# Viewing Faults and Logs

This chapter includes the following sections:



# Faults Summary

## Viewing the Fault Summary

### Procedure

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

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

**Step 3** In the **Faults Summary** tab, review the following information:

| Name | Description |
|---|---|
| **Time** | The time when the fault occurred. |

| Name | Description |
|---|---|
| **Severity** | This can be one of the following:<br>• **Cleared** - A fault or condition was cleared.<br>• **Critical**<br>• **Info**<br>• **Major**<br>• **Minor**<br>• **Warning** |
| **Code** | The unique identifier assigned to the fault. |
| **DN** | The distinguished name (DN) is a hierarchical representation of the device endpoint and its instance on the server. |
| **Probable Cause** | The unique identifier associated with the event that caused the fault. |
| **Description** | More information about the fault.<br>It also includes a proposed solution. |

# Fault History

## Viewing the Fault History

### Procedure

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

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

**Step 3** In the **Faults History** tab, review the following information:

| Name | Description |
|---|---|
| **Time** | The time when the fault occurred. |

| Name | Description |
|---|---|
| **Severity** | This can be one of the following:<br>• **Emergency**<br>• **Alert**<br>• **Critical**<br>• **Error**<br>• **Warning**<br>• **Notice**<br>• **Informational**<br>• **Debug** |
| **Source** | The software module that logged the event. |
| **Probable Cause** | The unique identifier associated with the event that caused the fault. |
| **Description** | More information about the fault.<br>It also includes a proposed solution. |

# Cisco IMC Log

## Viewing the Cisco IMC Log

### Procedure

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

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

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

**Step 4** Review the following information for each Cisco IMC event in the log.

| Name | Description |
|---|---|
| **Time** column | The date and time the event occurred. |

| Name | Description |
|---|---|
| **Severity** column | The event severity. This can be one of the following:<br>• **Emergency**<br>• **Alert**<br>• **Critical**<br>• **Error**<br>• **Warning**<br>• **Notice**<br>• **Informational**<br>• **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.<br>**Note** This option is only available if your user ID is assigned the **admin** or **user** user role. |

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

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

# Clearing the Cisco IMC Log

### Before You Begin

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

### Procedure

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

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

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

**Step 4** In the **Cisco IMC Log** pane, click **Clear Log**.

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

# System Event Log

## Viewing the System Event Log

### Procedure

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

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

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

**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 a color-coded icon. For the icon, 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.<br>**Note** This option is only available if your user ID is assigned the **admin** or **user** 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** tab.
**Step 2** On the **Server** tab, click **Faults and Logs**.
**Step 3** In the **Faults and Logs** window, click **System Event Log**.
**Step 4** In the **System Event Log** pane, click **Clear Log**.
**Step 5** In the dialog box that appears, click **OK**.

# Logging Controls

## Sending the Cisco IMC Log to a Remote Server

You can configure profiles for one or two remote syslog servers to receive Cisco IMC 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** tab.
**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** areas, complete the following fields:

| Name | Description |
|---|---|
| **Enabled** check box | If checked, Cisco IMC sends log messages to the Syslog server named in the **IP Address** field. |
| **Host Name/IP Address** field | The address of the Syslog server on which the Cisco IMC log should be stored. You can set an IPv4 or IPv6 address or a domain name as the remote system address. |
| **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 that will 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** Cisco IMC does not remotely log any messages with a severity below the selected severity. For example, if you select **Error**, then the Cisco IMC 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**.

# Configuring the Cisco IMC Log Threshold

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

### Procedure

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

**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 that will be included in the Cisco IMC log.
You can select one of the following, in decreasing order of severity:

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

- **Debug**

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

# Sending a Test Cisco IMC Log to a Remote Server

### 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** tab.

**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 **Action** area, click **Send Test Syslog**.
A test Cisco IMC log is sent to the configured remote servers.