



## Using the CSS Logging Features

---

This chapter describes how to enable logging, set up the log buffer, and determine where to send the activity information. Information in this chapter applies to all CSS models, except where noted.

This chapter contains the following sections:

- Logging Overview
- Specifying Logging Buffer Size
- Specifying Log File Destination
- Enabling Logging on a Subsystem
- Logging CLI Commands
- Showing Log Files
- Copying Log Files to an FTP or TFTP Server

For more detailed information on displaying and interpreting log messages for the CSS 11050, CSS 11150, and CSS 11800, refer to the *Cisco Content Services Switch Getting Started Guide*, Appendix A, Log Messages.

# Logging Overview

The CSS provides logging capabilities for debugging and system monitoring by generating the log files described in Table 8-1.

**Table 8-1 CSS Log File Descriptions**

Log File	Log File Destination		Records
	Default Location	Alternate Location	
Boot.log	Hard disk and console or flash disk and console	None	Results of the boot process.
Boot.bak	Hard disk and console or flash disk and console	None	Backup of a boot log file. Each time you reboot the CSS, the software renames the current boot log file to boot.log.prev and starts a new boot log file. The CSS overwrites an existing backup boot log file when a boot log file is renamed.
Sys.log	Hard disk or flash disk	Console syslogd VTY1 VTY2	Log information for user-defined subsystem or CLI commands. By default, logging is enabled and logs subsystem <b>all</b> with level <b>warning</b> . The CSS creates sys.log to record this log information.

**Table 8-1 CSS Log File Descriptions (continued)**

Log File	Log File Destination		Records
	Default Location	Alternate Location	
Sys.log.prev	Hard disk or flash disk	Console syslogd VTY1 VTY2	Backup of a system log file. When a system log file reaches its maximum size (50 MB, for a hard disk-based CSS; 10 MB, for a flash disk-based CSS), the software renames the system log file to sys.log.prev and starts a new system log file. The CSS overwrites an existing backup system log file when a system log file is renamed. When you reboot a CSS, the software continues to use the existing system log file until it reaches its maximum size.

By default, the CSS has boot logging and system logging enabled and writes the logged information to the log files on the hard disk or flash disk, depending on the type of storage in your CSS. The maximum size of a log file is 50 MB for hard disk-based systems and 10 MB for flash disk-based systems. Log file information is recorded as ASCII text.

You can display or copy a log file using the **show log** or **copy log** command, respectively. For details on the **show log** command, refer to “Showing Log Files” in this chapter. For details on the **copy log** command, refer to “Copying Log Files to an FTP or TFTP Server” in this chapter.

**Note**

You need SuperUser privileges to use the **show log** command.

## Logging Quick Start Table

If you are familiar with the CSS logging functions, refer to Table 8-2 for the commands and command options required to configure and enable logging. For detailed information on the CSS logging functions, refer to the sections following Table 8-2.



### Note

Configure all logging commands from **config** mode except for the **clear log** command. The **clear log** command is available in SuperUser mode at the root prompt (#).

**Table 8-2 Configuring and Enabling Logging**

Step	Logging Option	Example
1. Specify the disk buffer size.	<i>size</i> - Size of the disk buffer (0 to 64000)	<b>logging buffer 1000</b>
2. Specify the destination (disk, host, line) where you wish to log subsystem activity.	<b>disk filename</b> - New or existing filename in the log directory	<b>logging disk stubs</b>
	<b>host ip</b> or <i>host</i> - IP address of the syslog daemon on the host or a host name	<b>logging host 192.168.11.3</b>
	<b>log line</b> - CSS active session	<b>logging host myhost.domain.com</b> <b>logging line vty1</b>

**Table 8-2 Configuring and Enabling Logging (continued)**

Step	Logging Option	Example
<p>3. Select a CSS subsystem and determine which type of activity to log (default <b>all</b>) and level (default <b>warning</b>).</p>	<p><b>subsystem</b> - Valid subsystems:</p> <p><b>acl, all, app, boomerang, buffer, chassis, circuit, csdpeer, dql, fac, flowmgr, hfg, ipv4, keepalive, netman, nql, ospf, pcm, portmapper, proximity, publish, radius, redundancy, replicate, rip, security, sntp, syssoft, urql, vlanmgr, vpm, vrrp, wcc</b></p> <p><b>level</b> - Valid levels:</p> <p><b>fatal-0, alert-1, critical-2, error-3, warning-4, notice-5, info-6, debug-7</b></p>	<p><b>logging subsystem rip level alert-1</b></p>
<p>4. Optionally, enable the CSS to send log messages to an email address and specify a level.</p>	<p><b>sendmail</b> <i>email address</i> of mail recipient</p> <p><i>IP address</i> or <i>hostname</i> of SMTP host</p> <p><b>level</b> - Valid levels:</p> <p><b>fatal-0, alert-1, critical-2, error-3, warning-4, notice-5, info-6, debug-7</b></p>	<p><b>logging sendmail us@arrowpoint.com 172.3.6.58 critical</b></p>
<p>5. Show the log file.</p>	<p><i>filename</i> - Log file to display</p>	<p><b>show log stubs</b></p>

## Specifying Logging Buffer Size

The logging buffer size is the amount of information the CSS buffers in memory before outputting the information to disk. The larger you configure the buffer size, the less frequently the CSS outputs the contents to disk. Specifying a buffer size is only required if you configure logging to disk.

To set the disk buffering size, use the **logging buffer** command. Specify the buffer size from 0 to 64,000 bytes. The default is 0, where the CSS sends the logging output directly to the log file.

For example, to set the buffer size to 1000 bytes, enter:

```
(config)# logging buffer 1000
```

To send the logging output directly to the log file, enter:

```
(config)# no logging buffer
```

## Specifying Log File Destination

To specify a destination where the CSS logs subsystem activity, use the **logging** command. You can specify the following locations for log files:

- **disk filename** - New or existing filename in the disk log directory
- **host ip** or **host** - IP address of the syslog daemon on the host or a host name
- **log line** - CSS active session

For information on logging to these destinations, refer to the following sections.

## Specifying Disk for a Log File Destination

To send log information to disk, use the **logging disk** command and specify a log filename. The filename can be new or existing. Enter a text string from 0 to 32 characters.

For example:

```
(config)# logging disk stubs
```

When you issue this command, the CSS:

- Stops writing default log information to `sys.log`
- Creates the filename you specify in the disk log directory
- Sends subsystem and level information to the log filename

You can have only one active log file on the disk at a time. If you wish to send subsystem information to a different log file on the disk, reenter the logging disk command with a different filename.

## Disabling Logging to Disk

To disable logging to disk, enter:

```
(config)# no logging disk
```

When you disable logging to disk, the CSS stops logging to the specified file and reenables logging to the `sys.log` file.

## Specifying Host for a Log File Destination

To send log information to a syslog daemon on the host system, use the **logging host** command and specify:

- *An IP address or a host name* - The address of the syslog daemon on the host. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1) or the mnemonic host name (for example, myhost.mydomain.com).
- *facility number* - The syslog daemon facility level. Enter a number from 1 to 7. For more information on the syslog daemon and facility levels, refer to your syslog daemon documentation.

For example:

```
(config)# logging host 192.168.11.1 facility 3
```

To turn off logging to a host, enter:

```
(config)# no logging host
```

## Specifying a Line for a Log File Destination

To send log information to an active CSS session, use the **logging line** command and specify a valid log line on the CSS. Enter the line as a case-sensitive text string with a maximum length of 32 characters.

To display a list of active CSS lines, enter the **logging line** command as shown. The \* denotes your current session.

```
(config)# logging line ?  
  
console      Login Name:  Location:local  
*vty1        Login Name:  admin Location:10.0.3.35
```

For example, to send subsystem information to your monitor, enter:

```
(config)# logging line vty1
```

To turn off logging, enter the **no logging line** command.

```
(config)# no logging line vty1
```

## Enabling Logging on a Subsystem

Use the **logging subsystem** command to select a CSS subsystem and determine which type of activity to log. The level you specify instructs the CSS to log subsystem activity that occurs at that level and the activity greater than that level. For example, if you wish to log info messages, the CSS also logs error, critical, alert, and fatal error levels.

The following example enables logging for the **chassis** subsystem with a **critical-2** error level. The CSS will log all critical, alert, and fatal errors for the chassis.

```
(config)# logging subsystem chassis level critical-2
```

Table 8-3 defines the CSS subsystems for which you can enable logging.

**Table 8-3 Logging Subsystems**

<b>Subsystem</b>	<b>Definition</b>
<b>acl</b>	Access Control List (ACL)
<b>all (default)</b>	All CSS subsystems
<b>app</b>	Application Peering Protocol (APP)
<b>boomerang</b>	DNS Content Routing Agent (CRA)
<b>buffer</b>	Buffer manager
<b>chassis</b>	Chassis manager
<b>circuit</b>	Circuit manager
<b>csdpeer</b>	Content Server Database (CSD) peer
<b>dql</b>	Domain Qualifier List (DQL)
<b>fac</b>	Flow Admission Control (FAC)
<b>flowmgr</b>	Flow manager subsystem
<b>hfg</b>	Header Field Group (HFG)
<b>ipv4</b>	Internet Protocol version 4 (IPv4)
<b>keepalive</b>	Keepalive
<b>netman</b>	Network management
<b>nql</b>	Network Qualifier List (NQL)
<b>ospf</b>	Open Shortest Path First (OSPF)
<b>pcm</b>	Proximity CAPP Messaging (PCM)
<b>portmapper</b>	Port Mapper
<b>proximity</b>	Proximity
<b>publish</b>	Publish
<b>radius</b>	Remote Authentication Dial-In User Server (RADIUS)
<b>redundancy</b>	CSS redundancy
<b>replicate</b>	Content replication
<b>rip</b>	RIP

**Table 8-3 Logging Subsystems (continued)**

<b>Subsystem</b>	<b>Definition</b>
<b>security</b>	Security manager
<b>sntp</b>	Simple Network Time Protocol (SNTP)
<b>syssoft</b>	System software
<b>urql</b>	Uniform Resource Locator Qualifier List (URQL)
<b>vlanmgr</b>	VLAN manager
<b>vpm</b>	Virtual pipe manager
<b>vrrp</b>	Virtual Router Redundancy Protocol
<b>wcc</b>	Web conversation control

Table 8-4 defines the logging levels you can set for a CSS subsystem. The logging levels are listed in order of severity with a fatal error being the most severe and info being the least severe error.

**Table 8-4 Subsystem Logging Levels**

<b>Level</b>	<b>Definition</b>
<b>fatal-0</b>	Fatal errors only.
<b>alert-1</b>	Alert errors, including fatal errors.
<b>critical-2</b>	Critical errors, including alert and fatal errors. The following trap events log at the critical level: link down, cold start, warm start, service down, service suspended.
<b>error-3</b>	General errors, including critical, alert, and fatal errors.
<b>warning-4</b> (default)	Warning messages, including all lower levels (error, critical, alert, and fatal).
<b>notice-5</b>	Notice messages, including all trap events (except for events logged at critical) and all lower levels except for info and debug.
<b>info-6</b>	Informational messages, including all lower levels except for debug.
<b>debug-7</b>	Debug messages, including all other error levels.

## Disabling Logging for a Subsystem

To reset logging for a subsystem to the default logging level (warning-4), enter the **no** version of the logging command. For example:

```
(config)# no logging subsystem redundancy
```

## Configuring a Log Message for a Subsystem at a Logging Level

Use the **cliLogMessage subsystem** command to define a log message for a subsystem at a particular logging level. The syntax for this global configuration mode command is:

```
cliLogMessage subsystem name "message" level level
```

The variables are:

- *name* - The name of a CSS subsystem. Enter one of the following subsystem names:
  - **acl** - Access Control Lists
  - **all** - All subsystems
  - **app** - Application Peering Protocol (APP)
  - **boomerang** - DNS Content Routing Agent (CRA)
  - **buffer** - Buffer Manager
  - **chassis** - Chassis Manager
  - **circuit** - Circuit Manager
  - **csdpeer** - Content Server Database (CSD) Peer
  - **dql** - Domain Qualifier List (DQL)
  - **fac** - Flow Admission Control (FAC)
  - **flowmgr** - Flow Manager
  - **hfg** - Header Field Group (HFG)
  - **ipv4** - IPv4
  - **keepalive** - Keepalive
  - **netman** - Network Management
  - **nql** - Network Qualifier List (NQL)

- **ospf** - Open Shortest Path First (OSPF)
- **pcm** - Proximity CAPP Messaging (PCM)
- **portmapper** - PortMapper
- **proximity** - Proximity
- **publish** - Publish
- **radius** - Remote Authentication Dial-In User Server (RADIUS)
- **replicate** - Replication
- **redundancy** - CSS redundancy
- **rip** - RIP
- **security** - Security Manager
- **sntp** - Simple Network Time Protocol
- **syssoft** - System software
- **urql** - Uniform Resource Qualifier List
- **vlanmgr** - VLAN Manager
- **vpm** - Virtual Pipe Manager
- **vrp** - Virtual Router Redundancy Protocol
- **wcc** - Web Conversation Control

To see a list of subsystems, enter:

```
cliLogMessage subsystem ?
```

- **level** - The log level for the message. Enter one of these levels:
  - **fatal-0** - Fatal errors only
  - **alert-1** - Alert errors, including errors at the fatal-0 level
  - **critical-2** - Critical errors, including errors at the alert-1 level
  - **error-3** - Error errors, including errors at the critical-2 level
  - **warning-4** - Warning errors (default), including errors at the error-3 level
  - **notice-5** - Notice messages, including errors at the warning-4 level
  - **info-6** - Informational messages, including errors at the notice-5 level
  - **debug-7** - All errors and messages

## Logging ACL Activity

When you configure the CSS to log ACL activity, it logs the event of the packet matching the clause and ACL. The CSS sends log information to the location you specified in the **logging** command.

**Note**

---

Before you configure logging for a specific ACL clause, ensure that global ACL logging is enabled. To globally enable ACL logging, use the **logging subsystem acl level debug-7** command in config mode.

---

To configure logging for an ACL clause:

1. Enter the ACL mode for which you want to enable logging.

```
(config)# acl 7  
(config-acl[7])#
```

2. Enable logging for:

- A new clause by entering the **log** option at the end of the clause. For example:

```
(config-acl[7])# clause 1 deny udp any eq 3 destination any eq 3 log
```

- An existing clause by using the **clause log enable** command:

```
(config-acl[7])# clause 1 log enable
```

To disable ACL logging for a specific clause, enter:

```
(config-acl[7])# clause 1 log disable
```

To globally disable logging for all ACL clauses, enter:

```
(config)# no logging subsystem acl
```

## Sending Log Messages to an Email Address

To send the log activity of a subsystem to an email address, use the **logging sendmail** command. The syntax for this global configuration mode command is:

```
logging sendmail email_address ip_address level
```

The variables are:

- *email\_address* - The email address for the recipient. Enter the email address as a case-sensitive unquoted text string with a length of 1 to 30 characters.
- *IP\_address* - The IP address for the SMTP host. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
- *level* - The type of information to log. The valid levels are defined in Table 8-4.
- *domain* - The domain name for the SMTP host. Enter an unquoted text string with a maximum length of 64 characters (for example, arrowpoint.com). Do not insert an @ sign before the domain name. The CSS automatically prepends it to the domain name.

To turn off logging to an email address, enter:

```
(config)# no logging sendmail email_address
```

## Logging CLI Commands

When you want to keep track of all CLI commands issued from the CSS, use the **logging commands enable** command. This command logs each CLI command to the sys.log file. To log CLI commands to the sys.log file, enter:

```
(config)# logging commands enable
```

To disable logging CLI commands to the sys.log file, enter:

```
(config)# no logging commands
```

# Showing Log Files

Use the **show log** command to display the contents in a log or trap log file. You need SuperUser privileges to use the **show log** command.

The options for this command are:

- **show log** - Send the log activity to your current session, or display the contents in a log or a trap log file.
- **show log-list** - Display a list of all log files.
- **show log-state** - Display the state of logging for CSS facilities.

**Note**

---

When you use the **show log** command to send the log activity to your current session, and you want to stop sending log activity, press any key on the terminal or workstation. The **show log** command performs the same function as **(config) logging line**. Note that you cannot run these commands at the same time.

---

## Showing Log Activity

Use the **show log** command and its options to send the log activity to your current session, or to display the contents in a log or trap log file. You need SuperUser privileges to use the **show log** command. The syntax for the **show log** command is:

```
show log {log_filename {tail lines} {line-numbers}}
```

The options and variables for the **show log** command include:

- *log\_filename* - The name of the log file. Enter an unquoted text string with no spaces. To see a list of log files with their dates, enter:

```
show log ?
```

- **tail lines** - Display the bottom and most recent portion of the log file. You specify the number of lines to display, starting at the end of the log file. Enter a number from 1 to 1000.
- **line-numbers** - Include the line numbers when displaying the contents of the log file.

- **traplog** - Display all SNMP traps that have occurred. A trap log file is an ASCII file in the log directory containing generic and enterprise traps. By default, the following events generate level critical-2 messages:
  - Link Up
  - Link Down
  - Cold Start
  - Warm Start
  - Service Down
  - Service Suspended

All other SNMP traps generate level notice-5 messages.




---

**Note** Even though traps are disabled, the CSS still produces a log message for any event that would normally generate a trap.

---

To send the log activity to your current session, enter:

```
# show log
    Displaying Log events.
Press any key to abort...
APR 14 16:28:09 5/1 2398 NETMAN-7: HTTPC:HTTPC_Open:
ERROR->connect <-1,0> <192.20.1.7> <80>
APR 14 16:28:15 5/1 2399 NETMAN-7: HTTPC:HTTPC_Open:
ERROR->connect <-1,0> <192.20.1.7> <80>
APR 14 16:28:21 5/1 2400 NETMAN-7: HTTPC:HTTPC_Open:
ERROR->connect <-1,0> <192.20.1.7> <80>
APR 14 16:28:27 5/1 2401 NETMAN-7: HTTPC:HTTPC_Open:
ERROR->connect <-1,0> <192.20.1.7> <80>
```

To display information in a specific log file, enter the **show log** command with a valid log filename. For example:

```
# show log stubs
SEP 22 09:59:18 5/1 918 NETMAN-7: SNMP:SET RSP (3803)
SEP 22 09:59:53 5/1 919 NETMAN-7: SNMP:SET (3804)
SEP 22 09:59:53 5/1 920 NETMAN-7: SNMP: 1
apLogHostIpAddress.[1.2.3.4] VT_IPADDRESS <1.2.3.4>
SEP 22 09:59:53 5/1 921 NETMAN-7: SNMP: 2
apLogHostIpAddress.[1.2.3.4] VT_IPADDRESS <1.2.3.4>
```

## Showing Log Lists

Use the **show log-list** command to display a list of all log files. For example:

```
(config)# show log-list
```

## Showing Log State

Use the **show log-state** command to display the state of logging for CSS facilities. For example:

```
(config)# show log-state
```

Table 8-5 describes the fields in the **show log-state** output.

**Table 8-5** *Field Descriptions for the show log-state Command*

Field	Description
Subsystems	
acl	Access Control Lists subsystem
app	Application Peering Protocol (APP) subsystem
boomerang	Content Routing Agent (CRA)
buffer	Buffer Manager subsystem
chassis	Chassis Manager subsystem
circuit	Circuit Manager subsystem
csdpeer	Content Server Database (CSD) Peer subsystem
dql	Domain Qualifier List (DQL) subsystem
fac	Flow Admission Control (FAC) subsystem
flowmgr	Flow Manager subsystem
hfg	Header Field Group (HFG) subsystem
ipv4	IPv4 subsystem
keepalive	Keepalive subsystem
netman	Network Management subsystem
nql	Network Qualifier List (NQL) subsystem

**Table 8-5** Field Descriptions for the `show log-state` Command (continued)

Field	Description
ospf	OSPF subsystem
pcm	Proximity CAPP Messaging (PCM) subsystem
portmapper	PortMapper subsystem
proximity	Proximity subsystem
publish	Publish subsystem
radius	Remote Authentication Dial-In User Server (RADIUS)
replicate	Replication subsystem
redundancy	CSS redundancy subsystem
rip	RIP subsystem
security	Security Manager subsystem
sntp	Simple Network Time Protocol (SNTP)
syssoft	System software subsystem
urql	Uniform Resource Qualifier List subsystem
vlanmgr	VLAN Manager subsystem
vpm	Virtual Pipe Manager subsystem
vrrp	Virtual Router Redundancy Protocol subsystem
wcc	Web Conversation Control subsystem
Levels:	
debug	Log all errors and messages (Verbose)
info	Log informational messages, including errors at the notice level
notice	Log notice messages, including errors at the warning level
warning	Log warning errors (default), including errors at the error level
error	Log error errors, including errors at the critical level
critical	Log critical errors, including errors at the alert level

**Table 8-5** Field Descriptions for the *show log-state* Command (continued)

Field	Description
alert	Log alert errors, including errors at the fatal level
fatal	Log fatal errors only (Quiet)
Lines:	Lists the connected sessions (CSS 11800 only)
File:	
Filename:	The name of the log file
Current size:	The current size of the log file

## Copying Log Files to an FTP or TFTP Server

To copy log files from the CSS to a File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP) server, use the **copy log** command. The **copy log** command is available at the SuperUser prompt.

The options for this command are:

- **copy log** *log\_filename* **ftp**
- **copy log** *log\_filename* **tftp**

To see a list of log files, enter the **copy log ?** command.

## Copying Log Files to an FTP Server

To copy a log file to an FTP server, use the **copy log ftp** command. Before you copy a log file from the CSS to an FTP server, you must create an FTP record file containing the FTP server IP address, username, and password. For information on configuring an FTP record, refer to “Configuring an FTP Record” in Chapter 1, Logging in and Getting Started.

The syntax is:

```
copy log logfilename ftp ftp_record filename
```

For example:

```
# copy log starlog ftp ftpserv1 starlogthurs
```

The variables are:

- *logfilename* - The name of the log file on the CSS. Enter an unquoted text string with no spaces and a maximum length of 32 characters.
- *ftp\_record* - The name of the FTP record file that contains the FTP server IP address, username, and password. Enter an unquoted text string with no spaces.
- *filename* - The name you want to assign to the file on the FTP server. Include the full path to the file. Enter an unquoted text string with no spaces and a maximum length of 32 characters.

## Copying Log Files to a TFTP Server

To copy a log file to an TFTP server, use the **copy log tftp** command.

The syntax is:

**copy log** *logfilename* **tftp** *IP address or hostname filename*

The variables are:

- *logfilename* - The name of the log file on the CSS. Enter an unquoted text string with no spaces and a maximum length of 32 characters.
- *IP address* or *hostname* - The IP address or host name of the TFTP server to receive the file. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or in mnemonic host-name format (for example, myhost.mydomain.com). If you wish to use a hostname, you must first set up a host table using the **(config) host** command.
- *filename* - The name you want to assign to the file on the TFTP server. Include the full path to the file. Enter an unquoted text string with no spaces and a maximum length of 32 characters.