CHAPTER 5

Director

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

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

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

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

This section includes these topics:

- System: Configuration, page 5-2
- System: Topology, page 5-8
- System: Software, page 5-10
- System: Health, page 5-12
- System: Stats, page 5-13
- Application: Portal, page 5-13
- Application: Security, page 5-22
- Application: Integration, page 5-26

System: Configuration

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

- Unified Access, page 5-2
- NFS, page 5-3
- NTP, page 5-4
- Notifier, page 5-4
- Analytics Store Cron Job, page 5-6
- Health and Diagnostics, page 5-7
- SNMP, page 5-7
- Outbound Email, page 5-7
- Console Login Banner, page 5-8

Unified Access

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

To configure the Unified Access parameters, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Configuration** under System.

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

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

b. Click **Save**.

Table 5-1 Unified Access Settings

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

Table 5-1 Unified Access Settings (continued)

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

NFS

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

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

To configure this NFS mount point, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Configuration** under System.

Step 3 In the NFS area, take these actions:

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

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

/exported_root_folder

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

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

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

d. Click **Save**.

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

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

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

NTP

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

To configure NTP, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Configuration** under System.

Step 3 In the NTP area, take these actions:

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

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

c. Click **Save**.

Notifier

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

To configure the Notifier, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Configuration** under System.

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

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

Table 5-2 Notifier Settings

Parameter	Description
LDAP Settings	

Table 5-2 Notifier Settings (continued)

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

Table 5-2 Notifier Settings (continued)

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

Analytics Store Cron Job

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

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

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

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Configuration** under System.

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

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

b. Click **Save**.

Health and Diagnostics

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

To configure email IDs, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Configuration** under System.

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

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

b. Click **Save**.

SNMP

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

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

To configure the SNMP community string, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Configuration** under System.

Step 3 In the SNMP area, take these actions:

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

b. Click **Save**.

Outbound Email

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

To configure the Outbound Email parameters, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Configuration** under System.

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

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

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

c. Click **Save**.

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

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

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

b. Click **Save**.

Console Login Banner

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

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

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Configuration** under System.

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

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

b. Click **Save**.

System: Topology

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

- Provision New Server, page 5-8
- Server List, page 5-9

Provision New Server

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

To provision a server, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Topology** under System.

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

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

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

Step 5 Click **Add**.

Server List

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

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

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

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

Table 5-3 Server List Information and Controls

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

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

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

System: Software

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

The following sections describe these areas:

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

SCP File Upload

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

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

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

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Software** under System.

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

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

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

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

Step 7 Click **Upload**.

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

Upgrade

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

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

To perform a software upgrade, follow these steps.

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Software** under System.

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

Step 4 Click **Upgrade**.

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

System: Health

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

Downloading Log Files

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

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Health** under System.

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

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

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

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

d. Click **Download**.

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

Step 4 Click **Upgrade**.

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

Viewing Health Status

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

Service status is divided into these categories:

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

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

The health status includes the following information for each service:

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

System: Stats

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

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Stats** under System.

Step 3 Select either of these tabs:

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

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

Step 5 Take either of these actions:

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

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

Application: Portal

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

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

Compliance Officer Email

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

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

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Portal** under Application.

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

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

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

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

Step 5 Click **Save**.

Related Topic

Compliance Officer Role, page 1-29

Error Reporting

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

The Error Reporting area includes these fields:

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

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

Welcome Post Configuration

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

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

Procedure

Step 1 Sign in to the Director.

Step 2 Click **Portal** under Application.

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

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

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

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

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

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

e. Click **Save**.

Email Digest

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

- Digest notification (also called *WebEx Social Activity Snapshot*)—An e-mail message that contains a summary of Cisco WebEx Social activities that a user is interested in. A digest notification can include information about new followers, posts, community memberships, and community discussions that apply to the user. Users can receive digest notifications daily (these notifications include a summary of activities that occurred that day) or weekly (these notifications include a summary of activities that occurred the past week).
- Instant notification—An e-mail notification that is sent to a user immediately after certain actions occurs in Cisco WebEx Social. For example if User A starts to follow User B, mentions User B, or shares a post with User B, User B receive an instant notification of the action.
- Inbound e-mail—Allows users to create content in Cisco WebEx Social by replying to some instant notifications. For example if you reply by e-mail to an @mention e-mail notification, you create a comment on this update in Cisco WebEx Social just as if you created the comment through the Cisco WebEx Social user interface.

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

  – A forward zone for your mail domain.

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

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

Procedure

Step 1 Sign in to the Director.

Step 2 Click **Portal** under Application.

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

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

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

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

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

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

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

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

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

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

Separate multiple IP addresses with commas (,).

g. Click **Save**.

Configuring Properties for E-mail Integration

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

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

Table 5-4 Properties for E-mail Integration

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

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

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

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

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

Proxy Settings

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

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

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

Configuring Settings

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

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Portal** under Application.

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

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

b. Click **Save**.

The App Server nodes restart automatically.

Table 5-5 Proxy Settings

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

Table 5-5 Proxy Settings (continued)

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

Disabling Proxy Settings

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

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Portal** under Application.

Step 3 In the Proxy area, take these actions:

a. Clear the values in all fields.

b. Click **Save**.

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

Advanced Portal Properties

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

To change these properties, perform the following steps.

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

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Portal** under Application.

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

Step 4 Click **Save**.

The App Server nodes restart automatically.

Advanced Portal Properties for the Cisco WebEx Social API

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

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

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

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

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

Application: Security

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

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

Kerberos Properties

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

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

Before You Begin

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

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

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

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Security** under Application.

Step 3 In the Kerberos area, take these actions:

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

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

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

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

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

   See your Kerberos documentation for additional information about realms.

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

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

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

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

h. Click **Save**.

The HTTP service on the App Nodes restarts automatically.

SAML SSO

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

WebEx SSO

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

To configure the WebEx SSO parameters, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Security** under Application.

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

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

b. Click **Save**.

The App Server nodes restart automatically.

Table 5-7 WebEx SSO Parameters

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

WebEx IM SSO

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

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

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Security** under Application.

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

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

b. Click **Save**.

The App Server nodes restart automatically.

Table 5-8 WebEx IM SSO Parameters

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

Add New Trusted Certificate

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

To add a new trusted certificate, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Security** under Application.

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

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

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

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

c. Click **Save**.

Trusted Certificates

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

When you deploy trusted certificates, the following events occur:

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

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

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

Deploying Trusted Certificates

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

To deploy trusted certificates, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Security** under Application.

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

All certificates in the Trusted Certificates area are deployed.

Deleting a Trusted Certificates

To delete a trusted certificate, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Security** under Application.

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

Application: Integration

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

- SharePoint (Native), page 5-26
- WSRP Settings, page 5-27
- Chat Proxy, page 5-28

SharePoint (Native)

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

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

Before You Begin

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

To configure SharePoint, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Integration** under Application.

Step 3 In the SharePoint (Native) area, take these actions:

a. Check the **SharePoint Integration Enabled** box.

b. In the SharePoint URL field, enter the URL of the SharePoint site document library to which Cisco WebEx Social is to connect.

The URL should be in this format:

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

where:

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

The following example shows a URL that includes one site:

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

The following example shows a URL that includes a subsite:

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

c. Click **Save**.

The App Server nodes restart automatically.

WSRP Settings

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

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

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

Table 5-9 WSRP Settings

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

Chat Proxy

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

To configure the chat proxy settings, follow these steps:

Procedure

Step 1 Sign in to the Director.

Step 2 Select **Integration** under Application.

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

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

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

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

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

c. Click **Save**.