CentraSite

Users, Groups, Roles and Permissions

Version 9.5 SP1

November 2013

This document applies to CentraSite Version 9.5 SP1.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Document ID: IINM-AG-PERMITS-95SP1-20140410

Table of Contents

Users, Groups, Roles and Permissions

This document describes how to create and manage users, groups, roles and permissions on the CentraSite registry/repository. It also describes how to change passwords of predefined users and login users.

The content is organized under the following sections:

About Users	Describes how to create and manage users in CentraSite.
About Groups	Describes how to create and manage groups in CentraSite.
About Roles and Permissions	Describes how to create and manage roles and add permissions in CentraSite.
Changing Passwords of Predefined Users and Login Users	Describes how to change passwords of predefined users and login users.

1 About Users

Users identify individuals that are known to CentraSite. You assign roles and permissions to users to specify which operations they can perform and which registry objects they can access.

When you initially install an instance of CentraSite, it has only two user accounts: an account for the *bootstrap user* and an account for the *default user*.

- *The bootstrap user* refers to the user who installs CentraSite. This user belongs to the Default Organization and becomes the initial Organization Administrator for the organization as well as its primary contact. This user is also given the CentraSite Administrator role, which gives him or her "super admin" privileges. After CentraSite is installed, you can assign other users to the Organization Administrator role and/or the primary contact position for the Default Organization.
- *The default user* represents an internal user that owns the pre-define objects installed with CentraSite. The default user exists for CentraSite's internal use. You cannot edit or delete this account. You cannot use the default user account to log on to CentraSite.

Typically, the bootstrap user creates the initial set of organizations on the CentraSite registry/repository. Then, the organization administrators create user accounts for the users that belong to their organizations.

This document covers the following topics:

User Authentication Mechanisms

Although CentraSite maintains its own database of user accounts, the users associated with those accounts are authenticated by an external authentication system at log on time.

CentraSite is delivered with one predefined authentication configuration, namely the configuration to use an internal text file, and this configuration is the default configuration. However, after installation, you can configure it to also use the following types of authentication systems:

- The operating system's user repository.
- Active Directory Server (ADS).

  Note: If the CentraSite registry/repository is installed on a UNIX or Linux machine, you can only use the Active Directory Server as the user repository if it is configured via the LDAP interface.

- Lightweight Directory Access Protocol (LDAP).

See the section *Overview of User Repositories* in the document *Authentication Topics and LDAP* for more details.

If you are working in a distributed environment, where one or more Application Server Tiers and a separate registry/repository are involved, you must configure CentraSite to use an external au-

thentication system. If you are working in a mixed Windows and UNIX environment, CentraSite can use Active Directory or LDAP as the user repository for both.

Note: Although CentraSite allows you to define multiple user repositories for authentication, only one is the default at any given time. Users who log on to the system by just providing the user name will be authenticated against the default authentication system. If you wish to log on to CentraSite with a user name that does not reside in the default authentication system, you need to prefix the user name by the Domain ID that was defined for the respective authentication system.

Users defined in the external directory are not automatically entitled to log on to CentraSite. You must explicitly create users accounts for valid users on CentraSite as described in the topic *Adding a User* in the section *About Users* in the document *Users, Groups, Roles and Permissions*.

For information about how to configure the authentication for CentraSite, see the document *Authentication Topics and LDAP*.

Note: Any change of the external user management is not synchronized with CentraSite. If a user is removed from the external user management (for instance on operating system level) the corresponding CentraSite user is not automatically deactivated. The CentraSite user associated with a deleted external user must be deactivated manually in CentraSite.

Active and Inactive Users

The users that you define in CentraSite can be *active* or *inactive*. An active user has an associated user account on the external authentication system and is permitted to log on to CentraSite. Inactive users exist in the registry, but they are not permitted to log on to CentraSite. Additionally, permissions cannot be granted to inactive users nor can ownership of assets be given to them (inactive users retain ownership of objects that already belong to them).

Administrators generally deactivate users that leave the company or otherwise cease to be valid users of the registry. Inactive users are also useful for representing individuals who figure prominently in your SOA environment, but are not direct users of CentraSite. For example, you might create users to represent individual members of a key steering committee. Although these individuals might never use CentraSite, by including them in the registry as users, you enable assets and other objects to be associated with those individuals. Furthermore, if the user definitions for these individuals include email addresses, an administrator can develop policies that send email alerts to these individuals when significant events occur in the registry. Points-of-contact for external entities such as suppliers and distributors are other individuals that you might want to model as inactive users.

Guest Users

CentraSite supports the concept of a *guest user*. Guests are users that can access the registry without a user account (i.e., they can log on to CentraSite as anonymous users). Generally, guest users are given read-only access to a controlled set of assets.

In CentraSite, the capabilities given to guests are determined by the set of permissions specified in the Guest role. By default, CentraSite allows a guest to use the Asset Catalog screens in CentraSite Control. When they use the Asset Catalog screens, guest can see any asset on which the system-defined group called "Everyone" has View permission. (In other words, when you want to give guest users the ability to see an asset, you grant View permission to the group Everyone.)

You can include additional permissions in the Guest role as is required by your site. You must do this with great care, of course. Any additional permissions you assign to this role will significantly increase the capabilities of an anonymous user.

For additional information about the Guest role, see ***System Roles and Their Permissions***.

Who Can Create and Manage Users?

To create and manage (i.e., view, edit and delete) users for an organization, you must belong to a role that has the "Manage Users" permission. Users in the Organization Administrator role have this permission, although an administrator can assign this permission to other roles.

Note: Users that belong to a role that includes the "Manage Organizations" permission have the "Manage User" permission by implication. Such users can create and mange users in the organizations to which their "Manage Organizations" permission applies.

Adding a User

- Re-Associating Users

Overview

You can add users toCentraSite in any of the following ways:

- Using the **Add User** button on the Users page as described in ***Adding an Individual User to CentraSite***. This procedure enables you to define a single user and associate that user with an account in the external authentication system.
- Using the **Bulk Load Users from External Source** button on the Users page as described in ***Adding a User Using the Bulk Load Option***. This procedure enables you to load multiple users from the external authentication system into CentraSite in a single step.
- Using the **Users** profile on the Edit Organization page as described in ***Adding Users from the Organization's Users Tab***. This procedure enables you to load one or more users from the external authentication system into CentraSite in a single step.

Important: Do not begin adding users to CentraSite until after you configure CentraSite for the external authentication system that you intend it to use.

When you add a new user to CentraSite, keep the following points in mind:

- When you add a user from Active Directory or LDAP, CentraSite automatically populates many of the user's attributes in CentraSite with user information from the external authentication system. The exact set of attributes that CentraSite populates depends on how the user attributes in CentraSite have been mapped to the user properties in the external authentication system. For more information about mapping attributes, see the document *Authentication Topics and LDAP*.
- A user can belong to only one organization.
- Every user that you add to CentraSite automatically becomes a member of the Everyone group. This group represents the set of all users defined on CentraSite, including the guest user.
- If the user that you add has an associated user account on the external authentication system, CentraSite also does the following:
  - It adds the user to the following system-defined groups

Group	Description
Users	All users that belong to the user's organization.
Members	All users belonging to the user's organization or any of its descendants (i.e., children, children's children and so forth).

  - It assigns the Asset Consumer and Asset Provider roles to the user. (An administrator can modify these automatic role assignments, so the default role assignments for your organization might be different.)

- It activates the user, i.e., it allows the user to log on to CentraSite components such as CentraSite Control, using the user ID and password stored in the external authentication system.

Adding an Individual User to CentraSite

Use the following procedure to add an individual user to an organization and optionally associate that user with an account in the external authentication system.

To add an individual user to CentraSite

1 In CentraSite Control, go to **Administration > Users > Users**.

2 Click **Add User**.

3 In the **Organization** field, specify the organization to which you want to add the user. (The drop-down list only displays organizations for which you have "Manage Users" permission.)

4 Click **Associate** to select the user that you want to add from the external authentication system. (Skip this step if the user you are adding to CentraSite represents an individual that will not log on to CentraSite).

- If CentraSite is configured to authenticate users using the local OS user database and you need procedures for this step, see ***Selecting Users from the Local OS User Database***.
- If CentraSite is configured to authenticate users using Active Directory or LDAP and you need procedures for this step, see ***Selecting Users from an Active Directory or LDAP Server***.

Note that you can only search for users that are stored in the same repository as the user who is logged into CentraSite Control and is performing the current operation. For example, if your system has both internal users and LDAP users, an internal user cannot search for users that are stored in the LDAP repository.

5 Complete the following fields as necessary. (If you selected the user from an Active Directory or LDAP system, many of these fields will already be populated.)

In this field...	Do the following...
First Name	Specify the first name of the user.
Middle Name	*Optional*. Specify the middle name of the user.
Last Name	Specify the last name of the user.
E-mail Address	*Optional*. Specify the user's e-mail address. **Note:** Including an email address for a user makes it possible for CentraSite to notify the user of certain events using email.

6 On the **Address Information** tab, specify the following:

In this panel...	Do the following...
Address	*Optional*. Specify the user's address information.
Contact	*Optional*. Specify the phone and fax numbers for the user. You can specify multiple phone and fax numbers.

7 If you have any custom properties (key-value pairs) that you want to specify for the user, select the **Object-Specific Properties** profile and specify the key-value pairs as follows:

1. Click the **Add Property** button.
2. In the **Add Object-Specific Properties** dialog box, enter the name of the property and value for the property. You can add multiple values for a single property.
   - The name of the property can consist of letters, numbers and the underscore character (_). It cannot contain a space or other special characters.
   - You can optionally supply a namespace for the property.
3. Click **OK**.

8 If an administrator has added custom attributes to the User type definition, select the **Attributes** profile and specify the attributes as necessary. Attributes that are marked with an asterisk (*) are required. You must at least specify all required attributes.

Note: You will see the **Attributes** profile only if an administrator has added custom attributes to the User type definition.

9 Click **Save** to save the new user.

10 Update the **Groups** profile as necessary to add the user to additional groups. For procedures, see *Adding a User to a Group*.

11 Update the **Roles** profile as necessary to assign additional roles to the user. For procedures, see *Assigning Roles to a User*.

Selecting Users or Groups from the Local OS User Database

The following procedure describes how to use CentraSite's standard dialogs to search for users or groups in the local operating system's user database.

Keep the following points in mind when performing a search:

- This dialog opens to an empty list. You must type a search string to retrieve a list of users or groups. To retrieve all the users or groups, leave the **Search** field empty and click **Search.**
- Search strings are not case-sensitive .The search string “bar”, for example, will find “BAR” and “Bar”.
- Search strings are not accent-sensitive.

- When you are searching the user list, CentraSite searches the user ID attribute, not the user name attribute. Thus, if a user has the user ID "MyDomain\AdminUser01" and the name "John Smith", a search for "Admin" will find the user, whereas a search for "John" will not.
- CentraSite does a “starts with” search on the user ID or group name. *The domain portion of the name is not included in the search*. Thus, if a user has the user ID "MyDomain\AdminUser01", a search for "Ad" will find the user, whereas a search for "User01" or "My" will not.
- You can type the wildcard characters % or * alone in the Search field to retrieve the list of all users or groups. However, you cannot combine these wildcard characters with other character sequences. The sequences “xx%” and “%xx”, for example, are not valid search strings.
- CentraSite automatically filters out users that have already been added to CentraSite. For example, if the local machine has users CH001 and CH002, and user CH001 has already been added to CentraSite, a search for users starting with CH, will return user CH002, but not user CH001.

To search the local OS user database

1 In the **Search** field, type a search string that specifies the characters with which the user ID begins. The following are examples.

If you type...	CentraSite will return...
b	User IDs that begin with b.
bar	User IDs that begin with bar.
%	All user IDs.
*	All user IDs.
`emptyString`	All user IDs.

2 Click **Search.**

3 Repeat steps 1 and 2 until you obtain a list that contains the users that you want to add to CentraSite.

4 Select the users or groups that you want to add to CentraSite.

5 If the user that you want to add to CentraSite is not known to the local system, but is known to a domain server to which the local operating system is connected, type the user’s domain-qualified name into the **Type Domain Name field**. (This field is not available in all versions of this dialog.)

Note: If you type a user ID in the **Type Domain Name** field, CentraSite ignores any selections you have made in the user list.

6 Click **OK**.

Selecting Users or Groups from an Active Directory or LDAP Server

The following procedure describes how to use the standard dialogs to search for users or groups in an Active Directory or an LDAP server.

Keep the following points in mind when performing a search:

- CentraSite treats the text you enter as a partial string. For example, if you enter "al", then "Alex", "Allen" and "Salie" all fit the search criteria.
- You can use the asterisk (*) as a wildcard in the search text. CentraSite replaces the wildcard symbol with as many characters as necessary.
- Searches are not case sensitive.
- Searches are not accent-sensitive.
- The ADS or LDAP authentication system performs a user search based on the attribute mapping specified in the authentication configuration, and displays the users that fit the search criteria. See the section *Creating Authentication Configurations* in the document *Authentication Topics and LDAP* for more information about authentication configurations.

To search an Active Directory or LDAP server

1. In the **Search Criteria** panel, create the search criteria by selecting the attribute and the condition from the respective list boxes and typing the search string in the text box.
2. Select a search operator: “Equals” and “NotEquals”. The “Equals” tests for attributes that are equal to a certain value. The “NotEquals” finds for attributes that do not have the same or equal value.
3. For advanced search using multiple attribute conditions, click the plus button and add a new condition for the search.
4. Specify the way in which the criteria are to be combined:
   - To specify that a user or group must meet all criteria to be considered a match, select **AND Condition**.
   - To specify that a user or group must meet at least one of the criteria to be considered a match, select **OR Condition**.
5. Click **Search**.
6. Select the users or groups you would like to add to the organization.
7. Click **OK**.

Bulkloading Users from the External Authentication System

You use the following procedure to add multiple users from the external authentication system to CentraSite in a single step. You can specify which organization you want to add the users to.

To bulkload users into CentraSite

1 In CentraSite Control, go to **Administration > Users > Users**.

2 Click **Bulk Load Users from External Source**.

3 In the **Bulk Load Users from External Source** dialog box, select the users that you want to add to CentraSite.

- If CentraSite is configured to authenticate users using the local OS user database and you need procedures for this step, see ***Selecting Users or Groups from the Local OS User Database***.
- If CentraSite is configured to authenticate users using Active Directory or LDAP and you need procedures for this step, see ***Selecting Users or Groups from an Active Directory or LDAP Server***.

4 In the field **Import to Organization**, specify the organization into which the users will be added.

5 Scroll through the user list to confirm that the selected users were added successfully.

6 Examine each new user that you added to the specified organization and update the user's attributes as necessary. (If you selected users from an Active Directory or LDAP system, many of the new users' attributes will already be populated.)

Adding Users from the Organization's Users Tab

You use the following procedure to add one or more users to CentraSite from your external authentication system.

To use this procedure, you must have "Manage Organizations" permission on the organization to which you want to add users.

To add users from an organization's Users tab

1 Open the Edit Organization page. If you need procedures for this step, see the section *Viewing or Editing the Attributes of an Organization* in the document *Managing Organizations*.

2 Select the **Users** profile and click **Add Users**.

3 In the **Add Users** dialog box, select the users that you want to add to CentraSite.

- If CentraSite is configured to authenticate users using the local OS user database and you need procedures for this step, see ***Selecting Users or Groups from the Local OS User Database***.
- If CentraSite is configured to authenticate users using Active Directory or LDAP and you need procedures for this step, see ***Selecting Users or Groups from an Active Directory or LDAP Server***.

4 Scroll through the user list to confirm that the selected users were added successfully.

5 Click **Save** to save the updated organization.

6 Examine each new user that you added to the organization and update the user's attributes as necessary. (If you selected users from an Active Directory or LDAP system, many of the new users' attributes will be populated already.)

Re-Associating Users

Overview

If you have associated a CentraSite user with an external user, you may wish to change the association to a different external user.

This can be required, for example, if the responsibility for certain CentraSite assets moves from one person to another person in the same authentication domain. By reassociating the user, you can keep the name of the CentraSite user unchanged while changing to a new external owner.

Another possible use would be to handle user IDs when the default domain name changes, e.g. when switching from operating system authentication to LDAP authentication.

CentraSite provides a command line tool *ReassociateUsers* that allows you to reassociate one or more CentraSite users with new external user IDs. The script implemented as an executable jar and can only be run by a user who has the CentraSite Administrator role.

This command line tool reassociates CentraSite users with new external user IDs. Any permissions that were granted for the old external user ID will be modified to grant those permissions for the new external user ID.

Usage

Before you run the command line tool, create a database backup.

The tool consists of an executable jar file in the *bin* folder of the CentraSite installation. It requires a Java 6 runtime and needs to be called in the following way:

```
java -jar ReassociateUsers.jar <CentraSite DB URL>
<administrator user id> <password> <old user id> <new user id> ↩
```

or

```
java -jar ReassociateUsers.jar <CentraSite DB URL>
<administrator user id> <password> <mapping file name>
```

For example:

```
java -jar ReassociateUsers.jar "http://localhost:53307/CentraSite/CentraSite"
DOMAIN\admin pAsSwOrD OLDDOMAIN\oldUser NEWDOMAIN\newUser ↩
```

The first form (5 arguments) is for reassociating a single user, whereas the second form (4 arguments) is for reassociating multiple users in one execution of the tool.

When using the second form, the fourth argument specifies a text file that contains the user IDs. Each line of the mapping file contains one comma-separated pair of old and new user ID. A user ID must not occur more than once in these mappings.

The tool first checks for the following preconditions, which must all be met, otherwise the tool stops and no users will be reassociated:

- there is a unique registry object for the old user ID
- the old user ID can be uniquely identified in the security configuration
- there is no registry object for the new user ID
- there is no security configuration for the new user ID
- the reassociated user is a login user
- the reassociated user is not the CentraSite administrator user who is running the utility
- the domain of the new user ID must exist in the security configuration
- a GUI configuration does not exist for the new user ID

If all preconditions are met, the tool performs the reassociation. This process may take some time. The tool progress is reported to standard output.

Viewing the Users List

You use the Users page to view the list of users defined on CentraSite.

To view the users list

1 In CentraSite Control, go to **Administration > Users > Users** to view the list of all users that are defined in CentraSite.

Or:

Go to the Edit Organization page and choose the **Users** profile to view the list of users in that particular organization. If you need procedures for this step, see the section *Viewing or Editing the Attributes of an Organization* in the document *Managing Organizations*.

2 If you want to filter the list, type a partial string in the **Search** field. CentraSite applies the filter to the **Name** column.

If you type...	CentraSite Displays
`b`	Names that contain "b"
`bar`	Names that contain "bar"
`%`	All names

The users list provides the following information about each user:

Column	Description	
Name	The name of the user.	
User ID	The log in ID of the user.	
Organization	The name of the organization to which the user belongs.	
Can Log On	The status of the user.	
	Icon	**Description**
		The user is active (can log on to CentraSite).
		The user is inactive (cannot log on to CentraSite).

Viewing or Editing Information about a User

You use the Edit User page to examine or modify information about a user.

Note: Changing the value of the **Organization** field moves the user to the specified organization (without moving the user's assets). You can only change this field if you belong to the CentraSite Administrator role. For information about how CentraSite processes the movement of a user to another organization, see *Moving a User to a Different Organization*.

To view or edit a user information

1 In CentraSite Control, go to **Administration > Users > Users**.

2 On the Users page, locate the user whose details you want to view or edit.

3 From the user's context menu, select the **Details** command.

4 View or edit the attributes on the Edit User page as necessary. For additional information about the attributes on this page, see the relevant steps in *Adding an Individual User to CentraSite*.

5 If you have made any changes to the users, click **Save**.

You can view details for multiple users as follows:

To view details for multiple users

1 In CentraSite Control, go to **Administration > Users > Users**.

2 Mark the checkboxes of the users whose details you want to view.

3 In the **Actions** menu, click **Details**.

The **Details** view of each of the selected users is now displayed.

Adding a User to a Group

Use the following procedure to add a user to or remove a user from a locally managed group (i.e., a group whose membership is defined within CentraSite, not on the external authentication system).

To add a user to a group

1 Open the Edit User page for the user whose group assignments you want to edit. If you need procedures for this step, see *Viewing or Editing Information about a User*.

2 On the Edit User page, choose the **Groups** profile and do the following:

- To add a user to a group, click **Add User to Group** and select the groups to which you want to add the user.
- To remove a user from a group, select the groups from which you want to remove the user and click **Remove**.

Note: You cannot remove the user from any of the system-defined groups.

3 Click **Save**.

Assigning Roles to a User

Use the following procedure to assign a role to or remove a role from a user.

To assign roles to a user

1 Open the Edit User page for the user whose role assignments you want to edit. If you need procedures for this step, see *Viewing or Editing Information about a User*.

2 In the Edit User page, choose the **Roles** profile and do the following:

- To assign roles to the user, click **Assign Role** and select the roles that you want to give to the user.
- To remove roles assigned to a user, select the roles that you want to remove and click **Remove**.

3 Click **Save**.

Viewing the Assets Available to a User

Use the following procedure to display the list of assets that a particular CentraSite user owns.

To view a user's assets from the Edit User page

1 Open the Edit User page for the user whose role assignments you want to edit. If you need procedures for this step, see *Viewing or Editing Information about a User*.

2 In the Edit User page, choose the **Assets** profile, which displays the list of assets that the user currently owns.

Activating or Deactivating a User

CentraSite Control offers the ability to activate or deactivate a user.

Activating a user account changes its status to Activated and allows the user to log on to CentraSite Control. Deactivating a user account changes its status to Deactivated and denies the user the privilege to log on to CentraSite.

A deactivated user cannot be assigned permissions, execute policies or become owner of the new assets. Also, the deactivated user cannot be a part of the approval group. Furthermore, if a user who was part of an approval group or a user who is the only member of the approval group is deactivated, the policy with that particular approval group is itself marked as fail.

You usually deactivate a user to prevent that user from logging on to CentraSite (temporarily or permanently). You must also deactivate a user account in order to delete it.

When you activate or deactivate a user, keep the following points in mind:

- You cannot deactivate the only remaining user in the CentraSite Administrator role in the CentraSite registry/repository or the only remaining user in the Organization Administrator role within an organization.
- You cannot deactivate the user who is an authorized approver for an approval flow that is in the Pending state.

You can activate or deactivate users in any of the following ways:

- From the Users page.
- From the Edit User page.
- From the Edit Organization page.

To activate or deactivate a user via the Users page

1 In CentraSite Control, go to **Administration > Users > Users**.

2 On the Users page, enable the checkbox next to the name of the user that you want to activate or deactivate. (You can select multiple users.)

3 From the **Actions** menu, choose **Activate** or **Deactivate** as needed.

4 Verify that the user's state has changed by checking the icon in the **Can log on** column.

Icon	Description
	The user is active (can log on to CentraSite Control).
	The user is inactive (cannot log on to CentraSite Control).

To activate or deactivate a user via the Edit User page

1 Open the Edit User page for the user whom you want to activate or deactivate. If you need procedures for this step, see *Viewing or Editing Information about a User*.

2 In the Edit User page, click the **Activate User** or **Deactivate User** button as needed.

To activate or deactivate a user via the Edit Organization page

1 Open the Edit Organization page for the organization to which the user belongs. If you need procedures for this step, see the section *Viewing or Editing the Attributes of an Organization* in the document *Managing Organizations*.

2 On the Users tab, enable the checkbox next to the name of the user that you want to activate or deactivate. (You can select multiple users.)

3 From the **Actions** menu, choose **Activate** or **Deactivate** as needed.

Deleting a User

Deleting a user permanently removes a user from the CentraSite registry/repository. When deleting a user, keep the following points in mind:

- You cannot delete an active user. You must deactivate the user before you delete it. For procedures, see *Activating or Deactivating a User*.
- You cannot delete a user if any of the following conditions exist:
  - The user functions as the primary contact of an organization.
  - The user owns one or more assets in CentraSite.
- Deleting a user from CentraSite does not delete the user from the external authentication system.
- Make sure that at least one active user with the CentraSite Administrator role *always* resides in the Default Organization. Even if you plan to switch CentraSite's user authentication from one domain to another (such as, from the OS to an Active Directory or LDAP domain), to prevent a system lockout, make sure you have at least one user in the CentraSite Administrator role defined on CentraSite.

To delete a user

1 In the CentraSite Control, go to **Administration > Users > Users** to display the users list.

2 Ensure that the user is inactive (see **Activating or Deactivating a User**).

3 Enable the checkbox next to the name of the user that you want to delete.

4 Click **Delete**.

When you are prompted to confirm the delete operation, click **OK**.

User is permanently removed from the CentraSite registry/repository. If the user had an associated user account in the external authentication system, that account is not affected.

You can delete multiple users in a single step. The rules described above for deleting a single user apply also when deleting multiple users.

Important: If you have selected several users where one or more of them are predefined users (such as bootstrap user, for example), you can use the **Delete** button to delete the users. However, as you are not allowed to delete predefined users, only users you have permission for will be deleted. The same applies to any other users for which you do not have the required permission.

To delete multiple users in a single operation

1 In CentraSite Control, go to **Administration > Users > Users** to display the policy list.

2 Ensure that the users are inactive (see **Activating or Deactivating a User**).

3 Mark the checkboxes of the users that you want to delete.

4 From the **Actions** menu, choose **Delete**.

When you are prompted to confirm the delete operation, click **OK**.

Each selected user is permanently removed from the CentraSite registry/repository. If the user had an associated user account in the external authentication system, that account is not affected.

Command Line Tool for Deleting a User

In some circumstances, a user object cannot be deleted using the method described in the section **Deleting a User** above, because internal objects that reference the user object cannot be deleted. It can happen, for example, that there are internal references to a user object even though the user is no longer the owner of any assets. There can also be references to the user object in the audit log. In such circumstances, a user object can only be deleted by using a Java command line tool *DeleteUser* provided specifically for this purpose.

Important: This tool is for use by administrators only, and should only be used if the method described in **Deleting a User** is not successful. In particular, the tool does not activate any policies that you might have defined.

This command line tool deletes a user, after transferring ownership of all of the user's objects to another user (the "target" user). It also redirects to the target user all associations that referred to the user to be deleted. Any ACLs granting rights for the user to be deleted will be modified to grant those rights to the target user. If the user to be deleted was the primary contact of an organization, the target user will be assigned that role.

To make the ownership transfer visible in the audit logs, an "OWNERSHIPTRANSFERRED" event is created for every registry object that references the user object. The description of the auditable event includes the original owner and states that a delete user operation has been executed.

The tool's combined operation performs the following steps:

- Transfer ownership of objects to the target user
- Redirect internal references to the target user
- Transfer access rights to the target user
- Transfer group memberships to the target user
- Remove the GUI configuration
- Remove the user object

The tool consists of an executable jar file in the *bin* folder of the CentraSite installation. It requires a Java 6 runtime and needs to be called in the following way:

```
java DeleteUser <CentraSite DB URL> <administrator user id> <password> <id or key ↩
of user to be deleted> <id of target user>
```

Examples:

```
java DeleteUser
     "http://localhost:53307/CentraSite/CentraSite" DOMAIN\admin pAsSwOrD
     DOMAIN\oldUser DOMAIN\newUser
```

```
java DeleteUser
     "http://localhost:53307/CentraSite/CentraSite" DOMAIN\admin pAsSwOrD
     uddi:1e5aff10-f3e3-11df-86fc-a6e2fa0ea483 DOMAIN\newUser ↩
```

Please note that the target user must be active before using this tool. The user to be deleted must be deactivated.

Restrictions

The operation to delete a user requires several steps that cannot run within a single transaction. This means every parallel running transaction will be able to see intermediate results. Therefore please ensure that no other activity is in progress while you run the tool. Moreover if there is a failure of any of the steps during the execution, the registry will have an intermediate state. The original state cannot be recovered by rolling back the complete operation.

Moving a User to a Different Organization

The organization to which a user belongs determines, among other things, the organization to which the user's assets are published (by default) and the organization whose asset catalog the user can view (by default).

If a user transfers to a department or work group in another organization within your enterprise, you use the **Move** command to mirror that change in CentraSite. When you move a user to another organization, you can also move the user's assets to the target organization or you can leave them with their current organization.

Who Can Move a User?

To move a user to another organization, you must belong to the CentraSite Administrator role.

What Happens When You Move a User to Another Organization?

When you move a user to another organization, CentraSite does the following:

- Records the user's organization change in the audit log.
- Removes the user from the system groups in the user's former organization and adds the user to the system groups in the target organization.
- Triggers pre- and post-update policies on the User object as appropriate (see below).
- Transfers the assets that the user owns to the target organization (if specified).

- Sends a notification to the inbox of the moved user when the move is complete.

The following sections describe the effect that an organization change has on various aspects of a user. Before transferring a user to another organization, review this information so you understand how the user will be affected.

Effect of Moving a User on the Groups to Which the User Belongs

When you move a user to another organization, the user is removed from the following system groups in his or her former organization and added to these groups in the target organization:

- Users
- Members

The user retains all other group memberships.

Effect of Moving a User on the User's Access to Assets

Members of the Users group for an organization have implicit View permission on the organization's assets. Because CentraSite transfers users from one Users group to another during a move, the moved users lose implicit access to the assets in their former organization (except for the assets that they own) and receive implicit access to the assets in the target organization. If users require continued access to the assets in their former organization, consider granting the Asset Consumer role (in the former organization) to them after the move.

Important: If there are any explicit instance-level or role-based permissions assigned to the Users and/or Members groups in their former organization, be aware that users will also lose those permissions when they leave the organization.

Moving users to another organization does not affect any instance-level permissions or role-based permissions that are granted directly to their user accounts or to any non-system groups (i.e., groups besides Users and Members) to which they belong. Therefore, other than losing access to certain assets as a result of leaving the Users and/or Members groups in their former organization, users continue to have access to the same set of assets as they had before the move.

Effect of Moving a User on the User's Assigned Roles

When you move users to another organization, they lose the roles that were assigned to the Users and/or Members groups in their former organization and gain the roles that are assigned to the Users and/or Members groups in the target organization. Other than this change, users retain all of their other role assignments.

Transferring Inactive Users

You can transfer active or inactive users.

Users That You Cannot Move

You cannot move the default user or any other internal user that is installed by CentraSite.

Moving the User's Assets to the New Organization

When you move a user to another organization, you can optionally move all of the user's assets to the target organization at the same time. If you choose to do this, CentraSite will process the transfer of those assets as described in the section *Changing the Ownership of an Asset* in the document *Using the Asset Catalog*.

Note: Transferring a user and the user's assets is an "all or nothing" operation. If the transfer of any one asset fails, neither the user nor the user's assets are moved.

Policies That are Triggered When You Move a User

CentraSite treats the move operation as an update to the User object. Thus, moving a user to a different organization triggers the execution of pre-update and/or post-update policies that apply to User objects. If a pre-update policy fails, the user is not moved into the target organization.

Note: It is the policies of the *target organization* that CentraSite applies to the move.

How to Move a User to Another Organization

This section provides procedures for moving a user to another organization. (Note that the following contains procedures for transferring an individual user and for transferring multiple users.)

Moving an Individual User

Use the following procedure to move an individual user to a specified organization.

To move an individual user

1 In CentraSite Control, go to **Administration > Users > Users**.

2 Locate the user that you want to move, and from its context menu, select **Move**.

3 In the **Move User(s)** dialog box, select the organization to which you want to move the user.

If you want to filter the organization list, type a partial string in the search field.

4 **Note:** If you want CentraSite to also transfer the assets owned by the selected user, enable the **Move Assets owned by the selected user(s) to the new organization** option.

If you do not enable this option, the user's existing assets will remain in the organization to which they are currently assigned (the transferred user will continue to serve as their owner).

5 Click **OK**.

Note: You can also move a user from the **Users** tab on the Edit Organization page and from the **Organization** field on the Edit User page. (Be aware that if you move a user using the **Organization** field on the Edit User page, you cannot move the user's assets at the same time.)

Moving Multiple Users (Bulk Transfer)

Use the following procedure to move multiple users to a specified organization.

Important: If you have selected several users where one or more of them are predefined users (such as bootstrap user, for example), you can use the **Move** button to transfer the ownership of all of the selected users. However, as you are not allowed to transfer ownership of predefined users, only users you have permission for will be transferred.

To move multiple users

1 In CentraSite Control, go to **Administration > Users > Users**.

2 Select the users that you want to move to a particular organization.

3 Click the **Actions** link and select **Move**.

4 In the **Move User(s)** dialog box, select the organization to which you want to move the selected users.

If you want to filter the organization list, type a partial string in the search field.

5 If you want CentraSite to also transfer the assets owned by the selected users, enable the **Move Assets owned by the selected user(s) to the new organization** option.

If you do not enable this option, the assets will remain in the organizations to which they are currently assigned (the transferred users will continue to function as owners of the assets even though the assets are not transferred to the target organization).

6 Click **OK**.

Note: You can also move multiple users using the **Actions** link on the **Users** tab on the Edit Organization page.

2 About Groups

A *Group* describes a set of CentraSite users. The group always belongs to exactly one organization, but can contain users from different organizations. Groups are visible to all users.

A group can either be managed locally within CentraSite or can be imported from the external authentication system.

Groups can be used for many purposes within CentraSite, including:

- Granting roles to specified groups of users.
- Granting instance-based permissions to specified groups of users.
- Identifying the set of users who can approve certain types of requests.
- Identifying the users to which a particular policy action is to be applied.

CentraSite has three main types of groups:

- *System groups* are shipped with CentraSite. When a user is added to CentraSite, CentraSite automatically adds the user to a specified system group depending on the organization to which the user belongs. And when the user is deleted, CentraSite automatically removes that user from the group. The membership of these groups cannot be manually updated or deleted by an administrator. For more information, see ***System Groups***.
- *Locally managed custom groups* are user-defined groups that are defined and maintained within CentraSite.
- *Externally managed custom groups* are user-defined groups that are imported from the external authentication system.

System Groups

The membership of the following system groups is managed automatically by CentraSite. When you add a new user to CentraSite, CentraSite automatically adds the user to these system groups. When you delete a user from CentraSite, CentraSite automatically deletes the user from these groups. You cannot delete or edit the membership of these groups yourself. You can, however, assign roles and instance-level permissions to these groups.

This system group...	Contains...
Everyone	All users.
Users	All users in an organization. Each organization in the registry/repository has a Users group. By default, the Asset Provider and Asset Consumer roles are assigned to this group, which gives these roles to every user in the organization.
Members	All users in an organization or any of its descendant organizations (children, children's children and so forth) Each organization in the registry/repository has a Members group.

Custom Groups

Custom groups are groups that you define in CentraSite. A custom group can contain users from any organization in the registry/repository.

You can create a custom group of any one of the following types in CentraSite:

- **An externally managed custom group.**
  This is a group that is imported from the external authentication system. You cannot manually change the membership of such a group within CentraSite; CentraSite maintains the membership of an externally managed custom group by automatically synchronizing with the external authentication system.

  After an externally managed group is created, you cannot switch the group to a "locally managed" type of group, nor can you associate it with a different group on the external authentication system.

  If the external group includes members who are not existing users of CentraSite, those members will not become CentraSite users as a result of adding the group to CentraSite. If you subsequently add those individuals to CentraSite, however, they will automatically become members of this group.
- **A locally managed custom group.**
  This is a group that consists entirely of users who are registered in CentraSite. The users must be active users (see the section ***Active and Inactive Users*** for details).

  The membership of the group is maintained in CentraSite. You can perform administrative tasks manually on the group in CentraSite, such as adding or removing users from the group.

  If you have a locally managed group, you can switch it to an externally managed group. See the section ***Adding an Externally Managed Custom Group to CentraSite*** for details.

CentraSite supports static groups and nested groups.

Note: If you are using LDAP, note that only the "recurse up" option is supported for group resolution. The "recurse down" option is not supported.

External Group Synchronization

When you import a group from CentraSite's external authentication system, CentraSite fetches the group's details from the authentication system and automatically synchronizes (updates) the group's membership on CentraSite.

Group synchronization occurs in the following cases:

- **When you initially import a group from the external authentication system**
  This creates an externally managed custom group in CentraSite. When such an externally managed custom group is created, CentraSite queries the external system to determine which members of the group are registered users in CentraSite. Those users become members of the externally managed custom group on CentraSite.
- **When you add a user to CentraSite from the external authentication system**
  Whenever a new user is added from the external authentication system, CentraSite queries the external system to determine in which groups the user is a member. If any of those groups have been imported into CentraSite, the user is automatically added to the corresponding groups in CentraSite.
- **When a user is deleted from a group in the external authentication system**
  The removal of a user from a group can be done only in the external authentication system, and the change will be reflected in CentraSite when the synchronization occurs.

Example

Assume that the users User1, User2, User3, User4 and User5 are defined on the external authentication system, and do not belong to any group on the external authentication system. Assume that all of these users except User1 have already been imported from the external authentication system to CentraSite, but do not yet belong to any group in CentraSite. Now assume that a group called GroupA is created in the external authentication system, and GroupA has members User1, User2 and User3.

If GroupA is imported to CentraSite, the registered CentraSite users User2 and User3 become members of GroupA in CentraSite, as the membership of the group is maintained in external authentication system (User 1 is not registered in CentraSite, therefore it is not available as a member in Group A). We cannot add more users manually to GroupA in CentraSite, since CentraSite just refers to the external authentication system for the membership details. However, if User4 and User5 are added to GroupA in the external authentication system, they also become members of the GroupA in CentraSite when the automatic synchronization occurs.

In this scenario, User1 is not yet a member of GroupA in CentraSite, since User1 is not a registered user in CentraSite. To add User1 to the group in CentraSite, you need to define User1 as a user in CentraSite and associate this user with GroupA in the external authentication system.

Who Can Create and Manage Groups?

To create and manage (i.e., view, edit and delete) groups for an organization, you must belong to a role that has the "Manage Users" permission for the organization. Users in the Organization Administrator role have this permission, although an administrator can assign this permission to other roles.

Note: Users that belong to a role that includes the "Manage Organizations" permission have the "Manage User" permission by implication. Such users can create and mange groups in any organization to which their "Manage Organizations " permission applies.

Creating Custom Groups

There are three ways in which you can create custom groups in CentraSite:

- To create a locally managed group, see *Adding a Locally Managed Custom Group Using the Add Group Button*.
- To create an externally managed group, see *Adding an Externally Managed Custom Group to CentraSite*.
- To import multiple groups from the external authentication system, see *Bulk Loading Groups from the External Authentication System*.

Adding a Locally Managed Custom Group to CentraSite

Use the following procedure to add a locally managed custom group to CentraSite.

To create a locally managed group

1 In CentraSite Control, go to **Administration > Users > Groups**.

2 Click **Add Group**.

3 In the **Group Information** panel, specify the following fields:

In this field...	Do the following...
Name	Enter a name for the new group. A group name can contain any character (including spaces). **Note:** The group name must be unique within an organization.
Description	*Optional*. Enter a short description for the new group. This description appears when a user displays the list of groups on the CentraSite Control.

In this field...	Do the following...
Organization	Specify the organization to which this group belongs. (The drop-down list only displays organizations for which you have "Manage Users" permission.) **Important:** Choose the organization carefully. You cannot change this assignment after the group is created.

4 To add users to the group, do the following:

1. Click **Add User**.
2. Select the users that you want to add to the group.

   If you want to filter the list, type a partial string in the **Search** field. CentraSite applies the filter to the **Name** column.

If you type...	CentraSite displays...
b	Names that contain "b"
%	All names

3. Click **OK**.

5 Update the **Roles** profile as necessary to assign roles to this group. If you need procedures for this step, see *Assigning Roles to a Group*.

Important: Verify that the **Organization** field specifies the correct organization for this group before you proceed to the next step.

6 Click **Save**.

Adding an Externally Managed Custom Group to CentraSite

Use the following procedure to add an externally managed custom group to CentraSite.

When performing this procedure, keep the following points in mind:

- You do not need to assign a name to the group. The group name will be imported from the external authentication system. (If you assign a name in the group's **Name** attribute, it will be overwritten.)
- Do not assign users to the group using the **Users** tab. The members of this group will be specified by the external authentication system. (If any users appear on the **Users** profile when you perform this procedure, those users will be removed from the group.)
- If you have a locally managed group that you would like to switch to an externally managed group, you can open the group and then execute the following procedure starting with step 4.

Be aware, however, that the group's current name and membership will be replaced by the name and membership of the imported group.

To create an externally managed custom group

1 In CentraSite Control, go to **Administration > Users > Groups**.

The Groups page displays the list of system and custom groups for which you have permission.

2 Click **Add Group**.

3 In the **Organization** field, specify the organization to which this group belongs. (The drop-down list only displays organizations for which you have "Manage Users" permission.)

> **Important:** Choose the organization carefully. You cannot change this assignment after the group is created.

4 Click **Associate**.

5 In the **Associate Group** dialog box, select the groups that you want to add to CentraSite.

- If CentraSite is configured to authenticate users using the local OS user database and you need procedures for this step, see *Selecting Users or Groups from the Local OS User Database*.
- If CentraSite is configured to authenticate users using Active Directory or LDAP and you need procedures for this step, see *Selecting Users or Groups from an Active Directory or LDAP Server*.

> **Important:** Choose the external group with care. You cannot change this association after the group is created.

6 In the **Description** field, specify a descriptive comment or remark (optional).

7 Update the **Roles** profile as necessary to assign roles to this group. If you need procedures for this step, see *Assigning Roles to a Group*.

8 Click **Save**.

Bulk Loading Groups from the External Authentication System

You use the following procedure to add groups through the bulk load option. By this procedure, you can add one or more group(s) in a single step to your organization or to another specified organization.

To create group(s) and save it to CentraSite

1 In CentraSite Control, go to **Administration > Users > Groups**.

CentraSite displays the list of groups for which you have permission.

2 Click the **Bulk Load Groups from External Source** button.

3 In the **Bulk Load Groups from External Source** dialog box, select the groups that you want to add to CentraSite.

- If CentraSite is configured to authenticate users using the local OS user database and you need procedures for this step, see ***Selecting Users or Groups from the Local OS User Database***.
- If CentraSite is configured to authenticate users using Active Directory or LDAP and you need procedures for this step, see ***Selecting Users or Groups from an Active Directory or LDAP Server***.

4 In the field **Import to Organization**, specify the organization into which the groups will be added.

5 Scroll through the groups list to confirm that the groups you selected were added successfully.

6 Examine each new group and update its **Description** field and its **Roles** profile as necessary.

Viewing the Groups List

You use the Groups page to view the list of groups.

To view the groups list

- In CentraSite Control, go to **Administration > Users > Groups** to view the list of all groups that exist in CentraSite.

  The Groups page provides the following information about each group:

Column	Description
Name	The name of the group.
Organization	The name of the organization to which the group belongs.
Description	A short description about the group.

Viewing or Editing the Attributes of a Group

You use the Edit Group page to examine and/or edit the attributes of a group. When editing a group, keep the following points in mind:

- You cannot modify the system-defined groups (i.e., Everyone, Users and Members).
- You cannot modify the name or membership of an externally managed group.

To view or edit the properties of a group

1 In CentraSite Control, go to **Administration > Users > Groups**.

2 Locate the group whose attributes you want to view or edit.

3 From the group's context menu, select the **Details** command.

4 Examine or modify the properties on the Edit Group page as required.

Field	Description
Name	The name of the group. A group name can contain any character (including spaces).
Description	Additional comments or descriptive information about the group.
Organization	*Read-only.*. The organization to which this group belongs.
Associated with External Group	The group on the external authentication system with which this group is managed. If an external group has already been associated with this group, this field cannot be modified. If an external group has not been associated with the group, you can use the **Associate** button to associate an external group with it. *Doing this will switch the group from a locally managed group to an externally managed group*. The group's current name and member ship will be replaced by the name and membership information from the external group.
Users	The settings on this profile identify the users that are assigned to the group. To edit this list, see *Modifying the Membership of a Group*
Roles	The settings on this profile identify the roles that are assigned to the group. To edit this tab, see *Assigning Roles to a Group*

5 If you have edited the settings on the Edit Group page, click **Save** to save the updated group.

Editing the Membership of a Group

Use the following procedure to modify the membership of a locally managed custom group.

Note: You cannot modify the membership of a system group or an externally managed group. System groups are automatically maintained by CentraSite. Externally managed groups are maintained by the administrators of the external authentication system.

To modify the membership of a group

1 Open the Edit Group page for the group whose membership you want to modify. If you need procedures for this step, see *Viewing or Editing the Attributes of a Group*.

2 On the Edit Group page, choose the **Users** profile and, do the following:

1. To add users to the group, click **Add User** and select the users that you want to add to the custom group. If you need procedures for this step, refer to the user-selection steps in *Adding a Locally Managed Custom Group to CentraSite*.
2. To remove users from the group, select the users that you want to remove and click **Remove**.

3 When you have finished your edits, click **Save** to save the updated group.

Assigning Roles to a Group

Assigning roles to a group confers the permissions associated with the role to each member of the group.

To assign roles to a group

1 Open the Edit Group page for the group whose role assignments you want to modify. If you need procedures for this step, see *Viewing or Editing the Attributes of a Group*.

2 On the Edit Group page, choose the **Roles** profile and do the following:

1. To assign roles to the group, click **Assign Role** and select the roles that you want to give to the group.
2. To remove roles from a group, select the roles that you want to remove and click **Remove**.

3 Click **Save** to save the updated group.

Deleting a Group

You use the Groups page to delete one or more custom groups. When deleting a group, keep the following points in mind:

- Deleting a group from CentraSite does not delete the associated group from the external authentication system.
- You cannot delete a system-defined group (not even if you belong to the CentraSite Administrator role).

To delete a group

1 In the CentraSite Control, go to **Administration > Users > Groups** to display the groups list.

2 Enable the checkbox next to the name of the group that you want to delete.

3 Click **Delete**.

When you are prompted to confirm the delete operation, click **OK**.

Group is permanently removed from the CentraSite registry/repository. If the group was associated with a group definition in the external authentication system, the group in the external system is not affected.

You can delete multiple groups in a single step. The rules described above for deleting a single group apply also when deleting multiple groups.

Important: If you have selected several groups where one or more of them are system groups, you can use the **Delete** button to delete the groups. However, as you are not allowed to delete predefined groups, only groups you have permission for will be deleted. The same applies to any other groups for which you do not have the required permission.

To delete multiple groups in a single operation

1 In CentraSite Control, go to **Administration > Users > Groups** to display the groups list.

2 Mark the checkboxes of the groups that you want to delete.

3 From the **Actions** menu, choose **Delete**.

When you are prompted to confirm the delete operation, click **OK**.

The selected group is permanently removed from the CentraSite registry. If the group was associated with a group definition in the external authentication system, the group in the external system is not affected.

3 About Roles and Permissions

In CentraSite, access control is enabled through a system of *roles* and *permissions*. A permission enables a user to perform a specified operation on a specified object. Permissions also enable users to work with specified parts of the CentraSite Control user interface. A role is a collection of permissions that can be assigned to an individual user or a group. The roles to which you belong and the permissions they includes dictate what portions of the CentraSite Control user interface you see, what objects you can work with, and what operations you can perform.

This section describes how you use permissions and roles to apply access control to the objects in your registry.

About Permissions

A permission enables a user to perform a specified operation on a specified object. Permissions also enable users to work with specified parts of the CentraSite Control user interface. It is largely CentraSite's system of permissions and roles that enables it to manage and maintain the separation of organizations in the registry.

Within CentraSite, there are two basic types of permissions: *instance-level permissions* and *role-based permissions.*

- Instance-level permissions enable access to one specific instance of an object. They provide very fine-grain control over objects in the registry. You can use an instance-level permission, for example, to give one specific user the ability to modify one particular asset in the catalog. *Instance-level permissions are granted directly to individual users or to groups.*
- Role-based permissions enable access to an entire class of objects or give users the ability to perform certain general operations in CentraSite. Role-based permissions provide coarse-grain control over the objects in the registry. You might use role-based permissions, for example, to allow a group of users to edit all of an organization's assets. Role-based permissions are not granted directly to individual users or groups. *Role based permissions are assigned to roles, and the roles are assigned to individual users or groups.*

Instance-Level Permissions

An instance-level permission enables access to:

- A specific instance of an object in the registry
- A specific folder in the repository
- A specific file in the repository

Instance-level permissions are granted at the following levels: View, Modify and Full.

The following table describes the capabilities that each level gives to a user. Note that each level of access inherits the capabilities of the preceding level. That is, each level implicitly includes the lower levels of access. In CentraSite's permission model, it is not possible to give a user delete permission without also giving that user modify permission. The Full permission, which enables a user to delete an object, implicitly gives the user Modify and View permissions as well.

Permission Levels on Registry Objects

This permission level...	Enables a specified user or group to do the following...
View	Read the object.
Modify	Read and edit the object; view the object's instance-level permissions.
Full	Read, edit and delete the object; modify the object's instance-level permissions.

Permission Levels on Repository Folders

This permission level...	Enables a specified user or group to do the following...
View	Read and browse the folder and its properties.
Modify	Read and browse the folder and its properties; create files and subfolders in the folder; view the folder's instance-level permissions.
Full	Read and browse the folder and its properties; create files and subfolders in the folder; delete files and subfolders in the folder; modify the folder's instance-level permissions.

Permission Levels on Repository Files

This permission level...	Enables a specified user or group to do the following...
View	Read the file and its properties.
Modify	Read and edit the files and its properties; view the file's instance-level permissions.

This permission level...	Enables a specified user or group to do the following...
Full	Read and edit the file and its properties; modify the file's instance-level permissions. **Important:** Full permission on a repository file does not give a user the ability to delete the file. Permission to delete a file is given only to those who have Full permission on the folder in which the file resides.

On Which Objects Can You Assign Instance-Level Permissions?

You can assign instance-level permissions to the following types of registry and repository objects:

- Assets (of any type)
- Design/change-time policies
- Run-time policies
- Report templates
- Taxonomies
- Repository folders
- Repository files

Implicit View Permissions on Registry Objects

CentraSite grants implicit View permission to all users on the following types of registry objects:

- Organizations
- Users
- Groups
- Roles
- Design/change-time policies
- Taxonomies

The View permission that CentraSite grants to users on these objects is permanent and irrevocable. It cannot be taken away from users through any instance-level or role-based permission.

Who Can Assign Instance-Level Permissions?

To assign instance level permissions to registry or repository objects, you must have Full permission on the object itself or belong to a role that includes a permissions that effectively grants you Full access to the object.

By default, a user has implicit (and irrevocable) Full permission on all of the objects that he or she owns. Consequently, the object owner is one user that is always permitted to set the instance-level permissions on an object.

How to Assign Instance-Level Permissions

For information about how to set instance-level permissions on registry and repository objects, see the following procedures in the CentraSite user documentation.

For procedures on...	See this section...
Assets	*Setting Permissions on an Asset*, in the document *Using the Asset Catalog*
Report templates	*Setting Permissions on a Report Template*, in the document *Working with Reports and Report Templates*
Design/change-time policies	*Setting Permissions on a Design/Change-Time Policy*, in the section *Functional Scope* in the document *Working with Design/Change-Time Policies*
Run-time policies	*Setting Permissions on a Run-Time Policy*, in the document *Working with Run-Time Policies*
Taxonomies	*Setting Permissions on a Taxonomy*, in the document *Taxonomies*

Role-Based Permissions

Role-based permissions enable access to an entire set of objects or give users the ability to perform certain operations in CentraSite. Unlike instance-level permissions, which are assigned directly to individual users or groups, role-based permissions are assigned to roles, and roles are assigned to users and groups. You cannot assign a role-based permission to a user or group directly.

There are two basic types of role-based permissions:

- Permissions that enable access to areas of the CentraSite Control user interface.
- Permissions that enable users to create and/or work with certain types of registry and repository objects.

Some permissions are granted implicitly when you assign other permissions.

These topics are described in the following sections:

- Permissions that Enable Access to Areas of the User Interface
- Permissions that Enable Access to Objects
- Implication of Additional Permissions

- The Role-Based Permissions in CentraSite

Permissions that Enable Access to Areas of the User Interface

Role-based permissions include a set of permissions that enable access to certain features and screen sets in the CentraSite Control user interface. These permissions determine which tabs a user sees in the navigation bar in CentraSite Control. For example, CentraSite will not display the navigation bar's **Policies** profile to a user unless the user has the "Use the Policy UI" permission. The UI-related permissions also include permissions that enable users to view certain logs and use certain controls in CentraSite Control.

Note: The user interface permissions apply only to the CentraSite Control user interface. They *do not* affect access to features or screen sets in the CentraSite plug-in for Eclipse.

By default, all CentraSite users have implicit (and irrevocable) permission to use the Asset Catalog area of the CentraSite Control user interface. To use the other parts of the user interface, a user must belong to a role that includes the appropriate user interface permission either explicitly (i.e., the role includes the permission itself) or implicitly (i.e., the role includes a permission that implicitly grants the UI permission). For more information about implicitly granted permissions, see *Implication of Additional Permissions*.

The following table describes the user interface permissions that are available in each CentraSite edition:

Permission	Community Edition (CE)	ActiveSOA
Use the Home UI	✓	✓
Use the Policy UI		✓
Use the Administration UI	✓	✓
Use the Reports UI	✓	✓
Use the Operations UI		✓
View Policy Log		✓
View Approval History		✓

Permission	Community Edition (CE)	ActiveSOA
Register as Consumer	✓	✓

For a complete description of the user interface permissions, see ***The Role-Based Permissions in CentraSite***.

For more information about CentraSite editions, see the section *CentraSite Editions* in the document *Introducing CentraSite*.

Permissions that Enable Access to Objects

Role-based permissions include a second type of permissions that enable users to create and/or work with an entire class of objects.

Generally speaking, these types of role-based permissions grant a specified level of access on objects of a specific type. For example, the "Modify Assets" permission grants Modify-level access on all objects of the type Asset. Role-based permissions enable you to apply access controls over an entire class of objects instead of assigning permissions on each object individually.

Levels of Access Granted by the Role-Based Permissions

If a role-based permission grants access to an object, the name of the permission includes one of the following terms to indicate which level of access the permission provides.

If the name includes the following term...	The permission grants the following levels of access...
View	Read objects of a specified type. This level is equivalent to giving a user View instance-level permission on all objects of a given type.
Modify	Read and edit objects of a specified type. This level is equivalent to giving a user Modify instance-level permission on all objects of a given type.
Create	Create and read objects of a specified type. This level is equivalent to giving a user View instance-level permission of all objects of a given type and giving them the ability to create new instances of that type.
Manage	Create, read, edit, delete and modify the instance-level permission of objects of a specified type. This level is equivalent to giving a user Full instance-level permission of all objects of a given type.

Be aware that CentraSite does not provide role-based permissions at all levels for all object types. Access to certain objects types can only be granted at the Manage level, for example. For a complete list of the role-based permissions, see ***Predefined Roles in CentraSite***.

System-Level vs. Organization-Level Permissions

Role-based permissions that enable access to objects are either *organization-specific* or *system-wide*.

System-Level Permissions

A system-wide permission grants access to objects that are available to all organizations, such as taxonomies and asset types. Additionally, some system-wide permissions grant access to all objects of given type *in any organization in the registry/repository*.

The following table describes the system-level permissions that are available in each CentraSite edition:

Permission	Community Edition (CE)	ActiveSOA
Manage Organizations	✓	✓
Manage System-wide Lifecycle Models		✓
Manage System-wide Design/Change-Time Policies		✓
Manage System-wide Runtime Policies		✓
Manage Report Templates	✓	✓
Manage System-wide Roles	✓	✓
Manage UDDI Subscriptions	✓	✓
Create UDDI Subscriptions	✓	✓
View UDDI Subscriptions	✓	✓
Manage Federations		✓
Manage Taxonomies	✓	✓
Manage Asset Types		✓
Manage Runtime Targets		✓
Manage Runtime Event Types		✓
Manage Supporting Documents	✓	✓
View Supporting Documents	✓	✓

Organization-Level Permissions

An organization-specific permission grants a specific level of access to all objects of a given type *within a specified organization*. Permissions that enable access to assets, policies and lifecycle models are organization-specific.

The following table describes the user interface permissions that are available in each CentraSite edition:

Permission	Community Edition (CE)	ActiveSOA
Manage Assets	✓	✓
Create Assets	✓	✓
Modify Assets	✓	✓
View Assets	✓	✓
Manage Design/Change-Time Policies		✓
Manage Run-Time Policies		✓
Manage Lifecycle Models		✓
Manage Users	✓	✓
Manage Organizations	✓	✓

For a complete description of the system-level and organization-level permissions, see ***The Role-Based Permissions in CentraSite***.

For more information about CentraSite editions, see the section *CentraSite Editions* in the document *Introducing CentraSite*.

Implication of Additional Permissions

Most role-based permissions grant additional permissions by implication. That is, the permission grants not only the permission that its name indicates, it grants additional implied permissions.

For example, any permission that grant access to a particular type of object automatically includes (by implication) the UI permissions required to work with that object. Users that belong to roles that include the "Manage Taxonomy" permission, for instance, automatically receive the "Use the Administration UI" permission by implication.

The "Manage Organizations" permission is an example of another permission that grants additional permissions by implication. This permission, when given at the system-level, essentially implies

all other role-based permissions. Consequently, a user with "Manage Organizations" permission at the system-level can manage virtually any object in any organization.

For a description of the individual permissions, and the permissions they each imply, see *The Role-Based Permissions in CentraSite*.

The Role-Based Permissions in CentraSite

The following table describes the individual permissions and their implied permissions in CentraSite, if any.

Permission	Scope	Purpose	Implied Permissions
Use the Home UI	System-wide	Grants the right to use the Home area in CentraSite Control. Without this permission the UI will hide the **Home** top-level navigation item.	None
Use the Policy UI	System-wide	Grants the right to use the Policy area in CentraSite Control. Without this permission the UI will hide the **Policy** top-level navigation item.	None
Use the Administration UI	System-wide	Grants the right to use the Administration area in CentraSite Control. Without this permission the UI will hide the **Administration** top-level navigation item.	None
Use the Reports UI	System-wide	Grants the right to use the Reports area in CentraSite Control. Without this permission the UI will hide the **Reports** top-level navigation item.	None
Use the Operations UI	System-wide	Grants the right to use the Operations area in CentraSite Control. Without this permission, the UI will hide the **Operations** top-level navigation item.	None
View Policy Log	System-wide	Grants the right to view the policy log.	"Use the Administration UI"
View Approval History	System-wide	Grants the right to view the approval history.	"Use the Administration UI"
Register as Consumer	System-wide	Grants the right to register as a consumer of assets.	None
Manage Assets	Organization	Grants the right to manage assets and supporting documents within an organization.	"Create Assets" "Modify Assets" "View Assets"
Create Assets	Organization	Grants the right to create new assets within an organization.	None

Permission	Scope	Purpose	Implied Permissions
Modify Assets	Organization	Grants the right to modify all assets and supporting documents within an organization. The "Modify Assets" permission is important not just for applying updates to existing assets but also for performing consumer registrations.	"View Assets"
View Assets	Organization	Grants the right to view all assets and supporting documents within an organization.	None
Manage Design/Change-Time Policies	Organization	Grants the right to manage design/change-time policies within an organization. Additionally, this implies the right to manage all policy-related objects such as policy conditions and policy parameters. Note that there is no explicit permission for viewing design/change-time policies, since design/change-time policies are visible for everyone.	"Use the Policy UI"
Manage Run-Time Policies	Organization	Grants the right to manage run-time policies within an organization. Additionally, this implies the right to manage all policy-related objects such as policy conditions and policy parameters. Note that there is no explicit permission for viewing run-time policies, since run-time policies are visible for everyone.	"Use the Policy UI"
Manage Lifecycle Models	Organization	Grants the right to manage lifecycle models (LCMs) within an organization. Note that there is no explicit permission for viewing LCMs, since LCMs are visible for everyone.	"Use the Administration UI" "Modify Assets" "Manage Design/Change-Time Policies" "Manage Runtime Policies"
Manage Users	Organization	Grants the right to manage users of an organization. Additionally, this grants the right to manage groups and roles within an organization.	"Use the Administration UI"

Permission	Scope	Purpose	Implied Permissions
Manage Organizations	Organization	Grants the right to manage an organization and all its child organizations. Also grants the right to manage the organization folder in Supporting Document Library (SDL). By default, the content of an organization folder is visible for every user of that organization. Note that all organizations are visible for everyone.	"Manage Users" "Manage Design/Change-Time Polices" "Manage Run-Time Policies" "Manage Lifecycle Models" "Manage Assets"
Manage Organizations	System-wide	Grants the right to manage all organizations in the CentraSite instance. Note that all organizations are visible for everyone.	"Manage Organizations" (org-level permission for every organization) "Manage System-wide Design/Change-Time Policies" "Manage System-wide Run-Time Policies" "Manage-System-wide Lifecycle Models" "Manage Report Templates"
Manage System-wide Lifecycle Models	System-wide	Grants the right to manage lifecycle models. Note that there is no explicit permission for viewing system-wide lifecycle models, since system-wide lifecycle models are visible for everyone.	"Use the Administration UI" "Manage Lifecycle Models" (org-level permission for every organization) "Manage System-wide Design/Change-Time Policies" "Manage System-wide Runtime Policies"
Manage System-wide Design/Change-Time Policies	System-wide	Grants the right to manage design/change-time policies. Additionally, this implies the right to manage the following policy-related objects: • Action Categories • Action Templates • Action Parameters Note that there is no explicit permission for viewing system-wide design/change-time policies, since system-wide design/change-time policies are visible for everyone.	"Use the Policy UI"

Permission	Scope	Purpose	Implied Permissions
Manage System-wide Runtime Policies	System-wide	Grants the right to manage run-time policies. Additionally, this implies the right to manage the following policy-related objects: • Action Categories • Action Templates • Action Parameters Note that there is no explicit permission for viewing system-wide run-time policies, since system-wide run-time policies are visible for everyone.	"Use the Policy UI"
Manage Report Templates	System-wide	Grants the right to manage system-wide report templates. Note that there is no explicit permission for viewing system-wide report templates, since system-wide report templates are visible for everyone.	"Use the Reports UI"
Manage System-wide Roles	System-wide	Grants the right to manage system-level roles. Note that there is no explicit permission for viewing system-wide roles, since system-wide roles are visible for everyone.	"Use the Administration UI"
Manage UDDI Subscriptions	System-wide	Grants the right to manage UDDI Subscriptions.	"Create UDDI Subscriptions" "View UDDI Subscriptions"
Create UDDI Subscriptions	System-wide	Grants the right to create new UDDI Subscriptions and view existing UDDI Subscriptions.	"View UDDI Subscriptions"
View UDDI Subscriptions	System-wide	Grants the right to view UDDI Subscriptions.	"Use the Administration UI"
Manage Federations	System-wide	Grants the right to manage federations. Note that there is no explicit permission for viewing federations, since federations are visible for everyone.	"Use the Administration UI"
Manage Taxonomies	System-wide	Grants the right to manage taxonomies. Note that there is no explicit permission for viewing system-wide taxonomies, since system-wide taxonomies are visible for everyone.	"Use the Administration UI"
Manage Asset Types	System-wide	Grants the right to manage asset types. Note that there is no explicit permission for viewing asset types, since asset types are visible for everyone.	"Use the Administration UI"

Permission	Scope	Purpose	Implied Permissions
Manage Runtime Targets	System-wide	Grants the right to manage run-time targets and target types. Note that there is no explicit permission for viewing run-time targets and target types, since run-time targets and target types are visible for everyone.	"Use the Operations UI"
Manage Runtime Event Types	System-wide	Grants the right to mange run-time event types. Note that there is no explicit permission for viewing run-time event types, since run-time event types are visible for everyone.	"Use the Operations UI"
Manage Supporting Documents	System-wide	Grants the right to manage the content of all folders in the Supporting Documents Library (SDL).	"View Supporting Documents"
View Supporting Documents	System-wide	Grants the right to view the content of all folders in the Supporting Documents Library (SDL).	None

Combining Role-Based and Instance-Level Permissions

When a user receives multiple permissions for the same object, the permissions are combined and the user receives the union of all the permissions.

For example, if you give a user instance-level View permission on an asset and that user belongs to a role that gives him or her Modify permission on the asset, that user will get View permission plus Modify permission on the asset (or, in effect, Modify permission since it implies View permission).

You will need to keep this concept in mind when granting role-based access to a large group of users (particularly to an entire organization). Anytime you use a role-based permission to give a group of users access to the entire set of assets in an organization, you can no longer use instance-level permissions to reduce the level of access for those users. For example, when everyone in your organization is given "View Assets" permission, you no longer have a way to use instance-level permission to selectively hide assets from certain users in the organization. In effect, the View permission becomes irrevocable for the users in the organization.

About Roles

A role is a collection of role-based permissions. Assigning a role to a user gives the user the permissions specified in the role. Roles can be assigned to individual users or to groups.

CentraSite provides many predefined roles for you to use. You can also create custom roles as needed.

Predefined Roles in CentraSite

CentraSite provides many predefined roles. These roles fall into two categories:

- *System-level roles*, which contain permissions for working with system-wide objects (i.e., objects that affect or are available to all organizations). Asset types and taxonomies are examples of system-wide objects.

  The following table identifies the predefined system-level roles that are available in each CentraSite edition:

Role	Community Edition (CE)	ActiveSOA
CentraSite Administrator (CSA)	✓	✓
Asset Type Administrator (ATA)		✓
Operations Administrator (OPA)		✓
Guest (G)	✓	✓

  For detailed information about these roles, see ***System-Level Roles***.

- *Organization-level roles*, which contain permissions for working with organization-specific objects (i.e., objects that belong to and are used by one particular organization). Assets, policies and lifecycle models are examples of organization-specific objects. CentraSite maintains a set of organization-level roles for each organization in the registry/repository.

  The following table identifies the predefined organization-level roles that are available in each CentraSite edition:

Role	Community Edition (CE)	ActiveSOA
Organization Administrator (OA)	✓	✓
Asset Administrator (AA)	✓	✓
Policy Administrator (PA)		✓
Asset Provider (AP)	✓	✓
Asset Consumer (AC)	✓	✓

For detailed information about these roles, see *Organization-Level Roles*.

The following table summarizes the permissions that CentraSite assigns to each of the predefined roles by default. Be aware that the permission assignments for most of these roles can be customized by an administrator. If an administrator has customized a predefined role at your site, it might have different permissions than what is shown here.

Permission	Type	Scope	System-Level Roles				Organization-Level Roles				
			CSA	ATA	OPA	Guest	OA	PA	AA	AP	AC
Use the Home UI	UI	System-wide	✓	✓	✓		✓	✓	✓	✓	✓
Use the Policy UI	UI	System-wide	✓		✓		✓	✓			
Use the Administration UI	UI	System-wide	✓	✓			✓				
Use the Reports UI	UI	System-wide	✓		✓		✓		✓	✓	✓
Use the Operations UI	UI	System-wide	✓		✓						
View Policy Log	UI	System-wide	✓	✓	✓		✓	✓	✓		
View Approval History	UI	System-wide	✓	✓	✓		✓	✓	✓		
Register as Consumer	UI	System-wide	✓				✓		✓	✓	✓
Manage Assets	ORG	Organization					✓		✓		
Create Assets	ORG	Organization					✓		✓	✓	
Modify Assets	ORG	Organization					✓		✓		
View Assets	ORG	Organization					✓	✓	✓	✓	✓

Permission	Type	Scope	System-Level Roles				Organization-Level Roles				
			CSA	ATA	OPA	Guest	OA	PA	AA	AP	AC
Manage Design/Change-Time Policies	ORG	Organization					✓	✓			
Manage Run-Time Policies	ORG	Organization					✓	✓			
Manage Lifecycle Models	ORG	Organization					✓		✓		
Manage Users	ORG	Organization					✓				
Manage Organizations	ORG	Organization					✓				
Manage Organizations	SYS	System-wide	✓								
Manage System-wide Lifecycle Models	SYS	System-wide	✓	✓	✓						
Manage System-wide Design/Change-Time Policies	SYS	System-wide	✓	✓	✓						
Manage System-wide Runtime Policies	SYS	System-wide	✓		✓						
Manage Report Templates	SYS	System-wide	✓		✓						
Manage System-wide Roles	SYS	System-wide	✓								
Manage UDDI Subscriptions	SYS	System-wide	✓		✓						
Create UDDI Subscriptions	SYS	System-wide	✓		✓						
View UDDI Subscriptions	SYS	System-wide	✓		✓						
Manage Federations	SYS	System-wide	✓								
Manage Taxonomies	SYS	System-wide	✓	✓							
Manage Asset Types	SYS	System-wide	✓	✓							
Manage Runtime Targets	SYS	System-wide	✓		✓						
Manage Runtime Event Types	SYS	System-wide	✓		✓						

Permission	Type	Scope	System-Level Roles				Organization-Level Roles				
			CSA	ATA	OPA	Guest	OA	PA	AA	AP	AC
Manage Supporting Documents	SYS	System-wide	✓								
View Supporting Documents	SYS	System-wide	✓								

System-Level Roles

The following predefined roles in CentraSite are system-level roles. Generally speaking, these roles contain permissions that enable users to work with system-wide objects. Some of these roles also enable users to manage (view, edit or delete) all instances of a given object type in any organization in the CentraSite registry/repository. For example, a user in the Centrasite Administrator role has, in effect, Full permission on every asset in every organization.

The main characteristic that distinguishes a system-level role from an organization-level role is that a system-level role is not generated for each new organization.

As noted in the following descriptions, some system-level roles can be edited and/or deleted and others cannot.

- **CentraSite Administrator**

  The CentraSite Administrator role includes all available permissions. Users in this role have all the permissions to manage the complete system (that is, users with "superuser" permissions). The CentraSite Administrator only can change the permission set for a system role. Additionally, the CSA has permission to create and delete a system role. *This role cannot be modified or deleted*.

- **Asset Type Administrator**

  Users in the Asset Type Administrator role can manage the type definitions and taxonomies in CentraSite.

- **Operations Administrator**

  Users in the Operations Administrator role can manage the operational aspects of CentraSite. For example, the Runtime Event Types and Runtime Targets.

- **Guest**

  Users in the Guest role can browse and use the asset catalog.

For a summary of the permissions that CentraSite assigns to these predefined roles by default, see *Predefined Roles in CentraSite*.

Organization-Level Roles

CentraSite automatically populates any new organization that is created with the following organization-level roles and permissions.

- **Organization Administrator**

  Users in the Organization Administrator role can manage objects within a particular organization. This includes all child organizations of that organization. *This role cannot be modified or deleted*.

- **Asset Provider**

  Users in the Asset Provider role can create new assets and view assets. This role also has the ability to register users to consume assets.

- **Asset Consumer**

  Users in the Asset Consumer role can view all assets. This role also has the ability to register users to consume assets.

- **Asset Administrator**

  Users in the Asset Administrator role can manage all assets within the organization.

- **Policy Administrator**

  Users in the Policy Administrator role can manage design/change-time and run-time policies within an organization.

Note: By default, the Asset Provider and Asset Consumer roles are automatically assigned to the Users group that CentraSite creates for an organization. Consequently, every user in an organization is assigned these roles. If you do not want every user in your organization to have these roles (for example, if you do not want every user to have the Asset Provider role), edit the role assignments for your organization's Users group. For procedures, see *Assigning Roles to a Group*.

For a summary of the permissions that CentraSite assigns to these predefined roles by default, see *Predefined Roles in CentraSite*.

Creating and Managing Roles

You can create custom roles in CentraSite as needed. Custom roles can contain system-level permissions and/or organization-level permissions. A custom role can contain organization-level permissions for multiple organizations (i.e., you can create a role that allows a user to manage the policies in two different organizations). You can also modify many of the predefined organizations that CentraSite installs. For information about which predefined roles can be modified, see the topics *System-Level Roles* and *Organization-Level Roles* in the section *About Roles and Permissions* in the document *Users, Groups, Roles and Permissions*.

Who Can Create and Manage Roles?

To create and manage (i.e., view, edit and delete) roles for an organization, you must belong to a role that has the "Manage Users" permission for the organization. Users in the Organization Administrator role have this permission, although an administrator can assign this permission to other roles.

Note: Users that belong to a role that includes the "Manage Organizations" permission have the "Manage User" permission by implication. Such users can create and mange groups in any organization to which their "Manage Organizations" permission applies.

Be aware that you when you define a role, you cannot assign permissions to the role that you do not have yourself. Therefore, if you belong to the Organization Administrator role (and you have no additional role assignments), you cannot create roles that have any additional permissions than the ones provided by the Organization Administrator role. For example, you could not create a role that included system-level permission or permissions for other organizations. A user with the "Manage Organizations" permission at the system-level (such as someone in the CentraSite Administrator role) would need to do that.

Creating Custom Roles

To create a custom role

1 In CentraSite Control, go to **Administration > Users > Roles**.

2 On the Roles page, click **Add Role**.

3 In the **Role Information** panel, specify the following fields:

In this field...	Do the following...
Name	Enter a name for the new role. A role name can contain any character (including spaces). **Note:** The role name must be unique within an organization.
Description	*Optional*. Enter a short description for the new role. This description appears when the user displays the list of roles in CentraSite Control.
Organization	Specify the organization to which this role belongs. (The drop-down list only displays organizations for which you have "Manage Users" permission.)

4 In the **Permissions** panel, click **Assign permissions**.

5 In the **Assign Permissions** dialog box, do the following

1. Select the permission(s) that you want to assign to this role. (The list will only contain permissions that you are authorized to assign.)
2. Click **OK**.

6 Click **Save** to create the new custom role in the CentraSite registry/repository.

Viewing and Editing Roles

You use the Edit Role page to examine and/or edit the properties of a role. When viewing or editing a role, keep the following points in mind:

- You cannot modify the CentraSite Administrator role.
- You cannot modify the Organization Administrator.

To view or edit the properties of a role

1 In CentraSite Control, go to **Administration > Users > Roles**.

2 By default, all of the available roles are displayed.

If you want to filter the list to see just a subset of the available roles, type a partial string in the **Search** field. CentraSite applies the filter to the **Name** column. The **Search** field is a type-ahead field, so as soon as you enter any characters, the display will be updated to show only those roles whose name contains the specified characters. The wildcard character "%" is supported.

3 Locate the role that you want to view or edit.

4 From the role's context menu, select the **Details** command.

5 Examine or modify the attributes on the Edit Role page as necessary.

Field	Description
Name	The name of the role. A role name can contain any character (including spaces). **Note:** The role name must be unique within an organization.
Description	Additional comments or descriptive information about the role.
Organization	*Read-only.* The organization to which the role belongs.
Permissions	The settings on this profile identify the permissions that are assigned to this role.

6 If you want to add or remove permissions to/from the role, select the **Permissions** profile and do the following:

1. To add permissions to the role, click **Assign Permissions** and select the permission that you want to add.

2. To remove permissions from the role, select the permissions that you want to remove and click **Remove**.

7 If you have edited the settings on the Edit Role page, click **Save** to save the updated role.

Deleting Roles

You use the Roles page to delete the custom roles. When deleting a role, keep in mind that you cannot delete the CentraSite Administrator role or the Organization Administrator role (not even if you belong to the CentraSite Administrator role).

To delete a role

1 In the CentraSite Control, go to **Administration > Users > Roles** to display the roles list.

2 Enable the checkbox next to the name of the role that you want to delete.

3 Click **Delete**.

When you are prompted to confirm the delete operation, click **OK**.

You can delete multiple roles in a single step. The rules described above for deleting a single role apply also when deleting multiple roles.

Important: If you have selected several roles where one or more of them are predefined roles, you can use the **Delete** button to delete the roles. However, as you are not allowed to delete predefined roles, only roles you have permission for will be deleted. The same applies to any other roles for which you do not have the required permission.

To delete multiple roles in a single operation

1 In CentraSite Control, go to **Administration > Users > Roles** to display the roles list.

2 Mark the checkboxes of the roles that you want to delete.

3 From the **Actions** menu, choose **Delete**.

When you are prompted to confirm the delete operation, click **OK**.

4 Changing Passwords of Predefined Users and Login Users

CentraSite deals with two types of users:

- **Predefined users**
  These users are used for internal communication between the various components of CentraSite, and also for guest access to CentraSite.
- **Login users**
  These users represent real users who are defined in the user repositories that CentraSite uses for authentication of users. Login users can log in to CentraSite's graphical UIs.

There can be several Application Server Tiers (ASTs) accessing a single CentraSite registry, and any password change that occurs on one AST should be made known to the other ASTs.

Changing the Password of a Predefined User

The following users are predefined in CentraSite:

- **DefaultUser**
  This is the owner of all predefined objects. The predefined password for this user is "Pwd-For_CS21". You should change this password as soon as possible after you have installed CentraSite.
- **guest**
  This user is configured to have access to only some resources, and for those resources to have only read access. The predefined password for this user is "guest".

  If you wish to protect all data in the CentraSite Registry/Repository from read accesses from guest users you can change the password of this user.
- **UDDIsubscriptionUser**
  This user is used for communication between the application server and the CentraSite UDDI server. The predefined password for this user is "UDDI4CentraSite".
- **PurgeUser**
  This is a user who can purge log records. The predefined password for this user is "LogPurger4CS".
- **EventsUser**
  The CentraSite Events Listener will use this user name for authentication before persisting event data to the RuntimeEvents Collection database. The predefined password for this user is "EventsManager4CS". You can change this password or, alternatively you can change the "EventsUser" to a login user by configuring the Event Receiver, as described in the topic *Configuring the Event Receiver* in the section *Run-Time Events* of the document *Managing Targets and Run-Time Events*.

Caution: You cannot log on to CentraSite Control using the user ID/password combination for any of these predefined users. Guest users can log on to CentraSite Control without a password by using the **Browse as Guest** link on the login page.

If you wish to change the password of a predefined user, use a command of the following form:

```
CentrasiteCommand set Password [-url <CENTRASITE-URL>] -user <USER-ID> -password
<PASSWORD> -predefinedUser <PREDEFINED-USER> -newPassword <NEW-PASSWORD>
```

You can execute the above command in the command line interface *CentraSiteCommand.cmd* (Windows) or *CentraSiteCommand.sh* (UNIX) of Command Central. The tool is located in `<CentraSiteInstallDir>`/utilities.

If you start the command line tool with no parameters, you receive a help text summarizing the required input parameters.

The following table describes the complete set of input parameters that you can use with the `set Password` utility:

Parameter	Description
`-url`	The fully qualified URL (http://localhost:53307/CentraSite/CentraSite) for the CentraSite registry/repository.
`-user`	The user ID of a user who has the "CentraSite Administrator" role.
`-password`	The password of the user identified by the parameter "-user".
`-predefinedUser`	The user ID of the predefined user whose password you wish to change.
`-newPassword`	The new password for the predefined user.

For example:

```
CentrasiteCommand set Password [-url "http://localhost:53307/CentraSite/CentraSite"] ↩
-user "AdminUser" -password
"ABCXYZ123" -predefinedUser "DefaultUser" -newPassword "MyPassword2"
```

The parameters of the command are case-sensitive, so for example the parameter "-url" must be specified as shown and not as "-URL".

If you omit the passwords from the command, you will be prompted to provide them.

Note: When the password for a predefined user has been changed, any application using this user needs to be adapted to use the new password.

Changing a Login User's Password in the Password Store

CentraSite provides a secure password store for managing the passwords of login users whose credentials are required for internal communication between CentraSite components.

Examples of such scenarios that require authentication credentials for internal communication are the use of policies such as Promote Asset and Initiate Approval. These policies cause a lifecycle model state change that requires the approval of an authorized login user.

This password store exists in parallel to the user repository that CentraSite uses for authentication of users. There is no automatic synchronization of passwords between the user repository and the password store. The password for a given login user in the password store must be the same as the password for the same login user in the user repository. If you change a password in the user repository, you must manually update the password in the password store to the same new password.

The password store resides on the application server tier (AST). If your CentraSite configuration uses more than one application server tier (AST), you must ensure that each AST uses an up-to-date version of the password store.

If you wish to change the password of a login user in the password store, use a command of the following form:

```
CentrasiteCommand set Password [-url <CENTRASITE-URL>] -user <USER-ID> -password
<PASSWORD> -userToStore <USER-TO-STORE> -passwordToStore <PASSWORD-TO-STORE>
```

You can execute the above command in the command line interface *CentraSiteCommand.cmd* (Windows) or *CentraSiteCommand.sh* (UNIX) of Command Central. The tool is located in `<CentraSiteInstallDir>`/utilities.

If you start the command line tool with no parameters, you receive a help text summarizing the required input parameters.

The following table describes the complete set of input parameters that you can use with the `set Password` utility:

Parameter	Description
`-url`	The fully qualified URL (http://localhost:53307/CentraSite/CentraSite) for the CentraSite registry/repository.

Parameter	Description
`-user`	The user ID of a user who has the "CentraSite Administrator" role.
`-password`	The password of the user identified by the parameter "-user".
`-userToStore`	The user ID of the login user whose password you wish to change in the password store.
`-passwordToStore`	The new password to be stored in the password store for the login user identified by the parameter `-userToStore`.

For example:

```
CentrasiteCommand.sh set Password [-url ↩
"http://localhost:53307/CentraSite/CentraSite"] -user "AdminUser" -password
"ABCXYZ123" -userToStore "SomeLoginUserID" -passwordToStore "SomeNewPassword"
```

The parameters of the command are case-sensitive, so for example the parameter "-url" must be specified as shown and not as "-URL".

If you omit the passwords from the command, you will be prompted to provide them.