



## Viewing Log Files

---

This chapter describes how to store and view logged information about your GSS devices. Each GSS device contains a number of log files that retain records of specified GSS-related activities and the performance of various GSS subsystems. You can access these log files using the CLI to troubleshoot problems or to better understand the behavior of a GSS device.

This chapter contains the following major sections:

- [Understanding GSS Logging Levels](#)
- [Configuring System Logging for a GSS](#)
- [Viewing Device Logs from the CLI](#)
- [Viewing System Logs from the Primary GSSM GUI](#)
- [Viewing GSS System Logs Using CiscoWorks RME Syslog Analyzer](#)

## Understanding GSS Logging Levels

The GSS generates log messages to assist you with debugging and monitoring operations. The GSS maintains logged records for a wide range of GSS network activity in the `gss.log` file as well as through the system logs feature of the GSSM.

The subsystem log messages are subsystem events that occur during the operation of the GSS. The GSS saves these messages in the `system.log` file. The GSS determines which subsystem messages to log by its configured logging level. The logging level designates the GSS log emergency, alert, critical, error, and warning messages for the subsystem. The GSS also logs notification, informational, and debugging messages.

The GSS supports eight separate logging levels to identify the wide range of critical and noncritical logged events that may occur on a GSS device. [Table 8-1](#) describes the different logging levels. [Table 8-2](#) lists GSS subsystems for which you can enable logging.

**Table 8-1 GSS Logging Levels**

Level Number	Level Name	Description
0	Emergencies	The GSS has become unusable. For example, the GSS has shut down and cannot be restarted, or it has experienced a hardware failure.
1	Alerts	The GSS requires immediate attention. For example, one of the GSS subsystems is not running.
2	Critical	The GSS encountered a critical condition that requires attention. For example, a GSS device cannot connect to the primary GSSM and does not have a local configuration snapshot to use.
3	Errors	The GSS encountered an error condition that requires prompt attention but can still function. For example, a GSS device is out of available memory.
4	Warnings	The GSS encountered an error condition that requires attention but is not interfering with the operation of the device. For example, a GSS has lost contact with the primary GSSM but a local configuration snapshot exists.
5	Notifications	The GSS encountered a nonerror condition that should be brought to the administrator's attention. For example, a GSS software upgrade is required.

**Table 8-1 GSS Logging Levels (continued)**

Level Number	Level Name	Description
6	Information	Messages at this level are normal operational messages for the GSS device, such as status or configuration changes.
7	Debug	Messages at this level (such as detailed information about DNS request or keepalive handling and specific code path tracking) are intended for use by technical support personnel.

**Table 8-2 Logging Subsystems**

Subsystem	Definition
<b>boomerang</b>	Boomerang logging messages
<b>crdirector</b>	CrDirector logging messages
<b>crm</b>	GSSM logging messages
<b>ddos</b>	Distributed Denial of Service (DDoS) prevention module logging messages.
<b>dnsserver</b>	Domain Name System (DNS) logging messages
<b>drpagent</b>	Director Response Protocol (DRP) agent logging messages
<b>keepalive</b>	Keepalive Engine logging messages
<b>nodemgr</b>	Node manager logging messages
<b>proximity</b>	Proximity logging messages
<b>snmp</b>	SNMP logging messages
<b>sticky</b>	Sticky manager logging message
<b>system</b>	System logging messages
<b>tacacs</b>	TACACS+ logging messages

# Configuring System Logging for a GSS

By default, the GSS maintains system logged records in the `gss.log` file on the hard disk. You can change the location to log files to a remote host machine. You can make global decisions about what level of GSS logging to use, or instead make those decisions on a subsystem-by-subsystem basis. For example, you can configure the primary GSSM to log all error-level messages, but also configure the node manager (`nodemgr`) to log a larger set of all notice-level messages.

Set specific parameters for the GSS system log file by using the **logging** command. To disable logging functions, use the **no** form of this command.

The default logging settings are as follows:

- Logging to disk: Enabled
- Priority of message for disk: 5
- Priority of message for host: 4
- Log filename: `/home/gss.log`
- Log file recycle size: 10 MB
- Maximum number of log files: 25



## Note

In rare instances when a GSS runs out of user disk space, the device will stop logging messages to all log files. Logging does not automatically resume after you free up disk space on the GSS. This behavior may occur when you use FTP to transfer a significant number of files to the GSS, thus completely filling the available GSS disk space. Correct this problem by using **rotate-logs** CLI command to replace the log files and resume logging (see the [“Rotating Existing Log Files from the CLI”](#) section).

This section contains the following topics:

- [Specifying a Log File on the GSS Disk](#)
- [Specifying a Host for a Log File Destination](#)
- [Specifying a Syslog Facility](#)

## Specifying a Log File on the GSS Disk

You can send log information to the `gss.log` file on the GSS hard disk by using the **logging disk** command. By default, logging to disk is enabled.

The syntax of the command is as follows:

```
logging disk { enable | priority loglevel | subsystem name priority loglevel }
```

The keywords and arguments are as follows:

- **enable**—Enables logging to disk.
- **priority**—Sets the priority level of the messages to log to disk.
- *loglevel*—Threshold that system messages must meet to be logged. Messages with lower priorities than the specified log level cannot be logged. Use one of the following keywords to select the logging level, listed in order of priority:
  - **emergencies**—The GSS is unusable (Priority 0)
  - **alerts**—Immediate action needed (Priority 1)
  - **critical**—Immediate action needed (Priority 2)
  - **errors**—Error conditions (Priority 3)
  - **warnings**—Warning conditions (Priority 4)
  - **notifications**—Normal but significant conditions (Priority 5)
  - **informational**—Informational messages (Priority 6)
  - **debugging**—Debugging messages (Priority 7)
- **subsystem**—Sets the log for a named GSS subsystem. Each subsystem can have a different log level applied for its messages.
- *name*—Name of the GSS subsystem. Use one of the following keywords to select a subsystem:
  - **boomerang**—Boomerang logging messages
  - **crdirector**—CrDirector logging messages
  - **crm**—GSSM logging messages
  - **ddos**—Distributed Denial of Service (DDos) prevention module logging messages
  - **dnserver**—Domain Name System (DNS) logging messages

- **drpagent**—Director Response Protocol (DRP) agent logging messages
- **keepalive**—Keepalive Engine logging messages
- **nodemgr**—Node manager logging messages
- **proximity**—Proximity logging messages
- **snmp**—SNMP logging messages
- **sticky**—Sticky manager logging message
- **system**—System logging messages
- **tacacs**—TACACS+ logging messages

To enable logging to disk and to set the priority level for error conditions, enter:

```
gssm1.example.com(config) # logging disk enable
gssm1.example.com(config) # logging disk priority error
```

To enable logging to disk, set the log for CrDirector subsystem logging messages, and set the priority level to informational messages, enter:

```
gssm1.example.com(config) # logging disk enable
gssm1.example.com(config) # logging disk subsystem crdirector
gssm1.example.com(config) # logging disk priority information
```

To stop logging to GSS disk, enter:

```
gssm1.example.com(config) # no logging disk enable
```

## Specifying a Host for a Log File Destination

You can set logging to the IP address of a remote host by using the **logging host** command. By default, logging to host is disabled.

The syntax of this command is as follows:

```
logging host { enable | ip ip_address | priority loglevel | subsystem name
priority loglevel }
```

The keywords and arguments are as follows:

- **enable**—Enables logging to host.
- **ip**—Sets the remote host (or hosts) that are to receive the GSS log files.
- *ip\_address*—Address (or addresses) of the remote logging hosts.

- **priority**—Sets the priority level of the messages to log to the host.
- *loglevel*—Threshold that system messages must meet to be logged. Messages with lower priorities than the specified log level cannot be logged. Use one of the following keywords to select the logging level, listed in order of priority:
  - **emergencies**—The GSS is unusable (Priority 0)
  - **alerts**—Immediate action needed (Priority 1)
  - **critical**—Immediate action needed (Priority 2)
  - **errors**—Error conditions (Priority 3)
  - **warnings**—Warning conditions (Priority 4)
  - **notifications**—Normal but significant conditions (Priority 5)
  - **informational**—Informational messages (Priority 6)
  - **debugging**—Debugging messages (Priority 7)
- **subsystem**—Sets the log for a named GSS subsystem. Each subsystem can have a different log level applied for its messages.
- *name*—Name of the GSS subsystem. Use one of the following keywords to select a subsystem:
  - **boomerang**—Boomerang logging messages
  - **crdirector**—CrDirector logging messages
  - **crm**—GSSM logging messages
  - **dnserver**—Domain Name System (DNS) logging messages
  - **drpagent**—Director Response Protocol (DRP) agent logging messages
  - **keepalive**—Keepalive Engine logging messages
  - **nodemgr**—Node manager logging messages
  - **proximity**—Proximity logging messages
  - **snmp**—SNMP logging messages
  - **sticky**—Sticky manager logging message
  - **system**—System logging messages
  - **tacacs**—TACACS+ logging messages

To enable logging to a remote host and to set the priority level for notifications, enter:

```
gssml.example.com(config)# logging host enable
gssml.example.com(config)# logging host ip 172.16.2.3
gssml.example.com(config)# logging host priority notifications
```

To enable logging to a remote host, to set the log for the Keepalive Engine subsystem logging messages, and to set the priority level to error messages, enter:

```
gssml.example.com(config)# logging host enable
gssml.example.com(config)# logging host ip 172.16.2.3
gssml.example.com(config)# logging host subsystem kale
gssml.example.com(config)# logging host priority error
```

To stop logging to GSS disk, enter:

```
gssml.example.com(config)# no logging host
```

## Specifying a Syslog Facility

You can specify a syslog facility type to identify the behavior of the syslog daemon (syslogd) on the host by using the **logging facility** command in global configuration mode. The syslog daemon on the host uses the specified facility type to determine how to process messages.



### Note

---

For more information on the syslog daemon and facility levels, refer to your syslog daemon documentation.

---

The syntax of this command is as follows:

**logging facility** *type*

The *type* argument specifies the syslog facility type. The default facility type is local5. The GSS supports the following types:

- **auth**—Authorization system
- **daemon**—System daemon
- **kernal**—Kernel
- **local0**—Reserved for locally defined messages
- **local1**—Reserved for locally defined messages

- **local2**—Reserved for locally defined messages
- **local3**—Reserved for locally defined messages
- **local4**—Reserved for locally defined messages
- **local5**—Reserved for locally defined messages
- **local6**—Reserved for locally defined messages
- **local7**—Reserved for locally defined messages
- **mail**—Mail system
- **news**—USENET news
- **syslog**—System log
- **user**—User process
- **uucp**—UNIX-to-UNIX copy system

For example, to change the logging facility to local7, enter:

```
gssm1.example.com(config)# logging facility local7
```

To change the logging facility to back to the default of local5, enter:

```
gssm1.example.com(config)# no logging facility local7
```

## Viewing Device Logs from the CLI

Each GSS device contains a number of log files that retain records of both GSS-related activity as well as the performance of the various GSS subsystems. Access these log files from the CLI to troubleshoot problems or understand the behavior of a GSS device.

This section contains the following topics:

- [Viewing the gss.log File from the CLI](#)
- [Viewing System Message Logging](#)
- [Viewing Subsystem Log Files from the CLI](#)
- [Rotating Existing Log Files from the CLI](#)

## Viewing the gss.log File from the CLI

The gss.log file groups useful information for a GSS device, such as the keepalive, availability and load statistics. You can view this log file from the CLI by using the **show logs** command.



### Note

The **show logs** command shows all logged information in your terminal session. This output may be quite large and can exceed the buffer size set for the terminal. If you want to capture all logged information, use the **terminal-length** CLI command to adjust the size of your screen buffer (see the “[Configuring the Terminal Screen Line Length](#)” section in [Chapter 2, Managing the GSS from the CLI](#)). Otherwise, use the **tail** or **follow** options as described in this section to limit the output of the file.

The syntax of this command is as follows:

```
show logs {follow | tail}
```

The keywords are as follows:

- **follow**—Displays the log file as data that is appended to it.
- **tail**—Displays only the last ten lines of the log file.

To limit the output of the **show logs** command, specify one of the following:

- Use the **tail** option of the **show logs** command to view only the last ten lines of logged information.

```
gssm1.example.com# show logs tail
```

- Use the **follow** option of the **show logs** command to view data appended to the end of the log as it grows.

```
gssm1.example.com# show logs follow
```

To show all logged information, enter:

```
gssm1.example.com# show logs
gss.log
Jul 14 21:42:01 gss-css2 KAL-7-KALAP[1240] KAL-AP (seq# 29410)=> Host
192.10.2.1
Jul 14 21:42:02 gss-css2 KAL-7-KALAP[1240] KAL-AP (seq# 29412)=> Host
192.10.4.1
```

```
Jul 14 21:42:02 gss-css2 KAL-7-KALAP[1240] Retrying IP [192.10.4.1]
(Retry Count 3)
Jul 14 21:42:07 gss-css2 KAL-7-KALAP[1240] Timeout: Found outstanding
KAL [192.10.2.1]
Jul 14 21:42:07 gss-css2 KAL-7-KALAP[1240] KAL-AP (seq# 29411)=> Host
192.10.2.1
Jul 14 21:42:07 gss-css2 KAL-7-KALAP[1240] Retrying IP [192.10.2.1]
(Retry Count 1)
Jul 14 21:42:09 gss-css2 KAL-7-KALCRA[1240] rtt_task: waiting 1000
mseconds
Jul 14 21:42:12 gss-css2 KAL-7-KALAP[1240] KAL-AP (seq# 29412)=> Host
192.10.2.1
Jul 14 21:42:12 gss-css2 KAL-7-KALAP[1240] Retrying IP [192.10.2.1]
(Retry Count 2)
Jul 14 21:42:16 gss-css2 KAL-7-KALAP[1240] Sending circuit keepalive
=> [192.10.2.1]
...
```

## Viewing System Message Logging

You can display the system message log configuration for a GSS device by using the **show logging** command.

The syntax of this command is as follows:

```
show logging
```

For example, enter:

```
gssml.example.com# show logging
Logging to disk is enabled.
Priority for disk logging is Informational(6).

Logging to host is disabled.
Priority for host logging is Warning(4).
```

## Viewing Subsystem Log Files from the CLI

In addition to the gss.log file, each GSS device maintains a number of other log files that record GSS subsystem-specific information (for example, the keepalive engine or DNS server component of the GSS). You can view these log files from the CLI using the **type** command.

**Note**

The **type** command lists all logged subsystem information in your terminal session. This output may be quite large and may exceed the buffer size set for the terminal. If you want to capture all logged information, use the **terminal-length** CLI command to adjust the size of your screen buffer (see the “[Configuring the Terminal Screen Line Length](#)” section in [Chapter 2, Managing the GSS from the CLI](#)). Otherwise, use the **show logs tail** or **follow** options as described in this section to limit the output of the file.

To view your GSS subsystem log files, perform the following steps:

1. Navigate to the directory containing the log file or files that you want to view.

```
gssm1.example.com> cd ../sysout
```

2. Display the contents of the log file by entering the following command:

```
gssm1.example.com> type dnsserver.log
dnsserver.log
Starting dnsserver: Mon Jul  1 13:52:50 UTC 2003 [(1221)]
2003-07-10 16:23:08 relog: Booting...
Starting dnsserver: Wed Jul 10 16:23:33 UTC 2003 [(1201)]
End of file dnsserver.log
]
```

3. View only the last ten lines of the log file by using the following command:

```
gssm1.example.com# tail dnsserver.log
```

## Rotating Existing Log Files from the CLI

You can instruct the GSS to save archive copies of all existing log files in the \$STATE directory and subdirectories and replace them with fresh log files. You can force the GSS to restart its log files and save archive copies of all existing log files by using the **rotate-logs** command.

**Note**

In rare instances when a GSS runs out of user disk space, the device will stop logging messages to all log files. Logging does not automatically resume after you free up disk space on the GSS. This behavior may occur when you use FTP to

transfer a large number of files to the GSS, thus completely filling the available GSS disk space. Correct this problem by using the **rotate-logs** CLI command to replace the log files and resume logging.

---

The syntax of this command is as follows:

```
rotate-logs [delete-rotated-logs]
```

If you want to delete all rotated log files from the / directory and its subdirectories on the GSS disk, use the optional **delete-rotated-logs** keyword. The GSS does not delete active log files.

The GSS archives existing log files locally using the following naming convention:

```
logfile_name.log.number
```

where:

- *logfile\_name.log*—Name of the archived log file (for example, gss.log or kale.log).
- *number*—Incremented number that represents the number of times that the logs have been rotated (for example, .3). The number of the most recent rotated log file is .1. The maximum number of log files is 25 for the gss.log file; five for all other log files.

To rotate existing log files, enter:

```
gssm1.example.com# rotate-logs
```

To clear all rotated log files in the \$STATE directory and subdirectories, except for the active log files, enter:

```
gssm1.example.com# rotate-logs delete-rotated-logs
```

## Viewing System Logs from the Primary GSSM GUI

From the primary GSSM GUI, you can view messages logged in the GSS system.log file. The system.log file presents the logged information of interest to GSS administrators, such as the severity of the message, a brief description of the problem, and any relevant conditions encountered while the message was logged.

The system.log file, however, presents only a subset of all logged information. For information about viewing the entire contents of the individual GSS log file, see the “[Viewing System Message Logging](#)” section.

This section contains the following topics:

- [Viewing System Logs from the Primary GSSM GUI](#)
- [Purging System Log Messages from the GUI](#)
- [Common System Log Messages](#)

## Viewing System Logs from the Primary GSSM GUI

To view the GSS system logs, perform the following steps:

1. From the primary GSSM GUI, click the **Tools** tab.
2. Click the **System Logs** option. The System Log list page appears (see [Figure 8-1](#)) displaying system log information.

Figure 8-1 System Log List Page

The screenshot shows the Cisco Global Site Selector GUI. The main content area is titled "System Log" and displays a table of log entries. The table has the following columns: Time, Node Type, Node Name, Module, Severity, Description, and Message. The log entries are as follows:

Time	Node Type	Node Name	Module	Severity	Description	Message
Sun, Sep 7, 2003 14:34:16 UTC	GSS	geryon.cisco.com	Server	info	Server started	Node services: GSS
Sun, Sep 7, 2003 14:34:12 UTC	GSS	geryon.cisco.com	DataFeed	warning	Error occurred while processing received data	Clear cached node state
Sat, Sep 6, 2003 14:52:18 UTC	GSS	geryon.cisco.com	Server	info	Server started	Node services: GSS
Fri, Sep 5, 2003 19:52:09 UTC	GSSM	megara.cisco.com	Server	info	GSS status transition detected	GSS: ierna.cisco.com. Current status: Online. Previous status: Pending.
Fri, Sep 5, 2003 19:52:09 UTC	GSSM	megara.cisco.com	Server	info	GSS status transition detected	GSS: minos.cisco.com. Current status: Online. Previous status: Pending.
Fri, Sep 5, 2003 19:52:09 UTC	GSSM	megara.cisco.com	Server	info	GSS status transition detected	GSS: charon.cisco.com. Current status: Online. Previous status: Pending.
Fri, Sep 5, 2003 19:52:09 UTC	GSSM	megara.cisco.com	Server	info	GSS status transition detected	GSS: geryon.cisco.com. Current status: Online. Previous status: Pending.
Fri, Sep 5, 2003 19:52:09 UTC	GSSM	megara.cisco.com	Server	info	GSS status transition detected	GSS: icarus.cisco.com. Current status: Online. Previous status: Pending.
Fri, Sep 5, 2003 19:52:09 UTC	GSSM	megara.cisco.com	Server	info	GSS status transition detected	GSS: iadon.cisco.com. Current status: Online. Previous status: Pending.
Fri, Sep 5, 2003 19:52:09 UTC	GSSM	megara.cisco.com	Server	info	Server started	Node services: GSS; Primary GSSM

The page also shows a "Time on GSS: Friday, September 5, 2003 21:50 UTC" at the bottom right of the log area.

System log information includes:

- Time—Time in Universal Coordinated Time (UTC) at which the logged event occurred on the GSS device.
- Node type—Type of GSS node (GSS or GSSM) on which the logged event occurred.
- Node name—Name assigned to the GSS device using the primary GSSM.
- Module—GSS component that logs the message (for example, server or storeAdmin).
- Severity—Severity of the logged message. The GSS rates system log messages using one of the following four severity levels:
  - Fatal—A failure in the GSS or one of its components. Fatal errors are rare and are usually caused by exceptions from which it is impossible to recover, or by the failure of a GSS component to initialize properly.
  - Warning—A noncritical error or unexpected condition.

- Info—Information about the normal operation of the GSS and its components.
  - Debug—Detailed information about the internal operations of the GSS or one of its components. Debug log messages are intended for use by Cisco support engineers to troubleshoot a problem.
  - Description—Text description that explains the event.
  - Message—Information about any relevant conditions encountered while the event was being logged.
3. Click the column header of any of the displayed columns (except for Severity or Description) to sort the listed domains by a particular property.

## Purging System Log Messages from the GUI

You may want to remove older system log messages from the primary GSSM GUI. An excessive number of system log messages can make viewing difficult on the System Log list page of the Tools navigation tab. To purge system log messages from the primary GSSM database, use the **gssm database purge-log-records** privileged EXEC command from the primary GSSM CLI.

You can instruct the primary GSSM to purge a quantity of system log messages from the GSSM database except for the following:

- Specified number of recently generated messages
- Most recently generated messages (generated over a specified number of days before today)

The syntax for the **gssm database purge-log-records** command is as follows:

```
gssm database purge-log-records { count number_records_to_keep | days number_days_to_keep }
```

The options and variables are as follows:

- **count** —Purges all system log messages from the primary GSSM database, except the specified number of most recently generated log messages.
- *number\_records\_to\_keep*—Number of system log messages to keep, starting back from the most recently generated log message, when purging the primary GSSM database.
- **days**—Purges the system log messages from the primary GSSM database that were generated prior to a specified number of days before today.

- *number\_days\_to\_keep*—Number of days back, starting from today, to retain log messages when purging the primary GSSM database.

For example, to purge all system log messages except for the last three messages, enter:

```
gssm1.example.com# gssm database purge-log-records count 3
```

For example, to purge all system log messages except for those generated within the last seven days, enter:

```
gssm1.example.com# gssm database purge-log-records days 7
```

To verify that the GSS purged the specified system log messages, perform the following steps:

1. Click the **Tools** tab.
2. Click the **System Logs** navigation link. The System Log list page appears.

**Note**

---

System log messages are purged based on the criteria specified in the **gssm database purge-log-records** CLI command.

---

## Common System Log Messages

[Table 8-3](#) lists common GSS system messages that can appear on the System Log list page. Messages appear alphabetically with a brief description. If you require more detailed information about a specific system message, contact a Cisco technical support representative.

**Table 8-3 System Log Messages**

<b>System Log Message</b>	<b>Description</b>
CRM-5-CLUSTSTATUS Config update sent to <hostname_of_non_primary> [<IP_address>]. Config Change Marker = <change_marker_number>	Message logged by the primary GSSM that indicates that it transmitted its configuration to the specified non-primary GSS.
CRD-5-CLUSTSTATUS Received config update from PGSSM <X.X.X.X> Config Change Marker = <change_marker_number>	Message logged by a non-primary GSS that indicates that it received a configuration from the specified primary GSSM.
DNS-5-XXXX [pid] Manual activation enabled/disabled on the GSS mesh	The manual reactivation function has been enabled or disabled on the GSS mesh.
KAL-5-YYYY [pid] Manual activation enabled/disabled on the GSS mesh	The manual reactivation function has been enabled or disabled on the GSS mesh.
DNS-5-XXXX [pid] Clause <n> of DNS rule xxxx is operationally Suspended due to Manual Reactivation	The GSS operationally suspended the clause, which has the manual reactivation function enabled.
KAL-5-YYYY [pid] Answer yyyy is operationally suspended due to Manual Reactivation	The GSS operationally suspended the answer, which has the manual reactivation function enabled.
Deleted a Global Site Selector	The named GSS has been deleted from the primary GSSM.
Error occurred while processing received data	An error occurred in the GSS while processing configuration updates from the primary GSSM. The affected device will attempt to recover automatically.
Failed store invalidation	The GSS has failed the process of marking internally inconsistent database records. Errors can be viewed in the validation log.

**Table 8-3 System Log Messages (continued)**

<b>System Log Message</b>	<b>Description</b>
Failed store validation	The GSSM database failed its internal consistency checks.
Multiple primary GSSMs detected	The GSS detects multiple primary GSSMs operating concurrently.
Passed store invalidation	The GSS has successfully completed the process of marking internally inconsistent database records.
Passed store validation	The GSSM database passed its internal consistency checks.
Registered a new Global Site Selector	A new GSS is online and has identified itself to the primary GSSM.
Registered a new standby GSSM	A new standby GSSM came online and has identified itself to the primary GSSM.
Server is Shutting Down	The GSS software has been stopped from the CLI.
Server Started	The GSS software has been started from the CLI.
Standby GSSM database error	An error occurred on the standby GSSM embedded database.
Started store invalidation	The GSS has started the process of marking internally inconsistent database records.
Started store validation	An internal consistency check has started for the GSSM database.
Store is corrupted	The GSSM database failed the internal consistency checks.
x System Messages Dropped	The GSS dropped and did not report a certain number of messages in an effort to throttle message traffic to the primary GSSM.

**Table 8-3 System Log Messages (continued)**

System Log Message	Description
Unexpected GSSM activation timestamp warning	The primary GSSM received a report from a GSS device with a GSSM activation time stamp that was not consistent with the current time of the primary GSSM.  The clocks of the standby and primary GSSM are not synchronized.
User HTTP Password Change	A user has changed his or her password in the primary GSSM GUI using the Change Password details page from the Tools tab.

## Viewing GSS System Logs Using CiscoWorks RME Syslog Analyzer

You can also use CiscoWorks RME Syslog Analyzer to view GSS syslog messages. The Syslog Analyzer allows you to extract detailed device information by setting up filters that report specific errors, severity conditions, or events, such as a link-down or device reboot.



### Note

The GSS syslog host messages support the correct CiscoWorks RME Syslog Analyzer message format; however, these messages do not support the Syslog Analyzer MIBs. In addition, not all severity 7 debug messages are compliant with the syslog host message format.

The following is an example of the host syslog message format generated by a GSS. The fields are described in [Table 8-4](#).

```
<IP or DNS name of Device> <BLANK> <:> <Time Stamp> <BLANK><:>
%FACILITY-SEVERITY-MNEMONIC <:> Message-text
```

**Table 8-4 Syslog Message Format**

Field	Description
IP or DNS name of Device	IP address or DNS name, followed by one BLANK space, and followed by a colon (:)
Time Stamp	Nonoptional timestamp in the format: yyyy mmm dd hh:mm:ss (for example, 2005 MAY 14 19:20:10) or mmm dd hh:mm:ss (for example, MAY 14 19:20:10)
%FACILITY	Code consisting of two or more uppercase letters that indicate the facility to which the message refers. A facility can be a hardware device, a protocol, or a module of the system software (for example, KAL, TOMCAT, SYS, STK).  <b>Note</b> This is not the syslog server logging facility.
SEVERITY	Single-digit code from 0 to 7 that reflects the severity of the condition. The severity maps to the GSS logging level specified using the <b>logging host priority</b> command.
MNEMONIC	Code that uniquely identifies the error message (for example, TCPTRANS, GUIEXCEPTION, KALPING).
Message-text	Text string describing the condition (for example, KAL_RSP_OK [192.168.100.1] numSuccessfulProbes:2 OR Detected Ssh is stopped but should be started)

