System Management

System Policies

You can configure the system policies for all of Cisco UCS Central, or at the domain group level. To configure system policies at the domain group, see Domain Group System Policies, on page 9.

UCS Central system policies include the following:

- **Faults—**Allows you to determine when faults are cleared, the flapping interval (the length of time between the fault being raised and the condition being cleared), and the retention interval (the length of time a fault is retained in the system).
- **Syslog—**Allows you to determine the type of log files that you want to collect, and where you want to view them or store.
- **Core Dump—**Uses the Core File Exporter to export core files as they occur.

Configuring UCS Central System Policies

From the **Manage UCS Central System Policies** dialog box, you can configure the properties and settings for faults, syslog, and core dump export.

Step 1 From the System Settings icon, choose **System Policies**.
This launches the **Manage UCS Central System Policies** dialog box.

Step 2 Click the icon for the section that you want to configure.

- The **Fault** section allows you to perform the same tasks as the **Manage UCS Central Fault Policy** dialog box. For more information, see Managing a UCS Central Fault Policy, on page 4.
- The **Syslog** section allows you to perform the same tasks as the **Manage UCS Central Syslog** dialog box. For more information, see Managing UCS Central Syslog, on page 5.
- The **Core Dump Export** section allows you to perform the same tasks as the **Manage UCS Central Core Dump Export** dialog box. For more information, see Managing UCS Central Core Dump Export, on page 7.

Step 3 Complete the fields as required for each section.

Step 4 Click **Save**.

Related Topics

Managing a UCS Central Fault Policy, on page 4
Managing UCS Central Syslog, on page 5
Managing UCS Central Core Dump Export, on page 7

Managing Equipment Policies

Step 1 Click the **Domain Group Navigation** icon and choose a domain group.

Step 2 Click the **Configuration** icon and choose **System Policies**.

Step 3 In **Equipment**, click **Basic** and complete the following fields:

a) In **Rack Management Action**, select how server management is configured when a new rack server is discovered:

- **Auto Acknowledged**—Cisco UCS automatically configures server management by domain based on the available server connections.
- **User Acknowledged**—Cisco UCS does not automatically configure server management. It waits until acknowledged by the user.

b) In **MAC Address Table Aging Time**, select the length of time an idle MAC address remains in the MAC address table before it is removed:

- **Mode Default—**System uses the default value. For end-host mode, the default is 14,500 seconds. For switching mode, the default is 300 seconds.
- **Never—**Cisco UCS never removes MAC addresses from the table.
- **Other—**Enter a custom value in the dd:hh:mm:ss field.

c) In **VLAN Port Count Optimization**, select whether Cisco UCS can logically group VLANs to optimize the use of ports and reduce the CPU load on the FI.

d) In **Firmware Auto Server Sync State**, select the firmware synchronization policy for recently discovered blade servers or rack servers:

- **User Acknowledged—**Cisco UCS does not synchronize firmware until the administrator acknowledges the upgrade.
- **No Actions—**Cisco UCS does not perform any firmware upgrade on the server.

e) In **Info Action**, select whether the information policy displays the uplink switches that are connected to the Cisco UCS domain.

Step 4 Click **Discovery** and complete the fields to specify how you want the system to behave when you add a new chassis or FEX:

a) In **Chassis/FEX Link Action**, select the minimum threshold for the number of links between the chassis or FEX and the fabric interconnect.

b) In **Chassis/FEX Link Grouping Preference**, select whether the links from the system IO controllers, IOMs, or FEXes to the fabric interconnects are grouped in a port channel.

c) In the **Multicast Hardware Hash**, click **Enable** to specify if Cisco UCS can use all of the links from the IOMs or FEXes to the fabric interconnects for multicast traffic.

d) In the **Backplane Speed Preference**, choose the speed that you want to use.

Step 5 Click **Power** and complete the following fields:

a) In **Power Redundancy**, select the power redundancy policy that you want to use:

- **N+1—**The total number of power supplies, plus one additional power supply for redundancy, equally share the power load for the chassis. If any additional power supplies are installed, Cisco UCS sets them to a "turned-off" state.
- **Grid—**Two power sources are turned on, or the chassis requires greater than N+1 redundancy. If one source fails, the surviving power supplies continue to provide power to the chassis.
- **Non-Redundant—**All installed power supplies are turned on and the load is evenly balanced. Only power small configurations (requiring less than 2500W) by a single power supply.

b) In **Power Allocation**, select the power allocation management mode used in the Cisco UCS domain:

- **Policy Driven Chassis Group Cap—**Configures power allocation at the chassis level through power control policies included in the associated service profiles.
- **Manual Blade Level Cap—**Configures power allocation on each individual blade server in all chassis.

c) In **ID Soaking Interval**, specify the number of seconds Cisco UCS Central waits before reassigning a pool entity that Cisco UCS released. Enter an integer between 0 and 86400.

Step 6 Click **Save**.

Managing Rack Discovery Policies

Step 1 Navigate to the root **Domain Group** page.

Step 2 Click the **Settings** icon and select **System Profile**.

Step 3 In **Rack Discovery**, click **Basic**.

Step 4 In **Discovery Policy Action**, select how you want the system to behave when you add a new rack server.

- **User Acknowledged—**Cisco UCS domain waits until the user tells it to search for new servers.
- **Immediate—**Cisco UCS domain attempts to discover new servers automatically.

Step 5 Click **Policies** and select the scrub policy to run on a newly discovered server.
The server must meet the criteria in the selected server pool policy qualification.

Step 6 Click **Save**.

Managing a UCS Central Fault Policy

Step 1 In the Task bar, type **Manage UCS Central Fault Policy** and press Enter.
This launches the **Manage UCS Central Fault Policy** dialog box.

Step 2 In **Fault**, complete the following fields:

Note The **Initial Severity** and **Action on Acknowledgment** fields are read-only, and cannot be modified.

1 Enter a time in seconds in the **Flapping Interval (Seconds)** field.

Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, Cisco UCS Central does not allow a fault to change its state until this amount of time has elapsed since the last state change.

If the condition reoccurs during the flapping interval, the fault returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared. What happens at that point depends on the setting in the **Action on Clear** field.

2 In **Soaking Interval**, choose None, or select a custom soaking interval.

3 In **Clear Interval**, select whether Cisco UCS Central should automatically mark faults as cleared based on their age.

If you choose **None**, faults are not automatically cleared. If you choose **Custom Interval**, Cisco UCS automatically clears fault messages after the length of time you specify in the associated interval field.

4 In **Action on Clear**, select the action the system must take when a fault is cleared.

If you choose **Retain Cleared Faults**, then the cleared faults are retained for the length of time specified in the **Retention Interval**. If you choose **Delete Cleared Faults**, then the cleared faults are deleted immediately.

5 If **Action on Clear** is set to **Retain Cleared Faults**, then in **Retention Interval** specify the length of time Cisco UCS retains a fault that is marked as cleared.

If you choose **Forever**, Cisco UCS retains all cleared fault messages regardless of how old they are. If you choose **Custom Interval**, Cisco UCS retains cleared fault messages for the length of time you specify in the associated interval field.

Step 3 Click **Save**.

Related Topics

Configuring UCS Central System Policies, on page 2
Managing UCS Central Syslog, on page 5
Managing UCS Central Core Dump Export, on page 7

Managing UCS Central Syslog

Step 1 In the Task bar, type **Manage UCS Central Syslog** and press Enter.
This launches the **Manage UCS Central Syslog** dialog box.

Step 2 In **Syslog Sources**, choose **Enabled** for each source for which you want to collect log files.
This can be one of the following:

- **Faults**
- **Audits**
- **Events**

Step 3 In **Local Destination**, specify where the syslog messages can be added and displayed. This can be one of the following:

- **Console—**If enabled, syslog messages are displayed on the console as well as added to the log. Choose the logging level for the messages you would like displayed.
- **Monitor—**If enabled, syslog messages are displayed on the monitor as well as added to the log. Choose the logging level for the messages you would like displayed.
- **Log File—**If enabled, syslog messages are saved in the log file. If disabled, syslog messages are not saved. Choose the logging level, a file name, and the maximum file size.

Select the lowest message level that you want the system to store. The system stores that level and above. The logging levels can be one of the following:

- **Critical (UCSM Critical)**
- **Alert**
- **Emergency**
- **Error (UCSM Major)**
- **Warning (UCSM Minor)**
- **Notification (UCSM Warning)**
- **Information**
- **Debug**

Step 4 In **Remote Destination**, specify whether to store the syslog messages in a primary, secondary, and/or tertiary server. Specify the following information for each remote destination:

- **Logging Level—**Select the lowest message level that you want the system to store. The system stores that level and above in the remote file. This can be one of the following:
  - **Critical (UCSM Critical)**
  - **Alert**
  - **Emergency**
  - **Error (UCSM Major)**
  - **Warning (UCSM Minor)**
  - **Notification (UCSM Warning)**
  - **Information**
  - **Debug**
- **Facility—**The facility associated with the remote destination.
- **Host Name/IPAddress—**The hostname or IP address on which the remote log file resides. If you are using a host name rather than a IPv4 or IPv6 address, you must configure the DNS server in Cisco UCS Central.

Step 5 Click **Save**.

Related Topics

Configuring UCS Central System Policies, on page 2
Managing a UCS Central Fault Policy, on page 4
Managing UCS Central Core Dump Export, on page 7

Managing UCS Central Core Dump Export

Cisco UCS uses the Core File Exporter to export core files as soon as they occur to a specified location on the network through TFTP. This functionality allows you to export the core file in tar format.

Step 1 In the Task bar, type **Manage UCS Central Core Dump Export** and press **Enter**.
This launches the **Manage UCS Central Core Dump Export** dialog box.

Step 2 Click **Enable** to export core files.

Step 3 (Optional) Enter a description for the remote server used to store the core file.

Step 4 The **Frequency**, **Maximum No. of Files**, **Remote Copy**, and **Protocol** fields are set by default.

Step 5 (Optional) In **Absolute Remote Path**, enter the path to use when exporting the core file to the remote server.

Step 6 In **Remote Server Host Name/IP Address**, enter a hostname or IP address to connect with via TFTP

Step 7 (Optional) In **TFTP Port**, enter the port number to use when exporting the core file via TFTP. The default port number is 69.

Step 8 Click **Save**.

Related Topics

Configuring UCS Central System Policies, on page 2
Managing a UCS Central Fault Policy, on page 4
Managing UCS Central Syslog, on page 5

System Profile

The system profile allows you to configure the system information such as the interfaces, date and time, DNS, remote access, trusted points, and certificate information for all of Cisco UCS Central.

To configure the domain group system profile, see Domain Group System Profile, on page 10.

Managing the UCS Central System Profile

Step 1 From the System Settings icon, choose **System Profile**.
This launches the **Manage UCS Central System Profile** dialog box.

Step 2 In the **UCS Central** section, you can view the **UCS Central System Name**, **Mode**, and virtual IPv4 and IPv6 addresses. These values are populated when you first configure Cisco UCS Central. The system name and mode cannot be modified.

Step 3 In **Interfaces**, review or change the following management nodes:

- **Primary Node (IPv4)**
- **Primary Node (IPv6)**

- **Secondary Node (IPv4)**
- **Secondary Node (IPv6)**

Step 4 In **Date & Time**, choose the time zone and add an NTP server.

Step 5 In **DNS**, type the Cisco UCS Central domain name and add a DNS server.

Step 6 In **Remote Access**, choose a Key Ring.

Step 7 In **Trusted Points**, click **Add** to add a new trusted point and certificate chain.

Step 8 In **Certificates**, you can view the existing, or create a new key ring and certificate request.

Step 9 Click **Save**.

Related Topics

Managing the UCS Central NTP Servers, on page 8
Managing the UCS Central Management Node, on page 8
Managing the UCS Central DNS Servers, on page 9

Managing the UCS Central Management Node

Step 1 In the Task bar, type **Manage UCS Central Management Node** and press Enter.
This launches the **Manage UCS Central Management Node** dialog box.

Step 2 In **Management Node**, click the name of the node you would like to configure.

Step 3 Enter values for the **IP Address**, **Subnet Mask**, and **Default Gateway**.

Step 4 Click **Save**.

Related Topics

Managing the UCS Central System Profile, on page 7
Managing the UCS Central NTP Servers, on page 8
Managing the UCS Central DNS Servers, on page 9

Managing the UCS Central NTP Servers

Step 1 In the Task bar, type **Manage UCS Central NTP Servers** and press Enter.
This launches the **Manage UCS Central NTP Servers** dialog box.

Step 2 In **Time Zone**, select the time zone for the domain.

Step 3 In **NTP Servers**, click **Add** to add a new NTP server, or **Delete** to remove an existing one.

Step 4 Click **Save**.

Related Topics

Managing the UCS Central System Profile, on page 7
Managing the UCS Central Management Node, on page 8
Managing the UCS Central DNS Servers, on page 9

Managing the UCS Central DNS Servers

Step 1 In the Task bar, type **Manage UCS Central DNS Servers** and press Enter.
This launches the **Manage UCS Central DNS Servers** dialog box.

Step 2 In **UCS Central Domain Name**, type the name of the Cisco UCS Central domain.

Step 3 In **DNS Servers**, click **Add** to add a new DNS server, or **Delete** to remove an existing one.

Step 4 Click **Save**.

Related Topics

Managing the UCS Central System Profile, on page 7
Managing the UCS Central NTP Servers, on page 8
Managing the UCS Central Management Node, on page 8

Domain Group System Policies

You can configure the system policies at the domain group level, or for all of Cisco UCS Central. To configure system policies for UCS Central, see System Policies, on page 1.

Domain group system policies include the following:

- **Equipment—**Allows you to set policies for the equipment in your domain group, including discovery and power policies.
- **Rack Discovery—**Allows you to determine what action is taken when a rack-mount server is discovered, and assign a scrub policy.
- **Fault—**Allows you to determine when faults are cleared, the flapping interval (the length of time between the fault being raised and the condition being cleared), and the retention interval (the length of time a fault is retained in the system).
- **Syslog—**Allows you to determine the type of log files that you want to collect, and where you want to view them or store.

- **Core Dump—**Uses the Core File Exporter to export core files as they occur.
- **Interfaces—**Allows you to set criteria for monitoring your domain group interfaces.
- **System Events—**Allows you to set the criteria for domain group system event logs.

Managing Domain Group System Policies

Note If you are setting the system policies for a sub-domain, you need to enable each policy before you can set it.

Step 1 Navigate to the root **Domain Group** page.

Step 2 Click the **Settings** icon and select **System Profile**.

Step 3 In **Equipment**, complete the necessary fields.
For more information, see Managing Equipment Policies, on page 2.

Step 4 In **Rack Discovery**, complete the necessary fields.
For more information, see Managing Rack Discovery Policies, on page 4.

Step 5 In **Fault**, complete the necessary fields.
For more information, see Managing a UCS Central Fault Policy, on page 4.

Step 6 In **Syslog**, complete the necessary fields.
For more information, see Managing UCS Central Syslog, on page 5.

Step 7 In **Core Dump**, complete the necessary fields.
For more information, see Managing UCS Central Core Dump Export, on page 7.

Step 8 In **Interfaces**, choose whether to enable **Interface Monitoring Policy**.

Step 9 If you select **Enabled**, complete the interface monitoring information as required.

Step 10 In **System Events**, complete the necessary fields to determine how the system event logs will be collected.

Step 11 Click **Save**.

Domain Group System Profile

The domain group system profile allows you to configure the date and time, DNS settings, remote access, and trusted points for each domain group.

To configure the system profile for Cisco UCS Central, see System Profile, on page 7.

Managing the Domain Group System Profile

Step 1 Navigate to the root **Domain Group** page.
Step 2 Click the **Settings** icon and select **System Profile**.
Step 3 In **Date & Time**, choose the time zone and add an NTP server.
Step 4 In **DNS**, type the UCS Central domain name and add a DNS server.
Step 5 In **Remote Access**, type the HTTPS, HTTPS Port, and choose a Key Ring.
Step 6 In **Trusted Points**, click **Add** to create a trusted point and add a certificate chain.
Step 7 Click **Save**.

Maintenance Policy

When you make any change to a service profile that is associated with servers in the registered domains, the change may require a server reboot. The maintenance policy determines how Cisco UCS Central reacts to the reboot request.

You can create a maintenance policy and specify the reboot requirements to make sure the server is not automatically rebooted with any changes to the service profiles. You can specify one of the following options for a maintenance policy:

- **Immediately**: Whenever you make a change to the service profile, apply the changes immediately.
- **User Acknowledgment**: Apply the changes after a user with administrative privileges acknowledges the changes in the system.
- **Schedule**: Apply the changes based on the day and time you specify in the schedule.

When you create the maintenance policy if you specify a schedule, the schedule deploys the changes in the first available maintenance window.

Note A maintenance policy only prevents an immediate server reboot when a configuration change is made to an associated service profile. However, a maintenance policy does not prevent the following actions from taking place right away:

- Deleting an associated service profile from the system
- Disassociating a server profile from a server
- Directly installing a firmware upgrade without using a service policy
- Resetting the server

Creating or Editing a Maintenance Policy

To watch a video on creating a maintenance policy and associating it with a service profile, see Video: Creating a Global Maintenance Policy and Associating the Policy with a Service Profile.

Step 1 In the Task bar, type **Create Maintenance Policy** and press Enter.
This launches the **Create Maintenance Policy** dialog box.

Step 2 Click **Organization** and select the location in which you want to create the policy.

Step 3 Enter the **Name** and optional **Description**.
The name is case sensitive.

Step 4 Select when to apply the changes that require a reboot.
This can be one of the following:

- **User Acknowledgement—**Configuration changes must be acknowledged by the user, and reboots must be confirmed.
- **Schedule—**Configuration changes are applied depending on the schedule you select. To add a new schedule to the list of values, see Creating or Editing a Schedule, on page 12.
- **Save—**Configuration changes are applied immediately on save and cause a reboot.

Step 5 Choose whether to apply the changes on the next reboot, and ignore the selection in the **Apply Changes On** field.

Step 6 Click **Create**.

Creating or Editing a Schedule

Note Simple schedules, whether recurring or a one time occurrence, do not have the option to require user acknowledgment. If you want to require user acknowledgment, you must choose an advanced schedule.

Step 1 In the Task bar, type **Create Schedule** and press Enter.
This launches the **Create Schedule** dialog box.

Step 2 In **Basic**, enter a **Name** and optional **Description**.

Step 3 Choose whether the schedule should be **Recurring**, **One Time**, or **Advanced**.
If **Advanced**, choose whether to require user acknowledgment.

Step 4 In **Schedule**, complete the following:

a) For **Recurring** schedules, select the start date, frequency, time, and other properties.
b) For **One Time** schedules, select the start date, time, and other properties.

c) For **Advanced** schedules, enter a name for the schedule, choose whether to use a one time or recurring schedule, and select values for the other properties.

Step 5 Click **Create**.

Key Rings

Cisco UCS Central allows creation of key rings as a third party certificate for stronger authentication. HTTPS uses components of the Public Key Infrastructure (PKI) to establish secure communications between two devices.

Each PKI device holds a pair of asymmetric Rivest-Shamir-Adleman (RSA) encryption keys, one kept private and one made public, stored in an internal key ring. A message encrypted with either key can be decrypted with the other key. To send an encrypted message, the sender encrypts the message with the receiver's public key, and the receiver decrypts the message using its own private key. A sender can also prove its ownership of a public key by encrypting (also called 'signing') a known message with its own private key. If a receiver can successfully decrypt the message using the public key in question, the sender's possession of the corresponding private key is proven. Encryption keys can vary in length, with typical lengths from 2048 bits to 4096 bits. In general, a longer key is more secure than a shorter key. Cisco UCS Central provides a default key ring with an initial 2048-bit key pair, and allows you to create additional key rings.

Note If you regenerate the default key ring, logging into Cisco UCS Central after the regeneration might take a few minutes.

The default key ring certificate must be manually regenerated if the cluster name changes or the certificate expires.

Note When you create a key ring and certificate request, Cisco UCS Central generates the certificate request with required key usages set. The Key usages on certificate signed from a CA server should include **SSL Client Authentication**, and **SSL Server Authentication** . If you use Microsoft Windows Enterprise Certification Authority Server as Internal CA, you need to use the **Computer** template to generate the certificate, which will have both of these key usages set. If this template is not available in your setup, you need to use appropriate template which has both **SSL Client Authentication**, and **SSL Server Authentication** key usages set.

Creating a Key Ring

Step 1 On the menu bar, click **System Profile**.
Step 2 Click **Certificates** and complete all the fields.
Step 3 Click **OK**.
Step 4 Click **Save**.

Creating a Trusted Point

Cisco UCS Central allows you to create a trusted point containing the certificate of the root certificate authority (CA) and a subordinate CA in a bundled format. The root CA must contain a primary and self-signed certificate.

Step 1 On the menu bar, click **System Profile**.
Step 2 Click**Trusted Points**.
Step 3 In **Trusted Points**, click the + icon and complete all the fields.
Step 4 Click **OK**.
Step 5 Click **Save**.

Fault and Log Monitoring

Cisco UCS Central allows you to view fault logs, audit logs, sessions and other events.

Note If the screen or widget that you are viewing is not current, click the refresh icon to see the latest data.

System Faults

Cisco UCS Central collects and displays all the Cisco UCS Central system faults on the **Fault Logs** page. To view these system fault logs, click the **Alerts** icon and select **System Faults**. The **Faults Logs** page displays information on the type and severity level of the fault, and allow you to monitor and acknowledge the system faults, and filter the faults that are displayed.

The faults table includes the following information for each fault:

- **Code—**The ID associated with the fault

- **Timestamp—**Date and time at which the fault occurred
- **Type—**Origin of the fault
- **Cause—**Cause of the fault
- **Affected Object—**The component that is affected by this fault
- **Fault Details—**The details of the fault.
- **Severity—**The severity of the fault
- **Action—**Any action required by the fault

To manage the information that is collected, see Configuring UCS Central System Policies, on page 2.

UCS Domain Faults

Cisco UCS Central collects and displays faults from registered Cisco UCS domains in the UCS Domain **Faults Log** page. The faults are displayed by type and severity level. You can click on the fault type to expand and view the exact Cisco UCS domains where the faults have occurred. The UCS domain fault logs are categorized and displayed as follows:

- **Fault Level—**The fault level that triggers the profile. This can be one of the following:
  - **Critical—**Critical problems exist with one or more components. These issues should be researched and fixed immediately.
  - **Major—**Serious problems exist with one or more components. These issues should be researched and fixed immediately.
  - **Minor—**Problems exist with one or more components that might adversely affect the system performance. These issues should be researched and fixed as soon as possible before they become major or critical issues.
  - **Warning—**Potential problems exist with one or more components that might adversely affect the system performance if they are allowed to continue. These issues should be researched and fixed as soon as possible before they get worse.
  - **Healthy—**No fault in any of the components in a domain.
  - **Unknown—**No fault in any of the components in a domain.
- **No Of Domains—**The number of domains where the faults have occurred of each severity level.
- **Domain—**The domain where the faults have occurred. Click a type to see the Cisco UCS domains that have one or more faults of that type and the details of the fault.
- **Critical—**The number of critical faults of the selected type in the Cisco UCS domain.
- **Major—**The number of major faults of the selected type in the Cisco UCS domain.
- **Minor—**The number of minor faults of the selected type in the Cisco UCS domain.
- **Warning—**The number of warning faults of the selected type in the Cisco UCS domain.

This table is displayed only when you select a domain from the **UCS Domain Faults** page.

- **Filter—**Allows you to filter the data in the table.
- **ID—** The unique identifier associated with the fault.
- **Timestamp—**The day and time at which the fault occurred.
- **Type—** Information about where the fault originated.
- **Cause—** A brief description of what caused the fault.
- **Affected Object—**The component that is affected by this issue.
- **Fault Details—**More information about the log message.
- **Severity—**Displays an icon denoting the fault severity. The icon key appears below the table.

Event Logs

Cisco UCS Central collects and displays the events that occurred in the system, such as when a user logs in or when the system encounters an error. When such events occur, the system records the event and displays it in the **Event Logs**. To view these event logs, click the **Alerts** icon from the menu bar, and select **Events**. The event logs record information on the following:

- **ID—**Unique identifier associated with the event that caused the fault
- **Timestamp—**Date and time at which the event occurred
- **Trig. By—**Type of user associated with the event
- **Affected Object—**The component that is affected by the event

Audit Logs

You can view a comprehensive list of configuration changes in Cisco UCS Central in the **Audit Logs**. When you perform configuration changes involving creating, editing or deleting tasks in the Cisco UCS Central GUI or the Cisco UCS Central CLI, Cisco UCS Central generates an audit log. In addition to the information related to configuration, the audit logs record information on the following:

- Resources that were accessed.
- Date and time at which the event occurred.
- Unique identifier associated with the log message.
- The user who triggered an action to generate the audit log. This can be an internal session or an external user who made a modification using the Cisco UCS Central GUI or the Cisco UCS Central CLI.
- The source that triggered the action.
- The component that is affected.

Core Dumps

If an error occurs that causes the system to crash, then a core dump file is created. This core dump file includes information of the state of the system before the error occurred, and the time at which the system crashed. To view the core dump files, click the **Alerts** icon on the menu bar and select **Core Dumps**. In the **Core Dumps** log table you can view the following information:

- **Timestamp—**When the core dump file was created.
- **Name—**The full name of the core dump file.
- **Description—**The type of core dump file.

Active Sessions

You can view active sessions for remote and local users in Cisco UCS Central and choose to terminate those sessions from the server. To view the active sessions, click the **Alerts** icon on the menu bar and select **Sessions**. In the **Active Sessions** log table you can view the following information:

- **ID—**The type of terminal from which the user logged in.
- **Timestamp—**Date and time at which the user logged in.
- **User—**The user name.
- **Type—**The type of terminal from which the user logged in.
- **Host—**The IP address from which the user logged in.
- **Status—**Whether the session is currently active.
- **Actions—**Click **Terminate** to end the selected session.

Internal Services

Internal service logs provide information on various providers and the version of the Cisco UCS Central associated with the provider. To view the internal services, click the **Alerts** icon on the menu bar and select **Sessions**.

In the **Services** section of the **Internal Services** page, you can view the following information:

- **Name—**The type of the provider.
- **Last Poll—**Day and time on which Cisco UCS Central last polled the provider.
- **IP Address—**The IP address associated with the provider.
- **Version—**The version of Cisco UCS Central associated with the provider.
- **Status—**The operational state of the provider.

In the **Clean Up** section of the **Internal Services** page, you can view the following information:

- **Domain—**The domain name.

- **Last Poll—**Day and time on which Cisco UCS Central last polled the provider.
- **Lost Visibility—**When Cisco UCS Central lost visibility to the provider.
- **Clean Up—**Click **Clean Up** to remove all references of this Cisco UCS domain from Cisco UCS Central.

Note The domain must be re-registered with Cisco UCS Central before it can be managed again by Cisco UCS Central.

Enabling Tomcat Logging

SUMMARY STEPS

1. UCSC # **scope monitoring**
2. UCSC /monitoring # **scope sysdebug**
3. UCSC /monitoring/sysdebug # **scope mgmt-logging**
4. UCSC /monitoring/sysdebug/mgmt-logging # **set module tomcat_config** [**crit** | **debug0** | **debug1** | **debug2** | **debug3** | **debug4** | **info** | **major** | **minor** | **warn**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCSC # **scope monitoring**	Enters monitoring mode.
Step 2	UCSC /monitoring # **scope sysdebug**	Enters sysdebug mode.
Step 3	UCSC /monitoring/sysdebug # **scope mgmt-logging**	Enters management logging mode.
Step 4	UCSC /monitoring/sysdebug/mgmt-logging # **set module tomcat_config** [**crit** | **debug0** | **debug1** | **debug2** | **debug3** | **debug4** | **info** | **major** | **minor** | **warn**]	Sets the logging level.

The following example shows how to set tomcat logging to level debug 4.

```
UCSC # scope monitoring
UCSC /monitoring # scope sysdebug
UCSC /monitoring/sysdebug # scope mgmt-logging
UCSC /monitoring/sysdebug/mgmt-logging # set module tomcat_config debug4
UCSC /monitoring/sysdebug/mgmt-logging #
```

API Communication Reports

Cisco UCS Central, 1.4 enables you to generate reports on active API communication between the GUI and back-end from the Cisco UCS Central GUI. You can collect these communications for use in third party automation. You can start and stop collecting this report at any time during an active communication.

- After you stop logging the session, the report is available for you as text file from the GUI. If you want to use the file at a later time, make sure to save the file in your local desktop.
- If you log out or your sessions expires while recording is in progress, the text file is not generated.

Generating API Communication Reports

Step 1 On the menu bar, click **Operations** icon and select **Start Logging Session**.
Systems starts logging the active API communication between the Cisco UCS Central GUI and the back-end.

Step 2 On the menu bar, click **Operations** icon and select **Stop Logging Session**.
A pop-up dialog box displays the option to Open or Save the API report text file.

Step 3 Select your choice and click **OK** to open or save the file.