Logging Commands

banner login

To define and enable a customized banner to be displayed before the username and password login prompts, use the **banner login** command in global configuration mode. To disable the login banner, use **no** form of this command.

banner login *message*
no banner login

Command Default

Disabled (no login banner is displayed).

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

To configure multi-line banner use \\x0a as newline character. For usage guidelines, see the Cisco IOS XE banner login command.

Examples

The following example sets a login banner.

```
Device# banner login Access for authorized users only. Please enter your username and
password.


Device#show banner login
Access for authorized users only. Please enter your username and password.
Device#
```

logging buffered

To enable system message logging to a local buffer, use the **logging buffered** command in global configuration mode. To cancel the use of the buffer, use the **no** form of this command. To return the buffer size to its default value, use the **default** form of this command.

logging buffered *buffer-size*
no logging buffered
default logging buffered

Syntax Description

buffer-size	Size of the buffer, in bytes. The range is 4096 to 2147483647. The default size varies by platform.

Command Default

Varies by platform. For most platforms, logging to the buffer is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE logging buffered command.

Examples

The following example shows how to enable standard system logging to the local syslog buffer:

```
Router(config)# logging buffered
```

logging console

To send system logging (syslog) messages to all available TTY lines and limit messages based on severity, use the **logging console** command in global configuration mode. To disable logging to the console terminal, use the **no** form of this command.

logging console
no logging console

Command Default

The default varies by platform. In general, the default is to log all messages.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE logging console command.

Examples

The following is an example for this command:

```
Router(config)# logging console
```

logging discriminator

To create a syslog message discriminator, use the **logging discriminator** command in global configuration mode. To disable the syslog message discriminator, use the **no** form of this command.

logging discriminator *discr-name* [[**facility**] [**mnemonics**] [**msg-body**] { **drops** *string* | **includes** *string* }] [**severity** { **drops** *sev-num* | **includes** *sev-num* }] [**rate-limit** *msglimit*]
no logging discriminator *discr-name*

Syntax Description

discr-name	String of a maximum of eight alphanumeric, case-sensitive characters. Blank spaces between characters are not allowed.
facility	(Optional) Message subfilter for the facility pattern in an event message.
mnemonics	(Optional) Message subfilter for the mnemonic pattern in an event message.
msg-body	(Optional) Message subfilter for the msg-body pattern in an event message.
drops	Drops messages that match the pattern, including the specified regular expression.
includes	Delivers messages that match the pattern, including the specified regular expression string.

string	(Optional) Expression used for message filtering.
severity	(Optional) Message subfilter by severity level or group.
sev-num	(Optional) Integer that identifies the severity level or multiple levels. Multiple levels must be separated with a comma (,).
rate-limit	(Optional) Specifies a number of messages to be processed within a unit of time.
msglimit	(Optional) Integer in the range of 1 to 10000 that identifies the number of messages not to be exceeded.

Command Default

The logging discriminator function is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This command was introduced.

Usage Guidelines

If you enter a discriminator name that was previously specified, your entry is treated as a modification to the discriminator. The modification becomes effective when the configuration is completed. All associated sessions will use the modified value. When you remove a discriminator, the associations of all entries in the logging host list are removed.

When you issue the**no logging discriminator** command and the discriminator name is not found, an error message is generated. If the discriminator name is valid and actively associated with syslog sessions, the effect is immediate; the next syslog message to be processed will go through.

Subfilters are checked in the following order. If a message is dropped by any of the subfilters, the remaining checks are skipped.

1. Severity level or levels specified
2. Facility within the message body that matches a regular expression
3. Mnemonic that matches a regular expression
4. Part of the body of a message that matches a regular expression
5. Rate-limit

Examples

The following example shows how to enable the logging discriminator named msglog01 to filter messages with a severity level of 5.

```
Device(config)# logging discriminator msglog01 severity includes 5
```

logging host

To log system messages and debug output to a remote host, use the **logging host** command in global configuration mode. To remove a specified logging host from the configuration, use the **no** form of this command.

logging host { [{ *ip-address* }] [**vrf** *vrf-value*] }

Syntax Description

ip-address	(Optional) IP address of the host that will receive the system logging (syslog) messages.
vrf *vrf-value*	(Optional) Specifies a VPN routing and forwarding instance (VRF) that connects to the syslog server host.

Command Default

System logging messages are not sent to any remote host.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE logging host command.

Note Creating and deleting the logging host configurations in same transaction causes unexpected behaviour. For example, deleting **logging host** *ipv4-address* and creating **logging host** *ipv4-address* **vrf** *vrf-name* configuration in same transaction causes both configurations to disappear from the device. We recommend you to send the two requests in separate transactions.

Examples

In the following example, messages are logged to a host with an IP address of 172.16.150.63 connected through a VRF:

```
Router(config)# logging host 172.16.150.63 vrf 4
```

logging monitor

To enable system message logging to the terminal lines (monitor connections), use the **logging console** command in global configuration mode. To disable all logging to the monitor connections, use the **no** form of this command.

logging monitor
no logging monitor

Command Default

Logging to monitor connections is enabled.

The default severity level varies by platform, but is generally level 7 (messages at levels 0 through 7 are logged).

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE logging monitor command.

Examples

In the following example, the user enables system message logging to the console for messages:

```
Router(config)# logging monitor
```

logging persistent

To enable the storage of logging messages on the router's advanced technology attachment (ATA) disk, use the **logging persistent** command in global configuration mode. To disable logging message storage on the ATA disk, use the **no** form of this command.

logging persistent { **filesize** *logging-file-size* } { **size** *filesystem-size* }
no logging persistent

Syntax Description

filesize *logging-file-size*	(Optional) Specifies the size of individual logging files in bytes. • Minimum value is 8192. • Maximum value is 2147483647. • Default value is 262144.
size *filesystem-size*	(Optional) Specifies the amount of disk space, in bytes, allocated to syslog messages. • Minimum value is 16384. • Maximum value is 2147483647. • Default value is 10 percent of the total disk space.

Command Default

The logging messages are not stored in the router's ATA memory.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE logging persistent command.

Examples

The following is an example:

```
Router> enable
Router# configure terminal
Router(config)# logging persistent size 104857600 filesize 10485760
Router(config)# exit
```

logging rate-limit

To limit the rate of messages logged per second, use the **logging rate-limit** command in global configuration mode . To disable the limit, use the **no** form of this command.

logging rate-limit
no logging rate-limit

Command Default

The default is 10 messages logged per second.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE logging rate-limit command.

Examples

The following is an example of this command:

```
Router(config)# logging rate-limit
```

logging source-interface

To specify the source IPv4 or IPv6 address of system logging packets, use the **logging source-interface** command in global configuration mode. To remove the source designation, use the **no** form of this command.

logging source-interface [{ **interface-name** *number* **vrf** *vrf-name* }]
no logging source-interface [{ **interface-name** *number* **vrf** *vrf-name* }]

Syntax Description

Interface-name *number*	Interface type and number.
vrf *vrf-name*	Provides logging source-interface setting capability to Virtual Routing and Forwarding (VRF) syslog destinations. Name assigned to the VRF.

Command Default

The wildcard interface address is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE logging source-interface command.

Examples

The following example shows how to specify that the IP address of Ethernet interface 0 as the source IP address for all syslog messages:

```
Router(config)# logging source-interface loopback111 vrf4
```

logging tls-profile ciphersuite

To set the cipher suite for logging tls-profiles, use the **logging tls-profile ciphersuite** command in global configuration mode. To remove the cipher suite, use the **no** form of this command.

logging tls-profile *name* **ciphersuite** { **aes-128-cbc-sha** | **aes-256-cbc-sha** | **dhe-aes-cbc-sha2** | **dhe-aes-gcm-sha2** | **ecdhe-ecdsa-aes-gcm-sha2** | **ecdhe-rsa-aes-cbc-sha2** | **ecdhe-rsa-aes-gcm-sha2** | **rsa-aes-cbc-sha2** | **rsa-aes-gcm-sha2** }
no logging tls-profile *name* **ciphersuite** { **aes-128-cbc-sha** | **aes-256-cbc-sha** | **dhe-aes-cbc-sha2** | **dhe-aes-gcm-sha2** | **ecdhe-ecdsa-aes-gcm-sha2** | **ecdhe-rsa-aes-cbc-sha2** | **ecdhe-rsa-aes-gcm-sha2** | **rsa-aes-cbc-sha2** | **rsa-aes-gcm-sha2** }

Syntax Description

name	Name of existing or new logging tls-profile.
aes-128-cbc-sha	Specifies the ciphersuite to aes-128-cbc-sha.
aes-256-cbc-sha	Specifies the ciphersuite to aes-256-cbc-sha.
dhe-aes-cbc-sha2	Specifies the ciphersuite to dhe-aes-cbc-sha2.
dhe-aes-gcm-sha2	Specifies the ciphersuite to dhe-aes-gcm-sha2.
ecdhe-ecdsa-aes-gcm-sha2	Specifies the ciphersuite to ecdhe-ecdsa-aes-gcm-sha2.
ecdhe-rsa-aes-cbc-sha2	Specifies the ciphersuite to ecdhe-rsa-aes-cbc-sha2.
ecdhe-rsa-aes-gcm-sha2	Specifies the ciphersuite to ecdhe-rsa-aes-gcm-sha2.

rsa-aes-cbc-sha2	Specifies the ciphersuite to rsa-aes-cbc-sha2.
rsa-aes-gcm-sha2	Specifies the ciphersuite to rsa-aes-gcm-sha2.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

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. Use this **logging tls-profile ciphersuite** command to set the cipher suite of the logging tls-profile.

Example

The following example shows how to set the cipher suite of profile1 to aes-256-cbc-sha.

```
Device(config)# logging tls-profile profile1 ciphersuite aes-256-cbc-sha
```

Table 1: Related Commands

Command	Description
tls-version	Specifies the TLS version.
client-id-trustpoint	Specifies the client ID trustpoint.

logging tls-profile tls-version

To set the tls-version for logging tls-profiles, use the **logging tls-profile tls-version** command in global configuration mode. To remove the tls-version, use the **no** form of this command.

logging tls-profile *name* **tls-version** { **TLSv1.1** | **TLSv1.2** }
no logging tls-profile *name* **tls-version**

Syntax Description

name	Name of logging tls-profile.
TLSv1.1	Specifies TLSv1.1 as the version to be used.
TLSv1.2	Specifies TLSv1.2 as the version to be used.

Command Default

None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Cisco IOS XE Catalyst SD-WAN devices now support sending secure syslog messages over 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. Use this **logging tls-profile tls-version** command to set the tls-version of the logging tls-profile to TLSv1.1 or TLSv1.2.

Example

The following example shows how to set the tls-version of profile1 to TLSv1.1.

```
Device(config)# logging tls-profile profile1 tls-version TLSv1.1
```

Table 2: Related Commands

Command	Description
ciphersuite	Specifies the cipher suite.
client-id-trustpoint	Specifies the client ID trustpoint.

logging trap

To limit messages logged to the syslog servers based on severity, use the **logging trap** command in global configuration mode . To return the logging to remote hosts to the default level, use the **no** form of this command.

logging trap { [**errors**] }
no logging trap

Command Default Syslog messages at level 0 to level 6 are generated, but will only be sent to a remote host if the **logging host** command is configured.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines For usage guidelines, see the Cisco IOS XE logging trap command.

Examples In the following is an example for this command:

```
Router(config)# logging trap error
```

logging trap informational syslog-format rfc5424

To set the logging trap level to informational and the syslog format to rfc5424, use the **logging trap informational syslog-format rfc5424** command in global configuration mode. To remove the logging trap informational syslog-format rfc5424, use the **no** form of this command.

logging trap informational syslog-format rfc5424
no logging trap informational syslog-format rfc5424

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

There are various severity levels of message logging. Specifying a level causes messages at that level and numerically lower levels to be displayed at the destination. There are two syslog formats - RFC3164 and RFC5424. Use this **logging trap informational syslog-format rfc5424** command to set the logging trap level to informational and the syslog format to rfc5424.

Example

The following example shows how to set the trap level to informational and syslog format to rfc5424.

```
Device(config)# logging trap informational syslog-format rfc5424
```

service timestamps

To configure the system to apply a time stamp to debugging messages or system logging messages, use the **service timestamps** command in global configuration mode. To disable this service, use the **no** form of this command.

service timestamps [{ **debug** | **log** }] { **datetime** } [{ **msec** | **localtime** | **show-timezone** | **year** }]
no service timestamps [{ **debug** | **log** }]

Syntax Description

debug	(Optional) Indicates time-stamping for debugging messages.
log	(Optional) Indicates time-stamping for system logging messages.

datetime	(Optional) Specifies that the time stamp should consist of the date and time. • The time-stamp format for **datetime** is MMM DD HH:MM:SS, where MMM is the month, DD is the date, HH is the hour (in 24-hour notation), MM is the minute, and SS is the second. • If the datetime keyword is specified, you can optionally add the **msec**, **localtime**, **show-timezone**, or **year** keywords. • If the **service timestamps datetime** command is used without addtional keywords, time stamps will be shown using UTC, without the year, without milliseconds, and without a time zone name.
msec	(Optional) Includes milliseconds in the time stamp, in the format HH: DD: MM: SS. mmm, where .mmm is milliseconds.
localtime	(Optional) Time stamp relative to the local time zone.
year	(Optional) Include the year in the date-time format.
show-timezone	(Optional) Include the time zone name in the time stamp. **Note** If the localtime keyword option is not used (or if the local time zone has not been configured using the **clock timezone** command), time will be displayed in Coordinated Universal Time (UTC).

Command Default

Time stamps are applied to debug and logging messages.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE service timestamps command.

Examples

The following example shows how to enable time-stamping on logging messages using the current time and date in Coordinated Universal Time/Greenwich Mean Time (UTC/GMT), and enable the year to be displayed:

```
Device(config)# service timestamps log datetime show-timezone year
 Device(config)# end
! The following line shows the timestamp with datetime (11:13 PM March 22nd)
.Mar 22 2004 23:13:25 UTC: %SYS-5-CONFIG_I: Configured from console by console
```

In the following example, the **service timestamps log datetime** command is used to change previously configured options for the date-time time stamp.

```
Device(config)# service timestamps log datetime localtime show-timezone
Device(config)# end
! The year is not displayed.
Oct 13 15:44:46 PDT: %SYS-5-CONFIG_I: Configured from console by console
```

```
Enter configuration commands, one per line.  End with the end command.
Device(config)# service timestamps log datetime show-timezone year
Device(config)# end

! note: because the localtime option was not specified again, that option is removed from
the output,
and time is displayed in UTC (the default)

Oct 13 2004 22:45:31 UTC: %SYS-5-CONFIG_I: Configured from console by console
```