



Alarm Message Reference

This section provides reference information about alarm messages displayed in the Cisco MGC Node Manager Event Browser. Specifically:

- For the Cisco MGC and BAMS, this section provides:
 - References from which you can navigate to the relevant document to find the message you are interested in the (“Cisco MGC Host Alarm Messages” section on page A-2 and the “BAMS Alarm Messages” section on page A-3). A short description of each document is included.
 - Instructions for looking up the desired message in the referenced document (see the “Looking Up Cisco MGC and BAMS Alarm Messages” section on page A-2).
 - A list and short description of application-related alarm messages (see the “Cisco MGC Host and BAMS Resource Alarms” section on page A-4).
- For the Cisco SLT and Cisco LAN Switches, this section lists messages and provides short descriptions (see the “Cisco SLT Alarm Messages” section on page A-5).



Note

You can see SSH-related alarms, such as a mismatched security policy or an incorrect password, for the BAMS, Cisco PGW, and HSI server, in the Event Browser. These are Warning alarms. For a description of Cisco PGW 2200, BAMS, and HSI alarms caused by login failures related to SSH problems, refer to Cisco PGW 2200 Security Enhancements, Alarms and Messages at http://www.cisco.com/en/US/products/sw/voicesw/ps1913/products_installation_and_configuration_guide_chapter09186a00801bde43.html#wp1095818.

Overview of Cisco MGC Node Manager Alarm Management

Cisco MGC Node Manager converts traps received from managed devices to alarms which are displayed in the Event Browser. For the Cisco SLT and the Cisco LAN switches, each trap has a corresponding Cisco MGC Node Manager alarm. For example, the linkDown trap from the Cisco SLT corresponds to the “Link down” event description in the Cisco MGC Node Manager Event Browser. For the BAMS and the Cisco MGC, the trap serves as an envelope that can carry any one of numerous alarm messages.



Note

Cisco MGC Node Manager does not handle every possible trap that can be generated from each of the network elements, only those traps that are used for management of the devices as they are deployed to support the Cisco MGC node configuration.

In addition to device-specific traps, CMNM generates internal alarms. [Appendix C, “Troubleshooting Cisco MGC Node Manager”](#) provides an explanation of these internal messages.

Looking Up Cisco MGC and BAMS Alarm Messages

Use this procedure to locate information for a specific alarm message.

-
- Step 1** In the Event Browser, check the Object Name to determine the network object that generated the event. Note the event description.
 - Step 2** In this document, go to the section that applies to that object.
 - Step 3** Click on the name of the document or section (displayed in blue to indicate a link) that contains the information you want. The linked document opens.
 - Step 4** Press **Ctrl-F** for your browser’s Find dialog box.
 - Step 5** In the dialog box, enter some of the initial text of the event description, and click **OK**.



Note If your search text is not found, it means that the Event Browser description does not exactly match the generated message. You can search on a different part of the description string, or scroll through the document to find the message.

Cisco MGC Host Alarm Messages

Cisco MGC Node Manager handles the traps in [Table A-1](#) from the Cisco MGC hosts. Each trap is used as an envelope for alarms of that type.

Table A-1 Cisco MGC Host Traps

Trap	MIB
qualityOfService	CISCO-TRANSPATH-MIB
processingError	CISCO-TRANSPATH-MIB
equipmentError	CISCO-TRANSPATH-MIB
environmentError	CISCO-TRANSPATH-MIB
commAlarm	CISCO-TRANSPATH-MIB

The *Cisco MGC Messages Reference Guide* documents system messages. Consult the version for your release of the Cisco MGC:

- Cisco MGC Release 7
http://www.cisco.com/en/US/products/sw/voicesw/ps1913/products_technical_reference_book09186a0080091705.html
- *Cisco MGC Release 9 Messages Reference Guide* at
http://www.cisco.com/en/US/products/sw/voicesw/ps1913/products_technical_reference_book09186a008007dcb8.html

The alarm documentation includes the following information on each event:

- Alarm category—Alarm/event message, corresponding to the event description in the Cisco MGC Node Manager Event Browser.
- Description—Brief description of the alarm/event.
- Severity level—The severity of the alarm/event.
- Event reporting—Whether the event is reported to the management interface and can be obtained using SNMP. (The Event Browser lists only those events that are reported.)
- Alarm/event cause—The condition causing the alarm/event.
- SNMP trap type—Which SNMP trap type pertains to the event, displayed with a numeric code for the trap type:
 - 0 = No error
 - 1 = Communication alarm
 - 2 = Quality of service
 - 3 = Processing error alarm
 - 4 = Equipment error alarm
 - 5 = Environment error alarm
- Suggested Action—Recommendations for resolving the problem.

BAMS Alarm Messages

All BAMS alarms are carried on a single trap, the AlarmTrap, as shown in [Table A-1](#).

Table A-2 BAMS Traps

Trap	MIB
nusageAlarmTrap	ACECOMM-NUSAGE-MIB

The BAMS captures alarms and minor, major, or critical events and forwards them to network management systems such as Cisco MGC Node Manager. The severity level for message forwarding defaults to minor and above but may be changed by the BAMS system administrator.

The *Billing and Measurements Server (Version 3.x) User Guide*

http://www.cisco.com/en/US/products/sw/voicesw/ps522/products_user_guide_list.html includes an appendix (Appendix A. Troubleshooting) that provides a discussion of these messages and their use in troubleshooting. Messages are related to the tasks the BAMS performs, and the appendix also includes an explanation of BAMS tasks. The message documentation is organized by task.

The following categories of information are provided for each system message:

- Message ID—A six-character label that uniquely identifies each message. The first three characters are the application task ID, which identifies the application task that generated the message. (For example, MGR denotes the Manager task and MSC denotes the Mass Storage Control task.) The second three characters are the message number; (for example, 013 or 122).
- Text—The verbal part of the message that appears in the system log file, generally corresponding to the event description in the Cisco MGC Node Manager Event Browser.
- Arguments—Variable parts of the message, enclosed in angle brackets.

- Description—An explanation of the event that generated the message.

Action—What you should do as a result of the event described in the message. In some cases (for example, informational messages), no action may be required. Actions for error messages (manual, warning, minor, major, and critical) may include steps that should be followed to identify and correct problems. Error actions might also describe how BAMS responds to the specified error condition.

**Note**

The BAMS File Rename Failure alarm(POL115) must be manually cleared not only in Cisco MNM but also on the BAMS server before new alarms of that type will be generated.

>

HSI Server Alarm Messages

The Cisco HSI adjunct generates autonomous messages, or events, to notify you of problems or atypical network conditions. Depending on the severity level, events are considered alarms or informational events. HSI adjunct captures minor, major, and critical events and forwards them to the Cisco MNM.

The *Cisco H.323 Signaling Interface User Guide*, [http:](http://)

provides a discussion of these messages and their use in troubleshooting. The following information is provided for each alarm message:

- Description
- Severity Level and Trap Type
- Cause
- Troubleshooting Procedure

Cisco MGC Host and BAMS Resource Alarms

Cisco MGC Node Manager traps application-related events that occur on the Cisco MGC host or the BAMS, shown in [Table A-3](#).

**Note**

You can also monitor the performance of Cisco MGC host and BAMS system components—fixed disk storage used, processor load, and RAM and virtual memory used. See [Appendix B, “Performance Measurements Reference,” “Performance Data Collected for System Components” section on page B-8](#).

Table A-3 Resource Alarms

Alarm/Trap	MIB	Explanation
critAppDown	CRITAPP-MIB	A critical application is down.
critAppUp	CRITAPP-MIB	The application is up after being down. This clears the above alarm.
siFsAboveWarningThreshold	SIFSMONITOR-MIB	A monitored file system usage percentage is above the warning threshold.

Table A-3 Resource Alarms (continued)

Alarm/Trap	MIB	Explanation
siFsBelowWarningThreshold	SIFSMONITOR-MIB	The monitored file system usage is below the warning threshold. This clears the above alarm.
siFsAboveCriticalThreshold	SIFSMONITOR-MIB	A monitored file system usage percentage is above the critical threshold.
siFsBelowCriticalThreshold	SIFSMONITOR-MIB	The monitored file system usage is below the critical threshold. This clears the above alarm.

**Note**

Resource monitoring is done by the CIAgent application, resident in Cisco MGC Node Manager.

Cisco SLT Alarm Messages

Table A-4 Cisco SLT Alarms

Alarm/Trap	MIB	Explanation
coldStart	SNMPv2-MIB	The device was started from a power-off state. Note Clear this event manually.
warmStart	SNMPv2-MIB	The device was restarted from an on state. Note Clear this event manually.
linkUp	IF-MIB	An interface is up after being down.
linkDown	IF-MIB	An interface is down. This is cleared by one or more Link Up traps for the same interface.
authenticationFailure	SNMPv2-MIB	The device received an SNMP message that was improperly authenticated.
syslogAlarm	CISCO-SYSLOG-MIB	—
configChange	CISCO-CONFIG-MAN-MIB-VISMI	There has been a configuration change. (Informational)

Cisco LAN Switch Alarm Messages

Catalyst 5500 and 6509 Alarms

Table A-5 Catalyst 5500 Alarms

Alarm/Trap	MIB	Explanation
coldStart	SNMPv2-MIB	The device was started from a power-off state. Note Clear this event manually.
warmStart	SNMPv2-MIB	The device was restarted from an on state. Note Clear this event manually.
linkUp	IF-MIB	An interface is up after being down.
linkDown	IF-MIB	An interface is down. This is cleared by one or more Link Up traps for the same interface.
authenticationFailure	SNMPv2-MIB	The device received an SNMP message that was improperly authenticated.
configChange	CISCO-CONFIG-MAN-MIB-VISMI	There has been a configuration change. (Informational)
switchModuleUp	CISCO-STACK-MIB	A module is up after being down.
switchModuleDown	CISCO-STACK-MIB	A module is down.

Catalyst 2900XL Alarms

Table A-6 Catalyst 2900XL Alarms

Alarm/Trap	MIB	Explanation
coldStart	SNMPv2-MIB	The device was started from a power-off state. Note Clear this event manually.
warmStart	SNMPv2-MIB	The device was restarted from an on state. Note Clear this event manually.
linkUp	IF-MIB	An interface is up after being down.
linkDown	IF-MIB	An interface is down. This is cleared by one or more Link Up traps for the same interface.
authenticationFailure	SNMPv2-MIB	The device received an SNMP message that was improperly authenticated.

Table A-6 Catalyst 2900XL Alarms (continued)

syslogAlarm	CISCO-SYSLOG-MIB	—
configChange	CISCO-STACK-MIB	There has been a configuration change. (Informational)

