Administration

Administration of Core Platform Features

Cisco UCS Director administration includes core platform features, such as configuration for users and groups, and the ways in which you can add your own brand to Cisco UCS Director and End User Portal. These core platform features enable you to securely control how your users and customers access Cisco UCS Director and what they see after they log in.

For more information how to administer the core platform features, see the Cisco UCS Director Administration Guide.

Users

You can create locally authenticated users for Cisco UCS Director, or you can integrate Cisco UCS Director with your LDAP server and synchronize the LDAP users and groups with Cisco UCS Director. You can do the following with your users, whether they are local to Cisco UCS Director or they access Cisco UCS Director through an LDAP integration:

- Assign user roles and permissions to limit their access and the operations that they can perform
- Enable the Managed Service Provider feature
- Group internal and external customers to control which applications, resources, and tenants they can view
- Set resource limits on user groups or customer organizations
- Create a password policy to define the minimum password requirements for all users

User Groups

User groups provide a way for you to define logical associations between your users. For example, you could create user groups for the Development, Sales, and Marketing users within your business. Through the user group, you can then associate the users in that group with the following:

- One or more virtual data centers (vDCs) that define the infrastructure resources which the users can access when making service requests
- Resource limits that further control the maximum resources that users in a group can use.
- A cost center for chargeback on the infrastructure resources

Managed Service Provider and Customer Organizations

Managed service provider and customer organizations are available only when you enable the Service Provider feature in Cisco UCS Director.

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

Like user groups, you can associate users in customer organizations with the following:

- One or more virtual data centers (vDCs) that define the infrastructure resources which the users can access when making service requests
- Resource limits that further control the maximum resources that users in a group can use
- A cost center for chargeback on the infrastructure resources

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.

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).

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**.

- 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.

- 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.

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.

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.

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.

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

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 on viewing group membership

information, see the Cisco UCS Director Administration Guide. 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.

Branding Cisco UCS Director

Cisco UCS Director supports branding and customizing Cisco UCS Director and End User Portal at the following levels:

- Global level—This system level branding can be modified by the global administrator.
- MSP organization level or tenant level—The branding at this level can be modified by the administrator or the MSP administrator.
- Customer organization level—The branding at this level can be modified by an MSP administrator or a global administrator. Customer organizations are usually grouped with an MSP organization.

Branding for Customer Organizations

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.

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.