



# Configuring System Message Logging

This chapter contains the following sections:

- [Information About System Message Logging, on page 1](#)
- [Guidelines and Limitations for System Message Logging, on page 2](#)
- [Default Settings for System Message Logging, on page 3](#)
- [Configuring System Message Logging, on page 3](#)
- [Verifying the System Message Logging Configuration, on page 20](#)

## Information About System Message Logging

You can use system message logging to control the destination and to filter the severity level of messages that system processes generate. You can configure logging to terminal sessions, a log file, and syslog servers on remote systems.

System message logging is based on [RFC 3164](#). For more information about the system message format and the messages that the device generates, see the *Cisco NX-OS System Messages Reference*.

By default, the Cisco Nexus device outputs messages to terminal sessions.

By default, the switch logs system messages to a log file.

The following table describes the severity levels used in system messages. When you configure the severity level, the system outputs messages at that level and lower.

**Table 1: System Message Severity Levels**

Level	Description
0 – emergency	System unusable
1 – alert	Immediate action needed
2 – critical	Critical condition
3 – error	Error condition
4 – warning	Warning condition
5 – notification	Normal but significant condition

Level	Description
6 – informational	Informational message only
7 – debugging	Appears during debugging only

The switch logs the most recent 100 messages of severity 0, 1, or 2 to the NVRAM log. You cannot configure logging to the NVRAM.

You can configure which system messages should be logged based on the facility that generated the message and its severity level.

## Syslog Servers

Syslog servers run on remote systems that are configured to log system messages based on the syslog protocol. You can configure the Cisco Nexus Series switch to send logs to up to eight syslog servers. If CFS is enabled, you can configure up to three syslog servers.

To support the same configuration of syslog servers on all switches in a fabric, you can use Cisco Fabric Services (CFS) to distribute the syslog server configuration.




---

**Note** When the switch first initializes, messages are sent to syslog servers only after the network is initialized.

---

## Secure Syslog Servers

Beginning with Cisco NX-OS Release 9.2(1), you can configure the syslog server with support for a secure TLS transport connectivity to remote logging servers. Additionally, you can enforce the NX-OS switches (client) identity via the mutual authentication configuration. For NX-OS switches, this feature supports TLSv1.1 and TLSv1.2.

The Secure syslog server feature uses the TCP/TLS transport and security protocols to provide device authentication and encryption. This feature enables a Cisco NX-OS device (acting as a client) to make a secure, encrypted outbound connection to remote syslog servers (acting as a server) supporting secure connectivity for logging. With authentication and encryption, this feature allows for a secure communication over an insecure network.

## Guidelines and Limitations for System Message Logging

See the following guidelines and limitations for System Message Logging:

- System messages are logged to the console and to the logfile by default.
- The Cisco Nexus 3000 Series platforms syslog indicate the MAC collision events. The syslog message has the details, for example, the source MAC address, the VLANs, and the internal port number information. MAC collisions are normal and they are expected if the table usage crosses about 75% as observed on various setups. See the following example of the syslog: 2015 Mar 26 06:20:37 switch%-SLOT1-5-BCM\_L2\_HASH\_COLLISION: L2 ENTRY unit=0 mac=00:11:11:f7:46:40 vlan=1998 port=0x0800082e.

- Beginning with Cisco NX-OS Release 9.2(1), you can configure the syslog server with support for a secure TLS transport connectivity to remote logging servers. This feature supports TLSv1.1 and TLSv1.2.

## Default Settings for System Message Logging

The following table lists the default settings for system message logging parameters.

**Table 2: Default System Message Logging Parameters**

Parameters	Default
Console logging	Enabled at severity level 2
Monitor logging	Enabled at severity level 2
Log file logging	Enabled to log messages at severity level 5
Module logging	Enabled at severity level 5
Facility logging	Enabled
Time-stamp units	Seconds
Syslog server logging	Disabled
Syslog server configuration distribution	Disabled

## Configuring System Message Logging

### Configuring System Message Logging to Terminal Sessions

You can configure the switch to log messages by their severity level to console, Telnet, and Secure Shell sessions.

By default, logging is enabled for terminal sessions.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>terminal monitor</b>	Copies syslog messages from the console to the current terminal session.
<b>Step 2</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	switch(config)# <b>logging console</b> [ <i>severity-level</i> ]	Enables the switch to log messages to the console session based on a specified severity level or higher (a lower number value indicates

	Command or Action	Purpose
		<p>a higher severity level). Severity levels range from 0 to 7:</p> <ul style="list-style-type: none"> <li>• 0 – emergency</li> <li>• 1 – alert</li> <li>• 2 – critical</li> <li>• 3 – error</li> <li>• 4 – warning</li> <li>• 5 – notification</li> <li>• 6 – informational</li> <li>• 7 – debugging</li> </ul> <p>If the severity level is not specified, the default of 2 is used.</p>
<b>Step 4</b>	(Optional) switch(config)# <b>no logging console</b> [severity-level]	Disables logging messages to the console.
<b>Step 5</b>	switch(config)# <b>logging monitor</b> [severity-level]	<p>Enables the switch to log messages to the monitor based on a specified severity level or higher (a lower number value indicates a higher severity level). Severity levels range from 0 to 7:</p> <ul style="list-style-type: none"> <li>• 0 – emergency</li> <li>• 1 – alert</li> <li>• 2 – critical</li> <li>• 3 – error</li> <li>• 4 – warning</li> <li>• 5 – notification</li> <li>• 6 – informational</li> <li>• 7 – debugging</li> </ul> <p>If the severity level is not specified, the default of 2 is used.</p> <p>The configuration applies to Telnet and SSH sessions.</p>
<b>Step 6</b>	(Optional) switch(config)# <b>no logging monitor</b> [severity-level]	Disables logging messages to Telnet and SSH sessions.
<b>Step 7</b>	(Optional) switch# <b>show logging console</b>	Displays the console logging configuration.

	Command or Action	Purpose
<b>Step 8</b>	(Optional) switch# <b>show logging monitor</b>	Displays the monitor logging configuration.
<b>Step 9</b>	(Optional) switch# <b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.

### Example

The following example shows how to configure a logging level of 3 for the console:

```
switch# configure terminal
switch(config)# logging console 3
```

The following example shows how to display the console logging configuration:

```
switch# show logging console
Logging console:                enabled (Severity: error)
```

The following example shows how to disable logging for the console:

```
switch# configure terminal
switch(config)# no logging console
```

The following example shows how to configure a logging level of 4 for the terminal session:

```
switch# terminal monitor
switch# configure terminal
switch(config)# logging monitor 4
```

The following example shows how to display the terminal session logging configuration:

```
switch# show logging monitor
Logging monitor:                enabled (Severity: warning)
```

The following example shows how to disable logging for the terminal session:

```
switch# configure terminal
switch(config)# no logging monitor
```

## Configuring System Message Logging to a File

You can configure the switch to log system messages to a file. By default, system messages are logged to the file log:messages.

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>logging logfile</b> <i>logfile-name</i> <i>severity-level</i> [ <b>size bytes</b> ]	Configures the name of the log file used to store system messages and the minimum severity level to log. You can optionally specify a maximum file size. The default severity level is 5 and the file size is 4194304.  Severity levels range from 0 to 7: <ul style="list-style-type: none"> <li>• 0 – emergency</li> <li>• 1 – alert</li> <li>• 2 – critical</li> <li>• 3 – error</li> <li>• 4 – warning</li> <li>• 5 – notification</li> <li>• 6 – informational</li> <li>• 7 – debugging</li> </ul> The file size is from 4096 to 10485760 bytes.
<b>Step 3</b>	(Optional) switch(config)# <b>no logging logfile</b> [ <i>logfile-name severity-level</i> [ <b>size bytes</b> ]]	Disables logging to the log file. You can optionally specify a maximum file size. The default severity level is 5 and the file size is 4194304.
<b>Step 4</b>	(Optional) switch# <b>show logging info</b>	Displays the logging configuration. You can optionally specify a maximum file size. The default severity level is 5 and the file size is 4194304.
<b>Step 5</b>	(Optional) switch# <b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.

**Example**

The following example shows how to configure a switch to log system messages to a file:

```
switch# configure terminal
switch(config)# logging logfile my_log 6 size 4194304
```

The following example shows how to display the logging configuration (some of the output has been removed for brevity):

```
switch# show logging info
Logging console:                               enabled (Severity: debugging)
```

```

Logging monitor:                enabled (Severity: debugging)

Logging timestamp:              Seconds
Logging server:                 disabled
Logging logfile:                enabled
Name - my_log: Severity - informational Size - 4194304
Facility      Default Severity      Current Session Severity
-----
aaa           3
aclmgr        3           3
afm           3
altos        3
auth         0
authpriv     3
bootvar      5
callhome     2
capability   2
cdp          2
cert_enroll  2
...
    
```

## Configuring Module and Facility Messages Logging

You can configure the severity level and time-stamp units of messages logged by modules and facilities.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>logging module</b> [ <i>severity-level</i> ]	Enables module log messages that have the specified severity level or higher. Severity levels range from 0 to 7: <ul style="list-style-type: none"> <li>• 0 – emergency</li> <li>• 1 – alert</li> <li>• 2 – critical</li> <li>• 3 – error</li> <li>• 4 – warning</li> <li>• 5 – notification</li> <li>• 6 – informational</li> <li>• 7 – debugging</li> </ul> If the severity level is not specified, the default of 5 is used.
<b>Step 3</b>	switch(config)# <b>logging level</b> <i>facility severity-level</i>	Enables logging messages from the specified facility that have the specified severity level or higher. Severity levels from 0 to 7:

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• 0 – emergency</li> <li>• 1 – alert</li> <li>• 2 – critical</li> <li>• 3 – error</li> <li>• 4 – warning</li> <li>• 5 – notification</li> <li>• 6 – informational</li> <li>• 7 – debugging</li> </ul> <p>To apply the same severity level to all facilities, use the all facility. For defaults, see the <b>show logging level</b> command.</p> <p><b>Note</b> Starting with Release 7.0(3)I2(1), you cannot configure the logging level for the BCM_USD, ETHPC, FWM, and NOHMS processes. For the BCM_USD process, use <b>attach module 1</b> command and then configure the logging level.</p> <p><b>Note</b> If the default severity and the current session severity of a component is same, then it is expected to not see the logging level for the component in the running configuration. The default logging level is not displayed in the running configuration, but it is displayed in the <b>show logging level</b> command.</p>
<b>Step 4</b>	(Optional) switch(config)# <b>no logging module</b> [severity-level]	Disables module log messages.
<b>Step 5</b>	(Optional) switch(config)# <b>no logging level</b> [facility severity-level]	Resets the logging severity level for the specified facility to its default level. If you do not specify a facility and severity level, the switch resets all facilities to their default levels.
<b>Step 6</b>	(Optional) switch# <b>show logging module</b>	Displays the module logging configuration.
<b>Step 7</b>	(Optional) switch# <b>show logging level</b> [facility]	Displays the logging level configuration and the system default level by facility. If you do not specify a facility, the switch displays levels for all facilities.



	Command or Action	Purpose
<b>Step 8</b>	(Optional) switch# <b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.

### Example

The following example shows how to configure the severity level of module and specific facility messages:

```
switch# configure terminal
switch(config)# logging module 3
switch(config)# logging level aaa 2
```

## Configuring Logging Timestamps

You can configure the time-stamp units of messages logged by the Cisco Nexus Series switch.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>logging timestamp {microseconds   milliseconds   seconds}</b>	Sets the logging time-stamp units. By default, the units are seconds.
<b>Step 3</b>	(Optional) switch(config)# <b>no logging timestamp {microseconds   milliseconds   seconds}</b>	Resets the logging time-stamp units to the default of seconds.
<b>Step 4</b>	(Optional) switch# <b>show logging timestamp</b>	Displays the logging time-stamp units configured.
<b>Step 5</b>	(Optional) switch# <b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.

### Example

The following example shows how to configure the time-stamp units of messages:

```
switch# configure terminal
switch(config)# logging timestamp milliseconds
switch(config)# exit
switch# show logging timestamp
Logging timestamp:                Milliseconds
```

## Configuring the ACL Logging Cache

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>logging ip access-list cache entries</b> <i>num_entries</i>	Sets the maximum number of log entries cached in software. The range is from 0 to 1000000 entries. The default value is 8000 entries.
<b>Step 3</b>	switch(config)# <b>logging ip access-list cache interval</b> <i>seconds</i>	Sets the number of seconds between log updates. Also if an entry is inactive for this duration, it is removed from the cache. The range is from 5 to 86400 seconds. The default value is 300 seconds.
<b>Step 4</b>	switch(config)# <b>logging ip access-list cache threshold</b> <i>num_packets</i>	Sets the number of packet matches before an entry is logged. The range is from 0 to 1000000 packets. The default value is 0 packets, which means that logging is not triggered by the number of packet matches.
<b>Step 5</b>	(Optional) switch(config)# <b>copy running-config startup-config</b>	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

### Example

The following example show how to set the maximum number of log entries to 5000, the interval to 120 seconds, and the threshold to 500000:

```
switch# configure terminal
switch(config)# logging ip access-list cache entries 5000
switch(config)# logging ip access-list cache interval 120
switch(config)# logging ip access-list cache threshold 500000
switch(config)# copy running-config startup-config
```

## Applying ACL Logging to an Interface

### Before you begin

- Create an IP access list with at least one access control entry (ACE) configured for logging.
- Configure the ACL logging cache.
- Configure the ACL log match level.

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>interface mgmt0</b>	Specifies the mgmt0 interface.
<b>Step 3</b>	switch(config-if)# <b>ip access-group name in</b>	Enables ACL logging on ingress traffic for the specified interface.
<b>Step 4</b>	(Optional) switch(config-if)# <b>copy running-config startup-config</b>	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

**Example**

The following example shows how to apply the mgmt0 interface with the logging specified in acl1 for all ingress traffic:

```
switch# configure terminal
switch(config)# interface mgmt0
switch(config-if)# ip access-group acl1 in
switch(config-if)# copy running-config startup-config
```

## Configuring a Logging Source-Interface

You can set all system logging (syslog) messages that are sent to syslog servers to contain the same IP address as the source address, regardless of which interface the syslog message uses to exit the router. The system allows a user-configured source-IP in a syslog packet specified by the source-interface.



**Note** If a valid IP address is not assigned, the syslog is thrown and messages are sent out carrying the exit interfaces IP address.

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>[no] logging source-interface [ethernet slot/port   loopback interface-number   mgmt interface-number   port-channel port channel-number   vlan interface-number   tunnel interface-number]</b>	<ul style="list-style-type: none"> <li>• <b>ethernet</b>—The range for the Ethernet option source-interface is from 1 to 253.</li> <li>• <b>loopback</b>—The range for the loopback option source-interface is from 1 to 1023.</li> <li>• <b>mgmt</b>—The interface number for the management option source-interface is 0.</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• <b>port-channel</b>—The range for the port channel option source-interface is from 1 to 4096.</li> </ul>
<b>Step 3</b>	(Optional) switch(config)# <b>copy running-config startup-config</b>	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

### Example

The following example shows how to configure the source-interface as the ethernet interface:

```
switch# configure terminal
switch(config)# logging source-interface ethernet 2/1
switch(config)# copy running-config startup-config
```

## Configuring the ACL Log Match Level

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>acllog match-log-level</b> <i>number</i>	<p>Specifies the logging level to match for entries to be logged in the ACL log (acllog). The <i>number</i> is a value from 0 to 7. The default is 6.</p> <p><b>Note</b> For log messages to be entered in the logs, the logging level for the ACL log facility (acllog) and the logging severity level for the logfile must be greater than or equal to the ACL log match log level setting. For more information, see <a href="#">Configuring Module and Facility Messages Logging, on page 7</a> and <a href="#">Configuring System Message Logging to a File, on page 5</a>.</p>
<b>Step 3</b>	(Optional) switch(config)# <b>copy running-config startup-config</b>	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

## Configuring Syslog Servers

You can configure up to eight syslog servers that reference remote systems where you want to log system messages.



**Note** Cisco recommends that you configure the syslog server to use the management virtual routing and forwarding (VRF) instance. For more information on VRFs, see [Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide](#).

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>logging server</b> <i>host</i> [ <i>severity-level</i> [ <b>use-vrf</b> <i>vrf-name</i> [ <b>facility</b> <i>facility</i> ]]]  <b>Example:</b> <pre>switch(config)# logging server 172.28.254.254 5 use-vrf default facility local3</pre>	Configures a host to receive syslog messages. <ul style="list-style-type: none"> <li>• The <i>host</i> argument identifies the hostname or the IPv4 or IPv6 address of the syslog server host.</li> <li>• The <i>severity-level</i> argument limits the logging of messages to the syslog server to a specified level. Severity levels range from 0 to 7. See <a href="#">Table 1: System Message Severity Levels</a>, on page 1.</li> <li>• The <b>use vrf</b> <i>vrf-name</i> keyword identifies the default or management values for the VRF name. If a specific VRF is not identified, management is the default.</li> </ul> The <b>show running</b> command output can display or not display the VRF based on the following configuration scenarios: <ul style="list-style-type: none"> <li>• You have not configured any VRF and the system takes the management VRF as the default. Then this VRF is not displayed in the output.</li> <li>• You have configured management VRF. Then this VRF is not displayed in the output as the system identifies it as the default.</li> <li>• You have configured any other VRF. Then this VRF is displayed in the output.</li> </ul>

	Command or Action	Purpose
		<p><b>Note</b> The current Cisco Fabric Services (CFS) distribution does not support VRF. If CFS distribution is enabled, the logging server configured with the default VRF is distributed as the management VRF.</p> <ul style="list-style-type: none"> <li>The facility argument names the syslog facility type. The default outgoing facility is local7.</li> </ul> <p>The facilities are listed in the command reference for the Cisco Nexus Series software that you are using.</p> <p><b>Note</b> Debugging is a CLI facility but the debug syslogs are not sent to the server.</p>
<b>Step 3</b>	<p>(Optional) <b>no logging server</b> <i>host</i></p> <p><b>Example:</b></p> <pre>switch(config)# no logging server 172.28.254.254 5</pre>	Removes the logging server for the specified host.
<b>Step 4</b>	<p>(Optional) <b>show logging server</b></p> <p><b>Example:</b></p> <pre>switch# show logging server</pre>	Displays the syslog server configuration.
<b>Step 5</b>	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config)# copy running-config startup-config</pre>	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

### Example

The following examples show how to configure a syslog server:

```
switch# configure terminal
switch(config)# logging server 172.28.254.254 5
use-vrf default facility local3
```

```
switch# configure terminal
switch(config)# logging server 172.28.254.254 5 use-vrf management facility local3
```

## Configuring syslog on a UNIX or Linux System

You can configure a syslog server on a UNIX or Linux system by adding the following line to the `/etc/syslog.conf` file:

```
facility.level <five tab characters> action
```

The following table describes the syslog fields that you can configure.

**Table 3: syslog Fields in syslog.conf**

Field	Description
Facility	Creator of the message, which can be <code>auth</code> , <code>authpriv</code> , <code>cron</code> , <code>daemon</code> , <code>kern</code> , <code>lpr</code> , <code>mail</code> , <code>mark</code> , <code>news</code> , <code>syslog</code> , <code>user</code> , <code>local0</code> through <code>local7</code> , or an asterisk (*) for all. These facility designators allow you to control the destination of messages based on their origin.  <b>Note</b> Check your configuration before using a local facility.
Level	Minimum severity level at which messages are logged, which can be <code>debug</code> , <code>info</code> , <code>notice</code> , <code>warning</code> , <code>err</code> , <code>crit</code> , <code>alert</code> , <code>emerg</code> , or an asterisk (*) for all. You can use <code>none</code> to disable a facility.
Action	Destination for messages, which can be a filename, a hostname preceded by the at sign (@), or a comma-separated list of users or an asterisk (*) for all logged-in users.

### Procedure

**Step 1** Log debug messages with the `local7` facility in the file `/var/log/myfile.log` by adding the following line to the `/etc/syslog.conf` file:

```
debug.local7 /var/log/myfile.log
```

**Step 2** Create the log file by entering these commands at the shell prompt:

```
$ touch /var/log/myfile.log
$ chmod 666 /var/log/myfile.log
```

**Step 3** Make sure that the system message logging daemon reads the new changes by checking `myfile.log` after entering this command:

```
$ kill -HUP ~cat /etc/syslog.pid~
```

## Configuring Secure Syslog Servers

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>[no] logging server host [severity-level [port port-number]][secure[trustpoint client-identity trustpoint-name]][use-vrf vrf-name]]</b>  <b>Example:</b> <pre>switch(config)# logging server 192.0.2.253 secure</pre> <b>Example:</b> <pre>switch(config)# logging server 2001::3 5 secure trustpoint client-identity myCA use-vrf red</pre>	<p>Configures a syslog server at the specified hostname or IPv4 or IPv6 address. Optionally, you can enforce a mutual authentication by installing the client identity certificate that is signed by any CA and using the trustpoint client-identity option.</p> <p>The default destination port for a secure TLS connection is 6514.</p>
<b>Step 3</b>	<b>(Optional) logging source-interface interface name</b>  <b>Example:</b> <pre>switch(config)# logging source-interface lo0</pre>	Enables a source interface for the remote syslog server.
<b>Step 4</b>	<b>(Optional) show logging server</b>  <b>Example:</b> <pre>switch(config)# show logging server</pre>	Displays the syslog server configuration. If the secure option is configured, the output will have an entry with the transport information. By default, the transport is UDP if the secure option is not configured.
<b>Step 5</b>	<b>(Optional) copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

## Configuring the CA Certificate

For the secure syslog feature support, the remote servers must be authenticated via a trustpoint configuration.



## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>[no] crypto ca trustpoint <i>trustpoint-name</i></b> <b>Example:</b> switch(config)# crypto ca trustpoint winca switch(config-trustpoint)#	Configures a trustpoint. <b>Note</b> You must configure the ip domain-name before the trustpoint configuration.
<b>Step 3</b>	Required: <b>crypto ca authenticate <i>trustpoint-name</i></b> <b>Example:</b> switch(config-trustpoint)# crypto ca authenticate winca	Configures a CA certificate for the trustpoint.
<b>Step 4</b>	(Optional) <b>show crypto ca certificate</b> <b>Example:</b> switch(config)# show crypto ca certificates	Displays the configured certificate/chain and the associated trustpoint.
<b>Step 5</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration so that the trustpoint is persistent across the reload of the device.

## Enrolling the CA Certificate

For mutual authentication, where the remote server wants the NX-OS switch (the client) to identify, that the peer authentication is mandatory, this is an additional configuration to enroll the certificate on the switch.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	Required: <b>crypto key generate rsa label <i>key name</i> exportable modules 2048</b> <b>Example:</b>	Configure an RSA key pair. By default, the Cisco NX-OS software generates an RSA key using 1024 bits.

	Command or Action	Purpose
	<pre>switch(config-trustpoint)# crypto key generate rsa label myKey exportable modulus 2048</pre>	
<b>Step 3</b>	<b>[no] crypto ca trustpoint <i>trustpoint-name</i></b> <b>Example:</b> <pre>switch(config)# crypto ca trustpoint myCA switch(config-trustpoint)#</pre>	Configures a trustpoint. <b>Note</b> You must configure the ip domain-name before the trustpoint configuration.
<b>Step 4</b>	Required: <b>rsa keypair <i>key-name</i></b> <b>Example:</b> <pre>switch(config-trustpoint)# rsa keypair myKey</pre>	Associates the keypair generated to the trustpoint CA.
<b>Step 5</b>	<b>crypto ca trustpoint <i>trustpoint-name</i></b> <b>Example:</b> <pre>switch(config)# crypto ca authenticate myCA</pre>	Configures a CA certificate for the trustpoint.
<b>Step 6</b>	<b>[no] crypto ca enroll <i>trustpoint-name</i></b> <b>Example:</b> <pre>switch(config)# crypto ca enroll myCA</pre>	Generate an identity certificate of the switch to enroll it to a CA.
<b>Step 7</b>	<b>crypto ca import <i>trustpoint-name</i> certificate</b> <b>Example:</b> <pre>switch(config-trustpoint)# crypto ca import myCA certificate</pre>	Imports the identity certificate signed by the CA to the switch.
<b>Step 8</b>	(Optional) <b>show crypto ca certificates</b> <b>Example:</b> <pre>switch# show crypto ca certificates</pre>	Displays the configured certificate or chain and the associated trustpoint.
<b>Step 9</b>	Required: <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

## Configuring syslog Server Configuration Distribution

You can distribute the syslog server configuration to other switches in the network by using the Cisco Fabric Services (CFS) infrastructure.

After you enable syslog server configuration distribution, you can modify the syslog server configuration and view the pending changes before committing the configuration for distribution. As long as distribution is enabled, the switch maintains pending changes to the syslog server configuration.



**Note** If the switch is restarted, the syslog server configuration changes that are kept in volatile memory might get lost.

### Before you begin

You must have configured one or more syslog servers.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>logging distribute</b>	Enables distribution of the syslog server configuration to network switches using the CFS infrastructure. By default, distribution is disabled.
<b>Step 3</b>	switch(config)# <b>logging commit</b>	Commits the pending changes to the syslog server configuration for distribution to the switches in the fabric.
<b>Step 4</b>	switch(config)# <b>logging abort</b>	Cancels the pending changes to the syslog server configuration.
<b>Step 5</b>	(Optional) switch(config)# <b>no logging distribute</b>	Disables the distribution of the syslog server configuration to network switches using the CFS infrastructure. You cannot disable distribution when configuration changes are pending. See the <b>logging commit</b> and <b>logging abort</b> commands. By default, distribution is disabled.
<b>Step 6</b>	(Optional) switch# <b>show logging pending</b>	Displays the pending changes to the syslog server configuration.
<b>Step 7</b>	(Optional) switch# <b>show logging pending-diff</b>	Displays the differences from the current syslog server configuration to the pending changes of the syslog server configuration.
<b>Step 8</b>	(Optional) switch# <b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.

## Displaying and Clearing Log Files

You can display or clear messages in the log file and the NVRAM.

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	switch# <b>show logging last</b> <i>number-lines</i>	Displays the last number of lines in the logging file. You can specify from 1 to 9999 for the last number of lines.
<b>Step 2</b>	switch# <b>show logging logfile</b> [ <b>start-time</b> <i>yyyy mmm dd hh:mm:ss</i> ] [ <b>end-time</b> <i>yyyy mmm dd hh:mm:ss</i> ]	Displays the messages in the log file that have a time stamp within the span entered. If you do not enter an end time, the current time is used. You enter three characters for the month time field and digits for the year and day time fields.
<b>Step 3</b>	switch# <b>show logging nvram</b> [ <b>last</b> <i>number-lines</i> ]	Displays the messages in the NVRAM. To limit the number of lines displayed, you can enter the last number of lines to display. You can specify from 1 to 100 for the last number of lines.
<b>Step 4</b>	switch# <b>clear logging logfile</b>	Clears the contents of the log file.
<b>Step 5</b>	switch# <b>clear logging nvram</b>	Clears the logged messages in NVRAM.

**Example**

The following example shows how to display messages in a log file:

```
switch# show logging last 40
switch# show logging logfile start-time 2007 nov 1 15:10:0
switch# show logging nvram last 10
```

The following example shows how to clear messages in a log file:

```
switch# clear logging logfile
switch# clear logging nvram
```

## Verifying the System Message Logging Configuration

Use these commands to verify system message logging configuration information:

<b>Command</b>	<b>Purpose</b>
<b>show logging console</b>	Displays the console logging configuration.
<b>show logging info</b>	Displays the logging configuration.
<b>show logging ip access-list cache</b>	Displays the IP access list cache.
<b>show logging ip access-list cache detail</b>	Displays detailed information about the IP access list cache.

Command	Purpose
<b>show logging ip access-list status</b>	Displays the status of the IP access list cache.
<b>show logging last</b> <i>number-lines</i>	Displays the last number of lines of the log file.
<b>show logging level</b> [ <i>facility</i> ]	Displays the facility logging severity level configuration.
<b>show logging logfile</b> [ <b>start-time</b> <i>yyyy mmm dd hh:mm:ss</i> ] [ <b>end-time</b> <i>yyyy mmm dd hh:mm:ss</i> ]	Displays the messages in the log file.
<b>show logging module</b>	Displays the module logging configuration.
<b>show logging monitor</b>	Displays the monitor logging configuration.
<b>show logging nvram</b> [ <b>last</b> <i>number-lines</i> ]	Displays the messages in the NVRAM log.
<b>show logging pending</b>	Displays the syslog server pending distribution configuration.
<b>show logging pending-diff</b>	Displays the syslog server pending distribution configuration differences.
<b>show logging server</b>	Displays the syslog server configuration.
<b>show logging session</b>	Displays the logging session status.
<b>show logging status</b>	Displays the logging status.
<b>show logging timestamp</b>	Displays the logging time-stamp units configuration.
<b>show running-config acllog</b>	Displays the running configuration for the ACL log file.

