Managing System Administration Settings

This chapter contains the following sections:

Setting up the Outgoing Mail Server

All outgoing emails from Cisco UCS Director require an SMTP server.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **Mail Setup**.

Step 3 On the **Mail Setup** screen, complete the following fields:

Name	Description
Outgoing Email Server (SMTP) field	The outgoing SMTP server address.
Outgoing SMTP Port field	The outgoing SMTP server port number.
Outgoing SMTP User field	The user ID.
Outgoing SMTP Password field	The user password.
Outgoing Email Sender Email Address field	The sender's email address
Server IP address field	The IP address or DNS name of the Cisco UCS Director virtual appliance. This field is used to create proper links in emails for user workflow actions.
Send Test Email check box	Check this check box to test the current email settings.

Step 4 Click **Save**.

Working with Email Templates

Cisco UCS Director has a notification mechanism that enables you to configure emails to be sent to an administrator when specific events occur, such as when a VM is provisioned. In addition, if approvals are required for any task, an email notification can be sent to an administrator or to the group administrator.

Note You can specify multiple recipients for an email notification. Use a comma as a separator for multiple email addresses.

Cisco UCS Director provides a set of email templates in the HTML format that cover different scenarios. The following are some of the tasks that you can perform with email templates library:

- Add a new email template

- Edit an existing email template—You can edit the subject and message details, or the formatting and presentation fields of an email template. Do not modify any Java-related information in the template.

- Preview an email template—You can preview the email content and determine if the email template needs modification.

- Set an email template as default—You can set email notifications to be sent based on the default email template.

- Delete an email template—You can delete the templates that you have added. However, you cannot delete a template if it meets one of the following criteria:

  ◦ You added a template and set it as a default template.

  ◦ It is a system-provided template.

Adding an Email Template

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **Email Templates**.

Step 3 Click **Add**.

Step 4 On the **Add Template** screen, complete the following fields:

Name	Description
Email Template Name field	The name of the email template.
Template Description field	The description of the email template.
Template Type drop-down list	Select the type of email template that you are adding. This drop-down list is populated with the system-provided templates.
Subject field	The subject line for the email template.
Reset to Default Subject check box	If you check this check box, the subject line you entered is cleared, and the system-provided subject line is populated in the **Subject** field.
Body field	The HTML code that defines the email template, such as the email content, font size and color, the notification triggers, and so on.

Name	Description
Reset to Default Body check box	If you check this box, the HTML code used in the system-provided email template is populated in the **Script** field. After the HTML code is populated, to retain the changes you made to the code, you must uncheck this box.

Step 5 Click **Submit**.

What to Do Next

Preview the email template to determine if you need to make more changes.

Previewing an Email Template

After you create a new email template in Cisco UCS Director, you can preview the email content to determine if you need to make any additional changes.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **Email Templates**.

Step 3 Expand the folder with the email template type, and click the row with the email template that you want to preview.

Step 4 Click **Preview Template**.

Step 5 On the **Launch Report** screen, click **Submit**.
Note   The preview mode of an email template displays only static information. Dynamic information such as the customer name, or resources, is not displayed.

What to Do Next

If necessary, you can return to the email template to make additional changes.

Setting a Default Email Template

Usually, a system template is set as the default email template. If you have added multiple templates for a specific scenario, you can choose to select one of these templates as a default template. Setting a template as default means that the selected template is used for notification.

Procedure

Step 1	Choose **Administration** > **System**.
Step 2	On the **System** page, click **Email Templates**.
Step 3	Expand the folder with the email template type, and click the row with the email template that you want to set as the default.
Step 4	Click **Set As Default Email Template**.

Configuring System Parameters (Optional)

Configuring System Parameters

You should edit the system parameters only if you need to change the default values.

Procedure

Step 1	Choose **Administration** > **System**.
Step 2	On the **System** page, click **System Parameters**.
Step 3	On the **System** sreen, complete the following fields:

Name	Description
Number of Days to Keep Deleted VMs Data field	The user-defined number of days that the system retains VM data.
Number of Days to Keep Events field	The user-defined number of days that the system retains all events. **Note** Events older than the specified time period are deleted.
Number of Days to Keep Trend Data field	The user-defined number of days that the system retains trend data or historical data of the inventory (such as CPU, storage, and memory usage). **Note** This data is used for reporting.
Number of Days to Keep Metering Data drop-down list	Choose the number of days that the system retains VM metering records. **Note** This data is specific to VMs and their resources.

Name	Description
Download VM Locking Controls from URL field	The URL of the VM locking controls file that is hosted on a server that is accessible from the system that is running Cisco UCS Director. **Note** This file must be in XML format. For more information on creating this VM locking controls file, see Locking VMs in Cisco UCS Director.
Currency drop-down list	Choose the type of currency to use. Available currencies are US, EURO, GBP, KRW, CAD, CHF, CLP, NR, JPY, AUD, NZD, SGD, HKD, MYR, MXN, BRL, AED, DKK, SEK, KWD, CYN, RUB, ZAR, and Other.
Currency field	Enter the currency name (one only). **Note** This field appears when **Other** is chosen as the currency.
Currency Precision drop-down list	Choose the currency precision in decimal points. Available precision is from 0 to 5 decimal points.
Funds Availability Check Interval (mins) drop-down list	Choose a time interval to check the availability of funds.

Step 4   Click **Save**.

Configuring Infrastructure System Parameters (Optional)

You can set parameters for polling the virtual and physical system infrastructure resources.

Procedure

Step 1   Choose **Administration** > **System**.

Step 2   On the **System** page, click **Infrastructure System Parameters**.

Step 3   On the **Infrastructure System Parameters** screen, enter the number of days to keep trend data for the system infrastructure. The default is 30 days.

Step 4   Click **Save**.

Running an Object Search

Use the object search feature to locate a specific report from the following screens in the user interface:

- **Physical**
- **Virtual**
- **Workflows**
- **Custom Tasks**

Procedure

Step 1	Choose **Sitemap**.
Step 2	On the **Sitemap** screen, click **Object Search**.
Step 3	To determine the tabs that the search should run on, choose **Advanced Search**. Any report that contains the searchable objects in the **Physical** and **Virtual** screens are displayed, along with the options to choose **Workflows** and **Custom Tasks**. By default, all these options are selected.
Step 4	Clear the check boxes of the tabs that you do not want the search to include.
Step 5	In the **Search** field, we recommend that you enter 3 characters of the object you want to locate. The search field is case sensitive.
Step 6	Click the **Search** icon or press **Enter** on your keyboard. All reports that match the search criteria are displayed.

Updating the License

You can update the license using the Product Authorization Key (PAK).

Procedure

Step 1	Choose **Administration** > **License**.
Step 2	On the **License** page, click **License Keys**.
Step 3	Click **Update License**. The **Update License** screen is displayed.
Step 4	Click **Select a File** to navigate and to choose the PAK license file.
Step 5	Click **Upload** to upload the PAK license file. **Note** If the license file does not upload, check the check box and copy and paste the license text into the license text field.
Step 6	Click **Submit**.

The license is updated.

Replacing a License

You can use this procedure to replace a license in the system. This action will deactivate all other existing licenses on the systems.

Procedure

Step 1	Choose **Administration** > **License**.
Step 2	On the **License** page, click **License Keys**.
Step 3	Choose **Replace License**.
Step 4	In the **File** field, you can either drag and drop a PAK file or click **Select a File** to browse and select a file.
Step 5	(Optional) Check **Enter License Text** to copy and paste the license text.
Step 6	Click **Submit**. All existing licenses are replaced with the new license.

Verifying License Utilization

The **License Utilization** page shows the licenses in use and details about each license, including license limit, available quantity, status, and remarks. License audits can also be run from this page.

Procedure

Step 1	Choose **Administration** > **License**.
Step 2	On the **License** page, click **License Utilization**.
Step 3	Click the row with the license that you want to verify.
Step 4	(Optional) To run a license audit, click **Run License Audit**.
Step 5	On the **Run License Audit** screen, click **Submit**. This process takes several minutes to run.

Viewing License Utilization History

The number of licensed network and storage controllers, servers, server and desktop VMs, and small and medium pods can be tracked over time to see how network resources are being utilized.

Procedure

Step 1 Choose **Administration** > **License**.

Step 2 On the **License** page, click **License Utilization History**.

The license utilization history is displayed for the following resource categories, with timestamp:

- Network Controllers
- Storage Controllers
- Servers
- Server VMs
- Desktop VMs
- Small pods
- Medium pods

Viewing Resource Usage Data

You can view how resources are being utilized in your environment.

Procedure

Step 1 Choose **Administration** > **License**.

Step 2 On the **License** page, click **Resource Usage Data**.

Following are the available report categories:

- Resource Name—Name of the available resources associated with Cisco UCS Director.
- Resource Count—Quantity of each available resource.

Viewing Deactivated License Information

You can view the list of deactivated licenses from the user interface. You can view the following information on deactivated licenses:

- PAK file name
- File ID
- License Entry
- Licence Value

- Expiry Date

- Deactivated Time

- Name of user who deactivated the license

Procedure

Step 1	Choose **Administration** > **License**.
Step 2	On the **License** page, click **Deactivated Licenses**.
Step 3	Review the information displayed for all the deactivated licenses.

Application Categories

Application categories are an optional configuration that enable you to define the type of workload for a VM. If you do not use application categories, Cisco UCS Director assumes that all VMs provisioned for your users are generic VMs and configures them to handle CPU-intensive workloads. Whether you choose to use the default application categories or to create your own, you can provide your users with a pre-defined set of workloads that match their application needs.

The workload options for application categories include the following:

- CPU intensive

- Network I/O intensive

- Disk I/O intensive

- Memory intensive

- Any combination of the above

After you create your application categories, you can go to the desired cloud account and assign the vDC policies to the application categories. This assignment determines the boundaries of the infrastructure where the application can be provisioned. You can also use application categories to allocate clusters based on the type of application. For example, Cluster 1 is allocated for Web applications and Cluster 2 is allocated for database applications.

When an application category is chosen by a user, Cisco UCS Director uses the vDC assignment to determine which location, within the boundary of the vDC, best meets the application's workload needs. For example, if the user chooses a CPU-intensive application category, Cisco UCS Director provisions the application in the available infrastructure with the least CPU utilization.

Adding Application Categories

By default, Cisco UCS Director provides the following application categories for you to use or edit:

- Discovered VM

- Generic VM

- Web Server

- Application Server

- Database

- App—CPU Intensive

- App—Memory Intensive

- App—Disk Intensive

- App—Network Intensive

- Other App 1

- Other App 2

- Other App 3

Cisco UCS Director allows you to create application categories for multiple virtual data centers at a system level. This capability eliminates the repetitive task of selecting individual virtual data centers and assigning policies for categories.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **Application Categories**.

Step 3 Click **Add**.

Step 4 On the **Add Category** screen, complete the following fields:

Name	Description
Category Label field	A unique name for the category.
Category Code field	Specify a code for the category. You can use this code in the VM or host name templates.
Category Description field	A description of the category.
Category Enabled check box	Check this check box to enable the category. Enabling a category implies that you can select this category during VDC assignment. If you do not check this check box, then this category cannot be used in the system.
Default Smart Allocation Algorithm drop-down list	Choose a default algorithm that must be applied during VM provisioning.

Step 5 Click **Submit**.
The application category is displayed when you click the **Manage Categories** option for a virtual data center.

What to Do Next

After you have created an application category, you can perform the following tasks:

- Edit or clone the application category

- Assign the application category to multiple virtual data centers. For more information, see Managing Application Categories in a Virtual Data Centers.

Customizing the Portal

Organizations can customize the End User Portal. The logo, login page, home page, and so on can be customized for branding and user interface-related changes.

Customizing the Login Page and Background Images

You can change the login page and background images by uploading custom images.

Procedure

Step 1 Choose **Administration** > **User Interface Settings**.

Step 2 On the **User Interface Settings** page, click **Login Page**.

Step 3 Check **Use customizable Login page**.

Step 4 In the **Logo Images** section, click **Add** and complete the following fields:

Field	Description
Image Label field	A name for the image.
Description field	A description for the image that you upload.
Select a file for upload field	Click **Browse** to search and select an image file.
	Important An optimal image is 200 pixels in width and 100 pixels in height and is in the PNG format.
Upload option	Click this option to upload the image.
	This option is enabled only after you have browsed and selected an image.
Submit option	Click **Submit** after the image is uploaded.

Step 5 In the **Background Images** section, choose an item or click **Add** and complete the following fields:

Field	Description
Image Label field	A name for the image.
Description field	A description for the image that you upload.
Select a file for Upload field	Click **Browse** to search and select an image file.
	Important An optimal image is 890 pixels in width, 470 pixels in height, and has 255 pixels of white space. In addition, the image must be in the PNG format.
Upload option	Click this option to upload the image.
	This option is enabled only after you have browsed and selected an image.

Step 6 Click **Submit**.

Customizing the Application Logo

You can customize the application logo on the home page by uploading a custom image.

Procedure

Step 1 Choose **Administration** > **User Interface Settings**.

Step 2 On the **User Interface Settings** page, click **Application Logo**.

Step 3 In the **Images** section, click **Add** to add a new image that is not listed, and complete the following fields:

Field	Description
Image Label field	A name for the image.
Description field	A description for the image that you upload.
Select a file for upload field	Click **Browse** to search and select an image file.
	Important Supported image formats are PNG, JPG, and GIF. An optimal image size is 100 pixels in width and 50 pixels in height.
Upload option	Click this option to upload the image.
	This option is enabled only after you have browsed and selected an image.

Step 4 Click **Submit**.

Customizing Favicons

You can customize a favorites icon (Favicon) that is displayed in the browser's address bar or next to the page name, if it is bookmarked.

Procedure

Step 1 Choose **Administration** > **User Interface Settings**.

Step 2 On the **User Interface Settings** page, click **Favicon**.

Step 3 In the **Images** section, click **Add** to add a new image not listed and complete the following fields:

Field	Description
Image Label field	A name for the image.
Description field	A description for the image that you upload.
Select a file for upload field	Click **Browse** to search and select an image file. **Important** Supported image format is PNG. An optimal image size is 16x16 pixels.
Upload option	Click this option to upload the image. This option is enabled only after you have browsed and selected an image.

Step 4 Click **Submit**.

Customizing Application Header

You can customize the End User Portal labels, next to the customer logo, by modifying existing labels.

Procedure

Step 1 Choose **Administration** > **User Interface Settings**.

Step 2 On the **User Interface Settings** page, click **Application Header**.

Step 3 Complete the following fields:

Name	Description
Hide Entire Header check box	Check to hide the header section. If checked, the header that contains the logo image, application name, and links, such as **Logout**, are hidden.
Product Name field	The product name that must be displayed in the header.
Product Name 2nd Line field	The second title of the product.
Enable About Dialog check box	Check to enable the **About** link in the header. Uncheck to disable the **About** link in the header.
Administrator Portal	
Custom Link 1 Label field	The custom link label 1 for the administrator portal.
Custom Link 1 URL field	The custom link URL 1 for the administrator portal.
Custom Link 2 Label field	The custom link label 2 for the administrator portal.
Custom Link 2 URL field	The custom link URL 2 for the administrator portal.
End User Portal	
Custom Link 1 Label field	The custom link label 1 for the End User Portal.
Custom Link 1 URL field	The custom link URL 1 for the End User Portal
Custom Link 2 Label field	The custom link label 2 for the End User Portal.
Custom Link 2 URL field	The custom link URL 2 for the End User Portal.

Step 4   Click **Save**.

Customizing Date Display

Numerous data display formats are supported.

Procedure

Step 1 Choose **Administration** > **User Interface Settings**.

Step 2 On the **User Interface Settings** page, click **Date Display**.

Step 3 Edit the date format.

Step 4 If required, check **Hide Timezone** to hide the time zone display from the user interface.

Step 5 Click **Save**.

Customizing the Color Theme

Procedure

Step 1 Choose **Administration** > **User Interface Settings**.

Step 2 On the **User Interface Settings** page, click **Color Theme**.

Step 3 From the drop-down list, choose from the available theme styles.

Step 4 Click **Save**.

Customizing Logout Redirect

Procedure

Step 1 Choose **Administration** > **User Interface Settings**.

Step 2 On the **User Interface Settings** page, click **Logout Redirect**.

Step 3 In the **Logout Redirect** field, enter the URL.

Step 4 Click **Save**.

Customizing Reports

Report customization enables you to make a custom label or hide the available reports.

Note You cannot customize or hide reports for users and groups. You can customize the report table on all other pages. You can customize only those reports that are identified as **Tabular with actions**.

Procedure

Step 1	Choose **Administration** > **User Interface Settings**.
Step 2	On the **User Interface Settings** page, click **Reports Customization**.
Step 3	Click the row with the report that you want to customize.
Step 4	Click **Edit**.
Step 5	On the **Customize Report** screen, complete the following fields:

Name	Description
Hide Report check box	Check to hide the report. Uncheck to show the report.
New Label field	A new label for the report, if required.

Step 6	Click **Save**.

Enabling Advanced Controls

Procedure

Step 1	Choose **Administration** > **System**.
Step 2	On the **System** page, click **Advanced Controls**.
Step 3	Check the required fields:

Name	Description
Performance Monitoring check box	Check to enable virtual infrastructure monitoring, physical infrastructure monitoring, and external cloud monitoring. Check all additional check boxes under this category, as needed.
Resource Metering check box	Check to enable monitoring of VM metering functions. **Note** If the VM metering function is disabled, chargeback does not work.
Event Monitoring check box	Check to enable virtual and physical infrastructure events.
Auto Support check box	Check to enable automatic support.

Name	Description
Heat Map Report Computing check box	Check to enable generation of heat map reports for the virtual infrastructure.
Automatic Assessment check box	Check to generate reports on virtual assessment.
Adaptive Provisioning Indexing check box	Check to enable and compute the load indices for hosts for various host parameters every 4 hours. These indices are used in adaptive provisioning of the catalogs. A lower index indicates a better chance for the host being chosen for provisioning. This process works according to the computing policy of a specific VDC.
Delete Inactive VMs Based on VDC Policy check box	Check to enable and delete the inactive (powered off) VMs under a VDC after a time that is specified by the administrator. The deletion of these inactive VMs is also based on the VM management policy defined by the administrator. Before an inactive VM is is deleted, an email notification is sent to the user. This property is associated with the **Delete after inactive VM days** field in the VM management policy. **Note** By default, the property box is not checked.
System Task Remoting check box	Check to administratively enable the remote execution.

Step 4 Click **Submit**.

Enabling the Service Provider Feature

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **Service Provider Feature**.

Step 3 Complete the following fields:

Name	Description
Enable Service Provider Feature (Requires System Restart) check box	Check to enable service providers in Cisco UCS Director.

Name	Description
Organization Name (First Level) field	The name of the parent organization for which this feature should be enabled.
Organization Name (Second Level) field	The name of the child organization for which this feature should be enabled.

Step 4   Click **Submit**.

User Menus

You can enable customized menu operations for individual user roles. The menu settings that users can view and access in the application is dependent on the user roles that they have been assigned, and the menu operations that you set for the roles.

Setting User Menus

Procedure

Step 1   Choose **Administration** > **System**.

Step 2   On the **System** page, click **User Roles**.

Step 3   Click the row with the user role for which you want to edit the user menus.

Step 4   Click **Edit**.

Step 5   On the **Edit User Role** screen, click **Next**.

Step 6   On the **Menu Settings** screen, you can view the menu settings for the chosen user role.

Step 7   Check or uncheck the menu check boxes to allow menus for that role, or check **Reset to Defaults**.

Step 8   Click **Submit**.

Setting User Permissions

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **User Roles**.

Step 3 Click the row with the user role for which you want to edit the user permissions.

Step 4 Click **Edit**.

Step 5 On the **Edit User Role** screen, click **Next**.

Step 6 On the **User Permissions** screen, you can view the read and write operations for the chosen user role.

Step 7 Check or uncheck the check boxes to allow read and write operations for an individual role, or check **Reset to Defaults**.

Step 8 Click **Submit**.

System Tasks

The **System Tasks** screen displays all the system tasks that are currently available in Cisco UCS Director. However, this list of system tasks is linked to the type of accounts that you have created in Cisco UCS Director. For example, if you have logged in for the first time, then only a set of general system-related tasks or VMware related tasks are visible on this page. When you add accounts, such as rack accounts or Cisco UCS Manager accounts, system tasks related to these accounts are populated on this page.

Following are the tasks that you can complete from the **System Tasks** screen:

- View the available systems tasks—You can use the **Expand** and **Collapse** options to view all the system tasks that are available on this page. The tasks are categorized according to the accounts available in Cisco UCS Director. For example: Cisco UCS Tasks or NetApp Tasks.

- Disable and enable system tasks—In circumstances when there are multiple processes or tasks running on the appliance, you can choose to disable a system task. If you do so, then until such time that you manually enable it, the system task will not run. This will affect the data populated in other reports. For example, if you disable an inventory collection system task, then reports that require this data may not display accurate data. In this case, you will have to manually run an inventory collection process, or enable the system task.

  For more information, see Disabling or Enabling a System Task, on page 24.

In a single-node setup, where there is only one server, all system tasks run on this server. In a multi-node setup, where there are multiple servers configured, all system tasks run on the primary server by default. However, you can specify system tasks to run on the secondary servers. Following are the recommended steps to perform this task:

1 Ensure that the secondary servers are available in Cisco UCS Director as nodes. If the servers are not available, then you must add the servers as nodes. See Creating a Service Node, on page 22.

2 Create a node pool from the available servers. See Creating a Node Pool, on page 21.

3 Create a system task policy, and associate it with a node policy. See Creating a System Task Policy, on page 21.

4 Associate a node pool with the system task policy. See Assigning a Node Pool to a System Task Policy, on page 22.

5 Select a system task, and associate it with a system-task policy. See Assigning a System Policy to a System Task, on page 23.

Creating a Node Pool

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **Service Nodes**.

Step 3 Click **Service Node Pools**.

Step 4 On the **Service Node Pool** screen, click **Add**.

Step 5 On the **Add Entry to Service Node Pools** screen enter the node pool name in the **Name** field.

Step 6 (Optional) In the **Description** field, enter a description of the node pool name.

Step 7 Click **Submit**. The node pool is created.

Creating a System Task Policy

As an administrator, you can choose to combine a few policies and create a system task policy, in addition to the default system task policy. You can group system tasks into a system task policy to later determine which system tasks are running on which node.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **System Task Policy**.

Step 3 Click **Add**.

Step 4 On the **Add** screen, enter the name that you gave the system task policy in the **Name** field.

Step 5 (Optional) In the **Description** field, enter a description of the system task policy.

Step 6 From the **Node Pool** drop-down list, choose the node pool to which this system task policy belongs.

Step 7 Click **Submit**.
The selected node pool now belongs to the newly created system task policy.

Assigning a Node Pool to a System Task Policy

Procedure

Step 1   Choose **Administration** > **System**.

Step 2   On the **System** page, click **System Task Policy**.

Step 3   Click the row with the system task policy to which you want to assign a node pool.

Step 4   Click **Edit**.

  Note If the default system task policy is used, you can assign service nodes to this policy. See Creating a System Task Policy, on page 21, if you want to configure a policy that is different from the default.

Step 5   From the **Node Pool** drop-down list, choose a node pool that you want to assign to the system task policy.

Step 6   Click **Submit**.
  The selected node pool now belongs to the system task policy.

Creating a Service Node

Procedure

Step 1   Choose **Administration** > **System**.

Step 2   On the **System** page, click **Service Nodes**.

Step 3   Click **Add**.

Step 4   On the **Service Node** screen, complete the following fields:

Name	Description
Node Name field	The name of the service node.
Role field	You cannot edit this field. By default, this field displays **Service** as the role of this node.
Service Node Pool drop-down list	By default, the **default-service-node-pool** is displayed.
DNS Name field	Enter either the DNS name or IP address of the service node. **Note** This field cannot use the Primary Node's IP address. Ensure that a valid Service Node DNS name or IP address is entered.
Description field	The description of the of the service node.
Protocol drop-down list	Choose either http (default) or https.

Name	Description
Port field	The default TCP port for the Hypertext Transfer Protocol (HTTP) 80 is entered by default. Enter a different TCP port if necessary.
UserName field	The **infraUser** user name is entered by default.
	The infraUser is a user account created by default. To find this user account on the menu bar, choose **Administration** > **Users and Groups**.
	Click **Login Users** to find the **infraUser** user account in the **Login Name** column.
	Note The InfraUser user name is not the default administrator user to login to the system. Another user name can be added to this field. This user's API key is used to authenticate with the Service Node.

Step 5 Click **Submit**.

Assigning a System Policy to a System Task

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **System Tasks**.

Step 3 Choose a folder that contains system tasks. Click the folder arrow to expand its tasks.
Note 128 system tasks are available.

Step 4 Choose the task and click **Manage Task**.
The **Manage Task** screen appears.

Step 5 From the **Task Execution** drop-down list, choose **Enable**.

Step 6 From the **System Task Policy** drop-down list, choose a system policy.

Step 7 Click **Submit**.
The system task is assigned to the selected system policy.

Executing System Tasks

Cisco UCS Director includes a few system tasks that cannot be run remotely on a service node. Also, you can assign a system policy remotely from the local host or the primary node.

In addition, you can search and select a specific system task, and run it immediately in the system.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **System Tasks**.

Step 3 Choose a task from the list.

Step 4 Click **Run Now**.
The result of the executed system task is updated in the user interface.

Disabling or Enabling a System Task

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **System Tasks**.

Step 3 Choose a folder that contains one or more system tasks. Click the folder arrow to expand its tasks.
Note 128 system tasks are available.

Step 4 Choose the task and click **Manage Task**.
The **Manage Task** screen appears.

Step 5 To disable a system task, from the **Task Execution** drop-down list, choose **Disable**.

Step 6 To enable a system task, from the **Task Execution** drop-down list, choose **Enable**.

Step 7 Click **Submit**.

Managing Icons in the Cisco UCS Director User Interface

Cisco UCS Director supports customization and management of catalog icons, action-related icons, and status-related icons. Each icon set in the system contains several images that are available by default. You can change the icons that are displayed for either the catalogs, actions or status. You can either upload a new image and set it as the icon, or you can choose a different icon from the set of system-provided icons

☞

Important

- While uploading an icon, ensure that the icon is in either the .SVG format or in the .PNG format. If you are uploading a .SVG image, ensure that the pixel compression is as follows:

    ◦ For action icons— 24px x 24px

    ◦ For table icons—16px x 16px

    ◦ For status icons—16px x 16px

    ◦ For header icons— 20px x 20px (except for the alert icon)

- After you select an icon, you must log out and log in again to the system for the new icon to be visible in the user interface.

Following are the pre-populated icon sets in Cisco UCS Director:

- Standard Catalog Icon Set

- Status Icon Set

- Bare Metal Catalog Icon Set

- Advanced Catalog Icon Set

- Container Catalog Icon Set

- Catalog Folder Icon Set

- Action Icon Set

In addition to modifying an icon in the user interface, you can also revert to the default icon.

Modifying an Icon in the Cisco UCS Director User Interface

Procedure

Step 1 Choose **Administration** > **User Interface Settings**.

Step 2 On the **User Interface Settings** page, click **Icon Management**.

Step 3 Select an icon set category.
It can be one of the following:

- Standard Catalog Icon Set

- Status Icon Set

- Bare Metal Catalog Icon Set

- Advanced Catalog Icon Set

- Container Catalog Icon Set

- Catalog Folder Icon Set

- Action Icon Set

Step 4   Click **Icon Images**.

Step 5   Expand **Icon Images**.

Step 6   Select an icon image from the list of icons.

Step 7   Click edit.

Step 8   In the **Edit Icon Images Entry** page, complete one of the following steps:

    a) Choose an image that currently exists in the system using the **Use Existing icon** drop-down list.

    b) Upload a new image to the system by either dragging the image into the **File** field or by browsing and selecting an image using the **Select a File** option.

        Important   While uploading an icon, ensure that the icon is in either the .SVG format or in the .PNG format. If you are uploading a .SVG image, ensure that the pixel compression is as follows:

            • For action icons— 24px x 24px

            • For table icons—16px x 16px

            • For status icons—16px x 16px

            • For header icons— 20px x 20px (except for the alert icon)

Step 9   Click **Submit**.

What to Do Next

You must log out and log in again to the system for the new icon to be visible in the user interface.

Editing an Icon

Procedure

Step 1   Choose **Administration** > **User Interface Settings**.

Step 2   On the **User Interface Settings** page, click **Icon Management**.

Step 3   Choose the row with the icon category that contains the icon that you want to edit.

Step 4   Click **Icon Images**.

Step 5   On the **Manage Icon Images** screen, choose an icon image to edit.

Step 6   Click **Edit**.

Step 7   On the **Edit Icon Images Entry** screen, edit the **Description**.

Step 8   Choose a replacement file to upload by clicking **Browse** and browsing to an image.

Step 9   Click **Upload**.

Step 10   Once the upload is finished, click **Submit**.

Deleting an Icon

Procedure

Step 1	Choose **Administration** > **User Interface Settings**.
Step 2	On the **User Interface Settings** page, click **Icon Management**.
Step 3	Choose the row with the icon category that contains the icon that you want to delete.
Step 4	Click **Icon Images**.
Step 5	On the **Manage Icon Images** screen, choose an icon image and click **Delete**.
Step 6	Click **Submit**.

Previewing an Icon

Procedure

Step 1	Choose **Administration** > **User Interface Settings**.
Step 2	On the **User Interface Settings** page, click **Icon Management**.
Step 3	Choose the row with the icon category that you want to preview.
Step 4	Click **Icon Images**.
Step 5	On the **Manage Icon Images** screen, choose an icon image to preview.
Step 6	Click the **Information** icon to preview the image.

Tag Library

Tagging is when you assign a label to an object. As an administrator, you can decide to tag objects such as resource groups and user groups, in Cisco UCS Director. You can assign tags to a category such as Compute, Storage, Network, and Virtual. You can also apply a tag to a specific type of account in the selected category. For information on how to apply and remove tags on resource groups, see the *Managing Tags of a Resource Group* section in the *Cisco UCS Director APIC Management Guide*.

Once the tag is created, based on the defined applicability rules, the tags are filtered and displayed in an object report. You can associate the tag to an object such as resource group. To view the resource entities that are associated with a tag, choose the tag and click **View Details**. Alternatively, you can double click the tag.

Note If resource entity is not associated with the tag, the table is empty.

Creating a Tag

You can use the **Create** action on the **Tag Library** screen to create a tag that can be assigned to one or more objects in report page.

Procedure

Step 1 Choose **Policies** > **Tag Library**.

Step 2 Click **Create**.

Step 3 On the **Create Tag** screen, complete the following fields:

Name	Description
Name field	The name for the tag.
Description field	The description of the tag.
Type drop-down list	Choose **INTEGER** or **STRING** as the type of the tag.
Possible Tag Values field	The possible values for the tag.

Step 4 Click **Next**.

Step 5 On the **Applicability Rules** screen, complete the following fields:

Name	Description
Visible to End User field	Checko make the tag visible to end user.

Name	Description
Taggable Entities field	Choose the entities on which the tag need to be applied.
	To add an entity, do the following:
	1 Click the + icon.
	2 From the **Category** drop-down list, choose the category. It can be one of the following:
	• **Virtual_Compute**
	• **Virtual_Storage**
	• **Virtual_Network**
	• **Physical_Compute**
	• **Physical_Storage**
	• **Physical_Network**
	• **Administration**
	3 Choose the taggable entities.
	4 Click **Submit**.
	Note The tags are displayed under the respective category according to the set taggable entities.

Step 6   Click **Submit**.

What to Do Next

After creating a tag, you can edit, clone and delete it by selecting the respective option in the user interface.

Support Information

Cisco UCS Director support provides basic and advanced system information, including the license status, database tables, version, resource usage, logs, and debugging processes for troubleshooting.

The **Support Information** page lets you perform the following actions:

- View system information (Basic)

- View system information (Advanced)

- Show logs

- Download all logs

- Start and stop debug logging

- Start and stop API logging

Viewing System Information

Cisco UCS Director allows you to access system information from the user interface. You can access the following types of system information:

- Basic system information

- Advanced system information

Basic system information includes the following:

- Software version

- Uptime

- Service status

- System license status

- System usage

- Compute accounts status

- Compute server status

- Storage account status

- System catalogs

- Network device status and

- Cloud status

The advanced system information includes the following:

- Basic system information

- Database tables summary

- Product configuration

- Top process information

- Information on processors, memory, disks, log files, network, and login

- System task status

- Cloud inventory

- Monitoring status

Procedure

Step 1	Choose **Administration** > **Support Information**.
Step 2	From the **System Information** drop-down list, choose the type of system information you want to view.
Step 3	Click **Submit**. The **System Information** page opens in a new tab and displays information about the Cisco UCS Director appliance.

Showing Logs

Cisco UCS Director collates the following logs in the system:

- Infra Manager
- Web Context Cloud Manger
- Tomcat Log
- Authenticator Log
- Mail Delivery Log
- Patch Log

Procedure

Step 1	Choose **Administration** > **Support Information**.
Step 2	From the **System Information** drop-down list, choose **Show Log**.
Step 3	From the **Show Log** drop-down list, choose the log file that you want to view.
Step 4	Click **Show Logs**. The log file opens in a new tab or browser window and displays any available information, warning, and error logs.

Downloading Logs

You can download all the log files as a zipped file.

Procedure

Step 1 Choose **Administration** > **Support Information**.

Step 2 From the **System Information** drop-down list, choose **Download All Logs**.

Step 3 Click **Download**.

Starting the Debug Log

Debug logging enables you to record a maximum of 30 minutes debug logging to a log file.

Procedure

Step 1 Choose **Administration** > **Support Information**.

Step 2 From the **System Information** drop-down list, choose **Debug Logging**.

Step 3 Click **Start Debug Logging**.

Step 4 Click **Stop Debug Logging** to stop the recording.
The recording will automatically stop once it reaches the 30 minute limit.

Step 5 Click **Download Debug Logs from** *HH.MM.SS* (time) to download the zipped log file.

Generating API Logs

Procedure

Step 1 Choose **Administration** > **Support Information**.

Step 2 From the **System Information** drop-down list, choose **API Logging**.

Step 3 Click **Start API Logging**.

Step 4 Perform any tests that you want to run.

Step 5 Click **Stop API Logging** to stop the recording.

Step 6 Click **Download API Debug Logs from** *HH.MM.SS* (time) to download the zipped file.
A compressed (zip) file is generated and downloaded on to your desktop. This zipped file contains a text file that lists all the REST APIs that invoked on the appliance, along with the timestamp.

Database Audit Logging

Database audit logging lets the system record information on login events and query events. These events are logged in the `/var/lib/mysql/data/audit.log` file. By default, database audit logging is disabled. To enable database audit logging, use the **dbAuditLog.sh** command. For more information, see Enabling Audit Logging, on page 33.

✎

Note   You can disable database audit logging if the system encounters performance issues due to a heavy audit log output.

Enabling Audit Logging

Procedure

Step 1	Login as root on the Cisco UCS Director appliance directly or by using an SSH client.
Step 2	Run the following commands to stop all services running on the system.

```
[root@localhost infra]# pwd
/opt/infra
[root@localhost infra]# ./stopInfraAll.sh
[root@localhost infra]# ./statusInfra.sh
```

Step 3   Run the following command to enable audit logging.

```
[root@localhost infra]# cd bin
[root@localhost bin]# pwd
/opt/infra/bin
[root@localhost bin]# ./dbAuditLog.sh ON
```

Step 4   Run the following commands to restart the services:

```
[root@localhost infra]# pwd
/opt/infra/bin
[root@localhost infra]#./startInfraAll.sh
```

Step 5   Run the following command to check the status of audit logging.

```
[root@localhost bin]# ./dbAuditLog.sh STATUS
audit-log= ON
```

If you see a message that states that there is an issue with the database startup, you must remove or rename the `audit.log` file and restart the Cisco UCS Director database server.