



Managing System Administration Settings

This chapter contains the following sections:

- [Setting up the Outgoing Mail Server, on page 1](#)
- [Working with Email Templates, on page 2](#)
- [Configuring System Parameters \(Optional\), on page 5](#)
- [Running an Object Search, on page 7](#)
- [Viewing Workflow Tasks in the Workflow Designer, on page 8](#)
- [Working with Licenses in Cisco UCS Director, on page 8](#)
- [Application Categories, on page 15](#)
- [Customizing the Portal, on page 17](#)
- [Customizing Reports, on page 21](#)
- [Enabling Advanced Controls, on page 22](#)
- [Enabling the Service Provider Feature, on page 23](#)
- [User Menus, on page 24](#)
- [Setting User Permissions, on page 24](#)
- [System Tasks, on page 25](#)
- [Managing Icons in the Cisco UCS Director User Interface, on page 32](#)
- [Tag Library , on page 35](#)
- [Support Information, on page 36](#)
- [Database Audit Logging, on page 40](#)
- [Device Connector, on page 40](#)
- [Launching Cisco UCS Director from Cisco Intersight, on page 42](#)
- [Connector Pack Management, on page 43](#)

Setting up the Outgoing Mail Server

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



Note In the case of configuring an Outgoing Email Server with an SMTP FQDN, the DNS IP for the mail server remains cached indefinitely. Consequently, if the IP for the SMTP FQDN changes, UCS-Director fails to send emails as it continues to send them to the original IP address.

Although the returned IP has a TTL (Time to Live), UCS-Director does not utilize it. Instead, it caches the IP indefinitely until UCS-Director is restarted.

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	<p>If you check this box, the HTML code used in the system-provided email template is populated in the Script field.</p> <p>After the HTML code is populated, to retain the changes you made to the code, you must uncheck this box.</p>

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** screen, 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
Number of Days to Keep User-Created Files	Choose the number of days that the system retains user-created files. Note The Clean Up User Created Files task deletes the unused files created while generating reports, uploading files, and exporting content. The task deletes files that are older than the number of days you configure.
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**.

Configuring Proxy Settings

Perform this procedure when you want to configure proxy settings.

Procedure

Step 1 Choose **Administration > System**.

Step 2 On the **System** page, click **Proxy Configuration**.

Step 3 Complete the required fields, including the following, to configure proxy on the system:

Field	Description
Enable Proxy Configuration check box	(Optional) Check this check box to enable proxy and complete the following: <ul style="list-style-type: none"> • Host Name field - Enter a host name for the proxy configuration. • Port field - Enter the port for the proxy configuration.
Enable Proxy Authentication check box	(Optional) Check this check box to enable proxy authentication and complete the following: <ul style="list-style-type: none"> • Proxy User Name field - Enter a proxy user name for the proxy authentication. • Proxy Password field - Enter the password for the proxy user name.

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.
-

Viewing Workflow Tasks in the Workflow Designer

Before you begin

You must have read-only privileges for Orchestration assigned to your administrator user role. For information on creating or modifying user roles, see [Adding a User Role](#).

Procedure

- Step 1** Choose **Orchestration**.
- Step 2** On the **Orchestration** page, click **Workflows**.
- Step 3** Choose a workflow task from the list.
- Step 4** Choose **Workflow Designer**.
- The subsequent screen displays the details of the workflow. All information on this screen is read-only. You cannot edit the workflow tasks.
- Step 5** Double-click on a workflow task in the **Workflow Designer** to review the detailed information.
- Step 6** Review the information on the screen, and click **Close**.
-

Working with Licenses in Cisco UCS Director

Licenses enable you to add or manage resources in your environment. Cisco UCS Director supports the following licenses:

- Evaluation license—Free trial license with an expiry date. This license is also referred to as the default license. It is valid for 90 days.
- Production License—With this license, you can add server, storage and network licenses in your environment.
- ELA license—With this license, you can provided unlimited count of resources. For example, if you add a server license to an ELA license, then you can manage an unlimited number of servers in your environment.

These licenses are also referred as the base license, using which users can access resources such Users, Groups, VDCs, and Catalogs in Cisco UCS Director. In addition to the base licenses, Cisco UCS Director supports the use of subscription licenses. These subscription licenses may or may not include a base license.

The administrator user interface of Cisco UCS Director provides you with a number of options and reports, using which, you can perform several administrative tasks with licenses.

Following are the options that you can use to perform specific tasks:

Option Name	Description	Additional Information Available in
Update License	Use this option to add a new license to your system.	Updating the License, on page 12
Apply Upgrade License	Use this option to upgrade a specific license to get server, storage, network, and VM counts.	Applying Upgrade License, on page 11
Replace License	Use this option to deactivate and delete all existing licenses, including the base license, and replace it with a new license. However, the new license must include a base license. For example: Use the Replace Option if you have a base license currently installed, and have to install a subscription license that includes a base license within it.	Replacing a License, on page 12

Option Name	Description	Additional Information Available in
Migrate License	<p>Use this option to delete all existing system licenses, except the base license, and add a new license. The new license that you want to migrate to must be of the same license type.</p> <p>For example, you can migrate from one production license to another production license. But you cannot migrate from a production license to an Evaluation license.</p> <p>You can also use this option if you have a base license currently installed, and have to install a subscription license that does not include a base license.</p>	Migrating a License, on page 12

Following are some of the reports that you can view to understand license utilization and usage in Cisco UCS Director:

Report Name	Displays Information On	Additional Information in
License Keys	Lists all available license keys in the system. It also lists the license features, the license count and the expiry date.	Viewing License Key Information, on page 14
License Utilization	<p>Lists all the licenses that are in use, available licenses, and the actual license limit of all resources.</p> <p>This screen is populated with results from the License Audit task. This task collects license usage and license limit of all resources and displays it on the License Utilization screen. The License Audit task runs every 4 hours, by default.</p>	Verifying License Utilization, on page 13
License Status	<p>Displays information on license violations, if any.</p> <p>For example, violations such as exceeding license limit for a resource, or the absence of a permanent license in the system are displayed on this screen.</p>	Viewing License Status, on page 14

Report Name	Displays Information On	Additional Information in
License Utilization History	Displays periodic license utilization for Network controllers, storage controllers, servers, server VMs, desktop VMs, small pods and medium pod resources. This screen is populated with results from the System resource Util Snapshot scheduler task that runs every 24 hours.	Viewing License Utilization History, on page 13
Resource Usage Data	Displays the resource usage of different resources in the system, such as users, VDCs, service requests, public and private clouds, and physical servers. Every time you add or delete a resource from the system, this report is updated.	Viewing Resource Usage Data, on page 15
Deactivated Licenses	Displays all the licenses that were deleted when you used the Replace Licenses option. This screen also displays the user who replaced the license, and the time when the license was deactivated.	Viewing Deactivated License Information, on page 14

Applying Upgrade License

Use this option to upgrade a specific license to get server, storage, network, and VM counts. You can convert small pod or medium pod licenses to server, storage, network or VM counts. 1 pod license provides 8 physical servers, 8 storage resources, 8 network resources, 400 VMs and 8 other resources.

Procedure

-
- Step 1** Choose **Administration > License**.
 - Step 2** On the **License** page, click **License Keys**.
 - Step 3** Choose **Apply Upgrade License**.
 - Step 4** Choose an option from the **Select Upgrade Type** drop-down list.
 - Step 5** Specify the number of pods to upgrade.
 - Step 6** Click **Apply**.
-

Migrating a License

Use this procedure to delete all existing licenses, except the base license, and add a new license to the system.

Procedure

- Step 1** Choose **Administration > License**.
 - Step 2** On the **License** page, click **License Keys**.
 - Step 3** Choose **Migrate 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**.
-

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.

Updating the License

You can update the license using the Product Authorization Key (PAK). However, you cannot mix license types in your environment. For example, you cannot use this option to update a permanent license with a subscription license.

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.

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 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.
-

Viewing License Key Information

The **License Keys** screen lists all available license keys in the system. It also lists the license features, the license count and the expiry date.

Procedure

- Step 1** Choose **Administration > License**.
 - Step 2** On the **License** page, click **License Keys**.
 - Step 3** Review the information displayed on the screen.
-

Viewing License Status

The **License Status** page displays information on license violations, if any.

Procedure

- Step 1** Choose **Administration > License**.
- Step 2** On the **License** page, click **License Status**.
- Step 3** Review the information displayed in the screen.
-

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.

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.

Name	Description
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.

Field	Description
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.

Field	Description
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.
Heat Map Report Computing check box	Check to enable generation of heat map reports for the virtual infrastructure.

Name	Description
Automatic Assessment check box	Check to generate reports on virtual assessment.
Adaptive Provisioning Indexing check box	<p>Check to enable and compute the load indices for hosts for various host parameters every 4 hours.</p> <p>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.</p>
Delete Inactive VMs Based on VDC Policy check box	<p>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 deleted, an email notification is sent to the user.</p> <p>This property is associated with the Delete after inactive VM days field in the VM management policy. See Configuring a VM Management Policy.</p> <p>Note By default, the property box is not checked.</p>
System Task Remoting check box	Check to administratively enable the remote execution.
Force User Password Reset check box	<p>Check to make password reset mandatory for new users at first login.</p> <p>A user, whose password is changed by any other user, will be forced to reset the password upon his successive login.</p> <p>Note Force User Password Reset is applicable for Local users only.</p>

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.
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.
- Manage system tasks—You can select a system task on the **System Tasks** screen, and click **Manage Task**. From this **Manage Task** screen, you can perform the following 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 29](#).

- Modify the schedule for the system task—You can modify the schedule type for a system task, or you can configure a custom frequency for the task. For more information, see [Scheduling a System Task, on page 29](#)

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 27](#).
2. Create a node pool from the available servers. See [Creating a Node Pool, on page 26](#).
3. Create a system task policy, and associate it with a node policy. See [Creating a System Task Policy, on page 26](#).

4. Associate a node pool with the system task policy. See [Assigning a Node Pool to a System Task Policy, on page 27](#).
5. Select a system task, and associate it with a system-task policy. See [Assigning a System Policy to a System Task, on page 28](#).

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 26](#), 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.

Name	Description
Description field	The description of the of the service node.
Protocol drop-down list	Choose either http (default) or https.
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	<p>The infraUser user name is entered by default.</p> <p>The infraUser is a user account created by default. To find this user account on the menu bar, choose Administration > Users and Groups.</p> <p>Click Login Users to find the infraUser user account in the Login Name column.</p> <p>Note The InfraUser user name is not the default administrator user to login to the system.</p> <p>Another user name can be added to this field. This user's API key is used to authenticate with the Service Node.</p>

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**.
-

Scheduling a System Task

Procedure

- Step 1** Choose **Administration > System**.
- Step 2** On the **System** page, click **System Tasks**.
- Step 3** Choose a system task and click **Manage Task**.

Step 4 In the **Manage Task** screen, complete the following fields to schedule the system task:

Name	Description
<p>Schedule Type drop-down list</p>	<p>Specify the schedule type for the system task. It can be one of the following options:</p> <ul style="list-style-type: none"> • Fixed Delay—Implies the time period between the completion of one task execution and the initiation of the next task execution. • Fixed Rate—Implies the time period between successive tasks executions. If there is a delay in the execution of one task or if one task takes longer to execute than its scheduled time, it results in delays in subsequent task executions. Systems tasks that are configured with this setting will not run concurrently. These tasks will not run concurrently.
<p>Minutes or Hours or Days</p> <p>Note The field label is Minutes, Hours or Days depending upon the System Task you choose.</p>	<p>Choose a number from the drop-down list.</p> <p>If you chose Fixed Delay as the schedule type, then this number indicates the time gap, in hours, between the completion of one task execution and the initiation of the next task execution.</p> <p>If you chose Fixed Rate, then this number indicates time period, in hours, between successive task executions.</p>
<p>Enable Custom Frequency check box</p>	<p>Check this check box to enable a custom frequency for the system task.</p>
<p>Recurrence Type drop-down list</p>	<p>Specify the recurrence schedule for the system task. It can be one of the following:</p> <ul style="list-style-type: none"> • No End • Only Once
<p>Start Time field</p>	<p>Specify the date and time for the recurrence schedule.</p>

Name	Description
Frequency drop-down list	Choose a frequency for the system task. It can be one of the following: <ul style="list-style-type: none"> • Hourly • Daily • Weekly • Monthly <p>Note This field is displayed only when you select No End in the Recurrence Type drop-down list.</p>
Frequency Interval drop-down list	Choose a frequency interval from the drop-down list. The values in this list vary depending on the frequency you have specified.

Step 5 Click **Submit**.

System Tasks with Fixed Rate Option

The following table lists the system tasks that run only with the **Fixed Rate** option.

Category	System Task Label
Compute	Deleted UCSCentralAccount CleanUp Task
	UCS Daily Historical DataPurge Task
	Deleted UCSAccount CleanUp Task
	UCS Historical Data Aggregator Task
	UCS Monthly Historical DataPurge Task
	UCS Event Record Purge Task
	UCS Event Subscription Task
	UCS Fault Record Purge Task
	UCS Server Transition State Manager
Virtual SAN Ready Node Qualification Task	

Category	System Task Label
Admin	VM Metering Data Aggregator Task
	VM Metering Task
	VM LifeCycle Manager
Virtualization	UsageData Aggregator
	Performance Data Collector

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	Check to make the tag visible to end user.

Name	Description
Taggable Entities field	<p>Choose the entities on which the tag need to be applied.</p> <p>To add an entity, do the following:</p> <ol style="list-style-type: none"> a. Click the + icon. b. From the Category drop-down list, choose the category. It can be one of the following: <ul style="list-style-type: none"> • Virtual_Compute • Virtual_Storage • Virtual_Network • Physical_Compute • Physical_Storage • Physical_Network • Administration c. Choose the taggable entities. d. Click Submit. <p>Note The tags are displayed under the respective category according to the set taggable entities.</p>

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.

Note To view the log details and SQL information in debug mode for reports, log into the Cisco UCS Director using shelladmin or root credentials and do one of the following:

- As a shelladmin user, choose **Tail Inframgr Logs** option and press Enter
 - As a root user, execute **tail -f /opt/infra/inframgr/logfile.txt**.
-

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/mariadb/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 40](#).



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.

Device Connector

The device connector connects Cisco UCS Director to Cisco Intersight, the cloud-hosted server management system. It enables Cisco UCS Director to be managed and monitored through Cisco Intersight.

To register a device with Cisco Intersight in the cloud, you must do the following:

1. Configure the device connector proxy settings to connect Cisco UCS Director with Cisco Intersight.
This is required only if you have proxy configuration enabled.
2. Validate your access to the device from Cisco Intersight using the device serial number and the security code and claim the device.



Note After a system running Cisco UCS Director is claimed in Cisco Intersight, you must refresh the information displayed on the **Device Connector** screen. Choose **Administration > Device Connector** to view the updated information.

Configuring Device Connector

Procedure



- Step 1** Choose **Administration > Device Connector**.
- Step 2** Click **Settings**.
- Step 3** In the **Settings** dialog box, choose **Proxy Configuration**.
- Step 4** For the **HTTPS Proxy** field, move the slider to **Enabled**.
- Step 5** Enter the proxy hostname or IP address in the **Proxy Hostname/IP** field.
- Step 6** Enter the proxy port number in the **Proxy Port** field.
- Step 7** To authenticate access to the proxy server, turn the **Authentication** mode on and enter the **Username** and **Password**.
- Step 8** Click **Ok**.

Based on the connectivity to Cisco Intersight, the **Status** field displays one of the following messages:

- When the connection to Cisco Intersight is successful, the status messages could be one of the following:
 - **Unclaimed**—Implies that the connection is successful but the device is not claimed. You can claim an unclaimed connection through Cisco Intersight.

For information on claiming a device, see the integrated guided walkthrough titled *Learn How to Claim a Device* available within the **Online Help** menu in the Cisco Intersight user interface.
 - **Claimed**—Implies that the connection to Cisco Intersight is successful and you have claimed the device.

Note The header pane of the user interface now includes an icon to indicate the status of the device in Cisco Intersight. This icon is visible only to administrator users and the status change is reflected only when the browser is refreshed or when a new login session is initiated.

Icon	Description
	Indicates that the device is not claimed in Cisco Intersight.
	Indicates that the device is claimed in Cisco Intersight.

- When the connection to Cisco Intersight is unsuccessful, the status messages could be one of the following:
 - **Administratively disabled**—Implies that the administrator has disabled managing the device from Cisco Intersight.
 - **Certification Validation Error**—Implies that an invalid certificate exists on the system.
 - **Not Claimed**—Indicates that the device is registered, but not claimed in Cisco Intersight.
 - **DNS is not configured** or **DNS is mis-configured**.
 - **Unable to resolve DNS name of the service**—Indicates that although DNS is configured, the DNS name of the Cisco Intersight platform cannot be resolved.
 - **NTP is not configured**
 - **Unable to establish a network connection**—Indicates that Cisco UCS Director cannot connect to Cisco Intersight.

If you have enabled HTTP using option 28 from the Shell Admin console, then the status messages displayed on this screen may not be accurate.

Launching Cisco UCS Director from Cisco Intersight

After the device connector is configured and the device is claimed, you can launch the Cisco UCS Director user interface from Cisco Intersight.



Important If any of the Cisco UCS Director services are down, you cannot launch Cisco UCS Director from Cisco Intersight.

A message stating that there is no service is displayed.

Although you can launch Cisco UCS Director from Cisco Intersight, following are some of the restrictions that you need to be aware of:

- You cannot edit a user profile.
- You cannot perform any import and export actions.

- The main menu and the Dashboard are disabled.
- The **Device Connector** tab is not visible.
- You cannot perform any launch actions.
- You cannot upgrade connector packs.
- You cannot generate any summary reports.
- The user name is displayed as Cisco Intersight user when you launch Cisco UCS Director.
- All service requests and audit log details are logged as Admin user.

Procedure

- Step 1** Log into the Cisco Intersight user interface.
- Step 2** Choose **Devices**.
The **Devices** screen appears that displays a list of available Cisco UCS Director systems.
- Step 3** Select a Cisco UCS Director device from the list, and click

You must scroll to the far right of the list of devices to see the option.

Note The IP address displayed for the Cisco UCS Director device in Cisco Intersight is determined by the IP address you entered for the **Server IP address** field while configuring the outgoing mail server for Cisco UCS Director.

If you modify the server IP address after the Device Connector process is up, you must restart the Device Connector process. To do so, login to the Cisco UCS Director device, and run the following commands:

```
/opt/infra/bin/stopdc.sh  
/opt/infra/bin/startdc.sh
```

Refresh the **Devices** screen in Cisco Intersight to view the updated server IP address.

- Step 4** Choose **Launch UCSD**.
Cisco Intersight is connected to the Cisco UCS Director system and the Cisco UCS Director user interface opens in a new tab.
- Note** Users with read-only permissions created in Cisco Intersight cannot perform any actions. These users can only view reports.
-

Connector Pack Management

Connector packs help you perform connector level upgrade in Cisco UCS Director without impacting other connectors. After a system running Cisco UCS Director is claimed in Cisco Intersight, as a system administrator, you can view information on new versions of connector packs that are available for upgrade. The top header pane of the user interface displays a notification indicating that new connector pack versions are available.

You can select and upgrade the connector packs on the system. For more information, see [Upgrading Connector Packs, on page 45](#).

Connector packs help you perform connector level upgrade in Cisco UCS Director without impacting other connectors. As a system administrator, you can view information on new versions of connector packs that are available for upgrade.

Following are the connectors that are available in this release:

- Cisco UCS which includes Cisco UCS Central and Cisco UCS Manager
- ACI APIC
- ACI Multi-Site Controller
- F5 Load Balancer
- Network Devices
- EMC Isilon
- EMC RecoverPoint
- EMC VMAX
- EMC VNX
- EMC VNXe
- EMC VPLEX
- EMC Unity
- EMC XtremIO
- IBM
- NetApp ONTAP
- VCE VisionIO
- Microsoft Hyper-V
- RedHat KVM
- Vmware
- Bare Metal Agent
- Cisco IMC
- Cisco BigData Express
- Cisco HyperFlex

As a system administrator, you can upgrade connector packs from:

- Cisco UCS Director. For more information on upgrading the connector packs using Cisco UCS Director user interface, see [Upgrading Connector Packs, on page 45](#).
- Cisco Intersight user interface in which Cisco UCS Director is claimed. For more information on upgrading the connector packs from Cisco Intersight UI, see [Upgrading Connector Packs on UCS Director Instances](#).

The top header pane of the user interface displays a notification indicating that new connector pack versions are available.



Important Latest versions of these connectors are made available to Cisco UCS Director only through Cisco Intersight. So Cisco UCS Director must be claimed in Cisco Intersight.

Upgrading Connector Packs

As a system administrator, you can upgrade connector packs using the Cisco UCS Director graphical user interface. When new connector pack versions are available, the system notifies you in the following ways:

- Pop-up message when you log in to Cisco UCS Director user interface.

When you log in to the user interface of Cisco UCS Director, and if there are new connector pack versions available for upgrade, a pop-up message prompting you to upgrade these versions is displayed. Click **Yes** to upgrade these connector pack versions immediately or click **No** to upgrade at a later time.



Note This pop-up notification message is displayed once every 3 days. It is not displayed every time you log in to the user interface.

- An alert with a downward facing arrow image and a number in the header pane of the user interface.

This number indicates the number of connector packs that are available for upgrade.

The pop-up message and the alert on the header pane are displayed only when Cisco UCS Director has been claimed in Cisco Intersight. For information on establishing a connection with Cisco Intersight, see [Configuring Device Connector, on page 41](#).



Note You can upgrade system packs (System Update Manager, Base Platform Pack and Connector Pack versions) in a standalone setup and in a multi-node setup. In a multi-node setup, you must upgrade the versions only on the primary node.

Before you begin

- You must have system administrator privileges in Cisco UCS Director.
- Cisco UCS Director has been claimed in Cisco Intersight.
- Cisco UCS Director is successfully connected to Cisco Intersight.
- The latest version of the Base Platform connector pack is installed.

Procedure

Step 1 On the header, click **New Upgrades Available**.

The **Available System Upgrades** screen appears and will display all available connector packs for upgrade along with version information. Upon login, if you clicked **Yes** to the pop-up message, then the very same upgrade screen appears.

Note The **New Upgrades Available** icon is visible on the header only when new versions of the current running connector packs are available for upgrade.

Step 2 Check the check box of a connector pack from the list.
You can check the check boxes of multiple connector packs.

Step 3 Click **Upgrade**.

Step 4 In the **Confirm Upgrade** dialog box, click **Yes**.

After you confirm that the connector version must be upgraded, the validation process is initiated. If the validation process completes successfully, the upgrade process is initiated and the **System Upgrade Status** screen displays the upgrade status. After the upgrade process is successful, the **Logout** option is enabled.

For more information on possible outcomes of the validation and upgrade process, see [Upgrade Process Validation and Failure Scenarios, on page 49](#).

Step 5 Click **Logout**.

While upgrading a base platform pack that includes changes to all infrastructure components, all Cisco UCS Director services are restarted. As a result, after clicking **Logout**, the screen could appear to be unresponsive for a few minutes. After all the services are restarted, and the upgrade process is complete, you can login to Cisco UCS Director .

What to do next

You can view the upgrade reports by choosing **Administration > System > System Updates**. From this screen, you can double-click on a report, and view additional details on the upgrade process. For more information, see [Viewing Connector Pack Upgrade Information, on page 46](#).

Viewing Connector Pack Upgrade Information

Procedure

- Step 1** Choose **Administration > System**.
- Step 2** On the **System** page, click **Connector Pack Upgrades**.
Information such as upgrade request ID, user that initiated the upgrade, upgrade start time and end time, and the upgrade status are displayed.
- Step 3** Select a connector pack and choose **View Details** to view details such as connector pack name, upgraded version, and prior version.
- Step 4** Click **State History** to view the various states of the connector pack upgrade process. For example, upgrade request received, upgrade process initiated or upgrade process completed.
- Step 5** Click **Stages** to view the entire lifecycle of the connector pack upgrade request.
-

Base Platform Pack and System Update Manager

Cisco UCS Director includes the capability to update the following components of the software:

- **Base Platform Pack**—Includes basic infrastructure components such as the user interface, Shell admin console changes, and critical defect fixes.
- **System Update Manager**—Includes the framework that helps you upgrade all connector packs and the base platform pack.
- **Connector Packs**—Includes connector-specific updates and critical defect fixes, which you can upgrade in your environment without affecting other connectors. See [Connector Pack Management, on page 43](#).

Prior to upgrading any of these packs, ensure that the following prerequisites are met:

- You must have system administrator privileges in Cisco UCS Director.
- Cisco UCS Director has been claimed in Cisco Intersight.
- Cisco UCS Director is successfully connected to Cisco Intersight.
- The latest version of the Base Platform connector pack is installed.

When you login to the user interface, the header pane will indicate the number of updates that are available for your system. Clicking that number will display the **Available System Upgrades** screen. This screen displays information on base packs and the connector packs that are available for upgrade. From this screen, you can perform the following actions:

- Upgrade connector packs that you need for your environment.
See [Upgrading Connector Packs, on page 45](#).
- Upgrade the Base Platform pack—Selecting this base pack will also automatically select the System Update Manager Pack, and the connector packs that are available for upgrade.
- Upgrade only the System Update Manager
See [Upgrading the System Update Manager, on page 48](#).
- Upgrade the connector packs, Base Platform pack and System Update Manager together

If you select all three options, the System Update Manager is upgraded first, followed by the connector packs, and then finally the Base Platform pack. After the System Update Manager upgrade is complete, the System Update Manager service is restarted, following which the upgrade process for the connector packs and the Base Platform pack is initiated. If the upgrade process for the connector packs fail, then the versions on the system are reverted to the previously installed versions, and the upgrade of the Base Platform pack is also terminated.

Upgrading Base Platform Pack

Before you begin

- You must have system administrator privileges in Cisco UCS Director.
- Cisco UCS Director has been claimed in Cisco Intersight.
- Cisco UCS Director is successfully connected to Cisco Intersight.

- The latest version of the Base Platform connector pack is installed.

Procedure

Step 1 On the header, click **New Upgrades Available**.

The **Available System Upgrades** screen appears that displays a list of available connector packs for upgrade along with the version information.

Note The **New Upgrades Available** icon is visible on the header only when new versions of the current running connector packs are available for upgrade.

Step 2 Check the **Base Platform** check box.

Checking this check box will also automatically select the System Update Manager and connector packs, if available.

Step 3 Click **Upgrade**.

To complete the upgrade, the required Cisco UCS Director services will restart.

Step 4 In the **Confirm Upgrade** dialog box, click **Yes** to proceed with the upgrade.

After you click **Yes**, the validation process is initiated. If the validation process completes successfully, the upgrade process is initiated and the **System Upgrade Status** screen displays the upgrade status.

For more information on possible outcomes of the validation and upgrade process, see [Upgrade Process Validation and Failure Scenarios, on page 49](#).

Step 5 Review the status messages on the **System Upgrade Status** screen.

Step 6 After the upgrade process completes successfully, click **Logout**.

While upgrading a base platform pack that includes changes to all infrastructure components, all Cisco UCS Director services are restarted. As a result, after clicking Logout, the screen could appear to be unresponsive for a few minutes. After all the services are restarted, and the upgrade process is complete, you can login to Cisco UCS Director.

Step 7 Login to the user interface.

Upgrading the System Update Manager

Before you begin

- You must have system administrator privileges in Cisco UCS Director.
- Cisco UCS Director has been claimed in Cisco Intersight.
- Cisco UCS Director is successfully connected to Cisco Intersight.
- The latest version of the Base Platform connector pack is installed.

Procedure

-
- Step 1** On the header, click **New Upgrades Available**.
- The **Available System Upgrades** screen appears that displays a list of available connector packs for upgrade along with the version information.
- Note** The **New Upgrades Available** icon is visible on the header only when new versions of the current running connector packs are available for upgrade.
- Step 2** Check the **System Update Manager** check box.
- Step 3** Click **Upgrade**.
- To complete the upgrade, the required Cisco UCS Director services will restart.
- Step 4** In the **Confirm Upgrade** dialog box, click **Yes** to proceed with the upgrade.
- After you click **Yes**, the validation process is initiated. If the validation process completes successfully, the upgrade process is initiated and the **System Upgrade Status** screen displays the upgrade status.
- For more information on possible outcomes of the validation and upgrade process, see [Upgrade Process Validation and Failure Scenarios, on page 49](#).
- Step 5** Review the status messages on the **System Upgrade Status** screen.
- Step 6** After the System Update Manager upgrade process completes successfully, click **Logout**.
- After the upgrade process is complete, the System Update Manager service is restarted.
- Step 7** Login to the user interface.
-

Upgrade Process Validation and Failure Scenarios

After you initiate a system pack upgrade, a validation process is initiated in the system. The following table describes the possible outcomes of the validation for system packs:

Scenario	Validation Process Outcome	Information in the User Interface	Recommended Action
No problems with any system pack versions No workflows in progress No users logged into the system	Succeeds	The System Upgrade Validation screen displays the status	None. The upgrade process is initiated.
Problems with one or more system packs	Fails	The System Upgrade Validation screen displays an error message and corrective action.	Review the information and perform the corrective action suggested.

Scenario	Validation Process Outcome	Information in the User Interface	Recommended Action
Other users are logged into the system or Workflows are in progress	Fails	The System Upgrade Validation screen displays an error message and corrective action.	Review the corrective action, and click Force Upgrade to proceed with the upgrade. Note The Force Upgrade option is available only for Base Platform pack and connector packs. It is not displayed for the System Update Manager. The System Upgrade Status screen is displayed with current status for the upgrade request. Users are automatically logged out of the system with a system broadcast message about the upgrade.

After validation process completes successfully, the upgrade process is initiated and the **System Upgrade Status** screen displays the status. On successful completion of the upgrade process, the **Logout** option is enabled on the user interface. The following table describes the possible issues that you could encounter during an upgrade process:

Scenario	Information in the User Interface	Impact to Upgrade Process
System pack upgrade is in progress and other users with administrator privileges logs in to the user interface.	The System Upgrade Status screen is displayed to the user with current status for the upgrade request.	The upgrade process completes successfully.
System pack upgrade is in progress and an end user logs in to the user interface.	The system startup page is displayed to the user.	The upgrade process completes successfully.
You selected multiple packs for upgrade, and the upgrade for one system pack fails.	The System Upgrade Status screen displays the status of the upgrade. The overall upgrade status is indicated as partially completed. The status for each system pack will help you determine the system pack that was not upgraded.	When the upgrade process for any system pack fails, then the version of that system pack is reverted to the previously installed version.

Scenario	Information in the User Interface	Impact to Upgrade Process
You selected the base platform pack for upgrade and you are logged out of the user interface before the System Upgrade Status screen displays the complete workflow of the upgrade process.	If the base platform pack that you selected for upgrade includes an update to the Tomcat service, then the System Upgrade Status screen does not display the complete workflow of the upgrade process. This is because the Tomcat service restarts in the system which results in terminating your session in the user interface. Also, you are automatically directed to the system start-up screen. You can login to the user interface only after all Cisco UCS Director services are restarted.	Although the System Upgrade Status screen does not display the complete workflow, the upgrade process completes successfully.

