Managing the Chassis

Chassis Summary

Viewing Chassis Summary

By default, when you log on to CIMC, the **Summary** pane of the **Chassis** menu is displayed in the 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.
FPGA Version	The FPGA version number.
SBFPGA Version	The SBFPGA version number.
MCU Version	The MCU version number.

Name	Description
AIKIDO Version	The AIKIDO version number.
Last Reboot Reason field	Reason for the last reboot.
Uptime	The uptime for the server.
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 Integrated Management Controller (Cisco IMC) Information** area of the **Chassis Summary** pane, review the following information:

Name	Description
Hostname field	A user-defined hostname for the CIMC. By default, the hostname appears in EXXXX-YYYYYYYYYY format, where XXXX is the model number and YYYYYYYYYY is the serial number of the server.
IP Address field	The IP address for the CIMC.
MAC Address field	The MAC address for the CIMC.
Firmware Version field	The current firmware version.
Current Time field	The current date and time according to the clock. **Note** CIMC gets the current date and time from the server BIOS when NTP is disabled. When NTP is enabled, CIMC 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. Update the date or time using the options on the main BIOS configuration tab.
Local Time field	The local date and time for the CIMC.
Timezone field	The time zone for the CIMC.
Select Timezone dialog box	Dialog box to select the time zone for the CIMC.

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

Name	Description
Power State field	The current power state.

Name	Description
Post Completion Status field	The post completion status.
Overall Server Status field	The overall status of the server. This can be one of the following: • **Memory Test In Progress**—Theserver is performing a self-test of the installed memory. This condition normally occurs during the boot process. • **Good** • **Moderate Fault** • **Severe Fault** You can click the link in this field to view detailed status information.
Overall DIMM Status field	The overall status of the memory modules. This can be one of the following: • **Good** • **Fault** • **Severe Fault** You can click the link in this field to view detailed status information.

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 Enter the **Asset Tag Details** in the text box.
Step 4 Click **Save Changes**.

Selecting a Time Zone

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 In the **Cisco Integrated Management Controller (Cisco IMC) Information** area, click the **Select Timezone** link.

Step 4 In the **Select Timezone** dialog box, click your location on the map to select your time zone, or select your time zone from the **Timezone** drop-down menu.

Step 5 Click **Save**.

Chassis Inventory

Viewing CPU 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 **CPU** tab and review the following information for each CPU:

Name	Description
Socket Name column	The CPU socket name.
Vendor column	The CPU vendor.
Family column	The CPU product family.
Number of Threads column	The number of threads.
Version column	The CPU version.
Speed column	The CPU speed (Mhz).
Number of Cores column	The number of cores in the CPU.
Status column	The CPU status.

Name	Description
Signature column	The CPU signature.

Viewing Memory 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 **Memory** tab and review the following information:

Name	Description
Name column	The DIMM name.
Capacity column	The DIMM capacity.
Channel Speed column	The DIMM channel speed (Mhz).
Channel Type column	The DIMM channel type.
Memory Type Detail column	The DIMM memory type.
Bank Locator column	The DIMM bank locator.
Manufacturer column	The DIMM manufacturer name.
Serial Number column	The DIMM serial number.
Asset Tag column	The DIMM asset tag.
Part Number column	The DIMM part number.
Visibility column	The DIMM visibility status.
Operability column	The DIMM operability status.
Data Width column	The DIMM data width.

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
Name column	The name for the power supply unit.
Status column	The status of the power supply unit.
Product ID column	The product identifier for the power supply assigned by the vendor.
Serial column	The serial number of the power supply unit.
Power column	The power supply, in watts.

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 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.

Name	Description
External Ethernet Interfaces	**ID**—The ID for the external ethernet interface. **MAC Address**—The MAC address for the external ethernet interface.

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 TPM 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 **TPM** tab and review the following information:

Name	Description
Version field	The TPM version.
Model field	The TPM model.
Vendor field	The TPM vendor.
Revision field	The TPM revision.
Firmware Version field	The TPM firmware version.
Presence field	The TPM presence.
Enabled Status field	The TPM enabled status.
Active Status field	The TPM active status.
Ownership field	The TPM ownership.

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** area, click the **Power Supply** tab.

Step 4 Review the following sensor properties for power supply:

Table 1: Threshold Sensors Area

Name	Description
Sensor Name column	The name of the sensor.

Name	Description
Sensor Status column	The status of the sensor. This can be one of the following: • **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.

Table 2: Discreet 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: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
Reading column	The basic state of the sensor.

Viewing Fan 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** area, click the **Fan** tab.

Step 4 Review the following fan 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: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
Speed column	The current fan speed, in RPMS.
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 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** 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: • **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.
Non-Recoverable Threshold Max column	The maximum 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** area, click the **Voltage** tab.

Step 4 Review the following voltage sensor properties:

Name	Description
Sensor Name column	The name of the sensor.

Name	Description
Sensor Status column	The status of the sensor. This can be one of the following: • **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** area, click the **Current** tab.

Step 4 Review the following current sensor properties:

Name	Description
Sensor Name column	The name of the sensor.

Name	Description
Sensor Status column	The status of the sensor. This can be one of the following: • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
Current column	The current, in Ampere.
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 LED 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** area, click the **LEDs** tab.

Step 4 Review the following LED properties:

Name	Description
LED Status column	The status of the LED. This can be one of the following: • **ON** • **OFF** • **BLINKING**

Name	Description
LED Color column	The current color of the LED. For details about what the colors mean, see the hardware installation guide for the type of server you are using.

Viewing Storage 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** area, click the **Storage** tab.
Step 4 Review the following storage properties:

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

Faults and Logs

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:

Name	Description
Show drop-downlist	Customizethe way you want to view fault entries using filters. These can be: • **QuickFilter** - 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.
Time column	The time when the fault occurred.
Severity column	This can be one of the following: • **Cleared**-A fault or condition was cleared. • **Critical** • **Info** • **Major** • **Minor** • **Warning**
Code column	The unique identifier assigned to the fault.
Domain Name column	The distinguished name (DN) is a hierarchical representation of the device endpoint and its instance on the server.

Name	Description
Probable Cause column	The unique identifier associated with the event that caused the fault.
Description column	More information about the fault. It also includes a proposed solution.

Viewing the Fault 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:

Name	Description
Show drop-downlist	Customizethe way you want to view fault entries using filters. These can be: • **QuickFilter** - 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.
Time column	The time when the fault occurred.
Severity column	This can be one of the following: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Informational** • **Debug**

Name	Description
Probable Cause column	The unique identifier associated with the event that caused the fault.
Description column	More information about the fault. It also includes a proposed solution.

Viewing the System Event Log

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 **System Event Log** tab, review the following information:

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 role.

Name	Description
Show drop-downlist	Customizethe way you want to view fault entries using filters. These can be: • **QuickFilter** - 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.
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.

Viewing the CIMC Log

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 **Cisco IMC Log** tab, review the following information:

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 role.
Show drop-downlist	Customizethe way you want to view fault entries using filters. These can be: • **QuickFilter** - 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.
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.
Source column	The source of the event.

Name	Description
Description column	A description of the event.

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:

Table 3: Remote Logging Area

Name	Description
Enabled checkbox	If checked, the CIMC sends log messages to the syslog server named in the **IP Address** field.
Enable Secure Remote Syslog check box	If checked, the CIMC enables secure remote syslog.
HostName/IP Address field	The address of the Syslog server on which the Cisco IMC log should bestored. 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 field	Displays the handshake status.

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**

Table 4: Local Logging Area

Minimum Severity to Report drop-down	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 choose **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.

Table 5: Upload Status Area

Certificate Upload Status field	Displays the certificate upload status.

Certificate Upload Progress field	Displays the certificate upload progress.

Sending the CIMC 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.
- You can use the **Send Test Syslog** link to test the server.

Procedure

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

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

Step 3 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, the CIMC sends log messages to the syslog server named in the **IP Address** field.
Enable Secure Remote Syslog check box	If checked, the CIMC enables secure remote syslog.
Host Name/IP Address field	The address of the Syslog server on which the Cisco IMC log should bestored. 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

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 choose one of the following, in decreasing order of severity:

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

Note The system does not remotely log any messages with a severity below the chosen severity. For example, if you choose **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 6 Click **Save Changes**.

Uploading a Remote Syslog Certificate

Before you begin

At least one of the remote syslog servers must be enabled before uploading the remote syslog certificate.

Procedure

Step 1 In the **Chassis** menu, click **Faults and Logs**.

Step 2 In the **Faults and Logs** work are, click the **Logging Controls** tab.

Step 3 Click the **Upload Remote Syslog Certificate** link.

Step 4 In the **Upload Remote Syslog Certificate** dialog box, enter the following information:

Name	Description
Select Server drop-down	Selects the server to which the certificate is uploaded.
Upload from remote location radio button	If the certificate resides on a remote server, click this radio button, complete the required fields, and then click **Upload** to upload the certificate.

Name	Description
Upload from remote location drop-down	The remote server type. This can be one of the following: • **TFTP** • **FTP** • **SFTP** • **SCP** • **HTTP**
Server IP/Hostname field	The IP address or hostname of the server on which the certificate file resides. Depending on the setting in the **Upload from remote location** drop-down list, the fields displayed may vary.
Path and Filename field	The path and filename of the certificate file on the remote server.
Username field	Username for the server.
Password field	Password for the server.
Upload through Browser Client button	Allows you to browse and upload the certificate.
File field	The certificate file you want to upload.
Browse button	Opens a dialog box that allows you to navigate to the appropriate certificate file.
Paste Content radio button	Opens a dialog box that allows you to copy the entire content of the certificate and paste it in the **Paste Remote Syslog Certificate** text field.
Upload button	Uploads the content.
Close button	Cancels the process and closes the dialog box.

Step 5 Click **Save Changes** to save your changes, or **Reset Values** to reset the parameters to previous values.

Configuring the CIMC Log Threshold

Procedure

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

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

Step 3 Click the **Logging Controls** tab.

Step 4 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 choose one of the following, in decreasing order of severity:

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

Note The system does not remotely log any messages with a severity below the chosen severity. For example, if youchoose **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.