



CHAPTER 2

Portal Settings

The Portal drawer contains selections that allow system administrators to set up and maintain the portal. From this drawer, you can add and edit users, communities, roles, and configure the settings of the portal.

To access the Portal drawer, log in to Cisco WebEx Social with your administrator credentials, click the down-arrow ▼ to the right of your name in the Global Navigation bar, and then select **Account Settings** from the drop-down menu. To expand the Portal drawer so that you can access its selections, click the right-arrow ► next to **Portal**.

This chapter includes these topics, each of which is a selection in the Portal drawer:

- [Users, page 2-1](#)
- [Communities, page 2-11](#)
- [User Groups, page 2-15](#)
- [Roles, page 2-18](#)
- [Password Policies, page 2-23](#)
- [Community Manager, page 2-25](#)
- [WebEx Social Functionality, page 2-32](#)
- [WebEx Social Metrics, page 2-33](#)
- [Settings, page 2-39](#)
- [Plugin Settings, page 2-54](#)
- [WSRP, page 2-56](#)
- [Content Repositories, page 2-58](#)

Users

Users can be arranged in multiple ways, including:

- **User groups**—Collections of users, created by a Cisco WebEx Social system administrator. For example, the administrator could create a user group called Bloggers, and the members of this group would be able to create blog entries in their personal spaces.
- **Communities**—Organizations that have common interests. For example, one community might be called “Business Sales,” for people within a company focused on increasing business sales.

- **Roles**—Roles are used to define permissions across the scope of the role: portal or community. For example, suppose there is a role for granting access to creating a message board category. A portal role would grant that access across the portal wherever there was a message board application. A community role would grant that access only within a single community.

When you select **Users** from the Portal drawer, the **View All** default window displays all the current Cisco WebEx Social users.

This section contains the following topics:

- [Adding a User Manually, page 2-2](#)
- [Performing Other Functions from the Users Window, page 2-2](#)



Adding a User Manually

If you are using LDAP synchronization in your Cisco WebEx deployment as “[LDAP Directory Sync](#)” [section on page 2-44](#), the system adds new users as follows:

- When a scheduled LDAP synchronization occurs
- When a user logs in to Cisco WebEx Social, if the user was not added during the previous LDAP synchronization

If necessary, you can add a new user to Cisco WebEx Social manually. To do so, follow these steps:

Procedure

-
- Step 1** Access the Users window:
- a. Click the down-arrow  to the right of your name in the Global Navigation bar.
 - b. Select **Account Settings** from the drop-down menu.
 - c. Click the right-arrow  next to **Portal**
 - d. Click **Users** in the Portal drawer.

The Users window appears with the **View All** tab selected.

- Step 2** Select the **Add** tab in the Users window.

- Step 3** Complete the fields and click **Save**.

After you receive a message that the request was processed successfully, you are presented with the Users window again, which allows you to optionally enter additional information about the user. Click links under User Information, Calender and WebEx, Notifications, Identification, and Miscellaneous and enter information as needed.

At a minimum, you must click the **Password** link and set a password for the user.

- Step 4** Click **Save** when you are finished.
-

Performing Other Functions from the Users Window

Other functions you can perform from the Users window include the following:

- [Managing Custom Attributes, page 2-3](#)

- [Creating a CSV File of Current Users, page 2-4](#)
- [Deactivating a Current User Manually, page 2-4](#)
- [Updating User Information for a User, page 2-5](#)

Managing Custom Attributes

The **Custom Attributes** tab in the Users window displays a list of the custom attributes that Cisco WebEx Social is using. Many of these attributes are part of the Cisco WebEx Social product and do not require additional setup or configuration.

To access the Users window, click the down-arrow  to the right of your name in the Global Navigation bar, select **Account Settings** from the drop-down menu, click the right-arrow  next to **Portal**, and then click **Users** in the Portal drawer.



Note

Using custom attributes is optional, and is another way of configuring and passing parameter values to Cisco WebEx Social users. If you use custom attributes, make sure to communicate their usage with developers who are writing scripts that call these custom attributes.

Changing or Deleting a Custom Attribute

By clicking **Actions** to the right of the corresponding attribute, you access the following options from the drop-down menu:

- **Edit**—Lets you edit the default value and any of the properties of the attribute. For a description of a property, hover your mouse over its corresponding question mark icon. After making changes, click **Save**, or click **Cancel** to exit without saving your changes.
- **Permissions**—Use the boxes to set the permissions you want each role to have for the selected custom attribute. After making changes, click **Save**, or click **Cancel** to exit without saving your changes.
- **Delete**—Delete the custom attribute.

Adding a Custom Attribute

If you want to add your own custom attribute, follow these steps:

Procedure

- Step 1** Select the **Custom Attributes** tab in the Users window.
A list of currently used custom attributes appears.
- Step 2** Click **Add Custom Attribute**.
- Step 3** Enter a Key name for your attribute.

Cisco WebEx Social uses the Key name that you enter to access the attribute programmatically. If your Key name is more than one word, Cisco WebEx Social inserts an underscore between each word.

Cisco WebEx Social assigns a Name for the attribute that is the equivalent of the Key, except that each word in the Name begins with an uppercase letter.
- Step 4** Select a type for the custom attribute from the **Type** drop-down menu.
- Step 5** Click **Save**.



- Step 6** Make sure the attribute you just added now appears on the list of custom attributes and that the values are set as desired.

If the values are not set as desired, you can click **Actions** and select **Edit**, then to make changes. For example, if you add a Boolean attribute, its default value is **False**. If you want to immediately change the value to **True**, use the **Actions > Edit** function.

Creating a CSV File of Current Users

To create a CSV file of current users, follow these steps:

Procedure


- Step 1** Access the Users window:
- Click the down-arrow  to the right of your name in the Global Navigation bar.
 - Select **Account Settings** from the drop-down menu.
 - Click the right-arrow  next to **Portal**
 - Click **Users** in the Portal drawer.
- Step 2** Make sure that the View All tab is selected, and click **Export Users**.
- Step 3** Follow the on-screen instructions.
-

Deactivating a Current User Manually

This section describes how to manually deactivate a user. You can use this process to deactivate a user that you added as described in the [“Adding a User Manually” section on page 2-2](#).



If you are using LDAP synchronization in your Cisco WebEx deployment as [“LDAP Directory Sync” section on page 2-44](#), the system deactivates a user when the synchronization occurs if the user no longer exists or has been disabled in the LDAP directory.

If you manually deactivate a user who still is active in LDAP, the system reactivates that user when the next LDAP synchronization runs.

After you deactivate a user, the no longer appears in the Cisco WebEx Social People page, the user cannot be searched for in Cisco WebEx Social, and the user cannot log in to the system. Content that the user created remains in Cisco WebEx Social, but the profile picture of the user is replaced with a deactive user icon .

To deactivate a current user, follow these steps:

Procedure

- Step 1** Access the Users window:
- Click the down-arrow  to the right of your name in the Global Navigation bar.
 - Select **Account Settings** from the drop-down menu.
 - Click the right-arrow  next to **Portal**

d. Click **Users** in the Portal drawer.

Step 2 Take either of these actions:

- Check the box next to each user that you want to deactivate, then click **Deactivate** at the top of the list of users.
- Choose **Deactivate** from the drop-down menu next to the user that you want to deactivate.

You can use these functions to locate users:

- Sort the list of users in ascending or descending alphanumeric order by any field. To do so, click a field as needed to toggle the sort order. An up-arrow icon ▲ in a field indicates that users are sorted in ascending order on that field. A down-arrow icon ▼ indicates that users are sorted in descending order.
- Click the **Advanced** link and use the search options that appear.

Updating User Information for a User

On the View All tab in the Users window, an Actions drop-down menu appears next to each user name. [Table 2-1](#) describes the actions you can perform for each user:

Table 2-1 *Actions for Users*

Action	Description
Edit	<p>Opens a list of the following links, which you can use to change many settings for the user. You can also open this list of links by clicking the first name, last name, screen name, or job title of the user in the list of users.</p> <p>After making changes, click Save, or click Cancel to exit without saving your changes.</p> <p>The following sections describe the Edit options:</p> <ul style="list-style-type: none"> • Edit Options: Details, page 2-6 • Edit Options: Password, page 2-7 • Edit Options: Communities, page 2-7 • Edit Options: User Groups, page 2-7 • Edit Options: Roles, page 2-7 • Edit Options: Calendar and WebEx Login, page 2-8 • Edit Options: WebEx Instant Meetings, page 2-8 • Edit Options: Email Notifications, page 2-9 • Edit Options: Social Network, page 2-10 • Edit Options: Display Settings, page 2-10 • Edit Options: Custom Attributes, page 2-10 • Edit Options: Phone Control Preference, page 2-11 • Edit Options: CMIS Settings, page 2-11 • Edit Options: Chat Password, page 2-11

Table 2-1 **Actions for Users (continued)**

Action	Description
Permissions	<p>Displays a list of roles (with links to each role definition). From this list you can change which roles are given what permissions on the selected user record. You can assign these roles:</p> <ul style="list-style-type: none"> • Delete—Lets someone assigned to the corresponding role delete this user record from the portal • Impersonate—Not used • Permissions—Lets someone assigned to the corresponding role perform this Permissions action • Edit—Lets someone assigned to the corresponding role edit this user record • View—Lets someone assigned to the corresponding role view this user record <p>After you make changes to permissions, click Save.</p>
Manage Pages	<p>Allows you to edit any public or private page that the user has created. You can add and delete pages, change the order of the pages, hide page tabs, and more.</p> <p>For related information, see Appendix A, “Modifying Default Layouts and Creating a Custom Template.”</p> <p>Note Users have the rights to manage their Home and My Profile pages. Community owners and administrators inherit these rights.</p>
Deactivate	<p>Provides one method of deactivating a user. You also can deactivate a user as described in the “Deactivating a Current User Manually” section on page 2-4.</p>

Edit Options: Details

The Details area appears when you select **Edit** from the Actions drop-down menu next to a user name in the Portal > Users window, and then click **Details** in the panel that appears on the right of the window.

This area displays and lets you edit basic information about the user. (If you are using LDAP synchronization in your Cisco WebEx deployment as [“LDAP Directory Sync”](#) section on page 2-44, these fields are for display only.

[Table 2-2](#) describes the items in the Users area. If you update information in this area, click **Save** at the bottom of the panel on the right to save your changes.

Table 2-2 **Users Window, Detail Items**

Item	Description
User ID	System-assigned identifier of the user
Screen Name	Cisco WebEx Social screen name of the user
Email Address	E-mail address of the user
Job Title	Job title of the user
First Name	First name of the user
Middle Name	Middle name of the user
Last Name	Last name of the user

Edit Options: Password

The Password area appears when you select **Edit** from the Actions drop-down menu next to a user name in the Portal > Users window, and then click **Password** in the panel that appears on the right of the window.

The Password options is not available if you are using LDAP synchronization in your Cisco WebEx deployment as “[LDAP Directory Sync](#)” section on page 2-44.

[Table 2-3](#) describes the items in the Password area. If you update information in this area, click **Save** at the bottom of the panel on the right to save your changes.

Table 2-3 *Users Window, Password Items*

Item	Description
New Password	Enter a new password for the user
Enter Again	Reenter the new password for the user
Password Reset Required	Check this box if you want to require the user to reset the password when the user first logs in to Cisco WebEx Social

Edit Options: Communities

The Communities area appears when you select **Edit** from the Actions drop-down menu next to a user name in the Portal > Users window, and then click **Communities** in the panel that appears on the right of the window.

This area shows the name of each community in which the user is a member, and the roles that the user has in each community.

To remove the user from a community, click the **Remove** button next to the community.

To add the user to a community, click the **Select** link then select the desired community.

Edit Options: User Groups

The User Groups area appears when you select **Edit** from the Actions drop-down menu next to a user name in the Portal > Users window, and then click **User Groups** in the panel that appears on the right of the window. If you update information in this area for a user, click **Save** at the bottom of the panel on the right to save your changes.

This area shows the name of each user group to which the user is a belongs.

To add the user to a user group, click the **Select** link then select the desired user group.

Edit Options: Roles

The following areas appear when you select **Edit** from the Actions drop-down menu next to a user name in the Portal > Users window, and then click **Roles** in the panel that appears on the right of the window. If you update information in this area for a user, click **Save** at the bottom of the panel on the right to save your changes.

- Regular Roles—Lists each regular role that is assigned to the user.
To unassign a role, click the **Remove** button next to the role.
To assign a regular role to the user, click the **Select** link then select the role.
- Community Roles—Lists each community in which the user has role.

To unassign a role, click the **Remove** button next to the role.

To assign a community role to the user, click the **Select** link, select the community, then select the role.

Edit Options: Calendar and WebEx Login

The Microsoft Exchange and the Cisco WebEx areas appear when you select **Edit** from the Actions drop-down menu next to a user name in the Portal > Users window, and then click **Calendar and WebEx Login** in the panel that appears on the right of the window.

These areas provide configuration settings for the Calendar portlet on the Home page and WebEx integration.

[Table 2-4](#) describes the items in these areas. If you update information in these areas for a user, click **Save** at the bottom of the panel on the right to save your changes.

Table 2-4 *Users Window, Calendar and WebEx Login Items*

Item	Description
MicroSoft Exchange Area Items	
Connect to Microsoft Exchange	Check this box to cause Microsoft Exchange events to appear in the calendar of the user. The other items in this area become available when you check this box.
Username	Enter the user name (such as jsmith) or the user principal name (such as jsmith@cisco.com) for the user connection to the Exchange server.
Password	Enter the password for the user connection to the Exchange server.
Test	Click this button before you save your changes to ensure that the Username and Password values that you entered allow a connection to the Exchange server.
Cisco WebEx Area Items	
Connect to WebEx	Check this box to cause WebEx meetings to appear in the calendar of the user. The other items in this area become available when you check this box.
WebEx Site	Choose the WebEx site where the meetings of the user are stored.
Username	Enter the user name (such as jsmith) or the user principal name (such as jsmith@cisco.com) for the user connection to the WebEx server.
Password	Enter the password for the user connection to the WebEx server.
Test	Click this button to ensure that the Username and Password values that you entered allow a connection to the WebEx site that you designated.

Edit Options: WebEx Instant Meetings

The Meeting Options and the Audio Conference areas appear when you select **Edit** from the Actions drop-down menu next to a user name in the Portal > Users window, and then click **WebEx Instant Meetings** in the panel that appears on the right of the window.

These areas provide configuration settings for WebEx Instant Meeting functionality. For existing WebEx Meeting user, these settings are typically preconfigured by the user in a WebEx application or plugin, stored in the WebEx cloud, and populated in these areas automatically.

[Table 2-5](#) describes the items in these areas. If you update information in these areas for a user, click **Save** at the bottom of the panel on the right to save your changes.

Table 2-5 *Users Window, WebEx Instant Meetings Items*

Item	Description
Meeting Options Items	
Meeting Service Type	Choose the desired meeting service, which determines the features that are available for instant meetings.
Meeting Topic	Enter the topic for instant meetings.
Meeting Password	Enter the password to be used for instant meetings.
Confirm Password	Confirm the password to be used for instant meetings.
Audio Conference Items	
Use Audio	Choose the system to use for the audio portion of instant meetings. Additional options appear, depending on the value that you choose. Configure these items as needed.
Display toll-free number	If you choose WebEx Audio from the Use Audio drop-down menu, check this box to include in the e-mail messages that users receive about instant meetings a toll-free telephone number that can be used to join the meeting
Display global call-in numbers to attendees	If you choose WebEx Audio from the Use Audio drop-down menu, check this box to include in the e-mail messages that users receive about instant meetings a list of telephone numbers that can be used to join the meeting
Entry & Exit Tone	Choose Announce Name , Beep , or No Tone to indicate the action that occurs when a user joins or leaves a meeting

Edit Options: Email Notifications

The Email Notifications area appears when you select **Edit** from the Actions drop-down menu next to a user name in the Portal > Users window, and then click **Email Notifications** in the panel that appears on the right of the window.

**Note**

The **Email Notifications** option appears only if the `users.form.update.email-notifications` is configured in the director as described in the [“Configuring Properties for E-mail Integration” section on page 5-16](#).

This area lets you configure settings for digest notifications (also called *WebEx Social Activity Snapshots*) and instant notifications. Digest notifications are e-mail messages that contain summaries of Cisco WebEx Social activities that a user is interested in. Messages can include information about new followers, posts, community memberships, and community discussions that apply to the user. Users can receive digest notifications daily (these notifications include a summary of activities that occurred that day) or weekly (these notifications include a summary of activities that occurred the past week).

[Table 2-6](#) describes the items in the Email Notifications area. If you update information in this area, click **Save** at the bottom of the panel on the right to save your changes.

Table 2-6 *Users Window, Email Notifications Items*

Field	Description
Send me a summary of all important updates	Check this box to cause daily or weekly digest notifications to be sent to the user.

Table 2-6 *Users Window, Email Notifications Items (continued)*

Field	Description
Activity Snapshot frequency	Select Daily or Weekly to indicate how often the user receives digest notifications. This option is available only if you check the Send me a summary of all important updates box.
Send me individual emails for the following events	Check this box then check boxes that correspond to people, content, and community membership to designate the activities that are included in the instant notifications that the user receives.

Edit Options: Social Network

The Social Network area appears when you select **Edit** from the Actions drop-down menu next to a user name in the Portal > Users window, and then click **Social Network** in the panel that appears on the right of the window.

Use the **Delink my Twitter account** button in this area to de-link the Twitter account of the user from Cisco WebEx Social.

Edit Options: Display Settings

The Display Settings area appears when you select **Edit** from the Actions drop-down menu next to a user name in the Portal > Users window, and then click **Display Settings** in the panel that appears on the right of the window.

This area provides options for configuring the language and time zone that are used in the Cisco WebEx Social display for the user.

[Table 2-7](#) describes the items in the Display Settings area. If you update information in this area, click **Save** at the bottom of the panel on the right to save your changes.

Table 2-7 *Users Window, Display Settings Items*

Item	Description
Language	Choose the language to use for the Cisco WebEx Social display for the user. The available languages are defined in the Available Languages field as described in the “Display Settings” section on page 2-53 .
Time Zone	Choose the time zone to use for the Cisco WebEx Social display for the user

Edit Options: Custom Attributes

The Custom Attributes area appears when you select **Edit** from the Actions drop-down menu next to a user name in the Portal > Users window, and then click **Custom Attributes** in the panel that appears on the right of the window.

This area provides options for configuring custom attributes for a user. For assistance with configuring these options, contact a Cisco support representative.

Edit Options: Phone Control Preference

The Phone Control Preference area appears when you select **Edit** from the Actions drop-down menu next to a user name in the Portal > Users window, and then click **Phone Control Preference** in the panel that appears on the right of the window.

This area provides options for configuring the device or line to be used with the WebDialer Click to Call feature.

Edit Options: CMIS Settings

The options in the CMIS area that appears when you select **Edit** from the Actions drop-down menu next to a user name in the Portal > Users window are not use.

Edit Options: Chat Password

The Chat Password area appears when you select **Edit** from the Actions drop-down menu next to a user name in the Portal > Users window, and then click **Chat Password** in the panel that appears on the right of the window.

This area provides the **Password** and the **Enter Again** fields for designating the password for the user connection to the chat server.

Communities

Communities are areas of Cisco WebEx Social that users or administrators can create to house information about a specific topic. This information, which can include documents, videos, posts, discussion boards and so on, can be shared among people who join that community.

Communities have their own pages. Members of communities can maintain their own public and private pages (if they are granted the Manage Pages permission).

This section contains these topics:

- [Adding a Community, page 2-11](#)
- [Managing an Existing Community, page 2-12](#)



Note

When regular users create communities, they have permissions, as owner, to administer the communities they create. System administrators can administer any community in the portal.

Related Topic

[Community Manager, page 2-25](#)

Adding a Community

To add a community, follow these steps:



Procedure

-
- Step 1** Click **Communities** in the Global Navigation bar.

- Step 2** Click **New Community**.
- Step 3** Select a category from the choices presented.
- Step 4** Select the membership type (open, restricted, or hidden) for the community.
- **Open**—An open community appears in the All Communities application, which allows users to join and leave the community whenever they want.
 - **Restricted**—A restricted community also appears in the All Communities application, but users must request membership. A community administrator then must grant or deny that request.
 - **Hidden**—A hidden community does not appear in the All Communities application; therefore, users must be invited by a community administrator.
- Step 5** Click **Next**.
- Step 6** In the Community Name field, enter the name of the community you wish to create.
- Step 7** In the Description field, enter some descriptive text about the community.
- Step 8** In the Tags field, enter any tags, and separate multiple tags with a blank space.
- The Cisco WebEx Social tagging mechanism allows for easy searching. This is helpful if the community has a specific, topical purpose within the portal.
- Step 9** (Optional) In the Invite Additional Owners field, begin typing the name of someone you want to help you manage the community, then select a name from the list.
- You may select as many additional owners as you want.
- Step 10** Click **Next**.
- Step 11** Choose one of the templates presented, then click **Next**.
- Step 12** If you are satisfied with your choices, click **Create**.
- Your community is created in “draft mode” and a customization window for your community opens.
- Step 13** Use the links in the customization window to customize your community.
- Step 14** When you are ready for users to access and begin using the community, click **Go Live**.
- After you create a community, it appears in the list of communities within the main Communities tab.
-

Managing an Existing Community

When you click **Communities** in the Global Navigation bar, you can then view all communities within the portal by clicking **All Communities** in the upper-left portion of the window.

You can also view all communities within the portal by clicking the down-arrow  to the right of your name in the Global Navigation bar, selecting **Account Settings** from the drop-down menu, clicking the right-arrow  next to **Portal**, and then clicking **Communities** in the Portal drawer.

As an administrator, you can perform community-management activities for any community.

You can perform the actions that [Table 2-8](#) describes from the Actions drop-down menu next to a community:

Table 2-8 **Actions You Can Perform for An Existing Community**


Function	Description
Edit	<p>Lets you edit most of the information that entered when the community was first created.</p> <p>When you select this action, use the tabs that appear near the top of the menu to access the information that you want to change. After making changes, click Save, or click Cancel to exit without saving your changes.</p>
Join / Leave	If you are not a member of this community, you are presented with a Join or Request Membership option. If you are a member of this community, you are presented with a Leave option.
Delete	<p>Lets you delete this community. Make sure to notify member of a community when you delete it.</p> <div>  <p>Caution When you delete a community, it is permanently removed from the portal, along with any pages and other data that belonged to this community.</p> </div>
Deactivate	Lets you deactivate a community. After you do so, users who are not administrators no longer see the community in the list of communities, and the community is no longer searchable in Cisco WebEx social.

Table 2-8 **Actions You Can Perform for An Existing Community (continued)**


Function	Description
Assign User Roles	<p>Lets an administrator or community owner assign or remove one or more of the following roles to members of the community.</p> <p>Note Users can manage community roles for communities of which they are the administrator or owner by hovering the cursor over the gear icon  that appears on a page within the community and choosing Manage Community.</p> <ul style="list-style-type: none"> Community Administrator—Super user of the community. However, a community administrator does not have the capability to change users into community administrators. Community Member—Role automatically given to all users who are members of a specific community. This role has no special privileges. Community Owner—Creator of the community. Only a community owner can grant community administration rights to other users. Special community-scoped role created by the system administrator. For a description of such a role, see the “Roles” section on page 2-18. <p>To assign a role to a users, follow these steps:</p> <ol style="list-style-type: none"> 1. Select Assign User Roles from the drop-down menu next to the community. 2. Decide which role you want to assign to a particular member of the community, and click the Add Members button for that role. A window appears that displays any current members of the community who are already assigned to this role. 3. To assign this role to other members to this community, click Add Members, then enter then name of a user to add. When the name of the user appears in a pop-up list, select that user. 4. Click Add. <p>To remove members from this role:</p> <ol style="list-style-type: none"> 1. Select Assign User Roles from the drop-down menu next to the community. 2. Click the Add Members button for the role. 3. Click Remove next to the user to remove from the role.

Table 2-8 Actions You Can Perform for An Existing Community (continued)

Function	Description
Assign Members	<p>Takes you to a window that displays current members of the community and lets you add members.</p> <p>To invite a members to join a community, follow these steps:</p> <ol style="list-style-type: none"> 1. Select Assign Members from the drop-down menu next to the community. 2. Click the link under Members for the type of member that you want to invites (All Members or Owners). 3. Click the Invite Type button, where <i>Type</i> is Members or Owners, or Administrators, depending on the type of member that you are inviting. 4. Enter then name of a user to invite. When the name of the user appears in a pop-up list, select that user. 5. If you want to include a custom message with your invitation, check the Send a Personalized Note box, then enter the message in the field provided. 6. Click Invite. <p>To remove members from this community, if you are an administrator or community owner select Assign Members from the Actions drop-down menu next to the community, then choose Remove from Community from the drop-down menu next to each user to remove.</p>
View Membership Request	Applies to only restricted communities. Lets you view a request by a user to join a community, and either deny or accept the request.

User Groups

User Groups are arbitrary groupings of users. As a system administrator, you can create user groups to bring together users who do not have a community-based attribute in common. User groups cannot have permissions, but user groups can be assigned roles.


This section contains these topics:


- [Adding a User Group, page 2-15](#)
- [Performing Actions for a User Group, page 2-16](#)
- [Defining Page Templates for a User Group, page 2-17](#)

Adding a User Group

To add a user group, follow these steps:

Procedure

- Step 1** Access the User Groups window:
- a. Click the down-arrow  to the right of your name in the Global Navigation bar.
 - b. Select **Account Settings** from the drop-down menu.

- c. Click the right-arrow  next to **Portal**
- d. Click **User Groups** in the Portal drawer.

The User Groups window appears with the **View All** tab selected.

Step 2 Select the **Add** tab.

Step 3 In the **Name** field, enter the name of the user group you wish to create.

Step 4 In the **Description** field, enter descriptive text about the user group.

Step 5 Click **Save**.

The name of the user group now appears in the list of user groups shown when the **View All** tab is selected.

Performing Actions for a User Group

When the **View All** tab is selected in the User Groups window, all user groups within the portal are listed. Next to each user group is an **Actions** drop-down menu. [Table 2-9](#) lists and describes the selections in this menu.

Table 2-9 *Actions You Can Perform on an Existing User Group*

Action	Description
Edit	Lets you edit the name and the description of the user group. You can also edit a user group by clicking the name or description user group in the list of user groups. After making changes, click Save , or click Cancel to exit without saving your changes.

Table 2-9 **Actions You Can Perform on an Existing User Group (continued)**

Action	Description
Permissions	<p>When you select Permissions, a list of roles appears (with links to each role definition). This action allows you to change which roles are given what permissions on the selected user group. You can assign these permission types:</p> <ul style="list-style-type: none"> • Assign Members—Lets someone assigned to the corresponding role assign members to this user group • Delete—Lets someone assigned to the corresponding role delete this user group from the portal • Manage Announcements—Lets someone assigned to the corresponding role manage announcements for this user group • Permissions—Lets someone assigned to the corresponding role perform these Permissions action • Manage Pages—Lets someone assigned to the corresponding role create page templates for members of this user group • Edit—Lets someone assigned to the corresponding role edit information about this user group • View—Lets someone assigned to the corresponding role view the membership list of this user group. <p>After making changes, click Save, or click Cancel to exit without saving your changes.</p>
Manage Pages	<p>Though user groups do not have their own pages, you can create page templates for a user group. With page templates, any users added to the group have the group pages copied to their personal pages.</p> <p>For more information about defining page templates for user groups, see the “Defining Page Templates for a User Group” section on page 2-17.</p>
Assign Members	<p>Takes you to a window that displays current members of the user group and lets you add members.</p> <p>To add members to this user group, click the Available tab, check the box next to each user that wish to become members of this user group, then click Update Associations. (You can click the Advanced link and use the Search function to locate users.) Now, when you click the Current tab, the users that you added appear in the list of current members.</p> <p>To remove members from this user group, click the Current tab, uncheck the box next to the member you wish to remove, then click Update Associations. The name no longer appears in the list of current members.</p>
View Users	Lets you view the users who belong to this user group.
Delete	Deletes the user group.

Defining Page Templates for a User Group

When you select the **Manage Pages** action for a user group as described in the [“Performing Actions for a User Group”](#) section on page 2-16, you can create pages and manage them in a hierarchy.

You can create both public and private pages, which correspond to Home and My Profile, respectively. Each set is used as templates and is be copied to personal public or private page sets, respectively, of a user when the user becomes a member of the user group.

For example, suppose that you, as the system administrator, create a new private portlet page called *You are a student* within the *Students* user group. Because the page created is a portlet page, you can now click the *View Pages* button to open the page, then add as many portlets as desired to that page and configure them as needed.

Applying Page Templates by Assigning Members to the User Group

After you create a page template, perform the following steps to assign it to an existing member of the user group to verify that the page template gets copied as a private page of a user.

Because the pages are copied to a set of pages for a user, those pages are now owned by the user and they can be changed at any time if the portal is set up to allow users to edit their personal pages. When a user is removed from a user group, the associated pages are not removed.

If you modify page templates for a user group after users have already been added to the group, those changes are used only when new users are assigned to the user group.

Procedure

-
- | | |
|---------------|--|
| Step 1 | In the list of available user groups, from the Actions drop-down menu for the desired user group, select Assign Members . |
| Step 2 | Click the Available tab.
A list of available users appears. |
| Step 3 | Check the box for one or more users in this users list. |
| Step 4 | Click Update Associations .
Copies of any public or private page templates that are configured for the user group are copied to the page sets of the users you selected. |
-

Roles

Creating new roles, defining permissions for roles, and assigning roles to users in Cisco WebEx Social are among the most important tasks that a system administrator performs. You can assign roles to individual users, user groups, and communities.



Note

Modifying permissions for or deleting an existing role can prevent users from accessing certain system functionality.

Roles are groupings of users that share a particular function within the portal. Roles can be scoped across the entire portal or for only a particular community.

Some types of roles you can create are:

- A portal-wide role to which you assign permissions for portal-wide activities, such as setting password policies and adding roles and users.

- A portal-wide role for the purpose of granting permissions to various functions within a specific portlet application. An example is to create a portal-wide role called “Message Board Administrator,” then assign permissions on various functions of a message board application (see the [“How to Define Application Permissions” section on page 2-21](#)), such as moving threads, adding subcategories, and adding files. Users to whom you give this role would then have whatever portlet permissions you assign, and the permissions would apply across the entire portal wherever a message board portlet application has been added to a page.
- A community-wide role for the purpose of granting permissions to various functions within a specific portlet application. An example is to create a community-wide role called “Message Board Administrator,” then assign permissions on various functions of a message board application (see the [“How to Define Application Permissions” section on page 2-21](#)), such as moving threads, adding subcategories, and adding files. Users to whom you give this role would then have whatever portlet permissions you assign, but the permissions would apply only to users within a community who have been assigned this role. Community roles must be assigned from within that community.

**Note**

Community administrators can assign community-wide roles to users in their community.



This section contains these topics:

- [Adding a Role, page 2-19](#)
- [Performing Actions for a Role, page 2-20](#)
- [Defining Permissions for a Role, page 2-21](#)

Adding a Role

To add a role, follow these steps:

Procedure

- Step 1** Access the Roles window:
 - a. Click the down-arrow  to the right of your name in the Global Navigation bar.
 - b. Select **Account Settings from** the drop-down menu.
 - c. Click the right-arrow  next to **Portal**
 - d. Click **Roles** in the Portal drawer.

The rOLEs window appears with the **View All** tab selected.
- Step 2** Select the **Add** tab.
- Step 3** In the Name field, enter a name of the role you wish to create.
- Step 4** In the Description field, enter some descriptive text about the role.
- Step 5** From the **Type** drop-down menu, select one of the following types:
 - Regular—Select this type if the role is performed for the entire portal.
 - Community—Select this type if the role is to be assigned to various communities.
- Step 6** Click **Save**.

The name of the role appears in the list of roles shown when the **View All** tab is selected.

Performing Actions for a Role

When the **View All** tab is selected in the Roles window, all roles within the portal are listed. Next to each role is an Actions drop-down menu. [Table 2-10](#) describes the selections in this menu. Not all selections appear for all roles

Table 2-10 *Actions You Can Perform for an Existing Role*

Function	Description
Edit	Lets you edit the name and the description of the role.
Permissions	<p>When you select Permissions, a list of roles appears (with links to each role's definition). This action allows you to change which roles are given what permissions on the selected role. Permission types that you can assign are:</p> <ul style="list-style-type: none"> • Assign Members—Lets someone assigned to the corresponding role assign members to this role • Define Permissions—Lets someone assigned to the corresponding role perform the Define Permissions action that this table describes • Delete—Lets someone assigned to the corresponding role delete this role from the portal • Manage Announcements—Lets someone assigned to the corresponding role manage announcements for this role • Permissions—Lets someone assigned to the corresponding role perform this Permissions action • Edit—Lets someone assigned to the corresponding role edit information about this role • View—Lets someone assigned to the corresponding role view the membership list for this role
Define Permissions	Lets you define permissions for this role. For more information, see the “Defining Permissions for a Role” section on page 2-21.
Assign Members	<p>Takes you to a window that displays current members who are assigned to this role, and lets you assign additional users and user groups to this role. These users and user groups inherit any permissions given to the role.</p> <p>To assign members to this role, you can click the Available tab and you can use the Search capabilities to locate users in the portal. Check the box next to the users or user groups to which you wish to assign this role, then click Update Associations. Now, when you click the Current tab, the users and user groups you just assigned to this role appears in the list of current members.</p> <p>To remove members from this role, click the Current tab, uncheck the box next to the member you wish to remove from this role, then click Update Associations. The name no longer appears in the list of current users with this role.</p>

Table 2-10 **Actions You Can Perform for an Existing Role (continued)**

Function	Description
View Users	Lets you view the users who are assigned this role.
Delete	Deletes this role.

Defining Permissions for a Role

When you select the **Define Permissions** action for a portal-scoped role, you have a choice of two kinds of permissions that can be defined for this role: Portal Permissions and Application Permissions. For other roles, you only have the option of defining portlet permissions.

Portal permissions cover portal-wide activities that can exist in many categories, including Community, Location, and Password Policy.

Application permissions cover permissions that are defined within each application.



This section includes these topics:

- [Defining Portal Permissions, page 2-21](#)
- [How to Define Application Permissions, page 2-21](#)
- [Deleting Application Permissions:, page 2-22](#)

Defining Portal Permissions

To define portal permissions, follow these steps:



Procedure

-
- | | |
|---------------|--|
| Step 1 | Access the Roles window: <ul style="list-style-type: none">a. Click the down-arrow  to the right of your name in the Global Navigation bar.b. Select Account Settings from the drop-down menu.c. Click the right-arrow  next to Portald. Click Roles in the Portal drawer. |
| Step 2 | Select Define Permissions from the Actions drop-down list for the applicable role.
Not all actions appear for all roles. |
| Step 3 | In the Define Permissions tab, click Add Portal Permissions . |
| Step 4 | For all categories that appear, select Portal from the Scope drop-down menu next to the action that you want this role to perform across the portal. For actions you do not want the role to perform, do not select anything from the Scope drop-down menu. |
| Step 5 | Click Save . |
-

How to Define Application Permissions

To define application permissions, follow these steps:



Procedure

- Step 1** Access the Roles window:
- Click the down-arrow  to the right of your name in the Global Navigation bar.
 - Select **Account Settings** from the drop-down menu.
 - Click the right-arrow  next to **Portal**
 - Click **Roles** in the Portal drawer.
- Step 2** Select **Define Permissions** from the Actions drop-down list for the applicable role.
Not all actions appear for all roles.
- Step 3** In the Define Permissions tab, click **Add Application Permissions**.
A window displays the names of all applications that are currently installed in your portal.
- Step 4** Click the name of the application for which you want to define the actions that this role can perform.
A new window displays that shows all the configurable permissions for this application.
- Step 5** Select the scope from the Scope drop-down menu next to the actions that you want this role to perform.
There are two scoping choices for each action:
- Portal—Selecting this option means that the permission is granted across the portal, in any community where this application exists.
 - Communities—Selecting this option invokes a **Select** button, which you use to select specific communities (for a portal-scoped role) in which these permissions are valid for users in this role.
- For actions you do not want the role to perform, do not select anything from the Scope drop-down menu.
- Step 6** Click **Save**.
-

Deleting Application Permissions:

To delete application permissions, follow these steps:

Procedure

- Step 1** Access the Roles window:
- Click the down-arrow  to the right of your name in the Global Navigation bar.
 - Select **Account Settings** from the drop-down menu.
 - Click the right-arrow  next to **Portal**
 - Click **Roles** in the Portal drawer.
- Step 2** Select **Define Permissions** from the Actions drop-down list for the applicable role.
- Step 3** Choose **Delete** from the Actions drop-down menu for the permission that you wish to delete.
-

Password Policies

Password policies can enhance the security of your portal. Using password policies, you can set password rules such as password strength, and frequency of password expiration. You can assign different password policies to different sets of users in the portal.

Password policies apply only to users that you add to Cisco WebEx Social as described in the [“Adding a User Manually” section on page 2-2](#). If you are using LDAP synchronization to synchronize with an LDAP directory, passwords are managed in the LDAP directory.



This section contains these topics:

- [Adding a Password Policy, page 2-23](#)
- [Performing Actions for an Existing Password Policy, page 2-24](#)

Adding a Password Policy

To add a password policy, follow these steps:

Procedure

-
- Step 1** Access the Password Policies window:
- a. Click the down-arrow  to the right of your name in the Global Navigation bar.
 - b. Select **Account Settings** from the drop-down menu.
 - c. Click the right-arrow  next to **Portal**
 - d. Click **Password Policies** in the Portal drawer.
- The Password Policies window appears with the View All tab selected.
- Step 2** Select the **Add** tab.
- Step 3** In the Name field, enter a name for the password policy.
- Step 4** In the Description field, enter a description of the password policy.
- Step 5** If you want to allow users to change their passwords, take these actions:
- a. Check the Changeable box (unchecked by default).
The Change Required and Minimum Age options appear.
 - b. Check the Change Required box (unchecked by default) if you want to require users to change their passwords when they first sign in.
 - c. From the Minimum Age drop-down list, select how long users must wait before changing their passwords again.
- Step 6** If you check the Syntax Checking Enabled box (unchecked by default), Cisco WebEx Social allows you to select whether dictionary words can be passwords as well as allowing you to set minimal lengths for passwords.
- Step 7** If you check the History Enabled box (unchecked by default), Cisco WebEx Social does not allow users to use a password they have already used.
- Step 8** If you check the Expiration Enabled box (unchecked by default), you can configure how frequently users must change their passwords and also much advance warning to give users that their password is about to expire.

- Step 9** If you check the Lockout Enabled box (unchecked by default), you can configure several items relating to lockouts, including the maximum number of times users can attempt to log in to Cisco WebEx Social before their accounts get locked.
- Step 10** Click **Save**.

Performing Actions for an Existing Password Policy

When the **View All** tab is selected in the Password Policies window, all password policies are listed. Next to each policy is an **Actions** drop-down menu. [Table 2-11](#) describes the selections in this menu.

Table 2-11 *Actions You Can Perform for an Existing Password Policy*

Function	Description
Edit	Allows you to modify the selected password policy.
Permissions	<p>When you select Permissions, a list of roles appears (with links to each role's definition). This action allows you to change which roles are given what permissions on the selected password policy. You can assign these permission types:</p> <ul style="list-style-type: none"> Assign Members—Not used Delete—Lets someone who is assigned to the corresponding role delete this password policy from the portal Permissions—Lets someone who is assigned to the corresponding role perform this Permissions action Edit—Lets someone who is assigned to the corresponding role modify this password policy View—Lets someone who is assigned to the corresponding role view the membership list that this password policy is assigned to <p>After making changes, click Save, or click Cancel to exit without saving your changes.</p>
Assign Members	<p>Takes you to a window that displays current users who are assigned this password policy, and lets you assign this password policy to additional users.</p> <p>To assign this password policy to users, you can click the Available tab and you can use the Search capabilities to locate users in the portal. Check the box next to the users to which you wish to assign this password policy, then click Update Associations. Now, when you click the Current tab, the users you just assigned this password policy appears in the list of current members.</p> <p>To remove users from being assigned this password policy, click the Current tab, uncheck the box next to the users you wish to remove from this policy, then click Update Associations. The members no longer appears in the list of current members who are assigned this policy.</p>
Delete	<p>Allows you to delete any password policy that you added. However, you cannot delete the default policy.</p> <p>This option does not apply to the Default Password Policy.</p>

Community Manager

The Community Manager window in the Portal Drawer allows you to create categories of communities for your users. Then, when users create new communities, they can choose the category that best suits their needs. The main differentiator among community categories is which templates you choose to add to a category. You can create custom templates and include as many templates as you want for any category.

This section contains these topics:

- [Defining Settings for a Community Category, page 2-25](#)
- [Managing Templates for a Community Category, page 2-26](#)
- [Managing Community Categories, page 2-28](#)
- [Reassigning Community Categories, page 2-29](#)
- [Properties You can Change That Affect the User Click-to-Create-Community Feature, page 2-30](#)

Related Topic

[Communities, page 2-11](#)

Defining Settings for a Community Category

Before creating new categories, follow these steps to define general settings to apply to all categories that you create:

Procedure



-
- | | |
|---------------|---|
| Step 1 | Access the Community Manager window: <ol style="list-style-type: none">Click the down-arrow  to the right of your name in the Global Navigation bar.Select Account Settings from the drop-down menu.Click the right-arrow  next to PortalClick Community Manager in the Portal drawer. The Community Manager window appears with the Categories tab selected. |
| Step 2 | Select the Settings tab. |
| Step 3 | Complete the configuration in this window by referring to the field descriptions provided in Table 2-12 . |
| Step 4 | Click Save . |
-



Table 2-12 Community Manager Window—Settings Tab

Field	Description
Approval Required	<p>If unchecked, the following checkbox is included in the Create a Category window:</p> <p>“Communities in this category require approval”</p> <p>In this case, users creating new communities within this category need system-administrator approval before the new community can go live.</p> <p>Default: The checkbox called “Communities in this category require approval” does not appear in the Create a Category window.</p>
Code of Conduct or Terms and Conditions Disable	<p>If checked, causes the Code of Conduct box to appear in the Create Community dialog box when a user creates a new community.</p> <p>Default: The Code of Conduct box does appear in the Create Community dialog.</p>
Community profile picture customization Disable	<p>If checked, community creators do not have the option of importing their own picture for their community profile that can be different from the picture of the category itself.</p> <p>Default: Community profile picture customization is allowed.</p>
Default General Category	<p>If checked, the default General category is hidden in the Create Community dialog box.</p> <p>Default: General category is not hidden.</p>
Link to “Code of Conduct”	<p>URL to the location where you have stored the Code of Conduct text that you want displayed to new users of a community.</p>
Link to layout customization tutorial	<p>URL to the location where you have stored a video file of the tutorial for layout customization.</p> <p>This link is opened when users click the tutorial link in the banner of a community in draft mode.</p>

Managing Templates for a Community Category

You can view or modify templates for a community category, and you can upload custom templates in Cisco WebEx Social so that they can be used in community categories.

Procedure to View or Modify an Existing Template

- Step 1** Access the Community Manager window:
- Click the down-arrow  to the right of your name in the Global Navigation bar.
 - Select **Account Settings** from the drop-down menu.
 - Click the right-arrow  next to **Portal**
 - Click **Community Manager** in the Portal drawer.

The Community Manager window appears with the Categories tab selected.

- Step 2** Select the **Templates** tab.

Step 3 Click one of the templates to view or modify that template.



Note The default standard templates for Open, Hidden and Restricted communities should already appear in the Manage Templates window.

Step 4 Make any desired changes for the template that you selected (see [Table 2-13](#) for field definitions).



Step 5 Click **Save**.

Procedure to Add a Custom Template



Note To create a custom template, create a LAR file and save it as described in the [“Creating a Custom Community Template”](#) section on page A-1.

Step 1 Access the Community Manager window:

- a. Click the down-arrow  to the right of your name in the Global Navigation bar.
- b. Select **Account Settings** from the drop-down menu.
- c. Click the right-arrow  next to **Portal**.
- d. Click **Community Manager** in the Portal drawer.

The Community Manager window appears with the Categories tab selected.

Step 2 Select the **Templates** tab.

Step 3 Click **New Template**.

Step 4 In the Template window, enter values for the fields shown in [Table 2-13](#).

Step 5 Click **Save**.

Step 6 If you want to associate this template with a community category, follow the steps in the [Procedure to View or Modify an Existing Template](#), page 2-26.

Table 2-13 Community Manager Window—Template Tab

Field	Description
Name	A descriptive name for the template you are adding or modifying.
Upload Template (.lar) file	The .lar file of the template you are adding. Use the Browse button to locate the .lar file.
Upload Preview Image	The image that depicts the number and layout of the tabs the template uses. Use the Browse button to locate the image file.
Membership Type	Drop-down list from which you choose the type of community the template is designed for: an Open, Restricted, or Hidden community. Note Be sure that the membership type you choose is consistent with the page-level and portlet-level permissions of the .lar file. The system cannot detect inconsistencies of this type.



Table 2-13 Community Manager Window—Template Tab (continued)

Field	Description
Description	As complete a description as possible so that a user creating a community knows which template to select.
Tabs	Names of all tabs, separated by commas, to appear in the template.



Managing Community Categories

You can view or modify community categories, and you can add a new category.

Procedure to View or Modify Existing Categories

-
- Step 1** Access the Community Manager window:
- Click the down-arrow  to the right of your name in the Global Navigation bar.
 - Select **Account Settings** from the drop-down menu.
 - Click the right-arrow  next to **Portal**
 - Click **Community Manager** in the Portal drawer.
- The Community Manager window appears with the Categories tab selected.
- Step 2** Select the **Categories** tab.
- Step 3** Click one of the categories to view or modify that category.
- Step 4** Make any desired changes for the category you clicked on (see [Table 2-14](#) for field definitions).
- Step 5** Click **Save**.
-

Procedure to Add a New Category


-
- Step 1** Access the Community Manager window:
- Click the down-arrow  to the right of your name in the Global Navigation bar.
 - Select **Account Settings** from the drop-down menu.
 - Click the right-arrow  next to **Portal**
 - Click **Community Manager** in the Portal drawer.
- The Community Manager window appears with the Categories tab selected.
- Step 2** Select the **Templates** tab.
- Step 3** Click **New Category**.
- Step 4** In the Create a Category window, enter values for the fields shown in [Table 2-14](#).



Note You cannot delete a category after it has been saved.

- Step 5** Click **Save**.
-

Table 2-14 Community Manager Window—Categories Tab

Field	Description
Title	A descriptive name for the category you are adding or modifying.
Image	Image that depicts the category. Use the Browse button to locate the image file. This image is used for any community created within this category unless you have allowed (with the Settings tab) the community creator to import their own community image.
Description	A description of this category and the types of communities that should use this category. For example, if you create a category called “Hobbies and Leisure,” you might want to have a description such as: “Communities for all non-work related activities.” You would also probably create a template specifically for such a category with the pages named accordingly.
Contact email	E-mail address where questions about a community are sent.
Communities in this category require approval	Box that appears if you unchecked the Approval Required Disabled box in the Settings tab.  Caution This field should be used only by Cisco-Internal system administrators for Cisco-internal users. If you check this box, you then have the option to click a link called “Add a Question,” which allows you to add customized questions for a category, and assign an alternate, automated approval workflow based on the users’ responses. A maximum of two questions can be set per category.
Template	List of default templates and any custom templates you have added. You must select at least one template for a category. Then, when users create a community, they are given the choice of which template to select for the community category they select.

Reassigning Community Categories

You can reassign existing communities to new categories that you have created, and you can change categories for new communities.

The following guidelines apply for changing the category of a community:

- Communities that do not require approval can be changed to any category that does not require approval.
- Live communities can be moved to any community category.
- Communities remain in the same state they were in before they changed categories. States are either “live” or “draft.”

Properties You can Change That Affect the User Click-to-Create-Community Feature

As a system administrator, there are a number of properties that you can edit to change the appearance and text of the screens presented to users as they create new communities.

This section describes the screens with appearances that you can affect by changing specific properties:

- [Properties You Can Change for Step 1 of the Click-to-Create Feature, page 2-30](#)
- [Properties You Can Change for the Community Summary Window, page 2-30](#)
- [Properties You Can Change For A Community in Draft Mode, page 2-31](#)

Properties You Can Change for Step 1 of the Click-to-Create Feature

To create a new community, users start by clicking **Community** in the Global Navigation bar, and then clicking the **New Community** button. The first Create a Community window appears. You can change the “Select a Category and Membership Type” heading and the text that appears under this heading in this window. To do so, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Click **Portal** under Application.

Step 3 In the Advanced Portal Properties area, change the following property to **true**:

`com.cisco.ecp.communities.category_selection_configured=false`



Note If you want to revert to the default settings, set this property back to **false**.

Step 4 Take either or both of these actions:

- To change the “Select a Category and Membership Type” text, edit the `com.cisco.ecp.communities.category.name` property.
- To change the “Choose a category for your community to appear in. Some categories may require approval prior to activation” text, edit the `com.cisco.ecp.communities.category.desc` property.

Step 5 Click **Save** in the Advanced Portal Properties area.

Properties You Can Change for the Community Summary Window

The next window in the Click-to-Create community is the Review your community window, which is presented to users after they have completed Steps 2 and 3 (entering basic information and choosing a community template).


If you did not disable the Code of Conduct in the Community Manager Window> Settings Tab, a user creating a new community is presented with the Code of Conduct box.

There are two items you can change regarding Code of Conduct:

- The wording “I will abide by the Company”
- The wording of the “Code of Conduct” link before the box.

If you want to change either of these properties, follow these steps:

Procedure

-
- Step 1** Sign in to the Director.
- Step 2** Click **Portal** under Application.
- Step 3** In the Advanced Portal Properties area, change the following property to **true**:
`com.cisco.ecp.communities.code_of_conduct.configured=false`
- 
- Note** If you want to revert to the default settings, set this property back to **false**.
-
- Step 4** Take either or both of these actions:
- To change the “I will abide by the Company” text, edit the `com.cisco.ecp.communities.code_of_conduct.text` property.
 - To change the “Code of Conduct” link before the check box text, edit the `com.cisco.ecp.communities.code_of_conduct.link_text` property.
- Step 5** Click **Save** in the Advanced Portal Properties area.
-

Properties You Can Change For A Community in Draft Mode

After the community creator clicks **Create** in the Community Summary window, the community enters “draft mode.” You can change the default values of several properties that affect the appearance of communities that are in draft mode (see the items that are called out in [Figure 2-1](#)). If you want to change any of these properties, do the following:

Procedure



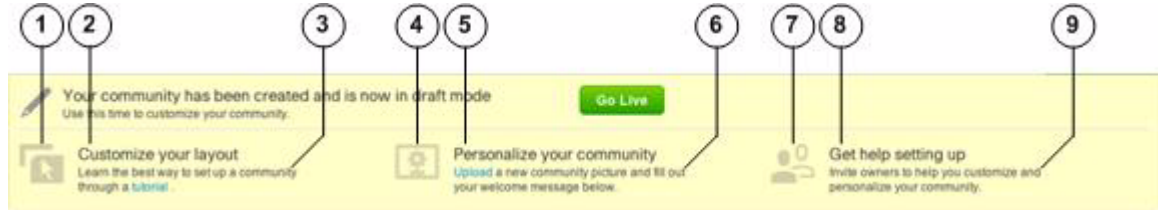
-
- Step 1** Sign in to the Director.
- Step 2** Click **Portal** under Application.
- Step 3** In the Advanced Portal Properties area, change the following property to **true**:
`create-community-draft-mode-enable-customize-text=false`
- 
- Note** If you want to revert to the default settings, set this property to **false**.
-
- Step 4** See [Figure 2-1](#) for an explanation of what you can change and the corresponding properties you can edit in the Advanced Portal Properties area.
- 
- Note** Make sure to place any images you are changing in the folder
`/opt/cisco/quad/tomcat/webapps/ROOT/html/themes/classic/images/communities`
-
- Step 5** Click **Save** in the Advanced Portal Properties area.
-

Figure 2-1 Properties You Can Change for a Community in Draft Mode

Item	Corresponding Property To Set in Advanced Portal Properties area
1	create-community-draft-mode-step1-image-path
2	create-community-draft-mode-step1-title
3	create-community-draft-mode-step1-description
4	create-community-draft-mode-step2-image-path
5	create-community-draft-mode-step2-title
6	create-community-draft-mode-step2-description
7	create-community-draft-mode-step3-image-path
8	create-community-draft-mode-step3-title
9	create-community-draft-mode-step3-description

WebEx Social Functionality



The WebEx Social Functionality window allows you to disable and reenable a number of Cisco WebEx Social features.

If you need to disable any features, Cisco recommends that you do so before your users begin using Cisco WebEx Social.

As a best practice, avoid enabling and disabling features that are used in a production environment unless necessary.

To disable or reenable a feature, follow these steps:

Procedure

- Step 1** Access the WebEx Social Functionality window:
 - a. Click the down-arrow  to the right of your name in the Global Navigation bar.
 - b. Select **Account Settings** from the drop-down menu.
 - c. Click the right-arrow  next to **Portal**
 - d. Click **WebEx Social Functionality** in the Portal drawer.
- Step 2** Check the box next to each feature that you want to disable (or reenable if they are already disabled).
- Step 3** Click **Save**.

- Step 4** Go to the Director, sign in with your administrator user ID and password, and take these actions to cause the changes that you made in the Cisco WebEx Social Functionality window to take effect:
- Click **Topology**
 - Click the **Disable** button for each App Server node.
 - Click the **Disable** button for the Cache node.
 - Click the **Enable** button for the Cache node.
 - Click the **Enable** button for each App Server node.
-

Notes About Behavior

- Any features that you disable or reenable apply to all Cisco WebEx Social users.
- When a feature is disabled or reenabled, all icons, tabs or other items related to that feature either disappear or reappear, depending on the action you took.
- If you decide to disable the videos or documents features later, existing videos and documents can still be located with a search.



WebEx Social Metrics

The WebEx Social Metrics window lets you view information and generate reports about the use of Cisco WebEx Social.

The **Total active unique users in the last minute** field shows how many unique users actively used Cisco WebEx Social in the last minute. (This field does not refresh automatically. To see current information this field, refresh your browser page.)

To generate and view reports, follow these steps:

Procedure

-
- Step 1** Access the WebEx Social Metrics window:
- Click the down-arrow  to the right of your name in the Global Navigation bar.
 - Select **Account Settings** from the drop-down menu.
 - Click the right-arrow  next to **Portal**
 - Click **WebEx Social Metrics** in the Portal drawer.
- Step 2** In the WebEx Social Metrics window, check the box for each type of information that you want to be included in the report.
- Step 3** In the Generate Report From and To fields, enter the start date and end date, respectively, for the information to be included in the report.
- Step 4** Click **Generate Reports**.
- The system generates the reports that contain the information that you requested and the reports appear in the list at the bottom of the WebEx Social Metrics window.

The reports contain information for a 24-hour period for each day in the date range that you specified. The start time and end time of the information in the report is defined by the Hour of Day (UTC) option in the Configuration page of the Director (see the [“Analytics Store Cron Job” section on page 5-6](#)). All dates and times that the reports show are in Coordinated Universal Time (UTC).

For a description of the reports that you can generate, see the [“Cisco WebEx Social Metrics Reports” section on page 2-34](#)

You can take either of these actions in the list of reports:

- Click the name in the File Name column for the report to open a comma-separated value (CSV) version of the report. You can then save the report to the location of your choice.
 - Click the box for one or more reports and then click **Delete** to delete the selected reports.
-

Cisco WebEx Social Metrics Reports

The following sections describes the Cisco WebEx Social metrics reports that you can generate:

- [Top Contributors Report, page 2-34](#)
- [Active Users Report, page 2-35](#)
- [Top Communities By Activity Volume Report, page 2-36](#)
- [Top Communities by Member Count Report, page 2-36](#)
- [Total Number of Communities Report, page 2-37](#)
- [Number of Discussion Messages per Community Report, page 2-37](#)
- [Storage Consumed Per User Library \(in Bytes\) Report, page 2-37](#)
- [Total Number of Microposts Report, page 2-38](#)
- [Total Number of Posts \(All, including Microposts\) Report, page 2-38](#)

Top Contributors Report

A Top Contributors report is named `metrics-top-contributors_ID.csv`.

A *contributor* is a Cisco WebEx User who has created or uploaded any single or combination of text posts, video posts, wall posts, community wall posts, microposts, discussion posts, documents, images, and attachments. The system calculates a *contribution score* for each contributor by multiplying the total number of each item by a default weighting value, then totaling the weighted product for each item. This calculation considers all items that a user has created or uploaded since the user was set up in Cisco WebEx Social.

By default, this report shows the five contributors with the highest contribution scores for each 24-hour period within the report period.

If you want to adjust the default number of contributors that this report shows for each 24-hour period or the default weights that the system assigns to the items in a contribution score, contact Cisco support.

[Table 2-15](#) describes the fields in the Top Contributors report.

Table 2-15 Top Contributors Report Fields

Field	Description
Date	Ending date and time of a 24-hour period
Top Contributors	Cisco WebEx Social users with the highest contribution scores as of the end of the corresponding 24-hour period

Active Users Report

An Active Users report is named `metrics-total-active-users_ID.csv`.

This report shows the total number of unique users who accessed at least one Cisco WebEx Social page, the total number of activities, and the browser on which activities were performed for each 60-minute period within the report period.

The system determines that single activity occurs when a user accesses one or more Cisco WebEx Social pages in a 1-minute period. For example, if a user accesses two pages in 1 minute, then one page in another 1 minute period, the system determines that two activities occurred.

[Table 2-16](#) describes the fields in the Active Users report.

Table 2-16 Active Users Report Fields

Field	Description
Date	Ending date and time of a 60-minute period
Unique Active Users	The number of unique users who accessed at least one Cisco WebEx Social page during the corresponding 60-minute period
Total Active Users	Total number of activities performed during the corresponding 60-minute period
Mobile	Total number of activities performed by a user using a mobile device during the corresponding 60-minute period
Firefox 5.x +	Total number of activities performed by a user using release 5 or above of the Mozilla Firefox browser during the corresponding the 60-minute period
Firefox 4	Total number of activities performed by a user using release 4 of the Mozilla Firefox browser during the corresponding the 60-minute period
Firefox 3	Total number of activities performed by a user using release 3 or above of the Mozilla Firefox browser during the corresponding the 60-minute period
IE 10	Total number of activities performed by a user using release 10 of the Internet Explorer browser during the corresponding the 60-minute period
IE 9	Total number of activities performed by a user using release 9 of the Internet Explorer browser during the corresponding the 60-minute period
IE 8	Total number of activities performed by a user using release 8 of the Internet Explorer browser during the corresponding the 60-minute period

Table 2-16 Active Users Report Fields (continued)

Field	Description
IE 7	Total number of activities performed by a user using release 7 of the Internet Explorer browser during the corresponding the 60-minute period
IE 6 and below	Total number of activities performed by a user using release 6 or below of the Internet Explorer browser during the corresponding the 60-minute period
Chrome	Total number of activities performed by a user using the Google Chrome browser during corresponding the 60-minute period
Safari	Total number of activities performed by a user using the Apple Safari browser during corresponding the 60-minute period
Opera	Total number of activities performed by a user using the Opera browser during corresponding the 60-minute period
Unknown	Total number of activities performed by a user using an unidentified browser during corresponding the 60-minute period

Top Communities By Activity Volume Report

A Top Communities By Activity Volume report is named `metrics-top-communities-by-volume_ID.csv`.

By default, this report shows the five communities with the highest *activity scores* for each 24-hour period within the report period. The system calculates an activity score for a community by multiplying the total number of posts, images, attachments, documents and discussions in the community by a default weighting value, then totaling the weighted product for each item.

If you want to adjust the default number of communities that this report shows for each 24-hour period or the default weights that the system assigns to the items in an activity score, contact Cisco support.

[Table 2-17](#) describes the fields in the Top Communities By Activity Volume report.

Table 2-17 Top Communities By Activity Volume Report Fields

Field	Description
Date	Ending date and time of a 24-hour period
Top Communities by Activity	Communities with the highest activity scores as of the end of the corresponding 24-hour period

Top Communities by Member Count Report

A Top Communities by Member Count report is named `metrics-top-communities-by-count_ID.csv`.

By default, this report shows the five communities with the highest number of members at the end of each 24-hour period within the report period. This number includes active and inactive members.

If you want to adjust the default number of communities that this report shows for each 24-hour period, contact Cisco support.

[Table 2-18](#) describes the fields in the Top Communities by Member Count report.

Table 2-18 Top Communities by Member Count Report Fields

Field	Description
Date	Ending date and time of a 24-hour period
Top Communities	Communities with the highest number of members as of the end of the corresponding 24-hour period
Member Count	Number of members in the corresponding community

Total Number of Communities Report

A Total Number of Communities report is named `metrics-total-communities_ID.csv`.

This report shows the total number of communities that exist in Cisco WebEx Social at the end of each 24-hour period within the report period. This number includes active and inactive communities.

[Table 2-19](#) describes the fields in the Total Number of Communities report.

Table 2-19 Total Number of Communities Report Fields

Field	Description
Date	Ending date and time of a 24-hour period
Total Number of Communities	Number of active and inactive communities in Cisco WebEx Social as of the end of the corresponding 24-hour period

Number of Discussion Messages per Community Report

A Number of Discussion Messages per Community report is named `metrics-num-discussion-threads_ID.csv`.

This report shows the following information:

- If the report period is 31 days or fewer, the number of discussion messages that exist in each community at the end of each 24-hour period in the report period
- If the report period is 32 days or more, the number of discussion messages that exist in each community at the end of each month in the report period

[Table 2-20](#) describes the fields in the Number of Discussion Messages per Community report.

Table 2-20 Number of Discussion Messages per Community Report Fields

Field	Description
Group Name	Ending date and time of a 24-hour period
<i>Month-Date-Year</i> or <i>Month-Year</i>	Number of discussion messages that exist in each community as of the end of the corresponding day or month

Storage Consumed Per User Library (in Bytes) Report

A Storage Consumed Per User Library (in Bytes) report is named `metrics-storage-consumed_ID.csv`.

This report shows, for each user, the number of bytes that are consumed by all images, documents, and attachments that the user has uploaded to Cisco WebEx Social. The report displays information as follows:

- If the report period is 31 days or fewer, the number bytes consumed at the end of each 24-hour period in the report period
- If the report period is 32 days or more, the number of bytes consumed at the end of each month in the report period

[Table 2-21](#) describes the fields in the Number of Discussion Messages per Community report.

Table 2-21 Storage Consumed Per User Library (in Bytes) Report Fields

Field	Description
Group Name	Cisco WebEx User
<i>Month-Date-Year</i> (Storage consumed in Bytes) or <i>Month-Year</i>	Number bytes consumed by all images, documents, and attachments that a user has uploaded as of the end of the corresponding day or month

Total Number of Microposts Report

A Total Number of Microposts report is named `metrics-total-micropost-num_ID.csv`.

This report shows the total number of microposts that exist in Cisco WebEx Social at the end of each 24-hour period within the report period.

[Table 2-22](#) describes the fields in the Total Number of Microposts report.

Table 2-22 Total Number of Microposts Report Fields

Field	Description
Date	Ending date and time of a 24-hour period
Total Microposts	Number microposts in Cisco WebEx Social as of the end of the corresponding 24-hour period

Total Number of Posts (All, including Microposts) Report

A Total Number of Posts (All, including Microposts) report is named `metrics-total-post-num_ID.csv`.

This report shows the total number of posts, including microposts, that exist in Cisco WebEx Social at the end of each 24-hour period within the report period.



[Table 2-23](#) describes the fields in the Total Number of Posts (All, including Microposts) report.

Table 2-23 Total Number of Posts (All, including Microposts) Report Fields

Field	Description
Date	Ending date and time of a 24-hour period
Total Posts	Number posts in Cisco WebEx Social as of the end of the corresponding 24-hour period

Settings

The Settings window in the Portal Drawer provides access to most global portal settings.

To access the Settings window, click the down-arrow  to the right of your name in the Global Navigation bar, select **Account Settings** from the drop-down menu, click the right-arrow  next to **Portal**, and then click **Settings** in the Portal drawer.

After making changes to setting options, click **Save**, or click **Cancel** to exit without saving your changes.

Settings are arranged in these categories:

- [General, page 2-39](#)—Lets you configure global settings, including the company name, domain, and virtual host
- [Authentication, page 2-40](#)—Lets you configure login IDs, connection to LDAP, single sign-on, and several other settings
- [Users, page 2-51](#)—Lets you configure default memberships to roles, user groups, and communities for new users.
- [Mail Host Names, page 2-52](#)—Lets you configure e-mail servers
- [Reported Content, page 2-53](#)—Lets you set the number of times that Cisco WebEx Social users can report content as inappropriate or incorrect before Cisco WebEx Social automatically hides the content
- [Display Settings, page 2-53](#)—Lets you configure the language, time zone, and custom log for Cisco WebEx Social
- [Custom Settings, page 2-53](#)—Lets you configure whether an activity is generated when a link is created or updated in a post

General

General settings include global settings, such as your company name, domain, and virtual host, and various navigation settings. To access the General settings options, click the **General** link at the right side of the Settings window (the “[Settings](#)” section on [page 2-39](#) describes how to access this window).

[Table 2-24](#) describes the General settings options.

Table 2-24 General Settings Options

Field	Description
Main Configuration Fields	
Name	The name of the company or organization that owns the portal.
Mail Domain	The domain of your company mail server.
Virtual Host	The fully qualified domain name of the Cisco WebEx Social node.
Navigation Fields	
Home URL	<p>The home page of the portal.</p> <p>For example, if the home page URL is <code>http://localhost:8080/web/guest/home</code> then set this field to <code>/web/guest/home</code>.</p> <p>In general, the value in this field does not need to be changed.</p>

Table 2-24 **General Settings Options (continued)**

Field	Description
Default Landing Page	<p>Page that users are automatically directed to after signing in to Cisco WebEx Social.</p> <p>For example, if the URL of the default landing page is <code>http://localhost:8080/web/guest/login</code> then set this field to <code>/web/guest/login</code>.</p> <p>This field typically needs to be updated only if you are using SSO.</p>
Default Logout Page	<p>Page that users are automatically redirected to after signing out of Cisco WebEx Social.</p> <p>For example, if the URL of the default landing page is <code>http://localhost:8080/web/guest/logout</code> then set this field to <code>/web/guest/logout</code>.</p> <p>This field typically needs to be updated only if you are using SSO.</p>

Authentication

Authentication settings control how users authenticate to Cisco WebEx Social. To access the Authentication settings options, click the **Authentication** link at the right side of the Settings window (the “Settings” section on page 2-39 describes how to access this window).

Authentication settings options are arranged on these tabs:

- [General, page 2-40](#)
- [LDAP Authentication, page 2-41](#)
- [LDAP Directory Sync, page 2-44](#)
- [LDAPS Authentication and Synchronization, page 2-46](#)
- [NTLM, page 2-47](#)
- [SiteMinder, page 2-49](#)
- [OAM, page 2-49](#)
- [Kerberos, page 2-50](#)
- [SAML SSO, page 2-51](#)

General

The General tab in the Settings > Authentication window allows you to customize default authentication behavior.

[Table 2-25](#) describes the options in this window.

Table 2-25 General Authentication Settings Options

Field	Description
How do users authenticate?	Choose one of these values from the drop-down list to designate how users authenticate to Cisco WebEx Social: <ul style="list-style-type: none"> • By screen name • By e-mail address (default)
Allow users to automatically sign in?	If this box is checked (unchecked by default), Cisco WebEx Social allows users to set up their own automatic login by checking the Remember Me box when they log in. If this box is not checked, Cisco WebEx Social users must log in manually.
Allow users to request forgotten passwords?	Not used.
Allow strangers to create accounts?	Not used.
Allow strangers to create accounts with a company e-mail address?	Not used.
Require strangers to verify their email address?	Not used.

LDAP Authentication

The LDAP Authentication tab in the Settings > Authentication window allows you to configure LDAP authentication options.

LDAP authentication uses directory servers, such as Microsoft Active Directory, to authenticate users. If a user is not already in the Cisco WebEx Social database, Cisco WebEx Social pulls user information such as first and last name, and e-mail address into its database.

[Table 2-26](#) lists describes the options in this tab. You need to contact the administrator of the LDAP server to obtain administrative user credentials.

Table 2-26 LDAP Authentication Options

Setting	Description
Enabled	Enables or disables LDAP authentication. Default: Enabled
Required	Requires LDAP authentication if this box is checked. Cisco WebEx Social does then not allow users to sign in unless they can first successfully <i>bind</i> (connect) to the LDAP directory. Leave this box unchecked (default) if you want to allow users who have Cisco WebEx Social accounts but no LDAP accounts to sign in to Cisco WebEx Social. Note If the Required box is checked and LDAP is down, no users are able to sign in to Cisco WebEx Social.

Table 2-26 LDAP Authentication Options (continued)

Setting	Description
Default Values	Identifies the LDAP server type. If you are using one of the directory servers listed under Default Values, select that directory, then click Reset Values . The fields in this window are then populated with the default values for that directory.
Connection These options cover the basic connection to LDAP.	
Base Provider URL	<p>Provides the URL of the LDAP server to the portal. Should match the value in the LDAP Hostname/IP and the LDAP Port fields in the Notifier area in the Configuration window of the Director (see the “Notifier” section on page 5-4). Make sure that the machine on which Cisco WebEx Social is installed can communicate with the LDAP server. If a firewall exists between the two machines, make sure that the appropriate ports are open.</p> <p>Format of the URL <code>ldap://host:portnumber</code></p> <p>Example <code>ldap://ds.cisco.com:389</code></p>
Base DN (optional)	The Base Distinguished Name specifies the initial search context in LDAP for users. Should match the value in the Base DN field in the Notifier area in the Configuration window of the Director (see the “Notifier” section on page 5-4).
Principal	<p>LDAP administrator ID. If you have removed the default LDAP administrator, enter the fully qualified name of the administrative credential that you use. Should match the value in the Admin DN field in the Notifier area in the Configuration window of the Director (see the “Notifier” section on page 5-4).</p> <p>You need an administrative credential because Cisco WebEx Social uses this ID to synchronize user accounts to and from the LDAP server.</p> <p>Example: The default Windows Domain Administrator is: <code>cn=administrator,cn=users,dc=your_domain,dc=[com net local].</code></p>
Credentials	Password of the LDAP administrator. Should match the value in the Credentials field in the Notifier area in the Configuration window of the Director (see the “Notifier” section on page 5-4).
Test LDAP Connection	Click this button to make sure that your connection to the LDAP server is working.

Table 2-26 LDAP Authentication Options (continued)

Setting	Description
Users These options are for finding users in the LDAP directory.	
Authentication Search Filter	<p>Maps a Cisco WebEx Social user attribute to an LDAP attribute for matching user data.</p> <p>This filter must be enclosed within parentheses (()).</p> <p>Examples</p> <p>(cn=@screen_name@) or (sAMAccountName=@screen_name@).</p> <p>If you change the authentication to e-mail address, for example, you must also change the filter to mail=@email_address@. Otherwise authentication for newly created AD users fails.</p>
Import Search Filter	<p>LDAP object type used to filter the search.</p> <p>Depending on the LDAP server, there are different ways to identify the user.</p> <p>Default: (objectClass=Person)</p> <p>This default value is required for the Identity Store.</p> <p>If you want to search for only a subset of users or users that have different object classes, you can change this setting.</p> <p>This option applies only to bulk import of users. It is not used for authentication purposes.</p>
User Mapping	<p>If you have a special LDAP schema, you must define mappings from LDAP attributes to Cisco WebEx Social fields. For the user to be recognized, you must define mappings to the corresponding attributes in LDAP for the following Cisco WebEx Social fields:</p> <ul style="list-style-type: none"> • Screen Name, which is the default login ID in Cisco WebEx Social and typically matches the Windows account name of a user. For the Identity Store, the Screen Name must be uid. • Password • E-mail Address • First Name • Last Name <p>The remaining User Mapping fields—Job Title, Group, and Phone—are optional. If Group is populated with the correct AD attribute (<i>memberOf</i>), Cisco WebEx Social pulls group membership from the AD during user sign in and creates the corresponding user groups in Cisco WebEx Social. This activity may affect performance during sign in for users who are members of many AD groups.</p>

Table 2-26 LDAP Authentication Options (continued)



Setting	Description
Test LDAP Users	<p>After you complete the user mapping, you can click the Test LDAP Users button and Cisco WebEx Social attempts to match LDAP users with their mappings.</p> <p>Cisco WebEx Social displays a list of LDAP users who were successfully mapped.</p> <p>Cisco WebEx Social does not import users who do not have all of the following attributes: Screen Name, First Name, Last Name, Email, and Password.</p> <p>It is a best practice to verify that mappings are correct.</p>
Password Policy	
Use LDAP Password Policy	<p>It is recommended that this box be unchecked (default).</p> <p>By default, Cisco WebEx Social uses the password policy configured in the Portal > Password Policies tab of the control panel. Therefore, if you enable the LDAP Password Policy setting, the Portal > Password Policies tab displays a message that you are not using a local password policy.</p> <p>Note If you enable the Use LDAP Password Policy field, you must use the LDAP directory mechanism for setting password policies. If you are using a different LDAP server, contact your Cisco support representative).</p>

LDAP Directory Sync

The LDAP Directory Synch tab in the Settings > Authentication window allows you synchronize your users with Cisco WebEx Social.

After you configure the items in the LDAP Authentication tab (see the [“LDAP Authentication” procedure on page 2-41](#)), follow these steps to synchronize users with Cisco WebEx Social:

Procedure

- Step 1** Access the Settings window:
 - a. Click the down-arrow  to the right of your name in the Global Navigation bar.
 - b. Select **Account Settings from** the drop-down menu.
 - c. Click the right-arrow  next to **Portal**
 - d. Click **Password Policies** in the Portal drawer.
- Step 2** Select **Authentication** in the right pane of the window.
- Step 3** Select the **LDAP Directory Sync** tab.
- Step 4** Check the **Enable Synchronizing from LDAP Server** box.
- Step 5** From the **Which node to run sync on** drop-down list, select the Cisco WebEx Social server that you want to synchronize to the LDAP server. This server cannot be the Director node. If this node is changed later, both the new and old nodes must be restarted.
- Step 6** Click **Save** in the right panel of the window.

- Step 7** Under the Agreements portion of the window, click **Add**, and fill out all the fields and information about when and how often you want synchronization to occur, as shown in [Table 2-27](#):



Note If you already have created agreements, you can click **View All** to view all existing agreements.

- Step 8** Click **Save**.
- Step 9** (Optional) If you want to modify an agreement, click on its link and make any changes you want, and save your changes.
- Step 10** Check the box next to the agreement you want.
- Step 11** Click **Save**.



Caution If you delete an agreement, all users imported associated with that agreement become inactive. Before proceeding, make sure that you intend to take this action.

Table 2-27 LDAP Agreement Settings

Field	Description
LDAP Directory Information	
LDAP Configuration Name	Name you assign for the LDAP Agreement you are configuring.
LDAP Manager Distinguished Name	Unique identifier that typically should match the value of the Principal field in Table 2-26 on page 2-41 . Example: CN=esspcialpha.gen,OU=Generics,OU=Cisco Users,DC=cisco,DC=com
LDAP User Search Base	Specifies the initial search context in LDAP for users. Typically, the value of this field should match the value of the Base DN field in Table 2-26 on page 2-41 . Example: OU=Employees,OU=Cisco Users, DC=cisco, DC=com
Password	Administrative password of the LDAP server.
Confirm Password	Reentering of the password.
LDAP Directory Synchronization Schedule	
Perform Sync Just Once	Checkbox to enable if you want the LDAP synchronization performed only one time.
Perform a Re-sync Every	Used in conjunction with the adjacent drop-down list to set synchronization for a certain number of times every day, week, or month.

Table 2-27 LDAP Agreement Settings (continued)

Field	Description
Next Re-sync Time	Time to perform the next resynchronization; given in the format of yyyy-MM-dd HH:mm.
User Fields To Be Synchronized	<p>In the fields in this area, configure the attributes of the LDAP User fields that correspond to the Cisco WebEx Social User field. The Cisco WebEx Social user fields will be synchronized with these LDAP user attributes.</p> <p>These fields are not editable after a directory agreement saved. To edit these fields, you must first delete the agreement. Create a new agreement after saving the this LDAP information.</p>
LDAP Server Information	
Host Name or IP Address for Server	Fully qualified domain name or the IP address of the LDAP server.
LDAP Port	Port of the LDAP server; 389 is the default.
Use SSL	Select if you will use LDAP over SSL.
Test LDAP Connection	Click this button to check the connection between Cisco WebEx Social and the LDAP server.
Add Another Redundant LDAP Server	<p>Lets you designate up to 3 LDAP servers for redundancy. If a server files, the system attempts to connect to redundant servers in the order in which they are specified.</p> <p>When you select this option, these fields appear:</p> <ul style="list-style-type: none"> • Hostname—Enter the host name or IP address of a redundant LDAP server • Port—Enter the number of a valid LDAP port (typically 389or 636) <p>After you configure a redundant server, you can click Test Connection to verify the connection to the server.</p>

LDAPS Authentication and Synchronization

You have the option of using LDAPS authentication instead of LDAP.

To enable (LDAPS) to connect to the Active Directory server for authentication and directory synchronization, follow these steps:

-
- Step 1** In the Director, click **Security** in the left panel.
- Step 2** In the Add New Trusted Certificate area, take these actions:
- In the Alias field, enter a string to uniquely identify the certificate that you are adding.
 - In the Trusted Certificate field, browse to and select the desired certificate.

- c. Click **Save**.

Step 3 In the Trusted Certificates area, click **Deploy Trusted Certificates**.



NTLM

Windows NT LAN Manager (NTLM) is a Microsoft protocol that can be used for authentication through Microsoft Internet Explorer. Cisco WebEx Social supports NTLM version 1.

The NTLM tab in the Settings > Authentication window allows you to use NTLM with Cisco WebEx Social.

To enable NTLM for use with Cisco WebEx Social, follow these steps:

Procedure

- Step 1** Access the Settings window:
- a. Click the down-arrow  to the right of your name in the Global Navigation bar.
 - b. Select **Account Settings** from the drop-down menu.
 - c. Click the right-arrow  next to **Portal**
 - d. Click **Settings** in the Portal drawer.
- Step 2** Select **Authentication** in the right pane of the window.
- Step 3** Select the **NTLM** tab.
- Step 4** Check the **Enabled** box to enable NTLM authentication.
- Step 5** Check the **Enable Login Time User Sync** box to cause user information to be synced from LDAP to the Cisco WebEx Social database means when the user successfully logs in.
- Step 6** In the Domain Controller field, enter the IP address of your domain controller, which is the server that contains the user accounts that Cisco WebEx Social to uses.
- Step 7** In the Domain field, enter the name of the domain or workgroup.
- Step 8** Click **Save**.
- Step 9** Select **General** in the right pane of the window.
- Step 10** In the Home URL field, enter the value:
/c/portal/login
- Step 11** Click **Save**.
- Step 12** On the Windows Active Directory server, ensure that the following digital signing communications are enabled:
- | | |
|--|---------|
| Microsoft network server: Digitally sign communications (always) | Enabled |
| Microsoft network server: Digitally sign communications (if client agrees) | Enabled |
- Step 13** Take these actions:
- a. Create a service user account on the Active Directory.
 - b. On each Cisco WebEx Social node, add the following JAVA_OPTS into
/opt/cisco/quad/tomcat/bin/setenv.sh:

```

JAVA_OPTS="$JAVA_OPTS
-Dorg.owasp.esapi.resources=$CATALINA_HOME/webapps/ROOT/WEB-INF/ESAPI
-Djcifs.util.loglevel=10 -Djcifs.smb.client.username=<serviceuser>
-Djcifs.smb.client.password=<servicepassword>"

```

- c. Restart each Cisco WebEx Social node.

Step 14 Instruct the users to take either of these sets of actions:

- For Internet Explorer:
 - a. Go to **Tools > Internet Options**.
 - b. Click the **Security** tab.
 - c. With “Local Intranet” highlighted, click **Sites**.
 - d. In the pop-up window, make sure the following boxes are checked:
 - “Include all local (intranet) sites not listed in other zones”
 - “Include all sites that bypass the proxy server”
 - “Include all network paths (UNCs)”
 - e. Click **Advanced**.
 - f. In the dialogue box, enter the following in the “Add this website to the zone:” field:

`http://Cisco_WebEx_Social_Server.company.com`



Note To enable Active Directory pass-through authentication for all the sites in a domain, you can instead enter the following in the “Add this website to the zone:” field:
`http://*.company.com`

- g. Click **Add**.
- For **Firefox**:
 - a. In the address bar of your Firefox browser, enter the following:
`about:config`
 - b. Press **Enter**.
 - c. In the configuration window that opens, scroll down to the following entry:
“network.automatic-ntlm-auth.trusted-uris”
 - d. Double-click on this entry.
 - e. In the popup window, enter the following:
`http://Cisco_WebEx_Social_Server.company.com`



Note To enable Active Directory pass-through authentication for all the sites in a domain, you can enter the following string instead:
`.company.com`

- f. Click **OK**.

Step 15 In the Director, click **Configuration** under System, and take these actions in the Notifier area:




- a. Check the Enable SSO Box.

- b. Click **Save**.
-

SiteMinder

The SiteMinder tab in the Settings > Authentication window allows you configure SiteMinder single sign-on. To make this configuration, follow these steps:




Procedure

- Step 1** Access the Settings window:
- a. Click the down-arrow  to the right of your name in the Global Navigation bar.
 - b. Select **Account Settings** from the drop-down menu.
 - c. Click the right-arrow  next to **Portal**
 - d. Click **Settings** in the Portal drawer.
- Step 2** In the Home URL field, enter the value:
/c/portal/login
- Step 3** Select **Authentication** in the right pane of the window.
- Step 4** Select the **SiteMinder** tab.
- Step 5** Check the **Enabled** box to turn on SiteMinder SSO integration.
- Step 6** If you check the **Import from LDAP** box, users authenticated from SiteMinder who do not exist in the portal are imported from LDAP, as long as LDAP is also enabled.
-  **Note** SiteMinder and Cisco WebEx Social must point to the same LDAP infrastructure.
-
- Step 7** The User Header must be the field that SiteMinder is populating with the userID (called the *screenname* in Cisco WebEx Social) of a user. Typically, this value is SM_USER, but if you populate another field with the userID, enter the name of the SiteMinder field that contains the user name in this field.
- Step 8** Click **Save**.
- Step 9** In the Director, click **Configuration** under System, and take these actions in the Notifier area:
- a. Check the Enable SSO Box.
 - b. Click **Save**.
-

OAM

The OAM tab in the Settings > Authentication window allows you configure Operations Administration and Maintenance (OAM) single sign-on. To make this configuration, follow these steps:



Procedure

-
- Step 1** Access the Settings window:
- Click the down-arrow  to the right of your name in the Global Navigation bar.
 - Select **Account Settings** from the drop-down menu.
 - Click the right-arrow  next to **Portal**
 - Click **Settings** in the Portal drawer.
- Step 2** In the Home URL field, enter the value:
/c/portal/login
- Step 3** Select **Authentication** in the right pane of the window.
- Step 4** Select the **OAM** tab.
- Step 5** Check the **Enabled** box to turn on OAM SSO integration.
- Step 6** If you check the **Enable Login Time User Sync** box, users authenticated from OAM who do not exist in the portal are imported from LDAP, as long as LDAP is also enabled.
- 
-
- Note** OAM and Cisco WebEx Social must point to the same LDAP infrastructure.
-
- Step 7** The User Header must be the field that OAM is populating with the userID (called the *screenname* in Cisco WebEx Social) of this user. Typically, this value is OAM_USER, but if you populate another field with the userID, enter the name of the OAM field that contains the user name in this field.
- Step 8** Click **Save**.
- Step 9** In the Director, click **Configuration** under System, and take these actions in the Notifier area:
- Check the Enable SSO Box.
 - Click **Save**.
-

Kerberos

The Kerberos tab in the Settings > Authentication window allows you enable and use Kerberos with Cisco WebEx Social.

To use Kerberos in your Cisco WebEx Social deployment, first configure Kerberos Properties settings in Security window of the Director as described in the [“Kerberos Properties” section on page 5-22](#). Then, follow these steps:

-
- Step 1** Access the Settings window:
- Click the down-arrow  to the right of your name in the Global Navigation bar.
 - Select **Account Settings** from the drop-down menu.
 - Click the right-arrow  next to **Portal**
 - Click **Settings** in the Portal drawer.
- Step 2** In the Home URL field, enter the value:
/c/portal/login

- Step 3** Select **Authentication** in the right pane of the window.
- Step 4** Select the **Kerberos** tab.
- Step 5** Check the **Enabled** box to turn on Kerberos.
- Step 6** (Optional) Check the **Enable Login Time User Sync** if you want information for a user to be synchronized from LDAP to the Cisco WebEx Social database when the user is successfully authenticated.
- Step 7** Click **Save**.
- Step 8** In the Director, click **Configuration** under System, and take these actions in the Notifier area:
 - a. Check the Enable SSO Box.
 - b. Click **Save**.

**Note**

To use the Cisco WebEx Social Email plugin in a deployment in which Kerberos is enabled, a proxy must be configured to use the Apache JServ Protocol (AJP) to redirect API calls from the Email plugin to Tomcat. The URL of the proxy should be provided to the Email plugin instead of Cisco WebEx Social URL.

The following is an example Apache configuration that allows the Email plugin to work when Kerberos is enabled, where *appnode* is the IP address of FQDN of an App Server node in your deployment:

```
ProxyVia on
    ProxyPassMatch \A(/quadopen|/plugin/email) ajp://appnode:8009
    ProxyPassReverse / ajp://appnode:8009
<Proxy *>
    Order deny,allow
    Deny from all
    Allow from all
</Proxy>
```

SAML SSO

The options in the SAML SSO tab in the Settings > Authentication window are not used for an on-premises installation of Cisco WebEx Social. For more information, contact your Cisco representative.

Users

Users settings let you specify whether Cisco WebEx Social users must accept a terms of use notice, and configure communities, roles, and user groups to which new users are added by default. To access the Users settings options, click the **Users** link at the right side of the Settings window (the “Settings” section on page 2-39 describes how to access this window).

Table 2-28 describes the Users settings options.

Table 2-28 Users Settings Options

Field	Description
Terms of Use Required	<p>Check this box if you want users to be required to accept a terms of use notice before they can use Cisco WebEx Social.</p> <p>Note Users must accept the terms of use notice before they can use the Mobility apps.”</p> <p>Note Default: Yes</p>
Communities	<p>Enter the names of any communities (one line for each name) to which newly created users automatically become members. Remember to click Save when you are done.</p> <p>Default: No communities are assigned.</p>
Roles	<p>Enter the names of any roles (one line for each name) to which newly created users automatically become members. Remember to click Save when you are done.</p> <p>Default: User, super user. (For definitions of various roles, see the “Roles” section on page 1-28.)</p> <p>Note You can remove any of the default roles by deleting the name of the role.</p>
User Groups	<p>Enter the names of any user groups (one line for each name) to which newly created users automatically become members. Remember to click Save when you are done.</p> <p>Example</p> <p>One reason to assign a default user group to a new user would be if you may have defined page templates in certain user groups to prepopulate end user private pages. If there is a particular configuration that you want everyone to have, you may want to enter those user groups here. For more information, see “Defining Page Templates for a User Group” section on page 2-17.</p> <p>Default: No user groups are assigned by default.</p>

Mail Host Names

The Mail Host Names setting lets you designate mail host names besides the host that you configured in the General settings window (see the [“General” section on page 2-39](#)). Cisco WebEx Social fails over to these host names if the main mail host fails.

To access the Mail Host Names settings option, click the **Mail Host Names** link at the right side of the Settings window (the [“Settings” section on page 2-39](#) describes how to access this window).

In the Mail Host Names field, enter the FQDN of each e-mail server is used for outbound e-mail (one per line).

Reported Content

The Reported Content setting lets you designate the number of times Cisco WebEx Social users can report the same content as inappropriate or incorrect before Cisco WebEx Social automatically hides the content. To access the Reported Content option, click the **Reported** link at the right side of the Settings window (the “[Settings](#)” section on page 2-39 describes how to access this window).

To set the number of times Cisco WebEx Social users can report the same content as inappropriate or incorrect before Cisco WebEx Social automatically hides the content, enter a value in the Reporting Threshold field.

The maximum value is 20. The default value is 5, which means that if a post, for example, is reported five times, Cisco WebEx Social automatically hides the post. Compliance officers must then take action (for example, have the author correct the offending content) to make the content visible again.

Related Topic

[Compliance Officer Role, page 1-29](#)

Display Settings

The Display Setting options lets you configure the language, time zone, and custom log for Cisco WebEx Social. To access the Display Settings options, click the **Display Settings** link at the right side of the Settings window (the “[Settings](#)” section on page 2-39 describes how to access this window).

[Table 2-29](#) describes Display Setting options.

Table 2-29 **Displays Settings Options**

Field	Description
Default Language	Choose the default language for Cisco WebEx Social.
Available Languages	Displays languages that are available for a Cisco WebEx Social user to select. Enter a language in the format <i>language-code_country-code</i> , where <i>language-code</i> is the ISO639 two-letter language code for the language that you want to use and <i>country-code</i> is an optional ISO3166 two-letter country code, which is used to specify a dialect for a language. Each language entry is separated by a comma.
Time Zone	Choose the time zone for Cisco WebEx Social.
Logo	<p>You can change the portal-wide logo that appears in the top-left corner of themes that are configured to display this logo. This logo also appears in all e-mails, including invitation emails. To change the logo, click Change, browse to select the logo that you want, then click Save.</p> <p>To delete a log, click Delete.</p> <p>Be sure that the logo image file fits the space in the Display Settings window.</p>

Custom Settings

The Custom Setting options lets you configure whether the system captures and stores a corresponding activity in the database when a link is created or updated in a post. You can then use the Cisco WebEx Social API to retrieve information about the activity.

To access the Display Settings options, click the **Display Settings** link at the right side of the Settings window (the “[Settings](#)” section on page 2-39 describes how to access this window).

To cause the system to generate an activity when a link is created or updated in a post, check the **Post Categories & Links Audit** box. This box is unchecked by default.

Plugin Settings

Use the Plugin Settings window to perform the following activities:

- Set which portal roles are given permissions to add specific Cisco WebEx Social application plugins to one of their pages. By default, all users are given the permissions to install supported Cisco WebEx Social applications, which are listed in [Table 1-4 on page 1-13](#).



Note Any changes you make to roles in the Plugins Installation window do not affect application plugins that users have already added to their pages.

- Change a Cisco WebEx Social application plugin from Active or to Inactive status. If you change the status of a plugin to Inactive:
 - The plugin is removed from the available Cisco WebEx Social applications (see [Table 1-4 on page 1-13](#))
 - If users already have added the application plugin to one of their pages, “Portlet inactive” appears for the application

Cisco WebEx Social provides these plugin types:

- Portlet plugins—Small web applications that run in a portion of a web page. All of the functionality of a portal is in its portlets.
- Layout template plugins—Determine how portlets are arranged on a page.

This section includes these topics:

- [Managing Portlet Plugins, page 2-54](#)
- [Managing Layout Template Plugins, page 2-55](#)

Managing Portlet Plugins


The Portlet Plugins tab in the Plugins Settings window shows which plugins already exist on the system for the selected tab, whether the plugin is active, and which portal roles can install each plugin.

To change the roles that can install a plugin, or to change the Active/Inactive status of a plugin, perform the following steps.

By default, all roles can install a plugin.

Procedure

Step 1 Access the Plugin Settings window:

- Click the down-arrow  to the right of your name in the Global Navigation bar.
- Select **Account Settings** from the drop-down menu.

- c. Click the right-arrow  next to **Portal**
- d. Click **Plugin Settings** in the Portal drawer.

The Plugins Settings window appears with the Portlet Plugins tab selected

Step 2 In the Portlet Plugins tab, click the link for the portlet for which you want to change roles or status.

Step 3 Take the desired actions:

- Check the **Active** box to set the status of the plugin to Active, or uncheck this box to set the status to Inactive.
- In the box provided for roles, enter or delete any role. Enter one role per line.
By default, no roles are included in this box, which means that all roles can install the plugin. If you enter one or more roles in this box, only these roles can install the plugin.

Step 4 Click **Save**.

For more information about defining roles, see the [“Defining Permissions for a Role” section on page 2-21](#).

Managing Layout Template Plugins

The Layout Template Plugins tab in the Plugins Settings window shows the layout templates that are available in Cisco WebEx Social.

To change the roles that can use a layout template, or to change the Active/Inactive status of a layout template, perform the following steps.





Note

By default, all roles can use a layout template.

Procedure

Step 1 Access the Plugin Settings window:

- a. Click the down-arrow  to the right of your name in the Global Navigation bar.
- b. Select **Account Settings** from the drop-down menu.
- c. Click the right-arrow  next to **Portal**
- d. Click **Plugin Settings** in the Portal drawer.

The Plugins Settings window appears with the Portlet Plugins tab selected

Step 2 Select the **Layout Template Plugins** tab.

Step 3 Click the link for the layout template for which you want to change roles or status.

Step 4 Take the desired actions:

- Check the **Active** box to set the status of the plugin to Active, or uncheck this box to set the status to Inactive.
- In the box provided for roles, enter or delete any role. Enter one role per line.
By default, no roles are included in this box, which means that all roles can use the layout template. If you enter one or more roles in this box, only these roles can use the layout template.

Step 5 Click **Save**.

For more information about defining roles, see the [“Defining Permissions for a Role”](#) section on page 2-21.

WSRP

Web Services for Remote Portlets (WSRP) defines a web service interface for accessing and interfacing with interactive, presentation-oriented web services. These web services are built on standard technologies and include SSL/TLS, URI/URL, WSDL, and SOAP.

The main components in the WSRP architecture are:

- **WSRP Producer**—A web service that offers one or more portlets and implements a set of WSRP interfaces, thus providing a common set of operations for consumers. Depending on the implementation, a producer could offer just one portlet, or could provide a run-time (or a container) for deploying and managing several portlets. The WSRP producer is a true web service, complete with a WSDL and a set of endpoints. Every producer in WSRP is described using a standardized WSDL document.
- **WSRP Portlet**—A pluggable user interface component that lives inside a WSRP producer and is accessed remotely through the interface defined by that producer. A WSRP portlet is not a web service because it cannot be accessed directly but instead is accessed through its parent producer.
- **WSRP**—A web service client that invokes producer-offered WSRP web services and provides an environment for users to interact with portlets offered by one or more such producers. The most common example of a WSRP consumer is a portal.

This section contains the following topics:



- [Configuring WSRP on an App Server Node, page 2-56](#)
- [Configuring the WSRP Cluster Link, page 2-58](#)

Configuring WSRP on an App Server Node

To configure a WSRP in Cisco WebEx Social, follow these steps on a App Server node:

Procedure

Step 1 Access the Plugin Settings window:

- a. Click the down-arrow  to the right of your name in the Global Navigation bar.
- b. Select **Account Settings** from the drop-down menu.
- c. Click the right-arrow  next to **Portal**
- d. Click **WSRP** in the Portal drawer.

The WSRP window appears with the Consumers tab selected

Step 2 Select the **Producers** tab.

Step 3 Click **Add Producer**.

The Add Producer window opens.

Step 4 In the Add Producer window, take these actions:

- a. In the Name field, assign a descriptive name such as *CiscoWebExSocialProducer*.
- b. From the Available portlets list, select a portlet that you want to expose, then click the **Add** button to move the portlet to the Current portlets list.

You can remove a portlet from the Current portlets list by clicking the portlet and then clicking the **Remove** button.



Note Many of the portlets in the list of available portlets will not run remotely.

- c. Click **Save**.

From the **Actions** drop-down menu next to a producer name, you can edit the producer name or change the portlets that belong to the producer, or you can delete the producer.

Step 5 To update a producer that you created, take these actions:

- a. Click the producer (in the Producer column). The window that appears shows the name and the URL of the producer. You can make any updates to the producer or portlets for this producer in this window.



Note You need the URL that this window shows when you add the consumer.

Step 6 In the WSRP window, click the **Consumers** tab.

Step 7 Click **Add Consumer**.

The Add Consumer window opens.

Step 8 In the Name field, assign a descriptive name, such as *CiscoWebExSocialConsumer*.

Step 9 In the URL field, past the URL that you copy from the corresponding producer.

Step 10 Click **Save**.

After you have added the consumer, perform the following steps to add the portlet to the list of applications:

Procedure


Step 1 From the Actions drop-down menu that appears when the Consumer tab is selected, select **Manage Portlets**.

Step 2 Enter a name for the remote portlet.

Step 3 Select the portlet from the provided drop-down list.

Step 4 Click **Save**.

Step 5 Navigate to your Home page.

Step 6 Click  to add an application.

Step 7 Drag and drop the portlet to the desired location on the page.

Other actions you can perform from the Actions list when the Consumer tab is selected are:

- Edit—Change the name of the consumer or the producer (URL) to which it belongs.
- Update Service Description—Updates services.
- Delete—Delete the consumer from the producer.

Configuring the WSRP Cluster Link

If your Cisco WebEx Social deployment uses WSRP portlets and contains multiple Cisco WebEx Social nodes, you must replicate the WSRP portlets across all Cisco WebEx Social nodes.

To perform this replication, perform these steps on the Director:

Procedure

-
- Step 1** Sign in to the Director.
- Step 2** Click **Integration** under Application.
- Step 3** In the WSRP Settings area, take these actions:
- a. Check Cluster Link Enabled box.
 - b. In the Autodetect Address field, enter the IP address of the WSRP cluster link gateway.
 - c. Click **Save**.

The settings are replicated to all App Server nodes.

Content Repositories

Cisco WebEx Social allows you to use SharePoint 2007 or a SharePoint 2007 or Documentum 6.5 or above as a document repository. These types of integrations are supported:

- External document repository—Document metadata is stored outside of Cisco WebEx Social. Regular users can add the Repository Library application to either their Home or My Profile page; a community administrator can add the Repository Library application to their community. This application provides a window view to the remote SharePoint document library. This type supports SharePoint 2007 or Documentum 6.5 or above
- Native repository— Document metadata, such as author and creation date, is stored in Cisco WebEx Social, and SharePoint serves as a flat-file storage system. Document folders are automatically built into user libraries and community libraries. This type supports only SharePoint 2007 for basic authentication.

This section contains the following topics:

- [Using a Native SharePoint Repository, page 2-59](#)
- [Using an External SharePoint Repository, page 2-62](#)
- [Using a Content Repository, page 2-64](#)
- [User Configuration Required for External Repository, page 2-65](#)

**Note**

If you are going to use an external SharePoint repository with Kerberos authentication, first perform the procedure that the [“Kerberos Properties” section on page 5-22](#) describes.

Using a Native SharePoint Repository

You can configure a Microsoft SharePoint 2007 server to use as the repository for documents in the Cisco WebEx Social library, and attachments to Cisco WebEx Social posts and discussion boards.

**Note**

If you do not want to use SharePoint as your repository, do not perform the steps provided in this section. In this case, Cisco WebEx Social continues to use its built-in repository.

This topic contains the following sections:

- [Preparing to Set Up a Native SharePoint Repository, page 2-59](#)
- [Configuration Required on the Director, page 2-59](#)
- [Configuration Required in the Portal Drawer, page 2-60](#)
- [Configuring the Community Template in Sharepoint, page 2-61](#)
- [Additional Notes, page 2-61](#)

Preparing to Set Up a Native SharePoint Repository

Communicate with the system administrator of the SharePoint server that Cisco WebEx Social uses. You must obtain the user ID and password of an administrative account on the SharePoint server because you need this information to integrate SharePoint with Cisco WebEx Social. This account, at minimum, must grant create, read, update, and delete operations on the SharePoint repository/homesite reserved for Cisco WebEx Social integration.

Configuration Required on the Director

You must perform the following configuration on the Director if you did not already do so during installation:

Procedure

-
- | | |
|---------------|---|
| Step 1 | Sign in to the Director. |
| Step 2 | Click Portal under Application. |
| Step 3 | In the Advanced Portal Properties area, take these actions: <ul style="list-style-type: none">a. Enter the following native sharepoint hook in the dl.hook.impl field:
com.liferay.documentlibrary.util.SP07Hookb. Click Save. |

**Note**

If you are using Native SharePoint for the document repository and want to change back to a native file system, enter **com.liferay.documentlibrary.util.FileSystemHook** in the `dl.hook.impl` field, and then restart each Cisco WebEx Social node.

Step 4 Click **Integration** under Application.

Step 5 In the SharePoint (Native) area, take these actions:

- a. Check the **SharePoint Integration Enabled** box.
- b. In the SharePoint URL field, enter the URL of the SharePoint site document library to which Cisco WebEx Social is connecting (example format shown below):

`http://<sharepoint host>/<sharepoint site>/<Document Library>`

- c. Click **Save**.

Step 6 Take these actions to restart all Cisco WebEx Social nodes:

- a. Click **Topology** under System.
- b. Click **Disable** in the Operational Status column for each node that includes this button.
- c. Power off other nodes.
- d. Click **Enable** in the Operational Status column for each node that includes this button.
- e. Power on other nodes.

Configuration Required in the Portal Drawer



Perform the following steps to configure the native repository:

Before You Begin

Before you perform this procedure, use Internet Information Services (IIS) to set the SharePoint 2007 server to use *Basic Authentication*.

Procedure

Step 1 Log in to Cisco WebEx Social as an administrator and access the Content Repositories window:

- a. Click the down-arrow  to the right of your name in the Global Navigation bar.
- b. Select **Account Settings** from the drop-down menu.
- c. Click the right-arrow  next to **Portal**
- d. Click **Content Repositories** in the Portal drawer.

The Content Repository window appears with the External Document Repositories tab selected.

Step 2 Select the **Native Repository** tab.

Step 3 In the Admin UserName field, enter the user ID of the administrative account on the SharePoint Server to which Cisco WebEx Social is connecting.

Step 4 In the Password field, enter the password of the administrative account on the SharePoint Server to which Cisco WebEx Social is connecting.

Step 5 Click **Save**.

Configuring the Community Template in Sharepoint

To configure the community template in SharePoint, follow these steps:

-
- Step 1** Use an SSH client to access an App Server node, log in as the admin user, and enter these commands:
- ```
[root]# sudo cd /mnt/auto/cms/document_library
[root]# sudo find . -name *.lar
```
- Step 2** Make a note of the path and file name for each file in the output of the **find** command that begins with DLFE and has the extension .lar.
- For example, if the output of the **find** command is as follows, make a note of each path and corresponding file name:
- ```
./10195/9910026/DLFE-2.lar
./10195/9910010/DLFE-1.lar
./10195/9910042/DLFE-3.lar
```
- Step 3** In SharePoint, take these actions:
- Create folders under the SharePoint home site that match the folders that you noted in [Step 2](#).
For example, using the output that is shown in that step, create these folders under the SharePoint home site:
10195/9910026
10195/9910010
10195/9910042
 - Upload each file that you noted in [Step 2](#) from the App Server node to the corresponding directory that you created in SharePoint.
For example, using the output that is shown in that step, upload the DLFE-2.lar file from the App Server node to the 10195/9910026 folder that you created in SharePoint.
- Step 4** Sign in to the Director and take these actions in the Director to restart each App Server node:
- Click **Topology** in the left panel.
 - Click the **Disable** button next to each App Server role in the Server List area.
 - Click the **Enable** button next to each App Server role in the Server List area.
-

Additional Notes

- After a SharePoint native repository is integrated with Cisco WebEx Social, do not allow users to add, move, delete, or modify documents on SharePoint web pages. Any changes to the document repository must be performed on the Cisco WebEx Social web pages (for example, in the Document Library, Post Attachments, and Message Board posts).
- You can use only one SharePoint server per Cisco WebEx Social node.
- There is no visible difference to the Cisco WebEx Social end user if SharePoint is used as the repository.

- You can also use external SharePoint repositories.

Using an External SharePoint Repository

You can use multiple external SharePoint repositories with Cisco WebEx Social.

This section contains the following topics:

- [Configuration Required in the Director, page 2-62](#)
- [Configuration Required in the Content Repositories Window, page 2-62](#)

Configuration Required in the Director



If you are using a SharePoint external repository with Cisco WebEx Social, follow these steps to add and deploy the required trusted certificate:

Procedure

-
- Step 1** In the Director, click **Security** in the left panel.
- Step 2** In the Add New Trusted Certificate area, take these actions:
- a. In the Alias field, enter a string to uniquely identify the certificate that you are adding.
 - b. In the Trusted Certificate field, browse to and select the desired certificate.
 - c. Click **Save**.
- Step 3** In the Trusted Certificates area, click **Deploy Trusted Certificates**.
-

Configuration Required in the Content Repositories Window

Procedure

-
- Step 1** Sign in to a App Server node with administrative credentials and access the Content Repositories window:
- a. Click the down-arrow  to the right of your name in the Global Navigation bar.
 - b. Select **Account Settings from** the drop-down menu.
 - c. Click the right-arrow  next to **Portal**
 - d. Click **Content Repositories** in the Portal drawer.
- Step 2** In the External Document Repositories tab, click **Add New Repository**.
The window to configure a new external repository opens.
From the Type drop-down list, choose **Sharepoint 2007 Server**.
- Step 3** Configure the values in the window as [Table 2-30](#) describes.
- Step 4** Click **Save**.

- Step 5** To test the connection, take of these actions in the Connection area at the bottom of the window:
- If you are testing with “Basic” authentication, in the Username field, enter the user name of an administrative or regular user account on the SharePoint 2007 server.
 - If you are testing with “Basic” authentication, in the Password field, enter the password of the account whose user name you just entered.
 - Click **Test Repository**.
- Step 6** Review the information in the [“User Configuration Required for External Repository”](#) section on page 2-65.

Table 2-30 External Document Repository SharePoint 2007 Settings

Field	Description
Name	Descriptive name for the external repository you are adding.
Protocol	Drop-down list from which you must choose either “http” or “https:” <ul style="list-style-type: none"> http is not secured, meaning that the password is sent as clear text. https is based on the Single Socket Layer (SSL) protocol, in which the entire user http session, including the password, is encrypted. With https, the server and client exchange certificates using a trusted Certified Authority (CA).
Host Name	Fully qualified domain name of the SharePoint 2007 server that you are using as an external document repository.
Port	Port that Cisco WebEx Social uses to connect to the SharePoint 2007 server.
Authentication	Drop-down list from which you must choose either Basic or Kerberos as the authentication method. <p>Note Kerberos is the more secure of these methods as it is designed to provide strong authentication for client/server applications by using secret-key cryptography. With Kerberos, user passwords are not circulated within the system. Only tickets are circulated within the system. In addition, the search feature in Cisco WebEx Social works only when Kerberos is the authentication method for external repositories.</p>
Max Retries	Enter a value that is less than the number of failed authentication attempts that are allowed in the repository. This setting prevents Cisco WebEx Social from attempting to connect to the repository multiple times and potentially locking out a user if a user enters an incorrect repository password.

Using a Content Repository

To use a Content repository, follow these steps:

Procedure



-
- Step 1** Sign in to a App Server node with administrative credentials and access the Content Repositories window:
- Click the down-arrow  to the right of your name in the Global Navigation bar.
 - Select **Account Settings** from the drop-down menu.
 - Click the right-arrow  next to **Portal**
 - Click **Content Repositories** in the Portal drawer.
- Step 2** In the External Document Repositories tab, click **Add New Repository**.
The window to configure a new external repository opens.
From the Type drop-down list, choose **CMIS Provider**.
- Step 3** Configure the values in the window as [Table 2-31](#) describes.
- Step 4** Click **Get List of Repositories**.
- Step 5** Click the radio button next to the repository that you want.
- Step 6** Click **Save**.
- Step 7** Take these actions to test the repository:
- In the Username Field, enter the user name of an administrative account on the server that you are using as an external document repository.
 - In the Password field, enter the password of the account whose user name you just entered.
 - Click **Test Repository**.
- Step 8** Review the information in the [“User Configuration Required for External Repository”](#) section on [page 2-65](#).
-

Table 2-31 External Repository Settings

Field	Description
Add Repository Details	
Name	Descriptive name for the external repository you are adding.
Protocol	Drop-down list from which you must choose either “http” or “https:” <ul style="list-style-type: none"> http is not secured, meaning that the password is sent as clear text. https is based on the Single Socket Layer (SSL) protocol, in which the entire user http session, including the password, is encrypted. With https, the server and client exchange certificates using a trusted Certified Authority (CA).
Host Name	Fully qualified domain name of the server that you are using as an external document repository.

Table 2-31 External Repository Settings (continued)

Field	Description
Port	Port that Cisco WebEx Social uses to connect to the server.
Authentication	Read only: Displays Basic.
AtomPub URL	Enter the URL for the Atom Publishing Protocol (AtomPub) for connecting to the repository. To determine this URL, see the documentation provided by the repository provider.
Max Retries	Enter a value that is less than the number of failed authentication attempts that are allowed in the repository. This setting prevents Cisco WebEx Social from connecting to the repository multiple times if a user enters an incorrect repository password.
Username	Username required to connect to the repository.
Password	Password required to connect to the repository.

User Configuration Required for External Repository

If you are a system administrator and have configured an external repository, your end users need to perform a few steps before they can begin using the external repository.

Provide them with the following information to complete the external-repository configuration:

Information for End Users

If your system administrator has configured an external repository for document management, you can add the Repository Library application to your Home or My Profile page.




Additionally, you can add the Repository Library application to any community of which you are the community administrator.



Note

If a community administrator adds the application to the community, the community administrator must grant community members the permissions to read and modify contents.

Procedure to Perform in the Cisco WebEx Social User Interface

- Step 1** Add the Repository Library application:
 - a. Click  to view the application icons.
 - b. Drag the External Document Repository application icon  and drop it to the desired location. You receive a message telling you to configure the application for the first time.
- Step 2** Click the gear icon  that appears when you move the cursor to the “External Document Repository” and select **Preference** from the drop-down menu that appears.
A window that contains the repository settings opens.
- Step 3** In the window with repository setting , enter values for only the following fields:
 - a. WorkSpace URL—This must be provided to you by your system administrator. This is the URL of the document library of the SharePoint server.

- b.** Credentials to Connect (Username and Password, required when “Basic” appears in the Authentication Mode field)—The username and password of your SharePoint account.

Step 4 Click **Save**.

You should receive the following message in the Preferences window: “Your request processed successfully.”

Step 5 Click **Go back**.

Step 6 You can now begin using the Repository Library application.
