Viewing Faults and Logs

This chapter includes the following sections:

Faults

Viewing the Fault Summary

Procedure

Step 1 In the **Navigation** pane, click the **Server** menu.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Faults and Logs** pane, click the **Fault Summary** tab.

Step 4 In the **Discrete Sensors** area, review the following information:

Name	Description
Sensor Name column	The name of the sensor.
Status column	The status of the sensor. This can be one of the following: • **Critical** • **Non-Recoverable** • **Warning**

Name	Description
Reading column	This can be one of the following: • **absent** • **present**

Step 5 In the **Threshold Sensors** area, review the following information:

Name	Description
Sensor Name column	The name of the sensor.
Status column	The status of the sensor. This can be one of the following: • **Critical** • **Non-Recoverable** • **Warning**
Reading column	The value reported by the sensor.
Units column	The units in which the sensor data is reported.
Warning Threshold Min column	The minimum warning threshold.
Warning Threshold Max column	The maximum warning threshold.
Critical Threshold Min column	The minimum critical threshold.
Critical Threshold Max column	The maximum critical threshold.

Viewing the Fault History

Procedure

Step 1 In the **Navigation** pane, click the **Server** menu.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Faults and Logs** pane, click the **Fault History** tab.

Step 4 Review the following information for each fault event in the log.

Name	Description
Timestamp column	The date and time the fault occurred.
Severity column	The fault severity. This can be one of the following: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Informational** • **Debug**
Source column	The software module that logged the fault.
Probable Cause	The unique identifier associated with the event that caused the fault.
Description column	Information about the fault. It also includes a proposed solution.

Step 5 From the **Entries Per Page** drop-down list, select the number of fault events to display on each page.

Step 6 Click **<Newer** and **Older>** to move backward and forward through the pages of fault events, or click **<<Newest** to move to the top of the list.
By default, the newest fault events are displayed at the top if the list.

System Event Log

Viewing the System Event Log

Procedure

Step 1 In the **Navigation** pane, click the **Server** menu.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Faults and Logs** pane, click the **System Event Log** tab.

Step 4 Above the log table, view the percentage bar, which indicates how full the log buffer is.

Step 5 Review the following information for each system event in the log:

Name	Description
Time column	The date and time the event occurred.
Severity column	The severity field includes both text and color-coded icons. For the icons, green indicates normal operation, yellow is informational, and warning, critical, and non-recoverable errors are shown in shades of red.
Description column	A description of the event.
Clear Log button	Clears all events from the log file. **Note** This option is available only if your user ID is assigned the **admin** or **user** role.

Step 6 From the **Entries Per Page** drop-down list, select the number of system events to display on each page.

Step 7 Click **<Newer** and **Older>** to move backward and forward through the pages of system events, or click **<<Newest** to move to the top of the list.
By default, the newest system events are displayed at the top if the list.

Clearing the System Event Log

Before You Begin

You must log in as a user with user privileges to clear the system event log.

Procedure

Step 1 In the **Navigation** pane, click the **Server** menu.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Faults and Logs** pane, click the **System Event Log** tab.

Step 4 In the **System Event Log** pane, click **Clear Log**.

Step 5 In the dialog box that appears, click **OK**.

Cisco IMC Log

Viewing the CIMC Log

Procedure

Step 1 In the **Navigation** pane, click the **Server** menu.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Faults and Logs** pane, click the **Cisco IMC Log** tab.

Step 4 Review the following information for each CIMC event in the log.

Name	Description
Timestamp column	The date and time the event occurred.
Severity column	The event severity. This can be one of the following: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Informational** • **Debug**
Source column	The software module that logged the event.
Description column	A description of the event.
Clear Log button	Clears all events from the log file. **Note** This option is available only if your user ID is assigned the **admin** or **user** role.

Step 5 From the **Entries Per Page** drop-down list, select the number of CIMC events to display on each page.

Step 6 Click **<Newer** and **Older>** to move backward and forward through the pages of CIMC events, or click **<<Newest** to move to the top of the list.
By default, the newest CIMC events are displayed at the top if the list.

Clearing the CIMC Log

Before You Begin

You must log in as a user with user privileges to clear the CIMC log.

Procedure

Step 1 In the **Navigation** pane, click the **Server** menu.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Faults and Logs** pane, click the **Cisco IMC Log** tab.

Step 4 In the **CIMC Log** pane, click **Clear Log**.

Step 5 In the dialog box that appears, click **OK**.

Configuring the CIMC Log Threshold

You can specify the lowest level of messages that will be included in the CIMC log.

Procedure

Step 1 In the **Navigation** pane, click the **Server** menu.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Faults and Logs** pane, click the **Logging Controls** tab.

Step 4 In the **Local Logging** area, use the **Minimum Severity to Report** drop-down list to specify the lowest level of messages to be included in the CIMC log.
You can select one of the following, in decreasing order of severity:

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice**
- **Informational**
- **Debug**

Note CIMC does not log any messages with a severity below the selected severity. For example, if you select **Error**, then the CIMC log will contain all messages with the severity Emergency, Alert, Critical, or Error. It will not show Warning, Notice, Informational, or Debug messages.

Sending the CIMC Log to a Remote Server

You can configure profiles for one or two remote syslog servers to receive CIMC log entries.

Before You Begin

- The remote syslog server must be configured to receive logs from a remote host.
- The remote syslog server must be configured to receive all types of logs, including authentication-related logs.
- The remote syslog server's firewall must be configured to allow syslog messages to reach the syslog server.

Procedure

Step 1 In the **Navigation** pane, click the **Server** menu.

Step 2 On the **Server** tab, click **Faults and Logs**.

Step 3 In the **Faults and Logs** pane, click the **Logging Controls** tab.

Step 4 In either of the **Remote Syslog Server** dialog boxes, complete the following fields:

Name	Description
Enabled check box	If checked, CIMC sends log messages to the Syslog server named in the **IP Address** field.
IP Address field	The IP address of the Syslog server on which the CIMC log should be stored.
Port field	Enter a destination port number of the Syslog server within the range 1 to 65535. The default port number is 514.

Step 5 (Optional) In the **Minimum Severity to Report** drop-down list, specify the lowest level of messages to be included in the remote logs.
You can select one of the following, in decreasing order of severity:

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice**
- **Informational**

- **Debug**

Note CIMC does not remotely log any messages with a severity below the selected severity. For example, if you select **Error**, then the CIMC remote log will contain all messages with the severity Emergency, Alert, Critical, or Error. It will not show Warning, Notice, Informational, or Debug messages.

Step 6 Click **Save Changes**.