default priority value. The debug log messages support various levels of logging based on the module. The different modules implement the logging levels differently. For example, the system manager (`sysmgr`) has two logging levels (on and off), while the chassis manager (`chmgr`) has four different logging levels (off, low, normal, and high). You cannot send debug messages to a remote host. Therefore, to enable debugging, use the **debug** operational command.
- `vsyslog.log`—All syslog messages from Cisco Catalyst SD-WAN processes (daemons) that are above the configured priority value. The default priority value is "informational", so by default, all "notice", "warning", "error", "critical", "alert", and "emergency" syslog messages are saved.
- `vmanage-syslog.log`—Cisco SD-WAN Manager NMS Audit log messages

The following are the standard LINUX files that Cisco Catalyst SD-WAN does not use and are available in the `/var/log` directory.

- `cron.log`
- `debug.log`
- `lpr.log`
- `mail.log`
- `syslog`

The messages sent to syslog files are not rate-limited and consequently:

- A storage limit of 10 log files with a capacity of up to 16 MB size is set for each syslog file.
 - When the storage capacity exceeds the 16 MB size limit, the log file is saved as a .GZ file along with the date appended to it.
 - When the storage limit exceeds 10 log files, the oldest log file is dropped.
- If many syslog messages are generated in a short span of time, the overflowing messages are buffered and queued to be stored in the syslog file.

For repeating syslog messages or identical messages that occur multiple times in succession, only one copy of the message is placed in the syslog file. The message is annotated to indicate the number of times the message occurred.

The maximum length of a log message is 1024 bytes. The longer messages are truncated.

The maximum length of a log message for Cisco SD-WAN Manager NMS audit logs is 1024 bytes. The longer messages are truncated into smaller fragments and each of these fragments are indicated by an identifier. The identifiers are, fragment 1/2, fragment 2/2, and so on. For example, a long audit log message when truncated into smaller fragments appears as:

```
local6.info: 18-Oct-2020 17:42:07 vm10 maintenance-fragment-1/2: {"logid":
"d9ed576a-43ae-49ce-921b-a51c1ed40698", "entry_time":
1576605512190, "statcycletime" 34542398334245, "logmodule":"maintenance", "logfeature":
"upgrade", "loguser": "admin", "logusersrcip":
"10.0.1.1", "logmessage": "Device validation Upgrade to version - Validation success",
"logdeviceid":"Validation", "auditdetails" :
["[18-Oct-2020 17:42:08 UTC] Published messages to vmanage(s)", "auditdetails":["[18-Oct-2020
17:42:07 UTC] Software image: vmanage-99.99.999-
x86_64.tar.gz", "Software image download may take up to 60}

local6.info: 18-Oct-2020 17:42:07 vm10 maintenance-fragment-2/2: { minutes", "logprocessid":
"software_install-7de0ec44-d290-4429-b24532435324", "tenant":, "default"}
```

The syslog messages related to AAA authentication and Netconf CLI access and usage are placed in the `auth.log` and `messages.log` files. Each time a Cisco SD-WAN Manager NMS logs into a router to retrieve statistics and status information and to push files to the router, the router generates AAA and Netconf log messages. So, over time, these messages can fill the log files. To prevent these messages from filling the log files, you can disable the logging of AAA and Netconf syslog messages by using the following commands from Cisco SD-WAN Manager NMS:



Note For information about available syslog messages on Cisco SD-WAN Manager, see [Syslog Messages](#).

Disable logging of AAA and Netconf Syslog Messages

1. `vManage# config`
Enters the configuration mode terminal
2. `vManage(config)# system aaa logs`
Configures the logging of AAA and Netconf system logging (syslog) messages
3. `vManage(config-logs)# audit-disable`
Disable logging of AAA events
4. `vManage(config-logs)# netconf-disable`
Disable logging of Netconf events
5. `vManage(config-logs)# commit`
Commit complete.

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 Catalyst SD-WAN device and the syslog server. The Cisco IOS XE Catalyst 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 Catalyst 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 Catalyst 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 Catalyst SD-WAN devices.

Prerequisite

Ensure that Cisco IOS XE Catalyst 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 Catalyst SD-WAN Device for Server Authentication](#).

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

1. [Configure Logging Feature Template Using Cisco SD-WAN Manager](#).
 - a. [Configure Logging Attributes to Local Disk](#).
 - b. [Configure Logging to Remote Servers](#).
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 Catalyst SD-WAN device authenticate each other at the same time. Cisco IOS XE Catalyst 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 Catalyst SD-WAN Device for Mutual Authentication](#).
2. [Configure Logging Feature Template Using Cisco SD-WAN Manager](#).
 - a. [Configure Logging Attributes to Local Disk](#).
 - b. [Generate Feature Certificate Signing Request and Install Feature Certificates, on page 16](#)
 - c. [Configure Logging to Remote Servers](#).
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 Catalyst SD-WAN Device](#).

Install Root Certificate Authority on Cisco IOS XE Catalyst 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 8](#).

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 Catalyst 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 8](#).

Example:

A sample base 64 encoded CA certificate:

```
-----BEGIN CERTIFICATE-----
MIID9jCCAt6gAwIBAgIJAM5b3nyjDAKIMA0GCSqGSIb3DQEBCwUAMIGPMQswCQYD
VQQGEwJTTjESMBAGA1UECAwJS2FybmF0YWhMRlweAYDVQQHDA1CYW5nYWxvcmUx
DjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQLDANDU0cxGzAZBgNVBAMMEmVtYmQtbG54
LmNpc2NvLmNvbTEdMBSGCSqGSIb3DQEJARYOYW5idkBJaXNjby5jb20wHhcNMTkw
OTIwMTQ1NjAxWhcNMjIwOTE5MTQ1NjAxWjCBjzELMAkGA1UEBhMCSU4xEjAQBGNV
BAGMCUthcm5hdGFrYTESMBAGA1UEBwwJQmFuZ2Fsb3JlMQ4wDAYDVQQKDAVdXNj
bzEMMAoGA1UECwwDQ1NHMRswGQYDVQQDDBJlbWJkLWxueC5jaXNjby5jb20xHTAB
BgkqhkiG9w0BCQEWdmFuZAY21zY28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ
AQ8AMIIBCgKCAQEAuof+Dh8EdAQ7bHJPDnXhy9ibTLAQ+OpQrMBoOqeAsU/Jru8y
3ht2Eqci35anJlDcsTU1ZyUHBNAMtL69t1HxTRVCOghOZmipzOS+q8rFykHa+bcA
FqmHyqxNwdQcW3cQFZ6rvWTFD9046ONX3xewpdCR+s+0KFOHDD+RxpAb2NyDWIvn
/1/xwq2a4Z1wgM2d0G8sit0i0D/+6FbZuJjAf+PRTypo4IJyQjcoHpZus1LzPztM
HxLI7pOmR+8+WcInt010dyGdpKKHXi6lEbeiYubIym0z0Des5OckDYFejXgXpJDX
9jCVkz+r0bijqbT5PMpSAYYcjdQ0kdH43sykwIDAQABo1MwUTAdBgNVHQ4EFgQU
OcOmN72TyBqD/Ud2qBLUWid1Yv0wHwYDVR0jBBgwFoAUOcOmN72TyBqD/Ud2qBLU
wId1Yv0wDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAVVWVJHwo
rKxfFV2w7jr7mLZS1VtEvZueMXWPvYYP+Qt09MrRqWNDUJEvggTxU71vLwtnITPM
l/dOmpoer8GhDtnxUnjsVeVWGIR74SjCS0GU/03bEJ2sto/eAJEOzI7wDg7Fubgy
Pc3RHbk4JWtWs4JF8+E64p2UzJMuu0eLDPQWx17p2wd3sr4DBHB3q1fbg31T3VHr
PCcuzJmOEdeZYGL1/LFvPx7NZS8lwFAohe6h8ptm3ENG7dzIeyZFZVfcq11Q1rer
+3RcM0VqjScIOZhp97dqfB1HEdquE/QfK1Bt12KU+0sj8yJJC+cuK1HQj5JGmGLI
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 SD-WAN Manager, on page 10](#)

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 Catalyst SD-WAN Device. See Step 3 of [Install Root Certificate Authority on Cisco IOS XE Catalyst SD-WAN Device for Server Authentication](#), on page 7.

What to do next

[Install Root Certificate Authority on Cisco IOS XE Catalyst SD-WAN Device for Server Authentication](#), on page 7

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

To configure Cisco IOS XE Catalyst 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 From the Cisco SD-WAN Manager menu, choose **Administration > Settings**.

Step 4 Click **Enterprise Feature Certificate Authorization**.

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

Step 6 (Optional) if you want to generate a Certificate Signing Request (CSR), check the **Set CSR Properties** check box.

Step 7 Click **Close**.

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

What to do next

[Configure Logging Feature Template Using Cisco SD-WAN Manager, on page 10](#)

Configure Logging Feature Template Using Cisco SD-WAN Manager

On Cisco IOS XE Catalyst SD-WAN device, you can log event notification system log (syslog) messages to files on the local device, or you can log them to files on a remote host using Cisco SD-WAN Manager.

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

Step 2 Click **Feature Templates**, and click **Add Template**.

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

Step 3 From **Select Devices**, choose the device for which you wish to create a template.

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

The Cisco Logging template form appears. This form contains fields for naming the template, and fields for defining the 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 list to the left of the parameter field.

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

The name may contain up to 128 alphanumeric characters.

Step 6 In **Template Description**, 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 10](#)

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 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 <i>syslogd</i> 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

- To save the feature template, click **Save**.
- To associate the feature template with a device template, see [Create a Device Template from Feature Templates](#).

What to Do Next

[Configure TLS Profile for Server Authentication, on page 11](#) or [Configure TLS Profile for Mutual Authentication, on page 13](#)

Configure TLS Profile for Server Authentication

- Click **TLS Profile**.
- Click **New Profile**, and configure the following parameters:

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	<p>Choose groups of cipher suites (encryption algorithm) based on the TLS version.</p> <p>The following are the list of cipher suites.</p> <ul style="list-style-type: none"> • 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. To create another profile, click **Add**.
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 [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 Logging to Remote Servers, on page 15](#)

Configure TLS Profile for Mutual Authentication

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

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	<p>Choose groups of cipher suites (encryption algorithm) based on the TLS version that must be used for encryption.</p> <p>The following are the list of cipher suites.</p> <ul style="list-style-type: none"> • 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. To create another profile, click **Add**.
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 [Create a Device Template from Feature Templates](#).

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

What to Do Next


[Configure Logging to Remote Servers, on page 15](#)

Configure Logging to Remote Servers

To include the TLS profile in IPV6 or IPV4 server configuration and configure logging of event notification system log messages to a remote server,



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

Table 6: Parameter Information

Parameter Name	Description
Hostname/IP Address	<p>Enter the DNS name, hostname, or IPv4, IPv6 address of the system on which to store syslog messages.</p> <p>To add another syslog server, click +.</p> <p>To delete a syslog server, click .</p>
VPN ID	<p>Enter the identifier of the VPN in which the syslog server is located or through which the syslog server can be reached.</p> <p>VPN ID Range: 0-65530</p>

Parameter Name	Description
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. See Syslog Message Levels .
TLS	For Cisco IOS XE Catalyst SD-WAN devices, click On to enable syslog over TLS.
Custom Profile	For Cisco IOS XE Catalyst SD-WAN devices, click On to enable choosing a TLS profile, or click Off to disable choosing a TLS profile.
TLS Profile	For Cisco IOS XE Catalyst SD-WAN devices, 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. To create another entry for a server, click **Add**.
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 [Create a Device Template from Feature Templates](#).

Generate Feature Certificate Signing Request and Install Feature Certificates

To validate and authenticate Cisco IOS XE Catalyst SD-WAN devices and syslog server, perform the following operation on the Cisco SD-WAN Manager Certificates screen. See [Cisco Catalyst SD-WAN Getting Started Guide](#) for information about enterprise certificates.

-
- Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration > Certificates**.
- Step 2** From **Certificates**, choose a Cisco IOS XE Catalyst 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.

- 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 Catalyst SD-WAN devices, [Install feature certificate](#).

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

After the feature certificate installation is successful, the [Revoke Feature Certificate](#) and [View Feature Certificate](#) options are available on Cisco SD-WAN Manager.

What to do next

[Verify Trustpoint Configuration on Cisco IOS XE Catalyst SD-WAN Device, on page 17](#)

Verify Trustpoint Configuration on Cisco IOS XE Catalyst SD-WAN Device

To display the contents of syslog file with trustpoint information for Cisco IOS XE Catalyst 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
```

Export Cisco SD-WAN Manager NMS Audit Log to Syslog Server

Table 7: Feature History

Feature Name	Release Information	Description
Export Cisco SD-WAN Manager Audit Log as Syslog	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	The Cisco SD-WAN Manager exports audit logs in syslog message format to a configured external syslog server. This feature allows you to consolidate and store network activity logs in a central location.

On Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices, you can log event notification system log (syslog) messages to files on a local device, or to files on a remote host using CLI. These event notification logs are converted to system log files and exported to the syslog server. You can then retrieve system log information from the syslog server.

Configure System Logging Using CLI

Log Syslog Messages to a Local Device

By default, a priority level of “information” is enabled when you log syslog messages to a file on a local device. Use the following commands:

1. logging disk

Logs syslog messages on a hard disk

Example:

```
vm01(config-system)# logging disk
```

2. enable

Enables logging to a disk

Example:

```
vm01(config-logging-disk)# enable
```

3. file size *size*

Specifies the size of syslog files in megabytes (MB) By default, the syslog files are 10 MB. You can configure the size of syslog files to be 1–20 MB.

Example:

```
vm01(config-logging-disk)# file size 3
```

4. file rotate number

Rotates syslog files on an hourly basis based on the size of the file By default, 10 syslog files are created. You can configure the rotate command to be a number from 1 through 10.

Example:

```
vm01(config-logging-disk)# file rotate 3
```

For more information about logging disk commands, see the [logging disk](#) command.

Log Syslog Messages to a Remote Device

To log event notification system log (syslog) messages to a remote host, use the following commands:

1. logging server

Logs syslog messages to a remote host or syslog server You can configure the name of the server by DNS name, hostname, or IP address. You can configure up to four syslog servers.

Example:

```
vm01(config-system)# logging server 192.168.0.1
```

2. (Optional) vpn vpn-id

Specifies the VPN ID of the syslog server

3. (Optional) source interface interface-name

Specifies the source interface to reach the syslog server. The interface name can be a physical interface or a sub-interface (a VLAN-tagged interface). Ensure that the interface is located in the same VPN as the syslog server. Otherwise, the configuration is ignored. If you configure multiple syslog servers, the source interface must be the same for all of them.

Example:

```
vm01(config-server-192.168.0.1)# source interface eth0
```

4. priority priority

Specifies the severity of the syslog message to be saved. The default priority value is "informational" and by default, all syslog messages are recorded.

Example:

In the following example, set the syslog priority to log alert conditions.

```
vm01(config-server-192.168.0.1)# priority alert
```

If the syslog server is unreachable, the system suspends sending syslog messages for 180 seconds. When the server becomes reachable, logging resumes. For more information about logging server commands, see the [logging server](#) command.

View System Logging Information

To view system log settings after logging syslog messages to a remote host, use the **show logging** command. For example:

```
vm01(config-server-192.168.0.1)# show logging

System logging
  server 192.168.0.1
  source interface eth0
  exit
!
!
```

To view the contents of the syslog file, use the **show log** command. For example:

```
vm01(config-server-192.168.0.1)# show log nms/vmanage-syslog.log tail 10
```

To view the configured system logging settings from Cisco SD-WAN Manager, see [Audit Log](#).

To view device-specific syslog files from Cisco SD-WAN Manager, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Administration > Settings**, and ensure that you enable **Data Stream**.
2. From the Cisco SD-WAN Manager menu, choose **Monitor > Devices**, and choose a Cisco IOS XE Catalyst SD-WAN device
Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor > Network**, and choose a Cisco IOS XE Catalyst SD-WAN device.
3. Click **Troubleshooting**.
4. From **Logs**, click **Debug Log**.
5. From **Log Files**, select a name of the log file to view the log information.

Remote Logging Over TCP and TLS in Cisco Catalyst SD-WAN Control Components

Information About Remote Logging Over TCP and TLS

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1, support for remote logging of syslog messages has been enhanced to include TCP and TLS transport methods in addition to UDP. This enhancement applies to Cisco Catalyst SD-WAN Control Components including Cisco Catalyst SD-WAN Controller, Cisco Catalyst SD-WAN Validator, and Cisco Catalyst SD-WAN Manager.

By default, UDP is enabled as the default transport type for remote logging. However, users now have the additional option to select either TCP or TLS as their transport method for remote logging.

For more information, see [System Logging, on page 2](#)

Benefits of Remote Logging Over TCP and TLS

- Syslog over TCP and TLS supports large-scale network environments. While TCP can handle large volumes of data, TLS can ensure that the log data is securely sent and protected from unauthorized access or tampering.
- You can configure up to four separate remote syslog servers with the option to assign each server a unique transport protocol such as UDP, TLS, or TCP. Alternatively, you can choose to use the same transport protocol for all four servers.
- For remote logging over TLS, a TLS profile supports TLS version 1.2. Also, various cipher suites can be accommodated within the TLS profile, depending on the TLS version.

Configure Remote Logging Over TCP and TLS

1. From the Cisco SD-WAN Manager menu, choose **Configuration > Templates**.
2. Click **Feature Templates**.
3. Click **Add Template** to select an appropriate device model.
4. In the left pane, from **Select Devices**, choose a Cisco Catalyst SD-WAN control component.
5. Under **OTHER TEMPLATES**, click **Logging** to select it as the feature template.

6. In the **Template Name** field, enter a name for the feature template.

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

7. In the **Description** field, enter a description for the feature template.

This field is mandatory, and it can contain all characters and spaces.

8. Configure Logging Attributes to Local Disk.
 - a. Click **Disk** and configure the following parameters:

Table 8: Parameter Information

Parameter	Description
Enable Disk	To save syslog messages in a file on the local hard disk, click On or 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 the configured value, the file is rotated and the <i>syslogd</i> process is notified. Range: 1 to 20 MB Default: 10 MB

Parameter	Description
Rotations	Enter the number of syslog files to create before discarding the earliest created files. Range: 1 to 10 MB Default: 10 MB

- b. To save the feature template, click **Save**.
- c. To associate the feature template with a device template, see [Create a Device Template from Feature Templates](#).

Configure TLS Profile for Server Authentication

1. From the **TLS Profile** section, click **New Profile** to configure a TLS profile.

Table 9: TLS Profile Parameters

Parameter Name	Description
Profile Name	Enter the TLS profile name
TLS Version	Choose TLS v1.2.

Parameter Name	Description
Ciphersuites	<p>Choose one or more ciphersuites based on the TLS version.</p> <p>The following ciphersuites are supported:</p> <ul style="list-style-type: none"> • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • DHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • DHE-RSA-AES256-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • DHE-RSA-AES128-SHA256 • RSA-PSK-AES256-GCM-SHA384 • DHE-PSK-AES256-GCM-SHA384 • AES256-GCM-SHA384 • PSK-AES256-GCM-SHA384 • RSA-PSK-AES128-GCM-SHA256 • DHE-PSK-AES128-GCM-SHA256 • AES128-GCM-SHA256 • PSK-AES128-GCM-SHA256 • AES256-SHA256 • AES128-SHA256

2. (Optional) Click **Add** to create another profile.

Configure Syslog Servers for TLS/TCP/UDP

1. From the **Server** section, click **New Server** to configure syslog servers.

Table 10: Syslog Servers Parameters

Parameter Name	Description
Hostname/IP Address	Enter the DNS name, hostname, IPv4 or IPv6 address of the server on which to store syslog messages. To add another syslog server and its details, click Add .
VPN ID	Enter the identifier of the VPN in which the syslog server is located or through which the syslog server can be reached. Range is 0 to 65530
Source Interface	Enter the specific interface to use for outgoing system log messages.
Priority	Choose a logging level for syslog messages that you want to log on the server. The logging level indicates the type of event that generated the syslog message. See Syslog Message Levels .
Transport for messages logged to remote host	Choose either TCP, UDP, or TLS as the transport type for forwarding syslog messages to a remote server.
Port for transport (default 514)	Specify the port number for the transport type.
TLS Profile	This field displays if you have chosen the transport type as TLS. Choose a TLS profile to attach a TLS profile. See Configure TLS Profile for Server Authentication, on page 22

- (Optional) Click **Add** to create another entry for a server.
- Click **Save** to save the feature template

Apply the Logging Feature Template to a Device

- From the Cisco SD-WAN Manager menu, choose **Configuration > Templates**.
- Click **Device Templates**.
- From the **Create Template** drop-down list, choose **From Feature Template**
- From the **Device Model** drop-down list, choose one of the devices.
- In the **Template Name** field, enter a name for the feature template.

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

This field is mandatory, and it can contain all characters and spaces.

7. From the **Cisco Logging** drop-down list, choose the template that you created for remote logging.
8. Click **Create** to apply the template to a device.
9. From the list of device templates, click ... next to the device template that you created.
10. Click **Attach Devices**.
11. Choose the devices to which you want to attach the device template.
12. Click **Attach** to the template to the devices.

Configure Remote Logging Over TCP and TLS

For more information about using CLI templates, see [CLI Add-On Feature Templates](#) and [CLI Templates](#).



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

This section provides sample CLI configurations to configure a remote server for logging with transport type as TCP and TLS.

Configure Remote Server with Transport Type as TCP

Configure Remote Server with Transport Type as TCP.

```
system
logging
server <server-ip-address>
transport tcp port 514
```

Configure Remote Server with Transport Type as TLS

Configuring a remote server for logging with Transport type as TLS is a three-step process.

1. Manage Certificate

To manage the Certificate Authority (CA) certificate from the syslog server, use the following commands below to install, list, and uninstall the certificates.

- Install a Certificate

A certificate can be installed from either a local directory, such as /home/admin, or remotely using secure copy (scp), HTTP, or FTP.

```
request logging ca-cert
install new syslog-ng ca
```

- List All Installed Certificates

```
show logging cacert
```

- Uninstall a Certificate

```
request logging ca-cert uninstall <cert-name>
```

2. Create a TLS Profile

Creating a TLS profile involves specifying the protocols and cipher suites that a device will use for secure communication. You can configure up to four TLS profiles.

Use the following configuration to create a TLS profile:

```
system
logging
tls-profile <profile-name>
  tls-version TLSv1.2
  ciphersuite <ciphersuite1> <ciphersuite2>
```

3. Attach a TLS Profile to a Remote Logging Server

Use the following configuration to attach a TLS profile to the remote logging servers:

```
server <server-ip-address>
vpn <vpn-instance-of-logging-server>
source-interface <interface-num>
transport tls
tls-profile <tls-profile-name>
```

Verify Remote Logging Over TCP and TLS

The following is a sample output from the **show logging cacert** command to view installed certificates.

```
Device# show logging cacert
INDEX  NAME          VALIDITY
-----
0      cert.pem     Fri Jun 21 20:35:10 2024
```

Configuration Example for Support for Syslog over TCP and TLS

Configuration Example for Logging Over TLS

This example shows the configuration for logging over TLS.

```
system
logging
  disk
  enable
  !
  tls-profile profile1
  version      TLSv1.2
  ciphersuite  ECDHE-ECDSA-AES128-SHA256 AES256-GCM-SHA384 PSK-AES256-GCM-SHA384
  PSK-AES128-GCM-SHA256 AES256-SHA256
  exit
  server 10.0.1.55
  source interface 10.1.1.12
  transport  tls
  tls-profile profile1
  exit
!
!
```

Configuration Example for Logging Over TCP

This example shows the configuration for logging over TCP.

```
system
logging
  disk
    enable
  !
  server 10.0.1.56
  transport tcp
exit
!
!
```

