C H A P T E R 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:

- Metrics Initialization, page 3-7
- Session Settings, page 3-7

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.

Table 3-1   Resources Tab Actions (continued)

Action	Result and When to Execute
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.
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 set or reset logging levels for the App Server, and Worker nodes in your Cisco WebEx Social cluster.

This section contains the following topics:

- Locating Log Files, page 3-5

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 Take one of the following of actions to set or reset log levels for a single node or for all App Server and Worker nodes in your deployment:

- To set log properties for a particular node in your Cisco WebEx Social topology:

  a. Select the desired node from the **Selected Node** drop-down list.

  b. Click **Go** to display the current settings for the that node.

  c. In the list of groups, select the desired logging level for each item in the Group column from the corresponding drop-down list in the Level column. Use the Right Arrow, Left Arrow, or page number buttons at the bottom of the list to see other pages in the list.

  d. Click the **Apply** button at the bottom of the window.

- To set log properties for all App Server and Worker nodes:

  a. In the list of groups, select the desired logging level for each item in the Group column from the corresponding drop-down list in the Level column. Use the Right Arrow, Left Arrow, or page number buttons at the bottom of the list to see other pages in the list.

  b. Click the **Apply All** button at the bottom of the window.

- To reset log properties for a particular node to their default values:

  a. Select the desired node from the **Selected Node** drop-down list.

  b. Click the **Reset** button at the bottom of the window.

- To reset log properties for all App Server and Worker nodes their default values, click the **Reset All** button at the bottom of the window.

For a description of groups for which you can set log levels, click the **Category Help Page** link.

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.

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.

In this tab, file sizes are in bytes and thumbnail dimensions are in pixels.

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 email 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 email 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

If SMTP authentication is being used, a Cisco WebEx Social account with user ID and password must be set up on the outgoing SMTP server. This configuration allows Cisco WebEx Social to communicate with the server and enable message board posts and user 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
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 regarding whether to check this box to enable SMTPS. Microsoft Exchange Server does not support this protocol. Do not check this box if you are using SMTP protocol.
User Name	User ID for SMTP authentication. Leave blank if SMTP authentication is not used.
Password	Password for SMTP authentication. Leave blank if SMTP authentication is not used.
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 Application > 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.

Session Settings

The Session Settings tab in the Server Administration window lets you configure the maximum number of times that any user can be logged in to Cisco WebEx Social concurrently. Because each log-in session consumes system resources, you can use this option to help manage system resources by limiting multiple concurrent login-ins by the same users.

Setting the Maximum number of concurrent sessions per user to a value of –1 causes the system to impose no limit on the number of times that any user can be logged in to Cisco WebEx Social concurrently.

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 2-53.

- 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 2-53.

- 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

Table 3-3 *Settings Options Plugins (continued)*

Parameter	Description
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
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
- Preferred Clients, page 3-30
- Notification Service, page 3-31
- Cisco Show And Share, page 3-33
- Voice Mail Server, page 3-34
- WebDialer, page 3-38
- WebEx Site, page 3-41

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 3-12

- 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 email 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 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 Application > Security window in the Director to delete imported certificates. For detailed instructions, see the, see the "Trusted Certificates" section on page 5-23.

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 **Application > Portal**.
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 and then click **Apply Config**.

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, select **Application > Portal** and in the Advanced Portal Properties area, locate the property and update its value. Then click **Save** in the Advanced Portal Properties area and click **Apply Config** in the left panel of the Director. (For related information, see the "Advanced Portal Properties" section on page 5-16.)

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

Table 3-7   Properties for Calendering (continued)

Property	Description	Default
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)
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 3-18
- 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, select **Application > Integration**, 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
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:

After you perform these steps, select Application > Integration 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.   Select **Application > Security**.

    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, select **Application > Integration** in the Director 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:

- Step 1: Configure Sametime in Cisco WebEx Social, page 3-28
- Step 2: Configure Client Priority in Sametime Community Server, page 3-29

After you perform these steps, select **Application > Integration** in the Director and select **sametime** from the Server Type drop-down list in the Chat Proxy area.

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**.

Preferred Clients

The Preferred Clients tab allows you to select the client that you want your users to use for the Click to Call and Click to Chat features when either of the following options is selected on the Chat tab:

- Cisco Unified Presence (CUP)
- WebEx IM

If you select the stand-alone client Cisco Jabber by using the procedure that this section describes, initiating a call or a chat session from within Cisco WebEx Social transfers the call or the chat session to Cisco Jabber.

Note See *Cisco WebEx Social Frequently Asked Questions* for OS-related, web browser-related, and other information when using Cisco Jabber as preferred client.

To configure a preferred client for Click to Call and Click to Chat, 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 **Preferred Clients** tab.

Step 3 Configure options as described in Table 3-14.

Step 4 Click **Save**.

Table 3-14   *Preferred Clients Configuration Options*

Parameter	Description
Select preferred client	Use this drop-down list to select a preferred client. Options include: • **WebEx Social Built-in**—Select this option if you want to use the default JavaScript web browser-based client that can handle both IM and voice and video calls (browser plug-in required for the latter) • **Cisco Jabber for Windows or Mac**—Select this option if you have the standalone Cisco Jabber client installed on user machines and you want to use it instead of the built-in client **Note** If you configure Cisco Jabber, instruct Cisco WebEx Social users to refresh their browsers after you save the configuration.
Allow the user to select an alternative client?	Select **No** if you want the client selection you made above to be the mandatory user option. Select **Yes** if you want to allow the user to decide for themselves, in which case the **Select preferred client** selection designates a default but non-mandatory option. **Note** If you set this option to **Yes** and select Cisco Jabber in the Select preferred client field, instruct Cisco WebEx Social users to refresh their browsers after you save the configuration.
Jabber for Windows download link	Type the URL where you placed the Jabber for Windows executable file download. This URL is used when the user selects to download the Jabber client from within Cisco WebEx Social. No download link is displayed if you leave this field empty. The URL must not exceed 512 characters or the download link becomes invalid.
Jabber for Mac download link	Type the URL where you placed the Jabber for Mac executable file download. This URL is used when the user selects to download the Jabber client from within Cisco WebEx Social. No download link is displayed if you leave this field empty. The URL must not exceed 512 characters otherwise the download link becomes invalid.

Notification Service

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

This section includes these topics:

- Synchronizing Notification Service, page 3-32
- Synchronization Buttons, page 3-32
- Adding a User to Notifier, page 3-32

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 5-7

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:

-
-

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 3-33 describes, follow these steps to add and deploy the required trusted certificate:

Procedure

Step 1   In the Director, select **Application > Security**.

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

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 3-35

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 3-37).

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 3-35).

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.

• By default, Cisco Unity Connection waits for four rings before dropping call. To change this value, select **Application > Portal** in the Director and in the Advanced Portal Properties area, locate the voicemail.ringtone.count property, and update its value. Then click **Save** in the Advanced Portal Properties area and click **Update Config**. (For related information, see the "Advanced Portal Properties" section on page 5-16.)

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 select **Application > Security**.

Step 8   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 9   In the Trusted Certificates area, click **Deploy Trusted Certificates**.

Step 10   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 3-37, 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 ![gear] 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

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 3-38
- Configuration Required if a Proxy Is Used in the Cisco WebEx Social Network, page 3-39
- Configuring WebDialer in Cisco WebEx Social, page 3-40
- User Selection and Testing of Phones, page 3-40

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 the Application > Portal page in the Director. For instructions, see the "Proxy Settings" section on page 5-14.

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 3-38.

 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 3-38.

 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.   Select **System > Topology**.

 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 3-41

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

- Step 2: Configuring Cisco WebEx Social for Cisco WebEx Meeting, page 3-43

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.   Select **Application > Security**.

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 3-41 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 3-44
- End-User Configuration, page 3-44

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 3-45
- De-Linking Your Twitter Account from Cisco WebEx Social, page 3-45
- Important Information for End Users, page 3-45

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 email 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.