Viewing Faults and Logs

This chapter includes the following sections:

Faults Summary

Viewing the Fault Summary

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

Step 2 In the **Chassis** menu, click **Faults and Logs**.

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

Table 1: Actions Area

Name	Description
Total	Displays the total number of rows in the Fault Entries table.
Column drop-down list	Allows you to choose the columns you wish to be displayed.

Name	Description
Show drop-down list	Customize the way you want to view fault entries using filters. These can be: • **Quick Filter** - Default view. • **Advanced Filter** - Filter options to display the fault entries based on one or more criteria. Using the matching rule, you can view entries matching all the rules or any one combination of rules you specified in the **Filter** fields. Click **Go** to view the entries matching the filter criteria that you set. Click the **Save** icon to save the filter criteria that you set. This becomes a user-defined filter which you can use later. **Note** The user-defined filter appears in the **Manage Preset Filters** dialog box. • **All** - Displays all entries • **Manage Preset Filters** - Displays user-defined filters. You can edit or remove the user-defined filter from this dialog box. • **List of pre-defined filters** - Displays the system-defined filters. **Note** You can use the **Filter** icon to hide or unhide the filter fields.

Table 2: Fault Entries Area

Name	Description
Time	The time when the fault occurred.
Severity	This can be one of the following: • **Cleared** - A fault or condition was cleared. • **Critical** • **Info** • **Major** • **Minor** • **Warning**
Code	The unique identifier assigned to the fault.

Name	Description
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. It also includes a proposed solution.

Fault History

Viewing Faults History

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

Step 2 In the **Chassis** menu, click **Faults and Logs**.

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

Table 3: Actions Area

Name	Description
Total	Displays the total number of rows in the Fault History table.
Column drop-down list	Allows you to choose the columns you wish to be displayed.

Name	Description
Show drop-down list	Customize the way you want to view fault history entries using filters. These can be: • **Quick Filter** - Default view. • **Advanced Filter** - Filter options to display the entries based on one or more criteria. Using the matching rule, you can view entries matching all the rules or any one combination of rules you specified in the **Filter** fields. Click **Go** to view the entries matching the filter criteria that you set. Click the **Save** icon to save the filter criteria that you set. This becomes a user-defined filter which you can use later. **Note** The user-defined filter appears in the **Manage Preset Filters** dialog box. • **All** - Displays all entries • **Manage Preset Filters** - Displays user-defined filters. You can edit or remove the user-defined filter from this dialog box. • **List of pre-defined filters** - Displays the system-defined filters. **Note** You can use the **Filter** icon to hide or unhide the filter fields.

Table 4: Faults History Area

Name	Description
Time	The time when the fault occurred.
Severity	This can be one of the following: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Informational** • **Debug**

Name	Description
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. It also includes a proposed solution.

What to do next

Cisco IMC Log

Viewing the Cisco IMC Log

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

Step 2 In the **Chassis** menu, click **Faults and Logs**.

Step 3 In the **Cisco IMC Log** tab, review the following information:

Table 5: Actions Area

Name	Description
Clear Log button	Clears all log files. **Note** This option is only available if your user ID is assigned the **admin** or **user** user role.
Total	Displays the total number of rows in the Cisco IMC Log table.
Column drop-down list	Allows you to choose the columns you wish to be displayed.

Name	Description
Show drop-down list	Customize the way you want to view Cisco IMC log entries using filters. These can be: • **Quick Filter** - Default view. • **Advanced Filter** - Filter options to display the log entries based on one or more criteria. Using the matching rule, you can view entries matching all the rules or any one combination of rules you specified in the **Filter** fields. Click **Go** to view the entries matching the filter criteria that you set. Click the **Save** icon to save the filter criteria that you set. This becomes a user-defined filter which you can use later. **Note** The user-defined filter appears in the **Manage Preset Filters** dialog box. • **All** - Displays all entries • **Manage Preset Filters** - Displays user-defined filters. You can edit or remove the user-defined filter from this dialog box. • **List of pre-defined filters** - Displays the system-defined filters. **Note** You can use the **Filter** icon to hide or unhide the filter fields.

Table 6: Cisco IMC Log Table

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: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Informational** • **Debug**
Source column	The software module that logged the event.
Description column	A description of the event.

System Event Log

Viewing System Event Logs

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

Step 2 In the **Chassis** menu, click **Faults and Logs**.

Step 3 On the **System Event Log** tab, review the following information:

Table 7: Actions Area

Name	Description
Clear Log button	Clears all events from the log file. **Note** This option is only available if your user ID is assigned the **admin** or **user** user role.
Chassis drop-down list	Select a chassis or a server to view its logs.
Total	Displays the total number of rows in the System Event Log table.
Column drop-down list	Allows you to choose the columns you wish to be displayed.

Name	Description
Show drop-down list	Customize the way you want to view events using filters. These can be: • **Quick Filter** - Default view. • **Advanced Filter** - Filter options to display the events based on one or more criteria. Using the matching rule, you can view entries matching all the rules or any one combination of rules you specified in the **Filter** fields. Click **Go** to view the entries matching the filter criteria that you set. Click the **Save** icon to save the filter criteria that you set. This becomes a user-defined filter which you can use later. **Note** The user-defined filter appears in the **Manage Preset Filters** dialog box. • **All** - Displays all entries • **Manage Preset Filters** - Displays user-defined filters. You can edit or remove the user-defined filter from this dialog box. • **List of pre-defined filters** - Displays the system-defined filters. **Note** You can use the **Filter** icon to hide or unhide the filter fields.

Table 8: System Event Log Table

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.

Logging Controls

Viewing Logging Controls

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

Step 2 In the **Chassis** menu, click **Faults and Logs**.

Step 3 In the **Logging Controls** tab, review the following information:

Remote Logging

Name	Description
Enabled check box	If checked, the Cisco IMC sends log messages to the Syslog server named in the **IP Address** field.
Enable Secure Remote Syslog	If checked, Cisco IMC makes a secure, encrypted outbound connection to remote syslog servers supporting secure connectivity for logging. **Note** If this check box is selected, then the **Protocol** field is disabled, by default.
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.
Protocol field	The transport layer protocol for transmission of syslog messages. You can select one of the following: • TCP • UDP
Handshake Status	If secured remote syslog is enabled, then Cisco IMC performs SSL handshake to verify if the certificate is for the given IP address.

Name	Description
Minimum Severity to Report field	Specify the lowest level of messages that will be included in the remote logs. You can select one of the following: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Informational** • **Debug**

Note The 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 contains all messages with the severity **Emergency**, **Alert**, **Critical**, or **Error**. It does not show **Warning**, **Notice**, **Informational**, or **Debug** messages.

Local Logging

This area displays only the **Minimum Severity to Report** drop-down list as shown in the table above. You can specify the lowest level of messages to be included in the local log

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.

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

Step 2 In the **Chassis** menu, click **Faults and Logs**.

Step 3 In either of the **Remote Syslog Server** areas, complete the following fields:

Name	Description
Enabled check box	If checked, the Cisco IMC sends log messages to the Syslog server named in the **IP Address** field.

Name	Description
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 4 (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 5 Click **Save Changes**.

Configuring the Cisco IMC Log Threshold

Before you begin

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

Step 2 In the **Chassis** menu, click **Faults and Logs**.

Step 3 Required: 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.

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

Step 2 In the **Chassis** menu, 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.

Managing the Remote Syslog Certificate

Beginning with release 4.2(2a), you can upload a remote syslog certificate to Cisco UCS C-series servers. You can upload the certificate to one or two Cisco UCS C-series servers.

Uploading a Remote Syslog Certificate

You can upload a remote syslog certificate either from a remote server location or from a local location.

Before you begin

- You must log in as a user with admin privileges.
- The certificate file to be uploaded must reside on a locally accessible file system.

- The following certificate formats are supported:
  - .crt
  - .cer
  - .pem

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

Step 2 In the **Chassis** menu, select **Faults and Logs**.

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

Step 4 To upload the remote syslog certificate, click the **Upload Remote Syslog Certificate** button.

The **Upload Remote Syslog Certificate** dialog box appears.

Step 5 Select a server to which you want to upload the remote syslog certificate from the **Select Server:** drop-down list

Step 6 You can upload the certificate using one of the following methods.

- Upload from remote location
- Upload through browser Client
- Paste the certificate content directly in the **Paste Remote Syslog Certificate** text box.

- **Upload from remote location**: Select this radio button to upload a remote syslog certificate from a remote location.

Name	Description
Upload from remote location field	Select from one of the following protocols: • TFTP • FTP • SCP • SFTP • HTTP **Note** If you select FTP, SCP or SFTP, you will be prompted to enter your username and password.
Server IP/ Hostname button	Enter the remote server IP address or hostname.
Path and Filename	Enter the filepath on the remote server from where you want to upload the remote syslog certificate along with the filename.
Username	Enter the user name for your remote server.
Password	Password for your remote server.

- **Upload through browser Client**: Select this radio button to upload a remote syslog certificate using a browser client.

Click **Browse** and navigate to the location from where you want to upload the remote syslog certificate.

- **Paste Remote Syslog Certificate Content**: Select this radio button to paste the remote syslog certificate details directly in the text box.

Deleting a Remote Syslog Certificate

You can delete a remote syslog certificate from the server.

Before you begin

You must log in as a user with admin privileges.

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

Step 2 In the **Chassis** menu, select **Faults and Logs**.

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

Step 4 To delete the remote syslog certificate, click the **Delete Remote Syslog Certificate** button.

The **Delete Remote Syslog Certificate** dialog box appears.

Step 5 Select the respective check box of the server from which you want to delete the remote syslog certificate.

Step 6 Click **Delete**.

The confirmation message of the deletion is displayed in a pop-up window.

Step 7 Click **OK**.