



# CHAPTER 1

## Cisco WebEx Social Administration Overview

---

Cisco WebEx Social is a collaboration platform that allows you to work with your colleagues in a single environment. With Cisco WebEx Social, you can easily share information such as documents, videos, and presentations, conduct meetings, click-to-dial a contact, post information, join communities, participate in discussion forums, create blogs, and much more. This administration guide is intended for the system administrator of the Cisco WebEx Social platform.

This chapter includes these topics:

- [Administrator Roles, page 1-2](#)
- [Browser Support and Compatibility With Other Components, page 1-2](#)
- [Overview of Cisco WebEx Social Nodes, page 1-2](#)
- [Assigning Yourself the Role of Administrator or Level 1 Administrator, page 1-4](#)
- [Using the Settings Drawer for System Administrators, page 1-5](#)
- [Configuration Reference Table, page 1-6](#)
- [Configuring Items in the Help Window, page 1-8](#)
- [Adding Users to Cisco WebEx Social, page 1-10](#)
- [Introduction to the Cisco WebEx Social User Interface, page 1-10](#)
- [Installation and Configuration for Cisco Web Communicator, page 1-14](#)
- [Introduction to Users, Collections of Users, and Roles, page 1-26](#)
- [Basic Verification Steps for the User Interface, page 1-32](#)
- [Enabling or Disabling Cisco WebEx Social Components, page 1-33](#)
- [Serviceability, page 1-34](#)
- [Backup and Restore, page 1-34](#)
- [Setting Up a CDN, page 1-34](#)
- [Proxy Server Authentication, page 1-35](#)
- [Submitting Cisco WebEx Social API Requests or Using a Mobility App through a Load Balancer, page 1-35](#)
- [Downloading Images and Attachments to Mobile Clients, page 1-36](#)

# Administrator Roles

*Cisco WebEx Social Administration Guide* picks up where *Cisco WebEx Social Installation and Upgrade Guide* leaves off, meaning that you should now have Cisco WebEx Social completely installed. This administration guide begins with instructions for setting yourself up as the system administrator so that you can deploy Cisco WebEx Social to your users and perform system administrator duties.

Cisco WebEx Social supports two administrator roles:

- Administrator—Can access all portal and server pages and functions in Cisco WebEx Social.
- Level 1 Administrator—Can access only these portal drawers and features: Users, Communities, User Groups, Roles, Community Manager, and WebEx Social Metrics. Cannot access Server drawers. Cannot change settings of the Administrator role.

Major responsibilities of the system administrator include:

- Configuring various aspects of the platform to use all functionality of Cisco WebEx Social
- Setting password policies
- Adding users
- Sending notifications to users
- Creating and maintaining user groups, and communities (including open, restricted, or hidden communities)
- Creating new user roles and setting permissions for these roles
- Redefining existing user roles
- Assigning user roles
- Monitoring performance and performing maintenance



## Note

The terms *Cisco WebEx Social administrator* and *system administrator* mean the same thing. In general, the term *system administrator* is used in this manual.

## Browser Support and Compatibility With Other Components

For a list of browsers and other components that are compatible with Cisco WebEx Social, see *Cisco WebEx Social Compatibility Matrix*.

## Overview of Cisco WebEx Social Nodes

[Table 1-1](#) provides a brief description of the service that each node in a Cisco WebEx Social environment performs. The service a node performs is often referred to as a *role* in Cisco WebEx Social. Some roles can run on multiple nodes in a Cisco WebEx Social deployment.

Table 1-1 Cisco WebEx Social Roles

| Role            | Description   | Requirements   |
|-----------------|---|--|
| Analytics Store | A Mongo database that contains information about user preferences for the purpose of providing suggestions for what communities or other aspects of Cisco WebEx Social may interest a particular user. Also used for the e-mail digest notification and metrics features. | Minimum: 1 node.<br>Maximum: 2 nodes.<br><b>Note</b> 2 nodes are recommended to provide for high availability and redundancy.          |
| App Server      | The core Cisco WebEx Social web application.  | Minimum: One node.<br>Maximum: No limit.   |
| Cache           | A distributed, high-performance, in-memory key/value store. This node is intended to increase the speed of data access. The system tries to fetch data from this node before accessing the database, and database access is a slower operation.                           | Minimum: 1 node.<br>Maximum: No limit.   |
| Director        | Used to set up your Cisco WebEx Social topology and manage various system setting and configuration options.  | 1 node.  |
| Index Store     | An autonomous, special-purpose instance of the Cisco WebEx Social search engine used as a pseudo-cache to offload a class of resource-intensive database queries.   | Minimum: 1 node.<br>Maximum: 1 node.   |
| JSON Store      | A MongoDB database that stores various Cisco WebEx Social data. Provides for faster access to certain data than using a relational database would allow.  | Minimum: 1 node.<br>Maximum: 2 nodes.<br><b>Note</b> 2 nodes are strongly recommended to provide for high availability and redundancy. |
| Message Queue   | A message bus that provides reliable, asynchronous database updates.  | Minimum: 1 node.<br>Maximum: 2 nodes.  |
| Notifier        | XMPP publisher for notification of end-user events, including system alerts, announcements, and activities.   | Minimum: 1 node.<br>Maximum: 1 node.   |
| RDBMS Store     | Data store for data from the Notifier and App Server.   | Minimum: 1 node.<br>Maximum: 1 node.   |

**Table 1-1** Cisco WebEx Social Roles (continued)

| Role         | Description   | Requirements   |
|--------------|---|--|
| Search Store | Cisco-provided search engine for Cisco WebEx Social.  | There must be a master/slave setup for the Search Store. You need one virtual machine for the Master node and one for each slave node.<br><br>Minimum: 1 Search Store master and 1 Search Store slave.<br><br>Maximum: 1 Search Store master and 10 Search Store slaves. |
| Worker       | Improves system performance and user interaction by handling asynchronous and background processing tasks and interacting with various other roles. | Minimum: 1 node (2 for high availability).<br><br>Maximum: No limit.   |

## Assigning Yourself the Role of Administrator or Level 1 Administrator

Cisco WebEx Social provides a default Administrator that is preconfigured in the system. Cisco recommends that you log in as this default user and add yourself as an Administrator.

This procedure that this section describes requires that you already be set up as a user in the LDAP directory. In this procedure, you perform an LDAP synchronization, then you can choose yourself and assign the desired role

### Before You Begin

Perform the LDAP synchronization procedure as described in the [“LDAP Directory Sync”](#) section on page 2-44.

To add yourself as a Administrator, follow these steps:

### Procedure

---

**Step 1** Launch Cisco WebEx Social and sign in with the following default Administrator credentials:

- User Name: **test@cisco.com**
- Password: **test**

The Cisco WebEx Social window appears. The top area of this window contains the Global Navigation bar, as shown in [Figure 1-1](#).

**Figure 1-1 Global Navigation Bar**

- Step 2** Click the down-arrow ▼ to the right of your name in the Global Navigation bar, then select **Account Settings** from the drop-down menu.
- Step 3** Click the right-arrow ► next to **Portal** to expand the Portal drawer, then select **Users**. The Users window shows a list of users who were imported from the LDAP directory.
- Step 4** Locate the user to whom you want to assign the Administrator or Level 1 Administrator role. You can use the search fields to locate a user.
- Step 5** Click **Roles** under User Information from the panel that appears on the right of the window.
- Step 6** Under the Regular Roles options, click **Select**.
- Step 7** Click **Administrator** or **Level 1 Administrator**, depending on the role that you want to assign.
- Step 8** Click **Save** under in the panel that appears on the right of the window. The user now has the role that you assigned.

You can now begin configuring Cisco WebEx Social. You can perform most configuration tasks by using the Cisco WebEx Social control panel, described in “[Using the Settings Drawer for System Administrators](#)” section on page 1-5.

## Using the Settings Drawer for System Administrators

Many functions that you need to maintain Cisco WebEx Social are available from the Settings drawers. To access these drawers, click the down-arrow ▼ to the right of your name in the Global Navigation bar, then select **Account Settings** from the drop-down menu.

Cisco WebEx Social includes the following drawers. To expand a drawer so that you can see its options, click the right-arrow ► next to the name of the drawer.

- **My settings**—Contains following selections, which let you change your account information and manage your public and private pages. These options appears for all Cisco WebEx Social users, although regular users might only have permissions to manage their own private pages.
  - **My Account**—Use this option to manage your Cisco WebEx Social account and various personal Cisco WebEx Social settings
  - **Manage Pages**—Lets you update Home and Library pages, as described in [Appendix A, “Modifying Default Layouts and Creating a Custom Template.”](#)
- **Portal**—Contains the following selections, which provide options for creating, maintaining, or configuration a variety of Cisco WebEx Social entities:
  - [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](#)
- [Settings, page 2-39](#)
- [Plugin Settings, page 2-54](#)
- [WSRP, page 2-56](#)
- [Content Repositories, page 2-58](#)
- **Server**—Contains the following selections, which provide options management, administration, or configuration a variety system features and operations. This drawer is not visible to users who do not have the Administrator role:
  - [Server Administration, page 3-1](#)
  - [Plugins Installation, page 3-7](#)
  - [Common Configurations, page 3-10](#)
  - [Twitter Administration, page 3-42](#)
  - [License Agreement \(EULA\), page 3-44](#)

## Configuration Reference Table

Cisco WebEx Social contains many features that require configuration through the Settings drawers or the Director before they can be used. [Table 1-2](#) describes these features. In this table, features that are noted with “configuration required” must be configured before they are operational. Other features can be configured as needed, but are operational with the default settings.

**Table 1-2** Configuration References

| Item  | Description  | Reference  |
|---|--|--|
| Application Plugin Installation Permissions | Sets which groups of users can add specific Cisco WebEx Social applications to their pages.                            | <a href="#">Plugin Settings, page 2-54</a>   |
| Application Plugin Active/Inactive Status   | Sets which Cisco WebEx Social applications are available or unavailable to all users.                                  | <a href="#">Plugin Settings, page 2-54</a>   |
| Calendar Server (configuration required)    | Allows users to access Calendar applications.  | <a href="#">Calendar Server, page 3-10</a>   |
| Chat (configuration required)               | Allows users to click the Chat icon in the Cisco WebEx Social bar to start an instant messaging chat with a colleague. | <a href="#">Chat, page 3-17</a>  |
| Cisco Web Communicator                      | Allows users to use Cisco Web Communicator within Cisco WebEx Social.  | <a href="#">Installation and Configuration for Cisco Web Communicator, page 1-14</a> |
| Communities                                 | Allows you to add, remove, assign roles, assign members, and so on, for Cisco WebEx Social communities.                | <a href="#">Communities, page 2-11</a>   |
| Community Manager                           | Allows you to create categories that users can use when they create new communities.                                   | <a href="#">Community Manager, page 2-25</a>   |

**Table 1-2 Configuration References (continued)**

| Item   | Description  | Reference   |
|--|--|---|
| Compliance Officer role (configuration required)   | Has the role of deciding what to do with content that Cisco WebEx Social users have reported as inappropriate or incorrect.  | <a href="#">Compliance Officer Role, page 1-29</a>                              |
| E-mail linked to message board posts (configuration required)  | Allows subscribers of message board topics to receive and reply to posts by using an e-mail client application.  | <a href="#">Mail, page 3-5</a>  |
| Help Links   | You can configure various items that are used in the Help window.  | <a href="#">Configuring Items in the Help Window, page 1-8</a>                  |
| Feature disablement and enablement   | Allows you to disable and reenable a number of Cisco WebEx Social features.  | <a href="#">WebEx Social Functionality, page 2-32</a>                           |
| Kerberos   | Allows you to configure the Kerberos authentication protocol, which enables devices to communicate securely over a non-secure network.   | <a href="#">Kerberos Properties, page 5-22</a>                                  |
| Keystore Generation  | Allows you to SSL certificates that are used to complete WebEx Site, WebEx IM, and VoiceMail configuration.  | <a href="#">WebEx SSO, page 5-24</a><br><a href="#">WebEx IM SSO, page 5-24</a> |
| LDAP Authentication (configuration required)   | Performs user authentication.  | <a href="#">LDAP Authentication, page 2-41</a>                                  |
| LDAP Directory Synchronization (configuration required)  | Synchronizes Cisco WebEx Social server with LDAP directory.  | <a href="#">LDAP Directory Sync, page 2-44</a>                                  |
| LDAPS Authentication and Directory Synchronization (configuration required if choosing this over LDAP) | Authenticates and synchronizes Cisco WebEx Social with LDAP directory using SSL.   | <a href="#">LDAPS Authentication and Synchronization, page 2-46</a>             |
| Log Properties   | Lets you configure various log levels for troubleshooting purposes.  | <a href="#">Log Properties, page 3-3</a>  |
| Notification service (configuration required)  | Allows the Cisco WebEx Social administrator to send notifications to users.  | <a href="#">Notification Service, page 3-30</a>                                 |
| Password Policies (configuration required)   | Sets password policies for your users.   | <a href="#">Password Policies, page 2-23</a>                                    |
| Plugin configuration   | Allows you to make various applications active or inactive, and to set which portal roles have permissions to add specific Cisco WebEx Social application plugin to one of their pages.  | <a href="#">Plugin Settings, page 2-54</a>                                      |
| Plugin installation  | Allows you to add applications that are not part of the default set of applications shown in <a href="#">Table 1-4 on page 1-13</a> .  | <a href="#">Plugins Installation, page 3-7</a>                                  |
| Presence (configuration required)  | Allows Cisco WebEx Social users to set their availability state (either Available, Away, or Do Not Disturb) from the drop-down menu that appears near their name in Cisco WebEx Social. When users sets their availability state, this state is visible to their contacts in many areas of Cisco WebEx Social. | <a href="#">Chat, page 3-17</a>   |

**Table 1-2 Configuration References (continued)**

| Item  | Description   | Reference  |
|---|---|--|
| Resource Monitoring   | Allows you to monitor and free memory, clear the cluster cache, generate thread dumps, and so on.   | <a href="#">Resources, page 3-2</a>                        |
| Roles   | Allows you to create a wide variety of specific functions and assign them to various users, user groups, and communities.   | <a href="#">Roles, page 2-18</a>                           |
| SharePoint—Using as Cisco Repository  | Allows you to use Microsoft SharePoint 2007 as the Cisco WebEx Social repository for documents in the Cisco WebEx Social library, and attachments to Cisco WebEx Social posts and discussion boards.  | <a href="#">Content Repositories, page 2-58</a>            |
| Show and Share (configuration required)   | Allows users to upload and share video.   | <a href="#">Cisco Show And Share, page 3-32</a>            |
| SiteMinder authentication   | Allows you to configure SiteMinder single sign-on authentication.   | <a href="#">SiteMinder, page 2-49</a>                      |
| Twitter (configuration required)  | Allows users to tweet to and from Cisco WebEx Social.   | <a href="#">Twitter Administration, page 3-42</a>          |
| User Associations—Changing Defaults   | Can designate communities, roles, and user groups that should, by default, be assigned to all new users.<br><br>If you make no changes, all new users have the role of User and Power User. For definitions of role, see the “Roles” section on page 1-28.  | <a href="#">Users, page 2-51</a>                           |
| User Groups   | Allows you to bring groups of users together that may not share common or communities.  | <a href="#">User Groups, page 2-15</a>                     |
| Users   | Allows you to add, remove, edit information, set permissions, and so on for Cisco WebEx Social users.   | <a href="#">Users, page 2-1</a>                            |
| Voice Messages (configuration required)   | Lets you configure visual voice mail so that users can retrieve voice messages, send replies, send new messages, forward messages, and delete voice messages by communicating with the Cisco Unity Connection server that controls their voice mail system. | <a href="#">Voice Mail Server Configuration, page 3-33</a> |
| Web Dialer (configuration required)   | Allows users to place click-to-dial calls.  | <a href="#">WebDialer Administration, page 3-36</a>        |
| WebEx (configuration required)  | Allows users to use Webex for creating meetings and sending instant messages.   | <a href="#">WebEx Site, page 3-39</a>                      |
| WSRP Configuration and Replication Across Cisco WebEx Social Nodes (configuration required) | WSRP defines a web-service interface for accessing and interfacing with interactive, presentation-oriented web services.  | <a href="#">WSRP, page 2-56</a>                            |

## Configuring Items in the Help Window

When you click the **Help** button at the bottom of the Cisco WebEx Social window, the Cisco WebEx Social Help window appears, as shown in [Figure 1-2](#).

Figure 1-2 Help Window

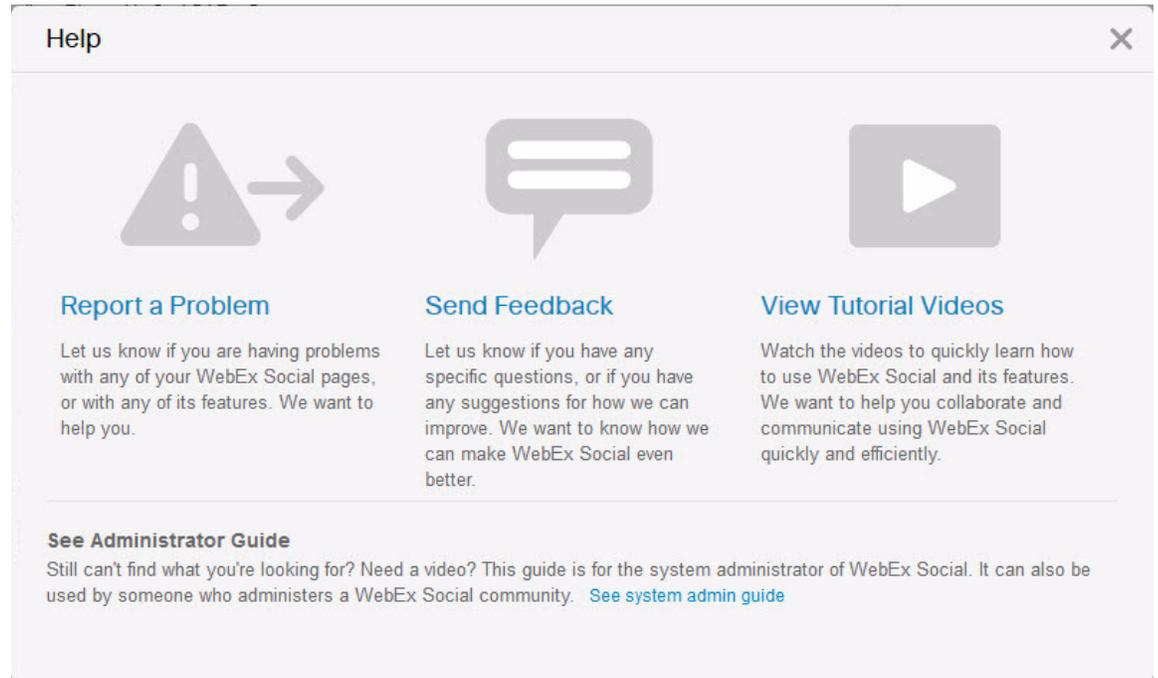


Table 1-3 describes the Help window items that you can configure, explains how to configure these items, and provides references for related information.

Table 1-3 Configuring Items in the Cisco WebEx Social Help Window

| Configurable Item   | Configuring  | Reference  |
|---|--|--|
| E-mail address or e-mail alias to which an e-mail message is sent when users use the <b>Report a Problem</b> link in the Help Window. | In the Director, click <b>Portal</b> , and in the Advanced Portal Properties area, enter the desired e-mail address or e-mail alias in the Value field for the <b>report.problem.email.to.address</b> property. Then click <b>Save</b> in the Advanced Portal Properties area. | See the “ <a href="#">Advanced Portal Properties</a> ” section on page 5-20. |
| Text that appears in the To field of the message that is sent when users use the <b>Report a Problem</b> link in the Help Window.     | In the Director, click <b>Portal</b> , and in the Advanced Portal Properties area, enter the desired string in the Value field for the <b>report.problem.email.to.name</b> property. Then click <b>Save</b> in the Advanced Portal Properties area.                            |  |

Table 1-3 Configuring Items in the Cisco WebEx Social Help Window (continued)

| Configurable Item   | Configuring   | Reference   |
|---|---|---|
| Page that appears when users click the <b>Send Feedback</b> link in the Help Window.          | In the Director, click <b>Portal</b> , and in the Error Reporting area, enter the desired link in the Send Feedback Link field. Then click <b>Save</b> in this area.      | See the “ <a href="#">Error Reporting</a> ” section on page 5-14. |
| Page that appears when users click the <b>View Tutorial Videos</b> link in the Help Window.   | In the Director, click <b>Portal</b> , and in the Error Reporting area, enter the desired link in the Tutorial Videos Link field. Then click <b>Save</b> in this area.    |   |
| Page that appears when users click the <b>See system admin guide</b> link in the Help Window. | In the Director, click <b>Portal</b> , and in the Error Reporting area, enter the desired link in the System Admin Guide Link field. Then click <b>Save</b> in this area. |   |

## Adding Users to Cisco WebEx Social

In general, you do not need to actively add users to Cisco WebEx Social. Users who are in LDAP Active Directory are authenticated and added to the Cisco WebEx Social database when they sign in. The Cisco WebEx Social password for such a user is the same as the LDAP password of that user.

However, if a user is not in LDAP and you manually add this user to Cisco WebEx Social, you need to create the same user on the Notifier node. For instructions, see the “[Adding a User to Notifier](#)” section on page 3-31.

## Introduction to the Cisco WebEx Social User Interface

Cisco WebEx Social is a portal server—a single environment in which all applications that a user needs can run. These applications are integrated in a consistent and systematic way within a single interface.

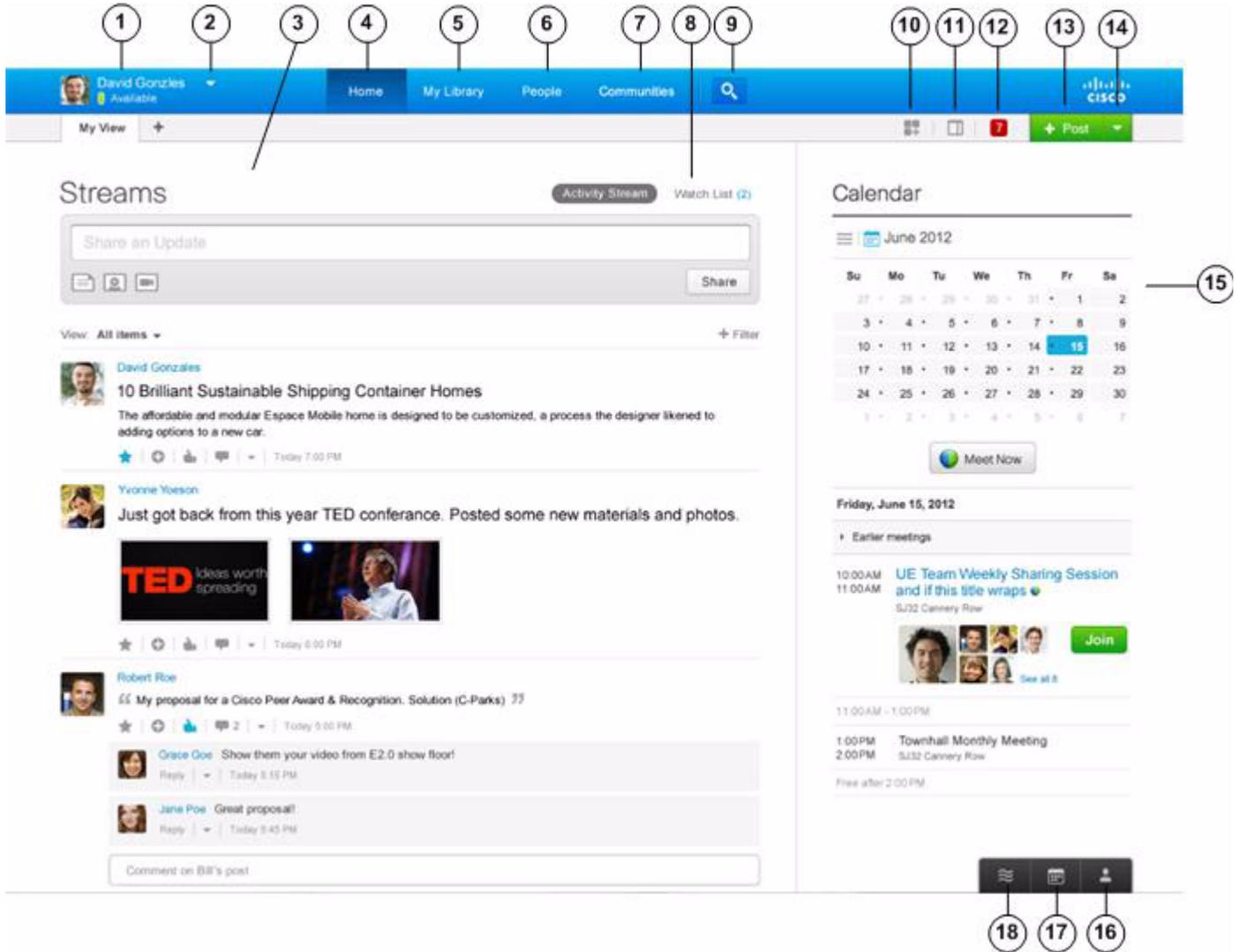
This section contains the following topics:

- [Global Navigation Options](#), page 1-10
- [Applications](#), page 1-12

## Global Navigation Options

When you sign in to Cisco WebEx Social, the Main window appears. [Figure 1-3](#) shows a typical Main window.

Figure 1-3 Cisco WebEx Social Main Window



|   |  |    |   |
|---|--|----|---|
| 1 | Your name. Click to access your My Profile page, which is a public page that everyone can see.   | 10 | Add Application button. Click to add an application to your Cisco WebEx Social pages. |
| 2 | Profile menu. Click to change your status and to access other features.  | 11 | Change Layout button. Click to manage the layout of your Cisco WebEx Social display.  |
| 3 | Streams area. Displays your activities and your watch list.  | 12 | Notifications indicator. Click to display current notifications.                      |
| 4 | Home button. Click to display your Home page, to which you can add desired applications and organize however you wish. The Home page is a private page that users can design for themselves. | 13 | Post button. Click to create a post.  |

|   |   |    |   |
|---|---|----|---|
| 5 | My Library button. Click to display your Library page. Your library provides a repository for your posts, documents, images, and videos.  | 14 | Drop-down menu. Click to access these options: <ul style="list-style-type: none"> <li>• <b>Share an Update</b>—Creates a short-form status update to be shared with your followers</li> <li>• <b>Ask a Question</b>—Creates a post that can be shared with subject matter experts in your organization</li> </ul> |
| 6 | People button. Click to display your Contacts page, which shows all available Cisco WebEx Social users.   | 15 | Calendar area. Shows your WebEx meetings and your corporate calendar (Exchange or Domino).  |
| 7 | Communities button. Click to display your Communities page. From this page, you can join communities and share information such as videos, files, and documents with communities. | 16 | My Contacts button. Shows a list of your Cisco WebEx Social contacts.   |
| 8 | Watch List button. Click to display your watch list.  | 17 | My Calendar button. Shows your WebEx meetings and your corporate calendar (Exchange or Domino).   |
| 9 | Search button. Click to search Cisco WebEx social based on search criteria that you enter.  | 18 | Activities Stream button. Click to see a list of your activities.   |

## Applications

All the application functionality within Cisco WebEx Social is divided into fragments of web applications that run in a portion of a web page. In this way, one or many applications can reside on a page, and users can (at the description of the system administrator) arrange these applications however they want.



### Note

The term *portlet* also is used in the manual and has the same basic meaning as *application*.

Some Cisco WebEx Social applications appear on certain pages by default. Those that do not appear by default can be added. Applications can be added to the Home page and the community pages. For more information about which applications can be added to which of these pages, see [Table 1-4 on page 1-13](#).

To add an application, or to see what applications are available, click the **Add Application** icon  the Home page, the Featured Content tab on the Profile page, or any community page for a community of which you are the owner or administrator. Cisco WebEx Social displays only the applications that you can add to the page that you opened.



### Note

By default, all users are given the permission to install any of the applications that [Table 1-4](#) lists. If you want to change which groups of users can install any application, or to make any of these applications unavailable for everyone to use, see the [“Plugin Settings” section on page 2-54](#).

## Application Configuration

After you have added an application to a page, you can move your cursor over the application and click the gear icon  that appears. From the drop-down menu that then appears, you can select **Edit Setting** for most applications. When you select **Edit Setting**, you are then allowed to edit Permissions for most applications. Some applications have additional options under Edit Setting, such as various Setup items. You should make sure to check what Edit Setting options are available for the applications you add, and configure these settings as you wish.

**Note**

For some applications, you need to go to the Community page to access Edit Settings.

## Application Descriptions

Table 1-4 provides an alphabetical listing and descriptions of all applications provided by Cisco WebEx Social. You can add an application to your page in these ways:

- Click the application, which adds it to the bottom of a column on your page
- Click and drag the application to the location on your page where you want it to appear

**Table 1-4 Applications Supported by Cisco WebEx Social From the Add Application Icon**

| Application Name             | Description   |
|------------------------------|---|
| Streams                      | <p>Activities allows you to display your recent activities as well as perform a number of actions.</p> <p>By default, already displays in <b>Home</b>.</p> <p>Watchlist allows you to display posts you have authored, posts you have made favorites, posts you have commented on or added something to, and posts that you have interacted with and that others have commented on, added something to, or made a favorite.</p> <p>By default, already displays in <b>Home</b>.</p> <p><b>Note</b> A dot that appears next to a post is called a badge, and indicates that you have not yet read the post. The number displayed inside a badge is the number of comments and additions that have been made to the post.</p> |
| Alerts                       | <p>Allows you to see system alert messages.</p> <p>Available only to Cisco WebEx Social system administrators.</p>  |
| Announcements                | <p>Allows you to see system announcements.</p> <p>Available only to Cisco WebEx Social system administrators.</p>   |
| Content Publisher            | <p>Allows you to display web content on your page.</p>  |
| Documents                    | <p>Allows you to access your document library and upload documents and create folders.</p> <p>By default, displays in <b>Communities &gt; Library</b>.</p>  |
| External Document Repository | <p>Allows you to access an external SharePoint 2007 or Documentum 6.5 or above repository.</p>  |
| IFrame                       | <p>Allows you to imbed another web page within a frame.</p> <p><b>Note</b> There are some sites that render your page unusable if you place them in an IFrame. This effect is commonly referred to as <i>frame busting</i>. It is recommended that, before you add an IFrame to any of your main pages, such as Home, create a new page, then add it there to test it.</p>  |
| Images                       | <p>Allows you to access to your image library and upload documents and folders.</p> <p>By default, displays in <b>Communities &gt; Library</b>.</p>   |

**Table 1-4 Applications Supported by Cisco WebEx Social From the Add Application Icon**

| Application Name          | Description  |
|---------------------------|--|
| Links                     | Allows you to create links to content for quick retrieval.   |
| Calendar                  | Allows you to place your Outlook or Lotus Domino calendar on the page.   |
| My Communities            | Allows you access your communities.<br>By default, already displays in <b>Communities &gt; My Communities</b> .  |
| OpenSocial App            | Allows you to add an OpenSocial gadget to your page.<br><br><b>Configuration Notes:</b><br>After you add the OpenSocial gadget application to your page, a small window is provided for you to paste in the URL to a gadget that you wish to add to your Cisco WebEx Social page. After you paste in the URL, click <b>Submit</b> , and the gadget appears on your page. |
| Post Library              | Allows you to display the posts of a community library.  |
| Recently Viewed Documents | Allows you to display the documents most recently accessed from the Document Library.  |
| Reported Content          | Allows you to view content that users have reported as inappropriate or incorrect.<br><br><b>Note</b> This application is available only to users who have been assigned the role of Compliance Officer by a system administrator. For information about the compliance officer role, see the <a href="#">“Compliance Officer Role”</a> section on page 1-29.            |
| RSS                       | Allows you to set up and display RSS feeds.  |
| Suggestions               | Allows you to receive suggestions for people to follow, posts to view, and communities to join.  |
| Tag Cloud                 | Allows you to navigate using tags.   |
| Voice Messages            | Allows you to see, listen, and reply to voice messages left on your phone.   |
| Wiki                      | Allows you to add a wiki.  |

## Installation and Configuration for Cisco Web Communicator

Cisco Web Communicator is a plug-in for Cisco WebEx Social. It is a softphone in your web browser. It also allows you to remotely control a physical telephone on your desk by using Computer Telephony Integration (CTI).

To use the Cisco Web Communicator softphone in Cisco WebEx Social, you must first configure the device in Cisco Unified Communications Manager. To remotely control a desk phone, that phone must be configured to allow CTI in Cisco Unified Communications Manager.

This section contains the following topics:

- [Adding Cisco Web Communicator to Cisco Unified Communications Manager, page 1-15](#)—Describes how to add a Cisco Web Communicator device to Cisco Unified Communications Manager using the Cisco Unified Communications Manager Administration user interface. (If you have many users and devices to add, you can use the Bulk Administration tool (BAT).)

- [Using BAT to Add Devices for Cisco Web Communicator, page 1-17](#)—Describes how to use the Bulk Administration Tool (BAT) to add many users and devices at one time for Cisco Web Communicator.
- [Configuring Cisco Unified Communications Manager for CTI, page 1-23](#).
- [Call Routing for Cisco Web Communicator, page 1-25](#).
- [Network Security Configuration for Cisco Web Communicator, page 1-25](#)—Provides TCP/IP port information for Cisco Web Communicator.
- [Obtaining the Plugin for Cisco Web Communicator, page 1-25](#)—Users must download the appropriate plugin for their operating systems to use Cisco Web Communicator. As the Cisco WebEx Social administrator, you can provide users with the information that they need from this section.
- [Using Cisco Web Communicator, page 1-26](#)—Provides information about how users can find training about how to use Cisco Web Communicator.

## Adding Cisco Web Communicator to Cisco Unified Communications Manager

This section describes how to add Cisco Web Communicator to Cisco Unified Communications Manager.

If a user will use Cisco Web Communicator in Computer Telephony Integration (CTI) mode only, you can skip this section and proceed to the [“Configuring Cisco Unified Communications Manager for CTI” section on page 1-23](#).

Before You Begin:

- Before configuring Cisco Web Communicator, you must configure WebDialer (if you have not already done so) to communicate properly with Cisco Unified Communications Manager. For instructions about how to configure WebDialer, see the [“WebDialer Administration” section on page 3-36](#).
- Make sure that the TFTP service is enabled on at least one WebDialer-enabled Cisco Communications Manager node.

To add a new Cisco Web Communicator device to Cisco Unified Communications Manager, perform the following steps. You must have administrative privileges on Cisco Unified Communications Manager or request that someone with these privileges perform the following procedure.

### Procedure

- 
- Step 1** Log into Cisco Unified Communications Manager Administration.
  - Step 2** Select **Device > Phone**.  
The Find and List Phones window opens.
  - Step 3** Click **Add New**.  
The Add a New Phone window opens.
  - Step 4** From the Phone Type drop-down list, select **Cisco Unified Client Services Framework**.
  - Step 5** Click **Next**.  
The Phone Configuration window opens.
  - Step 6** In the Device Information section of the Phone Configuration window, set the following:

- Device Name—Enter any name; the name must be of the form: ECP<username>. Example: ECPjohndoe
  - The device name is not case sensitive.
  - The device name is created by placing the prefix *ECP* in front of the username and then removing any characters that are not permitted. Symbols such as dots, hyphens, underscores must be stripped, as well as any accented characters or characters not in the Latin (English) alphabet.
  - Cisco Unified Communications Manager accepts a maximum length of 15 characters, so the generated name must be truncated to this length.

There may be some name clashes because names that are only unique in the 13th character and beyond become the same name when ECP is prepended and the total length is truncated to 15. Also, the names Joe.Bloggs and JoeBloggs both map to the same device name—ECPJoeBloggs. These ambiguities must be handled on a case-by-case basis, and may require that the user names be changed to make them unique.

Similarly, the user Frédéric will have a device name of ECPFrdric. Dropping the non-Latin characters can lead to further name clashes.

- Description—Enter a descriptive name, such as *John Doe's Web Communicator*.
- Device Pool—Set to the desired device pool.
- Phone Button Template—Set to **Standard Client Services Framework**.

**Step 7** In the Protocol Specific Information section of the Phone Configuration window, set the following:

- Device Security Profile—Set to Cisco Unified Client Services Framework - Standard SIP Non-Secure.
- SIP Profile—Set to Standard SIP Profile.

**Step 8** Click **Save**.

**Step 9** Click **Apply Config** if this button is available (and confirm when prompted).




---

**Note** If the **Apply Config** button is not available, click **Reset** (and confirm when prompted).

---

**Step 10** To add a line for the Cisco Web Communicator device, click **Line [1] - Add a New DN** on the upper-left portion of the Phone Configuration window.

The Directory Number Configuration window opens.

**Step 11** In the Directory Number field, enter the directory number.

**Step 12** Scroll down to the Multiple Call section and do the following:

- Set the Maximum Number of Calls to 1.
- Set the Busy Trigger to 1.

**Step 13** Click **Save**.

**Step 14** Click **Apply Config** if this button is available (and confirm when prompted).

**Step 15** Click **Associate End Users** near the bottom of the Directory Number Configuration window.

The Find and List Users window opens.

**Step 16** Use the search criteria to find the user you want to associate with the directory number, then check the box next to that user name and click **Add Selected**.

The Directory Number Configuration window should now show that the user is associated with the line. This information appears near the bottom of the window in the section called “User Associated With Line.”

- Step 17** Click on the user name in the User Associated with Line section of the window.  
The End User Configuration window opens.
- Step 18** Scroll down to the Direct Number Associations section of the window and select the primary extension from the Primary Extension drop-down list.
- Step 19** In the Permissions Information section at the bottom of the End User Configuration window, click **Add to User Group**.  
The Find and List User Groups window opens.
- Step 20** Use the search criteria to find Standard CCM End Users.
- Step 21** Check the box next to Standard CCM End Users, then click **Add Selected**.  
The Standard CCM End Users group should now appear in the Permissions Information section at the bottom of the End User Configuration window.
- Step 22** Click **Save**.  
The Cisco Web Communicator device is now configured in Cisco Unified Communications Manager.
- 

## Using BAT to Add Devices for Cisco Web Communicator

This section describes how to use the BAT to enable Cisco Web Communicator for multiple users. BAT allows you to add Cisco Unified Client Services Framework-based phone devices, and then associate these devices with a list of users.

This process requires two files—one file that lists the devices, and another file that lists the users to associate with these devices.

This section contains the following topics:

- [Required Input Files, page 1-18](#)
- [User List, page 1-18](#)
- [Device File, page 1-18](#)
- [Uploading Files, page 1-19](#)
- [Create Device Template, page 1-20](#)
- [Adding the Devices, page 1-21](#)
- [Updating the Users, page 1-21](#)
- [Enabling Cisco Unified Presence, page 1-21](#)
- [Considerations If You Use Multiple Device Pools, page 1-22](#)
- [Removing Devices, page 1-22](#)
- [File Format Issues, page 1-23](#)
- [References, page 1-23](#)

## Required Input Files

You need a user-list input file and a device-list input file. These files should always be stored in comma separated file (csv) format. The easiest way to edit the files is by using Excel, and it is recommended to always save each file as a .csv file and not as a .xls or .xlsx file.

### User List

This .csv user-list file contains two columns:

- USER ID is the name used to sign in to Cisco Unified Communications Manager.
- CONTROLLED DEVICE 1 is the device to be associated with that user.

Table 1-5 shows an example of the information to include in the user-list input file.

**Table 1-5** User-List File Example

| USER ID | CONTROLLED DEVICE 1 |
|---------|---------------------|
| jjones  | ECPjjones           |
| jmurphy | ECPjmurphy          |
| jsmith  | ECPjsmith           |

The list of usernames may be gathered from LDAP or a database, or by generating a report from Cisco Unified Communications Manager.

In Cisco Unified Communications Manager Administration, the **Bulk Administration > Users > Export Users** option can generate a list of names. The telephone number is also present when generating the list using this BAT option. Depending on the local convention, the telephone number may be only the telephone extension (typically four digits), but the number listed in the DIRECTORY NUMBER 1 column must be a complete directory number (which often has an office-code prefix).

The device name is created by placing the prefix *ECP* in front of the username and then removing any characters that are not permitted. Symbols such as dots, hyphens, underscores must be stripped, as well as any accented characters or characters not in the Latin (English) alphabet. (See Step 6 above for more details.)

If the list of usernames is generated in Cisco Unified Communications Manager Administration, then remove any columns other than USER ID and CONTROLLED DEVICE 1.



#### Note

To correctly add the device using this method, the user must already be configured on the Cisco Unified Communications Manager. If the user does not exist, the device is created but will be unusable.

### Device File

The list of devices must correspond, line for line, with the list of users. An example portion of the file is shown in Table 1-6.

**Table 1-6 Device File Example**

| DEVICE NAME | DESCRIPTION  | LOCATION | DIRECTORY NUMBER 1 | DISPLAY 1    | LINE TEXT LABEL 1 |
|-------------|--------------|----------|--------------------|--------------|-------------------|
| ECPjjones   | John's Phone |          | 61111              | John Jones   | J. Jones          |
| ECPjmurphy  | James' Phone |          | 61112              | James Murphy | J. Murphy         |
| ECPjsmith   | Jane's phone |          | 61113              | Jane Smith   | J. Smith          |

The DEVICE NAME and DIRECTORY NUMBER 1 entries are required. Other fields are optional. For example, if DISPLAY 1 and LINE TEXT LABEL 1 are populated, they appear in the device configuration in the Line 1 section of the Directory Number Configuration for that device. DIRECTORY NUMBER 1 may not be the same as the telephone number listed in LDAP, depending on local dialing rules.

## Uploading Files

To upload the user name and device name files, perform the following steps:

### Procedure

- 
- Step 1** In Cisco Unified Communications Manager Administration, select **Bulk Administration > Upload/Download Files**.
- The Find and List Files window opens.
- Step 2** Click **Add New**.
- The File Upload Configuration window opens.
- Step 3** In the File Upload Configuration window, do the following to first upload the file that lists user names:
- Use the **Browse** button to locate the file of user names.
  - From the **Select the Target** drop-down list, select **Users**.
  - From the **Select Transaction type** drop-down list, select **Update Users – Custom File**.
  - For the “**Overwrite File if it exists**” box, check the box if this is an update to a previous file; otherwise leave the box unchecked.
  - Click **Save**.
- Step 4** In the File Upload Configuration window, do the following to then upload the file that lists device names:
- Use the **Browse** button to locate the file of device names.
  - From the **Select the Target** drop-down list, select **Phones**.
  - From the **Select Transaction type** drop-down list, select **Insert Phones – Specific Details**.
  - For the “**Overwrite File if it exists**” box, check the box if this is an update to a previous file; otherwise leave the box unchecked.
  - Click **Save**.
-

## Create Device Template

To create a device template for fields that are not set by the input file, perform the following steps:

### Procedure

- 
- Step 1** From Cisco Unified Communications Manager, go to **Bulk Administration > Phones > Phone Template**.
- The Find and List Phone Templates window opens.
- Step 2** Click **Add New**.
- The Add a New Phone Template window opens.
- Step 3** From the Phone Type drop-down list, select **Cisco Unified Client Services Framework**.
- Step 4** Click **Next**.
- The Phone Template Configuration window opens.
- Step 5** In the Device Information portion of the Phone Template Configuration window, most fields can be left at default, but you must configure the following fields:
- Template Name—Give a descriptive name for the template.
  - Device Pool—Set to the desired device pool. All the devices created with this template are placed into the same device pool. If you have multiple device pools, see the [“Considerations If You Use Multiple Device Pools”](#) section on page 1-22.
  - Phone Button Template—Set to Standard Client Services Framework.
- Step 6** In the Protocol Specific Information portion of the Phone Template Configuration window, configure the following fields:
- Device Security Profile—Set to **Cisco Unified Client Services Framework – Standard SIP Non-Secure**.
  - SIP Profile—Set to **Standard SIP Profile**.
- Depending on your local requirements, you may wish to update other fields. For example, if you need a specific Calling Search Space applied to all Cisco Web Communicator devices, update that field.
- Step 7** Click **Save**.
- Step 8** In the upper-left portion of the Phone Template Configuration window, click **Line[1] – Add a new DN**.
- The Line Template Configuration window opens.
- Step 9** In the Line Template Name field, provide a descriptive name.
- Step 10** Scroll down to the Multiple Call section and do the following:
- Set the Maximum Number of Calls to 1.
  - Set the Busy Trigger to 1.
- Step 11** Other fields in the Line Template Configuration window can be left unchanged, but you may need to set some of these fields to match your local configuration requirements.
- Step 12** Click **Save**.
- The template now exists, so the next step is to add devices that will use this template.
-

## Adding the Devices

To add devices to the template you created, follow these steps:

### Procedure

- 
- Step 1** In Cisco Unified Communications Manager Administration, go to **Bulk Administration > Phones > Insert Phones**.
- The Insert Phones Configuration window opens.
- Step 2** From the File Name drop-down list, select the file (that lists devices) that you previously imported.
- Step 3** From the Phone Template Name drop-down list, select the template that you created in the “[Create Device Template](#)” section on page 1-20.
- Step 4** At the bottom of the window, select the “Run Immediately” radio button, then click **Submit**.
- The job is now in progress.
- Step 5** To view the progress and log file, go to **Bulk Administration > Job Scheduler**, then click **Find**.



---

**Note** Devices that already exist in the file are not modified.

---

## Updating the Users

After you have added the devices, you need to associate users to the devices:

### Procedure

- 
- Step 1** In Cisco Unified Communications Manager Administration, go to **Bulk Administration > Users > Update Users**.
- The Update Users Configuration window opens.
- Step 2** From the File Name drop-down list, select the file (that lists users) that you previously imported.
- Step 3** Select the “Run Immediately” radio button, then click **Submit**.
- Step 4** To view the progress, go to **Bulk Administration > Job Scheduler**.
- 

## Enabling Cisco Unified Presence

To make presence information available with Cisco Web Communicator, each line must be associated with a user. You can create a .csv file that contains this association. For an example of the type of information this file must contain, see [Table 1-7](#).

**Table 1-7 Example of Information in Line Association File**

| USER ID | DEVICE     | DIRECTORY NUMBER | PARTITION        |
|---------|------------|------------------|------------------|
| jjones  | ECPjjones  | 61111            | MyTestPartition1 |
| jmurphy | ECPjmurphy | 61112            | MyTestPartition2 |
| jsmith  | ECPjsmith  | 61113            | MyTestPartition3 |

If you are using route partitions, the PARTITION column must match the route partition that you applied to the line when you created the line template in Cisco Unified Communications Manager Administration.

To import the line-association file into Cisco Unified Communications Manager, follow these steps:

#### Procedure

- 
- Step 1** In Cisco Unified Communications Manager Administration, go to **Bulk Administration -> Upload/Download Files**.  
The Find and List Files window opens.
- Step 2** Click **Add New**.  
The File Upload Configuration window opens.
- Step 3** From the Select The Target drop-down list, select **User Line Appearance**.
- Step 4** From the Select Transaction Type drop-down list, select **Update Line Appearance - Custom File**.
- Step 5** Click **Save**.
- Step 6** Navigate to **Bulk Administration > Users > Line Appearance > Update Line Appearance**.  
The Update Line Appearance Configuration window opens.
- Step 7** From the File Name drop-down list, select the line-association file that you just uploaded.
- Step 8** Click the **Run Immediately** radio button, then click **Submit**.
- 

## Considerations If You Use Multiple Device Pools

If your users belong to different device pools, you must create a separate template for each device pool. The procedure for adding the devices must be run one time for each device pool, using the matching list and template.

## Removing Devices

If you want to remove devices, you must create a .csv file that contains only the DEVICE NAME column. The, go to **Bulk Administration > Phones > Delete Phones > Custom Files**, and use the fields in that window to define the phones to delete.

## File Format Issues

If you receive file-format error messages, examine the applicable file in Notepad to make sure no commas are missing. Sometimes, errors can occur during file-import with Excel.

## References

For more information about using BAT, see the following sources:

- Online help within Cisco Unified Communications Manager Administration.
- Bulk Administration User Guide:  
[http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_callmg/admin/bulk\\_adm/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/admin/bulk_adm/index.htm)

## Configuring Cisco Unified Communications Manager for CTI

Before configuring Cisco Web Communicator, you must configure WebDialer (if you have not already done so) to communicate properly with Cisco Unified Communications Manager. For instructions on how to configure WebDialer, see the “[WebDialer Administration](#)” section on page 3-36.



### Note

When using Cisco Web Communicator in CTI mode to control a deskphone, a user is prompted for a password. The password required they must enter is the Cisco Unified CM password. This password is not necessarily the same as the Cisco WebEx Social password, but if Cisco Unified CallManager is integrated with the same LDAP as Cisco WebEx Social and is using LDAP for authentication, these passwords will be the same. This set up is recommended to make the experience for end users as seamless as possible.

To control a device using CTI, the user must belong to the proper user group and the device must be CTI-enabled. If both these items are properly configured, no configuration changes are required.

However, if either one of these items is not configured properly or if the device has been turned off, follow these steps:

### Procedure

- Step 1** Sign in to Cisco Unified Communications Manager Administration.
- Step 2** Go to **User Management > End User**.  
The Find and List Phones window opens.
- Step 3** Enter the first few letters of the users name, then click **Find**.
- Step 4** Select the user from the list that appears.  
The End User Configuration window opens.
- Step 5** Scroll down to the Permissions Information section and click **Add to User Group**.  
The Find and List User Group window opens.
- Step 6** Click **Find**.  
All user groups are listed. Check the box to the left of each of the following groups:
  - Standard CTI Allow Call Monitoring
  - Standard CTI Allow Call Park Monitoring

- Standard CTI enabled
- Standard CTI Allow Control of Phones supporting Connected Xfer and conf

**Step 7** Click **Add Selected**.

The window closes and the End User Configuration window reopens.

**Step 8** Click **Save**.

The user is now enabled for CTI.



**Note**

Cisco Unified Communications Manager allows CTI control by default. However the “Standard CTI Allow Control of Phones supporting Connected Xfer and conf” group is not part of that default. It is recommended to add that group to the default if you have a large numbers of users who will be using CTI mode for Cisco Web Communicator.

You must also enable the phone that is associated with the user, so you must know the correct device name. Then, follow these steps:

**Procedure**

**Step 1** Sign in to Cisco Unified Communications Manager Administration

**Step 2** Select **Device > Phone**.

The Find and List Phones window opens.

**Step 3** Enter the device name, then click **Find**.

**Step 4** Select the device from the list.

The Phone Configuration Window appears.

**Step 5** In the Device Information section, locate the box labeled “Allow Control of Device from CTI.” Ensure this box is checked to allow Cisco Web Communicator to control the device.

**Step 6** Click **Save**.

**Step 7** Click **Apply Config** if this button is available (and confirm when prompted).



**Note** If the **Apply Config** button is not available, click **Reset** (and confirm when prompted).

You have now enabled both the end user and the device. The device should now be accessible from Cisco Web Communicator.

**Additional Cisco Unified Communications Manager Configuration for Video Calls**

To allow users to make video calls, make the following additional configuration settings in Cisco Unified Communications Manager:

- Set the Video Capabilities option in Cisco Unified Communications Manager to **Enabled** in the **Device > Phone** page for the devices that calls are placed on. For two-way video communication, video must be enabled for both endpoints.

- Set the RTCP option in Cisco Unified Communications Manager to **Enabled** in the Product Specific Configuration Layout area in the **Device > Device Settings > Common Phone Profile** page for the devices that calls are placed on.

## Call Routing for Cisco Web Communicator

Cisco Web Communicator uses contact numbers from the Cisco WebEx Social directory. These are typically E.164 numbers, which are fully qualified international number starting with +. Also on Cisco Web Communicator, or any other softphone client, users may copy and paste numbers in from other sources on the internet. Therefore, it is recommended that Cisco Unified Communications Manager be configured to support E.164 numbers. How this is configured depends on you Cisco Unified Communications Manager version and your local numbering scheme.

## Network Security Configuration for Cisco Web Communicator

If there are firewalls in your network, you may need to open the following ports on the client PC from which you access Cisco WebEx Social. These ports are used by Cisco Web Communicator:

- Port 69 for outward UDP traffic, for TFTP.
- Port 5060 for outward TCP connections, for SIP.
- Port 2748 for outward TCP connections, for QBE (which is the protocol used for CTI).
- Ports 16384 to 32766 for inward and outward TCP connections, for RTP (audio) streams.
- Port 80 for outward HTTP traffic to reach the web site hosting Cisco Web Communicator.

If any of the ports listed above are blocked, or if the service they offer is not accessible, Cisco Web Communicator fails to start.

If the Windows Firewall is running, you must add Mozilla Firefox and Internet Explorer to the list of allowed programs so that they can receive incoming network connections. Use the Exceptions tab in the firewall configuration dialog to perform this configuration.

## Obtaining the Plugin for Cisco Web Communicator

All users must download the appropriate plugin for their operating systems to use Cisco Web Communicator. As the Cisco WebEx Social administrator, you can provide the following instructions to your users for installing the plugin from a supported browser:



### Note

The system prompts users to install the plugin if it is not installed when they first try to make a call. The procedure below can be used by users who choose to install later.

### Procedure

- Step 1** Open a supported browser and log in to Cisco WebEx Social.
- Step 2** Click the Contacts icon in the lower right corner of your Cisco WebEx Social window .  
The My Contacts pop-up window appears.
- Step 3** In the My Contacts pop-up window, click the Settings icon .

- Step 4** Click **Call and Conversation Settings**.  
The Call and Conversation window appears.
- Step 5** In the Call and Conversation window, click **Download Plugin**.
- Step 6** Take the appropriate action, depending on your platform:
- On Windows platforms, the browser downloads a file called *CiscoWebCommunicator.exe*. After this file has downloaded, run it and follow the installation instructions.
  - On Mac platforms, the browser downloads a file called *CiscoWebCommunicator.dmg*. Once this file has downloaded, open the file. Wait for a few seconds, then a Finder window that contains “Cisco Web Communicator Plug-in.pkg” opens. Open the file and follow the instructions to install the plugin.
- Step 7** Repeat [Step 2](#) through [Step 4](#) and make sure that “Loading the Call Plugin” appears in the Call and Conversation window.
- 

## Using Cisco Web Communicator

To use Cisco Web Communicator to place a call, follow these steps:

### Procedure:

- Step 1** From Cisco WebEx Social, hover your mouse over the name of a person on any page that displays your contacts.  
A hover card for the user appears.
- Step 2** In the hover card, click the Call icon .
- 

## Introduction to Users, Collections of Users, and Roles

This section introduces some basic concepts used in the organization of a portal and its resources. The following concepts are used frequently in this guide:

- A *user* is anyone using Cisco WebEx Social.
- A *user group* is an arbitrary collections of users, which can be created only by system administrators.
- A *community* is a collection of users who have a common interest. Communities can also contain user groups. Communities can be created by any Cisco WebEx Social user, but only the system administrator has control over all communities in the portal. For example, the system administrator can control areas such as membership, roles and permissions for any community.
- *Roles* are used to define permissions and the scope of these permissions: across the portal, or across a community.

One way to conceptualize portal architecture is that you have users and various ways those users can be grouped together.

Other groupings may be done administratively by role assignments for other functions that may cut across the portal. An example is a Message Boards Administrator role made up of users from multiple communities, where these users can have system-administrator-type rights over any message board in the portal.

This section contains these topics:

- [Users, page 1-27](#)
- [User Groups, page 1-27](#)
- [Communities, page 1-27](#)
- [Roles, page 1-28](#)

## Users

Users can be collected in several ways. They can be collected into arbitrary user groups, such as *Bloggers*, which would enable them to create blog entries in their personal space. They can be members of organizational hierarchies. They can be members of communities that draw together common interests. They can also have roles that describe their functions in the system, and these roles can be scoped by portal or community.

For information about adding and administering users, see the [“Users” section on page 2-1](#).

## User Groups

User groups are simple, arbitrary collections of users, created by administrators. User groups can be members of communities or users that share a common role. They also can be used to assign users to communities. Permissions cannot be assigned to user groups. Though user groups do not have their own pages, user groups have page templates that can be used to customize users' personal sets of pages. For information about adding and administering user groups, see [“User Groups” section on page 2-15](#).

## Communities

Communities are collections of users who have a common interest. There are three types of communities:

- **Open (default)**—Cisco WebEx Social users can join and leave the community whenever they want, using the control panel or the Communities application added to a page that they can access.
- **Restricted**—Users can be added only by the community owner or the community administrator. For more information about roles, see the [“Roles” section on page 1-28](#). Users may use the control panel or the Communities application to request membership.
- **Hidden**—A hidden community it does not appear in the Communities application or the control panel. A user can be added to a hidden community only by an invitation from the community owner or the community administrator.

Communities are ideal workspaces for teams to collaborate on common projects. They provide an isolated area where a group of people can place all of their data pertaining to a particular topic. For example, within a community, you might use some Cisco WebEx Social applications as follows:

- **Documents**—This application lets users access and update documents pertaining to a specific project simultaneously, and all versions of the documents are preserved.

- Message Boards—This application can be used to keep all team discussions about a project in one place.

**Note**

Users can create communities, and the creator of a community automatically is the owner of that community and has full rights to that community. The system administrator has full rights over all communities in Cisco WebEx Social. After a community is created, its type cannot be changed.

For information about adding and administering communities, see the [“Communities” section on page 2-11](#).

## Roles

A role is of a set of permissions that is defined for a particular breadth of the portal (such as for a community or for the entire portal, and for some or all applications). One of your most important duties as a system administrator is to create and define new roles, redefine existing roles, and assign these roles to users, user groups, and communities in Cisco WebEx Social.

This section contains the following topics:

- [Default Roles You Can Assign, page 1-28](#)
- [Scopes of Roles, page 1-29](#)
- [Compliance Officer Role, page 1-29](#)

### Default Roles You Can Assign

[Table 1-8](#) describes the set of default roles that you, as system administrator, can assign to any Cisco WebEx Social user.

**Table 1-8 Roles and Definitions**

| Role                    | Definition   |
|-------------------------|--|
| Administrator           | A person (a <i>super user</i> ) who has can access and control all areas of Cisco WebEx Social.  |
| Level 1 Administrator   | A person who has limited access and control to Cisco WebEx Social. Can access these portal drawers and features: Users, Communities, User Groups, Roles, Community Manager, and WebEx Social Metrics. Cannot access Server drawers. Cannot change settings of the Administrator role |
| Community Owner         | A person who created a community, and is therefore automatically a super user of that community. They can assign community roles to other users.   |
| Community Administrator | A person who is a super user of their community but cannot assign the role of Community Administrator to any other users.  |
| Community Member        | A person who belongs to a community.   |
| Compliance Officer      | A person who monitors and can act on content that users have reported as inappropriate or incorrect. For more information, see the <a href="#">“Compliance Officer Role” section on page 1-29</a> .  |

**Table 1-8 Roles and Definitions (continued)**

| Role       | Definition   |
|------------|--|
| Guest      | A person who does not log in with a username and password, but can view content if permitted.  |
| Owner      | This is an implied role with respect to objects the user creates. Objects include blog entries, wikis, documents, and more.                          |
| Power User | A person who can create their own public and private pages.<br>By default, all users are assigned the Power User and the User roles.                 |
| User       | A person who can browse other pages but not create public or private pages.<br>By default, all users are assigned the User and the Power User roles. |

## Scopes of Roles

There are two kinds of roles:

- Portal Roles
- Community Roles

These are called role *scopes*. Roles are used to define permissions across their scope: across the portal or across a community. Roles exist as a bucket for granting permissions to the users who are members of them.

Portal permissions cover portal-wide activities that are in several categories, such as community, location, or password policy. In this way, you can create a role that, for example, can create new communities in the portal. With portal permissions, you can grant users a particular permission without making them overall system administrators. Cisco WebEx Social, by default, has been set up so that users can create communities.

Roles can also be granted permissions to various functions within Cisco WebEx Social applications. For example, consider a role that grants access to create 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.

Because roles are used strictly for portal security, they also do not have their own pages.



### Note

Users, user groups, and communities can all be members of a role.

For information about creating new roles, and defining and assigning roles, see the [“Roles” section on page 2-18](#).

## Compliance Officer Role

A compliance officer can be any Cisco WebEx Social user who is assigned this role by a Cisco WebEx Social system administrator. There can be any number of compliance officers on your Cisco WebEx Social platform.

**Note**

Even though the role of compliance officer can be performed by a non-system administrator, the role is described in this document because it is an administrative type of role. Make sure to provide the necessary information to your users.

The job of a compliance officer is to examine content that users report as inappropriate or missing and decide what to do with this content. The compliance officer can request that the author change the content in question or the compliance officer can decide to make a decision without contacting the author.

**Threshold Set by System Administrator**

One setting that affects reported content that only a system administrator can configure is the threshold for how many times the same content can be reported by Cisco WebEx Social users before Cisco WebEx Social automatically hides this content.

For information about where to set this threshold, see the [“Reported Content”](#) section on page 2-53.

**Compliance Officer E-Mail Setting**

Another setting that only a system administrator can configure is the e-mail address and “from” name that are associated with e-mails that are sent to users from the compliance officer.

For information about where to configure this setting, see the [“Compliance Officer Email”](#) section on page 5-14.

**Adding Reported Content Application to Home Page**

If you are assigned the role of compliance officer, you must first add the application called “Reported Content” to your Home page. To do so, follow these steps:

**Procedure**

- 
- Step 1** From your Home page, click  to add an application.
  - Step 2** Locate the Reported Content application (see [Figure 1-4](#)).
  - Step 3** Drag and drop the Reported Content application to your Home page.
- 

**Figure 1-4** *Reported Content Application*



After the application loads, the Reported Content window opens (see [Figure 1-5](#)). This window shows all cases of reported content and the status of each case, including cases that have already been resolved. To see case details, click on a case, and a window such as the example shown in [Figure 1-6](#) opens.

**Figure 1-5** *Reported Content Window*

Reported Content

Show All Types

All (9) New: 0 Hidden: 0 Change Requested: 0 Waiting Approval: 0 Resolved: 9

| Case/Report  | Reported By              | Modified        | CO Name      | Status   |
|--|--------------------------|-----------------|--------------|----------|
| <b>6378443: Nirali Upadhyaya's PostComment (1)</b><br>wfewfwe        | arjun Sirupa             | Nov 11 11:36 PM | arjun Sirupa | Resolved |
| <b>6377766: Public Profile (1)</b><br>awefaeef                       | arjun Sirupa             | Nov 11 10:46 PM | arjun Sirupa | Resolved |
| <b>6377981: shan user 1's Profile Picture (1)</b><br>flag this photo | Shanthi Nellaiappan      | Nov 11 4:48 PM  | shan user1   | Resolved |
| <b>6377959: post in sanity tcp community (1)</b><br>dddddddddddd     | ShanUser2<br>Shanuser222 | Nov 11 4:43 PM  | shan user1   | Resolved |
| <b>6377901: mark's new entry (1)</b><br>asfae                        | arjun Sirupa             | Nov 11 4:32 PM  | arjun Sirupa | Resolved |
| <b>6377779: sanity testing (1)</b><br>asdf                           | Mark Storus              | Nov 11 4:25 PM  | Mark Storus  | Resolved |

**Figure 1-6** *Example of a Case Details Window*

Case Details

Case ID: 6378443 Last Modified: Nov 11 11:36 PM  
 Status: Resolved Compliance Officer: arjun Sirupa

Reports

|                                    |                           |
|------------------------------------|---------------------------|
| Reported By: arjun Sirupa          | Reported: Nov 11 11:34 PM |
| Report Type: Inappropriate Content | Reported Version: N/A     |
| Description<br>wfewfwe             |                           |

Content Details

Reported Content Request Change Hide Content Edit Resolve

This content is not available.

## Duties of Compliance Officer

To handle a case, you click on one of the cases in the “New” column in the Reported Content window (Figure 1-5 on page 1-31), and take an action, whether it be to resolve the case right away, or to hide it and request a change of content from the author.

### Notes About Reported Content Cases:

- Only compliance officers and authors of reported content can view the content while the case is in progress.
- The compliance officer can decide to immediately hide the content permanently.

- Compliance officers and authors can go to their Library tab and locate a system-generated post that provides up-to-date status on the case.
- Authors of reported content are notified by e-mail and in their Cisco WebEx Social watch list of case developments.
- Compliance officers are notified by e-mail of case developments. Also, refreshing the Reported Content Window provides up-to-date status on every case.

## Basic Verification Steps for the User Interface

Before announcing to your users that Cisco WebEx Social is running and ready for them to use, you may want to perform some simple tasks to make sure you obtain the expected behavior. This section covers a few simple scenarios that you may want to try:

- [Editing Your Profile, page 1-32](#)
- [Using the New Post Application, page 1-33](#)
- [Adding an Application, page 1-33](#)

### Editing Your Profile

Follow these steps to edit your Home page, and check that the steps work as described:

#### Procedure

- 
- Step 1** Click your name or picture icon at the left of the Global Navigation bar.  
**Expected behavior:** Your Profile page appears.
- Step 2** Click the Edit Page  icon.  
**Expected behavior:** The page opens in edit mode.
- Step 3** Click **Edit Photo**.  
**Expected behavior:** A popup window appears that allows you to browse for a picture to upload.
- Step 4** Browse your hard drive to find the desired photo, click **Upload**, crop the photo as desired, then click **Save**.  
**Expected behavior:** The picture appears in the photo box.
- Step 5** Click the **Edit** button.  
The page opens in edit mode.
- Step 6** Use the provided boxes to enter other information about yourself, such as e-mail addresses, phone numbers, interests, areas of expertise, and tags, then click **Save**.  
**Expected behavior:** The page exits edit mode and returns to the regular Profile view. All changes you made while the page was in edit mode should have taken effect.
-

## Using the New Post Application

Follow these steps to create a post and share it with a community, and check that the steps work as described:

### Procedure

---

- Step 1** Click the + **Post** button in the global navigation bar.  
**Expected behavior:** The New Post dialog box opens.
- Step 2** Enter a message and give your post the title of “test post.”
- Step 3** Click the **Browse my Connections** icon .  
**Expected behavior:** The Share With dialog box opens.
- Step 4** Under My Communities in the dialog box, use the boxes to indicate that you want to share the post with the a few users, then click **Post**.  
**Expected behavior:** You should see a message that your post was successful and that it can be accessed in your Library, which is referring to the Library page that you access from the Library tab in the global navigation bar.
- Step 5** Your post appears in multiple locations. Check that the post appear in the following two places (navigate the user interface as follows):
- **Library > Posts > My Posts**
  - **Communities > Selected\_Community > Library > Posts**
- 

## Adding an Application

Follow these steps to add an application to your Home page:

### Procedure

---

- Step 1** Click **Home** in the Global Navigation bar.
- Step 2** Click the **Add Application** icon .
- Step 3** Locate the application that you want to add and drag and drop it in the desired location in your Home page.  
The application appears in your Home page.
- 

## Enabling or Disabling Cisco WebEx Social Components

Cisco WebEx Social components can be enabled and disabled by using the Topology window in the Director. For complete information, see the [“System: Topology” section on page 5-8](#).

# Serviceability

Cisco WebEx Social administrators can access a variety of serviceability features that allow monitoring Cisco WebEx Social operations and assist with diagnosing issues.

[Table 1-9](#) provides an overview of the Serviceability features and provides references for more detailed information. For additional related information, see *Cisco WebEx Social Troubleshooting Guide*.

**Table 1-9 Cisco WebEx Social Serviceability Features**

| Feature               | Description   | Reference   |
|-----------------------|---|---|
| Configuration options | Use the Configuration window in the Director to set up e-mail recipients for alert notifications and to configure an SNMP community stream. | See the “ <a href="#">System: Configuration</a> ” section on page 5-2 |
| Health information    | The Health window in the Director displays the health status of various services that run on each Cisco WebEx Social node                   | See the “ <a href="#">System: Health</a> ” section on page 5-12       |
| Statistics            | Displays metrics of various Cisco WebEx Social components   | See the “ <a href="#">System: Stats</a> ” section on page 5-13        |
| Logs                  | Logs collect a variety of information about the operation of Cisco WebEx Social.  | See the “ <a href="#">Log Properties</a> ” section on page 3-3        |

## Backup and Restore

For information about backing up Cisco WebEx Social, see *Cisco WebEx Social Disaster Recovery Using Snapshots, Release 3.0*.

## Setting Up a CDN

This section describes how to set up a content delivery network (CDN) for your Cisco WebEx Social deployment. A CDN can be useful when your users are geographically dispersed.

### Before you Begin

Obtain the Cisco WebEx Social installation image from Cisco.

To set up a CDN, follow these steps:

### Procedure

- 
- Step 1** Identify a Linux server that is running Apache or nginx to be used as the CDN web server. CDN files will be deployed in this server.
- Step 2** Take these actions to mount the Cisco WebEx Social installation image:
- a. Use an SSH client to access the CDN web server and log in as the admin user.
  - b. Enter this command on the CDN web server to copy the CDN zip file from the Director:
 

```
scp admin@director_hostname>:/opt/cisco/files/cdn.tar.gz
```

- Step 3** Unzip the `cdn.tar.zg` file in the root directory of the CDN web server.
- Step 4** Take either of these actions:
- If your CDN web server is running Apache, use **mod\_headers** add the following header in the `<VirtualHost>` sections:  
**Header set Access-Control-Allow-Origin \***  
With this configuration, an HTTP response that the CDN web server sends to a request for an asset includes this header, which allows a browser to accept the JavaScript that is served from this alternate domain
  - If your CDN web server is running nginx, enable Cross Origin Resource Sharing.
- Step 5** Sign in to the Director and take these actions:
- a. Click **Portal** under Application.
  - b. In the Advanced Portal Properties area:
    - If you are using HTTP for communication with the CDN web server, change the `static.cdn.host.http` property to the hostname URL of the CDN web server. Use the format **HTTP://hostname**. For example, `http://static.host.com`.
    - If you are using HTTPS for communication with the CDN web server, change the `static.cdn.host.https` property to the hostname URL of the CDN web server. Use the format **HTTPS://hostname**. For example, `https://static.host.com`.
  - c. Click **Save** in the Advanced Portal Properties area.
- 

## Proxy Server Authentication

Cisco WebEx Social supports the use basic and NTLMv1 authentication for proxies. If you are using features require access to the Internet (such as chat, RSS integration, or Twitter integration) and your proxy requires authentication, ensure sure that your proxy server supports one of these authentication types.

## Submitting Cisco WebEx Social API Requests or Using a Mobility App through a Load Balancer

Each time you submit a Cisco WebEx Social API request or use a mobility app that goes through a load balancer, the client and the server both use the request URL to generate an OAuth security signature (the *oauth\_signature*). Both *oauth\_signatures* that are generated for a request must match or the request is not validated. If the client sends an API request through a networking device that performs URL rewriting, the *oauth\_signatures* will not match and the request will be denied with the error `oauth_problem=signature_invalid`.

To avoid this situation, configure the expected URL in the networking device and pass it in the header of the API request. This URL is the one that your application uses to access the Cisco WebEx Social API.

**Procedure**

- 
- Step 1** In the Director, select **Portal** under Application and in the Advanced Properties area, set the `quadapi.auth.quad-oauth-header` to **True**.
- Step 2** Configure the networking device that API requests are sent through as follows:
- Remove all HTTP headers that start with **x-quad-oauth**
  - Add **x-quad-oauth *server\_URL***, *server\_URL* is the URL that the device uses to access Cisco WebEx Social

For example, on an Apache server, edit the configuration file named `httpd.conf` and add the following lines under `VirtualHost`. In the second line, replace *server\_URL* with the URL that a user enters to access Cisco WebEx Social from a client (for example, `https://mobileproxy.cisco.com`).

**RequestHeader unset x-quad-oauth**

**RequestHeader add x-quad-oauth *server\_URL***

---

## Downloading Images and Attachments to Mobile Clients

The Cisco WebEx Social portal redirects to HTTPS all HTTP requests for images or attachments that the portal receives from mobile clients, if the HTTPS option is enabled in Cisco WebEx Social.

If this option is enabled, the Cisco WebEx Social administrator should inform mobile client users to take either of actions to ensure that images and attachments appear on a mobile client:

- On the mobile client, start the Cisco WebEx Social application, select **Settings**, select **Clear Settings**, then select **Yes**. Next, log back in to Cisco WebEx Social using HTTPS (instead of HTTP) in the Cisco WebEx Social server URL. For subsequent log ins, users do not need to clear settings. They only need to use HTTPS in the Cisco WebEx Social server URL.
- On the mobile client, enable the option for using SSL.