Cisco WebEx Social Administration Guide, Release 3.1

Revised March 14, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-28096-01

Cisco WebEx Social Administration Guide, Release 3.1

CONTENTS

Preface

Overview

Cisco WebEx Social Administration Guide, Release 3.1 provides information for a Cisco WebEx Social system administrator. It explains how to use the Cisco WebEx Social Portal, Server, and Director pages to configure, manage, and monitor Cisco WebEx Social, and how to perform several related tasks.

Audience

This manual is intended for an administrator of Cisco WebEx Social. It can also be used by someone who administers a Cisco WebEx Social community.

Organization

This manual is organized as follows:

Chapter	Description
Chapter 1, "Cisco WebEx Social Administration Overview"	Provides general information about Cisco WebEx Social, including how to configure yourself as a system administrator, how to create user groups and communities, and how to define roles and set permissions
Chapter 2, "Portal Settings"	Describes how to use the Portal tab of Cisco WebEx Social administration to configure settings of the portal, including adding and editing user records
Chapter 3, "Server Settings"	Describes how to use the Server tab of Cisco WebEx Social administration to configure items such as system resources, log levels, and system properties
Chapter 4, "Mobile Settings"	Describes how to use the Mobile tab of Cisco WebEx Social administration to configure and manage the branding and extensibility features

Chapter 5, "Director"	Describes how to use the Director to configure topology, monitor system performance, and manage various system set up and configuration options
Appendix A, "Modifying Default Layouts and Creating a Custom Template"	Describes how to modify various default templates to change the layout of Cisco WebEx Social pages

Related Documentation

- *Cisco WebEx Social Installation and Upgrade Guide, Release 3.0*
- *Cisco WebEx Social Server: Getting Started Guide, Release 3.0*
- *Cisco WebEx Social Troubleshooting Guide, Release 3.0*
- *Cisco WebEx Social API Reference Guide, Release 3.0*
- *Open Source License Notices for Cisco WebEx Social*
- *Cisco WebEx Social Disaster Recovery Using Snapshots, Release 3.0*
- *Cisco WebEx Social Compatibility Guide*

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information about obtaining documentation, obtaining support, providing documentation feedback, security guidelines, recommended aliases, general Cisco documents, and new and revised Cisco technical documentation, see the monthly *What's New in Cisco Product Documentation* at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

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

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. Maximum: 2 nodes. **Note** 2 nodes are recommended to provide for high availability and redundancy.
App Server	The core Cisco WebEx Social web application.	Minimum: One node. 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. 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. 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. Maximum: 2 nodes. **Note** 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. Maximum: 2 nodes.
Notifier	XMPP publisher for notification of end-user events, including system alerts, announcements, and activities.	Minimum: 1 node. Maximum: 1 node.
RDBMS Store	Data store for data from the Notifier and App Server.	Minimum: 1 node. 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. Minimum: 1 Search Store master and 1 Search Store slave. 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). 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.	Plugin Settings, page 2-54
Application Plugin Active/Inactive Status	Sets which Cisco WebEx Social applications are available or unavailable to all users.	Plugin Settings, page 2-54
Calendar Server (configuration required)	Allows users to access Calendar applications.	Calendar Server, page 3-10
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.	Chat, page 3-17
Cisco Web Communicator	Allows users to use Cisco Web Communicator within Cisco WebEx Social.	Installation and Configuration for Cisco Web Communicator, page 1-14
Communities	Allows you to add, remove, assign roles, assign members, and so on, for Cisco WebEx Social communities.	Communities, page 2-11
Community Manager	Allows you to create categories that users can use when they create new communities.	Community Manager, page 2-25

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.	Compliance Officer Role, page 1-29
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.	Mail, page 3-5
Help Links	You can configure various items that are used in the Help window.	Configuring Items in the Help Window, page 1-8
Feature disablement and enablement	Allows you to disable and reenable a number of Cisco WebEx Social features.	WebEx Social Functionality, page 2-32
Kerberos	Allows you to configure the Kerberos authentication protocol, which enables devices to communicate securely over a non-secure network.	Kerberos Properties, page 5-22
Keystore Generation	Allows you to SSL certificates that are used to complete WebEx Site, WebEx IM, and VoiceMail configuration.	WebEx SSO, page 5-24 WebEx IM SSO, page 5-24
LDAP Authentication (configuration required)	Performs user authentication.	LDAP Authentication, page 2-41
LDAP Directory Synchronization (configuration required)	Synchronizes Cisco WebEx Social server with LDAP directory.	LDAP Directory Sync, page 2-44
LDAPS Authentication and Directory Synchronization (configuration required if choosing this over LDAP)	Authenticates and synchronizes Cisco WebEx Social with LDAP directory using SSL.	LDAPS Authentication and Synchronization, page 2-46
Log Properties	Lets you configure various log levels for troubleshooting purposes.	Log Properties, page 3-3
Notification service (configuration required)	Allows the Cisco WebEx Social administrator to send notifications to users.	Notification Service, page 3-30
Password Policies (configuration required)	Sets password policies for your users.	Password Policies, page 2-23
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.	Plugin Settings, page 2-54
Plugin installation	Allows you to add applications that are not part of the default set of applications shown in Table 1-4 on page 1-13.	Plugins Installation, page 3-7
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.	Chat, page 3-17

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.	Resources, page 3-2
Roles	Allows you to create a wide variety of specific functions and assign them to various users, user groups, and communities.	Roles, page 2-18
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.	Content Repositories, page 2-58
Show and Share (configuration required)	Allows users to upload and share video.	Cisco Show And Share, page 3-32
SiteMinder authentication	Allows you to configure SiteMinder single sign-on authentication.	SiteMinder, page 2-49
Twitter (configuration required)	Allows users to tweet to and from Cisco WebEx Social.	Twitter Administration, page 3-42
User Associations—Changing Defaults	Can designate communities, roles, and user groups that should, by default, be assigned to all new users. 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.	Users, page 2-51
User Groups	Allows you to bring groups of users together that may not share common or communities.	User Groups, page 2-15
Users	Allows you to add, remove, edit information, set permissions, and so on for Cisco WebEx Social users.	Users, page 2-1
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.	Voice Mail Server Configuration, page 3-33
Web Dialer (configuration required)	Allows users to place click-to-dial calls.	WebDialer Administration, page 3-36
WebEx (configuration required)	Allows users to use Webex for creating meetings and sending instant messages.	WebEx Site, page 3-39
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.	WSRP, page 2-56

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

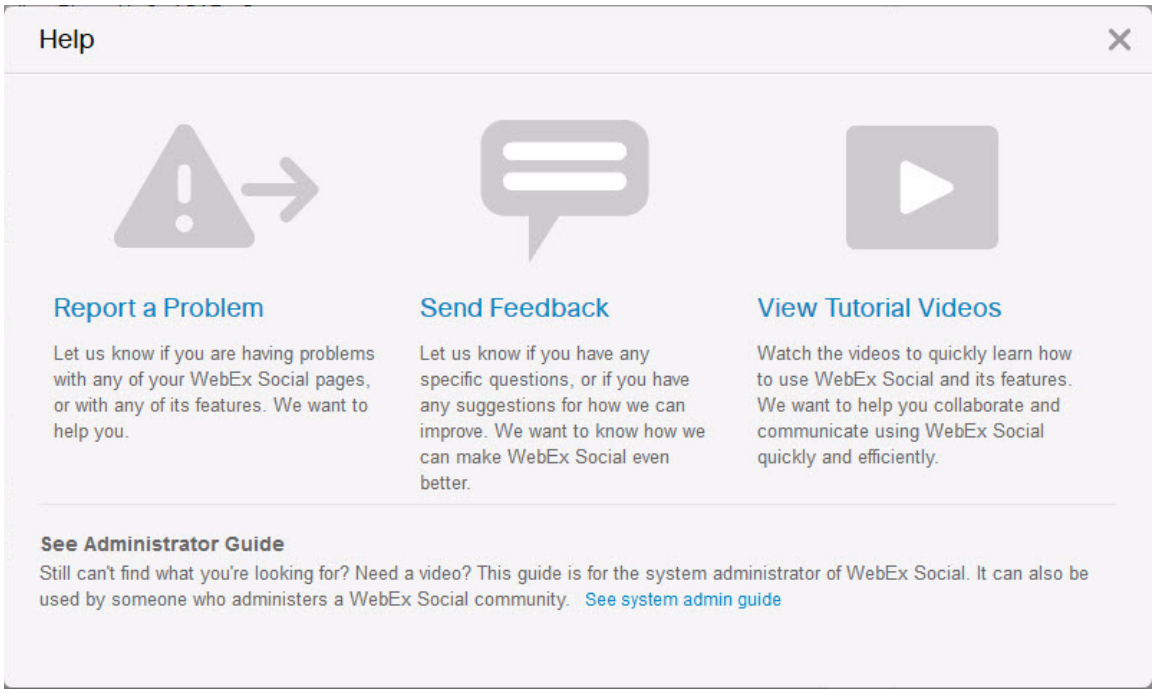


Table 1-3 describes the Help window items that you can configure, explains how to configure these items, and provides references for related information.

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 **Report a Problem** link in the Help Window.	In the Director, click **Portal**, and in the Advanced Portal Properties area, enter the desired e-mail address or e-mail alias in the Value field for the **report.problem.email.to.address** property. Then click **Save** in the Advanced Portal Properties area.	See the "Advanced Portal Properties" section on page 5-20.
Text that appears in the To field of the message that is sent when users use the **Report a Problem** link in the Help Window.	In the Director, click **Portal**, and in the Advanced Portal Properties area, enter the desired string in the Value field for the **report.problem.email.to.name** property. Then click **Save** 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 **Send Feedback** link in the Help Window.	In the Director, click **Portal**, and in the Error Reporting area, enter the desired link in the Send Feedback Link field. Then click **Save** in this area.	See the "Error Reporting" section on page 5-14.
Page that appears when users click the **View Tutorial Videos** link in the Help Window.	In the Director, click **Portal**, and in the Error Reporting area, enter the desired link in the Tutorial Videos Link field. Then click **Save** in this area.	
Page that appears when users click the **See system admin guide** link in the Help Window.	In the Director, click **Portal**, and in the Error Reporting area, enter the desired link in the System Admin Guide Link field. Then click **Save** 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

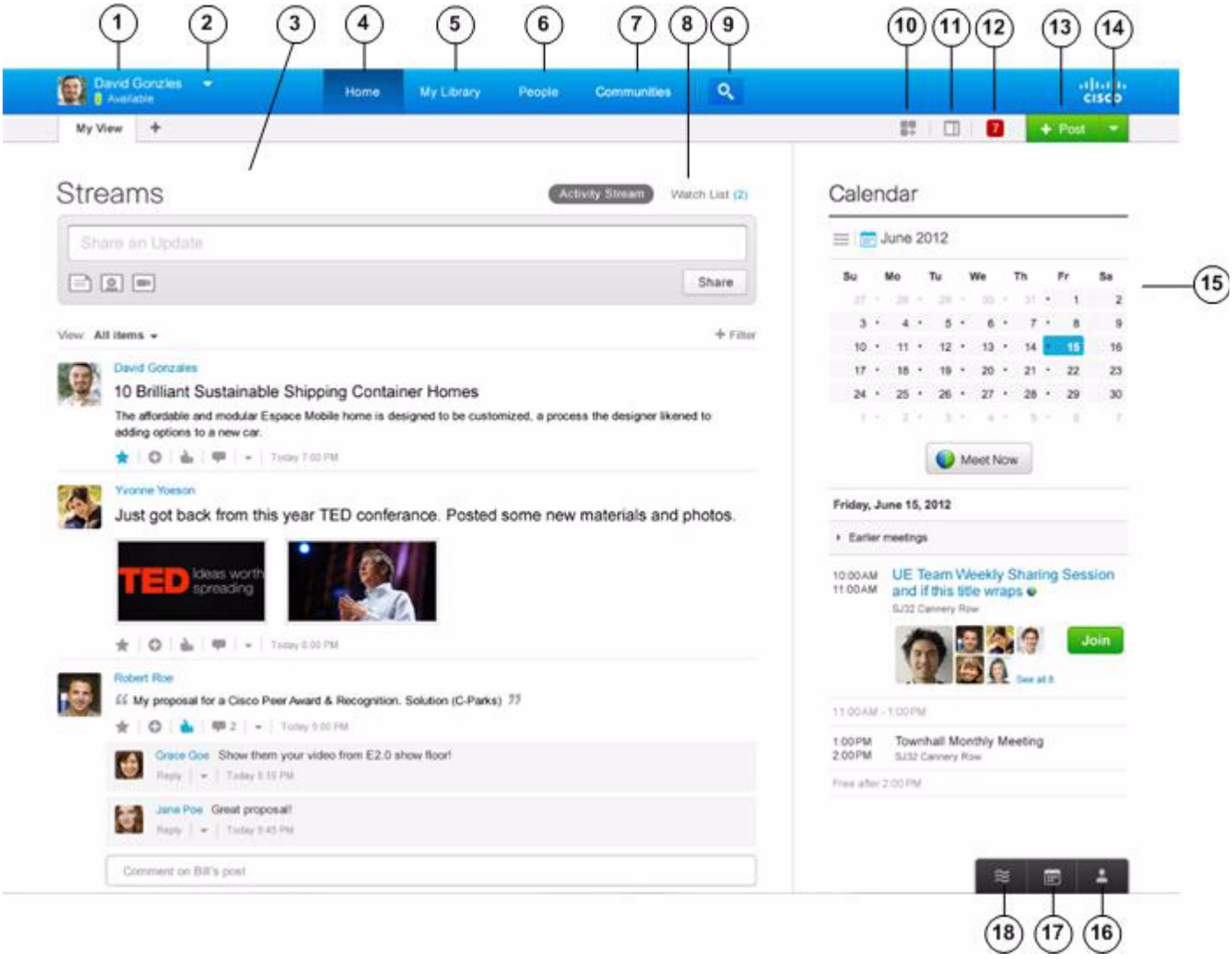
Cisco WebEx Social is a portal server—a single environment in which all applications that a user needs can run. These applications are integrated in a consistent and systematic way within a single interface.

This section contains the following topics:

Global Navigation Options

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: • **Share an Update**—Creates a short-form status update to be shared with your followers • **Ask a Question**—Creates a post that can be shared with subject matter experts in your organization
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 con 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	Activities allows you to display your recent activities as well as perform a number of actions. By default, already displays in **Home**. 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. By default, already displays in **Home**. **Note** 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.
Alerts	Allows you to see system alert messages. Available only to Cisco WebEx Social system administrators.
Announcements	Allows you to see system announcements. Available only to Cisco WebEx Social system administrators.
Content Publisher	Allows you to display web content on your page.
Documents	Allows you to access your document library and upload documents and create folders. By default, displays in **Communities > Library**.
External Document Repository	Allows you to access an external SharePoint 2007 or Documentum 6.5 or above repository.
IFrame	Allows you to imbed another web page within a frame. **Note** There are some sites that render your page unusable if you place them in an IFrame. This effect is commonly referred to as *frame busting*. 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.
Images	Allows you to access to your image library and upload documents and folders. By default, displays in **Communities > Library**.

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. By default, already displays in **Communities > My Communities**.
OpenSocial App	Allows you to add an OpenSocial gadget to your page. **Configuration Notes:** 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 **Submit**, 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. **Note** 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 "Compliance Officer Role" 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

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:

a. Use the Browse button to locate the file of user names.

b. From the Select the Target drop-down list, select **Users**.

c. From the Select Transaction type drop-down list, select **Update Users – Custom File**.

d. 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.

e. Click **Save**.

Step 4 In the File Upload Configuration window, do the following to then upload the file that lists device names:

a. Use the Browse button to locate the file of device names.

b. From the Select the Target drop-down list, select **Phones**.

c. From the Select Transaction type drop-down list, select **Insert Phones – Specific Details**.

d. 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.

e. 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

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

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

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 *super user*) 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 "Compliance Officer Role" section on page 1-29.

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. 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. 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:

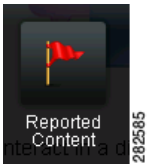
Procedure

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

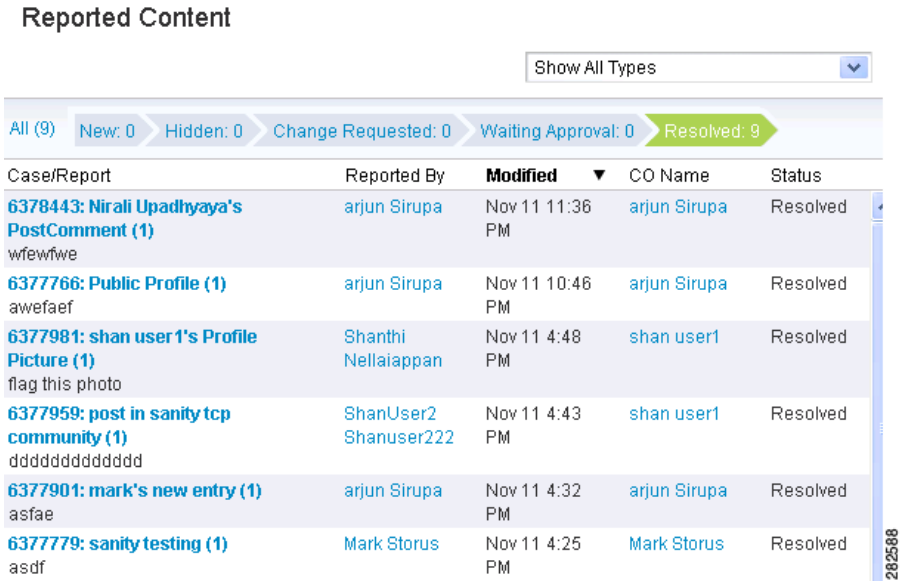
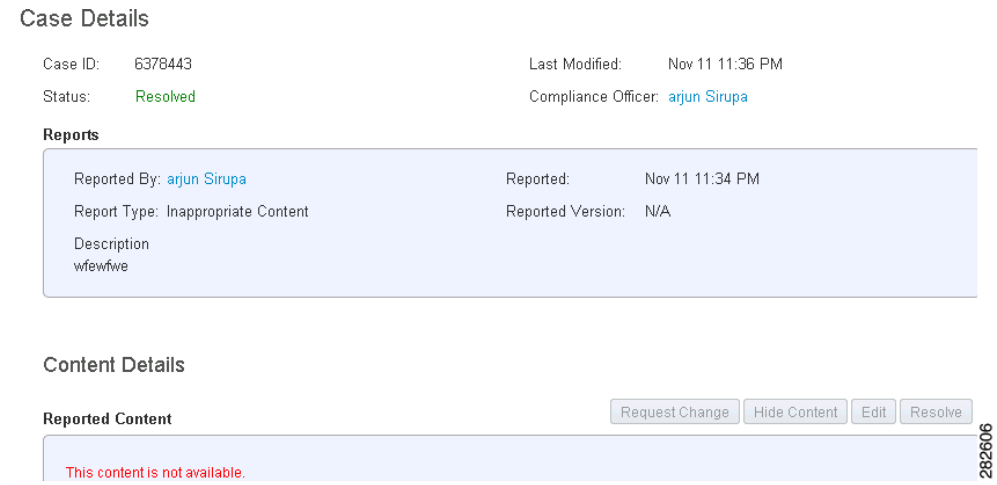


Figure 1-6 Example of a Case Details Window



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 "System: Configuration" 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 "System: Health" section on page 5-12
Statistics	Displays metrics of various Cisco WebEx Social components	See the "System: Stats" section on page 5-13
Logs	Logs collect a variety of information about the operation of Cisco WebEx Social.	See the "Log Properties" 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 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 JavasSript 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.

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

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

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

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:

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.

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:

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.

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	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. After making changes, click **Save**, or click **Cancel** to exit without saving your changes. The following sections describe the Edit options: • 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	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: • 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 After you make changes to permissions, click **Save**.
Manage Pages	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. For related information, see Appendix A, "Modifying Default Layouts and Creating a Custom Template." **Note** Users have the rights to manage their Home and My Profile pages. Community owners and administrators inherit these rights.
Deactivate	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.

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	Renter 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 Calender portlet on the Home page and WebEx integration.

Table 2-4 describes the items in these area. 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	Lets you edit most of the information that entered when the community was first created. 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.
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	Lets you delete this community. Make sure to notify member of a community when you delete it. ⚠ **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.
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	Lets an administrator or community owner assign or remove one or more of the following roles to members of the community. **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**. • 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. To assign a role to a users, follow these steps: 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**. To remove members from this role: 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	Takes you to a window that displays current members of the community and lets you add members. To invite a members to join a community, follow these steps: 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 *Type* 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**. 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.
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

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	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: • 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. After making changes, click **Save**, or click **Cancel** to exit without saving your changes.
Manage Pages	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. For more information about defining page templates for user groups, see the "Defining Page Templates for a User Group" section on page 2-17.
Assign Members	Takes you to a window that displays current members of the user group and lets you add members. 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. 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.
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

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	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: • 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	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. 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. 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.

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

To define portal permissions, 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.

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:

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.

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:

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.

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

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	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: • 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 After making changes, click **Save**, or click **Cancel** to exit without saving your changes.
Assign Members	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. 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. 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.
Delete	Allows you to delete any password policy that you added. However, you cannot delete the default policy. This option does not apply to the Default Password Policy.

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:

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:

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

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:

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 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 changed 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:

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 **Categories** tab.

Step 3 Click one of the categories to view or modify that category.

Step 4 Make any desired changed 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:

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 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 be 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_tex 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 node (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

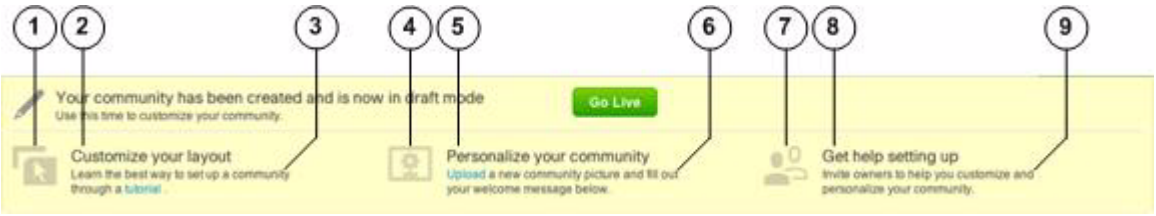
Note If you want to revert to the default settings, set this property to **false**.

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:

a. Click **Topology**

b. Click the **Disable** button for each App Server node.

c. Click the **Disable** button for the Cache node.

d. Click the **Enable** button for the Cache node.

e. 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:

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 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

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
Month-Date-Year or *Month-Year*	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
Month-Date-Year (Storage consumed in Bytes) or *Month-Year*	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	The home page of the portal. For example, if the home page URL is http://localhost:8080/web/guest/home then set this field to /web/guest/home. In general, the value in this field does not need to be changed.

Table 2-24 General Settings Options (continued)

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

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: • **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 *bind* (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	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. **Format of the URL** ldap://*host*:*portnumber* **Example** ldap://ds.cisco.com:389
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	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). You need an administrative credential because Cisco WebEx Social uses this ID to synchronize user accounts to and from the LDAP server. Example: The default Windows Domain Administrator is: cn=administrator,cn=users,dc=*your_domain*,dc=[com | net| | local].
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	Maps a Cisco WebEx Social user attribute to an LDAP attribute for matching user data. This filter must be enclosed within parentheses (( )). **Examples** (cn=@screen_name@) or (sAMAccountName=@screen_name@). 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.
Import Search Filter	LDAP object type used to filter the search. Depending on the LDAP server, there are different ways to identify the user. Default: (objectClass=Person) This default value is required for the Identity Store. If you want to search for only a subset of users or users that have different object classes, you can change this setting. This option applies only to bulk import of users. It is not used for authentication purposes.
User Mapping	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: • 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 The remaining User Mapping fields—Job Title, Group, and Phone—are optional. If Group is populated with the correct AD attribute (*memberOf*), 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.

Table 2-26 LDAP Authentication Options (continued)

Setting	Description
Test LDAP Users	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. Cisco WebEx Social displays a list of LDAP users who were successfully mapped. 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. It is a best practice to verify that mappings are correct.
Password Policy	
Use LDAP Password Policy	It is recommended that this box be unchecked (default). 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. **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).

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	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. 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.
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	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. When you select this option, these fields appear: • 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) After you configure a redundant server, you can click **Test Connection** to verify the connection to the server.

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:

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**.

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:

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 **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:

a. Check the Enable SSO Box.

b. 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:

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 **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 you 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	Check this box if you want users to be required to accept a terms of use notice before they can use Cisco WebEx Social. **Note** Users must accept the terms of use notice before they can use the Mobility apps." **Note** Default: Yes
Communities	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. Default: No communities are assigned.
Roles	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. Default: User, super user. (For definitions of various roles, see the "Roles" section on page 1-28.) **Note** You can remove any of the default roles by deleting the name of the role.
User Groups	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. **Example** 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. Default: No user groups are assigned by default.

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 *language-code_country-code*, where *language-code* is the ISO639 two-letter language code for the language that you want to use and *country-code* is an optional ISO3166 two-letter country code, which is used to specify a dialect for a language. Each language entry is separated by at comma.
Time Zone	Choose the time zone for Cisco WebEx Social.
Logo	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**. To delete a log, click **Delete**. Be sure that the logo image file fits the space in the Display Settings window.

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

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:

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 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

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:

Note If you are going to using 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

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:

a. Enter the following native sharepoint hook in the dl.hook.impl field:

com.liferay.documentlibrary.util.SP07Hook

b. Click **Save**.

Note If you are using Native SharePoint for the document repository and want to change back to a native file system, enter c**om.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:

a. 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
```

b. 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:

a. Click **Topology** in the left panel.

b. Click the **Disable** button next to each App Server role in the Server List area.

c. 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

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:

a. 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.

b. If you are testing with "Basic" authentication, in the Password field, enter the password of the account whose user name you just entered.

c. 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:" • 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. **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.
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:

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 **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:

a. In the Username Field, enter the user name of an administrative account on the server that you are using as an external document repository.

b. In the Password field, enter the password of the account whose user name you just entered.

c. 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:" • 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.

CHAPTER 3

Server Settings

The Server drawer contains selections that allow system administrators manage the portal server. From this drawer you can administer the server, install plugins, configure a variety of features, microblog to Twitter, and configure the end user license agreement.

To access the Server 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 Server 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 Server drawer:

Server Administration

The Server Administration window lets you perform tasks related to administering the portal server, as opposed to administering resources in the portal.

To access the Server Administration 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 **Server**, and then click **Server Administration** in the Server drawer.

The Server Administration window contains these tabs:

Resources

The Resources tab in the Server Administration window provides an informational area about memory as and buttons for executing actions.

Information Area

The Information area of the Resources tab shows these graphs, both of which relate to memory:

- Used Memory/Total Memory—Shows the percentage of resources being used out of the total available resources in the Java virtual machine (JVM).

  If the arrow points to the yellow portion of the graph, between 75 and 95 percent of the JVM resources are being used. If the arrow points to the red portion of the graph, between 95 and 100 percent of the JVM resources are being used.

- Used Memory/Maximum Memory—This graph shows the percentage of resources currently being used out of the maximum available resources in the JVM. This percentage is the same as the used memory/total memory if the total memory of the JVM and maximum memory allowed for Cisco WebEx Social are identical.

  If the arrow points to the yellow portion of the graph, between 75 and 95 percent of the JVM resources are being used. If the arrow points to the red portion of the graph, between 95 and 100 percent of the JVM resources are being used.

Actions

Table 3-1 describes the actions that you can perform from the Resources tab and explains when you might consider performing each action. To perform an actions, click its corresponding **Execute**. Each action is a server-wide action.

Note Actions in this Tab should be performed only during a system upgrade as instructed by the upgrade procedure or during a data loss recovery process as instructed by the recovery procedures or Cisco technical support.

Table 3-1 Resources Tab Actions

Action	Result and When to Execute
Run the garbage collector to free up memory.	Sends a request to the JVM to begin garbage collection task. This tool is used mostly to help diagnose performance issues. It immediately invokes the JVM garbage-collection routine, which automatically occurs at certain times during normal operation.
Clear content cached by this VM.	Sends a request to the JVM to clear a single VM cache. There are many caches in Cisco WebEx Social. This clears data cached only by this instance of Cisco WebEx Social. A distinction occurs in a clustered environment where there are separate caches for the local VM and a distributed cache that is shared among the nodes. This action would clear only the local VM cache.

Table 3-1 Resources Tab Actions (continued)

Action	Result and When to Execute
Clear content cached across the cluster.	Sends a request to the JVM to clear cached content across the entire cluster. A cluster consists of two or more Cisco WebEx Social servers operating as one portal to the end user. Clustering is done to increase the maximum number of concurrent users that the portal can support.
Clear the database cache.	Sends a request to the JVM to clear cached content across the Cisco WebEx Social database.
Reindex all search indexes.	Sends a request to regenerate all search indexes. If you are not using a Search node server, Cisco recommends that you perform this regeneration during non-peak times so as not to affect portal performance. Checking the Use Faster Multithreaded Approach box causes multiple threads to be spawned during this process, which makes this process faster. This box should always be checked in a production system.
Index JSON Store and Analytics Stores.	Sends a request to regenerate the JSON Store and Analytics Store Mongo database index files.
Re-index post for the past *n* days.	Sends a request to regenerate the post search indexes for the past *n* days.
Synchronize All Post Interaction	Copies Cisco WebEx Social Post metadata to the JSON Store.
Synchronize Recommendation.	Sends a request to synchronize Cisco WebEx Social data with data in the Analytics store. Can be used when you need synchronize Cisco WebEx Social data with data in the Analytics store, or when you need to repopulate data in the Analytics store.
Generate thread dump.	Typically done for performance testing, you can generate a thread dump to try to pinpoint any performance issues. This can gather data and tell you what the server is doing at that moment. It can be used to identify everything from performance issues to stability issues. This is not the only way to generate a thread dump, and thread dumps invoked from the console may be needed to resolve stability issues.

Log Properties

The Log properties tab allows you to specify logging levels for the App Server, and Worker nodes in your Cisco WebEx Social cluster.

This section contains the following topics:

Using the Log Properties Tab

To set logging for App Server and Worker nodes in your topology, perform the following steps:

Procedure

Step 1 Access the Server Administration 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 **Server**

d. Click **Server Administration** in the Server drawer.

Step 2 Select the **Log Properties** tab.

Step 3 From the **Selected Node** drop-down list, select the node in your Cisco WebEx Social topology for which you are setting log properties, then click **Go** to display the current settings for the selected node.

Step 4 Take the following actions to set the level individually for each logging group. (Most group names are descriptive. For a brief description of groups, click the **Category Help Page** link on the same page where you select the node for setting the log property.)

a. Select the desired logging level for each group from the corresponding Level drop-down list.Log levels are:

- Error—Logs error events that might allow the application to continue running. Also logs severe error events that can cause the program to abort. The Error setting is the default.
- Info—Logs all traces, which can be used to troubleshoot most issues. Setting this level of logging has minimal impact on performance. This setting also logs error messages described for the Error level.
- Debug—Turns on all levels of logging described for the levels previously listed, plus the Debug level, and logs all traces generated by the Error, Info, and Debug levels.
- Trace—Logs everything. Setting this level of logging has an impact on performance.

b. Click **Save**.

Step 5 If the role of the node you selected in Step 3 Worker, restart the Worker service from the Topology window in the Director.

Locating Log Files

Cisco WebEx Social creates log files that include information about the operation of the system. Log files fall into these categories:

- Centralized log files—Created and stored on the Director node in the /opt/logs/*yyyy_mm_dd* folder, where *yyyy_mm_dd* is the date that the logs are created. Includes log files that apply to individual nodes.
- Local log files—Created and stored on specific nodes. These files includes additional information that applies to the associated node.

For related information about log files, see *Cisco WebEx Social Troubleshooting Guide*.

File Uploads

The File Uploads tab in the Server Administration window lets you set file upload restrictions, such as maximum file sizes and permitted filename extensions, for Cisco WebEx Social in general and for the type of application.

Cisco WebEx Social rejects any file that a user attempts to upload that does not adhere to the configuration restrictions.

Mail

The Mail tab in the Server Administration window lets you configure connections to e-mail servers at your company. Then, if a user subscribes to any Cisco WebEx Social message board topics, the user also receives all posts to this message board in a Microsoft Outlook e-mail account. The user can also reply to posts from within Microsoft Outlook, and the reply appears in the applicable message board in Cisco WebEx Social.

Setting Up Communication with Pop and SMTP Servers

A Cisco WebEx Social account with user ID and password must be set up on both the incoming pop server and outgoing SMTP server for Cisco WebEx Social to communicate with each server and therefore enable the message board posts and users' Microsoft Outlook applications to communicate with each other.

Whatever Cisco WebEx Social user ID and passwords are created by you or the administrator(s) of those servers also must be configured in Cisco WebEx Social.

Configuring Mail Server Settings in Cisco WebEx Social

To configure mail server setting in Cisco WebEx Social, enter information in the Mail tab in the Server Administration window described in Table 3-2, then click **Save**.

Table 3-2 Mail Server Settings

Parameter	Description
Incoming Mail	
Incoming Pop Server	Fully qualified domain name or IP address of the pop server where incoming messages destined for the Cisco WebEx Social are temporarily stored.
Incoming Port	Port number used for the incoming pop server.
Use a Secure Network Connection	Consult with the administrator of the incoming pop server on whether to check this box.
User Name	User ID of the Cisco WebEx Social account that must first be created on the incoming pop server.
Password	Password of the Cisco WebEx Social account on the incoming pop server.

Table 3-2 Mail Server Settings (continued)

Parameter	Description
Outgoing Mail	
Outgoing SMTP server	Fully qualified domain name or IP address of the SMTP server where outgoing messages destined from Cisco WebEx Social are temporarily stored.
Outgoing port	Port number of the outgoing pop server.
Use a Secure Network Connection	Consult with the administrator of the outgoing SMTP server on whether to check this box.
User Name	User ID of the Cisco WebEx Social account that must first be created on the outgoing SMTP server. Only applicable when the **Use a Secure Network Connection** box is checked in this tab.
Password	Password of the Cisco WebEx Social account on the outgoing SMTP server. Only applicable when the **Use a Secure Network Connection** box is checked in this tab.
Advanced Properties	This field is not used.

System Properties

The System Properties tab in the Server Administration window shows a list of system properties for the JVM, and many Cisco WebEx Social system properties. This information can be used for debugging purposes or to check the configuration of the currently running portal.

Portal Properties

The Portal Properties tab in the Server Administration window shows a complete list of portal properties. You can view current values of all properties from this window without shutting down the portal or opening any properties files.

In general, these properties should not be changed. However, there are a few instances in this administration guide where you are instructed to change the value of some specific properties. In those cases, follow the given instructions to change only those properties. You change portal properties in the Portal window of the Director.

Partial Re-indexing

The Partial Reindexing tab in the Server Administration window lets you reindex only some data in the Cisco WebEx Social database. Reindexing data reconstructs the index so that users can successfully perform searches. The process is more efficient if you do not reindex the entire database.

Situations in which you may want to reindex data include:

- Cisco WebEx Social has been updated to point to a new database.
- The index for one of the categories shown in the Partial Reindexing tab is not correct.

To perform a partial reindex, follow these steps:

Procedure

Step 1 Access the Server Administration 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 **Server**

d. Click **Server Administration** in the Server drawer.

Step 2 Select the **Partial Re-indexing** tab.

Step 3 Use the checkboxes to select the items that you want to reindex.

Step 4 (Optional) Check the **Re-index portlets by date** box and enter a start date and through date for the reindexing.

Step 5 Check the **Use Faster Multithreaded Approach** box.

Checking this box causes multiple threads to be spawned during this process, which makes this process faster.

Step 6 Click **Execute**.

Metrics Initialization

The Metrics Initialization tab in the Server Administration window shows the status of the synchronization between the Oracle database and the Quad Analytics database in the Analytics Store. This synchronization occurs automatically after an upgrade. To avoid affecting system performance, perform metrics initialization only if instructed to do so by a Cisco support representative.

Plugins Installation

The Plugins Installation window drawer lets you see currently installed plugins and install new plugins.

Installed plugins are divided into the following categories. Each category has a tab in the Plugins Installation window.:

- 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.

Click a tab to view a list of currently installed portlets for that category. The list provides this information for each portlet.

- Active—Indicates if the portlet is in Active state. To change the state of a plugin, see the instructions in the "Plugin Settings" section on page 2-54.
- Roles—Cisco WebEx Social roles that can add the portlet to one of their pages. To change roles that can install specific portlets, see the instructions in the "Plugin Settings" section on page 2-54.
- Search Index—Applies to portlet plugins. Click the **Re-index** button to index the corresponding content. This action rebuilds search data for the portlet.

This sections contains the following topics:

Adding a Plugin

To install a new plugin, follow these steps:

Procedure

Step 1 Access the Plugins Installation 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 **Server**.

d. Click **Plugins Settings** in the Server drawer.

The Plugins Installation window appears with the Portlet Plugins tab selected

Step 2 Take either of these actions:

- To install a portlet plugin, select the **Portlet Plugins** tab and then click **Install More Portlets**.
- To install a layout template plugin, select the **Layout Template Plugins** tab and then click **Install More Layout Templates**.

The Plugin Installer Window appears. Use this window to browse and select from the Cisco WebEx Social repository of plugins or install your own plugin.

Situations in which you might need to install plugins manually include:

- Your server is firewalled without access to the Internet
- You are installing portlets that you have either purchased from a vendor, downloaded separately, or developed yourself
- For security reasons, you do not want to allow system administrators to install plugins from the Internet before they are evaluated

Step 3 Take one of these actions:

- To install a plugin from the Cisco WebEx Social repository of plugins:

  a. In the Browse Repository tab, use the Keywords, Tags, Repository, and Install Status search criteria to identify the desired plugin, then click **Search** to obtain a list of plugins in the Cisco WebEx Social repository that match the search criteria. The list contains the following information for each plugin:

     - Trusted
     - Tags
     - Installed Version
     - Available Version
     - Modified Date

  b. In the list, click the name of the plugin that you want to install.

     The install screen for that plugin appears and provides information about the plugin.

c. Click **Install.**

- To install your own plugin from your local machine, click **Upload File**, locate the desired plugin, then click **Install**.
- To install your own plugin from a URL, click **Download File**, enter the URL of the plugin, then click **Install**.

If you have the Cisco WebEx Social console open, you can view the plugin deployment as it occurs. When deployment finishes, you can add your new application plugin to a page in your portal. For more information about adding an application, see the "Applications" section on page 1-12.

Settings Tab for Plugins

The Settings tab in the Plugin Installer window lets you configure a variety of setting for plugins. The settings that are configured in this tab affect plugins that you subsequently install. (The Plugin Installer window appears when you install a plugin as described in the "Adding a Plugin" section on page 3-8.)

Table 3-3 describes the settings options for plugins.

Table 3-3 Settings Options Plugins

Parameter	Description
Enabled	This box must be checked to enable the plugin to install.
Deploy Directory	The directory to which plugin .war files are to be deployed. Default directory: /opt/cisco/quad/deploy
Destination Directory	Full path to your container's auto-deploy folder from the root of your file system.
Interval	Sets the frequency that you want Cisco WebEx Social to search the deploy directory for new plugins. Default: 10 seconds
Blacklist Threshold	The number of times Cisco WebEx Social attempts to deploy a .war file before blacklisting the file. Default attempts: 10
Unpack WAR	This box must be checked for Cisco WebEx Social to extract the contents of the .war file that contains the application.
Custom portlet.xml	Not used.
Tomcat Configuration Directory	Full path to the configuration directory on the tomcat server.
Tomcat Library Directory	Full path to the library directory on the tomcat server.
Trusted Plugin Repositories	A list of trusted URLs, entered one line at a time, of plugin repositories.
Untrusted Plugin Repositories	A list of untrusted URLs, entered one line at a time, of plugin repositories.
Plugin Notifications Enabled	If you check this box, you receive on-screen notifications when there is a new version of an installed plugin. Default: Yes

Table 3-3 Settings Options Plugins (continued)

Parameter	Description
Plugin Packages with Updates Ignored	If the Plugin Notifications Enabled field is enabled, you can list specific plugin packages here, one line at a time, for which you do not want to receive notifications about new versions.

Common Configurations

The Common Configurations window lets you configure settings for a variety of Cisco WebEx Social features. All settings except Notification Services involve integrations with other programs.

To access the Common Configurations 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 **Server**, and then click **Common Configurations** in the server drawer.

The Common Configurations window contains these tabs:

- Calendar Server, page 3-10
- Chat, page 3-17
- Notification Service, page 3-30
- Cisco Show And Share, page 3-32
- Voice Mail Server Configuration, page 3-33
- WebDialer Administration, page 3-36
- WebEx Site, page 3-39

Calendar Server

Configuring the Calendar server is necessary for the calendar applications to work. You can choose any of the following for configuring calendaring. Each one provides the same features:

- Using an Exchange WebDAV Server for Calendaring, page 3-11
- Using an Exchange Web Service Server for Calendaring, page 3-11
- Using IBM Lotus Domino for Calendaring, page 3-12

Cisco WebEx Social supports the use of Exchange WebDAV and Exchange Web Service simultaneously.

Users can override the default Calendar Server settings by following the steps in the "Overriding the Default Calendar Settings for a User" section on page 3-15.

Administrators can designate the Cisco WebEx Social node that is used to send community calendar event notifications as described in the "Designating the Node that is Used for Community Calendar Event Notifications" section on page 3-15.

Administrators can configure various properties that affect the calendering feature as described in the "Configuring Properties for Calendar Connections" section on page 3-16.

Using an Exchange WebDAV Server for Calendaring

To configure an Exchange WebDAV server for calendaring, perform the following steps. You can use an Exchange WebDav server with Microsoft Exchange 2003/2007.

Procedure

Step 1 Access the Common Configurations 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 **Server**

d. Click **Common Configurations** in the Server drawer.

Step 2 Select the **Calendar Server** tab.

Step 3 From the **Select Server Type** drop-down list, select **Exchange WebDAV**.

Step 4 Configure options as described in Table 3-4.

Step 5 Click **Save**.

Table 3-4 Exchange WebDAV Configuration Options

Parameter	Description
Exchange Server	Specifies the fully qualified URL of your company's exchange server.
USER_ID	Select the ID format. The user ID format makes up part of the URL in the Exchange Server field.
Use LDAP Directory Synchronization	If checked, a predefined (if any) exchange server is replaced with: https://*@msExchangeHostName@*.*@domain@*/exchange/USER_ID/calendar/ where the *@msExchangeHostName@* and *@domain@* fields are replaced with values that synced from the LDAP directory for each user.

Using an Exchange Web Service Server for Calendaring

To configure an Exchange Web Service server for calendaring, perform the following steps. You can use an Exchange Web Service server with Microsoft Exchange 2007/2010.

- Anonymous Authentication should always be enabled on the Exchange server, regardless of which other user authentications are used.
- Exchange 2010 integration supports Basic, Digest and Windows Authentication. Forms and Kerberos authentication are not supported.

Procedure

Step 1 Access the Common Configurations 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 **Server**

d. Click **Common Configurations** in the Server drawer.

Step 2 Select the **Calendar Server** tab.

Step 3 From the **Select Server Type** drop-down list, select **Exchange Web Service**.

Step 4 Configure options as described in Table 3-5.

Step 5 Click **Save**.

Table 3-5 Exchange Web Service Configuration Options

Parameter	Description
Exchange Web Service	URL of the server on which Exchange Web Service (EWS) runs. **Example** If the root domain is cisco.com, the Exchange mailbox server exmailbox.cisco.com, and EWS is installed on ews.cisco.com, the URL should be in the following format: https://ews.cisco.com/EWS/Exchange.asmx
Use Autodiscover Service	If checked, the Exchange Autodiscover service is used for fetching the user default exchange URL. When checked, the Exchange Web Service field name changes to Default Exchange Web Service. **Note** Autodiscovery requires a valid e-mail address to be associated with the Cisco WebEx Social user.

Using IBM Lotus Domino for Calendaring

To use IBM Lotus Domino for calendering in Cisco WebEx Social, perform the following general steps:

- Step 1: Configure Domino to Interoperate with Cisco WebEx Social, page 3-13
- Step 2: Configure Domino in Cisco WebEx Social, page 3-13
- Step 3: Configure the Connection Between Cisco WebEx Social and Lotus Domino, page 3-14

  This step is required only if you want to secure the connection between Cisco WebEx Social and Domino using SSL.

Note If Cisco WebEx Social is configured to use a proxy server for external connections, only the initial connection to the Domino server, which occurs during calendar settings configuration, goes through the proxy server. Subsequent connections go directly to the Domino server.

Step 1: Configure Domino to Interoperate with Cisco WebEx Social

Before you connect Cisco WebEx Social to Domino, you need to perform the following procedures on the Domino server:

- Enable the Domino IIOP (DIIOP) task
- Ensure that each Meeting Attendee has an Internet Address

Enable the Domino IIOP (DIIOP) task

Step 1 Open the Server document that you want to edit.

Step 2 Select **Ports > Internet Ports > DIIOP**.

Step 3 Select a **TCP/IP port number**.

Step 4 For **TCP/IP port status**, select **Enabled**.

Step 5 For **Name & password** select **Enabled**.

Be careful not to edit the SSL option with the same name.

Step 6 Save and close the Server document.

Step 7 Restart the DIIOP and HTTP tasks by executing these commands at the server console:

```
tell diiop quit
tell http restart
load diiop
```

Ensure that each Meeting Attendee has an Internet Address

For all meeting attendees to be properly displayed in Cisco WebEx Social, they need to have an Internet Address set up. See the Domino Administrator help for detailed instructions.

Step 2: Configure Domino in Cisco WebEx Social

To configure Domino in Cisco WebEx Social for calendaring, follow these steps:

Procedure

Step 1 Access the Common Configurations 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 **Server**

d. Click **Common Configurations** in the Server drawer.

Step 2 Select the **Calendar Server** tab.

Step 3 From the **Select Server Type** drop-down list, select **Domino**.

Step 4 Configure options as described in Table 3-6.

Step 5 Click **Save**.

Table 3-6 Domino Configuration Options

Parameter	Description
Domino Server	Specifies the fully qualified domain name (FQDN) or IP address of your company's Domino server. Remember to specify a port number if you have changed the default HTTP(S) port of your Domino server. **Example** dominoserver.organization.com:63148
Domino Domain	Specifies the fully qualified URL of the domain on which the Domino server runs. If this field is left empty, If this field is left empty, CISCO is used as the default Domino domain.
SSL enabled	Check this box to encrypt data between Cisco WebEx Social and the Domino server. This configuration requires additional steps as described in the "Step 3: Configure the Connection Between Cisco WebEx Social and Lotus Domino" section on page 3-14.

Step 3: Configure the Connection Between Cisco WebEx Social and Lotus Domino

If you want to enable SSL for the connection between Cisco WebEx Social and Lotus Domino, perform the following procedures.

Before you begin, make sure that the **SSL enabled** box is checked in the Calendar Server of the Server > Common Configurations window, as described in the "Step 2: Configure Domino in Cisco WebEx Social" procedure on page 3-13.

- Enable the SSL DIIOP Port on Lotus Domino
- Import the SSL Certificate from Lotus Domino

You may need to delete the previously imported certificate (to replace it), in which case follow the steps in Delete an Imported Certificate.

Enable the SSL DIIOP Port on Lotus Domino

Step 1 Open the Server document you want to edit.

Step 2 Select **Ports > Internet Ports > DIIOP**.

Step 3 Select an **SSL port number**.

Step 4 For **SSL port status**, select **Enabled**.

Step 5 For **Name & password** select **Enabled**. (Be careful not to edit the TCP/IP option with the same name, which should already be Enabled.)

Step 6 Save and close the Server document.

Step 7 Restart the DIIOP and HTTP tasks by executing these commands at the server console:

```
tell diiop quit
tell http restart
load diiop
```

Import the SSL Certificate from Lotus Domino

Step 1 Acquire the TrustedCerts.class from your Lotus Domino administrator and save it to your local hard drive.

Step 2 Having checked the SSL enabled box in the Cisco WebEx Social Control Panel, a Select Certificate link appears below it.

Step 3 Click the **Select Certificate** link.

A file selection dialog box appears.

Step 4 Select the TrustedCerts.class file and upload it.

Step 5 Click **Save**.

A label appears showing the date the certificate was installed.

Step 6 Repeat the procedure on each Cisco WebEx Social node.

Delete an Imported Certificate

You use the Security window in the Director to delete imported certificates. For detailed instructions, see the, see the "Trusted Certificates" section on page 5-25.

Overriding the Default Calendar Settings for a User

A user can use a server other than the default Calendar Server if the alternate server adheres to the same Calendar Server type.

Instruct users that they can update calendar settings from the My Account window, which they can access in either of these ways:

- By clicking the down-arrow to the right of the user name in the Global Navigation bar, selecting **Account Settings > My Account**, then clicking **Calendar and WebEx Login** from the list of links on the right pane.
- By clicking the **Modify Calendar Settings** link in the alert box in the Calendar area of the Home page. (This alert box appears only when Exchange or WebEx is not configured.)

Designating the Node that is Used for Community Calendar Event Notifications

A system administrator can designate a specific Cisco WebEx Social Node to used for community calendar event notifications. By default, all nodes send such notifications.

To designate the node to be used for community calendar event notifications, follow these steps:

Procedure

Step 1 Sign in to Director.

Step 2 Select **Portal** under Application.

Step 3 In the Search field in the Advanced Portal Properties area, enter **calendar.event.notifier.node**.

This property appears in the property list. The default value is empty, which means that all nodes send community calendar event notifications.

Step 4 Enter the host name of the node to be used to send community calendar event notifications.

For example, enter esc-webexsocial

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

Configuring Properties for Calendar Connections

Table 3-7 describes the Cisco WebEx Social properties that control various items for calender connections. To avoid affecting system performance, configure these properties only if instructed to do so by a Cisco support representative.

To change the value of a property, in the Director, click **Portal**, and in the Advanced Portal Properties area, locate the property and update its value. Then click **Save** in the Advanced Portal Properties area. (For related information, see the "Advanced Portal Properties" section on page 5-20.)

The following guidelines apply to these parameters:

- The calendar.cache.ui.request.timeout parameter should not be set to a smaller value than the calendar.cache.meetings.timeout parameter.
- The calendar.cache.ui.request.timeout parameter and the calendar.cache.meetings.timeout parameter should each specify longer periods than the periods that the webex.adapter.socket.timeout, the exchange.protocol.connection.timeout, and the exchange.protocol.socket.timeout parameter specify.

Table 3-7 Properties for Calendering

Property	Description	Default
webex.adapter.connection.timeout	Number of seconds that Cisco WebEx Social waits for a response from a WebEx server to a request to that server before an error is signaled.	60
webex.adapter.socket.timeout	Number of seconds that Cisco WebEx Social waits for a response from a WebEx server after a connection to that WebEx server is established. The connection times out after this period if no results are returned.	120
exchange.protocol.connection.timeout	Number of seconds that Cisco WebEx Social waits for a response from an Exchange server to a request to that server before an error is signaled.	30
exchange.protocol.socket.timeout	Number of seconds that Cisco WebEx Social waits for a response from an Exchange server after a connection to that Exchange server is established. The connection times out after this period if no results are returned.	100
calendar.cache.meetings.timeout	Number of milliseconds after which results from a calendar server are deleted from the Cisco WebEx Social internal memory cache. When a result is deleted, Cisco WebEx Social sends a new request for that information to the calendar server.	900000 (15 minutes)

Table 3-7 Properties for Calendering (continued)

Property	Description	Default
calendar.cache.ui.request.timeout	How often, in milliseconds, a Cisco WebEx Social client browser requests data for meetings from the Cisco WebEx Social server.	900000 (15 minutes)

Chat

Configuring Chat is necessary for Cisco WebEx Social users to use the chat and presence features.

Presence allows a Cisco WebEx Social users to set personal availability states (Available, Away, or Do Not Disturb) from the drop-down menu that appears near their name in their Cisco WebEx Social window. When a user sets availability, this state is visible to all Cisco WebEx Social users.

You can configure Cisco Unified Presence (CUP), WebEx IM, Microsoft Office Communications Server (OCS), or IBM Lotus Sametime for chat and presence, as described in the following sections.

- Using CUP for Chat and Presence, page 3-17
- Using WebEx IM for Chat and Presence, page 3-19
- Using Microsoft OCS for Chat and Presence, page 3-23
- Using IBM Lotus Sametime for Chat and Presence, page 3-27

After you configure options for chat and presence, instruct your users to configure their chat passwords as described in the "User Configuration Setting for Chat" section on page 3-29) if any of these situations exist:

- WebEx IM is selected and the Enable SSO field is disabled
- Microsoft OCS is selected and the Use Chat Password field is enabled
- IBM Sametime is selected
- Cisco Unified Presence (CUP) is selected

Users can disable sound notifications for incoming chats by following the steps in the "Disabling Sound for Incoming Chats" section on page 3-29.

Notes About Behavior

- If users set their presence state to Offline, active chats remain open but the text input box is disabled and the click-to-chat icon becomes inactive
- Sticky presence causes the presence of a user to be set to its latest state when the user signs in to Cisco WebEx Social
- The presence state of a user is consistent across all Cisco WebEx Social sessions that the user has open

Using CUP for Chat and Presence

To use CUP for chat and presence, consult with your CUP server administrator to determine which CUP server to connect to. You also should inform the CUP server administrator that Cisco WebEx Social needs to connect to an administrative account that has the role *Standard AXL API Access*.

CUP is configured in Cisco Unified Presence Server Administration and in Cisco Unified Communications Manager Administration. For detailed information, see the documentation for these products.

Note

- The CUP server that Cisco WebEx Social connects to must be configured with its fully qualified domain name under **System > Cluster Topology > Settings > Cluster-Wide Topology** in the Cisco Unified Presence Administration configuration interface. This domain name must contain lower case characters only. Be certain to inform the CUP administrator about these requirements.
- If you are using CUPS 8.5 or later, the CUP XCP Text Conference Manager service or the CUP Directory service must be running on the CUP server

To configure Cisco WebEx Social to use CUP for chat and presence, follow these steps:

Procedure

Step 1 Access the Common Configurations 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 **Server**

d. Click **Common Configurations** in the Server drawer.

Step 2 Select the **Chat** tab.

Step 3 From the **Chat and Presence Server** drop-down list, select **Cisco Unified Presence (CUP)**.

Step 4 Configure options as described in Table 3-8.

Step 5 Click **Save**.

Step 6 Sign in to the Director, go to the Integration window, and take these actions:

a. In the Chat Proxy URL field, enter the BOSH binding URL in this format, where *CUPS-Server* is the FQDN of the CUPS server and port is the port to use (the default port is 7335):.

[http | https]://*CUPS-Server*:*port*/httpbinding

b. Select **default** from the Server Type drop-down list.

Table 3-8 CUP Configuration Options

Parameter	Description
Maximum Number of Presence Subscriptions	Sets the maximum number of user presences to which Cisco WebEx Social can temporarily subscribe on a single page. Cisco WebEx Social uses these subscriptions to obtain the presence status of each Cisco WebEx Social user. Default: 100

Table 3-8 CUP Configuration Options (continued)

Parameter	Description
Resource ID Prefix	Allows the CUP server to determine which resource is being used to communicate with CUP. Each browser instance of Cisco WebEx Social uses this prefix concatenated with a large random number to generate a unique ID to represent itself. Default: quad.
Session Priority	This value is used by the CUP server to compose the presence of a user and to determine which resource receives chat messages. Valid values: –128 to 127 Default: 0
Primary Host	Fully qualified host name or IP address of the primary CUP server to which Cisco WebEx Social is to connect. This CUP server must already have been configured in the CUP Administration configuration interface.
Port Number	Port number of the AXL listener on the CUP server. Default: 8443
User Name	User ID of the administrator of the CUP server to which Cisco WebEx Social is to connect. This account must have AXL privileges on the CUP server. You need to obtain this information from the CUP server administrator, who also has the option of setting up a separate administrative user for Cisco WebEx Social on the CUP server.
Password	Password for the ID you just set in the User Name field.

Using WebEx IM for Chat and Presence

To use WebEx IM for chat and presence, perform the following general steps:

- Step 1: Configure WebEx IM in Cisco WebEx Social, page 3-20
- Step 2: Establish a Trust Relationship Between Cisco WebEx Social and the WebEx Connect Server, page 3-22

After you perform these steps, go to the Integration window in the Director and take these actions:

1. In the Chat Proxy URL field, enter this BOSH binding URL, where *X* is the value 1, 2, or 3 (contact the WebEx administrator for the appropriate value):

   https://im*X*.ciscowebex.com/isj*X*

2. Select **default** from the Server Type drop-down list.

Step 1: Configure WebEx IM in Cisco WebEx Social

To configure WebEx IM in Cisco WebEx Social for chat and presence, follow these steps:

Procedure

Step 1 Access the Common Configurations 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 **Server**

d. Click **Common Configurations** in the Server drawer.

Step 2 Select the **Chat** tab.

Step 3 From the **Chat and Presence Server** drop-down list, select **WebEx IM**.

Step 4 Configure options as described in Table 3-9.

Step 5 Click **Save**.

Table 3-9 WebEx IM Configuration Options

Parameter	Description
Chat & Presence Configuration	
Maximum Number of Presence Subscriptions	Sets the maximum number of users presences to which Cisco WebEx Social can temporarily subscribe on a single page. Cisco WebEx Social uses these subscriptions to obtain the presence status of each Cisco WebEx Social user. Default: 100
Resource ID Prefix	Allows the WebEx server to determine which resource is being used to communicate with WebEx. Each browser instance of Cisco WebEx Social uses the prefix *quad-* concatenated with a large random number to generate a unique ID to represent itself.
Enabled Features	Designates which features that related to presence are enabled. Options are: • **Presence + Browser Chat**—Default selection. When selected, users can see presence and change their user status, and chat messages appear in the browsers. • **Presence Only**—When selected, user status is shown but cannot be changed. Chat requires the use of a desktop chat client. In-browser chat is disabled. When selected, the Show Click-to-Chat Icon box appears. This box is selected by default. If deselected, the click-to-chat icon does not appear anywhere in the Cisco WebEx Social UI (including in the hover card, profile, search results, People page, and reporting structure).

Table 3-9 WebEx IM Configuration Options (continued)

Parameter	Description
Session Priority	Appears only if **Presence + Browser Chat** is selected for the Enabled Features parameter. Also known as *presence priority*, this value determines the priority of the Cisco WebEx Social chat session compared to chat sessions for the same user on non-Cisco WebEx Social clients. Cisco WebEx Social sends the session priority to the WebEx server, which uses the priority number to determine which session has higher priority. Higher-number priorities take precedence over lower numbers. Valid values: —128 to 127 Default: 0
WebEx IM Configuration	
JID Type	Jabber ID Type. Select **Screenname@Domain** or **Email** from the drop-down list, depending on how your company forms its Jabber ID. If you select Screenname@Domain, you also need to enter the fully qualified domain name of the WebEx server in the Domain field.
Domain	Appears if you select **Screenname@Domain** or **Email** from the JID Type drop-down list. Fully qualified domain name of the WebEx server you are using. Cisco WebEx Social uses the user's screen name concatenated with the Jabber Domain to form the user's Jabber ID (JID), which is then used to connect the user to the chat server. Example: cisco.com
Enable SSO	If you check this box, Cisco WebEx Social users do not need to enter their WebEx Connect passwords because Cisco WebEx Social acts as a trusted party to WebEx IM. Therefore, when a user gets authenticated by Cisco WebEx Social, Cisco WebEx Social notifies the WebEx IM server about that user. If you check this box to enable this field, the WebEx SSO IM Configuration fields appear. If this field is disabled, users must perform the steps described in the "User Configuration Setting for Chat" section on page 3-29.
WebEx IM Configuration **Note** These fields appear only if you check the Enable SSO box.	
Partner Issuer (IDP ID)	Identifier of the identity provider, this is used to make an SAML call for SSO authentication. The Cisco WebEx Social administrator must obtain this value from the WebEx Connect administrator. The WebEx connect administrator must set up a partner delegate organization for a Cisco WebEx Social instance.

Table 3-9 WebEx IM Configuration Options (continued)

Parameter	Description
WebEx SAML Issuer (SP ID)	Identifier of the service provider and used to make an SAML call for SSO authentication. The Cisco WebEx Social administrator must obtain this value from the WebEx Connect administrator.
Base SP Login URL	Used to make an SAML call for SSO authentication. The Cisco WebEx Social administrator must obtain this value from the WebEx Connect administrator.
Org	Used to make an SAML call for SSO authentication. The Cisco WebEx Social administrator must obtain this value from the WebEx Connect administrator.
Partner Org	Used to make an SAML call for SSO authentication. The Cisco WebEx Social administrator must obtain this value from the WebEx Connect administrator.
Name ID Type	Select one of the following options, which will be used to identify and authenticate users on the WebEx IM server. • **Username (JID)** • **E-mail** • **SSO ID**

Step 2: Establish a Trust Relationship Between Cisco WebEx Social and the WebEx Connect Server

If you are using SSO in your deployment, follow these steps to establish a trust relationship between Cisco WebEx Social and the WebEx Connect server:

Procedure

Step 1 Use an SSH client to access any App Server node, log in as the admin user, and enter this command:

sudo cd /usr/java/default/bin

Step 2 Using keytool (a key management utility that ships with JRE), enter the following command to create a certificate and key:

sudo ./keytool -genkey -keyalg RSA -alias *alias_name* **-keypass** *keystore_password* **-keystore /opt/system/java/im_keystore.jks -storepass** *store_password* **-dname "cn=***id***"**

where:

- *alias_name* is the alias for the new certificate
- *keystore_password* is the password for keystore
- *store_password* is the password for the truststore
- *id* is the WebEx Connect site/partner identifier

This command generates a new file called im_keystore.jks in the at /opt/system/java folder.

Step 3 Copy the generated file to your local PC.

Step 4 Sign in to the Director and take these actions:

a. Click **Security** under Application.

b. In the Keystore File field in the WebEx IM SSO area, click the **Choose File** button, then navigate to and select the file that you generated in Step 3.

c. In the Key Password field in the WebEx IM SSO area, enter the *key_password* that you used in Step 2.

d. In the Keystore Password field in the WebEx IM SSO area, enter the keystore_password that you used in Step 2.

e. Click **Save** in the WebEx IM SSO area.

The quad service on the App Servers restarts.

Step 5 Export the certificate by taking these actions on the App Server node that you used in Step 1:

a. Enter this command:

sudo cd /usr/java/default/bin

b. Enter the following command to export the certificate, using the alias and keystore that you used to generate the certificate:

sudo ./keytool -export -alias *alias_name* -keystore /opt/system/java/im_keystore.jks -file exported-der.crt

c. Convert the certificate to PEM format (required by WebEx) by running the following command:

sudo openssl x509 -out exported-pem.crt -outform pem -in exported-der.crt -inform der

d. Give the exported-pem.crt file to the WebEx site administrator, and provide all information that you used to generate the certificate.

Using Microsoft OCS for Chat and Presence

To use Microsoft OCS for chat and presence, make sure that these requirements are met:

- Both Cisco WebEx Social and OCS must be synchronized to the same Active Directory, and an LDAP directory synchronization must have completed (see the "LDAP Directory Sync" section on page 2-44).
- Cisco WebEx Social uses Communicator Web Access (CWA) to communicate with the OCS server, so CWA must be installed as described later in this section.
- You must be able to sign in successfully using the browser-based Thin client as described in *CWA Getting Started Guide*, which is available from the Microsoft website.

  A successful sign in confirms that CWA is provisioned and functioning properly before you configure Cisco WebEx Social to use CWA.

To use Microsoft OCS for chat and presence, perform the following general steps:

- Step1: Prepare OCS, page 3-25
- Step2: Configure OCS in Cisco WebEx Social, page 3-27

After you perform these steps, go to the Integration window in the Directory and take these actions:

1. In the Chat Proxy URL field, enter URL of the CWC client.
2. Select **default** from the Server Type drop-down list.

Behavior of Microsoft OCS IM with Multiple Clients Including Cisco WebEx Social

Table 3-10 describes how you can expect Microsfoft OCS IM to work when multiple clients, including Cisco WebEx Social, are enabled for chat. In this table:

- *Thin-c* is the Microsoft CWA Browser Client
- *Thick-c* is the Microsoft Office Communicator Desktop Client

Table 3-10 Microsoft OCS M Behavior Scenarios For Multiple Clients Including Cisco WebEx Social

Users In The Chat	Instance Getting Initial Chat	Can An Instance Steal Chat Session By Sending Chat to Initiator?	Can An Instance Steal Chat Session By Changing Presence State?	Can An Instance Steal Chat Session By Refreshing Connection?	Which Instance Gets Incoming Message When Both Users Close/Restart Chat?
User 1: Cisco WebEx Social, Cisco WebEx Social. User 2: Thick-c (Initiator)	Last to sign in.	Yes, but Thick-c opens another session (which is independent of the first session).	No, unless the other chat instances go to the offline state.	No, unless an IM is sent from the new session. The new chat would then be sent to the refreshed connection if the other instance has been closed.	Last to sign in.
User 1: Cisco WebEx Social, Cisco WebEx Social. User 2: Thin-c (Initiator)	Last to sign in.	Yes, but Thin-c opens another session (which is independent of the first session).	No, unless the other chat instances go to the offline state.	No, unless an IM is sent from the new session. The new chat would then be sent to the refreshed connection if the other instance has been closed.	Last to sign in.
User 1: Cisco WebEx Social, Cisco WebEx Social. User 2: Cisco WebEx Social (Initiator)	Last to sign in.	Yes.	No, unless the other chat instances go to the offline state.	No, unless an IM is sent from the new session. The new chat would then be sent to the refreshed connection if the other instance has been closed.	Last to sign in.
User 1: Cisco WebEx Social, Thick-c. User 2: Cisco WebEx Social (initiator)	IM first goes to Thick-c. If Thick-c does not reply, the IM then gets sent to Cisco WebEx Social.	Yes.	No, unless the other chat instances go to the offline state.	No, unless an IM is sent from the new session.	IM first goes to Thick-c. If Thick-c does not reply, the IM then gets sent to Cisco WebEx Social.
User 1: Cisco WebEx Social, Thin-c. User 2: Cisco WebEx Social (initiator	IM goes to Cisco WebEx Social only.	Yes.	No, unless the other chat instances go to the offline state.	No, unless an IM is sent from the new session.	IM goes to Cisco WebEx Social only.

Table 3-10 Microsoft OCS M Behavior Scenarios For Multiple Clients Including Cisco WebEx Social (continued)

Users In The Chat	Instance Getting Initial Chat	Can An Instance Steal Chat Session By Sending Chat to Initiator?	Can An Instance Steal Chat Session By Changing Presence State?	Can An Instance Steal Chat Session By Refreshing Connection?	Which Instance Gets Incoming Message When Both Users Close/Restart Chat?
User 1: Cisco WebEx Social, Thick-c. User 2: Thick-c (initiator)	IM first goes to Thick-c. If Thick-c does not reply, the IM then gets sent to Cisco WebEx Social.	Yes, but Thick-c opens another session.	No, unless the other chat instances go to the offline state.	No, unless an IM is sent from the new session.	IM first goes to Thick-c. If Thick-c does not reply, the IM then gets sent to Cisco WebEx Social.
User 1: Cisco WebEx Social, Thin-c. User 2: Thick-c (initiator)	IM first goes to Thin-c. If Thin-c does not reply, the IM then gets sent to Cisco WebEx Social.	Yes, but Thick-c opens another session.	No, unless the other chat instances go to the offline state.	No, unless an IM is sent from the new session.	IM first goes to Thin-c. If Thin-c does not reply, the IM then gets sent to Cisco WebEx Social.
User 1: Cisco WebEx Social, Thin-c. User 2: Thin-c (initiator)	IM first goes to Thin-c. If Thin-c does not reply, the IM then gets sent to Cisco WebEx Social.	Yes, but Thin-c opens another session.	No, unless the other chat instances go to the offline state.	No, unless an IM is sent from the new session.	IM first goes to Thin-c. If Thin-c does not reply, the IM then gets sent to Cisco WebEx Social.

In summary:

- If an IM is sent from a thick or thin client to a user who is signed in to both Cisco WebEx Social and a thick or thin client, the IM first gets sent to the thick or thin client. If there is no response, the IM then gets sent to Cisco WebEx Social.
- If a user is signed in to multiple Cisco WebEx Social instances (but not to a thick or thin client), the latest signed-in Cisco WebEx Social session receives the IM.
- A Cisco WebEx Social, thick, or thin client continues to receive chat messages regardless of any presence state except DND).
- The behavior shown in Table 3-10 is identical regardless of whether the Cisco WebEx Social browser is launched on one machine or two machines.

Step1: Prepare OCS

To prepare Microsoft OCS for chat and presence use with Cisco WebEx Social, take the actions for your scenario as described in Table 3-11

Table 3-11 Preparing Microsoft OCS

Scenario	Actions to Take
You are using OCS 2007 and already have CWA installed.	No action required.
You are using OCS 2007 but have not yet installed CWA.	Install CWA. Refer to your CWA documentation for instructions.
You are using OCS 2007R2 and already have the R2 version of CWA installed.	Take either of these actions: • Uninstall the R2 version of CWA, then perform the steps that are listed in the next row • Add a new OCS server that does not have R2 installed, then join that server to the OCS cluster
You are using OCS 2007R2 but have not yet installed CWA	These actions are based on recommendations from Microsoft. 1. On the Windows Server 2003-based computer that is to host CWA, install the installation files for OCS 2007. 2. From a command prompt, browse to the OCS 2007 Installation folder. 3. From the command prompt, run the following command: 4. **%installation folder%\i386\setup\LcsCmd /Forest /action:ForestPrep** 5. Make sure that the ForestPrep command completes successfully. 6. Resume the CWA 2007 activation process. **Note** It is possible to encounter the error message: "Could not load all ISAPI filters for site/service. Therefore startup aborted." (You can check for this error by navigating to **Administrative Tools > Computer Management > IIS Manager**.) For a workaround see the section "ASP.NET 2.0, 32-bit version" in the article *How to switch between the 32-bit versions of ASP.NET and the 64-bit version of ASP.net 2.0 on a 64-bit version of Windows*, which is available on the Microsoft support website. For the OCS thin client, if the conversation window remains blank when you use CWA to start a new instant messaging conversation, follow the workaround in the article *Description of the update package for Communications Server 2007 and for Communicator Web Access: November 30*, which is available on the Microsoft support website.

Step2: Configure OCS in Cisco WebEx Social

To configure OCS in Cisco WebEx Social for chat and presence, follow these steps:

Procedure

Step 1 Access the Common Configurations 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 **Server**

d. Click **Common Configurations** in the Server drawer.

Step 2 Select the **Chat** tab.

Step 3 From the **Chat and Presence Server** drop-down list, select **Microsoft OCS**.

Step 4 Configure options as described in Table 3-12.

Step 5 Click **Save**.

Table 3-12 Microsoft OCS Configuration Options

Parameter	Description
Domain	Domain of the Active Directory.
Use Chat Password	Check the box if you want Cisco WebEx Social to obtain user passwords from the profile of each user. If you check the box to enable this field, users must perform the steps described in the "User Configuration Setting for Chat" section on page 3-29. If you do not check this box, no user configuration is required. In this case, Cisco WebEx Social obtains user passwords from the user session as long as a user's Cisco WebEx Social credentials and OCS credentials are the same.

Using IBM Lotus Sametime for Chat and Presence

Cisco WebEx Social uses the Sametime Proxy API to provide chat and presence to Sametime users in Cisco WebEx Social.

To use IBM Lotus Sametime for chat and presence, perform the following general steps:

This section contains the following topics:

After you perform these steps, go to the Integration window in the Directory and take these actions:

a. In the Chat Proxy URL field, enter the URL of the Sametime proxy server in this format, where *SameTime_proxy_server* is the IP address or FQDN of the server and *port* is the port to use.

[http | https]:/*SameTime_proxy_server*:*port*

7. Select **sametime** from the Server Type drop-down list.

Step 1: Configure Sametime in Cisco WebEx Social

To configure Sametime in Cisco WebEx Social for chat and presence, follow these steps:

Procedure

Step 1 Access the Common Configurations 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 **Server**

d. Click **Common Configurations** in the Server drawer.

Step 2 Select the **Chat** tab.

Step 3 From the **Chat and Presence Server** drop-down list, select **IBM Sametime**.

Step 4 Configure options as described in Table 3-13.

Step 5 Click **Save**.

Table 3-13 IBM Sametime Configuration Options

Parameter	Description
Domino LDAP Sync	Enables the synchronization for the chat ID (distinguished name) to be performed from the Domino server. When you check this box, the following parameters appear, which must be configured: • URL—URL of the Domino LDAP server. Cisco WebEx Social connects to this URL to read the chat ID (the distinguishedName). • BaseDN— BaseDN of the organization, which is the DN of the container to which the Domino users directly belong. The chat ID of these is read. • User Name—User name of the user who has sufficient privileges to read the content of the container to which the Domino users directly belong. In most cases this user is the LDAP administrator. • Password—Password of the user who has sufficient privileges to read the content of the container to which the Domino users directly belong. In most cases this user is the LDAP administrator. After you configure these parameters, you can click the **Test Domino Connection** button to ensure that the connection works properly.

Step 2: Configure Client Priority in Sametime Community Server

The Sametime Community Server offers the VPS_PREFERRED_LOGIN_TYPES setting to specify which client type should receive the instant messaging session in case the same user has logged in using several different clients.

To put Cisco WebEx Social on the top of the priority list, follow these steps:

Procedure

Step 1 On the machine on which the Sametime Community Server is installed, go to the installation directory (usually %SystemRoot%\Program Files\IBM\Lotus\Domino).

Step 2 Open **sametime.ini** for editing.

Step 3 In the [Config] section, find the VPS_PREFERRED_LOGIN_TYPES option.

Step 4 Ensure the **14A3** login type is moved to the very beginning of the list. 14A3 is the Proxy 8.5.1 SDK clients ID.

The result should look similar to the following:

```
VPS_PREFERRED_LOGIN_TYPES=14A3,130C,130B,130A,1308,1306,1304,1436,1435,1434,1433,1432,1431
,1430,14A2,14A1,14A0
```

Step 5 Save the sametime.ini file.

Step 6 Restart Sametime for the changes to take effect.

User Configuration Setting for Chat

When you implement chat for Cisco WebEx Social, inform users which server is being used for chat/presence, and provide a link to how users can reset their passwords if they do not know how to connect to that server.

In addition, tell users to perform the following steps:

Procedure

Step 1 Access your account settings:

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. Select **My Account** in the left pane of the window.

Step 2 On the right pane, click **Chat Password** under Miscellaneous.

Step 3 Enter and re-enter the password that you use to connect to the chat/presence server.

Step 4 Click **Save**.

Disabling Sound for Incoming Chats

A user can disable sound for incoming chats by following these steps:

Procedure

Step 1 When you are in a chat session, click the gear icon in the Chat window.

The Chat Settings window opens.

Step 2 Uncheck the **Enable sound for incoming chats** box.

Step 3 Click **Save**.

Notification Service

The notification service enables instant updates to your watchlist, activities, chat, and notifications.

This section includes these topics:

- Synchronizing Notification Service, page 3-30
- Synchronization Buttons, page 3-31
- Adding a User to Notifier, page 3-31

Synchronizing Notification Service

This section explains how to synchronize Cisco WebEx Social data with the Notifier. This procedure should be performed only if you are instructed to do so by a Cisco support representative

To synchronize Cisco WebEx Social data with the Notifier, perform the following steps.

Before You Begin

- In the Director, configure the Notifier. See the "Notifier" section on page 5-4
- In the Director, add a Notifier node. See the "System: Topology" section on page 5-8

Procedure

Step 1 Access the Common Configurations 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 **Server**

d. Click **Common Configurations** in the Server drawer.

Step 2 Select t the **Notification Service** tab.

Step 3 Click **Validate** and ensure that a connection to the notifications server can be established.

Step 4 Click **Start Synchronization**.

Alert notifications that synchronization has started and completed are sent to all administrators.

Synchronization Buttons

The Notification Service tab includes the following buttons:

- **Validate**—Ensures that Cisco WebEx Social can connect to the Notifier node.
- **Start Synchronization**—Starts the process that synchronizes Cisco WebEx Social data with the Notifier.

  Only one synchronization operation can be started at a time regardless of the number of Cisco WebEx Social nodes in the cluster. When synchronization is running, all XMPP dynamic notifications are suspended.

  Alert notifications that synchronization has started and completed are sent to all administrators.
- **Resume Synchronization**—If you receive a synchronization-error notification, you can click this button to resume the synchronization where it was stopped
- **Reset Sync Flag**—If you receive a synchronization-error notification, you can restart the synchronization from the beginning by clicking this button and then clicking **Start Synchronization**

Adding a User to Notifier

If you manually created a user in Cisco WebEx Social who is not listed in LDAP, follow the steps in this section to create the same user on the notifications server.

Procedure

Step 1 Use an SSH client to access the Notifier node, log in as the admin user, and enter these commands:

sudo iptables -A INPUT -p tcp -m tcp --dport 9095 -j ACCEPT

sudo iptables -A INPUT -p tcp -m tcp --dport 9096 -j ACCEPT

Step 2 Sign in to the Notifier Administration console using the configured port (such as 9095), and use the following credentials:

- Username—**admin**
- Password—Unified password that was configured in the Director

Step 3 Click the **Users/Groups** tab.

Step 4 Click **Create New User**.

The Create User window opens.

Step 5 Enter the appropriate information in this window, using the same values for this user that are in Cisco WebEx Social.

Note For the Username field, enter the Cisco WebEx Social screen name for this user. The password should match the one used for Cisco WebEx Social.

Step 6 Click **Create User**.

Step 7 Use an SSH client to access the Notifier node, log in as an administrator, and enter this command:

sudo service firewall restart

Cisco Show And Share

Configuring Cisco Show and Share is necessary for users to post and share video files in Cisco WebEx Social. To configure Cisco WebEx Social with your Cisco Show and Share server, follow the steps in these sections:

- Configuration Required in the Show and Share Window, page 3-32
- Configuration Required in the Director, page 3-32

Note You can contact your Cisco representative about having a patch installed that allows only the author of a posted video to view their video on the Show and Share server. The author can use Cisco WebEx Social to share the video with Cisco WebEx Social users.

Configuration Required in the Show and Share Window

To configure Show and Share in Cisco WebEx Social, follow these steps:

Procedure

Step 1 Access the Common Configurations 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 **Server**

d. Click **Common Configurations** in the Server drawer.

Step 2 Select the **Show and Share** tab.

The Show and Share Configuration window opens.

Step 3 In the Server Host Name field, enter the fully qualified domain name of your Show and Share Server. For example: sns-server.cisco.com

Step 4 In the HTTP Port field, enter 80.

Step 5 In the HTTPS Port field, enter 443.

Step 6 In the Administrator User Name field, enter the user ID of the Show and Share server administrator.

Step 7 In the Administrator Password field, enter the password of the Show and Share server administrator.

Step 8 Click **Save**.

Configuration Required in the Director

After you perform the procedure that the "Configuration Required in the Show and Share Window" section on page 3-32 describes, 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**.

Voice Mail Server Configuration

The Voice Messages application allows users to use their voice messaging system from within their Cisco WebEx Social pages. Users can retrieve voice messages, send replies, send new messages, forward messages, and delete voice messages from within this application.

The following sections explain how to configure messaging mail servers so that Cisco WebEx Social users can use the voice mail application:

- Adding the Administrative User in Cisco Unity Connection, page 3-33
- Configuring Voice Mail Server in Cisco WebEx Social, page 3-34
- Generating the SSL Tomcat Certificate, page 3-35
- Configuration Performed By the Cisco WebEx Social End User From the Voice Messages Application, page 3-36

Adding the Administrative User in Cisco Unity Connection

This section describes how to add the Cisco Unity Connection application user that Cisco WebEx Social uses to perform all voice messaging tasks in Cisco Unity Connection.

Note This procedure requires a Cisco Unity Connection administrative user ID. If you do not have this ID, contact the Cisco Unity Connection system administrator.

Procedure

Step 1 In Cisco Unity Connection Administration, select **Users > Users**.

Step 2 On the Search Users page, select **Add New**.

The New User window opens.

Step 3 Enter information for the following fields for the application user that Cisco WebEx Social will use to log in to the Cisco Unity Connection server:

- Alias
- First Name
- Last Name
- SMTP Address—Use the same value you entered for Alias.

Step 4 Click **Save**.

The Edit User Basics window opens.

Step 5 Select **Edit > Roles**.

Step 6 Move the following roles to the Assigned Roles section of the Edit Roles window.

- System Administrator
- Remote Administrator
- User Administrator

Step 7 Click **Save**.

Step 8 Select **Edit > Change Password**.

Step 9 Enter the desired password and confirm the password.

Step 10 Select **Edit > Password Settings**.

Step 11 Uncheck the User Must Change at Next Sign-In box.

Step 12 Cisco recommends that you check the **Does Not Expire** box, unless your company policy requires passwords to expire.

Step 13 Click **Save**.

Configuring Voice Mail Server in Cisco WebEx Social

To configure voice mails servers in Cisco WebEx Social, perform the following steps. You can add as many Cisco Unity Connection voice mail servers as there are available:

Procedure

Step 1 Access the Common Configurations 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 **Server**

d. Click **Common Configurations** in the Server drawer.

Step 2 Select the **Voice Mail Server** tab.

The Add a Voice Mail Server window opens.

Step 3 In the Server URL field, enter the fully qualified domain name of the Cisco Unity Connection voice mail server.

This name must match both the server name in the SSL security certificate and the alias that is used to import the certificate into the keystore (see the "Generating the SSL Tomcat Certificate" section on page 3-35).

Step 4 In the User Name field, enter the user ID of the administrative user account of the Unity Connection server.

Enter the name of the user who is configured in Cisco Unity Connection to perform Cisco WebEx Social voice mail tasks (see the "Adding the Administrative User in Cisco Unity Connection" section on page 3-33).

Step 5 In the Password field, enter the password of the administrative user account of the Unity Connection server.

Step 6 (Optional) In the Pilot Number field, enter the number that connects to the Cisco Unity Connection Interactive Voice Response (IVR) system.

Step 7 Click **Add**.

The server now appears in the Registered Voice Mail Servers list.

Step 8 Repeat steps Step 3 through Step 7 for each server that you want to add.

Note

- To delete a voice mail server, check the corresponding box in the Registered Voice Mail Servers list, then click **Delete**.
- If you want to modify information for a voice mail server that is already configured, delete the server and then configure it again with the new information.

Generating the SSL Tomcat Certificate

You must generate an SSL Tomcat certificate and load it into Cisco WebEx Social before you can use voice messaging in Cisco WebEx Social.

Note This procedure requires a Cisco Unity Connection administrative user ID. If you do not have this ID, contact the Cisco Unity Connection system administrator.

To generate and deploy the SSL certificate, follow these steps:

Procedure

Step 1 Sign in to Cisco Unified OS Administration with administrative privileges.

Step 2 Select **> Security > Certificate Management**.

Step 3 Click **Find** to display all the certificates on the Cisco Unity Connection system.

The certificate named **tomcat.pem** appears at the top of the list.

Step 4 Left-click the **tomcat.pem** certificate.

Step 5 In the window that shows the certificate for **tomcat.pem**, click **Download** and save the file to your local PC.

Step 6 Rename the downloaded file to *fully_qualified_unity_server_name*.pem (for example, *unity-server.cisco.com.pem*).

Step 7 Sign in to the Director and take these actions:

Step 8 Click **Security** under Application.

Step 9 In the Add New Trusted Certificates area, take these actions:

a. In the Alias field, enter the FQDN of the Cisco Unity Server.

b. In the Trusted Certificate field, use the Browse button to locate the certificate file that you downloaded and select that file.

c. Click **Save**.

Step 10 In the Trusted Certificates area, click **Deploy Trusted Certificates**.

Step 11 Wait several minutes to make sure that Tomcat is back up. You can monitor Tomcat with the following command:

tail -f /opt/cisco/quad/tomcat/logs/catalina.out

Configuration Performed By the Cisco WebEx Social End User From the Voice Messages Application

After you have performed the procedure that is described in the "Configuration Performed By the Cisco WebEx Social End User From the Voice Messages Application" section on page 3-36, instruct users to do the following:

Procedure

Step 1 Add the Voice Messages Application to the desired location of their Home pages.

Step 2 Move the cursor over the **Voice Messages** application name and click the gear icon  that appears to the right of the name.

Step 3 Select **Edit Setting**.

Step 4 From the drop-down list that appears, select the voice mail server that they use.

If the appropriate voice mail server is not known, contact the Cisco Unity Connection system administrator, or check Cisco Unity Connection user documentation for information about how to obtain this information.

Step 5 Click **Save**.

WebDialer Administration

WebDialer is used for click-to-call from within Cisco WebEx Social and to allow you to place a call using your telephone from within Cisco WebEx Social. (Telephone dialing requires the installation of the Cisco Web Communicator browser plugin.)

Note WebDialer requires that the Cisco WebDialer service already be configured in Cisco Unified Communications Manager.

The following sections describe how to configure the WebDialer feature for Cisco WebEx Social.

- Adding a Cisco WebEx Social WebDialer User to Cisco Unified Communication Manager Administration, page 3-37
- Configuration Required if a Proxy Is Used in the Cisco WebEx Social Network, page 3-38
- Configuring WebDialer in Cisco WebEx Social, page 3-38
- User Selection and Testing of Phones, page 3-39

Adding a Cisco WebEx Social WebDialer User to Cisco Unified Communication Manager Administration

For Cisco WebEx Social to work with WebDialer on Cisco Unified Communications Manager, you must create a new user group within Cisco Unified Communications Manager, create an application user for Cisco WebEx Social, and map that application user to that user group.

To do so, perform the following steps. These steps require Cisco Unified Communications Manager administrator privileges.

Procedure

Step 1 Sign in to Cisco Unified Communications Manager Administration.

Step 2 Navigate to **User Management > User Group**. The Find and List User Groups window opens.

Step 3 Click **Add New**. The User Group Configuration window opens.

Step 4 Enter a descriptive name, such as *Cisco WebEx Social WebDialer Group*, then click **Save**.

Step 5 From the Related Links drop-down list in the upper-right corner of the User Group Configuration window, select **Assign Role to User Group**.

Step 6 Click **Go** next to the Related Links drop-down list.

Step 7 Click **Assign Role to Group**.

The Find and List Roles window opens.

Step 8 Check the boxes next to these roles:

- Standard AXL API Access
- Standard SERVICEABILITY Administration
- Standard CCM Admin Users
- Standard EM Authentication Proxy Rights

Step 9 Click **Add Selected**.

The User Group Configuration window appears. The roles that you added should appear in the Role Assignment area.

Step 10 Confirm that the correct roles appear and click **Save**.

Step 11 To create an application user to whom Cisco WebEx Social can send WebDialer requests, select **User Management > Application User**. The Find and List Application Users window opens.

Step 12 Click **Add New**. The Application User Configuration window opens.

Step 13 In the User ID field, enter a descriptive ID, such as *CiscoWebExSocialWDUser123*.

Step 14 In the Password field, enter a password for the User ID.

Step 15 In the Confirm Password field, re-enter the password.

Step 16 In the Permissions Information portion of the Application User Configuration window, click **Add to User Group**. The Find and List User Groups window opens.

Step 17 Find the Cisco WebEx Social WebDialer group that you have already created, select the box next to its name, then click **Add Selected**. You are now returned to the Application User Configuration window, and the Cisco WebEx Social WebDialer group that you added should appear in the Groups area of the window.

Step 18 Confirm that the user group appears, then click **Save**.

Configuration Required if a Proxy Is Used in the Cisco WebEx Social Network

If your Cisco WebEx Social deployment is configured to use a proxy server, add the Cisco Unified Communication Manager server or servers to the Exceptions field in the Proxy Settings area in Portal window in the Director. For instructions, see the "Proxy Settings" section on page 5-18.

Note The values or wildcards that you enter in the Exceptions field must exactly match the IP address or host name of the Cisco Unified Communication Manager servers.

Configuring WebDialer in Cisco WebEx Social

To configure WebDialer in Cisco WebEx Social, follow these steps:

Procedure

Step 1 Access the Common Configurations 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 **Server**

d. Click **Common Configurations** in the Server drawer.

Step 2 Select the **WebDialer** tab.

Step 3 Check the **Enable WebDialer** box.

Step 4 Take these actions in the Add a UCM Cluster area:

a. In the Unified Communications Manager field, enter either the hostname or the IP address that you used when you installed the Cisco Unified Communications Manager publisher node.

b. In the User Name field, enter name of the Cisco Unified Communications Manager application user that you created in the "Adding a Cisco WebEx Social WebDialer User to Cisco Unified Communication Manager Administration" section on page 3-37.

c. In the Password field, enter password of the Cisco Unified Communications Manager application user that you created in the "Adding a Cisco WebEx Social WebDialer User to Cisco Unified Communication Manager Administration" section on page 3-37.

d. Click **Add**.

The cluster appears in the Registered UCM Clusters list. Make sure the primary host name and WebDialer-enabled nodes appear correctly in the window.

You can click the **Refresh** button to update the list if there is an update to the UCM cluster.

You can delete a cluster from this list by checking the box for the cluster and clicking the **Delete** button.

Step 5 Take these actions to restart each Cache node in your deployment:

a. Log in to the Director.

b. Click **Topology** under System.

c. Click the **Disable** button in each row that shows "Cache."

d. Click the **Enable** button in each row that shows "Cache."

User Selection and Testing of Phones

Instruct each user who has more than one phone to perform these steps:

Procedure

Step 1 Access your account settings:

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. Select **My Account** in the left pane of the window.

Step 2 On the right pane, click **Phone control preference** under Miscellaneous.

Step 3 Click **Test Call** next to the devices listed and wait until you receive a success message.

Note **Test Call** is not supported for Extension Mobility and does not appear if you are using the Cisco Web Communicator plugin.

Step 4 Select a radio button for a device that had a successful test call to make that device the click-to-call device.

Step 5 Click **Save**.

Note The Cisco Web Dialer Preference Page shows an Extension Mobility Profile for all Cisco WebEx Social users, even if a user does not have an Extension Mobility profile in Cisco Unified Communications Manager. It is the responsibility of Cisco WebEx Social users with Extension Mobility profiles to sign in to their phones before attempting to use Extension Mobility click-to-dial. Multiple Extension Mobility profiles are not supported.

WebEx Site

This section describes how to integrate the Cisco WebEx meeting feature with Cisco WebEx Social. After you complete this integration, Cisco WebEx Social users can launch or join a WebEx meeting from within Cisco WebEx Social without needing to sign in to WebEx.

To integrate the Cisco WebEx meeting feature, perform the following general steps:

- Step 1: Generating and Storing Key Certificates, page 3-40

  This step is required only if you are using SSO in your deployment.

- Step 2: Configuring Cisco WebEx Social for Cisco WebEx Meeting, page 3-41

Step 1: Generating and Storing Key Certificates

If you are using SSO in your Cisco WebEx deployment, follow these steps to generate and store key certificates that WebEx uses to decrypt authentication tokens that Cisco WebEx Social sends:

Step 1 Use an SSH client to access any App Server node and log in as the admin user.

Step 2 Enter this command to generate a key certificate for a WebEx site and store the certificate in the keystore on the Cisco WebEx Social server:

[root]# **sudo /user/java/bin/keytool -genkey -keyalg RSA -alias** *WebEx_site* **-validity** *days_valid* **-keypass** *key_password* **-keystore** *store_name* **-storepass** *store_password* **-dname "cn=***partner_name***"**

where:

- *WebEx_site* is the name of a WebEx site that appears in the Site URL field in the Registered WebEx sites area when you select **Server > Common Configurations > WebEx Site name** from the control panel (do not include **http://** when you enter this name)
- *days_valid* is the number of consecutive days from now that the certificate is to be valid
- *key_password* is a password that protects the key certificate in the keystore
- *store_name* is the full path and file name of the keystore in which to store this certificate
- *store_password* is a password that protects the keystore
- *partner_name* is the partner name that was configured for the WebEx site when WebEx was set up

Repeat this step as needed to generate a key certificate for each WebEx site. Use the same values for *key_password*, *store_name*, and *store_password* each time.

Step 3 Enter this command to export a key certificate to a file that can be uploaded to the WebEx site:

[root]# **sudo /user/java/bin/keytool -export -alias** *WebEx_site* **-keypass** *key_password* **-keystore** *store_name* **-storepass** *store_password* **-file** *certificate_file*

where:

- *WebEx_site* is the name of a WebEx site that appears in the Site URL field in the Registered WebEx sites area when you select **Server > Common Configurations > WebEx Site name** from the control panel (do not include **http://** when you enter this name).
- *key_password* is a password that protects the key certificate in the keystore. Enter the same value that you used in Step 1.
- *store_name* is the full path and file name of the keystore in which to store this certificate. Enter the same value that you used in Step 1.
- *store_password* is a password that protects the keystore. Enter the same value that you used in Step 1.
- *certificate_file* is the full path and file name on the local drive of the export file.

Repeat this step for each key certificate that you generated in Step 1.

Step 4 Send each export file that you created in Step 3 to the WebEx site administrator for the corresponding WebEx site.

Step 5 In the Director, take these actions:

a. From the control panel, click **Security** under Application.

b. In the Webex SSO area, enter the Key Password and Keystore Password for the keystore.

Use the same values that you designated for *key_password* and *store_password* in Step 1.

a. In the Keystore File field, click the **Choose File** button, then navigate to and select the file that you generated in Step 3.

b. Click **Save.**

Step 6 Contact the WebEx site administrator at each WebEx site and ask them to take these actions:

a. Upload to the WebEx Site Administrator window the key certificate that you sent in Step 3.

b. In the WebEx Site Administrator window, enable Partner SAML Authentication Access for the certificate.

Step 2: Configuring Cisco WebEx Social for Cisco WebEx Meeting

To configure Cisco WebEx Social for Cisco WebEx meeting, perform the following steps.

Before You Begin

If you are using SSO in your Cisco WebEx deployment, follow the steps in the "Step 1: Generating and Storing Key Certificates" section on page 3-40 and obtain a partner ID from the WebEx Meeting administrator.

Procedure

Step 1 Access the Common Configurations 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 **Server**

d. Click **Common Configurations** in the Server drawer.

Step 2 Select the **WebEx Site** tab.

Step 3 In the Site URL field, enter the URL of the WebEx server.

Step 4 If you are using SSO in your Cisco WebEx deployment, take these actions:

a. If your WebEx site is SSO enabled, you can check the **SSO Enabled** box so that a user who is signed in to Cisco WebEx Social does not need to sign in again to WebEx. The WebEx site uses SSO to log the user in.

b. If you checked the **SSO Enabled** box, select one of the following values from the **How do users authenticate?** drop-down list:

- **By Screen Name**
- **By Email Address**

c. If you checked the **SSO Enabled** box, in the Partner ID field, enter the partner ID that the WebEx site administrator configured in WebEx side.

Step 5 Click **Add**.

The WebEx URL appears in the Registered WebEx sites list.

Step 6 Add a WebEx site for each WebEx server your company uses. For example, you may have one WebEx site for sales, one for support, and so on.

Step 7 Instruct your users to perform the following initial setup to use WebEx:

a. Click the **Modify Calendar Settings** link in the alert box in the Calendar area of the Home page.

The My Account window opens.

b. Select the appropriate site from the WebEx Site drop-down list.

c. If needed, enter the user name and password for the WebEx account.

A user name and password are not needed for sites that support Single Sign-On (SSO).

d. Click **Save** in the right column of the My Account window.

e. Click the **WebEx Instant Meetings** link in the alert box in right column of the My Account window.

The My Account window opens.

f. If needed, update settings in this window and click **Save** in the right column of the My Account window.

Twitter Administration

From Cisco WebEx Social, users can microblog to Twitter.com.

The following sections describe how to configure Cisco WebEx Social to allow microblogging to Twitter and the information that end users need to link their Twitter accounts with Cisco WebEx Social:

- Configuring Cisco WebEx Social for use with Twitter, page 3-42
- End-User Configuration, page 3-43

Configuring Cisco WebEx Social for use with Twitter

To configure Cisco WebEx Social to allow users to microblog to Twitter.com, follow these steps:

Procedure

Step 1 Access the Twitter Administration 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 **Server**

d. Click **Twitter Administration** in the Server drawer.

Step 2 In the Hashtag field, you can enter any name, but it makes the most sense to enter a descriptive name, such as the name of your company because Cisco WebEx Social users also need to know the hashtag you assign in this field. Cisco WebEx Social uses this hashtag to search for incoming tweets.

By default, Cisco WebEx Social searches twitter for incoming tweets every five minutes.

Note To stop Cisco WebEx Social from searching twitter for incoming tweets, leave the Hashtag field blank and click **Save**.

Step 3 Click **Save**.

End-User Configuration

After you configure Cisco WebEx Social to allow users to microblog to Twitter.com, provide the following information to users.

- Linking Your Twitter Account to Cisco WebEx Social, page 3-43
- De-Linking Your Twitter Account from Cisco WebEx Social, page 3-44
- Important Information for End Users, page 3-44

Linking Your Twitter Account to Cisco WebEx Social

Cisco WebEx Social users should perform the following steps to link their Twitter account to Cisco WebEx Social.

Note Users must have an account on www.twitter.com.

Procedure

Step 1 Click the down-arrow to the right of **Post** in the Global Navigation Bar.

Step 2 Select **Share an Update** from the drop-down menu.

Step 3 Check the box next to the Twitter icon .

The Twitter Configuration window appears If you have not already linked your Twitter account to Cisco WebEx Social.

If you are prompted to authorize Cisco WebEx Social to use your twitter account, enter your Enter your Twitter user name or e-mail address and your Twitter password

Step 4 Click **Authorize app**.

De-Linking Your Twitter Account from Cisco WebEx Social

If you ever want to de-link your account from Cisco WebEx Social, follow these steps:

Procedure

Step 1 Access your account settings:

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. Select **My Account** in the left pane of the window.

Step 2 On the right pane, click **Social Network** under Identification.

Step 3 Click **Delink my Twitter account**.

Important Information for End Users

Provide the following information to users who will microblog to Twitter.com:

- Users can enable their microblogs to post to Twitter by checking the applicable box in their microblog bubble.
- Users can tweet from within Cisco WebEx Social to twitter friends who are not Cisco WebEx Social users.
- Users see incoming tweets in the Social Activities application on their Home page if the following conditions are met:
  - Tweets contain a hash tag that is configured by the Cisco WebEx Social system administrator
  - Tweets were sent by someone who configured Twitter through Cisco WebEx Social

License Agreement (EULA)

Use the License Agreement (EULA) window to modify the end user license agreement (EULA) that is presented to your users when they first sign in to Cisco WebEx Social.

Procedure

Step 1 Access the License Agreement (EULA) 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 **Server**

d. Click **License Agreement (EULA)** in the Server drawer.

Step 2 From the Language drop-down list, select the language of the EULA that you want to modify.

Step 3 Click **Modify**.

Step 4 Using the editor that is brought up, make your changes to the license agreement and click **Save**.

To exit the editor without saving changes, click the **Close** button, then click **Close** in the Closer Editor dialog box.

To delete a EULA (other that the one that is currently the default), click the **Delete** button.

Step 5 (Optional) If you edited a EULA that is in a language other than the current default EULA, click the **Make Default** button to make it the default EULA that users see.

CHAPTER 4

Mobile Settings

The Mobile drawer contains selections that allow system administrators to configure and manage the following features that apply Cisco WebEx Social mobile clients:

- Branding—Lets a Cisco WebEx Administrator customize the look and feel of the Cisco WebEx Social app.
- Extensibility—Provides users of the Cisco WebEx Social app access to custom applications that are for mobile devices

To access the Mobile 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 Mobile drawer so that you can access its selections, click the right-arrow next to **Mobile**.

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

Settings

The Settings window in the Mobile drawer lets you configure whether the branding and extensibility functions are enabled or disabled. You must enable the function that you want to configure and use.

To enable branding or extensibility 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 **Mobile**

d. Click **Settings** in the Mobile drawer.

Step 2 Check the box for the feature that you want to enable:

- **Branding**
- **Extensibility**

To disable a feature, uncheck its box.

Step 3 Click **Save**.

Step 4 Restart the WebEx Social service on each App Server node and on each Worker node.

To do so, disable and then enable each node from the Server List area in the Topology window of the Director. For more information, see the "Server List" section on page 5-9.

Branding

The Branding window in the Mobile drawer lets you add, replace, or remove branding assets for supported Cisco WebEx Social mobile clients. An asset is a file that controls the look and feel of various elements of the Cisco WebEx Social app GUI that runs on mobile client.

This section includes these topics:

Adding or Replacing a Branding Asset

This section explains how to add or replace a branding asset.

Before you begin

- Enable the branding feature as described in the "Settings" section on page 4-1
- Make sure that a compatible asset has been created and that the file is stored in a location that can be accessed from Cisco WebEx Social

To add or replace a branding asset, follow these steps:

Step 1 Access the Branding 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 **Mobile**

d. Click **Branding** in the Mobile drawer.

The Branding window appears. This window lists and describes the mobile client types that Cisco WebEx Social supports. If an asset has already been uploaded for a mobile client, the asset filename and the date and time that it was uploaded appears under the corresponding mobile client description.

Step 2 Click the **Upload** button next to the mobile client type for which you want to upload an asset.

If an asset is not uploaded for the mobile client, the Upload Branding Asset dialog box appears, which allows you to upload a new asset for the mobile client.

If an asset is uploaded for the mobile client, the Edit Branding Asset dialog box appears, which allows you to replace an existing asset for the mobile client.

Step 3 Click **Choose File** in the Upload Branding Asset dialog box or in the Edit Branding Asset dialog box, navigate to the asset file, and then click **Upload**.

Removing a Branding Asset

This section explains how to remove a branding asset from Cisco WebEx Social. This procedure does not remove the asset file from its storage location, so you can access it later if needed.

Before you begin

Enable the branding feature as described in the "Branding" section on page 4-2.

To remove a branding asset, follow these steps:

Step 1 Access the Branding 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 **Mobile**

d. Click **Branding** in the Mobile drawer.

Step 2 Click the delete icon next to the asset that you want to delete, and then click **Delete** in the Delete Asset dialog box to confirm.

Extensibility

The Extensibility window in the Mobile drawer lets you add, update, or remove custom web applications that mobile device users can access from the Cisco WebEx Social app.

This section includes these topics:

This section includes these topics:

Adding an Application

This section explains how to add a custom application to Cisco WebEx Social.

Before you begin

- Enable the extensibility feature as described in the "Settings" section on page 4-1

- Make sure that a compatible custom application has been created and that properly sized icons for the application have been created stored in a location that can be accessed from Cisco WebEx Social. An icon must saved as a .bmp, .gif, .jpeg, or .png file. Icons must be created in these sizes:
  - Large icon—96 by 96 pixels
  - Medium icon—48 by 48 pixels
  - Small selected icon—30 by 30 pixels
  - Small unselected icon—30 by 30 pixels

To add an application, follow these steps:

Step 1 Access the Extensibility 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 **Mobile**

d. Click **Extensibility** in the Mobile drawer.

The Extensibility window appears. This window shows the title and a brief description of each application that has been added to Cisco WebEx social, and the date and time that the application was uploaded or updated. To see the complete text of a long description, hover your mouse cursor over the description.

Step 2 Click the **Add Application** button.

Step 3 In the Add Application area, take these actions:

a. In the Title field, enter a brief descriptive title for the application.

b. The the Description field, enter a description of the application.

c. In the Assets field, Click the right-arrow to the left of the device for which you want to add the application.

d. In the Application URL field, the URL that the Webex Social mobile app uses invoke the custom application.

e. For each icon size, click the **Choose File** button, and navigate and select the desired icon file.

f. Click **Save**.

Updating or Removing an Application

This section explains how to remove a custom application from Cisco WebEx Social. Removing an application from Cisco WebEx Social does not remove the application and icon files from their storage locations, so you can access them later if needed.

Before you begin

- Enable the extensibility feature as described in the "Settings" section on page 4-1
- Make sure that a compatible custom application has been created and that properly sized icons for the application have been created stored in a location that can be accessed from Cisco WebEx Social. An icon must saved as a .bmp, .gif, .jpeg, or .png file. Icons must be created in these sizes:
  - Large icon—96 by 96 pixels

- Medium icon—48 by 48 pixels
- Small selected icon—30 by 30 pixels
- Small unselected icon—30 by 30 pixels

To update or remove an application, follow these steps:

Step 1 Access the Extensibility 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 **Mobile**

d. Click **Extensibility** in the Mobile drawer.

The Extensibility window appears. This window shows the title and a brief description of each application that has been added to Cisco WebEx social, and the date and time that the application was uploaded or updated. To see the complete text of a long description, , hover your mouse cursor over the description.

Step 2 From the **Actions** drop-down menu next to the application that you want to update or remove, take either of these actions:

- To remove the application, select **Delete**, and then click **Delete** in the Delete Asset dialog box to confirm.
- To update the application, select **Edit**.

Step 3 If you selected Edit to update the application, update any or all of the following fields in the Edit Application area, and then click **Save**:

a. In the Title field, enter a brief descriptive title for the application.

b. The the Description field, enter a description of the application.

c. In the Assets field, Click the right-arrow to the left of the device for which you want to add the application.

d. In the Application URL field, the URL that the Webex Social mobile app uses invoke the custom application.

e. For each icon size, click the **Choose File** button, and navigate and select the desired icon file.

CHAPTER 5

Director

The Director is used to set up your Cisco WebEx Social topology and manage various system configuration options. It provides access to various configuration windows, which are arranged in the following categories:

- System—Configure and manage items that relate to various Cisco WebEx Social system settings
- Application—Configure various basic and advanced Cisco WebEx Social application settings

When you use the Director, be aware of the following:

- Several of the configuration options can greatly affect the operation of your Cisco WebEx Social topology. Use care when making these changes.
- When you click **Save** after making configuration changes, some Cisco WebEx Social nodes may be restarted automatically for your changes to take effect.

This section includes these topics:

System: Configuration

The Configuration window provides areas for configuring a variety of items that relate to your Cisco WebEx Social deployment. The following sections describe these areas:

Unified Access

Use the options in the Unified Access area in the Configuration window to configure a unified access password and components that can be accessed with this password.

To configure the Unified Access parameters, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Configuration** under System.

Step 3 In the Unified Access area, take these actions:

a. Enter values for the fields that Table 5-1 describes.

b. Click **Save**.

Table 5-1 Unified Access Settings

Parameter	Description
Credentials	
Unified Password	Password to be set for the administration interfaces that you choose with the Access Propagation option.

Table 5-1 Unified Access Settings (continued)

Parameter	Description
Access Propagation	Check the check box for each component for which to propagate the unified access password. Components are: • Search—Search Store and Index Store administration interface • Notifier—Notifier administration interface • Message Queue—Message Role administration interface • Grub—Linux GRUB • Index Store—Index Store administration interface

NFS

Use the options in the NFS area in the Configuration window to configure the Network File System (NFS) mount point.

Before you configure NFS, see the "NFS Requirements" section in *Cisco WebEx Social Installation and Upgrade Guide*.

To configure this NFS mount point, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Configuration** under System.

Step 3 In the NFS area, take these actions:

a. In the NFS Host field, enter the host name of the NFS server.

b. In the Exported Directory field, enter the path from which the four NFS mount points are exported. Use this format:

/exported_root_folder

For example, if you export the /export/webex_social directory in the exports file on the NFS server, specify a slash (/) as the Exported Directory in the Director GUI.

c. In the NFS Domain field, enter the fully qualified domain name or the IP address of the NFS server.

This item is required in the NFS server is not in the same NFS domain as the Cisco WebEx Social nodes.

d. Click **Save**.

You can check NFS status and related log files as follows:

- Use these commands to check the status of NFS on Cisco WebEx Social nodes:
  - [root@webexsocial-1 ~]# **df -Tht nfs4**
  - [root@webexsocial-1 ~]# **service autofs status**

- Use these commands to check the status of NFS on the NFS server:
  - [root@nfs ~]# **exportfs -v**
  - [root@nfs ~]# **service nfs status**
- Check these log files on the Director node:
  - /opt/logs/*date*/*hostname*_messages—For RSyslog failures

NTP

Use the options in the NTP area in the Configuration window to designate the Network Time Protocol (NTP) server for use with Cisco WebEx Social.

To configure NTP, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Configuration** under System.

Step 3 In the NTP area, take these actions:

a. In the Primary field, enter the fully qualified domain name of the primary NTP server.

b. In the Secondary field, enter the fully qualified domain name of the secondary NTP server.

c. Click **Save**.

Notifier

The Notifier is an XMPP publisher that is used to notify Cisco WebEx Social users of events, including system alerts, announcements, and activities. Use the options in the Notifier area in the Configuration window to configure the Notifier.

To configure the Notifier, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Configuration** under System.

Step 3 In the Notifier area, configure the fields that Table 5-2 describes.

Step 4 Click the **Save** button that appears under the Enable SSO box.

Table 5-2 Notifier Settings

Parameter	Description
LDAP Settings	

Table 5-2 Notifier Settings (continued)

Parameter	Description
LDAP Hostname/IP	Fully qualified domain name or IP address of the LDAP host. 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.
LDAP Port	Port used for communication with the LDAP host. 389 is commonly used.
Credentials	Password of the LDAP administrator.
Base DN	Specifies the initial search context in LDAP for users. It is the top level of the LDAP directory tree. For example: **cn=users,dc=ad1,dc=webexsocial,dc=com**
Full Name	LDAP field for obtaining the first and last name of users. This value must match the entry in the Full Name field in the LDAP Authentication window (you access this window by selecting **Portal > Settings > Authentication > LDAP Authentication** from the control panel for the system administrator). For example, this value can be set to *cn*.
Principal	LDAP administrator ID. If you have removed the default LDAP administrator, enter the fully qualified name of the administrative credential that you use. You need an administrative credential because Cisco WebEx Social uses this ID to synchronize user accounts to and from the LDAP server. For example, the default Windows Domain Administrator is: cn=administrator,cn=users,dc=*your_domain*,dc=[com | net | local]
Screen Name	This value should map to the LDAP attribute that Cisco WebEx Social uses for screen name (typically sAMAccountName for Active Directory). Make sure that the value you enter here matches the Screen Name field in the LDAP Authentication window (you access this window by selecting **Portal > Settings > Authentication > LDAP Authentication** from the control panel for the system administrator).

Table 5-2 Notifier Settings (continued)

Parameter	Description
Import Search Filter	LDAP object type used to filter the search. Depending on the LDAP server, there are different ways to identify the user. The default value is (objectClass=Person). If you want to search for only a subset of users or users that have different object classes, you can change this setting. Make sure that the value you enter here matches the Import Search Filter field in the LDAP Authentication window (you access this window by selecting **Portal > Settings > Authentication > LDAP Authentication** from the control panel for the system administrator).
Enable SSO	If you check this box, single sign-on is enabled. In this case, Notifier does not authenticate a user against LDAP because the password of the user is not sent to Cisco WebEx Social. Notifier does verify the existence of the user in LDAP. This option is disabled by default.
Enable Secure LDAP	Check this box to enable a secure communications protocol, such as HPPTS, for the Notifier.

Analytics Store Cron Job

The Analytics Store is a Mongodb database that contains information about user activities and Cisco WebEx Social metrics. Cisco WebEx Social uses data from the Analytics Store to provide suggestions about what communities or other aspects of the system may interest a particular user. Cisco WebEx Social also uses the Analytics Store to calculate the raw data used in the Metrics reporting that you access in the Portal > WebEx Social Metric window (see the "WebEx Social Metrics" section on page 2-33 for more information).

The system executes a CRON job on the primary Analytics Store to compute suggested content and connections, and to calculate the raw data used in the Metrics reporting. You use the Analytics Store Cron Job area in the Configuration window to configure the hour of the day that the CRON job starts.

To configure the start time for a the CRON job, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Configuration** under System.

Step 3 In the Analytics Store Cron Job area, take these actions:

a. From the Hour of Day (UTC) drop-down list, select the UTC time that the configured Cron task runs each day. Cisco recommends that you set this time to be during off-peak hours. Alternatively, you might find it convenient to set this time to correspond to midnight local time.

b. Click **Save**.

Health and Diagnostics

Use the option in the Health and Diagnostics area in the Configuration window to configure email IDs for alerts.

To configure email IDs, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Configuration** under System.

Step 3 In the Health and Diagnostics area, take these actions:

a. In the EmailID(s) for Alerts text field, enter email IDs, separated by commas.

b. Click **Save**.

SNMP

Use the option in the SNMP area in the Configuration window to configure the SNMP community string.

When you make this configuration, you can use SNMP v2c for monitoring of statistics that apply to the operating system.

To configure the SNMP community string, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Configuration** under System.

Step 3 In the SNMP area, take these actions:

a. In the Community String text field, enter the SNMP community string.

b. Click **Save**.

Outbound Email

Use the options in the Outbound Email area in the Configuration window to configure the email relay host and relay TCP port.

To configure the Outbound Email parameters, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Configuration** under System.

Step 3 In the Outbound Email area, take these actions:

a. In the Email Relay Host field, enter the name of the email relay host.

b. In the Email Relay TCP Port field, enter the number of the email relay TCP port.

c. Click **Save**.

Step 4 If Email Digest is not configured, select **Portal** under Application and take these actions in the Email Digest area:

a. In the Mail Domain field, enter the SMTP domain of the Cisco WebEx Social application.

For related information, see the "Email Digest" section on page 5-15.

b. Click **Save**.

Console Login Banner

Use the option in the Console Login Banner area in the Configuration window to configure the message of the day, which appears when a user logs in to the OS console in the VMware environment when setting up virtual machines.

To configure the daily message that appears when you log in to the OS console, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Configuration** under System.

Step 3 In the Console Login Banner area, take these actions:

a. In the Message of the Day field, enter the text you want displayed when you log in to the console.

b. Click **Save**.

System: Topology

The Topology window provides areas for configuring a variety of items that relate to your Cisco WebEx Social deployment. The following sections describe these areas:

Provision New Server

Use the options in the Provision New Server area in the Topology window to configure the role for a server in your Cisco WebEx Social deployment.

To provision a server, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Topology** under System.

Step 3 From the Role drop-down list, choose one of the following options to designate the role of the server:

For an explanation of each role, see the "Overview of Cisco WebEx Social Nodes" section on page 1-2.

Step 4 In the FQDN field, enter the fully qualified domain name or the IP address of the server.

Step 5 Click **Add**.

Server List

The Server List area in the Topology window provides information about the servers (nodes) that are in your Cisco WebEx Social topology and lets you enable, disable, or delete a server.

When you are viewing this area, you can click the **Refresh All** button to fetch and display current version information and operational status for all servers in the Server List area.

When you enable or disable servers, enable App Server roles last, and disable App Server roles first.

Table 5-3 describes the information and controls that the Server List area provides for each server.

Table 5-3 Server List Information and Controls

Item	Description
Role	Cisco WebEx Social role that is assigned to the server.
FQDN	Fully qualified domain name of the server.
Version Info	Provides three lines of information: • Line 1—Cisco WebEx Social software version that is running on the server. • Line 2—Date and time of the last successful software configuration check. • Line 3—Information about a server failure, if a failure occurred. Otherwise, displays "OK."

Table 5-3 Server List Information and Controls (continued)

Item	Description
Operational Status	Displays the current status of the server, which can be: • Running • Stopped • Not Installed • Unreachable Host • Connection Failed Also includes these buttons: • **Refresh**—Fetches current version information and operational status and displays this information for server • **Disable/Enable**—Toggle button. **Disable** stops the service for the corresponding role. **Enable** starts the service for the corresponding role. These buttons apply only to App Server, Cache, and Worker roles. To disable other roles, use an SSH connection to access the node.
Action	Clicking the **Delete** button removes the server from the Cisco WebEx Social topology and updates the global configuration. JSON Store and Analytics Store nodes cannot be removed.

System: Software

Use the Software window to upgrade the Cisco WebEx Social software that runs on the nodes in your Cisco WebEx Social deployment. This window includes these areas with options for uploading an upgrade file and performing the upgrade.

The following sections describe these areas:

- SCP File Upload, page 5-10
- Upgrade, page 5-11

SCP File Upload

Before you can use this window to perform an upgrade, you must have received the patch .img file for the upgrade and stored this file on a Linux or Unix node that supports SCP.

Note Before performing a software upgrade, see the upgrade information in *Cisco WebEx Social Installation and Upgrade Guide*. In particular, see the "Using the Software Window" section in that document. This information includes important steps that you should follow before and after the procedure that is provided here.

To upload the patch .img file, follow these steps.

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Software** under System.

Step 3 In the Host Name field, enter the fully qualified domain name or the IP address of the node where you placed the patch .img file.

Step 4 In the File Name field, enter the complete path and file name of the .img file.

Step 5 In the Linux/Unix User Name field, enter the user ID of the node on which the patch .img file has been placed.

Step 6 In the Password field, enter the password for the User ID that you entered.

Step 7 Click **Upload**.

The software version that you uploaded appears in the Available Upgrade Version field in the Upgrade area of the window.

Upgrade

Before you can use this window to perform an upgrade, you must have uploaded a patch .img file for the upgrade so that it appears in the Available Upgrade Version field.

Note Before performing a software upgrade, see the upgrade information in *Cisco WebEx Social Installation and Upgrade Guide*. In particular, see the "Using the Software Window" section in that document. This information includes important steps that you should follow before and after the procedure that is provided here.

To perform a software upgrade, follow these steps.

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Software** under System.

Step 3 Ensure that the software version that you uploaded appears in the Available Upgrade Version field.

Step 4 Click **Upgrade**.

The software on each node in your Cisco WebEx Social cluster is upgraded.

System: Health

The Health window lets you view or download Cisco WebEx Log files and displays the health status of various Cisco WebEx Social services.

Downloading Log Files

You can view or download up to 30 Cisco WebEx Log files at one time. To do so, follow these steps.

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Health** under System.

Step 3 In the Download Logs area, take these actions:

a. From the Date drop-down list, select the date of the log files that you want.

b. From the Module drop-down list, select the module for which you want log files.

c. From the Node drop-down list, select the Cisco WebEx Social node for which you want log files.

d. Click **Download**.

e. In the dialog box that appears, make settings as desired, then click **OK** to open or save the log files.

Step 4 Click **Upgrade**.

The software on each node in your Cisco WebEx Social cluster is upgraded.

Viewing Health Status

The Health area of the Health window displays the health status of various services that run on each Cisco WebEx Social node. The information in this area refreshes automatically every 60 seconds.

Service status is divided into these categories:

- Critical—The service has failed or has exceeded critical levels
- Warning—The service has experienced a non-critical error
- OK—The service is performing as expected

The display near the top of the screen indicates how many messages in each category are displayed. The system retains messages indefinitely.

The health status includes the following information for each service:

- Service—Name of the service
- Host—FQDN of the hose that is reporting the status
- Duration—Length of time that the report has been running
- Flapping—Indicates whether the report is periodically changing status is in same state for the period that is indicated by Duration
- Message—System generated message that provides additional information

System: Stats

The Stats window allows you to view statistics and metrics for various Cisco WebEx Social components. To view statistics and metrics, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Stats** under System.

Step 3 Select either of these tabs:

- **Dashboard**—Lets you view a predefined set of statistics and metrics for Cisco WebEx Social nodes
- **Raw**—Lets you view statistics and metrics for Cisco WebEx Social node component categories

Step 4 In the Fetch last field, enter the number of units for which you want to view metrics, and select the units for which you want to view metrics (**minutes**, **hours**, **days**, **weeks**, or **months**).

Step 5 Take either of these actions:

- If you selected the **Dashboard** tab, take either of these actions in the menu tree:
  - Check the box next to a node category to see combined statistics and metrics for all nodes of that type.
  - Expand a node type so see a list of individual nodes of that type, then check the box next to a node for which you want to view statistic and metrics. If you check the box for more than one node, combined statistics and metrics for those nodes are displayed.
- If you selected the **Raw** tab, Use the Select Metrics menu tree to expand the component categories for which you want to view statistics and metrics. When you reach the node level, check the box that appears in front of each component for which you want to view statistic and metrics.

The metrics information is displayed in the graph in the main portion of the screen.

Application: Portal

The Portal window provides areas for configuring a variety of items that relate to your Cisco WebEx Social deployment. The following sections describe these areas:

- Compliance Officer Email, page 5-14
- Error Reporting, page 5-14
- Welcome Post Configuration, page 5-15
- Email Digest, page 5-15
- Proxy Settings, page 5-18
- Advanced Portal Properties, page 5-20

Compliance Officer Email

Use the options in the Compliance Officer Email Area in the Portal window to configure how you want e-mails from a compliance officer to appear when they are sent to users.

To configure the compliance officer e-mail, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Portal** under Application.

Step 3 In the Compliance Officer Email area, take these actions:

a. In the Name field, you can leave the default "Compliance Manager" or change it to a different name. A user sees this name when receiving an e-mail from the company compliance officer.

b. In the Address field, enter the e-mail address of your compliance officer. A user sees this name when receiving an e-mail from the company compliance officer.

Step 4 Make sure that the default selection of **Compliance Officer** appear in the Role Name drop-down list.

Step 5 Click **Save**.

Related Topic

Compliance Officer Role, page 1-29

Error Reporting

Use the options in the Error Reporting area in the Portal window to configure actions that occur when a user clicks links in the Cisco WebEx Social Help window. For related information, see the "Configuring Items in the Help Window" section on page 1-8.

The Error Reporting area includes these fields:

- Portal Help Link—Not used
- Send Feedback Link—Page that appears when users click the **Send Feedback** link in the Cisco WebEx Social Help Window
- System Admin Guide Link—Page that appears when users click the **See system admin guide** link in the Cisco WebEx Social Help Window
- Portal Feedback Link—Not used
- Tutorial Videos Link—Page that appears when users click the **View Tutorial Videos** link in the Cisco WebEx Social Help Window

If you make changes to any of these fields, make sure to click the **Save** button in the Error Reporting area to save your changes.

Welcome Post Configuration

Use the options in the Welcome Post Configuration area in the Portal window to set up a welcome post that you want to appear in the library of a each new Cisco WebEx Social user. You can designate the name that users see as the creator of the post, the title of the post, and the text of the post.

To set up a welcome post for new Cisco WebEx Social users, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Click **Portal** under Application.

Step 3 In the Welcome Post Configuration area, take these actions:

a. In the Admin First Name field, enter the first name of the system administrator.

This name and the last name that you enter in the next field appear as the creator of the post.

b. In the Admin Last Name field, enter the last name of the system administrator.

c. In the Post Title field, enter the title of the post.

d. In the Post Body field, enter the text of the post in HTML format.

e. Click **Save**.

Email Digest

Use the options in the Email Digest area in the Portal window to set up the e-mail integration feature. E-mail integration can include the following:

- Digest notification (also called *WebEx Social Activity Snapshot*)—An e-mail message that contains a summary of Cisco WebEx Social activities that a user is interested in. A digest notification 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).
- Instant notification—An e-mail notification that is sent to a user immediately after certain actions occurs in Cisco WebEx Social. For example if User A starts to follow User B, mentions User B, or shares a post with User B, User B receive an instant notification of the action.
- Inbound e-mail—Allows users to create content in Cisco WebEx Social by replying to some instant notifications. For example if you reply by e-mail to an @mention e-mail notification, you create a comment on this update in Cisco WebEx Social just as if you created the comment through the Cisco WebEx Social user interface.

  To enable Inbound e-mail, Cisco WebEx Social creates unique, auto-generated e-mail addresses for communities and discussion categories. The domain in which these email address are set as described in the procedure in this section. in addition to the configuration that the procedure describes, you must configure your DNS server so that it knows how to route e-mail addressed to auto-generated Cisco WebEx Social email addresses. To do so, create these resources:

  – A forward zone for your mail domain.

– An MX record in your new forward zone for the Worker node. If you have multiple Worker nodes you can add an MX record for each of them, which will also enable DNS load balancing.

To configure e-mail integration parameters, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Click **Portal** under Application.

Step 3 In the Email Digest area, take these actions:

a. In the Mail Domain field, enter the SMTP domain of the Cisco WebEx Social application.

b. Check the **Enable Inbound Mail** box so that incoming e-mail adheres to Cisco WebEx Social policies and permissions.

If you do not check this box, incoming e-mail bounces.

c. Check the **Enable Expand Sender** or the **Mailing List** box to if you want Cisco WebEx to use the SMTP EXPN command to expand mailing lists to identify e-mail senders

Note The **Enable Failure Feedback** box is not used for e-mail digest notification.

d. In the Weekly Digest Notification Date (day:hh:mm:timezone) field, enter day of the week and the time and time-zone offset at which weekly e-mail digest notification is summary is sent each week.

e. In the Daily Digest Notification Time (hh:mm) field, enter the time at which a daily e-mail digest notification is summary is sent each day. A setting of **0 0** indicates midnight.

f. In the Mail Networks field, enter a list of IP addresses of client servers that can use the Postfix Mail Transfer Agent (MTA) for e-mail messages.

At a minimum, enter the IP addresses of the App Server nodes and the Worker nodes in your deployment.

Separate multiple IP addresses with commas (,).

g. Click **Save**.

Configuring Properties for E-mail Integration

Table 5-4 describes the Cisco WebEx Social properties that control various items for the e-mail integration feature.

To change the value of a property, in the Director, click **Portal**, and in the Advanced Portal Properties area, locate the property and update its value. Then click **Save** in the Advanced Portal Properties area. (For related information, see the "Advanced Portal Properties" section on page 5-20.)

Table 5-4 Properties for E-mail Integration

Property	Explanation
mail.digest.notification.user-defaults	Set this property to **weekly** or **daily** to indicate the frequency at which the system sends e-mail digest notifications.

Table 5-4 Properties for E-mail Integration (continued)

Property	Explanation
mail.instant.notification.user-defaults	Set the property to any of combination of the following values to designate for what types of activities instant e-mail notifications will be sent. If you include multiple values, separate each one with a comma (,) only (do not include spaces). • **FOLLOW_ME** • **POST_MENTION** • **POST_SHARE** • **POST_SHARE_OTHER** • **POST_EDIT** • **POST_EDIT_CONTRIBUTED** • **POST_EDIT_WATCHLIST** • **COMMUNITY_JOIN_REQUEST** • **COMMUNITY_CREATE_REQUEST** • **COMMUNITY_ROLE_CHANGED** • **COMMUNITY_INVITE_ME** • **COMMUNITY_REQUEST_MEMBERSHIP**
outbound.email.from.address	Set this property to the e-mail address of the outbound e-mail notification sender. The default value is empty. In this case, the sender e-mail address is **noreply@*mail_domain***, where *mail_domain* is the value that you defined in the Mail Domain field as described in the "Email Digest" section on page 5-15.
outbound.email.from.name	Set this property to the name of the outbound e-mail notification sender. The default value is **Cisco WebEx Social**.
outbound.enabled	Set this property to **true** to enable outbound e-mail.
users.form.my.account.email-notifications	Set this property to **email-notifications-quad** and restart the App Server node if you want the **Email Notifications** selection to be available to users on their My Account pages. If you leave this property blank, the **Email Notifications** selection is not available on the My Account pages.
users.form.update.email-notifications	Set this property to **email-notifications-quad** and restart the App Server node if you want the **Email Notifications** option to be available to administrators when they select Users from the Portal drawer. If you leave this property blank, the **Email Notifications** option is not available to administrators on the Portal > Users page.

Table 5-4 Properties for E-mail Integration (continued)

Property	Explanation
worker.digestscheduler.isActive	Set this property to **true** to enable the scheduler for e-mail digest notifications.

Proxy Settings

Use the options in the Proxy Settings area in the Portal window to configure Cisco WebEx Social nodes to use an existing proxy server to access services that are outside of Cisco WebEx Social. You can then set up your Cisco WebEx Social nodes to communicate with remote servers via a proconfigured proxy server.

Cisco WebEx Social supports HTTP and HTTPS proxy to access remote servers and connects to the proxy server by using whichever protocol the proxy server requires. If the proxy supports both HTTP and HTTPS, Cisco first attempts to connect using by HTTP. If HTTP fails, Cisco WebEx Social attempts to connect by using the HTTPS settings.

The App Server nodes use the proxy or proxies that you configure.

Configuring Settings

To configure proxy settings. Be aware that this procedure causes App Server nodes to restart automatically.

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Portal** under Application.

Step 3 In the Proxy Settings area, take these actions:

a. Enter values for the fields that Table 5-5 describes.

b. Click **Save**.

The App Server nodes restart automatically.

Table 5-5 Proxy Settings

Parameter	Description
HTTP Settings	
Host/IP	Fully qualified domain name or IP address of the proxy server.
Port	Port on the proxy server that nodes in the Cisco WebEx Social environment use to communicate with the proxy. The typical port for HTTP communication is 80.
Username	User ID that the proxy server requires for authentication. Required if proxy server requires authentication.

Table 5-5 Proxy Settings (continued)

Parameter	Description
Password	Password that the proxy server requires for authentication. Required if proxy server requires authentication.
Authentication type	Drop-down list from which you select the authentication type that the proxy server uses. Select Basic or NTLM. (Required if proxy server requires authentication.)
Use the same settings for HTTPS	Checking this box populates the HTTPS (Secure) Settings fields with the same information that you entered in the HTTP Settings field.
HTTPS Settings	
Host/IP	Fully qualified domain name or IP address of the proxy server.
Port	Port on the proxy server that nodes in the Cisco WebEx Social environment use to communicate with the proxy. The typical port for HTTP communication is 8080.
Username	User ID that the proxy server requires for authentication. Required if proxy server requires authentication.
Password	Password that the proxy server requires for authentication. Required if proxy server requires authentication.
Authentication type	Drop-down list from which you select the authentication type that the proxy server uses. Select Basic or NTLM. (Required if proxy server requires authentication.)
Exceptions	
Exceptions	Host name or IP address of each node to which Cisco WebEx Social should connect directly. All nodes in your Cisco WebEx Social topology should be entered here so that request between them are not redirected to the proxy server. If you make multiple entries, separate each one with a pipe symbol (|). Do not include any spaces in this field. You can use an asterisk (*) in a host name or IP address as a wildcard to represent one or more characters. For example if all servers in the webexsocial-cisco.com domain should be connected directly from Cisco WebEx Social, you could enter *.webexsocial-cisco.com.

Disabling Proxy Settings

To stop using a proxy server, perform the following steps. Be aware that this procedure causes App Server nodes to restart automatically.

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Portal** under Application.

Step 3 In the Proxy area, take these actions:

a. Clear the values in all fields.

b. Click **Save**.

All proxies are removed and the App Server nodes restart automatically.

Advanced Portal Properties

The Advanced Portal Properties window allows various Cisco WebEx Social properties to be changed.

To change these properties, perform the following steps.

Caution Do avoid disrupting the operation of Cisco WebEx Social, update properties only when instructed to do so by Cisco technical support or when you are certain of the changes that you are making.

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Portal** under Application.

Step 3 To change a property, search or navigate to the property you want to change, and enter the new value in the Value field.

Step 4 Click **Save**.

The App Server nodes restart automatically.

Advanced Portal Properties for the Cisco WebEx Social API

The Advanced Portal Properties area in the Portal page of the Director includes properties that control the operation of the Cisco WebEx Social Application Programming Interface (API). Table 5-6 describes these properties.

Table 5-6 Advanced Portal Properties for Cisco WebEx Social API

Parameter	Description	Valid Values
quadapi.oauth.token-request-expire-ms	Number of milliseconds after it is created that a Request Token expires. This parameter applies to the Cisco WebEx Social API.	Valid values are integer 1 or greater. The default value is 300000 (5 minutes).
quadapi.oauth.token-access-expire-ms	Number of milliseconds after it is created that a Access Token expires. This parameter applies to the Cisco WebEx Social API.	Valid values are any integer. The default value is 1800000 (30 minutes). 0 means never expire.
quadapi.oauth.max-verifier-callback-count	Number of times that oauth_verification will be tried to be exchanged. After that, the exchange fails. This parameter applies to the Cisco WebEx Social API.	Valid values are any integer. The default value is 5.
quadapi.oauth.version	Specifies the OAuth version that is used for the Cisco WebEx Social API.	Must 1.0.
quadapi.auth.user-cache-expire-secs	Maximum number of seconds that user log in credentials are stored in cache. This parameter applies to the Cisco WebEx Social API.	Valid values are any integer. The default value is 600 (10 minutes).
quadapi.auth.allowBasicAuthentication	Designates whether to allow base 64 encoding for authentication of API calls	Valid values are true and false. The default value is true (allow base 64 encoding).
quadapi.auth.resourcesForBasic Authentication	Comma-separated list of resources for basic access authentication (user ID and password encoded with the base 64 algorithm)	Valid values are: • ROOT—Cisco WebEx Social API server resource. • management/apiconsumers—Designates the management/apiconsumer resource. • ALL—Makes all resources available by the Basic Access Authentication mechanism. By default, all resources other than those defined by ROOT and management/apiconsumers are protected by OAuth. The default value is ROOT,management/apiconsumers.
quadapi.auth.quad-oauth-header	Enables or disables the Oauth header. If enabled, the custom Apache header is used for OAuth signature validation.	Valid values are true and false. The default value is true (enables signature validation).

Table 5-6 Advanced Portal Properties for Cisco WebEx Social API (continued)

Parameter	Description	Valid Values
quadapi.common.events.allOn	Enables or disables the eventing framework.	Valid values are true and false. The default value is false (which disables the eventing framework).
quadapi.contextpath.root	Sets the root context path for API URIs. The value must be preceded with a slash (/).	The default value is /api/quad/rest.
quadapi.contextpath.url-rewrite-enabled	Enables or disables Cisco WebEx Social API URI rewrite.	Valid values are true and false. The default value is false (which disables Cisco WebEx Social API URI rewrite).
quadapi.auth.allowed_unauthenticated_methods	Reserved for future user.	—

Application: Security

The Security window provides areas for configuring a variety of items that relate to your Cisco WebEx Social deployment. The following sections describe these areas:

- Kerberos Properties, page 5-22
- SAML SSO, page 5-23
- WebEx SSO, page 5-24
- WebEx IM SSO, page 5-24
- Add New Trusted Certificate, page 5-25
- Trusted Certificates, page 5-25

Kerberos Properties

Kerberos is an authentication protocol that allows devices to communicate securely over a non-secure network. With Kerberos, user passwords are not circulated among nodes. Instead, only tickets are circulated.

You should configure Kerberos in Cisco WebEx Social deployments in which Kerberos is the authentication method for external applications. The Kerberos window provide options for performing this configuration.

Before You Begin

- Create a service principal name (SPN) for the Cisco WebEx Social load balancer on the Microsoft Active Directory server. For instructions, see your Microsoft Active Directory documentation.
- Create a service account in Microsoft Active Directory to be used to generate a keytab file.
- Use the SPN and service account that you created to generate a keytab file and name it *krb.keytab*. For instructions, see your Microsoft Active Directory documentation.

- Copy the keytab file that you generated to the */etc/kerberos/* folder on each App Server node. Create this directory if it does not exist.
- Make sure that each App Server node can access port 389 on the LDAP server.
- Make sure that each App Server node can reach the content repository server on the port that is configured for that server. See the "Content Repositories" section on page 2-58.
- LDAP must be configured in the Portal tab. See the "Authentication" section on page 2-40.
- Make Kerberos configuration settings in the Portal tab of the Control Panel. See the "Users" section on page 2-51.

To configure Kerberos on Cisco WebEx Social nodes, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Security** under Application.

Step 3 In the Kerberos area, take these actions:

a. Check the **Apply to App Server Nodes** box.

b. In the Server Name field, enter the host name of a Microsoft Active Directory server in your network.

   Cisco WebEx Social validates users by using tickets against this server.

c. In the Realm Name field, enter the Microsoft Active Directory realm for Kerberos.

   The value that you enter must be in all upper case letters.

   See your Kerberos documentation for additional information about realms.

d. In the Domain Name field, enter the Cisco WebEx Social domain name.

e. In the Service Name field, enter the name of the service principal for the Cisco WebEx Social load balancer

f. In the Service Account Name field, enter the user name for the service account that is defined in Microsoft Active Directory for the Cisco WebEx Social load balancer SPN.

g. In the Service Account Password field, enter the password for the service account that is defined in Microsoft Active Directory for the Cisco WebEx Social load balancer SPN.

h. Click **Save**.

The HTTP service on the App Nodes restarts automatically.

SAML SSO

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

WebEx SSO

Use the options in the WebEx SSO area in the Security window to configure the WebEx single sign-on (SSO) parameters.

To configure the WebEx SSO parameters, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Security** under Application.

Step 3 In the WebEx SSO area, take these actions:

a. Enter values for the fields that Table 5-7 describes.

b. Click **Save**.

The App Server nodes restart automatically.

Table 5-7 WebEx SSO Parameters

Item	Description
WebEx SSO Area	
For detailed information about configuring WebEx, see the "WebEx Site" section on page 3-39.	
Keystore File	Keystore file that you are using for WebEx. Use the **Choose File** button to locate and select the keystore file.
Keystore Password	Password for the keystore that you are using for WebEx.
Key Password	Password for the key that you are using for WebEx.

WebEx IM SSO

Use the options in the WebEx IM SSO area in the Security window to configure the WebEx IM single sign-on (SSO) parameters.

To configure the WebEx IM SSO parameters, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Security** under Application.

Step 3 In the WebEx IM SSO area, take these actions:

a. Enter values for the fields that Table 5-8 describes.

b. Click **Save**.

The App Server nodes restart automatically.

Table 5-8 WebEx IM SSO Parameters

Item	Description
WebEx IM SSO Area	
For detailed information about configuring WebEx IM, see the "Using WebEx IM for Chat and Presence" section on page 3-19.	
Keystore Path	Keystore file that you are using for WebEx IM. Use the **Choose File** button to locate and select the keystore file.
Keystore Password	Password for the keystore that you are using for WebEx IM.
Key Password	Password for the key that you are using for WebEx IM.
SSO Alias	Key alias to be used for WebEx SSO.

Add New Trusted Certificate

Use the options in the Add New Trusted Certificate area in the Security window to add a new trusted certificate to Cisco WebEx social. A trusted certificate is a third-party certificate that you can use instead of a self-signed certificate. When you add a trusted certificate, it is saved to a local database and appears in the Trusted Certificates area in the Security window, but it is not deployed. To deploy a trusted certificate, see the "Trusted Certificates" section on page 5-25.

To add a new trusted certificate, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Security** under Application.

Step 3 In the Add New Trusted Certificate area, take these actions:

a. In the Alias field, enter the alias to be used for the trusted certificate.

b. In the Trusted Certificate field, click the Browse button to browse your local computer for the trusted certificate file. Select the file and click **Open**.

The name of the certificate is displayed in the Trusted Certificate field.

c. Click **Save**.

Trusted Certificates

Use the options in the Trusted Certificates area in the Security window to deploy and delete trusted certificates.

When you deploy trusted certificates, the following events occur:

- The certificates are pushed to each App Server node and appended to the existing certificates file on each node
- The App Server nodes and the Notifier nodes restart

When you delete a trusted certificate, it is removed from Cisco WebEx Social.

The Trusted Certificates lists each trusted certificate that has been added to Cisco WebEx Social, and displays the alias, subject, issuer, and expiration date and time of each one.

Deploying Trusted Certificates

Before you can deploy a trusted certificate, it must be added to Cisco WebEx social as described in the "Add New Trusted Certificate" section on page 5-25.

To deploy trusted certificates, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Security** under Application.

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

All certificates in the Trusted Certificates area are deployed.

Deleting a Trusted Certificates

To delete a trusted certificate, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Security** under Application.

Step 3 In the Trusted Certificates area, click the **Delete** button in the Actions column for the trusted certificate to delete.

Application: Integration

The Integration window provides areas for configuring a variety of items that relate to your Cisco WebEx Social deployment. The following sections describe these areas:

SharePoint (Native)

Use the options in the SharePoint area to make some configuration settings that are required when Microsoft 2007 SharePoint is to be used as a document repository.

For more detailed information about repositories and SharePoint, see the "Content Repositories" section on page 2-58.

Before You Begin

Configure SharePoint as described in the "Content Repositories" section on page 2-58.

To configure SharePoint, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Integration** under Application.

Step 3 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 to connect.

The URL should be in this format:

http://*sharepoint_host*/*sharepoint_site*/*document_library*

where:

- *sharepoint_host*—IP address host name of the SharePoint server or farm.
- *sharepoint_site*—Name of the SharePoint sites. You can include subsite names. If you specify subsites, separate each site with a slash (/).
- *document_library*—Name of the document library.

The following example shows a URL that includes one site:

```
http://mysharepointhost/mysharepointsite/mydocumentlibrary
```

The following example shows a URL that includes a subsite:

```
http://mysharepointhost/mysharepointsite/
mysharepointsubsite/mydocumentlibrary
```

c. Click **Save**.

The App Server nodes restart automatically.

WSRP Settings

Use the options in the WSRP Settings area in the Integration window to configure the Web Services for Remote Portlets (WSRP) cluster link in your Cisco WebEx Social topology.

For detailed information about implementing WSRP, see the "WSRP" section on page 2-56.

Table 5-9 describes the parameters in the WSRP Settings area.

Table 5-9 WSRP Settings

Parameter	Description
Cluster Link Enabled	Checking this check enables the cluster link
Autodetect Address	IP address of the WSRP cluster link gateway

Chat Proxy

Use the option in the Chat Proxy area in the Integration window to configure the chat proxy settings. A chat proxy enables Cisco WebEx Social to communicate with a chat server.

To configure the chat proxy settings, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Integration** under Application.

Step 3 In the Chat Proxy area, take these actions:

a. In the Chat Proxy URL field, enter the following, as appropriate:

- If you are using Cisco Unified Presence (CUP) or WebEx IM for chat and presence, enter the BOSH binding URL
- If you are using Microsoft OCS for chat and presence, enter the URL of the CWC client
- If you are using IBM Lotus SameTime for chat and presence, enter the URL of the SameTime proxy server

b. From the Server Type drop-down list, select the type of chat proxy server to be used:

- If you are using CUP, WebEx IM, or Microsoft OCS for chat and presence, select **default**
- If you are using IBM Lotus SameTime for chat and presence, select **sametime**

c. Click **Save**.

APPENDIX A

Modifying Default Layouts and Creating a Custom Template

As community owner or system administrator, you can change the default layout of several pages of Cisco WebEx Social for your users. You can also create custom templates.

This appendix contains the following topics:

Creating a Custom Community Template

To change the default layout of a template for a community (open, restricted, or hidden), follow these steps:

Procedure

Step 1 Create a new community of the type you want to modify (open, restricted or hidden). For instructions, see the "Adding a Community" section on page 2-11.

Step 2 Add or remove applications in the community as desired.

Step 3 From a community Home page, click the Change Layout icon .

Step 4 Click **Advanced page management**.

Step 5 Select the **Pages** tab from the list of tabs near the top of the screen.

Step 6 Select the **Pages** tab under the text "Edit Pages for Community: *community_name*."

Step 7 Click the **Export/Import** tab.

Step 8 In the provided space, enter the name of the LAR file as follows depending on the community type:

- Community_template_open.lar (for open communities)
- Community_template_restricted.lar (for restricted communities)
- Community_template_private.lar (for hidden communities):

Step 9 Select checkboxes for the items you want to export.

These items will be exported from the layout of the Community that you chose to the LAR file that you entered.

Step 10 Click the **Export** button at the bottom of the page.

The new LAR file is created.

Step 11 If you are prompted to save the LAR file, save the file in the location of your choice.

Creating a Custom Home Page Template

To create a custom template to be used for the Home page of users, follow these steps:

Procedure

Step 1 Go to the Home page of an administrator.

Step 2 Add or remove applications in the Home page as desired.

Step 3 Click the Change Layout icon .

Step 4 Click **Advanced page management**.

Step 5 Click the **Export/Import** tab.

Step 6 In the provided space, enter the name of the LAR file as follows:

MyView_default_layout.lar

Step 7 Select checkboxes for the items you want to export.

These items will be exported from the layout of the Home that you chose to the LAR file.

Step 8 Click the **Export** button at the bottom of the page.

The new LAR file is created.

Step 9 If you are prompted to save the LAR file, save the file in the location of your choice.

Step 10 Click the down-arrow to the right of your name in the Global Navigation bar and select **Account Settings from** the drop-down menu.

Step 11 Take either of these actions:

- To import the Home page settings for a specific user:
  1. Click the right-arrow next to **Portal**.
  2. Click **Users** in the Portal drawer.
  3. In the Users window, select the desired user.
  4. From the Actions drop-down menu next to the user, select **Manage Pages**.
  5. Select the **Home Pages** tab.
  6. Select the **Export/Import** tab.
  7. Select the **Import** tab.
  8. In the **Import a LAR file to overwrite the selected data** field, click **Browse** and navigate to and select MyView_default_layout.lar file.
  9. Check the boxes for the options that you want to import.

10. Click the **Import** button.

- To import the Home page settings for all users:
  1. Click the right-arrow next to **My Settings**.
  2. Click **Manage Pages** in the My Settings drawer.
  3. Select the **Home Pages** tab.
  4. Select the **Export/Import** tab.
  5. Select the **Import** tab.
  6. In the **Import a LAR file to overwrite the selected data** field, click **Browse** and navigate to and select MyView_default_layout.lar file.
  7. Check the boxes for the options that you want to import.
  8. Click the **Import All (Users)** button.

     It can take some time for all information to be imported, depending on the number of users. Do not close your browser until you see a message that indicates that the process has completed.

Creating a Custom Profile Page Template

To create a custom template to be used for the Profile page of users, follow these steps:

Procedure

Step 1 Go to the Profile page of an administrator.

Step 2 Add or remove applications in the Featured Content tab as desired.

Step 3 Click the right-arrow next to **My Settings**.

Step 4 Click **Manage Pages** in the My Settings drawer.

Step 5 Select the **Profile Pages** tab.

Step 6 Select the **Pages** tab.

Step 7 Click the **Export/Import** tab.

Step 8 Click the **Export** tab.

Step 9 In the provided space, enter the name of the LAR file as follows:

MyProfile_default_layout.lar

Step 10 Select checkboxes for the items you want to export.

These items will be exported from the layout of the Home that you chose to the LAR file.

Step 11 Click the **Export** button at the bottom of the page.

The new LAR file is created.

Step 12 If you are prompted to save the LAR file, save the file in the location of your choice.

Step 13 Take either of these actions:

- To import the Profile page settings for a specific user:
  1. Click the right-arrow next to **Portal**.
  2. Click **Users** in the Portal drawer.
  3. In the Users window, select the desired user.
  4. From the Actions drop-down menu next to the user, select **Manage Pages**.
  5. Select the **Profile Pages** tab.
  6. Select the **Export/Import** tab.
  7. Select the **Import** tab.
  8. In the **Import a LAR file to overwrite the selected data** field, click **Browse** and navigate to and select MyProfile_default_layout.lar file.
  9. Check the boxes for the options that you want to import.

     Make sure the **Permissions** box is not checked.
  10. Click the **Import** button.
- To import the Profile page settings for all users:
  1. Click the right-arrow next to **My Settings**.
  2. Click **Manage Pages** in the My Settings drawer.
  3. Select the **Profile Pages** tab.
  4. Select the **Export/Import** tab.
  5. Select the **Import** tab.
  6. In the **Import a LAR file to overwrite the selected data** field, click **Browse** and navigate to and select MyProfile_default_layout.lar file.
  7. Check the boxes for the options that you want to import.

     Make sure the **Permissions** box is not checked.
  8. Click the **Import All (Users)** button.

     It can take some time for all information to be imported, depending on the number of users. Do not close your browser until you see a message that indicates that the process has completed.

INDEX

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W