



## Configuring System Message Logging

---

This chapter describes how to configure system message logging on the Cisco MDS 9020 Fabric Switch. It includes the following sections:

- [About System Message Logging, page 14-1](#)
- [System Message Logging Configuration, page 14-3](#)
- [Displaying System Message Logging Information, page 14-5](#)
- [Default Settings, page 14-7](#)

### About System Message Logging

The system message logging software saves messages in a log file or directs the messages to other devices. This feature provides you with the following capabilities:

- Provides logging information for monitoring and troubleshooting
- Allows you to select the types of captured logging information
- Allows you to select the destination server to forward the captured logging information

By default, the switch logs normal but significant system messages to a log file and sends these messages to the system console. You can specify which system messages should be saved based on the type of facility (see [Table 14-1](#)) and the severity level (see [Table 14-2](#)). Messages are time-stamped to enhance real-time debugging and management.

You can access logged system messages using the CLI or by saving them to a properly configured system message logging server. The switch software saves system messages in a file that can save up to 1200 entries. You can monitor system messages remotely by accessing the switch through Telnet, SSH, or the console port, or by viewing the logs on a system message logging server.



**Note**

When the switch first initializes, the network is not connected until initialization completes. Therefore, messages are not redirected to a system message logging server for a few seconds.

[Table 14-1](#) describes some samples of the facilities supported by the system message logs.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).**

**Table 14-1 Internal Logging Facilities**

Facility Keyword	Description
<b>all</b>	All facilities
<b>auth</b>	Authorization system
<b>fcdomain</b>	fcdomain
<b>fcns</b>	Name server
<b>fcs</b>	FCS
<b>fspf</b>	FSPF
<b>ipconf</b>	IP configuration
<b>module</b>	Switching module
<b>ntp</b>	NTP
<b>port</b>	Port
<b>sysmgr</b>	System manager
<b>user</b>	User process
<b>zone</b>	Zone server

Table 14-2 describes the severity levels supported by the system message logs.

**Table 14-2 Error Message Severity Levels**

Level Keyword	Level	Description	System Message Definition
<b>emergencies</b>	0	System unusable	LOG_EMERG
<b>alerts</b>	1	Immediate action needed	LOG_ALERT
<b>critical</b>	2	Critical conditions	LOG_CRIT
<b>errors</b>	3	Error conditions	LOG_ERR
<b>warnings</b>	4	Warning conditions	LOG_WARNING
<b>notifications</b>	5	Normal but significant condition	LOG_NOTICE
<b>informational</b>	6	Informational messages only	LOG_INFO
<b>debugging</b>	7	Debugging messages	LOG_DEBUG



**Note**

Refer to the *Cisco MDS 9020 Fabric Switch System Messages Reference* for details on the error log message format.

[Send documentation comments to mdsfeedback-doc@cisco.com.](mailto:mdsfeedback-doc@cisco.com)

## System Message Logging Configuration

System logging messages are sent to the console based on the default (or configured) logging facility and severity values.

### Facility Severity Level

To configure the severity level for a logging facility, perform this task:

	Command	Purpose
Step 1	switch# <b>config t</b> switch(config)#	Enters configuration mode.
Step 2	switch(config)# <b>logging level all 4</b>	Configures Telnet or SSH logging for the all facilities at level 4 (warning). As a result, logging messages with a severity level of 4 or above are displayed.

### Log Files

You can display the log file using the **show logging logfile** command.

### System Message Logging Servers

You can configure a maximum of three system message logging servers.

To send log messages to a UNIX system message logging server, you must configure the system message logging daemon on a UNIX server. Log in as root, and follow these steps:

**Step 1** Add a line like the following to the `/etc/syslog.conf` file:

```
local0.debug                /var/log/myfile.log
```



**Note** As shown in this example, you must add five tab characters between **local0.debug** and **/var/log/myfile.log**. Refer to entries in the `/etc/syslog.conf` file for further examples.

The switch sends messages based on the specified facility types and severity levels. The **local0** keyword specifies the UNIX logging facility; local0 is the only facility type that Cisco FabricWare supports. The messages from the switch are generated by user processes. The **debug** keyword specifies the severity level of the condition being logged. You can set UNIX systems to receive all messages from the switch.

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

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

**Step 3** Make sure the system message logging daemon reads the new changes by entering this command:

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

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).**

To configure system message logging servers, perform this task:

	Command	Purpose
Step 1	switch# <b>config t</b> switch#	Enters configuration mode.
Step 2	switch(config)# <b>logging server</b> <b>172.22.00.00</b>	Configures the switch to forward log messages according to the specified facility types and severity levels to remote multiple servers specified by its hostname or IP address (172.22.00.00).
	switch(config)# <b>no logging server</b> <b>172.16.00.00</b>	Removes the specified server (172.16.00.00) and reverts to factory default.

## Outgoing System Message Logging Server Facilities

All system messages have a logging facility and a level. The logging facility can be thought of as *where* and the level can be thought of as *what*.

The single system message logging daemon (syslogd) sends the information based on the configured **facility** option. If no facility is specified, local7 is the default outgoing facility.

The internal facilities are listed in [Table 14-1](#) and the outgoing logging facilities are listed in [Table 14-3](#).

**Table 14-3 External Logging Facilities**

Facility Keyword	Description	Standard or Cisco MDS Specific
<b>auth</b>	Authorization system	Standard
<b>authpriv</b>	Authorization (private) system	Standard
<b>cron</b>	Cron or at facility	Standard
<b>daemon</b>	System daemons	Standard
<b>ftp</b>	File Transfer Protocol	Standard
<b>kernel</b>	Kernel	Standard
<b>local0 to local7</b>	Locally defined messages	Standard (local7 is the default)
<b>lpr</b>	Line printer system	Standard
<b>mail</b>	Mail system	Standard
<b>news</b>	USENET news	Standard
<b>syslog</b>	Internal system messages	Standard
<b>user</b>	User process	Standard
<b>uucp</b>	UNIX-to-UNIX Copy Program	Standard



**Note**

The only facility type that Cisco FabricWare supports is **local0**.

[Send documentation comments to mdsfeedback-doc@cisco.com.](mailto:mdsfeedback-doc@cisco.com)

## Displaying System Message Logging Information

Use the **show logging** command to display the current system message logging configuration. (See Examples 14-1 to 14-7.)

### Example 14-1 Displays Current System Message Logging

```
switch# show logging
Logging monitor:          disabled
Logging server:          disabled
Logging logfile:         enabled (Severity: information)

Facility      Default Severity      Current Session Severity
-----
fcns          6                      6
fcs           6                      6
zone         6                      6
auth         6                      6
ipconf       6                      6
module       6                      6
ntp          6                      6
sysmgr       6                      6
user         6                      6
port         6                      6
fcdomain     6                      6
fspf         6                      6
[1][Fri Jan 21 17:50:12.072 UTC 2005][I][8400.0001][Switch][Modifying configured DomainID
1 to negotiated value 97]
[2][Fri Jan 21 17:50:18.629 UTC 2005][A][1005.0040][Port: 1][Unsupported SFP within port.]
[3][Fri Jan 21 17:50:18.662 UTC 2005][A][1005.0040][Port: 2][Unsupported SFP within port.]
[4][Fri Jan 21 18:47:27.879 UTC 2005][I][8400.0023][Switch][Successful login user
(admin@OB-session4) with admin privilege from address 10.0.0.254]
[5][Fri Jan 21 19:24:27.097 UTC 2005][I][8400.0023][Switch][Successful login user
(maint@OB-session5) with admin privilege from address 10.0.0.254]
...
```

### Example 14-2 Displays the Log File

```
switch# show logging logfile
Jul 16 21:06:50 %DAEMON-3-SYSTEM_MSG: Un-parsable frequency in /mnt/pss/ntp.drift
Jul 16 21:06:56 %DAEMON-3-SYSTEM_MSG: snmpd:snmp_open_debug_cfg: no snmp_saved_dbg_uri ;
Jul 16 21:06:58 172.22.91.204 %PORT-5-IF_UP: Interface mgmt0 is up
Jul 16 21:06:58 172.22.91.204 %MODULE-5-ACTIVE_SUP_OK: Supervisor 5 is active
...
```

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).**

### Example 14-3 Displays Logging Facility

```
switch# show logging level
```

Facility	Default Severity	Current Session Severity
-----	-----	-----
fcns	6	2
fcs	6	2
zone	6	2
auth	6	2
ipconf	6	2
module	6	2
ntp	6	2
sysmgr	6	2
user	6	2
port	6	2
fcdomain	6	2
fspf	6	2

### Example 14-4 Displays Logging Information

```
switch# show logging info
```

```
Logging monitor:      disabled
Logging server:      disabled
Logging logfile:     enabled (Severity: critical)
```

Facility	Default Severity	Current Session Severity
-----	-----	-----
fcns	6	2
fcs	6	2
zone	6	2
auth	6	2
ipconf	6	2
module	6	2
ntp	6	2
sysmgr	6	2
user	6	2
port	6	2
fcdomain	6	2
fspf	6	2

### Example 14-5 Displays Last Few Lines of a Log File

```
switch# show logging last 2
```

```
[7][Fri Jan 21 22:45:07.672 UTC 2005][I][8400.0023][Switch][Successful login user
(admin@OB-session3) with admin privilege from address 10.0.0.254]
[8][Fri Jan 21 22:49:06.768 UTC 2005][I][8400.0023][Switch][Successful login user
(maint@OB-session4) with admin privilege from address 10.0.0.254]
```

### Example 14-6 Displays Monitor Logging Status

```
switch# show logging monitor
```

```
Logging monitor:      enabled
```

### Example 14-7 Displays Server Information

```
switch# show logging server
```

```
Logging server:      disabled
```

[Send documentation comments to mdsfeedback-doc@cisco.com.](mailto:mdsfeedback-doc@cisco.com)

## Default Settings

Table 14-4 lists the default settings for system message logging.

**Table 14-4**      *Default System Message Log Setting*

Parameters	Default
System message logging to the console	Enabled for messages at the critical severity level.
System message logging to Telnet sessions	Disabled.
Logging file size	1200 entries.
Log file name	Message (change to a name with up to 200 characters).
Logging server	Disabled.
Syslog server IP address	Not configured.
Number of servers	Three servers.
Server facility	Local 7.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).***