



Managing Chassis

This chapter includes the following sections:

- [Chassis Summary, on page 1](#)
- [Chassis Inventory, on page 3](#)
- [Viewing Chassis Sensors, on page 5](#)
- [Faults Summary, on page 9](#)
- [Fault History, on page 11](#)
- [System Event Log, on page 13](#)
- [Logging Controls, on page 15](#)

Chassis Summary

Viewing Chassis Summary

By default when you log on to the Cisco UCS E-Series rack-mount server, the **Summary** pane of the Chassis is displayed in the Web UI. You can also view the Chassis summary when in another tab or working area, by completing the following steps:

Procedure

- Step 1** In the **Navigation** pane, click the **Chassis** menu.
- Step 2** In the **Chassis** menu, click **Summary**.
- Step 3** In the **Server Properties** area of the **Chassis Summary** pane, review the following information:

Name	Description
Product Name field	The model name of the chassis.
Serial Number field	The serial number for the chassis.
PID field	The product ID.
UUID	The UUID assigned to the server.
BIOS version	The BIOS version name.

Name	Description
Description field	A user-defined description for the server.
Asset Tag field	A user-defined tag for the server. By default, the asset tag for a new server displays Unknown .

Step 4 In the **Cisco IMC Information** area of the **Chassis Summary** pane, review the following information:

Name	Description
Hostname field	A user-defined hostname for the . By default, the hostname appears in EXXXX-YYYYYYYYYYYYY format, where XXXX is the model number and YYYYYYYYYYYY is the serial number of the server.
IP Address field	The IP address for the .
MAC Address field	The MAC address assigned to the active network interface to the .
Firmware Version field	The current firmware version.
Current Time field	The current date and time according to the clock. Note gets the current date and time from the server BIOS when the NTP is disabled. When NTP is enabled, gets the current time and date from the NTP server. To change this information, reboot the server and press F2 when prompted to access the BIOS configuration menu. Then change the date or time using the options on the main BIOS configuration tab.

Step 5 In the **Router Information** area of the **Chassis Summary** pane, review the following information:

Name	Description
Router Model field	The router model name.
Serial Number field	The serial number for the router.

Step 6 In the **Chassis Status** area of the **Chassis Summary** pane, review the following information:

Name	Description
Power State field	The current power state.
Overall Server Status field	The overall status of the server. This can be one of the following: <ul style="list-style-type: none"> • Memory Test In Progress—The server is performing a self-test of the installed memory. This condition normally occurs during the boot process. • Good • Moderate Fault • Severe Fault

Name	Description
Overall DIMM Status field	The overall status of the memory modules. This can be one of the following: <ul style="list-style-type: none">• Good• Fault• Severe Fault You can click the link in this field to view detailed status information.
Overall Storage Status field	The overall status of all controllers. This can be one of the following: <ul style="list-style-type: none">• Good• Moderate Fault• Severe Fault

Creating a Server Asset Tag

Before you begin

You must log in with user or admin privileges to perform this task.

Procedure

- Step 1** In the **Navigation** pane, click the **Chassis** menu.
 - Step 2** In the **Chassis** menu, click **Summary**.
 - Step 3** Click **Save Changes**.
-

Chassis Inventory

Viewing Power Supply Properties

Procedure

- Step 1** In the **Navigation** pane, click the **Chassis** menu.
- Step 2** In the **Chassis** menu, click **Inventory**.

- Step 3** In the **Inventory** work pane, click the **Power Supplies** tab and review the following information for each power supply:

Name	Description
Device ID column	The identifier for the power supply unit.
Status column	The status of the power supply unit.
Input column	The input into the power supply, in watts.
Max Output column	The maximum output from the power supply, in watts.
FW Version column	The firmware version for the power supply.
Product ID column	The product identifier for the power supply assigned by the vendor.

Viewing Storage Properties

Before you begin

The server must be powered on, or the properties will not display.

Procedure

- Step 1** In the **Navigation** pane, click the **Chassis** menu.
- Step 2** In the **Chassis** menu, click **Inventory**.
- Step 3** In the **Inventory** work pane, click the **Storage** tab and review the following information:

Name	Description
Controller field	PCIe slot in which the controller drive is located.
PCI Slot field	The name of the PCIe slot in which the controller drive is located.
Product Name field	Name of the controller.
Serial Number field	The serial number of the storage controller.
Firmware Package Build field	The active firmware package version number.
Product ID field	Product ID of the controller.
Battery Status field	Status of the battery.
Cache Memory Size field	The size of the cache memory, in megabytes.
Health field	The health of the controller.

Viewing Network Adapter Properties

Before you begin

The server must be powered on, or the properties will not display.

Procedure

- Step 1** In the **Navigation** pane, click the **Chassis** menu.
- Step 2** In the **Chassis** menu, click **Inventory**.
- Step 3** In the **Inventory** work pane, click the **Network Adapters** tab and review the following information:

Name	Description
Slot ID column	The slot in which the adapter is installed.
Product Name column	The product name for the adapter.
Number of Interfaces column	The number of interfaces for the adapter.
External Ethernet Interfaces	ID —The ID for the external ethernet interface. MAC Address —The MAC address for the external ethernet interface.

Viewing Chassis Sensors

Viewing Power Supply Sensors

Procedure

- Step 1** In the **Navigation** pane, click the **Chassis** menu.
- Step 2** In the **Chassis** menu, click **Sensors**.
- Step 3** In the **Sensors** working area, click the **Power Supply** tab.
- Step 4** Review the following sensor properties for power supply:

Properties Area

Name	Description
Redundancy Status field	The power supply redundancy status.

Threshold Sensors Area

Name	Description
Sensor Name column	The name of the sensor
Sensor Status column	The status of the sensor. This can be one of the following: <ul style="list-style-type: none"> • Unknown • Informational • Normal • Warning • Critical • Non-Recoverable
Reading column	The current power usage, in watts.
Critical Threshold Min column	The minimum critical threshold.
Critical Threshold Max column	The maximum critical threshold.
Non-Recoverable Threshold Min column	The minimum non-recoverable threshold.
Non-Recoverable Threshold Max column	The maximum non-recoverable threshold.

Discrete Sensors Area

Name	Description
Sensor Name column	The name of the sensor.
Sensor Status column	The status of the sensor. This can be one of the following: <ul style="list-style-type: none"> • Unknown • Informational • Normal • Warning • Critical • Non-Recoverable
Reading column	The basic state of the sensor.

Viewing Temperature Sensors

Procedure

- Step 1** In the **Navigation** pane, click the **Chassis** menu.
- Step 2** In the **Chassis** menu, click **Sensors**.
- Step 3** In the **Sensors** working area, click the **Temperature** tab.
- Step 4** Review the following temperature sensor properties:

Name	Description
Sensor Name column	The name of the sensor
Sensor Status column	The status of the sensor. This can be one of the following: <ul style="list-style-type: none"> • Unknown • Informational • Normal • Warning • Critical • Non-Recoverable
Temperature column	The current temperature, in Celsius.
Critical Threshold Min column	The minimum critical threshold.
Critical Threshold Max column	The maximum critical threshold.
Non-Recoverable Threshold Min column	The minimum non-recoverable threshold.

Viewing Voltage Sensors

Procedure

- Step 1** In the **Navigation** pane, click the **Chassis** menu.
- Step 2** In the **Chassis** menu, click **Sensors**.
- Step 3** In the **Sensors** working area, click the **Voltage** tab.
- Step 4** Review the following voltage sensor properties:

Name	Description
Sensor Name column	The name of the sensor
Sensor Status column	The status of the sensor. This can be one of the following: <ul style="list-style-type: none"> • Unknown • Informational • Normal • Warning • Critical • Non-Recoverable
Voltage (V) column	The current voltage, in Volts.
Critical Threshold Min column	The minimum critical threshold.
Critical Threshold Max column	The maximum critical threshold.
Non-Recoverable Threshold Min column	The minimum non-recoverable threshold.
Non-Recoverable Threshold Max column	The maximum non-recoverable threshold.

Viewing Current Sensors

Procedure

- Step 1** In the **Navigation** pane, click the **Chassis** menu.
- Step 2** In the **Chassis** menu, click **Sensors**.
- Step 3** In the **Sensors** working area, click the **Current** tab.
- Step 4** Review the following current sensor properties:

Viewing Storage Sensors

Procedure

- Step 1** In the **Navigation** pane, click the **Compute** menu.
- Step 2** In the **Chassis** menu, click **Sensors**.

Step 3 In the **Storage** tab's **Storage Sensors** area, view the following storage-related statistics for the server:

Name	Description
Name column	The name of the storage device.
Status column	A brief description of the storage device status.

Faults Summary

Viewing the Fault Summary

Procedure

- 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
<p>Show drop-down list</p>	<p>Customize the way you want to view fault entries using filters. These can be:</p> <ul style="list-style-type: none"> • 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. <p>Click Go to view the entries matching the filter criteria that you set.</p> <p>Click the Save icon to save the filter criteria that you set. This becomes a user-defined filter which you can use later.</p> <p>Note The user-defined filter appears in the Manage Preset Filters dialog box.</p> <ul style="list-style-type: none"> • 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. <p>Note You can use the Filter icon to hide or unhide the filter fields.</p>

Table 2: Fault Entries Area

Name	Description
<p>Time</p>	<p>The time when the fault occurred.</p>
<p>Severity</p>	<p>This can be one of the following:</p> <ul style="list-style-type: none"> • Cleared - A fault or condition was cleared. • Critical • Info • Major • Minor • Warning
<p>Code</p>	<p>The unique identifier assigned to the fault.</p>

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

Procedure

- 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	<p>Customize the way you want to view fault history entries using filters. These can be:</p> <ul style="list-style-type: none"> • 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. <p>Click Go to view the entries matching the filter criteria that you set.</p> <p>Click the Save icon to save the filter criteria that you set. This becomes a user-defined filter which you can use later.</p> <p>Note The user-defined filter appears in the Manage Preset Filters dialog box.</p> <ul style="list-style-type: none"> • 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. <p>Note You can use the Filter icon to hide or unhide the filter fields.</p>

Table 4: Faults History Area

Name	Description
Time	The time when the fault occurred.

Name	Description
Severity	This can be one of the following: <ul style="list-style-type: none"> • Emergency • Alert • Critical • Error • Warning • Notice • Informational • 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. It also includes a proposed solution.

What to do next

System Event Log

Viewing System Event Logs

Procedure

- 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 5: 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.

Name	Description
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.
Show drop-down list	<p>Customize the way you want to view events using filters. These can be:</p> <ul style="list-style-type: none"> • 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. <p>Click Go to view the entries matching the filter criteria that you set.</p> <p>Click the Save icon to save the filter criteria that you set. This becomes a user-defined filter which you can use later.</p> <p>Note The user-defined filter appears in the Manage Preset Filters dialog box.</p> <ul style="list-style-type: none"> • 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. <p>Note You can use the Filter icon to hide or unhide the filter fields.</p>

Table 6: 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

Procedure

- 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.
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.
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: <ul style="list-style-type: none"> • 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

What to do next

Sending the Cisco IMC Log to a Remote Server

You can configure profiles for one or two remote syslog servers to receive 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 **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.
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 does not remotely log any messages with a severity below the selected severity. For example, if you select **Error**, then the 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

Procedure

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 log.

You can select one of the following, in decreasing order of severity:

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

Note does not log any messages with a severity below the selected severity. For example, if you select **Error**, then the 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 **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 log is sent to the configured remote servers.
