Managing Users and Groups

This chapter contains the following sections:

Note You must be logged in to the appliance before you can run any of the following procedures.

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 will view and use the Administrative Portal when they log in, which is described in this guide.

User Types

Cisco UCS Director supports a number of user types:

- All Policy Admin
- Billing Admin
- Computing Admin
- Group Admin - An end user with the privilege of adding users. This user can use the Self-Service Portal.
- IS Admin
- Network Admin
- Operator
- Service End User - This user only views and uses the Self-Service Portal.

- Storage Admin
- System Admin

Default User Permissions

Each user type has a default set of system permissions.

All Policy Admin

Task	Permission
Computing Clouds	Read-only
Storage Clouds	Read-only
Network Clouds	Read-only
Group Service Request	Read/write
Approver Service Request	Read/write
Chargeback	Read-only
Catalog	Read-only
vDC	Read-only
Computing Policy	Read/write
Storage Policy	Read/write
Network Policy	Read/write
Service Delivery Policies	Read/write
System Admin	Read-only
Users and Groups	Read-only
Budgeting	Read-only
Cloud Accounts	Read-only
Resource Accounting	Read-only
Resource Limit Report	Read-only
Group Users	Read-only

Billing Admin

Task	Permission
Computing Clouds	Read-only
Storage Clouds	Read-only
Network Clouds	Read-only
Group Service Request	Read-only
Approver Service Request	Read/write
Chargeback	Read-only
Catalog	Read-only
vDC	Read-only
Computing Policy	Read-only

Task	Permission
Storage Policy	Read-only
Network Policy	Read/write
Service Delivery Policies	Read-only
System Admin	Read-only
Users and Groups	Read-only
Budgeting	Read-only
Cloud Accounts	Read-only
Resource Accounting	Read-only
Resource Limit Report	Read-only
Group Users	Read-only

Computing Admin

Task	Permission
Computing Clouds	Read-only
Storage Clouds	Read-only
Network Clouds	Read-only
Computing Infrastructure	Read/write
Group Service Request	Read-only
Approver Service Request	Read/write
Chargeback	Read-only
Catalog	Read-only
vDC	Read-only
Computing Policy	Read/write
Storage Policy	Read-only
Network Policy	Read-only
Service Delivery Policies	Read-only
System Admin	Read-only
Users and Groups	Read-only
Budgeting	Read-only
Cloud Accounts	Read-only
Resource Accounting	Read-only
Resource Limit Report	Read-only
Group Users	Read-only

Group Admin

Task	Permission
Computing	Cloud write only
Group Service Request	Read/write
Approver Service Request	Read/write

Task	Permission
Chargeback	Read-only
Catalogs	Read-only
vDC	Read-only
Resource accounting	Read-only
Resource limit report	Ready only.
VM label	Write only.
Group users	Read/write

IS Admin

Task	Permission
Computing Clouds	Read-only
Storage Clouds	Read-only
Network Clouds	Read-only
Computing Infrastructure	Read-only
Group Service Request	Read-only
Approver Service Request	Read/write
Chargeback	Read-only
Catalog	Read/write
vDC	Read/write
Computing Policy	Read-only
Storage Policy	Read-only
Network Policy	Read-only
Service Delivery Policies	Read/write
System Admin	Read-only
Users and Groups	Read-only
Budgeting	Read-only
Cloud Accounts	Read-only
Resource Accounting	Read-only
Resource Limit Report	Read-only
Group Users	Read-only

Network Admin

Task	Permission
Computing Clouds	Read-only
Storage Clouds	Read-only
Network Clouds	Read-only
Group Service Request	Read-only
Approver Service Request	Read/write
Chargeback	Read-only
Catalog	Read-only
vDC	Read-only
Computing Policy	Read-only
Storage Policy	Read-only
Network Policy	Read/write
Service Delivery Policies	Read-only
System Admin	Read-only
Users and Groups	Read-only
Budgeting	Read-only
Cloud Accounts	Read-only
Resource Accounting	Read-only
Resource Limit Report	Read-only
Group Users	Read-only

Operator

Task	Permission
Computing Clouds	Read-only
Storage Clouds	Read-only
Network Clouds	Read-only
Group Service Request	Read/write
Approver Service Request	Read/write
Chargeback	Read-only
Catalog	Read-only
vDC	Read-only
Computing Policy	Read-only
Storage Policy	Read-only
Network Policy	Read-only
Service Delivery Policies	Read-only
System Admin	Read-only
Users and Groups	Read-only
Budgeting	Read-only
Cloud Accounts	Read-only

Task	Permission
Resource Accounting	Read-only
Resource Limit Report	Read-only
Group Users	Read-only

Service End User

Task	Permission
Computing Cloud	Write-only
Group Service Request	Read/write
Approver Service Request	Read/write
Chargeback	Read-only
Catalogs	Read-only
vDC	Read-only
Resource accounting	Read-only
Resource limit report	Read-only

Storage Admin

Task	Permission
Computing Clouds	Read-only
Storage Clouds	Read-only
Network Clouds	Read-only
Group Service Request	Read-only
Approver Service Request	Read/write
Chargeback	Read-only
Catalog	Read-only
vDC	Read-only
Computing Policy	Read-only
Storage Policy	Read/write
Network Policy	Read-only
Service Delivery Policies	Read-only
System Admin	Read-only
Users and Groups	Read-only
Budgeting	Read-only
Cloud Accounts	Read-only
Resource Accounting	Read-only
Resource Limit Report	Read-only
Group Users	Read-only

System Admin

Task	Permission
Computing Clouds	Read/write
Storage Clouds	Read/write
Network Clouds	Read/write
Group Service Request	Read/write
Approver Service Request	Read/write
Chargeback	Read-only
Catalog	Read/write
vDC	Read/write
Computing Policy	Read/write
Storage Policy	Read/write
Network Policy	Read/write
Service Delivery Policies	Read/write
System Admin	Read/write
Users and Groups	Read/write
Budgeting	Read/write
Cloud Accounts	Read/write
Resource Accounting	Read-only
Resource Limit Report	Read-only
Resource Limit	Write-only
Group Users	Read-only

Administration Profile

You must first configure your system administrator profile before you can configure groups and their users.

Creating the admin Profile

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

Step 2 Choose the **Login Users** tab.

Step 3 Click **Add**.

Step 4 In the **Add User** dialog box,complete the following fields:

Name	Description
User Type drop-down list	Choose the administrator's user type. The system administrator has full privileges.
User Group drop-down list	Choose the administrator's user group.
Login Name field	The login name. The default is admin.

Name	Description
Password field	Enter the admin password.
Confirm Password field	Enter the admin password again to confirm it.
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.

Changing the admin Password

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

Step 2 Choose the **Login Users** tab.

Step 3 In the **Login Name** column, choose **admin**.

Step 4 Click **Change Password**.

Step 5 In the **Change Password** dialog box, enter a new password for the **admin** user and confirm it.

Step 6 Click **Save**.

Step 7 In the **Add User** dialog box, complete the following fields:

What to Do Next

Configure groups and customer organizations.

Adding Users

Before You Begin

Create the group to which the user will belong.

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

Step 2 Choose the **Login Users** tab.

Step 3 Click **Add** (+).

Step 4 In the **Add User** dialog box, complete the following fields:

Name	Description
User Type drop-down list	Choose the user type.
User Group drop-down list	Choose the group or customer organization to which the user belongs.
Login Name field	The user's login name.

Name	Description
Password field	The user's password. **Note** If the Lightweight Directory Access Protocol (LDAP) authentication is configured for the user, the password is validated only at the LDAP server, not at the local server.
Confirm Password field	Confirm the user password.
User Contact Email field	The user's email address. **Note** The email address is used to notify the group owner about service request status and to request approvals.
First Name field	The user's first name.
Last Name field	The user's last name.
Phone field	The user's phone number.
Address field	The user's address.

Step 5 Click **Add**.

What to Do Next

After choosing a user from the main page and then clicking **Manage Profiles**, you can optionally assign multiple roles for that user.

Viewing Current Online Users

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

Step 2 Choose the **Current Online Users** tab to view online user details.You can view the user name, IP address, session start time, last data access, and client.

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 an all-policy administrator, if both types of access are appropriate.

Note One of the profiles can be set as the default user access profile.

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

Creating a User Access Profile

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

Step 2 Choose the **Login Users** tab.

Step 3 Choose a user from the list.

Step 4 Click **Manage Profiles**.

Step 5 In the **Manage Profiles** page, click **Add** (+).

Step 6 In the **Add Entry to Access Profiles** dialog box, complete the following fields:

Name	Description
Name field	The profile name.
Description field	The description of the profile.
Type drop-down list	Choose the user role type.
Group drop-down list	Choose the user's group.
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.

Editing A User Access Profile

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

Step 2 Choose the **Login Users** tab.

Step 3 Choose a user from the list.

Step 4 Click **Manage Profile**s.

Step 5 In the **Manage Profiles** page, choose a user from the list.

Step 6 Click **Edit.**

Step 7 In the **Edit Access Profiles Entry** dialog box, edit the **Name**, **Description**, **Type**, **Group**, or the **Default Profile** fields, as needed.

Step 8 Click **Submit**.

Deleting a User Access Profile

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

Step 2 Choose the **Login Users** tab.

Step 3 Choose a user from the list.

Step 4 Click **Manage Profile**s.

Step 5 In the **Manage Profiles** page, choose a user from the list.

Step 6 In the **Manage Profile**s dialog box, click **Delete**.

Logging in to a Profile

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

Note 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 the Default Profile

Step 1 At the upper right of the page (to the left of **logout**), click the user name**.**

Step 2 In the **User Information** page, click the **Access Profiles** tab.

Step 3 Choose a user profile, and click **Set as Default Profile**.

Note A profile can also be set as default while adding or editing a profile.

Managing Groups

Creating a Group or Customer Organization

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

Step 2 Choose the **User Groups** tab.

Step 3 Click **Add**.

Step 4 In the **Add Group** dialog box, complete the following fields:

Name	Description
Name field	The a name of the group/customer organization.
Description field	The description of the group/customer organization if required.
Code field	Enter 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 a group is associated with. This name can be used in a VMware System policy for the VM naming convention. **Note** For more information about using **Cost Center** for naming conventions, see Chapter 6 "Managing Policies".
Contact Email field	The contact email address. This email is 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.

Step 5 Click **Add**.

What to Do Next

Repeat this procedure if you want to add more groups.

Group Password Policy

The password policy for a group 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 reset the current password as a new password
- Regular expressions that are disallowed in a password.

Creating A Password Policy

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

Step 2 Choose the **Password Policy** tab.

Step 3 In the **Password Policy** pane, complete the following fields:

Name	Description
Minimum Password Length drop-down list	Choose the minimum number of characters for the password.
Maximum Password Length drop-down list	Choose the maximum number of characters for the password.
Minimum Character Classes drop-down list	Choose the minimum number of character classes such as upper case, lower case, numbers, and special characters.
Disallow Login in Password check box	Check the check box to disallow passwords, which are the same as the login ID.
Disallow Previous Password check box	Check the check box to disallow a change of passwords.
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”.

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, as well as configure a group or customer organization to stay within or exceed the provisioned budget.

Viewing and Editing a Group Budget Policy

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

Step 2 Choose the **User Groups** tab.

Step 3 Choose a group from the list.

Step 4 Click **Budget Policy**.

Step 5 In the **Budget Policy** dialog box, complete the following fields:

Name	Description
Enable Budget Watch check box	Check the check box to monitor the groups budget usage. Uncheck the check box to ignore all budget entries for this group.
Allow Over Budget check box	Check if the group members are allowed over the provisioned budget. Uncheck the check box to reject all 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 or customer organization to help manage group resource utilization. You can specify limits on the following:

- Virtual resources
- Operating system resources
- Physical resources

Viewing Resource Limits

Step 1 Click **Organizations > Summary**.

Step 2 Click a group to view.

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

Editing Resource Limits

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

Step 2 Choose the **User Groups** tab.

Step 3 Choose a group and click **Edit Resource Limits.**

Step 4 In the **Resource Limit** dialog box appears.

Step 5 In the **Resource Limit** dialog box, check the **Enable Resource Limits** check box and complete the following fields:

Name	Description
Group display-only field	The group name.
Enable Resource Limits check box	Check the check box to enable the resource limits, 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.
Provisioned vCPUs Limit field	The maximum number of provisioned vCPUs.
Provisioned Memory (GB) Limit field	The provisioned CPU limit, in gigahertz.
Provisioned CPU (GHz) 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.

Name	Description
Count CPU and Memory for Inactive VMs check box	Check the checkbox to include the group's inactive VM CPU or memory data in the computation of resource limits. Uncheck the check box to exclude inactive VMCPU or memory data from the computation of resource limits.
OS Resource Limits	
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.
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 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**.

Authentication and LDAP Integration

You can configure a preference with or without a fallback choice for local authentication and a preference with a fallback for the LDAP. You can also configure a preference with no fallback for Verisign Identity Protection (VIP) authentication.

Name	Description
Local Authentication	Authentication is local only (Cisco UCS Director), and not through the LDAP server.
Local First, fallback to LDAP drop-down list option	Authentication is done first at the local server (Cisco UCS Director). If the user is unavailable at the local server, the LDAP server is checked.

Name	Description
LDAP First, fallback to Local drop-down list option	Authentication is done first at the LDAP server. If the user is unavailable at the LDAP server, the local server is checked (Cisco UCS Director).
Verisign Identity Protection drop-down list option	VIP Authentication Service (two-factor authentication) is enabled.

Configuring Authentication Preferences

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

Step 2 Choose the **Authentication Preferences** tab.

Step 3 In the **Authentication Preferences** pane, complete the following fields:

Name	Description
Authentication Preferences drop-down list	Choose the Authentication Preference. If you chose Local Authentication, continue to Step 4. If you chose VIP, continue to Step 5.
User Name field	The user name.
Password field	The user password.
Port Number field	The port number.
Server field	The IP address of the server.
Domain Name field	The domain name.
LDAP Sync Interval drop-down list	Choose the LDAP synchronization interval.
Enable LDAP Sync check box	Check the check box if you want to enable LDAP synchronization. Uncheck the check box if you do not want LDAP synchronization.
Modify Existing Users and Groups check box	Check the check box if you want to enable modification of existing users and groups.
Test LDAP	Check the check box if you want to test LDAP connectivity to Cisco UCS Director.

Step 4 (Optional) For local authentication, click **Save**.

Step 5 (Optional) In the **VIP Certificate** field, browse to the VIP Certificate file and choose it.

Step 6 Enter the **Password**.

Step 7 Click **Save**.

What to Do Next

If you configured LDAP first as the authentication preference, you must configure the LDAP credentials.

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.

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

You cannot choose users and groups that exist locally or are synchronized externally in 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 the Cisco UCS Director.
- A maximum of 1000 Users (subject to availability) are displayed for selection in manual search when you use the advanced search option. This option is available by clicking **Request Manual LDAP Sync**.

User Synchronization Rules

- If a chosen LDAP user already exists in Cisco UCS Director and the source is type **Local**, the user is ignored during synchronization.
- If a chosen LDAP user already exists in Cisco UCS Director and the source type is **External**, the user's name, description, email, and other attributes are updated for the user.

User Synchronization Limitations

- A user password cannot be retrieved from the LDAP server. Instead, a random password is generated for the user during LDAP synchronization.
- If a user has multiple group membership, that user has single group membership in Cisco UCS Director.

Note Be sure that the user is assigned to the correct group after the LDAP synchronization process.

Note Cisco UCS Director currently supports a single domain.

Managing LDAP Integration

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

Step 2 Choose the **LDAP Integration** tab to view the status of LDAP server synchronization.

Step 3 (Optional) Choose a 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 **Enable LDAP Sync** check box is checked in the Authentication Preferences tab. This action is also considered to be an automatic sync process.
Request LDAP Sync	Enables on-demand synchronization of the LDAP server. This action syncs the users/groups from the selected organization in "Search Base DN". Groups and users added from LDAP appear as type **External**. Groups and users added by Cisco UCS Director appear as type **Local**. Click **Submit** to synchronize the server. LDAP user changes are immediately reflected. **Note** Make sure that the user is assigned to the correct group after the LDAP Sync is processed. Continue to Step 4.
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. Continue with Step 6.

Step 4 (Optional) For LDAP synchronization request, verify the IP address/domain name, and click **Submit**.

Step 5 (Optional) If you chose **LDAP Manual Server Sync**, complete the following fields:

Name	Description
Basic Search field	Check the check box to enable **Basic Search** by organization unit. If checked, continue to Step 6.
Advanced Search field	Check the check box to enable **Advanced Search**. If checked, continue to Step 8.

Step 6 For basic search, click **Select**.

Step 7 Choose the distinguished name to search, and click **Select**.

Step 8 For advanced search, in the **Select Users and Groups** pane, add or edit attribute names for **User Filters and Group Filters**.

Step 9 Click **Next**.

Step 10 Choose the **LDAP Groups** and **LDAP Users**.

Step 11 Click **Submit** to synchronize the LDAP server.

Single Sign-On

Cisco UCS Director provides a single sign-on using One Login. Single sign-on prevents a user from having to enter a password multiple times to access the application.

When Single Login is enabled, a user can log into that portal to access Cisco UCS Director.

Note A single sign-on is available for Cisco UCS Director after you register a One Login certificate.

Enabling a Single Sign-On

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

Step 2 Click the **Single Sign-On** tab.

Step 3 In the **Single Sign-On** pane, check the **Enable Single Sign On** check box.

Step 4 In the **Select a File for Upload** field, browse to the One Login certificate file and choose it.

Step 5 Click **Upload**.

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

Branding

For a group or customer organization, the branding options are as follows:

- Logo image in PNG, JPG, or GIF format
- Customized application labels
- URL to forward the Self-Service Portal to upon logout
- Custom links with labels and URLs specified
- Login page background and logo.

Branding Groups and Customer Organizations

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

Step 2 Choose the **User Groups** tab.

Step 3 Choose the group to brand.

Step 4 Click **Branding**.

Step 5 In the **Group Branding** dialog box, complete the following fields: check the **Logo Image** check box and

Name	Description
Logo image check box	Check the check box to upload a logo image. Continue to Step 6.
Application Labels check box	Check the check box to customize an application label to appear in the application header. Continue to Step 8.

URL Forwarding on Logout check box	Check the check box to forward to a specific URL upon logout. Continue to Step 9.
Custom Links check box	Check the check box to brand custom links. Continue to Step 10.

Step 6 In the **Select a File for Upload** field, browse to the 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.

Step 7 Click **Upload**.

Step 8 (Optional) For application labels, enter at least one application label in the **Label 1** and **Label** 2 fields.

Step 9 (Optional) In the URL field, enter the **URL** to direct the user to upon logout.

Step 10 (Optional) Complete at least the first two fields:

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

Step 11 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. We recommend 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

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

Step 2 Choose the **Login Page Branding** tab.

Step 3 Click **Add**.

Step 4 In the **Domain Branding** dialog box, complete the following fields:

Name	Description
Domain Name field	Enter the domain name to brand.
Custom Domain Logo check box	Check the check box to enable login page branding from a specified domain name.
Select a file for upload field	Upload the logo file. **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**.