System Management

This chapter includes the following sections:

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 2.
- 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 3.
- 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 4.

Step 3 Complete the fields as required for each section.

Step 4 Click **Save**.

Related Topics

Managing a UCS Central Fault Policy, on page 2
Managing UCS Central Syslog, on page 3
Managing UCS Central Core Dump Export, on page 4

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 1
Managing UCS Central Syslog, on page 3
Managing UCS Central Core Dump Export, on page 4

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 1
Managing a UCS Central Fault Policy, on page 2
Managing UCS Central Core Dump Export, on page 4

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 1
Managing a UCS Central Fault Policy, on page 2
Managing UCS Central Syslog, on page 3

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 6
Managing the UCS Central Management Node, on page 5
Managing the UCS Central DNS Servers, on page 6

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 5
Managing the UCS Central NTP Servers, on page 6
Managing the UCS Central DNS Servers, on page 6

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 5
Managing the UCS Central Management Node, on page 5
Managing the UCS Central DNS Servers, on page 6

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 5
Managing the UCS Central NTP Servers, on page 6
Managing the UCS Central Management Node, on page 5

Managing Domain Group System Policies

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

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

Step 3 In **Fault**, complete the necessary fields.
For more information, see Managing a UCS Central Fault Policy, on page 2.

Step 4 In **Syslog**, complete the necessary fields.
For more information, see Managing UCS Central Syslog, on page 3.

Step 5 In **Core Dump**, complete the necessary fields.
For more information, see Managing UCS Central Core Dump Export, on page 4.

Step 6 In **Interfaces**, choose whether to enable **Interface Monitoring Policy**.

Step 7 If you select **Enabled**, complete the interface monitoring information as required.

Step 8 In **Equipment**, select the **Power Redundancy**, the **Power Allocation Method**, and enter an **ID Soaking Interval**.

Step 9 In **System Events**, complete the necessary fields to determine how the system event logs will be collected.

Step 10 Click **Save**.

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**.

Tech Support Files

You can generate and tech support files for Cisco UCS Central and registered Cisco UCS Domains. Collecting remote tech support includes the following:

- **Generate Tech Support**: You can generate tech support files for Cisco UCS Central or each registered UCS domains.

- **Download tech support files**: Download the created tech support file to view information.

Note You can download the tech support file only from the Cisco UCS Central GUI.

Generating Tech Support File

Step 1 On the menu bar, click **Operation** icon, and select **Tech Support**.

Step 2 Under **Domains** select **UCS Central** or the domain for which you want to generate tech support files for. This displays any available tech support files and the generate menu option.

Step 3 Click flash icon to **Generate Tech Support** files.

Step 4 In the pop-up confirmation dialog box, click **Yes**.

Step 5 The list page displays tech support file collection status when the collection is in progress. When the process is complete, displays the collected time, file name and availability status.

Downloading a Tech Support File

Step 1 On the menu bar, click **Operation** icon, and select **Tech Support**.

Step 2 Under **Domains** select **UCS Central** or the domain for which you want to generate tech support files for.

Step 3 The right pane displays the list of available tech support files for the selected system.

Step 4 Click to select the file you want to download.

Step 5 Click **Download** icon on the menu bar.

Step 6 In the download dialog box, click **Save** to save the tech support file in your local download folder.

Monitoring System Faults and Logs

Pending Activities

If you configure deferred deployment in a Cisco UCS domains, Cisco UCS Central enables you to view all pending activities. You can view all the activities that are waiting for user acknowledgment and those that have been scheduled.

If a Cisco UCS domain has pending activities, the Cisco UCS Central GUI notifies users with admin privileges when they log in.

Cisco UCS Central displays information about all pending activities, including the following:

- Name of the service profile to be deployed and associated with a server
- Server affected by the deployment
- Disruption caused by the deployment
- Change performed by the deployment
- Whether an activity is acknowledged.

You can also acknowledge the activities.

You cannot specify the maintenance window in which a specific pending activity is applied to the server. The maintenance window depends on the number of pending activities and on the maintenance policy assigned to the service profile. However, any user with admin privileges can manually initiate a pending activity and reboot the server immediately, whether an activity is waiting for an user acknowledgment or for a maintenance window.

To view the pending activities on Cisco UCS Central GUI, click the **Alerts** icon from the menu bar.

Important A pending activity is not displayed in the log, if the activity is caused by a local service profile using a local maintenance policy with a local scheduler. Such pending activities must be acknowledged from Cisco UCS Manager .

Viewing and Acknowledging Pending Activities

Step 1 On the menu bar, click the **Alerts** icon.

Step 2 Select **Pending Activities**.

Step 3 In **Pending Activities**, note the activities that are pending.
You can use the checkboxes in the **Filters** area to narrow down the activities.

Step 4 Click **Acknowledge** to acknowledge a pending activity.

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 1.

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.