Managing Users and Groups

This chapter contains the following sections:

User Roles

Cisco UCS Director supports the following user roles:

- All Policy Admin
- Billing Admin
- Computing Admin
- Group Admin—An end user with the privilege of adding users. This user can use the End User Portal.
- IS Admin
- MSP Admin
- Network Admin
- Operator

- Service End User—This user can only view and use the End User Portal.
- Storage Admin
- System Admin

These user roles are system-defined and available in Cisco UCS Director by default. You can determine if a role is available in the system by default, if the **Default Role** column in the **Users** page is marked with **Yes**.

Note As an administrator in Cisco UCS Director, you can assign users to system-provided user roles or to custom-defined user roles. In addition, at a later point in time, you can view information on the role that a user is assigned to. For more information, see Viewing User Role Information for Users.

As an administrator in the system, you can perform the following tasks with user roles:

- Create a custom user role in the system, and create user accounts with this role or assign the role to existing users.

  When you create a new user role, you can specify if the role is that of an administrator or an end user. For more information on creating a user role, see Adding a User Role, on page 3. For information on creating user accounts for a role, see Adding Users, on page 4.

- Modify existing user roles, including default roles, to change menu settings and read/write permissions for users associated with that role.

  The procedure to modify menu settings and permissions for a role is the same as the procedure to add a user role.

Defining Permissions to Perform VM Management Tasks to Users

Previously, user permissions for VM management tasks could only be created by defining them in an end-user self-service policy. As an administrator in the system, you can now map permissions to perform VM management tasks to any user role. Users that are mapped to the given role can complete the selected VM management related tasks. However, to assign VM management tasks to end users using the end-user self service policy, you must first disable all VM management actions for this user role, and then enable all other management tasks.

For any user in the system, the capability to perform VM management tasks is determined by the following:

- The permissions assigned to the user role that the user is mapped to
- The end user self-service policy that is mapped to the VDC.

If you have upgraded to the current release, then the permissions to perform VM management tasks is retained in the end user self service policy that was created with the previous release version. However, the permissions that you defined or set for the user role after upgrading to the current release, takes precedence.

Note You can provide permissions to perform VM management tasks to other administrators, such as MSP Admin or Group Admin, by defining them in the user role only.

Adding a User Role

You can create any number of user roles in Cisco UCS Director and define the menu settings for the users created with these roles.

Procedure

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

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

Step 3 Click **Add**.

Step 4 In the **Add User Role** screen, complete the required fields, including the following:

Name	Description
User Role field	Name of the user role.
Role Type drop-down list	Choose the type of role that you are adding. It can be one of the following: • **Admin** • **End user**
Description field	The description of the role being added.
Deny Role List	Click **Select** to view a list of user roles in the **Deny Role List** screen. Check the roles that you want to deny for users created with this role and click **Select**. For example, as an administrator, you are creating a new group admin role in the system using the clone feature, and this group admin role must include the capability to create users with privileges higher than the group admin role. However, by default, the Group Admin role does not allow creating users with privilege higher than the group admin. So in this situation, as the administrator, you will need to select the default group admin role in the deny list.

Step 5 Click **Next**.

Step 6 In the **Menu Settings** pane, check the menu options that will be visible to users who are defined in this role.

Step 7 Click **Next**.

Step 8 In the **User Permissions** pane, choose the read or write permissions associated with various available user tasks.

Step 9 Click **Submit**.

What to do next

Create a user account with this role type.

Adding Users

Before you begin

Ensure that you have created a group before you add a user to it.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Users**.

The **Users** page displays the following information for all user accounts currently available in the system:

- Status
- Login name and access level
- Email address
- Date when the user account will be disabled
- Current status of the password, and the date on which the password will expire

Step 3 Click **Add**.

Step 4 On the **Add User** screen, complete the required fields, including the following:

Field Name	Description
User Role drop-down list	Choose the role type for the user. **Note** This drop-down list displays all the available user roles in Cisco UCS Director. In addition to the user roles available by default, you can create additional user roles. For more information on creating user roles, see Adding a User Role, on page 3.
User Group drop-down list	Select the group that the user will have access to. You can either select a group already available, or you can add a new group. **Note** This field is visible only when you select Service End-User or Group Admin as the user role.

Field Name	Description
MSP Organization drop-down list	Select the MSP organization that the user will manage. You can either select an organization that is currently available, or you can add a new organization. **Note** This field is visible only when you select **MSP Admin** as the user role.
Login Name field	The login name. You can include special characters such as ( ). & - _ `~ $% ^ {}! ' @
Password field	The password. **Note** If Lightweight Directory Access Protocol (LDAP) authentication is configured for the user, the password is validated only at the LDAP server, and not at the local server.
Confirm Password field	The password is entered again for confirmation.
User Contact Email field	The email address. **Note** The email address is required to notify the group owner about the service request status and to request approval.
First Name field	The first name.
Last Name field	The last name.
Phone field	The phone number of the user.
Address field	The office address of the user.
Set user disable date check box	Check to set the date and time when the user account must be disabled in the system. Disabling a user account means that the user can no longer log in into the system. A week prior to this date, an email message stating that the account will be disabled is sent to the user. This automatic email message is generated and sent by the **PeriodicNotificationToUserTask** system task. On the specified date and time, the user account is disabled automatically. If the user is logged in to the system on the date specified, then the login session is terminated automatically.

Field Name	Description
Locale drop-down list	Choose a language for the system specifically for this user. By default, the language is set to English. When this user logs in, the user interface is displayed in the language you selected. This locale selection applies only to this user.

Step 5 Click **Add**.

What to do next

Click a row with a user and click **Manage Profiles**, to optionally assign multiple roles for that user.

Managing User Types

As the system administrator, you have full privileges to manage Cisco UCS Director, including adding users, viewing users and user permissions, and modifying individual user read/write permissions for different system components.

Most users access the Administrative portal when they log in.

Default User Permissions

Each admin user has a set of permissions to access Cisco UCS Director. The types of user permissions are as follows:

- Read—An admin user with Read permission has the ability to only read a file.
- Write—An admin user with Write permission has the ability to read, write, and modify a file. This permission includes the ability to delete or rename files.
- Read/Write—An admin user with Read/Write permission has the ability to read and write a file.

User Roles and Permissions

The following table shows a list of the permissions that are mapped to each user role:

Permission	All Policy Admin	Billing Admin	Computing Admin	Group Admin	IS Admin	MSP Admin	Network Admin	Operator	Service End User	Storage Admin
Virtual Computing	Read		Read	Read / Write	Read	Write	Read	Read	Read / Write	Read
VM Label	Write		Write	Write	Write	Write	Write	Write	Write	Write

Permission	All Policy Admin	Billing Admin	Computing Admin	Group Admin	IS Admin	MSP Admin	Network Admin	Operator	Service End User	Storage Admin
Assign VM to vDC	Write				Write			Write		
Virtual Storage	Read		Read		Read		Read	Read		Read
Virtual Network	Read		Read		Read		Read	Read		Read
Physical Computing	Read / Write		Read / Write		Read		Read	Read	Read	Read
Physical Storage	Read / Write		Read	Read / Write	Read		Read	Read	Read	Read / Write
Physical Network	Read / Write		Read		Read		Read / Write	Read / Write		Read
Group Service Request	Read / Write	Read	Read	Read / Write	Read	Read / Write	Read	Read / Write	Read / Write	Read
Create Service Request	Write			Write		Write		Write	Write	
Approver Service Request	Read / Write		Read / Write	Read /Write	Read / Write	Read / Write	Read / Write	Read	Read / Write	Read / Write
Budgeting	Read	Read / Write	Read		Read	Read / Write	Read	Read		Read
Resource Accouting	Read	Read	Read	Read	Read	Read	Read	Read	Read	Read
Chargeback	Read	Read	Read	Read	Read	Read	Read	Read	Read	Read
System Admin	Read		Read		Read		Read	Read		Read
Users and Groups	Read		Read		Read		Read	Read		Read
Virtual Accounts	Read		Read		Read		Read	Read		Read
Catalogs	Read		Read	Read	Read	Read	Read	Read	Read	Read

Permission	All Policy Admin	Billing Admin	Computing Admin	Group Admin	IS Admin	MSP Admin	Network Admin	Operator	Service End User	Storage Admin
vDC	Read		Read	Read	Read / Write	Read	Read	Read	Read	Read
Computing Policy	Read / Write		Read / Write		Read		Read	Read		Read
Storage Policy	Read / Write		Read		Read		Read	Read		Read / Write
Network Policy	Read / Write		Read		Read		Read / Write	Read		Read
Deployment Policy	Write		Read		Read / Write		Read	Read		Read
Service Delivery	Read / Write		Read		Read / Write		Read	Read		Read
Resource Limit Report	Read	Read	Read	Read	Read	Read	Read	Read	Read	Read
Group Users	Read		Read	Read / Write	Read	Read / Write	Read	Read		Read
Cloudsense Reports	Read	Read / Write	Read	Read / Write	Read		Read	Read	Read	Read
Cloudsense Assessment Reports	Read	Read / Write	Read				Read			Read
Orchestration	Read / Write		Read / Write		Read / Write		Read / Write			Read / Write
Discovery	Read	Read	Read		Write		Read / Write			Read / Write
Open Automation Modules										
CS Shared Reports				Read / Write		Read			Read	
CS Shared Assessments				Read / Write						

Permission	All Policy Admin	Billing Admin	Computing Admin	Group Admin	IS Admin	MSP Admin	Network Admin	Operator	Service End User	Storage Admin
Remote VM Access										
Mobile Access Settings										
End User Chargeback				Read		Read			Read	
UCSD Cluster										
Resource Groups			Read / Write		Read / Write		Read / Write			Read / Write
Tag Library			Read / Write		Read / Write		Read / Write			Read / Write
Allow Deployability Assessment	True	True	True	True	True	True	True	True	True	True
Write CloupiaScript	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write
Execute CloupiaScript	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write

Permissions for Server Management

In prior releases, to manage physical servers, Cisco UCS Director only provided the following options:

- **Read Physical Computing**
- **Write Physical Computing**

As an administrator, if you enabled the write permission, then users had the capability to manage all Cisco UCS physical servers in the environment. With this release, within the **Write Physical Computing** permission, the following new categories of permissions have been introduced:

- **Physical Server Management**
- **Other Physical Compute Management**

Enabling **Physical Server Management** implies enabling management of Cisco UCS Servers only. This category includes the following actions:

- Power Management (Power On and Power Off)
- Group Management (Assign Group and Unassign Group)
- Inventory Management
- Server Management
- Server Access

If you enable these tasks for users, then those users can view these actions or tasks in the portal. However, for end users, even if you enable these tasks, they can only perform the following tasks on Cisco UCS servers:

- Power on and off servers
- Associate and disassociate groups
- KVM console

Enabling **Other Physical Compute Management** implies enabling management tasks for other UCS servers in the environment. Uses from whom this permission is enabled can perform tasks such as working with service profiles or VLANs.

All Policy Admin

The following table shows a list of operations that an **All Policy** admin can perform:

Operations	**Permissions**	
	Read	**Write**
Virtual Computing	Yes	
VM Label		Yes
Assign VM to vDC		Yes
Virtual Storage	Yes	
Virtual Network	Yes	
Physical Computing	Yes	Yes
Physical Storage	Yes	Yes
Physical Network	Yes	Yes
Group Service Request	Yes	Yes
Create Service Request		Yes
Approver Service Request	Yes	Yes
Budgeting	Yes	
Resource Accounting	Yes	

Operations	Permissions	
Chargeback	Yes	
System Admin	Yes	
Users and Groups	Yes	
Virtual Accounts	Yes	
Catalogs	Yes	
vDC	Yes	
Computing Policy	Yes	Yes
Storage Policy	Yes	Yes
Deployment Policy		Yes
Network Policy	Yes	Yes
Service Delivery	Yes	Yes
Resource Limit Report	Yes	
Group Users	Yes	
Cloudsense Reports	Yes	
Cloudsense Assessment Reports	Yes	
Orchestration	Yes	Yes
Discovery	Yes	
Open Automation Modules		
CS Shared Reports		
CS Shared Assessments		
Remote VM Access		
Mobile Access Settings		
End User Chargeback		
Write Resource Accounting		
UCSD Cluster		
Resource Groups		
Tag Library		

Operations	Permissions	
Allow Deployability Assessment		True

Billing Admin

The following table show a list of operations that a Billing admin can perform:

Operation	Permission	
	Read	**Write**
Virtual Computing		
VM Label		
Assign VM to vDC		
Virtual Storage		
Virtual Network		
Physical Computing		
Physical Storage		
Physical Network		
Group Service Request	Yes	
Approver Service Request		
Budgeting	Yes	Yes
Resource Accounting	Yes	
Chargeback	Yes	
System Admin		
Users and Groups		
Virtual Accounts		
Catalogs		
vDC		
Computing Policy		
Storage Policy		
Deployment Policy		

Operation	Permission	
Network Policy		
Service Delivery		
Resource Limit Report	Yes	
Group Users		
Cloudsense Reports	Yes	Yes
Cloudsense Assessment Reports	Yes	Yes
Orchestration		
Discovery	Yes	
Open Automation Modules		
CS Shared Reports		
CS Shared Assessments		
Remote VM Access		
Mobile Access Settings		
End User Chargeback		
Write Resource Accounting		Yes
UCSD Cluster		
Resource Groups		
Tag Library		
Allow Deployability Assessment		True

Computing Admin

The following table shows a list of operations that a **Computing** admin can perform:

Operation	Permission	
	Read	**Write**
Virtual Computing	Yes	
VM Label		Yes
Assign VM to vDC		

Operation	Permission	
Virtual Storage	Yes	
Virtual Network	Yes	
Physical Computing	Yes	Yes
Physical Storage	Yes	
Physical Network	Yes	
Group Service Request	Yes	
Approver Service Request	Yes	Yes
Budgeting	Yes	
Resource Accounting	Yes	
Chargeback	Yes	
System Admin	Yes	
Users and Groups	Yes	
Virtual Accounts	Yes	
Catalogs	Yes	
vDC	Yes	
Computing Policy	Yes	Yes
Storage Policy	Yes	
Deployment Policy	Yes	
Network Policy	Yes	
Service Delivery	Yes	
Resource Limit Report	Yes	
Group Users	Yes	
Cloudsense Reports	Yes	
Cloudsense Assessment Reports	Yes	
Orchestration	Yes	Yes
Discovery	Yes	

Operation	Permission	
Open Automation Modules		
CS Shared Reports		
CS Shared Assessments		
Remote VM Access		
Mobile Access Settings		
End User Chargeback		
Write Resource Accounting		
UCSD Cluster		
Resource Groups	Yes	Yes
Tag Library	Yes	Yes
Allow Deployability Assessment		True

Group Admin

The following table shows a list of operations that a **Group** admin can perform:

Task	Permission	
	Read	**Write**
Virtual Computing	Yes	Yes
VM Label		Yes
Assign VM to vDC		
Virtual Storage		
Virtual Network		
Physical Computing		
Physical Storage	Yes	Yes
Physical Network		
Group Service Request	Yes	Yes

Task	Permission	
Create Service Request		Yes
Approver Service Request	Yes	Yes
Budgeting		
Resource Accounting	Yes	
Chargeback	Yes	
System Admin		
Users and Groups		
Virtual Accounts		
Catalogs	Yes	
vDC	Yes	
Computing Policy		
Storage Policy		
Deployment Policy		
Network Policy		
Service Delivery		
Resource Limit Report	Yes	
Group Users	Yes	Yes
Cloudsense Reports	Yes	Yes
Cloudsense Assessment Reports		
Orchestration		
Discovery		
Open Automation Modules		
CS Shared Reports	Yes	Yes
CS Shared Assessments		
Remote VM Access		
Mobile Access Settings		
End User Chargeback	Yes	

Task	Permission	
Write Resource Accounting		
UCSD Cluster		
Resource Groups		
Tag Library		
Allow Deployability Assessment		True

IS Admin

The following table shows a list of operations that an **IS** admin can perform:

Task	Permission	
	Read	**Write**
Virtual Computing	Yes	
VM Label		Yes
Assign VM to vDC		Yes
Virtual Storage	Yes	
Virtual Network	Yes	
Physical Computing	Yes	
Physical Storage	Yes	
Physical Network	Yes	
Group Service Request	Yes	
Approver Service Request	Yes	Yes
Budgeting	Yes	
Resource Accounting	Yes	
Chargeback	Yes	
System Admin	Yes	
Users and Groups	Yes	
Virtual Accounts	Yes	
Catalogs	Yes	
vDC	Yes	Yes

Task	Permission	
Computing Policy	Yes	
Storage Policy	Yes	
Deployment Policy	Yes	Yes
Network Policy	Yes	
Service Delivery	Yes	Yes
Resource Limit Report	Yes	
Group Users	Yes	
Cloudsense Reports	Yes	
Cloudsense Assessment Reports	Yes	
Orchestration	Yes	Yes
Discovery		Yes
Open Automation Modules		
CS Shared Reports		
CS Shared Assessments		
Remote VM Access		
Mobile Access Settings		
End User Chargeback		
Write Resource Accounting		
UCSD Cluster		
Resource Groups	Yes	Yes
Tag Library	Yes	Yes
Allow Deployability Assessment		True

Network Admin

The following table shows a list of operations that a **Network** admin can perform:

Task	Permission	
	Read	**Write**

Task	Permission	
Virtual Computing	Yes	
VM Label		Yes
Assign VM to vDC		
Virtual Storage	Yes	
Virtual Network	Yes	
Physical Computing	Yes	
Physical Storage	Yes	
Physical Network	Yes	Yes
Group Service Request	Yes	
Approver Service Request	Yes	Yes
Budgeting	Yes	
Resource Accounting	Yes	
Chargeback	Yes	
System Admin	Yes	
Users and Groups	Yes	
Virtual Accounts	Yes	
Catalogs	Yes	
vDC	Yes	
Computing Policy	Yes	
Storage Policy	Yes	
Deployment Policy	Yes	
Network Policy	Yes	Yes
Service Delivery	Yes	
Resource Limit Report	Yes	
Group Users	Yes	
Cloudsense Reports	Yes	
Cloudsense Assessment Reports	Yes	

Task	Permission	
Orchestration	Yes	Yes
Discovery	Yes	Yes
Open Automation Modules		
CS Shared Reports		
CS Shared Assessments		
Remote VM Access		
Mobile Access Settings		
End User Chargeback		
Write Resource Accounting		
UCSD Cluster		
Resource Groups	Yes	Yes
Tag Library	Yes	Yes
Allow Deployability Assessment		True

Operator

The following table shows a list of operations that an **Operator** can perform:

Task	Permission	
	Read	**Write**
Virtual Computing	Yes	
VM Label		Yes
Assign VM to vDC		Yes
Virtual Storage	Yes	
Virtual Network	Yes	
Physical Computing	Yes	
Physical Storage	Yes	
Physical Network	Yes	
Group Service Request	Yes	Yes
Create Service Request		Yes

Task	Permission	
Approver Service Request	Yes	Yes
Budgeting	Yes	
Resource Accounting	Yes	
Chargeback	Yes	
System Admin	Yes	
Users and Groups	Yes	
Virtual Accounts	Yes	
Catalogs	Yes	
vDC	Yes	
Computing Policy	Yes	
Storage Policy	Yes	
Deployment Policy	Yes	
Network Policy	Yes	
Service Delivery	Yes	
Resource Limit Report	Yes	
Group Users	Yes	
Cloudsense Reports	Yes	
Cloudsense Assessment Reports	Yes	
Orchestration		
Discovery		
Open Automation Modules		
CS Shared Reports		
CS Shared Assessments		
Remote VM Access		
Mobile Access Settings		
End User Chargeback		
Write Resource Accounting		

Task	Permission	
UCSD Cluster		
Resource Groups		
Tag Library		
Allow Deployability Assessment		True

Service End User

The following table shows a list of operations that a **Service End User** can perform:

Task	Permission	
	Read	**Write**
Virtual Computing	Yes	Yes
VM Label		Yes
Assign VM to vDC		
Virtual Storage		
Virtual Network		
Physical Computing	Yes	
Physical Storage	Yes	
Physical Network		
Group Service Request	Yes	Yes
Create Service Request		Yes
Approver Service Request	Yes	Yes
Budgeting		
Resource Accounting	Yes	
Chargeback	Yes	
System Admin		
Users and Groups		
Virtual Accounts		
Catalogs	Yes	
vDC	Yes	

Task	Permission	
Computing Policy		
Storage Policy		
Deployment Policy		
Network Policy		
Service Delivery		
Resource Limit Report	Yes	
Group Users		
Cloudsense Reports	Yes	
Cloudsense Assessment Reports		
Orchestration		
Discovery		
Open Automation Modules		
CS Shared Reports	Yes	
CS Shared Assessments		
Remote VM Access		
Mobile Access Settings		
End User Chargeback	Yes	
Write Resource Accounting		
UCSD Cluster		
Resource Groups		
Tag Library		
Allow Deployability Assessment		True

Storage Admin

The following table shows a list of operations that a **Storage** admin can perform:

Task	Permission	
	Read	**Write**

Task	Permission	
Virtual Computing	Yes	
VM Label		Yes
Assign VM to vDC		
Virtual Storage	Yes	
Virtual Network	Yes	
Physical Computing	Yes	
Physical Storage	Yes	Yes
Physical Network	Yes	
Group Service Request	Yes	
Approver Service Request	Yes	Yes
Budgeting	Yes	
Resource Accounting	Yes	
Chargeback	Yes	
System Admin	Yes	
Users and Groups	Yes	
Virtual Accounts	Yes	
Catalogs	Yes	
vDC	Yes	
Computing Policy	Yes	
Storage Policy	Yes	Yes
Deployment Policy	Yes	
Network Policy	Yes	
Service Delivery	Yes	
Resource Limit Report	Yes	
Group Users	Yes	
Cloudsense Reports	Yes	
Cloudsense Assessment Reports	Yes	

Task	Permission	
Orchestration	Yes	Yes
Discovery	Yes	Yes
Open Automation Modules		
CS Shared Reports		
CS Shared Assessments		
Remote VM Access		
Mobile Access Settings		
End User Chargeback		
Write Resource Accounting		
UCSD Cluster		
Resource Groups	Yes	Yes
Tag Library	Yes	Yes
Allow Deployability Assessment		True

Viewing User Role Information for Users

As an administrator in the system, you can assign users to system-provided user roles or to custom-defined user roles. You can view this information at a later point in time for all users in a group.

Procedure

Step 1 Choose **Organizations** > **Summary**.

Step 2 On the **Summary** page, choose the user group.

Step 3 Click **Users**.

From this page, you can view detailed information on the users that belong to the selected group. The **Access Level** column displays the roles, system-defined or custom-defined roles, that the users are assigned to. Optionally, you can choose **Administration** > **User and Groups** > **Users** to view all user information. If you are a group administrator, then to view this information, choose **Organizations** > **Users**.

If you are a group administrator, then this page displays the password expiry date and time for each user. This information is derived from the Password policy that is configured in the system. This page also graphically represents the password expiry status for each user. The column titled **Password Expiry Status** displays a green icon for passwords that have not yet expired, and a red icon for passwords that have expired.

Reviewing Recent Login History of Users

As an administrator in the system, you can review the login history for all users. The system records the following details for every login attempt:

- Login Name—The user name of the logged in user.
- Remote Address—The IP address of the system or the server that the user has logged in from.
- Client Detail—The browser information.
- Client Type—Information on whether the user logged in to the brower or the REST API.
- Authentication Status—Information on whether the login action resulted in success or failure.
- Comments—The cause for authentication failure.
- Accessed On—The date and time of the login activity for the user.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **All Users Login History**.

Step 3 Review the information displayed on the screen.

Configuring Session Limits for Users

You can configure the number of user interface sessions and REST API requests that users can initiate on the system.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Session Management**.

Step 3 In the **Session Management** screen, complete the required fields, including the following:

Name	Description
Maximum Concurrent Sessions Per User field	The maximum number of concurrent GUI sessions that are supported for each user. Enter a number between 1 and 128. The default value is 16.
Maximum Concurrent REST API Requests Per User field	The maximum number of concurrent REST API requests that are supported for each user. Enter a number between 1 and 256. The default value is 128.

Step 4 Click **Submit**.

What to do next

When users initiate a GUI session or a REST API request to exceed the limit specified on this screen, an error message is displayed in the **System Messages** screen. In this scenario, either users should clear their sessions and API requests, or as an administrator, you can use the Shell utility and clear the sessions and requests for a user. For more information, see *Cisco UCS Director Shell Guide*, Release 6.5.

Managing User Account Status

Cisco UCS Director provides you with the capability to enable and disable users in the system. When you disable a user record, the user cannot log in to the system, and cannot use the APIs. In addition, the disabled user record is no longer present in any of the **User** fields that are displayed while performing administrative actions, such as assigning VMs or port groups. However, the records of all system users, whether enabled or disabled, are listed in the **Users** tab. In this tab, view the **Status** column to see if a user account status is **Disabled** or **Enabled**.

You can disable a user in one of the following ways:

- At account creation, you can set a date for disabling the user. For more information, see Adding Users, on page 4.
- Disable a user from the **Users** page. For more information, see Disabling a User Account in Cisco UCS Director, on page 28.
- Disable all users in an MSP Organization or a Customer Organization. For more information, see Disabling User Accounts within a Group, on page 28.

Note After you disable a user account, you can re-enable the account at a later point.

Unassigning Resources From a User

Cisco UCS Director allows you to unassign resources from a user.

Note You can unassign resources from a user prior to disabling the user account in the system.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Users**.

Step 3 Choose a user from the report, and click **View**.

Step 4 From the **User Details** screen, choose the resources you want to unassign from the user.

You can select multiple resources.

Step 5 Click **Unassign**.

Step 6 In the **Unassign Resource** screen, click **Unassign**.

Step 7 Click **OK**.

What to do next

You can assign this resource to another user in the system.

Disabling a User Account in Cisco UCS Director

Perform this procedure to disable a specific user account in Cisco UCS Director.

Procedure

Step 1 On the menu bar, choose **Administration** > **Users and Groups**.

Step 2 Click the **Users** tab.

Step 3 Choose the user account from the table.

You can choose multiple users.

Step 4 On the toolbar, choose **Disable**.

Step 5 In the **Disable User** dialog box, click **Disable**.

Step 6 Click **OK**.

If the user whose account that you disabled is currently logged in to the system through the graphical user interface or the API, then that user session is terminated immediately. The disabled user cannot log in to the application.

What to do next

You can choose to enable the user's account at a later point in time. To do so, return to the **Users** page, select the user and click **Enable**.

Disabling User Accounts within a Group

Perform this procedure to disable user accounts within an MSP organization or a customer organization.

Procedure

Step 1 On the menu bar, choose **Administration** > **Users and Groups**.

Step 2 Click the **MSP Organizations** tab or the **Customer Organizations** tab.

These tab names are only indicative. If you have enabled the **Service Provider Feature**, you have to specify the names of the organization at the first and second level. The names that you specify are displayed as tabs in the interface.

Step 3 Select a group from the table.

You can select multiple groups.

Step 4 Click **Disable Users**.

Step 5 In the **Disable Users** dialog box, click **Disable Users**.

Step 6 Click **OK**.

What to do next

You can enable all the user accounts in this group by returning to **MSP Organizations** tab or the **Customer Organizations** tab, selecting the group, and clicking **Enable Users**.

MSP Administrator Role

A Managed Service Provider (MSP) organization is a type of customer group in Cisco UCS Director. It can be considered as a parent organization in the system. Within this MSP organization, multiple sub-categories or child organizations can be grouped. For example, a company name such as 'Cisco Systems' would represent an MSP organization. Within this MSP organization, you can create multiple customer groups, such as HR, Finance, and Operations. These groups would be considered as customer groups within an MSP organization.

An administrator is required for each MSP in Cisco UCS Director. This administrator is referred to as the MSP Admin. This administrator manages the MSP organization and all the customer organizations within the MSP organization.

If you are a global administrator in Cisco UCS Director, following is the recommended sequence of steps to create an MSP organization and an MSP administrator:

1. Enable the Service Provider Feature in Cisco UCS Director. For more information, see Enabling the Service Provider Feature.
2. Create the MSP organization. For more information, see Creating an MSP Organization, on page 32.
3. Create the customer groups within the MSP organization. For more information, see Creating a Customer Organization, on page 33.
4. Create a user account with MSP administrator role privileges in Cisco UCS Director. While creating this user account, you can also select the MSP organizations that this user can manage and you can create a new MSP organization. For information on creating a user account with a specific role, see Adding Users, on page 4.

   The role defines the menus and tabs that this user can view in Cisco UCS Director. Typically, an MSP administrator will require the following menus:

   - Organization
   - Policies
   - CloudSense

In addition to creating MSP organizations and MSP administrator roles, you can also brand these organizations with customized logos and application labels. For more information, see Branding Customer Organizations, on page 72.

Note Cisco UCS Director supports branding at the global level, MSP organization level, and customer organization level. However, the branding details visible to a user are limited by certain guidelines. For more information, see Branding for Customer Organizations, on page 70.

If you are an MSP administrator, then the following table lists the tasks that you can perform in Cisco UCS Director. It also lists sections in this guide where you can find procedural information.

Task	Link to the information in the guide
Create customer organizations to manage	Creating a Customer Organization, on page 33
Apply specific branding to customer organizations.	Branding Customer Organizations, on page 72
Create and manage policies to provision VMs	Managing Policies
Use CloudSense Analytics to generate reports	Managing CloudSense Analytics

Managing Groups

Creating a User Group

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **User Groups**.

Step 3 Click **Add**.

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

Field Name	Description
Name field	The name of the group or the customer organization. You can include special characters such as ( ). & - _ `~ $% ^ {}! '@
Description field	The description of the group or the customer organization, if required.
Code field	A shorter name or code name for the group. This name is used in VM and hostname templates.

Field Name	Description
Cost Center field	(Optional) The cost center name or number if required. This name or number represents a cost center that a group is associated with. This name can be used in a VMware System policy for the VM naming convention. For more information about using a cost center for naming conventions, see Managing Policies.
Contact Email field	The email used to notify the group owner about the status of service requests and request approvals if necessary.
First Name field	The contact's first name.
Last Name field	The contact's last name.
Phone field	The contact's phone number.
Address field	The contact's address.
Group Share Policy drop-down list	Choose the group share policy for the users in this group. This drop-down list is populated only when you have created group share policies. For more information on creating this policy, see Creating a Group Share Policy.
Allow Resource Assignment To Users check box	If checked, the users of this group can have resources assigned to them and can own these resources. Also, these users can view resources belonging to the group. However, the resources among these users cannot be shared.

Step 5 Click **Add**.

What to do next

Repeat this procedure if you want to add more groups. For each group that you add, you can edit resource limits, manage tags, and customize the logo and application labels.

Using the Global Dashlet Setup Option

This procedure describes how you can customize the number of dashlets that all end users in all groups can view in the End User Portal. In addition, you can customize the number of dashlets that end users in a specific group can view. For more information on customizing the dashlets for a specific group, see Configuring Dashlets.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Global Dashlet Setup**.

Step 3 In the **Dashlets Report** screen, click **Select**.

Step 4 In the **Dashlet Name** screen, uncheck the check boxes of the dashlets that should not be displayed for all end users of all groups in the system.

Step 5 Click **Select**.

Step 6 In the **Dashlets Report** screen, click **Submit**.

Creating an MSP Organization

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 Click **MSP Organizations**.

These tab names are only indicative. If you have enabled the **Service Provider Feature**, you must specify the names of the organization at the first and second level. The names that you specify are displayed as tabs in the interface.

Step 3 Click **Add**.

Step 4 In the **Add MSP Organizations** screen, complete the required fields, including the following:

Field Name	Description
Name field	The name of the MSP organization. You can include special characters such as ( ). & - _ `~ $% ^ {}! '
Description field	The description of the MSP organization, if necessary.
Code field	A shorter name or code name for the group. This name is used in VM and hostname templates.
Cost Center field	The cost center name or number if required. This name or number represents a cost center that a group is associated with. This name can be used in a VMware System policy for the VM naming convention. For more information about using a cost center for naming conventions, see Managing Policies.
Contact Email field	The email used to notify the MSP administrator about the status of service requests and request approvals, if necessary.
First Name field	The contact's first name.
Last Name field	The contact's last name.
Phone field	The contact's phone number.
Address field	The contact's address.

Step 5 Click **Add**.

What to do next

For each MSP organization that you create, you can edit resource limits, manage tags, and customize the logo and application labels. You can also create customer organizations within each MSP organization.

Creating a Customer Organization

You can follow this procedure to create a customer organization within an MSP organization.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 Click **Customer Organizations**.

This tab name is only indicative. If you have enabled the **Service Provider Feature**, you must specify the names of the organization at the first and second level. Those names are displayed as tabs in the interface. If you have disabled the **Service Provider Feature**, then only the **Customer Organizations** tab is displayed.

Step 3 Click **Add**.

Step 4 In the **Add Group** screen, complete the required fields, including the following:

Field Name	Description
Name field	The name of the group or the customer organization. You can include special characters such as ( ). & - _ `~ $% ^ {}! '
Description field	The description of the group or the customer organization, if necessary.
MSP Group Name field	Select the MSP organization name from the drop-down list. This list includes all the groups that you can currently manage. For example, if you are a global administrator of the system, then this list displays all the organizations that you manage. But, if you are an MSP administrator, then this list displays only the organization that you have administrative privileges for.
Code field	A shorter name or code name for the group. This name is used in VM and hostname templates.
Cost Center field	(Optional) The cost center name or number if required. This name or number represents a cost center that a group is associated with. This name can be used in a VMware System policy for the VM naming convention. For more information about using a cost center for naming conventions, see Managing Policies.
Contact Email field	The email used to notify the group owner about the status of service requests and request approvals, if necessary.
First Name field	The contact's first name.
Last Name field	The contact's last name.

Field Name	Description
Phone field	The contact's phone number.
Address field	The contact's address.
Group Share Policy drop-down list	Choose the group share policy for the users in this group. This drop-down list is populated only when you have created group share policies. For more information on creating this policy, see Creating a Group Share Policy.
Allow Resource Assignment To Users check box	If checked, the users of this group can have resources assigned to them and can own these resources. Also, these users can view resources belonging to the group. However, the resources among these users cannot be shared.

Step 5 Click **Add**.

What to do next

Repeat this procedure to add more customer organizations. For each customer organization that you add, you can edit resource limits, manage tags, and customize the logo and application labels.

Password Policy

The password policy applies to all users and is enforced when you add a user or change the password for all user types. This policy enables the following password constraints:

- Password length
- Whether the password can be the same as the username
- Whether a user can set the current password as a new password
- Whether certain regular expressions are disallowed in a password

Creating a Password Policy

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Password Policy**.

Step 3 In the **Password Policy** screen, complete the required fields, including the following:

Name	Description
Minimum Password Length drop-down list	Choose the minimum number of characters for the password. **Note** The minimum length of a password cannot be lesser than 4 characters.

Name	Description
Maximum Password Length drop-down list	Choose the maximum number of characters for the password. **Note** The maximum length of a password can be up to 127 characters.
Minimum Character Classes drop-down list	Choose the minimum number of character classes, such as uppercase, lowercase, numbers, and special characters.
Disallow Login in Password check box	Check the check box to disallow passwords that are the same as the login ID.
Disallow Previous Password check box	Check the check box to disallow the previous password from being used as the new password.
Previous Passwords Counts drop-down list	Choose the number of previous passwords that must be stored in the system.
Disallow Passwords that match Regular Expression field	The regular expressions (one per line) that are not allowed for passwords. For example,.*abc.* specifies that a given password cannot contain the string “abc”.
Password expiry (in days) field	Specify the number of days for which the password will remain active. By default, the value for this field is set to 180.
Warn Password expiry (in Days) drop-down list	Specify the number of days prior to the password expiration that a warning message is sent to the user.
Grace Period for Password (in Days) drop-down list	Specify the number of days, after password expiration, that a user can use the password to log in to the system.

Step 4 Click **Submit**.

Group Budget Policy

Resources are accounted for by using the Chargeback feature. For resource usage by a group or customer organization, you associate the entity with a budget policy.

You can configure a group or customer organization with a budget watch, and configure a group or customer organization to stay within or exceed the provisioned budget.

Viewing and Editing a Group Budget Policy

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **User Groups**.

Step 3 Choose a group from the list.

Step 4 From the **More Actions** drop-down menu, click **Budget Policy**.

Step 5 In the **Budget Policy** screen, complete the required fields, including the following:

Name	Description
Enable Budget Watch check box	Check the check box to monitor the budget usage for the group. Uncheck the box to ignore all budget entries for this group.
Allow Over Budget check box	Check the check box to allow group members to exceed the provisioned budget. Uncheck the box to reject requests, once the budget is exhausted, until a new budget is added.

Step 6 Click **Save**.

Resource Limits

You can configure resource limits for a group, a customer organization, or a tenant, to manage resource utilization. You can specify limits for the following:

- Virtual resources
- Operating system resources
- Physical resources

Note Configuration of operating system resource and physical resource limits are not supported for public clouds.

Guidelines for Resource Limits with Service Provider Enabled

If you have enabled the Service Provider feature in Cisco UCS Director, keep in mind the following considerations while configuring resource limits:

- The limit set for the parent organization determines the limits that you can set for customer groups and containers within the parent organization.
- If you have not added resource limits to a specific customer group but have specified limits for containers within that group, you must consider the total resource limits before setting a limit for another customer group within the parent organization.

- The total number of resource limits configured for all customer groups and containers within those groups cannot exceed the resource limit set for the parent organization.
- If you do not add resource limits to a specific customer group but do specify resource limits for containers within that group, you must consider the total of all container resource limits before you set a limit for the parent organization.

For example, the parent organization, Tenant 1, includes three customer groups: Group A, Group B, and Group C. If you configure a resource limit of ten for Tenant 1, the cumulative resource limits specified for all customer groups within Tenant 1 must not exceed ten. The cumulative resource limits include resource limits applied to customer groups and containers.

Group A includes containers C1 and C2, and has a resource limit of 4 assigned to the customer group. Group B includes containers C3 and C4, and each of these containers has a resource limit of two. This configuration means that two is the maximum available resource limit you can configure for Group C and all its containers (the resource limit for Tenant 1, minus the total resource limits for Group A, Group, B, and containers C1, C2, C3, and C4).

Guidelines for Resource Limits with Service Provider Disabled

If you have disabled the Service Provider feature, there is only one parent organization. Therefore, if you set a resource limit for the parent organization, the total of the limits specified for all customer groups must not exceed the parent resource limit.

For example, the parent organization includes two customer groups: Group A and Group B. If you set a limit of ten for the parent organization and five for Group A. The resource limit that you set for Group B, must not exceed five (the resource limit for the parent organization minus the resource limit for Group A).

Viewing Resource Limits

Procedure

Step 1 Choose **Organizations** > **Summary**.

Step 2 On the **Summary** page, choose the user group.

Step 3 Click **Resource Limits** to view the current limit, usage, pending SR usage, and status of the resources for the selected group.

Editing Resource Limits

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 If you are editing a resource limit for an organization or a customer group, choose **Customer Organization**, or **MSP Organization**.

Important These tab names are only indicative. If you have enabled the **Service Provider Feature**, you have to specify the names of the organization at the first and second level. The names that you specify are displayed as tabs in the interface.

Step 3 To edit the resource limit for a user group, choose **User Groups**.

Step 4 Choose a group from the table, and click **Edit Resources Limits**. The **Resource Limit** screen appears.

Step 5 In the **Resource Limit** screen, check **Enable Resource Limits** and complete the required fields, including the following:

Field Name	Description
Group field	The group name that you selected.
Enable Resource Limits check box	Check the check box to enable the resource limits or uncheck the check box to disable the resource limits. If checked, the user is provided with the option to set resource limits for a group and all nonzero resource limits are applied.
Maximum Active VM Count field	The maximum number of active VMs.
Maximum Total VM Count field	The total number of VMs.
Maximum Total VDC Count field	The total number of VDCs. While provisioning a VM, if the number of VDCs you specify exceeds the number you specify in this field, then an error message is displayed.
Provisioned vCPUs Limit field	The maximum number of provisioned vCPUs.
Provisioned Memory (GB) Limit field	The provisioned memory limit, in gigabytes.
Provisioned Disk (GB) Limit field	The provisioned limit for disks, in gigabytes.
Reserved CPU (GHz) Limit field	The reserved limit of CPUs, in gigahertz.
Reserved Memory (GB) Limit field	The reserved memory limit, in gigabytes
Maximum Snapshot (GB) Limit field	The maximum limit for snapshots, in gigabytes.
Count CPU and Memory for Inactive VMs check box	Check the box to include the group's inactive VM CPU or memory data in the computation of resource limits. Uncheck the box to exclude inactive VM CPU or memory data from the computation of resource limits.
OS Resource Limits **Note** The configuration of OS resource limits and physical resource limits is not supported for public clouds.	
CentOS field	The maximum number of CentOS (Community Enterprise Operating System) servers.
Windows Server 2003 field	The maximum number of Windows 2003 servers.
Windows Server 2008 field	The maximum number of Windows 2008 servers.

Field Name	Description
Windows Server 2012 field	The maximum number of Windows 2012 servers.
Windows Server 2016 field	The maximum number of Windows 2016 servers.
Windows 7 field	The maximum number of Windows 7 machines.
Windows XP field	The maximum number of Windows XP machines.
Red Hat field	The maximum number of Red Hat machines.
Ubuntu field	The maximum number of Ubuntu machines.
FreeBSD field	The maximum number of FreeBSD machines.
Other Linux field	The maximum number of other Linux OS.
Other field	The maximum number of other OS.
Physical Resource Limits	
Maximum Physical Server Count field	The maximum number of servers.
Maximum Full Width Physical Server Count field	The maximum number of full length physical servers. The number of servers specified in this field, when added with the number of servers specified for the **Maximum Half Width Physical Server Count** field must be less than or equal to the number of servers specified in the **Maximum Physical Server Count** field. **Important** This field is applicable only for Cisco UCS blade servers.
Maximum Half Width Physical Server Count field	The maximum number of half length physical servers. The number of servers specified in this field, when added with the number of servers specified for the **Maximum Full Width Physical Server Count** field must be less than or equal to the number of servers specified in the **Maximum Physical Server Count** field. **Important** This field is applicable only for Cisco UCS blade servers.
Maximum Physical Server Memory (GB) field	The maximum amount of server memory.
Maximum Physical Server CPU Count field	The maximum number of server CPUs.
Maximum vFiler Count field	The maximum number of vFilers.
Maximum Physical Storage Space (GB) field	The maximum amount of storage space.

Step 6 Click **Save**.

Configuring the Administration Profile

Creating the Admin Profile

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Users**.

Step 3 Click **Add**.

Step 4 In the **Add User** screen, complete the required fields, including the following:

Field Name	Description
User Type drop-down list	Choose the user type option as **System Admin**. The system administrator has full privileges.
Login Name field	The login name. The default is admin.
Password field	The admin password.
Confirm Password field	The admin password that is entered again for confirmation.
User Contact Email field	The administrator's email address.
First Name field	The administrator's first name.
Last Name field	The administrator's last name.
Phone field	The administrator's phone number.
Address field	The administrator's address.

Field Name	Description
Set user disable date check box	Check to set the date and time when the user account must be disabled in the system. Disabling a user account means that the user can no longer log in into the system. A week prior to this date, an email message stating that the account will be disabled is sent to the user. This automatic email message is generated and sent by the **PeriodicNotificationToUserTask** system task. On the specified date and time, the user account is disabled automatically. If the user is logged in to the system on the date specified, then the login session is terminated automatically.
Locale drop-down list	Choose a language for the system specifically for this user. By default, the language is set to English. When this user logs in, the user interface is displayed in the language you selected. This locale selection applies only to this user.

Step 5 Click **Add**.

Editing Your Administrative Profile

As an administrator in the system, you can edit your own profile in the system.

Procedure

Step 1 Mouse-over your login name on the top right corner of the screen.

Step 2 Choose **Edit My Profile**.

All information that was specified while creating the account is displayed.

Step 3 In the **Edit My Profile** screen, complete the required fields, including the following:

Name	Description
Language drop-down list	Choose a new language for the user interface
Old Password field	Enter your current password.
New Password field	Enter your new password.
Confirm Password field	Re-enter your new password.
Access Profiles	Choose a new profile as the default profile.

Name	Description
Enable Dashboard check box	Check this check box to view the **Dashboard** screen soon after logging into the system.

Step 4 Click **Show Advanced Settings** and complete the required fields, including the following:

Name	Description
REST API Access Key field	Choose either **Copy Key Value** or **Regenerate Key** option.
Enable Developer Menu check box	Check this check box to enable the Developer menu on the system. You must restart the system for this change to take effect.
System Broadcast Message field	Enter a message that must be broadcast on the system.

Step 5 Click **Save**.

Step 6 Restart the system.

All changes that require a system restart are available in the interface.

Sending a Broadcast Message

As an administrator on the system, you can send a broadcast message to all the users that are currently logged into Cisco UCS Director. While configuring this message, you can either choose to have this message set with or without a timer.

Procedure

Step 1 Move the cursor over your login name on the top right corner of the screen.

Step 2 Choose **Edit My Profile**.

Step 3 Choose **Show Advanced Settings** and complete the required fields, including the following:

Name	Description
System Broadcast Message field	Enter the message that you want to send as a broadcast to all users.
Dismiss Message Automatically check box	Check this check box to dismiss the message automatically after a specific period of time. If you do not check this check box, the user will necessarily have to close the message.
Number of Minutes to Display drop-down list	Choose the number of minutes that the message must be visible to users, after which it automatically closes.

Step 4 Click **Send**.

Changing the Admin Password

Procedure

Step 1 Choose **Administration** > **Users and Groups**.
Step 2 On the **Users and Groups** page, click **Users**.
Step 3 Choose the administrator user account from the list of accounts.
Step 4 From the **More Actions** drop-down menu, click **Change Password.**
Step 5 In the **Change Password** screen, enter a new password for the **admin** user and confirm it.
Step 6 Click **Save**.

Viewing Current Online Users

Procedure

Step 1 Choose **Administration** > **Users and Groups**.
Step 2 Choose **Current Online Users** to view a list of online users. The list displays each user's username, IP address, session start time, last data access, and client.

Viewing Workflow Task Details

Before you begin

You must have read-only privileges for Orchestration assigned to your administrator user role. For information on creating or or modifying user roles, see Adding a User Role, on page 3.

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 **View**.

The subsequent screen displays a textual summary of the entire workflow task and the inputs provided.

Step 5 Review the information and click **Close**.

Managing User Access Profiles

Multi-Role Access Profiles

A user can be assigned to more than one role, which is reflected in the system as a user access profile. For example, a user might log into Cisco UCS Director as a group administrator and as an all-policy administrator, if both types of access are appropriate.

Access profiles also define the resources that can be viewed by a user. With Cisco UCS Director Release 5.4, support for multiple profiles for a single user was introduced. So when you install version 5.4, and if a user account is associated with multiple groups, the system creates multiple profiles for the user account. But if you upgrade the system from a prior version to version 5.4, and if the **LDAPSyncTask** system task is not yet run, then, by default, only one profile is listed for a user account in the system.

When LDAP users are integrated with Cisco UCS Director, if a user belongs to more than one group, then the system creates a profile for each group. But by default, the domain users profile is added for LDAP users.

Note The **Manage Profiles** feature enables you to add, log into, edit, or delete a user access profile.

The **Authentication Type** column in the **Manage Profiles** screen indicates the authentication mechanism specified for the user accounts. It can be Local, LDAP or TACACS.

Creating a User Access Profile

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Users**.

Step 3 Choose a user from the list.

Step 4 From the **More Actions** drop-down menu, click **Manage Profiles**.

Step 5 In the **Manage Profile** screen, click **Add**.

Step 6 In the **Add Entry to Access Profiles** screen, complete the required fields, including the following:

Field Name	Description
Name field	The profile name.
Description field	The description of the profile.
Type drop-down list	Choose the user role type.

Field Name	Description
Customer Organizations drop-down list	Choose the organization to which this user profile applies.
Show Resources From All Other Groups the User Has Access check box	Select this checkbox to specify that the user can view resources from all other groups that they have access to or are a part of.
Shared Groups field	Click **Select** to choose the groups to which the user profile applies. The user will be able to access all the resources associated with the selected groups.
Default Profile check box	Check the check box if this is the default user access profile. Uncheck the check box if it is not the default.

Step 7 Click **Submit**.

What to do next

Create additional user access profiles as needed.

Logging in to a Profile

As a user in the system, if you have multiple profiles for your account, then you can log in to the system with a specific profile.

Procedure

Step 1 In the **Cisco UCS Director login** dialog box, enter your username in the **Username** field, in the format Username: Access Profile Name.

For example, Alex: GrpAdmin

Step 2 In the **Password** field, enter your password.

Step 3 Click **Login**.

Default Profile

The default profile is the first profile that you created in the system. You can change the default to another profile. Using the new default profile, you log in by entering the username and password.

Changing a Default Profile

Procedure

Step 1 In the user interface, click the username displayed on the top right corner.

Step 2 In the drop-down menu, click **Edit My Profile**.

Step 3 In the **Edit My Profile** screen, select the profile that you want to set as a default profile.

Note A profile can also be set as default while it is being added, or being edited.

Authentication and LDAP Integration

As an administrator, you can specify an authentication mechanism for the user accounts in the system. You can configure an authentication preference with a fallback choice for LDAP.

Important Starting with Release 6.6, configuring an LDAP authentication preference using the Verisign Identity Protection authentication service is no longer supported.

Name	Description
Local First, fallback to LDAP	Authentication is done first at the local server (Cisco UCS Director). If the user record is not found in the local server, then the authentication process shifts to the LDAP server.

Configuring Authentication Preferences

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Authentication Preferences**.

Step 3 In the **Authentication Preferences** screen, complete the required field:

Name	Description
Authentication Preferences drop-down list	• **Local First, fallback to LDAP** If you select this option, then you must configure the LDAP servers. For more information, see Configuring LDAP Servers, on page 51.

Step 4 Click **Save.**

LDAP Integration

You can use LDAP integration to synchronize the LDAP server's groups and users with Cisco UCS Director. LDAP authentication enables synchronized users to authenticate with the LDAP server. You can synchronize LDAP users and groups automatically or manually. While adding an LDAP account, you can specify a frequency at which the LDAP account is synchronized automatically with Cisco UCS Director. Optionally, you can manually trigger the LDAP synchronization by using the **LDAPSyncTask** system task.

After you configure an LDAP account and after the synchronization process is run, either manually or automatically, the recently added LDAP information is displayed in Cisco UCS Director. This information is displayed in a tree view that depicts the hierarchical structure of all organizational units (OUs), groups, and users that have been added to the system. You can view this information by choosing **Administration** > **LDAP Integration**. You can select and expand an OU in the left pane to view all the groups within it. If you select a group in this left pane, you can view a list of users that are associated with that group. If an OU has several sub OUs within it, then you can click the **Organization** tab in the right pane to view detailed information. In addition, the **Groups** and **Users** tabs in the right pane display groups and users respectively that are synchronized within the selected OU.

Note Please note that we provide support for a total of 10,000 users and groups. It is not recommended to synchronize a number exceeding this limit.

In addition to running a system task, Cisco UCS Director also provides an additional option for you to synchronize the LDAP directory with the system:

- **Cleanup LDAP Users** system task—This system task determines if the synchronized users in the system are deleted from the LDAP directories or not. If there are user records that have been deleted from the LDAP directories, then after this system task is run, these user accounts are marked as disabled in the system. As an administrator, you can unassign resources of these disabled user accounts. By default, this task is in the enabled state. After the second system restart, this system task is changed to the disabled state. This applies to both, a standalone and multi-node setup.

  In a multi-node setup, this system task runs only on the primary node, even if there is a service node configured.

Important Users that do not belong to a group or to a domain user's group display in LDAP as **Users with No Group**. These users are added under the domain user's group in Cisco UCS Director.

You can add LDAP users with the same name in different LDAP server accounts. The domain name is appended to the login user name to differentiate multiple user records. For example: abc@vxedomain.com. This rule is applicable to user groups as well.

Appending the domain name to the user name to login to the system is only applicable to LDAP users. It does not apply to local users. All local users can login to the system with the user names.

When a single LDAP account is added, and a user logs in by specifying only the user name, Cisco UCS Director first determines if the user is a local user or is an LDAP user. If the user is identified as a local user and as an external LDAP user, then at the login stage, if the user name matches the local user name, then the local user is authenticated into Cisco UCS Director. Alternatively, if the user name matches that of the external user, then the LDAP user is authenticated into Cisco UCS Director.

LDAP Integration Rules and Limitations

Note Recommended version for security PSB is TLS: 1.2 and above.

If you do not want to upgrade and break the existing functionality, you need to update the `service.properties` manually and configure to the older version.The path for the `service.properties` file is **/resources/properties/service.properties**.The supported versions of **ldap.ssl.socket.protocols** for Cisco UCS Director, Release 6.8 are TLSv1.2 and TLSv1.3.

Group Synchronization Rules

- If a chosen LDAP group already exists in Cisco UCS Director and the source is type **Local**, the group is ignored during synchronization.
- If a chosen LDAP group already exists in Cisco UCS Director and the group source is type **External**, the group's description and email attributes are updated in Cisco UCS Director.
- While adding an LDAP server, you can now specify user filters and group filters. When you specify a group filter, all users that belong to the specified group are added to the system. In addition, the following actions are also performed:
  - If the specified group includes sub-groups, then the group, the sub-groups and the users in those sub-groups are added to the system (only applicable when you manually synchronize the LDAP directory).
  - If the user is part of multiple groups, and the other groups do not match the group specified as the group filter, then those additional groups are not added to the system.
- A user can be part of multiple user groups. However, the group that is mentioned first in the list of groups that the user is part of is set as the default primary group for the user. If the user is not part of any group, then the default primary group is set as **Domain Users**.

Note You can view information on all the groups that a user is part of only after the **LDAPSyncTask** system task is run.

- When an LDAP group is synchronized, all users that are in the group are first added to the system. Also, if users in the specified LDAP group are associated with other groups that are in the same OU or in a different OU, then those groups are also retrieved and added to the system.
- The LDAP synchronization process will retrieve the specified LDAP groups for the system, along with nested groups, if any.
- Prior to this release, a user was part of only one group. After an upgrade to the current release, and only after the **LDAPSyncTask** system task is run, the **Manage Profiles** dialog box displays the other groups that the user is part of. This is applicable only when the other groups match the group filters that you specified while configuring the LDAP server.

User Synchronization Rules

- LDAP users that have special characters in their names are now added to Cisco UCS Director.
- While adding an LDAP server, you can now specify user filters and group filters. When you specify a user filter, all the users that match the filter you specified, and the groups that they belong to, are retrieved for the system.
- An LDAP user can have multiple group memberships. When the LDAP user is synchronized with the system, this multiple group membership information is retained. Cisco UCS Director provides you with an option to view this information for every user. For more information, see Viewing Group Membership Information, on page 59. In addition, multiple access profiles are also automatically created for the user.

Note You can view this information only when the groups match the filter you specified while configuring the LDAP server, and when the groups have been assimilated into the system.

- Cisco UCS Director now displays the User Principal Name (UPN) for each user that is added into the system. This is applicable for users that have been added into the system in prior releases. Users can log in to the system using their login name or their user principal name. Logging in using the user principal name along with the profile name is not supported.
- If a chosen LDAP user already exists in Cisco UCS Director and the source type is **External**, then that user is ignored at synchronization. The user's name, description, email, and other attributes are not updated again.
- If a user account is created in two different LDAP directories, then the user details of the LDAP directory that was synchronized first are displayed. The user details from the other LDAP directory are not displayed.
- After multiple LDAP directories are synchronized, the LDAP external users must log in to Cisco UCS Director by specifying the complete domain name along with their user name. For example: vxedomain.com\username. However, this rule does not apply if there is only one LDAP server directory added to Cisco UCS Director.

Note After an LDAP synchronization process, verify that the user is assigned to the correct group.

Managing LDAP Integration

Procedure

Step 1 Choose **Administration** > **LDAP Integration**.

Step 2 Required: Choose an LDAP server and click the following buttons, as needed, to manage LDAP integration:

Name	Description
Search BaseDN button	Enables you to choose a distinguished domain name to search. All users and groups from the chosen organization units are fetched into Cisco UCS Director when the LDAP synchronization process is completed. This action is also considered to be an automatic synchronization process. **Note** You can initiate LDAP server synchronization as a system task. For more information, see Executing the LDAP Synchronization System Task, on page 57.
Request Manual LDAP Sync	Displays a dialog box that enables you to specify either basic or advanced search criteria to fetch LDAP users and groups.

Step 3 (Optional) If you chose **Request Manual LDAP Sync**, complete the following fields:

Name	Description
Manual Search Base check box	Enables search on the manually added organization units. When you check this check box, the manually added OUs are displayed.
Basic Search check box	Enables basic search by organization unit.
Advanced Search check box	Enables advanced search.

Important When you use either of the search options, if users and groups that match the search criteria already exist in Cisco UCS Director, then they are not displayed as part of the search results.

Step 4 For basic search, click **Select** to specify the search base.

Step 5 Choose the search base DN, click **Select**, and continue to Step 9.

Step 6 For advanced search, in the **Advanced Filtering Options** pane add or edit attribute names for **User Filters** and **Group Filters**.

Step 7 Click **Next**.

Step 8 In the **Select Users and Groups** pane, complete the following fields:

Name	Description
LDAP Groups field	The LDAP groups from which the users must be synchronized.
LDAP Users field	The LDAP users that must be synchronized.

Step 9 Click **Submit** to synchronize the LDAP server.

Configuring LDAP Servers

You can configure multiple LDAP servers and accounts in Cisco UCS Director. While adding LDAP accounts, you can specify the following:

- An organization unit (OU) that is part of the search base DN.
- A frequency at which the LDAP account is automatically synchronized with the system.
- A group or user filter to narrow down the results, and specify an LDAP role filter on the groups and users

Soon after an LDAP server account is added, a system task for this account is created automatically, and it immediately begins to synchronize the data. All the users and groups in the LDAP server account are added to the system. By default, all the users from the LDAP account are automatically assigned to the service end-user profile.

Before you begin

You should have set the authentication preferences to the following:

- **Local First, fallback to LDAP**

Procedure

Step 1 Choose **Administration** > **LDAP Integration**.

Step 2 Click **Add**.

Step 3 In the **LDAP Server Configuration** screen, complete the required fields, including the following:

Name	Description
Account Name field	The name of the account. This name must be unique.

Name	Description
Server Type field	The type of LDAP server. It can be one of the following: • OpenLDAP • MSAD - Microsoft Active Directory
Server field	The IP address or the host name of the LDAP server.
Enable SSL check box	Enables a secure connection to the LDAP server.
Port field	The port number. It is automatically set to 636 for SSL, and 389 for non-secure mode.
Domain Name field	The domain name. If you selected **OpenLDAP** as the LDAP Directory Type, then this domain name must match the domain specified with the user name. **Important** You must specify the complete domain name. For example: vxedomain.com.
User Name field	The user name. You can specify the user name in one of the following formats: • <username>@domain.com • Distinguished Name of the user in the following format: **CN=PowerUser,CN=Users,DC=domain,DC=com** If you selected **OpenLDAP** as the LDAP Directory Type, then specify the user names in the following format: **uid=users,ou=People,dc=ucsd,dc=com** where **ou** specified is the one all the other users are placed in the directory hierarchy.
Password field	The user password.

Name	Description
Synchronization Frequency drop-down list	Select the frequency (hours) at which the LDAP server must be synchronized. It can be one of the following: • 1 • 4 • 12 • 24
Enable Manual Search Base check box	Check this check box to manually enter the search base organization units (OU). If you do not check this check box, then the search base organization units (OU) are retrieved from the LDAP server automatically.
Enable TACACS Authentication check box	Check this check box to enable TACACS authentication for user accounts in Cisco Identity Services Engine (Cisco ISE). This option is not displayed if you have not added a Cisco ISE server in Cisco UCS Director.
ISE Server drop-down list	Choose the Cisco ISE server from the list.

Step 4 Click **Next**.

Step 5 If you checked the **Enable Manual Search Base** check box, the **Add Entry to Search Base** screen is displayed. In this screen, enter the organization units (OU) and click **Submit**.

You can enter multiple organization units (OU) from this screen.

a) After the OU is added to the system, click **Next** to configure user and group filters.

Step 6 If you did not check the **Enable Manual Search Base** check box, the **LDAP Search Base** pane is displayed. In this pane, click **Select** to specify LDAP search base entries and click **Select**.

All organization units (OU) that are available in Cisco UCS Director are displayed in this list.

Step 7 Click **Next**.

Step 8 In the **Configure User and Group Filters** pane, complete the following fields:

Name	Description
User Filters	Click the + sign to select specific users that must be synchronized with the system. All groups that the selected users are part of are retrieved and added into the system.

Name	Description
Group Filters	Click the + sign to select groups that must be synchronized with the system. All users that are part of the selected group filters are retrieved and added into the system. However, if the users in the selected group are also part of other groups, then those groups are not retrieved and added to the system unless you select them.
Add Entry to Group Filters dialog box	
Attribute Name drop-down list	Choose either **Group Name** or **User Name**.
Operator drop-down list	Choose the filter to retrieve groups and users. It can be one of the following: • **Equals to** • **Starts with**
Attribute Value field	Specify a keyword or a value that must be included in the search.

Based on the filters, the groups or users are retrieved.

Step 9 Click **Next**.

Step 10 In the **LDAP User Role Filter** pane, click the **(+)** sign to add a user role filter.

Step 11 In the **Add Entry to User Role Filters** dialog box, complete the following fields:

Name	Description
Attribute Name field	The name of the attribute. It can be **Group Name**.
Operator drop-down list	It can be one of the following: • **Equal to** • **Starts with**
Attribute Value field	Specify a value in this field. All users that match the values of the **Operator** field and the **Attribute Value** field are assigned to the user role you select in the **Map User Role** drop-down list.

Name	Description
Map User Role drop-down list	Select a user role that you want the users mapped to. You can choose a role that was available by default, or you can choose a role that you created in the system. Following are the roles that are available by default in Cisco UCS Director: • All Policy Admin • Billing Admin • Computing Admin • Service End-User • Group Admin • IS Admin • Network Admin • Operator Admin • Storage Admin • System Admin
Enable TACACS Authentication check box	Check this check box to enable TACACS-based authentication for users configured in Cisco ISE.

Step 12 Click **Submit**.

Step 13 Click **OK**.

The user role filters are added to the **User Role Filters** table.

Note If you have multiple user role filters specified, then the filter specified in the first row is processed.

If you manually update a user role for a user from the **Login Users** tab, then the user role that you mapped the group to is no longer applied to the user.

What to do next

If you have not set the authentication preference to LDAP, then you are prompted to modify the authentication preference. For more information on changing the authentication preference, see Configuring Authentication Preferences, on page 46.

Testing LDAP Server Connectivity

Procedure

Step 1 Choose **Administration** > **LDAP Integration**.

Step 2 In the **LDAP Integration** tab, choose an LDAP account name from the table.

Step 3 Click **Test Connection**.

Step 4 In the **Test LDAP Connectivity** screen, click **Close**.

Viewing LDAP Server Summary Information

Procedure

Step 1 Choose **Administration** > **LDAP Integration**.

Step 2 In the **LDAP Integration** tab, choose an LDAP account name from the table.

Step 3 Click **View**.

The **View LDAP Account Information** screen displays summary information of the LDAP account.

Step 4 Click **Close**.

Adding LDAP Search BaseDN Entries

Procedure

Step 1 Choose **Administration** > **LDAP Integration**.

Step 2 In the **LDAP Integration** tab, choose an LDAP account name from the table.

Step 3 Click **Search BaseDN**.

Step 4 If you have not checked **Enable Manual Search Base** while configuring the LDAP server, then in the **LDAP Search Base** screen, click **Select** to view the list of search base entries that are currently added.

a) Check the check boxes of the search base entries you want to include.
b) Click **Select**.
c) Click **Submit**.

Step 5 If you have checked **Enable Manual Search Base** while configuring the LDAP server, then in the **LDAP Search Base** screen, click **+** to add a new entry to the search base table.

For search base entries that are already added in the system, you can either edit, delete or re-order them using the options displayed on the screen.

Step 6 Click **Submit**.

Executing the LDAP Synchronization System Task

Procedure

Step 1 Choose **Administration** > **System**.
Step 2 On the **System** page, click **System Tasks**.
Step 3 Enter **LDAP** in the Filter field.
Step 4 Select **LDAPSyncTask** from the **System Tasks** table.
Step 5 Click **Run Now**.
Step 6 (Optional) Click **Manage Task** to enable or disable the synchronization process.

What to do next

The results of the synchronization process are displayed in Cisco UCS Director. Select an LDAP account on the **LDAP Integration** pane, and click **Results** to view the summary of the synchronization process.

Modifying LDAP Server Details

You can only modify the following details for a configured LDAP server:

- Port numbers and SSL configuration
- User name and password
- Synchronization frequency
- Search BaseDN selections
- User roles and groups that are mapped

Procedure

Step 1 Choose **Administration** > **LDAP Integration**.
Step 2 In the **LDAP Integration** tab, choose an LDAP account name from the table.
Step 3 Click **Modify**.
Step 4 In the **Modify LDAP Server Configuration** screen, edit the required fields, including the following:

Name	Description
Enable SSL check box	Enables a secure connection to the LDAP server.
Port field	The port number. It is automatically set to 636 for SSL, and 389 for non-secure mode.

Name	Description
User Name field	The user name. If you selected **OpenLDAP** as the LDAP Directory Type, then specify the user names in the following format: **uid=users,ou=People,dc=ucsd,dc=com** where **ou** specified is the one all the other users are placed in the directory hierarchy.
Password field	The user password.
Synchronization Frequency drop-down list	Choose the frequency (in hours) at which the LDAP server is synchronized with the system database. It can be one of the following: • 1 • 4 • 12 • 24

Step 5 Click **Next**.

Step 6 In the **LDAP Search Base** pane, click **Select** to specify LDAP search base entries and click **Select**.

Step 7 Click **Next**.

Step 8 In the **Configure User and Group Filters** pane, complete the following fields:

Name	Description
User Filters	Click the + sign to select specific users that must be synchronized with the system.
Group Filters	Click the + sign to select groups that must be synchronized with the system.

Step 9 Click **Next**.

Step 10 In the **LDAP User Role Filter** pane, click the **(+)** sign to add a user role filter.

Step 11 In the **Add Entry to User Role Filters** dialog box, complete the following fields:

Name	Description
Attribute Name field	The name of the attribute. It can be **Group Name**.
Operator drop-down list	It can be one of the following: • **Equal to** • **Starts with**

Name	Description
Attribute Value field	Specify a value in this field. All users that match the values of the **Operator** field and the **Attribute Value** field are assigned to the user role you select in the **Map User Role** drop-down list.
Map User Role drop-down list	Select a user role that you want the users mapped to. You can choose a role that was available by default, or you can choose a role that you created in the system. Following are the roles that are available by default in Cisco UCS Director: • All Policy Admin • Billing Admin • Computing Admin • Service End-User • Group Admin • IS Admin • Network Admin • Operator Admin • Storage Admin • System Admin

Step 12 Click **Submit**.

Step 13 Click **OK**.

The user role filters are added to the **User Role Filters** table.

Note If you have multiple user role filters specified, then the filter specified in the first row is processed.

Viewing Group Membership Information

Any user in the system can be part of multiple user groups. When a user is added to the system, all groups that the user is part of are also added to the system. However, the group that the user was most recently added to is set as the default primary group for the user. If the user is not part of any group, then the default primary group is set as **Domain Users**. While you can use the **Manage Profiles** option to view and modify group membership for users, Cisco UCS Director also provides you with an additional option to view a list of all groups that a specific user is part of.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Users**.

Step 3 Select a user from the table.

Step 4 From the **More Actions** drop-down menu, click **Group Membership**.

The **MemberOf** screen displays all the groups that the user is part of.

Step 5 Click **Close**.

Deleting LDAP Server Information

When you delete an LDAP server account, the following actions are initiated:

- Resources that have been assigned to LDAP users are un-assigned.
- VMs that have been assigned to the LDAP users are un-assigned.
- Resources that have been assigned to LDAP groups are un-assigned.
- VMs that have been assigned to the LDAP groups are un-assigned.
- VM share policies that have been assigned to LDAP users are un-assigned.
- Tags that have been applied to the LDAP users and groups are cleared
- Users and groups are immediately deleted from the database.
- The LDAP server details are removed from the tree view.

Procedure

Step 1 Choose **Administration** > **LDAP Integration**.

Step 2 In the **LDAP Integration** tab, choose an LDAP account name from the table.

Step 3 Click **Delete**.

Step 4 In the **Delete LDAP Account** screen, click **Delete**.

Step 5 Click **OK**.

This initiates the deletion of the LDAP account in Cisco UCS Director. Based on the number of users and groups in the LDAP account, this deletion process could take a few minutes to complete. During such time, the LDAP account may still be visible in Cisco UCS Director. Click **Refresh** to ensure that the account has been deleted.

Single Sign On with OneLogin

Cisco UCS Director provides a Single Sign-On (SSO) service based on SAML 2.0. To enable SSO, Cisco UCS Director must be registered as a Service Provider (SP) with the OneLogin Identity Provider (IDP). SSO

enables users to access multiple systems seamlessly without having to log in to individual systems. With SSO configured and enabled between the SP and IDP, a user can log in to the OneLogin portal and then access Cisco UCS Director without having to log in again.

To enable Single Sign-On with OneLogin, you must complete the following:

1. Create a user account at the OneLogin site.
2. Map the Cisco UCS Director appliance details in the OneLogin site.

   For more information, see Mapping the Cisco UCS Director Appliance at the OneLogin Site, on page 61
3. Generate a Single Sign-On certificate at the OneLogin site.

   For more information, see Generating a OneLogin Certificate, on page 62.
4. Create a user account in Cisco UCS Director with the same credentials as the account created at the OneLogin site. The user account must be created on the same appliance that was mapped in the OneLogin site.

   For information on adding a user, see Adding Users, on page 4.
5. Enable Single Sign-on by uploading the certificate on the appliance that you referenced in the OneLogin site.

   For more information, see Enabling Single Sign-On, on page 63.

After you complete this procedure, when you return to the OneLogin site and click on Cisco UCS Director, the user will no longer be prompted to enter their user name and password information.

Mapping the Cisco UCS Director Appliance at the OneLogin Site

To enable Single Sign-On, you must first map the system that is running Cisco UCS Director.

Before you begin

You must have a OneLogin account.

Procedure

Step 1 Access the OneLogin site from the following link: https://www.onelogin.com.

Step 2 Log in to the site using your account details.

Step 3 From the menu bar, choose **Apps** > **Add Apps**.

Step 4 In the **Find Applications** field, enter **SAML**.

Step 5 In the search results that are displayed, select and double-click **OneLogin SAML Test (IdP) SAML 2.0**.

The **Info** pane is displayed.

Step 6 In the **Info** pane, enter the following information:

Field	Description
Display Name field	Enter a unique name for the system that is running Cisco UCS Director. This name is displayed on the home page of the OneLogin portal. You can register multiple Cisco UCS Director appliances at this portal. Be sure to enter a name that helps you identify the system accurately.

Step 7 Click **Save**.

Step 8 Choose **Configuration** from the menu bar, and enter the following information:

Field	Description
SAML Consumer URL field	Enter the URL of the system that is running Cisco UCS Director. **Important** Enter the URL that is displayed after a user logs into the Cisco UCS Director user interface. It should look similar to the following: https://<ip_address>/app/cloudmgr/cloudmgr.jsp. For example: https://10.10.10.10/app/cloudmgr/cloudmgr.jsp. For releases 6.0 and later, the URL should look similar to the following: https://<ip_address>/app/ux/index.html. For example: https://10.10.10.10/app/ux/index.html.

Step 9 Click **Save**.

On the home page of this site, an icon is created for the server details that you specified. For every appliance that you register at the OneLogin site, an icon is displayed on the home page. If you click this icon, you are automatically directed to the Cisco UCS Director user interface.

What to do next

Generate a OneLogin certificate and enable SSO on the Cisco UCS Director appliance.

Generating a OneLogin Certificate

Before you begin

- You must have a OneLogin account
- The Cisco UCS Director application must be registered with the OneLogin website.

Procedure

Step 1 Access the OneLogin site from the following link: https://www.onelogin.com.

Step 2 Log in to the site using your account details.

Step 3 From the menu bar, choose **Settings** > **SAML**.

Step 4 Select **Standard Strength Certificate (2048-bit)**.

Step 5 Click **Download**.

Step 6 Click **OK**.

A file with the name `onelogin.pem` is downloaded to your system.

What to do next

You must upload this certificate on the Cisco UCS Director appliance.

Enabling Single Sign-On

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Single Sign-On**.

Step 3 Check **Enable Single Sign-On**.

Step 4 In the **File** field, either drag and drop a file, or click **Select a File** to browse and select the OneLogin certificate file on your system.

The OneLogin certificate file is saved on your system with the name `onelogin.pem`.

Step 5 Click **Upload**.

Step 6 When the upload is complete, click **Submit**.

When you launch Cisco UCS Director from the OneLogin site, you are not prompted to log in to the system.

Single Sign-on with Ping Federate

You can enable Single Sign-on (SSO) for Cisco UCS Director with Ping Federate. SSO enables users to access multiple systems seamlessly without having to log in to individual systems.

To enable Single Sign-On with Ping Federate, you must complete the following:

1. Create an adaptor.

   See Creating an Adapter in Ping Federate, on page 65

2. Create Service Provider (SP) connectors.

   See Creating Service Provider Connections, on page 65

3. Upload the certificate on the Cisco UCS Director appliance.

4. Navigate to the URL specified while creating the SP connection, and login using the credentials you had specified.

Creating a User in Ping Federate

Procedure

Step 1 Launch the Ping Federate user interface.

Step 2 Click **Server Configuration**.

Step 3 Click **Password Credential Validators** displayed under Authentication.

Step 4 Click **Create New Instance** and complete the following:

a) In the **Type** tab, enter unique values for **INSTANCE NAME** and **INSTANCE ID** fields.
b) In the **TYPE** drop-down list, choose **Simple Username Password Credential Validator**.
c) In the **PARENT INSTANCE** drop-down list, choose **None**.
d) In the **Instance Configuration** tab, click **Add a new row to Users**.

Step 5 Add a new user and click **Update**.

Step 6 Click **Next**.

Step 7 Review the summary.

Step 8 Click **Done**.

Creating LDAP Users

Procedure

Step 1 Launch the Ping Federate user interface.

Step 2 Click **Server Configuration**.

Step 3 Click **Password Credential Validators** link displayed below **Authentication**.

Step 4 Click **Create New Instance** and complete the following fields:

a) In the **Type** tab, enter unique values for **INSTANCE NAME** and **INSTANCE ID** fields and click **Next**.
b) In the **TYPE** drop-down list, choose **LDAP Username Password Credential Validator**.
c) In the **Parent Instance** drop-down list, choose **None**.
d) In the **Instance Configuration** tab, click **Manage Data Stores** displayed at the botton of the page.
e) Choose **Add New Data Store**.
f) In the **Data Store Type** drop-down list, choose **LDAP**.
g) Add appropriate values for the LDAP configuration fields.
h) Click **Done**.

Creating an Adapter in Ping Federate

Before you begin

You must create a user in Ping Federate with the same credentials of the user created in Cisco UCS Director. You can create a user in multiple ways in Ping Federate. Following are the commonly used procedures to create a user:

- Create a single user.

  See Creating a User in Ping Federate, on page 64

- Configure LDAP users.

  See Creating LDAP Users, on page 64

Procedure

Step 1 Launch the Ping Federate user interface.

Step 2 Choose **Adapter** > **Type**.

Step 3 Complete the following fields on the **Type** screen:

a) Enter unique values for the **INSTANCE NAME** and **INSTANCE ID** fields.
b) Choose **HTML Form IDP Adapter or LDAP** from the **Type** drop-down list.
c) Choose **None** from the **Parent Instance** drop-down list.
d) Click **Next**.

Step 4 Complete the following fields on the **IDP Adapter** screen:

a) Click **Add a new row to Credential Validators** and select the form that you created earlier.
b) Click **Update**.
c) Click **Next**.

Step 5 In the **Extended Contract** screen, click **Next**.

Step 6 In the **Adapter Attributes** screen, choose the user name as the pseudonym.

Step 7 Click **Next**.

Step 8 In the **Adapter Contract Mapping** screen, click **Next**.

Step 9 Review the information displayed in the **Summary** screen, and click **Done**.

Step 10 Click **Save**.

What to do next

Configure Service Provider (SP) connections.

Creating Service Provider Connections

Procedure

Step 1 Launch the Ping Federate user interface.

Step 2 Click **SP Connections**.

Step 3 Click **Create New**.

Step 4 In the **Connection Type** tab, check the **Browser SSO Profiles** check box and click **Next**.

Step 5 In the **Connection Options** tab, check the **Browser SSO** check box and click **Next**.

Step 6 In the **Import Metadata** tab, click the **None** radio button for the **METADATA** field.

Step 7 In the **General Info** tab, enter the values for the following fields:

- **Connection ID**
- **Connection Name**
- **BASE URL**—Enter the URL of Cisco UCS Director.

Step 8 Click **Next**.

Step 9 In the **Browser SSO** tab, choose **Configure Browser SSO** and complete the following:

a) In the **SAML Profiles** tab, check the **IDP-INITIATED SSO** checkbox and click **Next**.

b) In the **Assertion Lifetime** tab, retain the default values and settings, and click **Next**.

c) In the **Assertion Creation** tab, choose **Configure Assertion Creation** and complete the following:

1. In the **Identity Mapping** tab, choose the **Standard** option and click **Next**.
2. In the **Attribute Contract** tab, retain the default values and click **Next**.
3. In the **Authentication Source Mapping** tab, choose **Map New Instance** tab.

   You must select the adapter instance you previously created, and and click **Next**.
4. In the **Mapping Method** tab, retain the default values and click **Next**.
5. In the **Attributes Contract Fulfillment** tab, choose **Adapter** in the **Source** column and **username** in the **Value** column. Retain the default values for other columns, and and click **Next**.

Step 10 In the **Protocol Setting** tab, choose **New Protocol**, and complete the following:

a) In the **Assertion Consumer Service URL** screen, choose **POST** in the **Binding** column and enter the Cisco UCS Director URL in the **Endpoint URL** column and click **Next**.

b) Choose the default values in the subsequent screen and click **Done**.

Step 11 In the **Credentials** tab, create a certificate and download it. Click **Next**.

Step 12 In the **Activation and Summary** screen, choose **Active** as the **Connection Status** and click **Done**.

Step 13 Upload the certificate in Cisco UCS Director.

The user name you specify must be the same as the user name specified in Ping Federate.

Step 14 Navigate to the URL you specificed as the SSO Application Endpoint and login to complete enabling single sign-on.

Authentication and Cisco Identity Services Engine (Cisco ISE)

Cisco Identity Services Engine (Cisco ISE) Integration

You can integrate a Cisco Identity Services Engine (Cisco ISE) server into Cisco UCS Director using TACACS to synchronize Cisco ISE users and user groups. With this integration, users configured in Cisco ISE are retrieved and integrated in Cisco UCS Director. Following are the prerequisites to configuring the Cisco ISE server in Cisco UCS Director:

- Add Cisco UCS Director as a network device in Cisco ISE and enable TACACS authentication.

  The shared secret key that you enter in Cisco ISE to enable TACACS authentication must be entered in Cisco UCS Director when you add the Cisco ISE server.

- Specify an authentication protocol in Cisco ISE. It can either be PAP/ASCII or CHAP.

  The authentication protocol that you select in Cisco ISE must be selected in Cisco UCS Director as well.

- Enable the External RESTful Services (ERS) APIs in Cisco ISE.

  In a cluster-setup, you must enable ERS for the primary administration node and for all the other nodes.

Note You can integrate a Cisco ISE server that is running release version 2.6.0.156 or later.

For information on completing these prerequisites, see the *Cisco Identity Services Engine Administrator Guide*.

After addng the Cisco ISE server in Cisco UCS Director, you can synchronize the users and groups automatically or manually. While adding the Cisco ISE account, you can specify a frequency at which the account is synchronized automatically with Cisco UCS Director. Optionally, you can manually trigger the synchronization by using the **ISE Sync Task** system task. After the system task runs, all user accounts are retrieved and displayed on the **Users** page, and **User Groups** page. By default, a user group called TACACS Users Group is available on the **User Groups** page. Cisco ISE users that do not belong to any user group are automatically added to this user group when their accounts are retrieved in Cisco UCS Director.

Cisco UCS Director also includes the **Cleanup ISE Users** system task to disable accounts of users that have been removed from Cisco ISE. By default, this system task is disabled. If you enable this system task, it runs automatically every day.

Configuring Cisco Identity Services Engine (Cisco ISE) Server Integration

Before you begin

- Add Cisco UCS Director as a network device in Cisco ISE and enable TACACS authentication.

  The shared secret key that you enter in Cisco ISE to enable TACACS authentication will have to be entered in Cisco UCS Director when you add the Cisco ISE server.

- Specify an authentication protocol in Cisco ISE.

It can either be Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). The authentication protocol that you select in Cisco ISE must be selected in Cisco UCS Director when you add the Cisco ISE server.

- Enable the External RESTful Services (ERS) APIs in Cisco ISE.

  In a cluster-setup, you must enable ERS for the primary administration node and for all the other nodes.

For information on completing these prerequisites, see the *Cisco Identity Services Engine Administrator Guide*.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **ISE Server Integration**.

Step 3 Click **Add**.

Step 4 In the **ISE Configuration** screen, complete the required fields, including the following:

Name	Description
Account Name field	The name of the account. This name must be unique.
Server field	The IP address or the host name of the Cisco ISE server.
Port field	The port number. By default this port number is set to 49.
Username field	The user name of the user who has access to the REST APIs of the Cisco Identity Services Engine (ISE).
Password field	The password of the user who has access to the REST APIs of the Cisco Identity Services Engine (Cisco ISE).
Authentication Type	The authentication type to be used. It can be one of the following: • Password Authentication Protocol (PAP) or • Challenge Handshake Authentication Protocol (CHAP)—not supported for LDAP users.
Secret Key	The shared secret key you configured in Cisco ISE.
Connection Timeout	The time (in seconds) that the system waits after which the connection is timed out.

Name	Description
Synchronization Interval field	Select the frequency (hours) at which the ISE server must be synchronized. It can be one of the following: • 4 • 12 • 24

Step 5 Click **Next**.

Step 6 In the **Configure User and Group Filters** pane, complete the following fields:

Name	Description
User Filters	Click the + sign to select specific users that must be synchronized with the system. All groups that the selected users are part of are retrieved and added into the system.
Group Filters	Click the + sign to select groups that must be synchronized with the system. All users that are part of the selected group filters are retrieved and added into the system. However, if the users in the selected group are also part of other groups, then those groups are not retrieved and added to the system unless you select them.
Add Entry to Group Filters dialog box	
Attribute Name drop-down list	Choose either **Group Name** or **User Name**.
Operator drop-down list	Choose the filter to retrieve groups and users. It can be one of the following: • **Equal to** • **Starts with**
Attribute Value field	Specify a keyword or a value that must be included in the search and click **Submit**.

Based on the filters, the groups or users are retrieved.

Step 7 Click **Next**.

Step 8 In the **Configure User Role Filters** pane, click the **(+)** sign to add a user role filter.

Step 9 In the **Add Entry to User Role Filters** dialog box, complete the following fields:

Name	Description
Attribute Name field	The name of the attribute. It can be **Group Name**.

Name	Description
Operator drop-down list	It can be one of the following: • **Equal to** • **Starts with**
Attribute Value field	Specify a value in this field. All users that match the values of the **Operator** field and the **Attribute Value** field are assigned to the user role you select in the **Map User Role** drop-down list.
Map User Role drop-down list	Select a user role that you want the users mapped to. You can choose a role that was available by default, or you can choose a role that you created in the system. Following are the roles that are available by default in Cisco UCS Director: • All Policy Admin • Billing Admin • Computing Admin • Service End-User • Group Admin • IS Admin • Network Admin • Operator Admin • Storage Admin • System Admin

Step 10 Click **Submit**.

Step 11 Click **Submit** in the **Configure User Role Filters** page.

Branding for Customer Organizations

Cisco UCS Director supports branding and customizing the portal at the following levels:

- Global level—This system-level branding can be modified by the global administrator.
- MSP Organization level or the tenant level—The branding at this level can be modified by the administrator or the MSP administrator.

- Customer organization level—Customer organizations are usually grouped with an MSP organization. An MSP administrator or a global administrator can modify the branding details.

With the introduction of branding support at the MSP organization level, certain rules apply to what branding changes users may view. The settings that are applied depend on the following:

- User role—Is the user an end user, a group administrator, or an MSP administrator?
- User's customer organization and the branding set for it.
- MSP Organization branding settings.

The following table elaborates the branding behavior in Cisco UCS Director.

Table 1: Branding Behavior in Cisco Cisco UCS Director

Branding set at MSP Organization Level	Branding set at Customer Organization Level	MSP Administrator	Group Administrator	End User
Yes	Yes	Branding details set at the MSP organization level are displayed.	Branding details set at the customer organization level is displayed.	Branding details set at the customer organization level to which this user belongs to is displayed.
No	Yes	Global branding details are displayed.	Branding details set at the customer organization level is displayed.	Branding details set at the customer organization level to which this user belongs to is displayed.
Yes	No	Branding details set at the MSP organization level are displayed.	Branding details set at the MSP organization level to which this customer organization belongs to is displayed.	Branding details set at the MSP organization level to which the customer organization belongs to is displayed.
No	No	Global branding details are displayed.	Global branding details are displayed.	Global branding details are displayed.

Branding User Groups

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **User Groups**.

Step 3 Choose the group to brand.

Step 4 From the **More Actions** drop-down menu, click **Branding**.

The **Group Branding** screen displays the options that you can customize.

Step 5 Check **Logo image** to customize the image that is displayed on the top left corner of the user interface.

a) Click **Upload** to browse to a logo image file and choose it.

Note Make sure that the logo image is in PNG, JPG, or GIF format. The optimal image size is 200 pixels in width and 100 pixels in height. We recommend that you use a small file size to enable faster download.

b) Click **Submit**.

Step 6 Check **Application Labels** to specify a label that is displayed on the top header of the user interface.

a) Enter at least one application label in the **Label 1** and **Label 2** fields.

Step 7 Check **URL Forwarding on Logout** to re-direct users to a specific URL after logging out of the user interface.

a) In the **URL** field, enter the **URL**.

Step 8 Required: Check **Custom Links** to specify the links that appear on the top right corner of the user interface.

a) Complete at least the first two fields.

Name	Description
Custom Link 1 Label field	The label for custom link 1.
Custom Link 1 URL field	The URL for custom link 1.
Custom Link 2 Label field	The label for custom link 2.
Custom Link 2 URL field	The URL for custom link 2.

Step 9 Click **Submit**.

Branding Customer Organizations

You can customize the logo and application labels for customer organizations in Cisco UCS Director.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 Choose the **Customer Organizations** tab or the **MSP Organizations** tab.

These tab names are only indicative. If you have enabled the **Service Provider Feature**, you have to specify the names of the organization at the first and second level. The names that you specify are displayed as tabs in the interface. If you have disabled the **Service Provider Feature**, then only the **Customer Organizations** tab is displayed.

Step 3 Choose the customer organization to brand.

Step 4 From the **More Actions** drop-down menu, click **Branding**.

The **Group Branding** screen displays the options that you customize.

Step 5 Check **Logo image** to customize the image that is displayed on the top left corner of the user interface.

a) Click **Upload** to browse to a logo image file and choose it.

Note Make sure that the logo image is in PNG, JPG, or GIF format. The optimal image size is 200 pixels in width and 100 pixels in height. We recommend that you use a small file size to enable faster download.

b) Click **Submit**.

Step 6 Check **Application Labels** to specify a label that is displayed on the top header of the user interface.

a) Enter at least one application label in the **Label 1** and **Label 2** fields.

Step 7 Check **URL Forwarding on Logout** to re-direct users to a specific URL after logging out of the user interface.

a) In the **URL** field, enter the **URL**.

Step 8 Required: Check **Custom Links** to specify the links that appear on the top right corner of the user interface.

a) Complete at least the first two fields.

Name	Description
Custom Link 1 Label field	The label for custom link 1.
Custom Link 1 URL field	The URL for custom link 1.
Custom Link 2 Label field	The label for custom link 2.
Custom Link 2 URL field	The URL for custom link 2.

Step 9 Click **Submit**.

Login Page Branding

A login page can be configured to display a logo that is associated with a domain name. When the end user logs in from that domain, the user sees the custom logo on the login page. The optimal image size for a logo is 890 pixels wide and 470 pixels high, with 255 pixels allowed for white space. Cisco recommends that you keep the image size small to enable faster downloads.

Note The group or customer organization login page must first be configured (enabled) for branding.

Configuring a Custom Domain Logo

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Login Page Branding**.

Step 3 Click **Add**.

Step 4 In the **Domain Branding** screen, complete the required fields, including the following:

Name	Description
Domain Name field	The domain name to brand.
Custom Domain Logo check box	Check the check box to enable login page branding from a specified domain name.
File field	The logo file to upload. You can either drag and drop a file in this field, or you can click **Select a File** to browse and select the file to upload. **Note** The optimal image size for a logo is 890 pixels wide by 470 pixels high, with 255 pixels for white space. We recommend that you keep the image size small to enable faster downloads.

Step 5 Click **Submit**.