System Logging

Feature history for system logging

This shows the history of the system logging feature.

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.

Feature Name	Release Information	Description
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

System logging is a process that

- records a text log of system events using a mechanism similar to the UNIX syslog command,
- allows devices to send log messages with configurable priority levels to UNIX-style syslog services, and
- supports secure transmission over the Transport Layer Security (TLS) protocol.

Priority levels

Log messages have levels that indicate their priority. These are the same as for standard UNIX commands. You can configure the priority of syslog messages.

Security

Cisco IOS XE Catalyst SD-WAN devices send syslog messages to syslog servers on configured external hosts using TCP and UDP. When the devices send 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 support sending secure syslog messages over TLS as described in RFC 5425. 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 support both mutual and server authentication for sending syslog messages over TLS.

Benefits of using TLS

- Message confidentiality

  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.

- Message integrity

  Integrity-checking of the content of each message to disable modifications to a message during transit on a hop-by-hop basis.

- Authentication

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.

System log files

System log (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 log files contain these items.

Table 2: Log files

File	Contents
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. 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. 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 audit log messages

Unused log files

Cisco Catalyst SD-WAN does not use these standard Linux files, which are available in the `/var/log` directory:

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

System log formats

Syslog messages begin with a percent sign (%) and come in these formats:

- Sequence and timestamp

  sequence-number:timestamp: %*facility-severity-MENEMONIC*:*description (hostname-n)*

- Format based on RFC5424

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

  The optional fields such as *hostname*, *appname*, *procId*, *msgId*, and *structured-data* are specified with a -.

Table 3: Field descriptions

Field	Description
facility	Sets the logging facility to a value other than 20, which UNIX systems expect.
severity	Importance or severity of the message, 0 to 7. A lower number indicates a greater severity of the system condition.
msg or description	Text string that describes the condition of the 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 is: *%facility-severity-MENEMONIC:description*

Examples

This system logging message includes a priority value, sequence number, and timestamp:

*<45>10: polaris-user1: *Jun 21 10:76:84.100: %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down*

This RFC5424-format message has a priority value, version of syslog protocol specification, and timestamp:

<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 message levels

Each system log (syslog) message has a severity, or priority, level. A lower severity number means a higher severity. The default priority value is 6 (informational). By default, all syslog messages are recorded.

Table 4: System log message severity levels

Severity level	Name	Description
0	Emergency	System is unusable.
1	Alert	System in a state that requires immediate action.
2	Critical	Serious condition.
3	Error	Error condition that does not fully impair system usability.
4	Warning	Minor error condition.
5	Notice	Normal operation, but with a significant condition requiring notice.
6	Informational	Routine condition (default).
7	Debug	Debug messages.

Sending system log messages to a server, using TLS

Transport layer security (TLS) is a networking protocol that provides secure communication through a network.

Benefits of using TLS for sending syslog messages

The benefits of using TLS for sending syslog messages are:

- Confidentiality

  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

  Integrity-checking of the content of each message to disable modifications to a message during transit on a hop-by-hop basis.

- Mutual authentication

  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.

Authentication type

- **Server**

  With server authentication, edge 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.

  As part of server authentication, the syslog server shares its public certificate with the devices.

  See the prerequisite in the "Before you begin" section of this procedure.

  With this option, all information about TLS profiles, except the trustpoint information, is saved.

- **Mutual**

  With mutual authentication, edge devices and the syslog server authenticate each other at the same time.

  Devices require root or identity certificates for mutual authentication of the TLS session.

  With this option, a trustpoint, such as SYSLOG-SIGNING-CA certificate, is saved on the device. This enables SD-WAN Manager to install the certificate from the edge device.

Restrictions for system logging

Disabling system logging to disk

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

Storage restrictions

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.

Repeating or identical messages

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.

Maximum length

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 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-...",
 "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-...", "tenant":, "default"}
```

AAA authentication and Netconf CLI access

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 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. 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.

Configure system logging

Use one of these methods to configure system logging:

- Configuration group
- Feature template
- CLI commands

Note Some configurations and protocols are identified as insecure and is a security risk for Cisco devices. Existing deployments continue to function, but new installations require intentional enablement. For more information on remediation, refer to Resilient Infrastructure: Cisco Catalyst SD-WAN and Routing

Configure system logging using a configuration group

System logging is the process of keeping a text log of system events.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Follow these steps to configure system logging for a device, using a configuration group:

Procedure

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

Step 2 Create and configure a Logging feature in a System profile.

a) Enter the disk information.

Table 5: Disk

Field	Description
Enable Disc	Enable this option to allow syslog messages to be saved in a file on the local hard disk, or disable this option to disallow it. By default, logging to a local disk file is enabled on all Cisco IOS XE Catalyst SD-WAN devices.
Max File Size(In Megabytes)	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 syslog process is notified. Range: 1 to 20 MB Default: 10 MB
Rotations	Enter the number of syslog files to create before discarding the oldest files. Range: 1 to 10 Default: 10

b) Enter the TLS Profile information.

Table 6: TLS Profile

Field	Description
Add TLS Profile	
TLS Profile Name*	Enter the name of the TLS profile.
TLS Version	Choose a TLS version: • **TLSv1.1** • **TLSv1.2**
Authentication Type*	Choose **Server**.

Field	Description
Cipher Suite List	Choose groups of cipher suites (encryption algorithm) based on the TLS version. 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-cbc-sha2**: Encryption type tls_dhe_rsa_with_aes_cbc_sha2 (TLS1.2 and above) • **dhe-aes-gcm-sha2**: Encryption type tls_dhe_rsa_with_aes_gcm_sha2 (TLS1.2 and above) • **ecdhe-ecdsa-aes-gcm-sha2**: Encryption type tls_ecdhe_ecdsa_aes_gcm_sha2 (TLS1.2 and above) SuiteB • **ecdhe-rsa-aes-cbc-sha2**: Encryption type tls_ecdhe_rsa_aes_cbc_sha2 (TLS1.2 and above) • **ecdhe-rsa-aes-gcm-sha2**: Encryption type tls_ecdhe_rsa_aes_gcm_sha2 (TLS1.2 and above) • **rsa-aes-cbc-sha2**: Encryption type tls_rsa_with_aes_cbc_sha2 (TLS1.2 and above) • **rsa-aes-gcm-sha2**: Encryption type tls_rsa_with_aes_gcm_sha2 (TLS1.2 and above)

c) Enter the server information.

Table 7: Server

Field	Description
Add Server	
Hostname/IPv4 Address*	Enter the DNS name, hostname, or IP address of the system on which to store syslog messages. To add another syslog server, click the plus sign (+). To delete a syslog server, click the trash icon to the right of the entry.
VPN*	Enter the identifier of the VPN in which the syslog server is located or through which the syslog server can be reached. Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.
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 is ignored. If you configure multiple syslog servers, the source interface must be the same for all of them.

Field	Description
Priority	Select the severity of the syslog message to save. The severity indicates the seriousness of the event that generated the message. Priority can be one of these: • **informational**: Routine condition (the default) (corresponds to syslog severity 6) • **debugging**: Prints additional logs to help debugging the issue. • **notice**: A normal, but significant condition (corresponds to syslog severity 5) • **warn**: A minor error condition (corresponds to syslog severity 4) • **error**: An error condition that does not fully impair system usability (corresponds to syslog severity 3) • **critical**: A serious condition (corresponds to syslog severity 2) • **alert**: Action must be taken immediately (corresponds to syslog severity 1) • **emergency**: System is unusable (corresponds to syslog severity 0)
TLS Enable*	Enable this option to allow syslog over TLS. When you enable this option, these fields appear: **TLS Properties Custom Profile**: Enable this option to choose a TLS profile. When you enable this option, the following field appears: **TLS Properties Profile**: Choose a TLS profile that you have created for server or mutual authentication in the IPv4 server configuration.
Add IPv6 Server	
Hostname/IPv6 Address*	Enter the DNS name, hostname, or IP address of the system on which to store syslog messages. To add another syslog server, click the plus sign (+). To delete a syslog server, click the trash icon to the right of the entry.
VPN*	Enter the identifier of the VPN in which the syslog server is located or through which the syslog server can be reached. Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.
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 is ignored. If you configure multiple syslog servers, the source interface must be the same for all of them.

Field	Description
Priority	Select the severity of the syslog message to save. The severity indicates the seriousness of the event that generated the message. Priority can be one of these: • **informational**: Routine condition (the default) (corresponds to syslog severity 6) • **debugging**: Prints additional logs to help debugging the issue. • **notice**: A normal, but significant condition (corresponds to syslog severity 5) • **warn**: A minor error condition (corresponds to syslog severity 4) • **error**: An error condition that does not fully impair system usability (corresponds to syslog severity 3) • **critical**: A serious condition (corresponds to syslog severity 2) • **alert**: Action must be taken immediately (corresponds to syslog severity 1) • **emergency**: System is unusable (corresponds to syslog severity 0)
TLS Enable*	Enable this option to allow syslog over TLS.
TLS Properties Custom Profile*	Enable this option to choose a TLS profile.
TLS Properties Profile	Choose a TLS profile that you have created for server or mutual authentication in the IPv6 server configuration.

What to do next

Refer to Deploy a Configuration Group in the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.

Configure system logging using a template

System log (syslog) messages are a text log of system events.

On Cisco IOS XE Catalyst SD-WAN devices, you can save system log messages locally or to a remote server.

Before you begin

Follow these steps to configure system logging for a device, using a feature template.

Procedure

Step 1 Create a System Logging feature template.

See Create a System Logging feature template, on page 12.

Step 2 Choose whether to save system log messages locally or to a syslog server. If saving messages to a server, choose whether to use the Transport Layer Security (TLS) protocol.

Configure a device to save system log messages to a server, using TLS, on page 13

a) If you choose to save syslog messages locally, do this:

Configure a device to save system log messages locally, on page 12

b) If you choose to save syslog messages to a syslog server, without using TLS, do this:

c) If you choose to save syslog messages to a syslog server, using TLS, with authentication by the server, do this:

d) If you choose to save syslog messages to a syslog server, using TLS, with mutual authentication by the edge device and the server, do this:

Create a System Logging feature template

System log (syslog) messages are a text log of system events.

Procedure

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

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

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

Step 3 From **Select Devices**, select 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 displays fields for naming the template and defining the logging parameters. Click a tab or the plus sign (+) to view additional fields.

When you first open a feature template, SD-WAN Manager sets the scope to default, for parameters that have a default value. The default setting or value appears next to each parameter. To change the default or enter a value, select a different option from 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.

Configure a device to save system log messages locally

System log (syslog) messages are a text log of system events.

You can save system log messages locally or to an external server. This procedure configures a device to save system messages locally.

Before you begin

Follow these steps to configure a device to save system log messages to a local drive.

Procedure

Step 1 In a System Logging template, in the **Disk** section, configure these parameters:

Field	Description
Enable Disk	To save syslog messages in a file on the local hard disk, click **On** or **Off** to disallow saving. Default: Logging to a local disk file is enabled.
Maximum File Size	Enter the maximum size of syslog files. The system log 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 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

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

Configure a device to save system log messages to a server, using TLS

System log (syslog) messages are a text log of system events.

You can send system log messages to an external server over a Transport Layer Security (TLS) connection.

For the TLS connection, there are two methods of authentication, configured by the **Authentication Type** parameter.

- Server authentication: Authentication by the server.
- Mutual authentication: Authentication by both the device and the server.

See Sending system log messages to a server, using TLS, on page 5.

Before you begin

For the server authentication option, edge devices must have a root certificate authority (CA) preinstalled, which you configure using cryptographic module CLIs. See Install root CA on Cisco IOS XE Catalyst SD-WAN device.

Follow these steps to configure the TLS parameters for saving syslog messages to an external server over a TLS connection.

Procedure

Step 1 In a System Logging template, in the **TLS** section, click **New Profile**.

Step 2 Configure these parameters:

Field	Description
Profile Name	Enter the TLS profile name.
TLS Version	Choose TLS versions v1.1 or v1.2.
Authentication Type	Choose the authentication type: • **Server** With server authentication, edge 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. As part of server authentication, the syslog server shares its public certificate with the devices. See the prerequisite in the "Before you begin" section of this procedure. With this option, all information about TLS profiles, except the trustpoint information, is saved. • **Mutual** With mutual authentication, edge devices and the syslog server authenticate each other at the same time. Devices require root or identity certificates for mutual authentication of the TLS session. With this option, a trustpoint, such as SYSLOG-SIGNING-CA certificate, is saved on the device. This enables SD-WAN Manager to install the certificate from the edge device.
Ciphersuites	Choose cipher suites (encryption algorithms) based on the TLS version.

Step 3 To save the feature template, click **Save**.

Configure a device to save system log messages to a server

System log (syslog) messages are a text log of system events.

Before you begin

Follow these steps to configure a device to save system log messages to a server.

Procedure

Step 1 Click **Server**.

Step 2 Click **Add New Server**, and configure these parameters:

Field	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 to 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. See System log message levels, on page 5.
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.

Step 3 To save the feature template, click **Save**.

Configure system logging using CLI commands

You can save event notification system log (syslog) messages locally or to a remote server. 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, saved locally, using CLI commands, on page 16
- Configure system logging, saved remotely, using CLI commands, on page 17

Configure system logging, saved locally, using CLI commands

System logging is the process of keeping a text log of system events.

By default, a priority level of "information" is enabled when you log syslog messages to a file on a local device.

For more information about logging disk commands, see the logging disk command.

Before you begin

Follow these steps to configure system logging for a device, saving syslog messages locally, using CLI commands:

Procedure

Step 1 Log syslog messages to a drive.

logging disk

Step 2 Enable logging to a drive.

enable

Step 3 Specify 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 to 20 MB.

file size *size*

Step 4 Rotate 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.

file rotate *number*

Example

```
Device(config-system)# logging disk
Device(config-logging-disk)# enable
Device(config-logging-disk)# file size 3
Device(config-logging-disk)# file rotate 3
```

Configure system logging, saved remotely, using CLI commands

System logging is the process of keeping a text log of system events.

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.

Before you begin

Follow these steps to configure system logging for a device, saving syslog messages a remote server, using CLI commands:

Procedure

Step 1 Log 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.

logging server

Step 2 If using a VPN, specify the VPN ID of the syslog server.

vpn *vpn-id*

Step 3 (Optional) Specify 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.

source interface *interface*

Step 4 Specify the severity of the syslog message to be saved.

The default priority value is "informational" and by default, all syslog messages are recorded. See the logging server command reference documentation for priority values.

priority *alert*

Example

```
Device(config-system)# logging server 192.168.0.1
Device(config-server-192.168.0.1)# source interface eth0
Device(config-server-192.168.0.1)# priority notice
```

Install a root certificate on a 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.

Before you begin

Follow these steps to install a root certificate on a device for mutual authentication.

Procedure

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 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 SD-WAN Manager, and SD-WAN Manager saves the root certificate to the device.

Install a root certificate authority on a syslog server for server authentication

This procedure sets up the syslog-ng server tool on a server using Linux. The tool supports TLS.

The details of setting up a server, and installing the syslog-ng tool are beyond the scope of this documentation. The basic information provided here is for reference, and is subject to change.

Before you begin

Follow these steps to install a root certificate authority on a syslog server for server authentication.

Procedure

Step 1 On the Linux server, install the syslog-ng package.

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

Step 2 In the directory of the syslog-ng tool, create directories to store root certificates.

```
# 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 contents of the `cacert.pem` file when installing root certificate on a device.

Install a root certificate authority on a device for server authentication, using CLI commands

Before you begin

Generate an encoded CA certificate on the syslog server. This is required in one of the steps. For instructions, see Install a root certificate authority on a syslog server for server authentication, on page 18.

Follow these steps to install a root certificate authority on a device, for server authentication.

Procedure

Step 1 To configure a public key infrastructure (PKI) trustpoint for a certificate authority, use these commands on a device, for authorizing and revocation of certificates in PKI.

a) Enable privileged EXEC mode.

```
enable
```

b) Enter configuration mode.

```
config-transaction
```

c) Declare the trustpoint and a given name and enter CA-trustpoint configuration mode. Specify the enrollment parameters and fingerprint for the CA. Obtain the fingerprint from the fingerprint.txt.

```
crypto pki trustpoint name
```

Example:

```
Device(config)# crypto pki authenticate PROXY-SIGNING-CA
        enrollment url bootflash:
        revocation-check none
        rsakeypair PROXY-SIGNING-CA 2048
        subject-name cn=proxy-signing-cert
        fqdn none
        fingerprint 54F371C8EE2BFB06E2C2D0944245C288FBB07163
```

d) If the authentication in the previous step fails, contact the PKI team for assistance.

For information about syslog configuration, see Cisco SD-WAN IOS XE TLS Syslog Configuration on syslog-ng Server.

e) Configure the level to which a certificate chain is processed on all certificates.

```
chain-validation [{stop | continue}[parent-trustpoint]]
```

Example:

```
Device(ca-trustpoint)# chain-validation stop
```

f) Optionally, check the revocation status of a certificate.

```
revocation-check method
```

Example:

```
Device(ca-trustpoint)# revocation-check none
```

g) Return to global configuration mode.

exit

Example:

```
Device(ca-trustpoint)# exit
```

Step 2 Authenticate the root CA.

This is necessary before installing the server's root certificate.

crypto pki authenticate

Example:

```
Device(config)# crypto pki authenticate root
```

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

The prerequisites section refers to the instructions for generating the encoded CA certificate on the syslog server.

Example:

An example encoded CA certificate:

```
-----BEGIN CERTIFICATE-----
MIID9jCCAt6gAwIBAgIJAM5b3nyjDAKIMA0GCSqGSIb3DQEBCwUAMIGPMQswCQYD
VQQGEwJJTjESMBAGA1UECAwJS2FybmF0YWthMRIwEAYDVQQHDAlCYW5nYWxvcmUx
...
+3RcM0VqjScIOZhp97dqfBlHEdqUE/QfKlBt12KU+0sj8yJJC+cuKlHQj5JGmGLI
Y6r7bMcn99Y6Rw==
-----END CERTIFICATE-----
```

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

The root CA certificate from the syslog server is installed on a device, enabling server authentication.

```
crypto pki trustpoint PROXY-SIGNING-CA
    enrollment url bootflash:
    revocation-check none
    rsakeypair PROXY-SIGNING-CA 2048
    subject-name cn=proxy-signing-cert
    fqdn none
    fingerprint 54F3...7163  >> The fingerprint configured was obtained from the
fingerprint.txt file.
commit
```

```
crypto pki authenticate PROXY-SIGNING-CA
Reading file from bootflash:PROXY-SIGNING-CA.ca
Certificate has the following attributes:
Fingerprint MD5: 7A97B30B ... 66488DCF
Fingerprint SHA1: 21E0F09B ... D39A268A
Trustpoint Fingerprint: 21E0F09B ... D39A268A
Certificate validated - fingerprints matched.
Trustpoint CA certificate accepted.
```

View system logs

System logging records a text log of system events.

Before you begin

In SD-WAN Manager, in **Administration** > **Settings**, enable **Data Stream**.

View device-specific system log (syslog) files in Cisco SD-WAN Manager.

Procedure

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

In Cisco vManage Release 20.6.x and earlier, choose **Monitor** > **Network**.

Step 2 Select a device.

Step 3 Click **Troubleshooting**.

Step 4 In the **Logs** section, click **Debug Log**.

Step 5 From **Log Files**, select the name of a log file to view the log information.

Viewing system log information using CLI commands

You can use these CLI commands to view system log (log) information.

Viewing system log settings

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

```
Host(config-server-192.168.0.1)# show logging
System logging
    server 192.168.0.1
    source interface eth0
    exit
!
!
```

Viewing system log files

To view the contents of the system log file, use the **show log** command.

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

Create a certificate signing request and install feature certificates

This procedure validates and authenticates devices and the syslog server.

Procedure

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

Step 2 From **Certificates**, select a device.

a) Generate a feature certificate signing request (CSR).

Refer to Certificate Management in the *Cisco Catalyst SD-WAN Getting Started Guide*.

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

b) View and download the feature CSR.

Refer to Certificate Management in the *Cisco Catalyst SD-WAN Getting Started Guide*.

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

Step 4 Import the certificate into Cisco IOS XE Catalyst SD-WAN devices.

Refer to Certificate Management in the *Cisco Catalyst SD-WAN Getting Started Guide*.

SD-WAN Manager uses the signed certificate and installs it on devices.

After the feature certificate installation is successful, options are available in SD-WAN Manager to revoke or view a feature certificate.

Verifying the trustpoint configuration on a device

Display the contents of a syslog file to verify the trustpoint configuration.

Verifying server authentication

Example:

```
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-..._vManage Root CA
```

Verifying mutual authentication

Example:

```
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-..._vManage Root CA
```

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

Example:

```
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
```

Remote logging over TCP and TLS

Remote logging refers to saving system log information on a remote server.

From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1, remote logging of syslog messages can include TCP and TLS transport methods, in addition to UDP. This applies to SD-WAN Control Component.

The default transport type for remote logging is UDP. But you can optionally select TCP or TLS as the transport method for remote logging.

Benefits of remote logging over TCP and TLS

These are 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 using CLI commands

Before you begin

Follow these steps to configure remote logging over TCP using CLI commands.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure a remote server with transport type TCP.

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

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

Configure remote logging over TLS using CLI commands

Before you begin

Follow these steps to configure remote logging over TLS using CLI commands.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Use these steps to install, list, and uninstall the certificate authority (CA) certificate from the syslog server.

a) Install a certificate.

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

b) List all installed certificates.

```
show logging cacert
```

c) Uninstall a certificate if necesseary.

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

Step 3 Create a TLS profile.

```
system
 logging
 tls-profile profile-name
```

```
  tls-version TLSv1.2
  ciphersuite ciphersuite1 ciphersuite2
```

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.

Step 4 Attach a TLS profile to a remote logging server.

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

```
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
!
!
```

Verifying remote logging over TCP and TLS

View the installed certificates to verify that remote logging is possible over TCP and TLS.

The **show logging cacert** command shows installed certificates.

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