

SYSLOG Commands

This chapter contains the following sections:

- aaa logging, on page 2
- clear logging, on page 3
- clear logging file, on page 4
- file-system logging, on page 5
- logging buffered, on page 6
- logging console, on page 7
- logging file, on page 8
- logging file threshold percent, on page 9
- logging host , on page 10
- logging on, on page 11
- logging source-interface, on page 12
- logging source-interface-ipv6, on page 13
- logging aggregation on, on page 14
- logging aggregation aging-time, on page 15
- logging origin-id, on page 16
- logging cbd module, on page 17
- logging cbd level, on page 18
- show logging, on page 19
- show logging file, on page 20
- show syslog-servers, on page 21

aaa logging

To enable logging AAA logins, use the **aaa logging** Global Configuration mode command. To disable logging AAA logins, use the **no** form of this command.

Syntax

aaa logging {**login**}

no aaa logging {**login**}

Parameters

login—Enables logging messages related to successful AAA login events, unsuccessful AAA login events and other AAA login-related events.

Default Configuration

Enabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables logging messages related to successful login events, unsuccessful login events and other login-related events. Other types of AAA events are not subject to this command.

Example

The following example enables logging AAA login events.

```
switchxxxxxx(config)# aaa logging login
```

clear logging

To clear messages from the internal logging buffer, use the **clear logging** Privileged EXEC mode command.

Syntax

clear logging

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example clears messages from the internal logging buffer.

```
switchxxxxxx# clear logging
Clear Logging Buffer ? (Y/N)[N]
```

clear logging file

To clear messages from the logging file, use the **clear logging file** Privileged EXEC mode command.

Syntax

clear logging file

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example clears messages from the logging file.

```
switchxxxxxx# clear logging file
Clear Logging File [y/n]
```

file-system logging

To enable logging file system events, use the **file-system logging** Global Configuration mode command. To disable logging file system events, use the **no** form of this command.

Syntax

file-system logging *{***copy** | **delete-rename***}*

no file-system logging *{***copy** | **delete-rename***}*

Parameters

- **copy**—Specifies logging messages related to file copy operations.
- **delete-rename**—Specifies logging messages related to file deletion and renaming operations.

Default Configuration

Enabled.

Command Mode

Global Configuration mode

Example

The following example enables logging messages related to file copy operations.

```
switchxxxxxx(config)# file-system logging copy
```

logging buffered

To limit the SYSLOG message display to messages with a specific severity level, and to define the buffer size (number of messages that can be stored), use the **logging buffered** Global Configuration mode command. To cancel displaying the SYSLOG messages, and to return the buffer size to default, use the **no** form of this command.

Syntax

logging buffered [*buffer-size*] [*severity-level* | *severity-level-name*]

no logging buffered

Parameters

- **buffer-size**—(Optional) Specifies the maximum number of messages stored in buffer. (Range: 20–1000)
- **severity-level**—(Optional) Specifies the severity level of messages logged in the buffer. The possible values are: 1-7.
- **severity-level-name**—(Optional) Specifies the severity level of messages logged in the buffer. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

Default Configuration

The default severity level is informational.

The default buffer size is 1000.

Command Mode

Global Configuration mode

User Guidelines

All the SYSLOG messages are logged to the internal buffer. This command limits the messages displayed to the user.

Example

The following example shows two ways of limiting the SYSLOG message display from an internal buffer to messages with severity level **debugging**. In the second example, the buffer size is set to 100 and severity level **informational**.

```
switchxxxxxx(config)# logging buffered debugging
switchxxxxxx(config)# logging buffered 100 informational
```

logging console

To limit messages logged to the console to messages to a specific severity level, use the **logging console** Global Configuration mode command. To restore the default, use the **no** form of this command.

Syntax

logging console *level*

no logging console

Parameters

level—Specifies the severity level of logged messages displayed on the console. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

Default Configuration

Informational.

Command Mode

Global Configuration mode

Example

The following example limits logging messages displayed on the console to messages with severity level **errors**.

```
switchxxxxxx(config)# logging console errors
```

logging file

To limit SYSLOG messages sent to the logging file to messages with a specific severity level, use the **logging file** Global Configuration mode command. To cancel sending messages to the file, use the **no** form of this command.

Syntax

logging file *level*

no logging file

Parameters

level—Specifies the severity level of SYSLOG messages sent to the logging file. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

Default Configuration

The default severity level is **errors**.

Command Mode

Global Configuration mode

Example

The following example limits SYSLOG messages sent to the logging file to messages with severity level **alerts**.

```
switchxxxxxx(config)# logging file alerts
```

logging file threshold percent

To enable the logging file usage alarm, and to configure the alarm threshold, use the logging file threshold Global Configuration mode command. To disable the logging file usage alarm, use the no form of this command.

Syntax

logging file threshold *percent*

no logging file threshold

Parameters

percent —Specifies the alarm threshold in percents (range 1-99).

Default Configuration

Logging file usage alarm is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the logging file threshold command to enable logging file usage alarm and to set the threshold at which the alarm will be generated. Once the logging file capacity passes the defined threshold a syslog message will be generated to indicate the logging file passed the defined threshold. Using the no form of the command will disable the logging file threshold alarm.

Example

The following example defines 50% as the threshold for the logging file.

```
switchxxxxxx(config)# logging file threshold 50
```

logging host

To log messages to the specified SYSLOG server, use the **logging host** Global Configuration command. To delete the SYSLOG server with the specified address from the list of SYSLOG servers, use the **no** form of this command.

Syntax

logging host *{ip-address | ipv6-address | hostname}* [**port** *port*] [**severity** *level*] [**facility** *facility*] [**description** *text*]

no logging host *{ipv4-address | ipv6-address | hostname}*

Parameters

- **ip-address**—IP address of the host to be used as a SYSLOG server. The IP address can be an IPv4, IPv6 or Ipv6z address.
- **hostname**—Hostname of the host to be used as a SYSLOG server. Only translation to IPv4 addresses is supported. (Range: 1–158 characters. Maximum label size for each part of the host name: 63)
- **transport {udp| tcp}**—(Optional) specify UDP or TCP as the transport protocol for SYLSOG messages. If unspecified, the UDP transport protocol is used.
- *port port*—(Optional) Port number for SYSLOG messages. If unspecified, the port number defaults to 514. (Range: 1–65535)
- *severity level*—(Optional) Limits the logging of messages to the SYSLOG servers to a specified level: Emergencies, Alerts, Critical, Errors, Warnings, Notifications, Informational, Debugging.
- *facility facility*—(Optional) The facility that is indicated in the message. It can be one of the following values: local0, local1, local2, local3, local4, local5, local 6, local7. If unspecified, the port number defaults to local7.
- *description text*—(Optional) Description of the SYSLOG server. (Range: Up to 64 characters)

Default Configuration

No messages are logged to a SYSLOG server.

If unspecified, the **severity level** defaults to Informational.

Command Mode

Global Configuration mode

User Guidelines

You can use multiple SYSLOG servers.

Examples

```
switchxxxxxx(config)# logging host 1.1.1.121
switchxxxxxx(config)# logging host 3000::100
```

logging on

To enable message logging, use the **logging on** Global Configuration mode command. This command sends debug or error messages asynchronously to designated locations. To disable the logging, use the **no** form of this command.

Syntax

logging on

no logging on

Parameters

This command has no arguments or keywords.

Default Configuration

Message logging is enabled.

Command Mode

Global Configuration mode

Example

The following example enables logging error messages.

```
switchxxxxxx(config)# logging on
```

logging source-interface

To specify the source interface whose IPv4 address will be used as the source IPv4 address for communication with IPv4 SYSLOG servers, use the **logging source-interface** Global Configuration mode command. To restore the default configuration, use the **no** form of this command.

Syntax

logging source-interface *interface-id*

no logging source-interface

Parameters

interface-id—Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the interface IP address belonging to the next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface, the lowest IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 SYSLOG server.

OOB cannot be defined as a source interface.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# logging source-interface vlan 100
```

logging source-interface-ipv6

To specify the source interface whose IPv6 address will be used as the source IPv6 address for communication with IPv6 SYSLOG servers, use the **logging source-interface-ipv6** Global Configuration mode command. To restore the default configuration, use the **no** form of this command.

Syntax

logging source-interface-ipv6 *interface-id*

no logging source-interface-ipv6

Parameters

interface-id—Specifies the source interface.

Default Configuration

The IPv6 source address is the defined IPv6 address of the outgoing interface and selected in accordance with RFC6724.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

If the source interface is not the outgoing interface, the minimal IPv6 address defined on the source interface with the scope of the destination IPv6 address is applied.

If there is no available IPv6 source address, a SYSLOG message is issued when attempting to communicate with an IPv6 SYSLOG server.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# logging source-interface-ipv6 vlan 100
```

logging aggregation on

To control aggregation of SYSLOG messages, use the **logging aggregation on** Global Configuration mode command. If aggregation is enabled, logging messages are displayed every time interval (according to the aging time specified by logging aggregation aging-time, on page 15). To disable aggregation of SYSLOG messages, use the **no** form of this command.

Syntax

logging aggregation on

no logging aggregation on

Parameters

This command has no arguments or keywords.

Default Configuration

Disabled

Command Mode

Global Configuration mode

Example

To turn off aggregation of SYSLOG messages:

```
switchxxxxxx(config)# no logging aggregation on
```

logging aggregation aging-time

To configure the aging time of the aggregated SYSLOG messages, use the **logging aggregation aging-time** Global Configuration mode command. The SYSLOG messages are aggregated during the time interval set by the aging-time parameter. To return to the default, use the **no** form of this command.

Syntax

logging aggregation aging-time *sec*

no logging aggregation aging-time

Parameters

aging-time *sec*—Aging time in seconds (Range: 15–3600)

Default Configuration

300 seconds.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# logging aggregation aging-time 300
```

logging origin-id

To configure the origin field of the SYSLOG message packet headers sent to the SYSLOG server, use the **logging origin-id** Global Configuration mode command. To return to the default, use the **no** form of this command.

Syntax

logging origin-id {***hostname*** | ***IP*** | ***IPv6*** | ***string*** *user-defined-id*}

no logging origin-id

Parameters

- **hostname**—The system hostname will be used as the message origin identifier.
- **IP**—IP address of the sending interface that is used as the message origin identifier.
- **IPv6**—IPv6 address of the sending interface that is used as the message origin identifier. If the sending interface is IPv4, the IPv4 address will be used instead.
- **string** *user-defined-id*—Specifies an identifying description chosen by the user. The *user-defined-id* argument is the identifying description string.

Default Configuration

No header is sent apart from the PRI field.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# logging origin-id string “Domain 1, router B”
```

logging cbd module

To define supported modules for Cisco Business Dashboard (CBD) logging, use the **logging cbd module** Global Configuration mode command. To restore the default, use the **no** form of this command.

Syntax

logging cbd module {*module* [*module2 … module6*] | ***none*** | **all}**

no logging cbd module

Parameters

- ***module*** - list includes: ***call-home, discovery, northbound, services, southbound, system***. The list replaces the previously configured list.
- **none** — disable logging for all modules.
- **all** — enable logging for all modules.

Default Configuration

Logging CBD is enabled on all modules.

Command Mode

Global Configuration mode

User Guidelines

This setting affect the CBD agent logging.

Example

The following example enables logging messages of all CBD modules.

```
switchxxxxxx(config)# logging cbd module all
```

logging cbd level

To limit messages logged of the Cisco Business Dashboard (CBD) to messages to a specific severity level, use the **logging cbd level** Global Configuration mode command. To restore the default, use the **no** form of this command.

Syntax

logging cbd level *level*

no logging cbd level

Parameters

level—Specifies the severity level of logged messages displayed on the console. The possible values are: errors, warnings, informational and debugging. This enable logging of messages with this level or higher.

Default Configuration

Informational.

Command Mode

Global Configuration mode

Example

The following example limits logging messages of the CBD to messages with severity level **errors**.

```
switchxxxxxx(config)# logging cbd errors
```

show logging

To display the logging status and SYSLOG messages stored in the internal buffer, use the **show logging** Privileged EXEC mode command.

Syntax

show logging

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example displays the logging status and the SYSLOG messages stored in the internal buffer.

```
switchxxxxxx# show logging
Logging is enabled.
```

Origin id: hostname

```
Console Logging: Level info. Console Messages: 0 Dropped.
Buffer Logging: Level info. Buffer Messages: 61 Logged, 61 Displayed, 200 Max.
File Logging: Level error. File Messages: 898 Logged, 64 Dropped.
4 messages were not logged
Application filtering control
Application            Event                 Status
--------------------   ----------------      ---------
AAA                    Login                 Enabled
File system            Copy                  Enabled
File system            Delete-Rename         Enabled
Management ACL         Deny                  Enabled
Aggregation: Disabled.
Aggregation aging time: 300 Sec
Logging cbd level: Informational
Logging cbd  modules Enabled: call-home
01-Jan-2010 05:29:46 :%INIT-I-Startup: Warm Startup
01-Jan-2010 05:29:02 :%LINK-I-Up:  Vlan 1
01-Jan-2010 05:29:02 :%LINK-I-Up:  SYSLOG6
01-Jan-2010 05:29:02 :%LINK-I-Up:  SYSLOG7
01-Jan-2010 05:29:00 :%LINK-W-Down:  SYSLOG8
```

show logging file

To display the logging status and the SYSLOG messages stored in the logging file, use the **show logging file** Privileged EXEC mode command.

Syntax

show logging file

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example displays the logging status and the SYSLOG messages stored in the logging file.

```
switchxxxxxx# show logging file
Logging is enabled.
```

Origin id: hostname

```
Console Logging: Level info. Console Messages: 0 Dropped.
Buffer Logging: Level info. Buffer Messages: 61 Logged, 61 Displayed, 200 Max.
File Logging: Level error. File Messages: 898 Logged, 64 Dropped.
4 messages were not logged
Application filtering control
Application            Event                 Status
--------------------   ----------------      ---------
AAA                    Login                 Enabled
File system            Copy                  Enabled
File system            Delete-Rename         Enabled
Management ACL         Deny                  Enabled
Aggregation: Disabled.
Aggregation aging time: 300 Sec
1-Jan-2010 05:57:00 :%SSHD-E-ERROR: SSH error: key_read: type mismatch: encoding error
01-Jan-2010 05:56:36 :%SSHD-E-ERROR: SSH error: key_read: type mismatch: encoding error
01-Jan-2010 05:55:37 :%SSHD-E-ERROR: SSH error: key_read: type mismatch: encoding error
01-Jan-2010 05:55:03 :%SSHD-E-ERROR: SSH error: key_read: key_from_blob bgEgGnt9
z6NHgZwKI5xKqF7cBtdl1xmFgSEWuDhho5UedydAjVkKS5XR2... failed
01-Jan-2010 05:55:03 :%SSHD-E-ERROR: SSH error: key_from_blob: invalid key type.
01-Jan-2010 05:56:34 :%SSHD-E-ERROR: SSH error: bad sigbloblen 58 != SIGBLOB_LEN
console#
```

show syslog-servers

To display the SYSLOG server settings, use the **show syslog-servers** Privileged EXEC mode command.

Syntax

show syslog-servers

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example provides information about the SYSLOG servers.

```
switchxxxxxx# show syslog-servers
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
Device Configuration
--------------------
IP address    Port   Facility Severity  Description
------------ ----   --------- -------- --------------
1.1.1.121     514    local7    info
3000::100     514    local7    info
OOB host Configuration
----------------------
IP address    Port   Facility Severity  Description
------------ ----   --------- -------- --------------
2.1.1.200     514    local7    warning
```