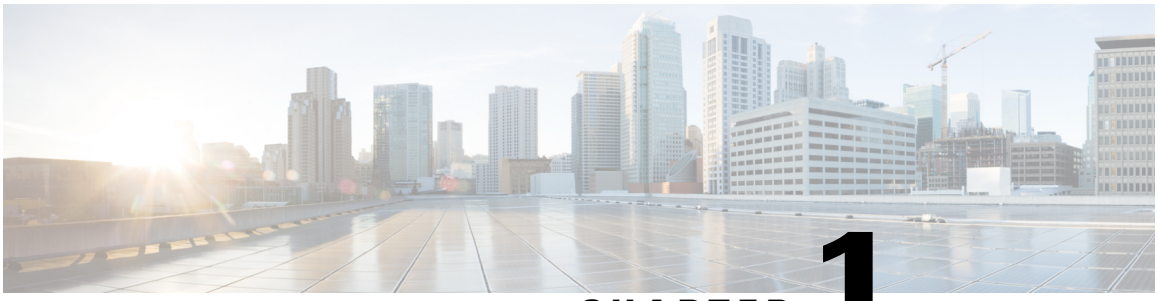
Cisco WebEx Messenger Administration Guide

First Published: 2015-03-05

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

CONTENTS



CHAPTER 1

Cisco WebEx Administration Tool

Overview

The Cisco WebEx Messenger Administration Tool enables Organization Administrators to monitor, manage, control, and enhance user access to Cisco WebEx. The Cisco WebEx administrator is known as the Organization Administrator. The Organization Administrator controls what features are available to Cisco WebEx users and determines how they can use these features.

Important The Cisco WebEx Connect service has been rebranded as Cisco WebEx Messenger. The Cisco WebEx Administration Tool will be updated shortly to reflect this change.

The client application is branded as Cisco Jabber.

This section includes a summary of tasks to quickly get started using the Cisco WebEx Messenger Administration Tool.

Note Customers with Single Sign-On or Directory Integration enabled need to contact a Cisco WebEx representative for assistance in getting started with launching Cisco WebEx Messenger Administration Tool.

Desktop Requirements

The following are the minimum and recommended desktop requirements to install and run the following Cisco WebEx Applications:

Cisco Jabber for Windows

Please refer to the Cisco Jabber Windows application documentation (http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/tsd-products-support-series-home.html) for the minimum and recommended desktop requirements to install and run the Cisco Jabber application.

Cisco Jabber for Mac

Please refer to the Cisco Jabber Mac application documentation (http://www.cisco.com/en/US/products/ps11764/prod_release_notes_list.html) for the minimum and recommended desktop requirements to install and run the Cisco Jabber application.

Cisco Jabber Mobile Clients

Please refer to the following Cisco Jabber Mobile applications documentation for the minimum and recommended desktop requirements to install and run the Cisco Jabber applications.

- Cisco Jabber for iPhone and iPad:
  http://www.cisco.com/c/en/us/support/customer-collaboration/jabber-iphone-ipad/tsd-products-support-series-home.html
- Cisco Jabber for Android:
  http://www.cisco.com/c/en/us/support/unified-communications/jabber-android/tsd-products-support-series-home.html

Network Requirements

The following network requirements are required to access the Cisco WebEx Messenger service. The application computer must have Internet connectivity and be able to connect to the following hosts and ports.

Note: Cisco WebEx Jabber application uses the Web Proxy information configured in Internet Explorer to access the application configuration service. If the proxy in the customer network is an authenticated proxy, the proxy is appropriately configured to allow access to this URL without requiring any authentication.

Domains

You need to open connectivity over ports 80 and 443 for the following domains:

- webex.com
- webexconnect.com
- The sub-domains of above: *.webex.com and *.webexconnect.com.

  If you intend to use third-party XMPP applications such as http://adium.im, you need to open port 5222 as well. For more information about using third-party XMPP applications, see Third Party XMPP IM Application Support, on page 6.

Certificate Revocation List (CRL) Domains

The Cisco Jabber clients check x509 CRLs or use online certificate status protocol (OCSP) when establishing TLS connections to the servers. These lists are obtained by following URL addresses embedded in the x509 certificate. These URLs are controlled by the certificate issuing authorities.

Cisco periodically updates these x509 certificates and changes certificate authorities due to normal maintenance or security concerns and reserves the right to change certificates and certificate authorities without notification.

Below is the current list of certificate provider domains which should be white-listed in firewall rules:

- *.verisign.com
- *.comodo.com
- *.usertrust.com
- *.cisco.com

IP Ranges

WebEx services are offered over the following IP ranges:

- 64.68.115.0 - 64.68.115.255
- 64.68.116.0 – 64.68.116.255
- 66.163.32.0 – 66.163.63.255
- 209.197.192.0 - 209.197.223.255
- 173.243.12.0 - 173.243.12.255 (Subnet)

It is generally not recommended to restrict access based on IP ranges as WebEx may acquire new IP addresses or reassign IP addresses.

To receive notifications from Cisco WebEx, set your SPAM Filter to allow emails from mda.webex.com. Notifications typically include important information about new Cisco WebEx accounts, password resets and similar information, communicated to users through emails.

Audio-Video Firewall and Bandwidth Requirements

This section lists the recommended port and bandwidth requirements for the Video sessions initiated from the Cisco WebEx Jabber application.

P2P refers to the ability to make Jabber to Jabber calls.

In general, audio and video functionality is offered over the following ports:

Item	Port Type	Port Number
A/V Server port	TCP	80 and 443
	UDP	5101
STUN server	TCP	80
	UDP	8070/8090

Item	Port Type	Port Number
P2P port/audio and video media/Jabber to Jabber Calling	TCP	Random (not supported)
	UDP	Default 32434-33598 (entire range)

Note If you choose a different port range for Jabber to Jabber calling, you must change the port range in the Cisco WebEx Messenger Administration tool and then open the company network ports based on those changes.

Sign in to the WebEx Messenger Administration tool, select **P2P Settings** > **Configure Ports Manually**.

The UDP port 5101 is used to establish the server connection. If the connectivity fails, ports 80/443 are used to establish connectivity.

Jabber to Jabber calling always uses UDP ports it will never default to TCP ports.

For more information on the hostnames required for Jabber to Jabber calling, HTTP, and URLs, see https://support.ciscospark.com/customer/en/portal/articles/1911657-firewall-and-network-requirements-for-the-cisco-spark-app

Bandwidth Requirement for Video

Resolution	Jabber to Jabber Calling Bandwidth	Remarks
90p	0~120kbps	Additional bandwidth may be consumed if severe packet loss is detected. This will compensate for lost packets.
180p	120~360kbps	Additional bandwidth may be consumed if severe packet loss is detected in order to compensate for lost packets.
360p	360~1200kbps	Actual resolutions include 360p, 432p, and 512p. Additional bandwidth may be consumed if severe packet loss is detected. This will compensate for lost packets.
720p	1200kbps~2000kbps	Actual resolutions include 576p and 720p. Additional bandwidth may be consumed if severe packet loss is detected. This will compensate for lost packets.

Jabber to Jabber calling leverages the Cisco Spark platform. As a result, customers must open the Media Cisco hybrid services UDP port range settings to use Jabber to Jabber calling. The spark platform network and firewall settings can be found here: https://support.ciscospark.com/customer/en/portal/articles/1911657-firewall-and-network-requirements-for-the-cisco-spark-app?b_id=8722

Any customer that wants to enable Jabber to Jabber calling needs to have their organization synced with the Cisco Common Identity system, which controls access to the Spark platform. Contact your Customer Success Manager for information or assistance.

WebEx with Other IM Providers

Cisco WebEx Messenger can federate with users of leading instant messaging providers such as AIM, IBM Lotus Sametime, Microsoft Lync, and XMPP-based IM networks like GoogleTalk and Jabber.org. A list of public XMPP-based IM networks is available at the XMPP Standards Foundation website: http://xmpp.org/services.

Federation with XMPP-based IM networks or IM solutions that support XMPP

Federation between Cisco WebEx and XMPP-based Instant Messaging networks or IM solutions that support XMPP requires the publishing of a Service (SRV) record in DNS. Examples of XMPP-based IM networks include Google Talk, and Jabber.org. For more information on enabling XMPP federation, refer to Specifying IM Federation settings.

The following example shows how XMPP federation is provisioned for an organization called acme.com.

If acme.com wants federation with external domains (domains not within the Cisco WebEx Collaboration cloud), it publishes the following Service (SRV) records in DNS:

```
_xmpp-server._tcp.acme.com. 86400 IN SRV 5 0 5269 s2s.acme.com.webexconnect.com
```

Note The SRV records for your domain can be found in **IM Federation** under the **Configuration** tab. For more information, see Specify IM Federation Settings.

The TCP port, 5269 should be open to enable XMPP federation.

Configuring a DNS server sample

The following are sample IM Federation settings for each of the options available:

- SRV (Service):
- Service = _xmpp-server
- Protocol = _tcp
- Name = acme.com (domain name)
- Priority = 5
- Weight = 0
- Port = 5269
- Target = s2s.acme.com.webexconnect.com

Requiring encryption with Federation

If encryption is required then this can only be accomplished by using the NextPlane service.

Federating with the AOL IM Network

Cisco WebEx Messenger can federate with AOL's IM network. Contact your Cisco WebEx account representative if you would like to federate with AOL's IM network.

Federating with IBM Lotus Sametime

Note We recommend you use NextPlane federation services to federate between Cisco WebEx Messenger and IBM Lotus Sametime.

Cisco does not provide support for the IBM Lotus Sametime XMPP Gateway. This is due to numerous known issues that exist with the Gateway, and our inability to provide support for another company's product.

Federating with Microsoft Lync

Note We recommend you use NextPlane federation services to federate between Cisco WebEx Messenger and Microsoft Lync.

Cisco does not provide support for the Migrosoft Lync XMPP Gateway. This is due to numerous known issues that exist with the gateway, and our inability to provide support for another company's product.

Third Party XMPP IM Application Support

Instead of the Cisco Jabber for Windows application, third party applications (for example, Pidgin for Linux) that support XMPP can also be used for basic IM communication. However, organization policies cannot be enforced on third party XMPP applications. Additionally, features such as end-to-end encryption, desktop sharing, video calls, computer-to-computer calls, and teleconferencing are not supported with third party applications. A list of third party applications that support XMPP is available at the XMPP Standards Foundation website http://xmpp.org/software/clients.shtml.

To allow the use of third party applications with the Cisco WebEx Messenger service, you need to enable a setting in Cisco WebEx Administration Tool. For more information refer to Specifying IM Federation settings.

You will also need to publish a Service (SRV) record in DNS to enable third party XMPP applications to work with the Cisco WebEx Collaboration cloud. For example, the Cisco WebEx Organization, acme.com publishes the following SRV record in DNS to allow the use of third party XMPP applications:

_xmpp-client._tcp.acme.com. 86400 IN SRV 5 0 5222 c2s.acme.com.webexconnect.com

- The SRV records for your domain can be found in IM Federation under the Configuration tab. For more information, see IM Federation Settings, on page 47.
- The TCP port 5222 should also be opened to enable the use of third party XMPP applications.
- Polices cannot be enforced when users in your Cisco WebEx Organization use third party XMPP applications to connect to your domain. Policies can only be enforced on users who use Cisco Jabber clients.

Sign in to the Administration Tool

Important If your Cisco WebEx Messenger organization is enabled with Single sign-on integration, the URL that you need to type in your Web browser should be in the format: https://<WAPIserver>/wbxconnect/sso/acme.com/orgadmin.app where acme.com is the Cisco WebEx Messenger organization enabled with Single sign-on integration.

Procedure

Step 1 To sign in go to http://www.webex.com/go/connectadmin.
The **Cisco WebEx Messenger Administration Tool** page is displayed.

Step 2 Enter your sign in details in the Username and Password fields.

Step 3 Select **Remember Username** to avoid typing in the username each time you sign in.

Step 4 Select **Sign In**.

Cisco WebEx Messenger Administration Tool Interface

The following tabs are available in the Cisco WebEx Messenger Administration Tool.

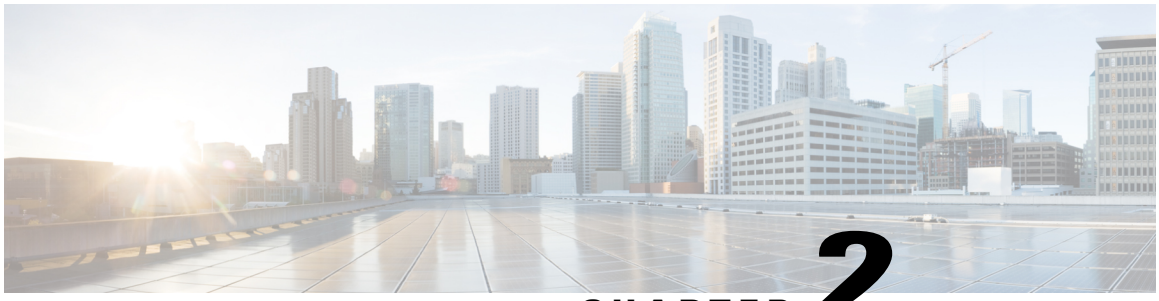
Tab	Description
User	Add and configure user information.
Configuration	Configure settings for various features of Cisco WebEx such as general information about your organization, domains, password enforcement, user provisioning, IM settings, and additional services such as IM federation, IM archiving, and unified communications.
Policy Editor	Set policies and rules for users.
Group	Assign group policies.
Report	View usage reports on users.
About	View Cisco WebEx Messenger Administration Tool version information.
Help	View Cisco WebEx Messenger Administrator's Guide.

From the **Administrative Tools** tab, you can:

- Enable self-registration.

- Customize various system-generated emails sent to Cisco WebEx users.
- Add new Cisco WebEx users and assign Roles and Groups to these users.
- Enforce password requirements.
- Import and export users from or to comma-separated value (CSV) files.
- Define and apply policies and policy actions.

Note When a User-Only administrator signs into Organization Administration, only the User, Report, About, and Help tabs are displayed.



CHAPTER 2

User Management

Overview

The **User** tab enables you to manage users in your organization. Typical user management tasks include searching for users, viewing a specific user's details, creating new users, activating and deactivating existing users, and assigning policy groups to users. The **User** tab is the default tab that is displayed when an Organization Administrator signs in to Cisco WebEx Messenger. The following graphic shows the default view of the User tab after you sign in into Cisco WebEx Messenger.

The default view of the **User** tab provides a search box that is always visible, and instructions for searching users in your Cisco WebEx Messenger organization. A toolbar provides additional options for accomplishing specific tasks with respect to users in your Cisco WebEx Messenger organization.

The **User** tab provides a powerful search facility with several filters to quickly and easily locate specific users in your organization.

Search for Users and Administrators

Procedure

Step 1 To search for users or administrators, in the **Search** drop down list, select the applicable search criteria. See the Related Topics section for information about the available search criteria.

Step 2 Depending on what search criterion you have selected, enter the corresponding search term. For example, if you have selected **All Users**, enter at least one letter of the user name in the search field.

Step 3 Select **Search** to display the list of users that match the search criteria.

Step 4 If the search result displays more users than can fit on one page, use the arrow icons (>> and <<) at the bottom of the page to navigate through the search result.

Step 5 To view a list of active users, you need to first export all the users in your Cisco WebEx Messenger organization and then view the active users in Microsoft Excel or a CSV editor of your choice. To learn how to export users, see Import and Export Users Using a CSV File, on page 13.
Searching for only active users is currently unsupported.

Related Topics

Search Criteria, on page 10

Search Criteria

Filters enable you to limit the number of user records showing at any one time. The following table lists the different filters available to search for users.

List by	Definition
All Users	Enter at least one letter of the user's first or last name. All active users with a name matching those letters are displayed in the search results.
Employee ID	Enter the exact employee ID of the user. This function is only visible when the organization has been turned on as a directory integrated organization.
Inactive Users	Select **Inactive Users** and select **Search** to view all inactive users. To narrow down the search results, specify the starting letters of the user's first name or last name.
Organization Administrators	Select this option and select **Go** to display all users with Organization Administrator privileges.
User Administrators	Select this option and select **Go** to display all users with User Administrator privileges.

List by	Definition
Meeting Users	This option is displayed only if your Cisco WebEx Messenger organization is integrated with Cisco WebEx Meeting application. Select **Meeting Users** and select **Go** to view all users that have a Cisco WebEx Meeting application account. In this case, you cannot search for users who do not have a Cisco WebEx Meeting application account.
Logged Users	Select **Logged Users** and select **Go** to view all users whose IM sessions are currently being logged for archival. The search results also show the archiving endpoint these users are associated with.

New Users

An Organization Administrator can add new users, one at a time from the **User** tab. A newly-created user does not necessarily belong to any group unless the Organization Administrator explicitly assigns the user to a specific group. A new user's default role is **Member** unless the Organization Administrator does not explicitly assign the **Organization Administrator** role.

The Organization Administrator role can only be assigned to users who are members of the top level group. A top level group, with the name of the Cisco WebEx Messenger Organization is provided at the time of provisioning. The name of the top level group typically begins with the name of the Organization where Cisco WebEx Messenger is provisioned.

Organization Administrators have the ability to create User-Only Administrator roles. These User Administrators have rights pertaining to User Management only. User Administrators cannot create new Organization Administrators.

Organization Administrators can update the roles and profiles of User Administrators. The User Administrators have rights pertaining to User Management only. User Administrators cannot update the roles of Organization Administrators but they can update other profile information including first name, last name, and business email.

The process is different for adding and editing users when Single sign-on (SSO) and Directory Integration are enabled. For more information on adding users with SSO and Directory Integration enabled, see Single Sign-on and Directory Integration Users, on page 16.

The Organization Administrator can determine if users are permitted to change their profile. This includes specifying if users can upload their profile pictures from within the Cisco WebEx Messenger application. In this case, the Organization Administrator can upload the user's profile picture from the corporate database.

The primary purpose of the User Administrator role is to have administrators who can perform only User Management actions. These users do not have the authorization to make configuration or policy changes at an organization level. Additionally, they do not have the authorization to create or update Policy Groups.

Create New Users

Procedure

Step 1 To create a new user or administrator, select the **User tab** > **Add**.

Step 2 Enter the applicable information in each field. The default Role is User (non-administrator).
Note The Business Email is the Username. You cannot edit the Username.

Step 3 (Optional) Select the **Policy Group Assignment** tab to assign a policy group to the user. For more information on assigning policy groups, see Assign Users to Policy Groups, on page 14.

Step 4 If IM Archiving is enabled for your Cisco WebEx Messenger Organization, the **Archive IMs** check box is displayed on the **Add User** dialog box. To log IMs for this user for archival, select the **Archive IMs** check box.
The name of the **Archiving endpoint** is displayed. To configure an archiving endpoint, see Set Up IM Archiving, on page 50.

Step 5 To change the endpoint, select a different endpoint from the drop down list.
Archiving endpoints are defined in the **IM Archiving** screen of Cisco WebEx Messenger Administration Tool. Selecting **Default** assigns the user to the endpoint preconfigured as the default endpoint in the **IM Archiving** screen. For more information, see Set Up IM Archiving, on page 50.

Step 6 To assign this user to an upgrade site, select a site from the **Upgrade Site** drop-down list.
For information about upgrade sites, see Create Upgrade Sites, on page 35.

Step 7 If your Cisco WebEx Messenger Organization is enabled with Cisco Unified Communications, the Unified Communications tab is displayed on the Add User dialog box. Select the **Unified Communications** tab to view the settings available for Cisco Unified Communications.

Step 8 Under **Cluster**, select the applicable Cisco Unified Communications cluster to which you want to add this user.
For more information, see Create Unified Communications Clusters, on page 67.

Step 9 If your Cisco WebEx Messenger Organization is enabled with Cisco WebEx Meeting Center integration, the Add User dialog box is displayed. To assign the Organization Administrator role to the user, select the **Organization Administrator** check box.
Note
- If you have enabled **Automatically enable Meeting account when creating a new user** in the **Meetings** page, the **Meeting Account** check box is selected by default. In such a case, you cannot clear the Meeting Account check box. For more information, see Provision Tightly Coupled Integration, on page 39.
- When the **Meeting Account** check box is selected, it means a corresponding Cisco WebEx Meeting Center account is created for this user.

Step 10 Select **Save.**
New users receive a welcome email based on the Welcome Email template in Cisco WebEx Messenger Administration Tool.

Step 11 Repeat the previous steps to continue adding new users.
Note If there is missing information or errors when you add new users, the errors are highlighted in yellow and a message is displayed.

Edit Users and Administrators

An Organization Administrator can edit all the properties of an existing user including altering the policy groups that the user is assigned to.

Procedure

Step 1 To edit a user or administrator, in the **User** tab search for the user whose information you want to edit. For information about searching for users, see Search for Users and Administrators, on page 10.

Step 2 Select **Edit** to open the **Edit User** dialog box.
The existing information of the user is displayed.

Step 3 Make the applicable changes.

Step 4 Select **User Administrator** from the **Role** list, if applicable.

Step 5 Select **Save**.

Note To reset a user's password, select the user in the **User** tab and select the **Reset Password** icon.

Import and Export Users Using a CSV File

You can easily import a large number of users from a comma separated values (CSV) file into your Cisco WebEx Messenger organization. Similarly, you can export your users to a CSV file. Importing is a useful way of painlessly adding a large number of users to your organization thereby saving the effort of manually adding each user.

After the import is complete, the Organization Administrator who initiated the import receives an email with the status of the import. The email states whether the import was a success, failure, or terminated.

The CSV file is imported and the users appear in the **User** tab. For more information on CSV file format and a sample file, see CSV File Format, on page 113.

Note Use an UTF-8 or UTF-16LE Encoded spreadsheet for optimal results.

Import and Export Users

Procedure

Step 1 To import users from a CSV file, in the Cisco WebEx Messenger Administration Tool, select the **User tab** > **More Actions > Import/Export**.

Step 2 Select **Browse** and select the CSV file that contains the list of users you want to import.

Step 3 Select **Import** to begin the import process.

Step 4 To export users, select **Export** in the **Import/Export User** dialog box.
A progress message indicates the progress of the export process.

Step 5 To view the CSV file that contains the exported users, select the time stamp of the export message.
A confirmation prompt appears. The message resembles the following example: `Last export: 2009-06-24 09:02:01`.

Step 6 Select **Open** to view the CSV file containing your Messenger organization's users. Alternatively, select **Save** to save the CSV file to your local computer.

Policy Group Users

When you assign a user to a policy group, all policies applied to that particular group automatically apply to the user. You can assign only one policy group to a user. When you try to assign a different policy group to the same user, the new policy group will replace the currently-assigned policy group. You can assign a policy group to both new and existing users.

Additionally, you can add multiple users to a group by importing a CSV file containing user information. For more information, see Import and Export Users Using a CSV File, on page 13.

Note By default users are not assigned to any policy group and have access to all Cisco WebEx Messenger features. After you assign a policy group to users, they are governed by the policies associated with that policy group.

For more information about applying policies to groups, see Assign Policies to a Group, on page 95.

Assign Users to Policy Groups

Procedure

Step 1 To assign users to policy groups, select the **User tab**.

Step 2 If you want to assign a policy group to a new user, create the new user first by selecting **Add**.
For information on adding a new user, see New Users, on page 11.

Step 3 If you want to assign a policy group to an existing user, search for the user.
For information on searching for users, see Search for Users and Administrators, on page 10.

Step 4 In the search result, double-click the appropriate user's name to open the **Edit User** dialog box.

Step 5 Select the **Policy Group Assignment tab** to open the **Policy Group Assignment**dialog box.

Step 6 In the **Search** field, enter at least one letter of the policy group that you want to search for and assign to this user.

Step 7 Select **Search.**

Step 8 In the **Search Result** window, select the appropriate policy group and select **Assign** to assign the policy to this user.

Step 9 Select **Save** to save the policy group assignment and return to the **User** tab.

User Deactivation and Reactivation

Users can be deactivated for a variety of reasons. For example, they leave the company or violate policies. When you deactivate users, they are not removed from the Cisco WebEx Messenger system but are disabled and not allowed to log into their accounts. You can reactivate deactivated users at a later time as required.

Note Primary Administrators cannot be deactivated.

Deactivate Users

Procedure

Step 1 To deactivate users, in the **User** tab search for the user to deactivate.
For information about searching for users, see Search for Users and Administrators, on page 10.

Step 2 Select the user to deactivate.

Step 3 Select **More Actions** > **Deactivate** to display a confirmation message.

Step 4 Select **Yes** in the message box to deactivate the selected user.

Reactivate Users

Procedure

Step 1 To reactivate a deactivated user (or to migrate Guest Edition users), search for the appropriate user using the **Inactive Status** search filter. For more information on search filters, see Search for Users and Administrators, on page 10.

Step 2 Select the user to activate.

Step 3 Select **More Actions** > **Activate** to display a confirmation message.

Step 4 Select **Yes** in the message box to reactivate the selected user.

Customize the User Tab View

You can customize the default view of the **User** tab to suit your needs. Customization settings include hiding or showing columns and sorting the order in which users are displayed.

Procedure

Step 1 To customize the user tab view, select **User tab** > **More Actions > Customize View**.

Step 2 Under **Select columns for display in the user tab**, select or clear the applicable fields.
If you have enabled integration with Cisco WebEx Meeting application, the **Meeting Account** field is displayed in addition to the default fields. Similarly, if you have enabled IM Archiving, and Cisco Unified Communication Manager, the **IM Archiving Endpoint** and **CUCM Cluster** fields are displayed.

Step 3 Under **Select default sort order of user records**, select the field (or column) by which you want to sort the list of users.

Step 4 Select either **Ascending** or **Descending** as the sort order.

Step 5 Select **Save**.

Single Sign-on and Directory Integration Users

The procedure for adding users enabled with Single Sign-on and Directory Integration is different from adding users who do not have these features enabled. For more information on single sign-on and Directory Integration, see Single Sign-on and Directory Integration.

When Single Sign-on and Directory Integration are enabled, you cannot use the following features in the **User** tab:

- Importing and exporting users
- Resetting user passwords

- Editing existing user information
- Creating new users

When **Directory Integration** is implemented with Cisco WebEx:

- Users and groups are created from corporate directory files provided by the company.
- Organization Administrators cannot directly edit the user and group data. When the user and group data needs updating, the company provides an updated corporate directory file that can be imported into Cisco WebEx.
- The CSV file import function is not available.

Migration of Guest Edition Users to Business Edition Users

When Cisco WebEx Messenger is provisioned with specific domain names, any users using the Cisco WebEx Connect application version 5.x or earlier with the same domain names are prevented from signing in to Cisco WebEx Messenger. These users receive an email notifying that their Cisco WebEx Messenger accounts have been deactivated.

The earlier versions of Cisco WebEx Messenger displayed the **Migration** tab in Cisco WebEx Administration Tool. The **Migration** tab displayed the list of Guest Edition users pending migration to the Business Edition of Cisco WebEx Messenger. The **Migration** tab was hidden in case there were no users pending migration.

The **Migration** tab no longer appears in Cisco WebEx Messenger version 6.0 or later. Guest Edition users pending migration now appear as inactive users.

The Organization Administrator needs to migrate the Guest Edition users to the Business Edition of Cisco WebEx Messenger.

After migration, the user is subject to the policies configured by the Organization Administrator. All the resources that the user consumes as a Business Edition user including the Cisco WebEx Messenger license, forms part of the total amount of resources (user licenses and storage) assigned to the Cisco WebEx Messenger Organization.

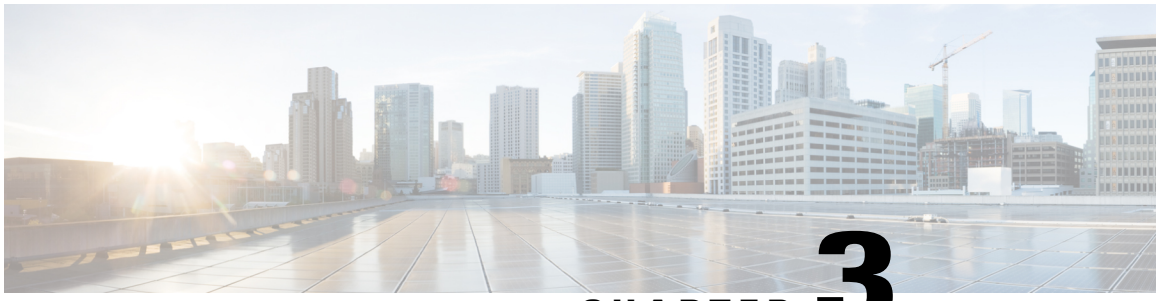
Migrate Guest Edition Users to Business Edition Users

Procedure

Step 1 Review the list of "inactive" users in the Cisco WebEx Administration Tool and identify the users who need to be migrated to Cisco WebEx Messenger Business Edition.

Step 2 Send instructions to the selected users with the download URL for the latest version of Cisco WebEx application. The URL can be found in the email that the administrator would have received at the time when the service is provisioned.

Step 3 Set the status to "active" and reset the password for the selected users.
For more information on activating inactive users, see User Deactivation and Reactivation, on page 15.
These users will receive emails with a password reset link. The link allows users to specify a new password. Users can then use this new password to sign in to the latest version of Cisco WebEx Messenger Business Edition. Users' contacts is not transferred to the Business Edition.



CHAPTER 3

Configuration Tab

Overview

The Configuration tab controls the Cisco WebEx Messenger service. These settings impact areas such as licensing, policies, user administration, and integration with additional services. Changing a specific setting therefore might have an organization-wide impact. It is recommended that you plan thoroughly before making configuration changes.

The Configuration tab displays items that you can configure under a particular category. For example, you can configure domain names and URLs under the System Settings category and contact list settings under the Connect Client category. Each category opens a work area where you enter the actual configuration settings for a specific configuration item.

When you click a particular configuration item, configurable details of that item are displayed. For example, clicking Resource Management lets you view license information for your Organization and allows you to enable storage enforcement for users.

Note For Apple Push Notifications support, Jabber IOS client version 11.x or later is required. The cloud-based Push Notification Service sends instant message notifications to Cisco Jabber on iPhone and iPad clients that are running in the background. For more information, see Deploying Push Notifications for iPhone and iPad with the IM and Presence Service and WebEx Messenger and the Cisco Unified Communications Manager Express System Administrator Guide.

Organization Information

The **Organization Information** window enables you to provide relevant information about your Cisco WebEx Messenger Organization. A Cisco WebEx Messenger Organization signifies any organization where Cisco WebEx Messenger has been purchased and provisioned.

Note You cannot enter or modify the Company name. This name is the same name provided at the time of purchase.

Contact information such as address and business phone is for information purposes.

The Notification Email address is the Organization Administrator's email address by default. You can change it to any other email ID including a distribution list.

Enter the Organization Information

Procedure

Step 1 To enter Cisco WebEx Messenger Organization information select the **Configuration** tab to open the **Organization Information** window as the default view.

Step 2 Enter the appropriate information in each of the settings fields.

Step 3 Verify that the name and email address of the **Primary Administrator** of your Cisco WebEx Messenger Organization is already present.
This information is set when your Cisco WebEx Messenger Organization is provisioned. All critical information about Cisco WebEx services, such as the availability of newer versions and maintenance schedules is sent to this email address. To change this information, contact your Cisco WebEx representative.

Step 4 In the **Notification Email** field, specify the email address used for sending alerts to Administrators when a critical event occurs.
A typical example of a critical event is when storage usage for an organization exceeds its allocated limit.

Step 5 Select **Save** to save your organization information.

Domain Information

The **Domain** window enables you to view the domains provisioned for your Cisco WebEx Messenger Organization. Additionally, you can specify a domain whitelist, which is a list of "trusted" domains outside your Messenger Organization.

The process of provisioning the Cisco WebEx Messenger Organization begins when the Cisco WebEx Messenger provisioning team receives a provisioning request from the company or organization that has purchased Cisco WebEx Messenger. When you create the Cisco WebEx Messenger Organization as part of the provisioning request, you will typically enter domain names or sub domain names that will be part of this Cisco WebEx Messenger Organization.

Examples of a domain include acme.com, mydomain.net, myorg.com, and so on. Examples of sub domains include test.acme.com, docs.mydomain.net, and prod.myorg.com.

A domain whitelist is a list of trusted domains that are external to your Cisco WebEx Messenger Organization's domains and sub domains. A trusted domain is one that has a relationship of trust established with your Cisco WebEx Messenger Organization's domains. For example, if acme.com is your Cisco WebEx Organization, you can add customeracme.com, vendoracme.com to your domain whitelist after establishing a relationship of trust with such (external) domains.

The list of domain names that appear in the **Domain(s)** box is already created by the Cisco WebEx Messenger provisioning team when the Cisco WebEx Messenger Organization is provisioned. To add, modify or remove domain names, contact your Cisco WebEx representative.

The domains you enter in the **Domain(s)** and **Domain Whitelist** boxes impact how contacts are added in the Cisco Jabber application.

Contacts belonging to the domain whitelist can only be viewed if you select **My Organization & My Network** when you setup the user profile view settings. For more information, see Enter the Contact List Settings for the Cisco Jabber applications, on page 29 and Enter User Profile View Settings, on page 31.

Enter the Domain Information

Procedure

Step 1 To enter domain information, select the **Configuration** tab.

Step 2 Under **System Settings**, select **Domain(s)** to open the **Domain(s)** window.

Step 3 In the **Domain Whitelist** box, enter the names of trusted domains.
The domain whitelist is used in conjunction with the policies. For more information, see Policy Actions Available in Cisco WebEx, on page 85.

Step 4 Select **Save** to save your domain information settings.

Resource Management Information

Resource management information includes specifying details about the number of user licenses and storage space allotted for your Cisco WebEx Messenger organization.

You can only view the number of user licenses purchased for your Cisco WebEx Messenger organization. You can also view the number of active users in your Cisco WebEx Messenger organization. Active users are users who are actually using the Cisco Jabber application. The number of active users is automatically updated when you activate or deactivate users. For information on activating and deactivating users, see User Deactivation and Reactivation, on page 15.

To increase the number of user licenses, contact your Cisco WebEx representative.

Storage

The total amount of storage you have already used is indicated by Storage Used. Total storage used includes space consumed by files and persistent chat in all spaces created by users in your Messenger organization.

The total amount of storage you have already used is indicated by Storage Used. Total storage used includes space consumed by files and persistent chat in all spaces created by users in your Messenger organization.

Space used up for storing NBR (Network based recording) is not calculated for computing the storage used.

The IM Logging User Licenses Purchased and IM Logging User Licenses Used fields are displayed if your organization has purchased the IM Archiving feature. For more information, see Set Up IM Archiving, on page 50.

By default, storage enforcement is not enabled for each user. In such a case, storage is used based on the “First Come First Served” basis until the total storage utilization reaches the licensed storage limit.

When storage enforcement for each user is enabled, the Organization Administrator can specify a default storage limit when creating new users. When you change this value, it does not change the storage limit that you have specified for a user in the Add User or Edit User dialog box

Enter Resource Management Information

Procedure

Step 1 To specify resource management information, select the **Configuration** tab.

Step 2 Under **System Settings**, select **Resource Management** .

Step 3 To allocate a fixed amount of storage space for each user in your Messenger organization, select **Enable storage enforcement for each user**.

Step 4 In the **Default file storage allocation per user**, enter the number of megabytes you want to allocate for each user as the default storage space.

Step 5 Select **Save** .

URL Configuration

The **URL Configuration** screen enables you to specify URLs for the following websites:

- **Password retrieval:** enables users to retrieve their password.
- **Cisco WebEx Messenger support website:** for users to log their support requests.

Enter URL Configuration Information

Procedure

Step 1 To specify URL configuration information, select the **Configuration** tab.

Step 2 Under **System Settings**, select **URL Configuration**.

Step 3 In the **Forgot Password URL** field, enter the URL of the password retrieval page.
The Organization Administrator can override the default URL by specifying a custom **Forgot Password** URL. This can be customized in special cases where a company or organization has enabled SAML integration.

Step 4 In the **Connect Support URL** field, enter the URL of the Cisco WebEx Messenger support page. The Organization Administrator can override the default Cisco WebEx Support URL by specifying an internal first level support page.

Step 5 Select **Save** to save the URL configuration information.

Security Settings

The Partner Delegated Authentication screen enables you to specify options for integrating a Cisco WebEx certified Delegation Authentication partner Organization with your Cisco WebEx Messenger Organization. This option is available only when a pre-configured correlation is setup via a Super Administrator configuration. Integrating a partner Organization simply means you allow the partner Organization to authenticate with your Cisco WebEx Messenger Organization as a Member, an Organization Administrator, or both. When such an authentication is enabled, users using applications developed by these Cisco WebEx certified partner Organizations can access Cisco WebEx Messenger without the need to use a separate set of credentials.

For example, acme.com is a Cisco WebEx Messenger Organization that has enabled integration with Verizon Communications, a Cisco WebEx Messenger certified partner. Users of acme.com can authenticate to an application offered by Verizon Communications and access Cisco WebEx Messenger without having to enter different sign in credentials.

If you grant Organization Administrator access, your partner Organization is able to perform administrative tasks on your Cisco WebEx Messenger Organization and the partner Organization. You can enable partner Organization integration with more than one partner Organization.

You can disable the partner Organization integration at any time.

Note The SSO Related Options link display is set by the super administrator.

Enter Security Settings

Procedure

Step 1 To enable partner organization integration, under the **Configuration** tab select **Security Settings** > **SSO Related Options**.

Step 2 Select:

- **Partner Delegated Authentication** to display the dialog for an administrator whose organization is not Delegated Authentication. See, Configure Partner Delegated Authentication, on page 62.
- **Federated Web SSO Configuration** to display the dialog for an administrator who has turned on single sign-on. See, Federated Web SSO Settings, on page 58.
- **Organization Certificate Management** to display the dialog for an administrator who has turned on single sign-on or is a “Delegated Authentication” administrator. See, Configure Organization Certificate Management, on page 60.
- **WebEx Certificate Management** to display the dialog for an administrator who has turned on single sign-on. See, Configure WebEx Certificate Management, on page 60.
- **Partner Web SSO Configuration** to display the dialog for an administrator who is “Delegated Authentication”. See, Configure Partner Delegated Authentication, on page 62.

See the Related Topics section for information about SSO Related Options.

Step 3 Select **Member** or **Org Admin** as the applicable level of access to permit for each partner Organization. If you select **Organization Administrator**, **Member** is selected by default.
The NameID selection should match the identifier for your organization in Cisco WebEx Messenger. For example, if your organization is authenticated based on EmployeeID, your Delegated Authentication Partner must use EmployeeID to federate your user account. The available selections are UserName, Email, and EmployeeID.

Step 4 Select **Save** to display a confirmation message.

Step 5 Select **Grant Partner Access** to save the partner Organization integration settings.

Related Topics

SSO Related Options, on page 25

SSO Related Options

Use the following table to determine the SSO Related Options link display.

SSO Org	Delegated Authentication Org	Display
False	False	SSO Related Options • Partner Delegated Authentication
True	False	SSO Related Options • Federated Web SSO configuration • Org Certification management • WebEx Certification management • Partner Delegated Authentication
True	True	SSO Related Options • Federated Web SSO configuration • Org Certification management • WebEx Certification management • Partner Delegated Authentication
False	True	SSO Related Options • Org Certification management • Partner Web SSO configuration

Directory Settings

This topic applies only if your Cisco WebEx Messenger Organization has enabled directory integration. For more information, see Configure Directory Integration, on page 98 and Directory Integration Import Process and File Formats, on page 98.

Password Settings

An Organization Administrator can specify password settings for users in your Cisco WebEx Messenger Organization. Password settings determine how passwords are enforced in various scenarios such as when a new user signs up for a Cisco WebEx Messenger account or existing users want to change their passwords.

A password does not come into effect until it meets all the rules you have set for it in this screen.

Enter Password Settings

Procedure

Step 1 To specify password settings, under **System Settings**, select **Password Settings**.

Step 2 Set the applicable choices by following the on-screen instructions.
By default, every Cisco WebEx Messenger Organization is provisioned with the following password settings:

- Minimum password length = 6
- Minimum number of alphabets = 1
- Minimum number of numerals = 1

If you want to reset these minimum password length requirements, contact your Cisco WebEx representative.

Step 3 In the **List of Unacceptable Passwords** box, enter the words or terms that are prohibited to be used in a password. Typically, this includes terms such as your organization name, the word password, URLs, and so on. Separate each term with a comma.

Step 4 Select **Save**.

Email Templates

Cisco WebEx Messenger Administration Tool provides templates for email notifications and alerts that Cisco WebEx Messenger users receive. Organization Administrators can customize email templates. Once customized, any updates made to these templates by Cisco WebEx are lost. You can however, revert to the default templates at any time.

You can use variables to more fully customize email templates. For detailed information about using variables to customize email templates, see Email Template Variables, on page 27.

Cisco WebEx will continue to enhance the content of email templates from time to time. Organization Administrators who do not customize their email templates will get the updated content automatically.

Once email templates are customized, only the customized templates is used. Organization Administrators revert to using Cisco WebEx default email templates by selecting the email template and clicking Reset to Default.

Any changes made to email templates is lost once they are reset to Cisco WebEx default email templates.

Email Template Variables

This topic describes the various email templates available in Cisco WebEx Messenger and how you can edit or customize these templates. Typically, you can customize an email template by editing its built-in variables. Variables are building blocks that define what an email template (and emails based on that template) will contain. For example, the **Welcome Message** email template contains the %USERNAME% variable. This variable will display the Cisco WebEx Messenger user's username in the email that is sent to the user.

Every email template contains pre-existing message text in the Message box. You can customize or change it according to your requirements.

Cisco WebEx Messenger email templates are pre-populated with appropriate templates for out of the box use.

The following table describes each email template, the variables used in each email template and their definitions.

Email Template	Variables and Macros
Welcome Message—Default email contains links to reset password, download the application, documentation, and community links.	%USERNAME%—The name of the user. %CLIENTDOWNLOADURL%—The URL that takes the user to the welcome message. %NEWPASSWORDURL%—The new password variable.
Get or Reset Password Email—Email is sent when Cisco WebEx Messenger Administrator resets password.	%NEWPASSWORDURL%—URL that will take the user to reset password.

Select an Email Template

Procedure

Step 1 To use email templates, under **System Settings**, select **Email Templates**.

Step 2 Select the email template that you want to modify.
The **Edit Email Template** window appears.

Step 3 Enter the appropriate information in each field starting with **Email Name**.

Step 4 In the **Message** box, enter the text of the email template.

Step 5 Select **Save** .

User Provisioning Information

User provisioning includes specifying user-provisioning information such as registration, and fields required when creating a user's profile. The settings you make here impact when users are provisioned in your Cisco WebEx Messenger Organization. For example, if you set specific fields as mandatory here, the user needs to compulsorily fill in those fields when creating the user profile.

Cisco WebEx Messenger customers can enable self-registration when there is no SAML or Directory Integration enabled. In such a case, the Organization Administrator does not need to specify the registration URL. When registration is not enabled, customers can specify a custom web page. Any user trying to register with an email address that matches with customer's domain is redirected to the custom web page. Customers can use this webpage to display information about their internal processes required for creating a new Cisco WebEx Messenger account.

For example:
To obtain the Cisco WebEx Messenger service, send an email to ithelpdesk@mycompany.com, or call +1 800 555 5555.

Enter User Provisioning Information

Procedure

Step 1 To enter user provisioning information, under the **Configuration** tab select **System Settings** > **User Provisioning**.

Step 2 To enable users to self-register for an account with the Cisco Jabber application, select **Enable user self-registration using Cisco WebEx registration page**.
The URL for the self-registration page is www.webex.com/go/wc. The Cisco WebEx Messenger organization Administrator typically provides this URL.

Note If you do not select Enable user self-registration using Cisco WebEx registration page, the Custom Registration URL field and the Custom Message box is displayed. In this case, you will need to enter the URL for the custom user registration page.

Step 3 In the **Custom Registration URL** field, enter the URL of the customized self-registration page.
If you do not enter a custom URL, the following self-registration page (default) URL is displayed: www.webex.com/go/wc.

Step 4 In the **Custom Message** box, enter a description for the custom self-registration page.

Step 5 To notify the Organization Administrator via email each time a user registers using the self-registration page, select **Send notification to Administrator when users self register using Cisco WebEx registration page**.

Step 6 Under **Set mandatory fields for user profile**, select the fields that are compulsorily displayed each time a user's profile is created or viewed. These fields always appear each time you:

- create a new user

- edit an existing user profile
- import users from a CSV file

Step 7 Select **Save**.

Enter the Contact List Settings for the Cisco Jabber applications

The **Contact List** screen enables you to specify settings for how users of your Cisco WebEx Messenger organization can manage their contact lists. These settings control features such as displaying contact pictures, displaying quick contacts and observer group in the user's Contact List.

Procedure

Step 1 Select the **Configuration** tab to open the **Organization Information**.

Step 2 To specify contact list settings, under **Connect Client**, select **Contact List**.

Step 3 Specify the appropriate settings.
See the Related Topics section for information about the contact list.

Step 4 Select **Save**.

Related Topics

Contact List Settings, on page 29

Contact List Settings

Select	To
Allow users to set "Show contact pictures in my contact list" **Note** This option is applicable only to Cisco WebEx Messenger versions 6.x or earlier.	Allows the Organization Administrator to directly control whether users can see contact pictures. If this option is selected, the **Show contact pictures in my contact list** check box is shown in the Cisco Jabber application and users can specify their preferences for showing contact pictures. If this option is not selected, the **Show contact pictures in my contact list** check box is not shown in the Cisco Jabber application.

Select	To
Show contact pictures in my contact list **Note** This option is applicable only to Cisco WebEx Messenger versions 6.x or earlier.	If this option is selected, contact pictures are displayed in the users' contact list on the Cisco Jabber application. Contact pictures are displayed at the right side of the contact name. This option is grayed out if **Allow users to set "Show contact pictures in my contact list"** is selected.
Allow users to set "Show quick contacts" **Note** This option is applicable only to Cisco WebEx Messenger versions 6.x or earlier.	Enables the Organization Administrator to directly control whether users can see the Quick Contacts group in the Cisco Jabber application. If this option is selected, the **Show quick contacts** check box is shown in the Cisco Jabber application and users can specify their preferences accordingly. If this option is not selected, the **Show quick contacts** check box is not shown in the Cisco Jabber application.
Show quick contacts **Note** This option is applicable only to Cisco WebEx Messenger versions 6.x or earlier.	If this option is selected, Quick Contacts are shown in the users' contact list on the Cisco Jabber application. Quick Contacts is a way of grouping your contacts in the Cisco Jabber application. This option is grayed out if **Allow users to set "Show quick contacts"** is selected.
Allow users to set "Show observer group on my contact list" **Note** This option is applicable only to Cisco WebEx Messenger versions 6.x or earlier.	Allows the Organization Administrator to directly control whether users can see the Observer Group in the Cisco Jabber application. If this option is selected, the **Show observer group on my contact list** check box is shown the Cisco Jabber application and users can specify their preferences accordingly. If this option is not selected, the **Show observer group on my contact list** check box is not shown in the Cisco Jabber application.
Show observer group on my contact list **Note** This option is applicable only to Cisco WebEx Messenger versions 6.x or earlier.	Selecting this option shows the Observer Group in the Cisco Jabber application. The Observer Group is a special grouping of your contacts in the Cisco Jabber application. By default, this option is selected. This option is grayed out if **Allow users to set "Show observer group on my contact list"** is selected.

Enter User Profile View Settings

You can specify who can view users in your Cisco WebEx Messenger organization. Additionally, you can permit users to change their profile view settings in the Cisco Jabber application. The user profile is typically displayed in the Cisco Jabber application similar to the user's business card.

Procedure

Step 1 To specify user profile view settings, select **Connect Client** > **Profile Settings**.

Step 2 Select **Allow users to change their profile view settings** if you want to allow users to edit their profile view settings directly in the Cisco Jabber applications.
If you enable this option, users can open and edit their profiles directly in the Cisco Jabber application.

Note
- When clearing the **Allow users to change their profile view settings** check box, users are unable to change any information about their profile in the Cisco WebEx application.
- The Organization Administrator can restrict users' ability to change profile view settings by applying the **Edit View Profile Setting** policy action. If this policy action is set to **FALSE**, the ability to change profile view settings is disabled even if the **Allow users to change their profile view settings** check box is selected.

For more information about this policy, see Policy Actions Available in Cisco WebEx, on page 85.

Step 3 Under **Default user profile view settings**, select one of the following options:

- **Anyone:** Permits all users to view the user's profile information. This includes users external to your Cisco WebEx Messenger organization with whom a relationship of trust has been established.
- **My Organization & My Network:** Permits all users within both your Cisco WebEx Messenger organization and network to view the profile information of users as well as any user belonging to an external domain added to the contact list.
- **My Organization:** Permits all users within your Cisco WebEx Messenger organization to view the user's profile information. Users who can view your profile are determined according to how your Cisco WebEx Messenger organization was provisioned. This setting does not allow users to view user profiles belonging to an external domain added to the whitelist.

Step 4 Select **Save**.

Enter Instant Message Blocking Settings

Instant message (IM) blocking settings include specifying the following:

- File types that you want to prohibit from being exchanged over IM communications
- URLs that you want to prohibit from being accessed over IM communications

Note You can create an XML file that contains configuration parameters for your organization. You can then use **Import Jabber Client Config File** to upload that XML configuration file to the Cisco WebEx Messenger Administration Tool. When users sign in, the Messenger Administration Tool retrieves the XML file and applies the configuration. For more information, see the latest *Deployment and Installation Guide for Cisco Jabber*.

Procedure

Step 1 Select the **Configuration** tab to open the **Organization Information**.

Step 2 To enter instant message blocking settings, under **Connect Client** select **IM Block Settings**.

Step 3 In the **Blocked File Types** box, enter the file types you want to block in IM communications. Separate each file type with a semicolon.

Step 4 In the **Blocked URLs** box, enter the URLs you want to prohibit in IM communications. Separate each URL with a semicolon.

Step 5 Select **Save**.

XMPP IM Clients

The **XMPP IM Clients** window allows you to specify whether users within your Cisco WebEx Messenger organization are permitted to sign in using a third party IM application.

Instead of the Cisco Jabber application, third party applications (for example, Pidgin for Linux) that support XMPP can also be used for basic IM communication. However, organization policies cannot be enforced on third party XMPP applications. Additionally, features such as end-to-end encryption, Desktop sharing, video calls, computer-to-computer calls, and teleconferencing are not supported with third party applications. A list of third party applications that support XMPP is available at the XMPP Standards Foundation website: http://xmpp.org/software/clients.shtml.

Configure Settings for XMPP IM Clients

Procedure

Step 1 To configure settings for XMPP IM clients, select the **Configuration tab** > **Connect Client > XMPP IM Clients**.

Step 2 Select **Allow use of non-Connect XMPP IM clients** to allow users in your Cisco WebEx Messenger Organization to sign in using a third party XMPP-based IM client.
The SRV records for your domain can be found in the **IM Federation** screen under the **Configuration** tab. For more information, see Specify IM Federation Settings, on page 47.

Step 3 Select **Save**.

Upgrade Management Settings

The **Upgrade Management** window enables you to specify how upgrades to the Cisco Jabber application should be rolled out to users in your organization. You can roll out upgrades using the following upgrade modes:

- **Default:** all users are automatically upgraded to the latest version of Cisco Jabber. This is the default upgrade mode.
- **Custom:** you can manually configure how you want to roll out the upgrades to users. In this case, you need to select a baseline version and create an upgrade task, which defines how the upgrades are rolled out.

  You can switch between the two upgrade modes at any point time but this has an impact on how upgrades are rolled out. For example, if you select a specific version (using the Custom mode) to roll out to users, and then change the mode to Default and users will be upgraded to whatever is the default version of the client at that time, except if they were on a version that was later than the default version.

  You can set a baseline version if you want all your users on the same version of the application. This requires all users that are on older versions to upgrade but users on newer application versions than the baseline are not required to downgrade.

  Setting the baseline version is optional. We recommend that the baseline version is set to the version of application you require all your current and future users to be running as the minimum version.

  Setting a baseline version ensures that any new users you provision will download the version of the client that you have set as your baseline.

  You can upgrade one or more of your users to a version of the application higher than the baseline by creating an Upgrade Task. However, the upgrade management service prevents users from running any earlier version of the application. Any user on a version earlier than the baseline are immediately asked to upgrade to the baseline version at login. Setting a baseline version ensures that all your current and new users will at least be running that version of the application.

  If you decide not to set a baseline version, any new user you provision is directed to download the current default version of the application.

Configure Upgrade Management Settings

Procedure

Step 1 To set a baseline version, in the **Upgrade Mode** section, select **Change** to view the available upgrade modes.

Step 2 Select an Upgrade Mode.

Step 3 Select the baseline as applicable.

Step 4 Select the version to deploy and select **OK**.

Note If you do not select a baseline, the following message is displayed: You have not set baseline versions. The URL in the Welcome email to download the Cisco Jabber client is directed to the latest versions of Cisco Jabber for both platforms.

Step 5 Select **Yes** to view the selected version on the **Upgrade Management** screen listed under **Baseline Versions**. If you select an older version in step 7, all newer versions are displayed above **Baseline Versions**.

Step 6 (Optional) Select **Download** next to the applicable version to download the application.

Step 7 Select **Release Notes** next to the release notes for that version.
The version listed under **Baseline Versions** is the version that is deployed to your organization.

Create an Upgrade Task

Procedure

Step 1 To create an upgrade task, select the **Configuration tab** > **Connect Client > Upgrade Management**.

Step 2 Select **Create Upgrade Task** to open **Create Upgrade Task for Windows** in the Upgrade Management work area.

Step 3 From the **Target Version** drop down list, select the applicable version to deploy.
You need to select a version higher than the previously set baseline as the target version.

Step 4 Select **Provide Customized URL** to specify a custom link from where the Cisco WebEx Messenger Setup Program can be downloaded. This field is optional.

Step 5 In the **Optional Upgrade** box, select a date and time on which the upgrade will be optionally deployed. Or select **Skip** to skip applying the optional upgrade.

Step 6 In the **Mandatory Upgrade** box, select a date and time on which the upgrade is deployed. Or select **Skip** to skip applying the mandatory upgrade.

Step 7 From the **Time Zone** drop down list, select the time zone based on which the upgrade is deployed.
The date and time that you select for optional and mandatory upgrades are calculated according to this time zone.

Step 8 Under **Target User**, select:

- **All users**: to deploy the upgrade to all the users in your organization.
- **Specific Upgrade Sites**: to deploy the upgrade to the selected upgrade sites. In this case, the upgrade will be deployed to all users within those sites. If no upgrade sites are listed, you will need to create them. For more information, see Create Upgrade Sites, on page 35.

Step 9 Select **Save**.
The upgrade is displayed on the **Upgrade Management** page.

Edit or Cancel an Upgrade Task

Procedure

Step 1 To edit, select **Edit** to edit the details of the upgrade task.

Step 2 Or to cancel an upgrade task, select **Close Upgrade Task** .

Step 3 Select **Yes** to delete the upgrade task.

Upgrade Sites

An upgrade site allows you to specify what users to deploy Cisco Jabber client upgrades to. An upgrade site is used when you create an upgrade task to deploy the upgrade to specific users in your organization. For information on creating an upgrade task, see Configure Upgrade Management Settings, on page 33.

Create Upgrade Sites

Procedure

Step 1 Select the **Configuration tab** > **Connect Client > Upgrade Management** .

Step 2 Scroll down if required to locate the **Upgrade Site** section.
If you have selected **Default** as the upgrade mode, the **Upgrade Site** section is not displayed. Additionally, if no upgrade sites have been created, this section is blank.

Step 3 Select **Add** to open the **Add Upgrade Site** window.

Step 4 In the **Upgrade Site Name** box, enter a name for the upgrade site and select **Save**.
The new upgrade site appears on the **Upgrade Management** screen. You can add any number of upgrade sites in your organization.

Step 5 To view users belonging to an upgrade site, select the **View Users** icon.
To learn how to add users to an upgrade site, see Create New Users, on page 12.

P2P Settings

P2P refers to the ability to make Jabber to Jabber calls.

The **P2P Settings** window provides the following options for configuring P2P settings:

- Manual configuration of UDP ports: Where the administrator at the customer's organization can manually provide a range of UDP ports to be used by the Cisco Jabber application when it attempts to make a Jabber to Jabber call. Allowing the customer's administrator to manually specify a port range helps

minimize security risk because the Cisco Jabber application will only ping the ports within this range. Port range is specified as port numbers allowable within a minimum and maximum port number.

- For example, if your range is 7050—7550, the Cisco Jabber application scans all ports only in this range. If the port range specified is too restrictive then Jabber to Jabber calling is not available to the user.

Note Jabber to Jabber calling leverages the Cisco Spark platform. As a result, customers must open the Media Cisco hybrid services UDP port range settings to use P2P. The spark platform network and firewall settings can be found here: https://support.ciscospark.com/customer/en/portal/articles/1911657-firewall-and-network-requirements-for-the-cisco-spark-app?b_id=8722.

- Ensure that the **Max** port number is always greater than the **Min** port number. For example, **Min=1034** and **Max=1024** is an invalid port range.
- The lower and upper values for the **Min** and **Max** port ranges are system-defined. You can only enter a port number that falls within these predefined ranges; between 1024—65525 and 1034—65535.

Configure P2P Settings

Procedure

Step 1 Select the **Configuration tab** > **Connect Client > P2P Settings**.

Step 2 Select **Configure Ports Manually** to specify the UDP port range manually.

Step 3 Under **UDP Port Range**, enter:

- The minimum port number in the **Min** box. You can enter any port number between 1024 and 65525.
- The maximum port number in the **Max** box. You can enter any port number between 1034 and 65535.

Step 4 Select **Save**.

Step 5 To revert to a previous configuration of P2P settings, select **Reset**.

Understanding Additional Services

Cisco WebEx Messenger provides certain additional services over and above the regular or default options that are part of every Cisco WebEx Messenger deployment. Additional services involve separate configuration so they can be seamlessly integrated into Cisco WebEx Messenger.

The following additional services are available:

- **Integration with Cisco WebEx Meeting application**: You can enable integration between Cisco WebEx Messenger and Cisco WebEx Meeting application to simplify administration and user experience. For information about specifying Cisco WebEx Meeting application integration details, see Understanding Cisco WebEx Messenger integration with the Cisco WebEx application, on page 37.
- **Integration with Unified Communication**: Enables your Cisco WebEx Messenger organization's users to use Cisco Unified Communications Integration (Click-to-Call) and Cisco Unified Call Manager (CUCM) directly from Cisco WebEx Messenger. For information about specifying Unified Communications Integration information, see Cisco Unified Communications Integration with Cisco WebEx, on page 63.
- Integration of older Cisco WebEx Messenger organizations with the Cisco WebEx application: When you enable integration of older Cisco WebEx Messenger organizations with the Cisco WebEx application, you can only enable Loosely Coupled Integration. You still need to use separate credentials to sign in to Cisco WebEx Messenger and the Cisco WebEx application. For more information, see Cisco Unified Communications Integration with Cisco WebEx, on page 63.
- **IM Federation:** Enables you to specify IM federation settings so your Cisco WebEx organization's users can communicate with public XMPP networks such as Google Talk. For information about specifying IM federation settings, see Specify IM Federation Settings, on page 47.
- **IM Logging and Archiving**: Cisco WebEx Messenger allows you to log and archive IMs that users in your organization exchange with each other. For more information, see IM Archiving Notifications, on page 49.

Understanding Cisco WebEx Messenger integration with the Cisco WebEx application

You can enable integration between Cisco WebEx Messenger and the Cisco WebEx application to simplify user administration and user experience. This integration is available at two levels: **Tightly Coupled** and **Loosely Coupled**. Administrators need to select the appropriate level of integration based on their requirements and the specific deployment scenario involved. The following table lists major features and differences between the two levels of integration.

Tightly Coupled Integration	Loosely Coupled Integration
All Cisco WebEx Meeting application users are required to have a Cisco WebEx Messenger account. Provides the "Click-to-meeting" experience to users with no additional settings	Provides the "Click-to-meeting" experience to users with no additional settings
Provides a Single point of User Provisioning, User Password Management, and User Administration	Cisco WebEx Messenger and Cisco WebEx Meeting application are managed as independent services. Not all Cisco WebEx Messenger users need to have a Cisco WebEx application account and vice-versa.
Enables use of just one set of sign in credentials across both Cisco WebEx Messenger and the Cisco WebEx application	Users can continue to use their Cisco WebEx application sign in credentials for signing into the Cisco WebEx web site.

In general, Tightly Coupled Integration is recommended for enterprises that have not deployed a single sign-on system. Loosely Coupled Integration is recommended for enterprises that have deployed a single sign-on system. However, you can enable the Loosely Coupled Integration even for enterprises that have not deployed a single sign-on system. For detailed information about each level of integration, see:

- Overview of Tightly Coupled Integration, on page 38
- Overview of Loosely Coupled Integration, on page 44

  Both Tightly Coupled and Loosely Coupled levels involve different scenarios in the integration process and can vary accordingly.

  Tightly and Loosely Coupled Integration applies if your Cisco WebEx Messenger organization supports an existing Cisco WebEx Meeting Center site for starting a WebEx meeting from the application.

Overview of Tightly Coupled Integration

Tightly Coupled Integration provides a single point of user management from the Cisco WebEx Messenger Administration Tool. Organization Administrators can create Cisco WebEx Messenger accounts with or without enabling the Cisco WebEx Meeting application service for such accounts. Organization Administrators can access the Cisco WebEx Meeting application administration tool from the Cisco WebEx Messenger Administration Tool to perform administration functions specific to Cisco WebEx Meeting application accounts.

Tightly Coupled Integration provides significant value for customers who have not integrated with the Enterprise Single sign-on infrastructure. Customers who have integrated with the Enterprise Single sign-on infrastructure use Enterprise Identity Management system as their primary means of user management. Loosely Coupled Integration is recommended for such customers.

Three typical scenarios are available for enabling a Tightly Coupled Integration for an enterprise as shown in the following table.

Integration Scenario	Cisco WebEx Messenger	Cisco WebEx Meeting application
1	New deployment	New deployment
2	New deployment	Existing deployment. The enterprise already has a fully functional deployment of Cisco WebEx Meeting application.
3	Existing deployment. The enterprise already has a fully functional deployment of Cisco WebEx Messenger.	New deployment

The steps for enabling a Tightly Coupled Integration between Cisco WebEx Messenger and Cisco WebEx Meeting application vary for each of these scenarios. For more information about each scenario, see the following topics:

- Verify the Success of Tightly Coupled Integration for a New Deployment of Both Cisco WebEx and Cisco WebEx Meeting Application, on page 41

- Verify the Success of Tightly Coupled Integration for a New Cisco WebEx Messenger Deployment with an Existing Cisco WebEx Meeting Application, on page 42
- Verify the Success of Tightly Coupled Integration for a New Cisco WebEx Meeting Application Deployment with an Existing Cisco WebEx Messenger Deployment, on page 43

System requirements for Tightly Coupled Integration

Ensure that the following system requirements are met before you enable the Tightly Coupled Integration.

Item	Requirement
Cisco WebEx Meeting application	Version T27L SP 9 or later. Note that you can integrate only one Cisco WebEx Meeting application site with Cisco WebEx Messenger. To know which version of Cisco WebEx Meeting application you are currently running, type the URL of your Cisco WebEx Meeting application in the address bar of your Browser in the following format: https://[sitename].webex.com/version/wbxversionlist.do?siteurl=[sitename] Alternatively, contact your Cisco WebEx sales representative to obtain the version. XML API version 5.3.0 or later
Organization	• A Tightly Coupled Integration does not support Single sign-on for authentication. • A non-Single sign-on enabled Cisco WebEx Messenger organization can only be integrated with a non-Single sign-on enabled Cisco WebEx Meeting application site.

Provision Tightly Coupled Integration

The following describes the provisioning steps for each of the three Tightly Coupled Integration scenarios. For more information on the different scenarios for Tightly Coupled Integration, see Overview of Tightly Coupled Integration, on page 38.

Scenario 1: Tightly Coupled Integration Between a New Deployment of Both Cisco WebEx Messenger and Cisco WebEx Meeting Application

Make sure that the following preparatory steps are completed prior to enabling tightly coupled integration between Cisco WebEx Meeting application and Cisco WebEx:

1. The Cisco WebEx provisioning team creates a brand new Cisco WebEx Meeting application site.
2. The Cisco WebEx provisioning team creates a brand new Cisco WebEx Messenger organization with the Cisco WebEx Meeting application site (URL) specified for the Tightly Coupled Integration.
3. The integration is successful if the **Meetings** screen under the **Configuration** tab shows the Cisco WebEx Meeting application site URL. Additionally, when the Organization Administrator signs in to the Cisco WebEx Meeting application site, a corresponding Administrator account is automatically created in the site. For more information, see Verify the Success of Tightly Coupled Integration for a New Deployment of Both Cisco WebEx and Cisco WebEx Meeting Application, on page 41.

Scenario 2: Tightly Coupled Integration for a New Cisco WebEx Messenger Deployment with an Existing Cisco WebEx Meeting Application Deployment

Make sure that the following preparatory steps are completed prior to enabling tightly coupled integration between Cisco WebEx Meeting application and Cisco WebEx Messenger:

1. Modify the email addresses of all the Cisco WebEx Meeting application user accounts. The domain of the modified email addresses should match the Cisco WebEx Messenger organization's email domain. For example, if the existing email address of the Cisco WebEx Meeting application user account is user@domain.com and the new Cisco WebEx Messenger organization's email domain is acme.com, modify user@domain.com in Cisco WebEx Meeting application to user@acme.com.
2. Create Cisco WebEx Messenger accounts for existing Cisco WebEx Meeting application accounts. If you do not create Cisco WebEx Messenger accounts for existing Cisco WebEx Meeting application users, the Cisco WebEx Meeting application users will be unable to sign in to their Cisco WebEx Meeting application site. The remaining steps describe the procedure for creating Cisco WebEx Messenger accounts for existing Cisco WebEx Meeting application users.
3. Export all the Cisco WebEx Meeting application user accounts.
4. Open the exported file containing Cisco WebEx Meeting application user accounts. Modify the column headers as shown in the following table. There may be additional column headers than the ones listed below, however, they do not need to be modified or deleted.

Column Header Name	What to do
UserName	Delete this column
FirstName	Rename to firstName
LastName	Rename to lastName
Email	Rename to email
Address1	Rename to address1
Address2	Rename to address2
City	Rename to city
State/Prov	Rename to state
Zip/Postal	Rename to zipCode
Country/Region	Rename to country
PhoneCntry	Rename to phoneBusinessCountryCode
PhoneLocal	Rename to phoneBusinessNumber
CellCntry	Rename to phoneMobileCountryCode
CellLocal	Rename to phoneMobileNumber

Column Header Name	What to do
All tracking codes	Rename to "TC#" based the amount of defined tracking codes.

5 Save the file in the UTF-8 format or UTL-16 LE format.

6 Import this modified file into your Cisco WebEx Messenger organization via the Cisco WebEx Messenger Administration Tool.

7 Verify the Cisco WebEx Messenger accounts are created for Cisco WebEx Meeting application users by viewing the “status” and “statusMessage” columns in the import status file.

After the Tightly Coupled Integration is active, Cisco WebEx Meeting application users will no longer be able to sign in with their previous sign in credentials (username/password). Cisco WebEx Meeting application users signing in to Cisco WebEx Meeting application will be required to use their Cisco WebEx Messenger sign in credentials (username/password). Ensure that all users are aware of this change and the time of change. It is recommended for the Organization Administrator to notify all users of the proposed change well in advance.

Request the Cisco WebEx provisioning team to enable the Tightly Coupled Integration between Cisco WebEx Messenger and Cisco WebEx Meeting application.

8 See Verify the Success of Tightly Coupled Integration for a New Cisco WebEx Messenger Deployment with an Existing Cisco WebEx Meeting Application, on page 42 to verify successful integration.

Scenario 3: Tightly Coupled Integration for a New Cisco WebEx Meeting Application Deployment with an Existing Cisco WebEx Messenger Deployment

The provisioning steps for enabling a Tightly Coupled Integration for a New Cisco WebEx Meeting application deployment with an existing Cisco WebEx Messenger deployment is similar to enabling a Tightly Coupled Integration for a New Cisco WebEx Meeting application deployment with a new Cisco WebEx Messenger deployment. For more information, see *Scenario 1* above.

Verify the Success of Tightly Coupled Integration for a New Deployment of Both Cisco WebEx and Cisco WebEx Meeting Application

Make sure you have completed all the provisioning steps before verifying the success of a Tightly Coupled Integration between a new deployment of both Cisco WebEx and Cisco WebEx Meeting application. For more information, see *Scenario 1* of Provision Tightly Coupled Integration, on page 39

Procedure

Step 1 To verify the Tightly Coupled Integration is successful, select the **Configuration** tab and under the **Additional Services** section, select **Meetings**.

Step 2 Verify that the Cisco WebEx "ball" is displayed before the URL of the Cisco WebEx Meeting application site. The site URL cannot be changed.

Step 3 Select **Enable Meeting Integration** to enable the integration between Cisco WebEx and Cisco WebEx Meeting application.

If you are using Cisco WebEx version 7.2.2 or later and this checkbox is disabled, all meeting-related preference options and features will be hidden for the users in the Cisco WebEx application.

Step 4 Select the **Display to User** check box to display the Cisco WebEx Meeting application site URL to users in the host account setup section of the application.

Step 5 In the **Brief Description** box, enter a meaningful description for the Cisco WebEx Meeting application site.

Step 6 Select the **Select as Default** button against a particular Cisco WebEx Meeting application URL to indicate it as the default site to be displayed as the default site when a user sets up the host account in the application. If there is one Cisco WebEx Meeting application URL, it will be selected as default.

Step 7 Verify that **Automatically enable Meeting account when creating a new user** is selected by default. If you do not plan to provide the Cisco WebEx Meeting application service to all users by default, clear this check box.
This automatically creates a corresponding Cisco WebEx Meeting application account for each new user you create in your Cisco WebEx Messenger organization.

Note If you clear **Automatically enable Meeting account when creating a new user**, you need to manually enable the Cisco WebEx Meeting application account for each new user you create.

Step 8 To verify if the Cisco WebEx Meeting application account was automatically created, open the newly-created user's profile and click **Advanced Settings**.
The Cisco WebEx Meeting application **Site Administration** page opens showing the user's profile.

Step 9 Select **Save.**

Verify the Success of Tightly Coupled Integration for a New Cisco WebEx Messenger Deployment with an Existing Cisco WebEx Meeting Application

Before You Begin

Make sure you have completed all the provisioning steps before verifying the success of a Tightly Coupled Integration between a new deployment of both Cisco WebEx and Cisco WebEx Meeting application. For more information, see Provision Tightly Coupled Integration, on page 39

Procedure

Step 1 To verify the Tightly Coupled Integration is successful, select the **Configuration tab** > **Additional Services > Meetings**.

Step 2 Verify that the Cisco WebEx "ball" is displayed before the URL of the Cisco WebEx Meeting application site. The site URL cannot be changed.

Step 3 Select **Enable Meeting Integration** to enable the integration between Cisco WebEx and Cisco WebEx Meeting application.
If you are using Cisco WebEx version 7.2.2 or later and this checkbox is disabled, all meeting-related preference options and features are hidden for the users in the Cisco WebEx application.

Step 4 Select the **Display to User** check box to display the Cisco WebEx Meeting application site URL to users when they host and join meetings.

Step 5 In the **Brief Description** box, enter a relevant description for the Cisco WebEx Meeting application site.

Step 6 Select the **Select as Default** button against a particular Cisco WebEx Meeting application URL to indicate it as the default site to which users are directed for setting up their host account in the application.
If there is one Cisco WebEx Meeting application URL, it is selected as default.

Step 7 Verify that **Automatically enable Meeting account when creating a new user** is selected by default. If you do not plan to provide the Cisco WebEx Meeting application service to all users by default, clear this check box.
This automatically creates a corresponding Cisco WebEx Meeting application account for each new user you create in your Cisco WebEx Messenger organization.

Note If you clear **Automatically enable Meeting account when creating a new user**, you need to manually enable the Cisco WebEx Meeting application account for each new user you create.

Step 8 To verify if the Cisco WebEx Meeting application account was automatically created, open the newly-created user's profile and click **Advanced Settings**.
The Cisco WebEx Meeting application **Site Administration** page opens showing the user's profile.

Step 9 Select **Save**.

Verify the Success of Tightly Coupled Integration for a New Cisco WebEx Meeting Application Deployment with an Existing Cisco WebEx Messenger Deployment

Make sure you have completed all the provisioning steps before verifying the success of a Tightly Coupled Integration for a New Cisco WebEx Meeting application Deployment with an existing Cisco WebEx Messenger deployment. The provisioning steps are similar to that of a Tightly Coupled Integration for a New Cisco WebEx Meeting application deployment with a new Cisco WebEx Messenger deployment. For information on the provisioning steps, see the section titled *Scenario 3* under Provisioning Steps for Tightly Coupled Integration.

The steps for verifying if the Tightly Coupled Integration is successful is the same as described in the topic for Verifying the success of Tightly Coupled Integration for a new deployment of both Cisco WebEx Messenger and Cisco WebEx Meeting application.

After the Tightly Coupled Integration is complete, the Cisco WebEx Messenger Organization Administrator typically performs the following administrative tasks:

- Creates Cisco WebEx Meeting application accounts for existing or new Cisco WebEx Messenger users. For more information on creating users, see Create New Users, on page 12.
- Imports Cisco WebEx Meeting application accounts directly into Cisco WebEx Messenger using a CSV file. For more information, see Import and Export Users Using a CSV File, on page 13.

Overview of Loosely Coupled Integration

Loosely Coupled Integration enables customers to minimize the configuration required for the Cisco WebEx Messenger organization. Users benefit from Loosely Coupled Integration by not having to manually configure the Cisco WebEx Meeting application accounts in Cisco WebEx Messenger.

Loosely Coupled Integration is typically recommended for Organizations that have:

- Users who are Cisco WebEx Meeting application users but not Cisco WebEx Messenger users
- Existing Cisco WebEx Meeting application sites but do not want to change how users sign in to Cisco WebEx Meeting application sites

Two typical scenarios are available for enabling a Loosely Coupled Integration for an enterprise:

- Enterprises with Single sign-on Integration
- Enterprises without Single sign-on Integration

  The steps for enabling a Loosely Coupled Integration between Cisco WebEx Messenger and Cisco WebEx Meeting application vary for each of these scenarios. For more information about each scenario, see the following topics:

  - Provision Loosely Coupled Integration, on page 45
  - Verify the Success of Loosely Coupled Integration for Organizations with Single Sign-on Infrastructure, on page 45
  - Verify the Success of Loosely Coupled Integration for Organizations without Single Sign-on Infrastructure, on page 46

System requirements for Loosely Coupled Integration

Ensure that the following system requirements are met before you enable the Loosely Coupled Integration.

Item	Requirement
Cisco WebEx Meeting application	Version T26L with Service Pack EP 20 or Version T27L with Service Pack 9 To know which version of Cisco WebEx Meeting application you are currently running, type the URL of your Cisco WebEx Meeting application in the address bar of your Browser in the following format: https://[sitename].webex.com/version/wbxversionlist.do?siteurl=[sitename] Alternatively, contact your Cisco WebEx sales representative to obtain the version.

Item	Requirement
Organization	• A Single sign-on enabled Cisco WebEx Messenger organization can only be integrated with a Single sign-on enabled Cisco WebEx Meeting application site. • A non-Single sign-on enabled Cisco WebEx Messenger organization can only be integrated with a non-Single sign-on enabled Cisco WebEx Meeting application site.

Provision Loosely Coupled Integration

This topic describes the provisioning steps for enabling Loosely Coupled Integration between Cisco WebEx Messenger and Cisco WebEx Meeting application. The provisioning steps are the same for organizations with or without single sign-on infrastructure. Organizations without single sign-on infrastructure can integrate only one Cisco WebEx Meeting application site with Cisco WebEx Messenger. For more information on Loosely Coupled Integration, see Overview of Loosely Coupled Integration, on page 44.

Verify the following preparatory steps are completed before enabling a Loosely Coupled Integration between Cisco WebEx Messenger and Cisco WebEx Meeting application.

- Request the Cisco WebEx provisioning team to set up a Loosely Coupled Integration with a single sign-on enabled Cisco WebEx Meeting application site.
- Provide the Cisco WebEx Meeting application site URLs and Common User Identity between Cisco WebEx Messenger and Cisco WebEx Meeting application.
- Verify the success of the Loosely Coupled Integration by signing in to the Cisco WebEx Messenger Administration Tool.

Verify the Success of Loosely Coupled Integration for Organizations with Single Sign-on Infrastructure

Make sure that you have completed the provisioning steps before verifying the success of the integration. For more information, see Provision Loosely Coupled Integration, on page 45.

Procedure

Step 1 To verify the success of the Loosely Coupled Integration, select the **Configuration tab** > **Additional Services > Meetings**.

Step 2 If you have enabled the integration with multiple Cisco WebEx Meeting application sites, verify that all these sites are listed.

Step 3 Select **Set as default** for the Cisco WebEx Meeting application that will be the default for the Cisco WebEx Messenger organization.
Each time a user starts the One-Click Meeting from the Cisco Jabber application, this default site is used.

Step 4 Select **Save**.

Note The **Common User Identity** determines a one-to-one mapping of users between the Cisco WebEx Messenger and Cisco WebEx Meeting application.

Verify the Success of Loosely Coupled Integration for Organizations without Single Sign-on Infrastructure

Make sure that you have completed the provisioning steps before verifying the success of the integration. For more information, see Provision Loosely Coupled Integration, on page 45.

Procedure

Step 1 To verify the success of Loosely Coupled Integration, select the **Configuration tab** > **Additional Services > Meetings**.

Step 2 Verify that the Cisco WebEx Meeting application site URL for which you have enabled the Loosely Coupled Integration is displayed.

Note The **Activate Integration** button activates Tightly Coupled Integration with Cisco WebEx Meeting application. See, Overview of Tightly Coupled Integration, on page 38.

Integrate Older Cisco WebEx Messenger Organizations with Cisco WebEx Meeting Application

Procedure

Step 1 To enable integration between a Cisco WebEx Messenger organization and the Cisco WebEx application, select the **Configuration tab** > **Additional Services > Meetings**.

Step 2 In the **Site URL** field, enter the URL of the Cisco WebEx Meeting application site that you want to integrate with your Cisco WebEx Messenger organization. The **Site URL** field is blank for the first time.
After the site URL is configured, the **Meetings, Site Options** window is displayed.

Step 3 In the **Brief Description** box, enter a description for the Cisco WebEx application site for which you want to enable the integration.

Step 4 Select **Save** to save your Cisco WebEx Messenger and the Cisco WebEx application integration settings.

IM Federation Settings

Cisco WebEx Messenger can be configured to enable federation with public XMPP-based IM networks such as Google Talk. It also permits the use of third party XMPP applications to connect to your Cisco WebEx Messenger domain.

Note You can publish two types of records to DNS:

- Publishing the first SRV record enables your users to communicate with users of public XMPP networks
- Publishing the second SRV record enables your users to use third party XMPP applications and connect to your Cisco WebEx Messenger domain

Specify IM Federation Settings

Procedure

Step 1 To specify IM Federation settings, select the **Configuration** tab and under **Additional Services**, select **IM Federation**.

Step 2 Update your DNS SRV records according to the information displayed on the **IM Federation** screen.

Overview of IM Logging and Archiving

Cisco WebEx Messenger allows you to log and archive Instant Messages (IMs) that users in your organization exchange with each other or with users outside your organization. IM logging and archiving allows your organization to monitor and review IM exchanges. In most cases, this is done to comply with the enterprise's information audit processes.

You can enable IM logging and archiving for users in your Cisco WebEx Messenger organization. Cisco WebEx Messenger can send the logged messages for archival to the following archival solutions:

- HP Autonomy's DRC-CM (previously called Iron Mountain DRC-CM)
- Global Relay's Message Archiver
- Secure SMTP Service: This option allows you to configure a SMTP server to receive IMs within the body of an email. In this case, IMs become part of the same archival system as your emails enabling you to use the same archival and auditing solution that you use for email.

  HP Autonomy DRC-CM and Global Relay Message Archiver are Saas-based message archiving services.

Information Logged in an IM Session

The following is logged in an IM session:

- Date and Time
- Participants (user names)
- Plain text
- HTML (including the text equivalent of an emoticon)
- System messages such as invitations and participants joining and leaving.
- File transfer initiation and termination, including name of file, and size of file.
- Video call initiation and termination
- PC-to-PC call initiation and termination
- Audio conference initiation and termination
- Cisco WebEx Meeting initiation and termination
- Desktop Share initiation and termination
- Phone call initiation and termination

Restrictions for Logged IM Users

The following restrictions are applicable for logged IM users:

- Users whose IM needs to be logged must use the Cisco Jabber application version 9.x or later desktop client. However, other participants can be using older or different IM applications while participating in an IM session with the logged user.
- The system prevents usage of third-party IM applications for users that are being logged.
- Logged users must not have end-to-end (AES) encryption enabled. If a logged user has end-to-end encryption enabled, the “logged” status of the user will take precedence and end-to-end encryption will be disabled for the user.
- A logged user is unable to join a group chat session that is encrypted.
- A logged user cannot participate in a group chat hosted by a federated user (e.g. user on the AIM or GoogleTalk network). However, federated users can participate in a group chat hosted by a logged Cisco WebEx Messenger user.

  IMs are temporarily stored in Cisco data centers before they are transmitted to the customer's servers over a secure channel. Once the transmission is complete, these IMs are permanently deleted from Cisco data centers.

IM Archiving Notifications

By setting up IM archiving notifications you can choose whether or not to notify users that their IMs are being archived. This notification is sent by the system, and the the default message text is shown below.

All instant messages sent in this session to and from this account, as well as the initiation and termination of any other communication modes (e.g. voice call, video call) are logged and are subject to archival, monitoring, or review and/or disclosure to someone other than the recipient.

However, you can choose to override the default message text to suit your organization's requirements. For more information, see Set Up IM logging and Archiving Notifications, on page 52.

When one or more IM logged users are engaged in a one-to-one or group chat, the system sends a notification message to all users involved that their conversation is being logged and archived by one or more of the user's organizations.

IM Logging and Archiving Notification Frequency

Notifications are sent to all users in a conversation, one for each logged user in the conversation. For example, if five users are in a group chat where three are logged, three notifications are sent to all five users. The exceptions to this are as follows:

- To avoid duplication, users are sent one copy of notification messages with identical text. Regardless if users are in a one to one or group chat, if they are in organizations that are using an identical message text, default or custom, they see only one notification.
- If the organization of any logged user in a conversation is using a custom notification message, it is seen by all users. For example, if three users are in a group chat of which two have the default message and one has a custom message, all users see two notifications, the default and the custom.

  The system does not send notifications for specific conversations more than once an hour.

  After a notification timeout expires, no new notifications are sent unless there is new activity, such as the exchange of IM's or users joining group chats.

Defining an IM Archiving Endpoint

Setting up IM archiving for your Cisco WebEx Messenger organization involves configuring the archiving endpoint in Cisco WebEx Messenger Administration Tool. The IM archiving endpoint is the place to which the logged IM data is sent. You can configure multiple endpoints.

Endpoint configuration involves specifying the following parameters:

- Endpoint name
- Endpoint type
- Endpoint parameters: Parameters vary according to the endpoint type.

  To learn how to set up IM archiving endpoints, see Set Up IM Archiving, on page 50.

  After configuring IM archiving endpoints, you need to assign users in your Cisco WebEx Messenger organization to be logged. There are several provisioning methods that allow you to assign users to be logged as listed below:

- By creating new users. For more information, see Create New Users, on page 12.

- By using CSV files. For more information, see CSV File Format, on page 113.
- Through Directory Integration. For more information, see Directory Integration Import Process and File Formats, on page 98.
- Using SAML. For more information, see Configuration of Single Sign-on in Cisco WebEx Messenger Administration Tool, on page 55.

Enable IM Logging and Archiving for your Organization

IM Archiving is a separate solution that you need to get provisioned from Cisco WebEx. For information on how get IM Archiving provisioned for your organization, contact your Cisco WebEx Customer Success Manager.

Provisioning information is displayed in Cisco WebEx Administration Tool under Resource Management in the Configuration tab. IM Archiving will not work for users over and above the number of users your Cisco WebEx Messenger organization has been provisioned with. For more information, see Resource Management Information, on page 22.

Set Up IM Archiving

The **IM Archiving** screen enables you to set up endpoints for archiving instant messages exchanged between users in your Cisco WebEx Messenger organization. You can set up more than one endpoint. However, a user can be assigned to only one endpoint at a time.

Procedure

Step 1 To set up IM Archiving, select the **Configuration tab** > **IM Archiving**.
If you have not set up any endpoint, the **IM Archiving** window is blank.

Step 2 Select **Add** to open the **Add Archiving Endpoint** window.

Step 3 In the **Endpoint Name** field, type a name for the endpoint. Your endpoint name should not contain spaces.

Step 4 Depending on the type of endpoint you select, the fields that you need to fill in vary. From the **Type** drop down list, select the endpoint type:

- Global Relay Message Archiver
- HP Autonomy DRC-CM (previously called Iron Mountain DRC-CM)
- Secure SMTP Service

- **Note** Cisco WebEx Messenger always negotiates a secure connection to the archiving endpoint. The archiving endpoint needs the following settings for Secure SMTP Service:
  - Support of STARTTLS is required. Even if SSL is being used, the endpoint MUST support STARTTLS.
  - If using SSL use port 465 not port 25.
  - Certificates presented by the archiving endpoint must be issued by publicly trusted Certificate Authorities (CAs). Any self-signed certificates are not supported.

Step 5 After you have filled out all the fields, to test the endpoint configuration select **Test**.
You cannot save the endpoint unless the test is successful. If the test fails, a failure message is displayed.

Step 6 Select **View Results** to view the configuration problems that resulted in the test failure.
You can correct the problems and then select **Test** again. If the test is successful, a success message is displayed.

Step 7 After the configuration test is successful, select **Save** to save the endpoint configuration and return to the .

Step 8 To add another endpoint, follow the same steps described earlier in this section.

Step 9 Select **Refresh** if the endpoint you have successfully configured doesn't appear in the list of endpoints in the **IM Archiving** window.

Step 10 To set an endpoint as the default endpoint, select the appropriate button under the **Default Endpoint** column.
Any users not assigned to a specific endpoint (by name) are assigned to the default endpoint.

Step 11 If you have associated users with an endpoint, select **View Users** to view the list of users associated with that endpoint.

The endpoint begins to receive logs within a maximum of one hour. The system takes this time to register the endpoint.

Batching of IMs in an Email

The archiving service attempts to group messages between two users or a user and a group chat room in a single email. As user communication occurs in blocks, the service waits 8 hours before transmitting the series of user messages. This avoids a large set of emails, containing a very small number of IMs in each email, being sent. As a result of this batching, the mail endpoint does not receive any archived emails before those 8 hours have passed.

Note A maximum of 50 messages are batched at a time when transmitted to an archiving endpoint.

System behavior if an archiving endpoint is not reachable

In case the archiving endpoint is not reachable, Cisco WebEx Messenger retries delivering to the endpoint at 1 hour, 2 hour, 4 hour, and 8 hour intervals. Beyond this, Cisco WebEx Messenger retries once a day for a maximum period of 90 days. At each retry, an email notification is sent to the email address configured for your Organization Administrator. To view the log of each retry and response for the archiving endpoint, select **Configuration > IM Archiving > View Results**.

Important It is vital that the Organization Administrator take action to correct any issues with the archiving endpoint immediately upon receipt of the email notification so there is not a backlog of messages waiting to be transmitted.

Set Up IM logging and Archiving Notifications

The **IM Archiving** screen also enables you to send automatic notifications to IM users that instant messages exchanged between them are being logged and archived.

Procedure

Step 1 To set up IM logging and archiving notifications, select the **Configuration tab > IM Archiving** and do one of the following:

- Select **Notify users in your Organization that their IMs are being archived**. This is enabled by default; notifications are sent to all users in your organization when a one-to-one or group chat session is initiated with one or more logged users. When this setting is disabled, no notifications are sent to users in your organization.
- Select **Override default notification message** to edit the default archiving notification message text to suit your organization's needs. Custom notification messages are limited to 500 (UTF-8) characters.

  Note If you edited the default notification text but want to revert to the original default text, select **Reset**.

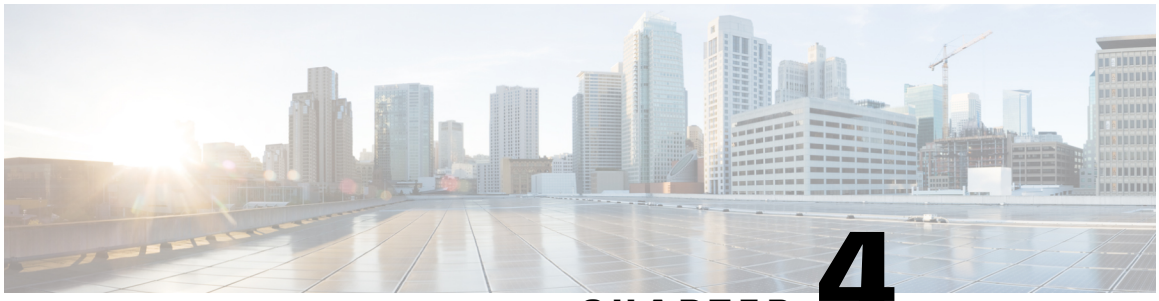
Step 2 Select **Save**.

Note Any changes to the above settings will take several hours to take effect. This is the length of time needed for the changes to propagate to all the servers.

The format of the IM transcript is sent to the archiving endpoint when instant messages are logged.

You can check details such as the logged message text, timestamps, and the subject of the email set in the endpoint.

The **Timestamps** denote the UTC time zone according to XEP-0082 protocol in the format CCYY-MM-DDThh:mm:ss.



CHAPTER 4

Single Sign-on

Overview

In a standard configuration, the sign in name and password of a user are independent from the authentication credentials used by their company or organization. This requires users to remember another set of sign in credentials. Additionally, Organization Administrators are required to manage a separate set of user accounts.

Single sign-on also permits companies to use their on-premise single sign-on system to simplify the management of Cisco WebEx Administration. With single sign-on, users securely sign in to the application using their corporate sign in credentials. The user's sign in credentials are not sent to Cisco WebEx, protecting the user's corporate sign in information.

As a single sign-on configuration option, user accounts can be automatically created the first time a user signs in. Single sign-on also prevents users from accessing Cisco WebEx application if their corporate sign in account has been deactivated.

The Cisco WebEx application supports single sign-on systems based on the industry standard Security Assertion Markup Language SAML2 and WS-Federation protocol.

Using SSO with the Cisco WebEx and Cisco WebEx Meeting Applications

One of the goals of the Cisco WebEx services is to provide comprehensive management of user identities for an organization. User identity management involves providing secure mechanisms for authentication and authorization. These mechanisms facilitate ease of use and policy controls based on the user's role and group affiliations inside the organization.

Federated Single sign-on standards such as SAML2 (Security Assertion Markup Language) and WS-Federation provide such secure mechanisms for authentication. SAML-compliant identity management systems send

SAML assertion to Cisco WebEx services. A SAML assertion is an XML document containing trusted statements about a subject. Typically, these trusted statements include information such as user name, email and other profile information. SAML assertions are digitally signed to ensure their authenticity.

Normally, enterprises deploy a federated Identity and Access Management system (IAM) to manage user identities. These IAM systems use SAML, and WS-Federation standards for user identity management activities. Some of the more prominent enterprise-class IAM systems include CA SiteMinder, Ping Federate, and Windows Active Directory Federation Services (ADFS). These IAM systems form part of an organization's corporate intranet which handles the user authentication and single sign-on requirements for employees and partners. IAM systems use the SAML or WS-Federation protocols to interoperate with partner websites outside their firewalls. Customers, partners, and vendors can utilize their IAM systems to automatically authenticate their users to Cisco WebEx services. This will increase efficiency as users are not required to recall their username and password to use Cisco WebEx services.

Additionally, employees leaving an organization do not have to be explicitly disabled in external administration tools. As soon as they are removed from the customers IAM system, they are not able to authenticate against any of the Cisco WebEx services.

Note Contact your Customer Success Manager to enable Single sign-on for Cisco WebEx Messenger.

Single Sign-on Requirements

The following system requirements are required to implement federated single sign-on for your Cisco WebEx organization. These system requirements are the same for Cisco WebEx Messenger and the Cisco WebEx Meeting applications.

Item	Requirement	Notes
Identity and Access Management (IAM) system	Any IAM that conforms to SAML versions (for Cisco WebEx Meeting only) 2.0 or WS-Federation 1.0 standard.	Customers can develop their own SAML-compliant IAM system using programming libraries such as OpenSAML or purchase commercial third party IAM systems such as Ping Federate, CA SiteMinder, Microsoft Windows Server ADFS, Oracle Identity Federation/OpenSSO, Novell Identity Manager and IBM Tivoli Federated Identity Manager.
X509 Certificate has public key, digitally sign uses private key	From trusted organizations like VeriSign and Thawte in the PEM format.	Alternatively, customers can serve their own X.509 certificates developed in house using self-signed certificates.

Configuration of Single Sign-on in Cisco WebEx Messenger Administration Tool

The Cisco WebEx Administration Tool allows the Organization Administrator to configure Single sign-on settings and modify the security setting and certificates for your Cisco WebEx Organization. Options are displayed based on organization settings set by the Administrator. Not all options are displayed at all times.

- Select **Federated Web SSO Configuration** to display the dialog for an administrator whose organization has turned on single sign-on.
- Select **Organization Certificate Management** to display the dialog for an administrator whose organization has turned on single sign-on or is a "Delegated Authentication" administrator. Used to manually import, validate, or remove X.509 certificates, Organization Certification Management is a management tool for Organization Administrators.
- Select **WebEx Certificate Management** to display the dialog for an administrator whose organization has turned on single sign-on. Used as a management tool for Organization Administrators to create service provider certificates, this tool is used for SP-initiated situations. A self-signed certificate by Cisco WebEx is generated and requires upload to the IAM system. Certificates are generated:
  - for signing the AuthnRequest
  - for SAML assertion encryption
  - to enable Single Logout

  A self signed certificate or a certificate authority will have been previously generated and made available for import. Administrators can select which to apply to the organization.
- Select **Partner Web SSO Configuration** to display the dialog for an administrator whose organization is "Delegated Authentication. Partner delegation allows administrators to setup up a single user name and password authentication sign on page for partner applications. Administrators should use this functionality to increase security and reduce multiple sign on and password requirements, eliminating the need for users to track multiple sign on credentials.
- You can also set SAML 2.0 configurations. Attributes are displayed in the following table:

Attribute	Required (Yes/No)	Usage
uid	Yes	
firstname	Yes	
lastname	Yes	
email	Yes	
groupid	No	Supports only create, not update
updateTimeStamp	No, but recommended	Supports long value, UTC time format, & LDIF time format

Attribute	Required (Yes/No)	Usage
displayName	No	
companyName	No	
businessFax	No	
streetLine1	No	
streetLine2	No	
city	No	
state	No	
zipcode	No	
jobTitle	No	
mobilePhone	No	
businessPhone	No	
employeeid	No	
imloggingenabled	No	When an organization has IMLogging enabled, and if no such attribute exists, it would be set to false.
imloggingendpointname	No	When an organization has IMLogging enabled, and if no such attribute exists, it would be set to wbx_default_endpoint.
ISOCountry	No	2-letter ISO country code
upgrade site	No	If there is a not-null 'upgradesite' attribute, the action will correspond with the (enabled/disabled) auto account creation and auto account update features. If the 'upgradesite' attribute is not provided or the value is empty, no action is required.

Note The Allow Connect account username and password login via CAS API checkbox is selected in a transition phase when an organization is moving their authentication mechanism from "username/password store in the cloud" to SSO with an IdP. It allows the organization to move gradually over to SSO.

Configure Federated Web SSO

Procedure

Step 1 Select the **Configuration tab** > **System Settings > Security Settings**.

Step 2 Select **Federated Web SSO Configuration** .

Step 3 From the **Federation Protocol** drop down, select the federation protocol **SAML 2.0**.
The fields displayed in the window vary based on the selected federation protocol. By default, the configuration fields for SAML 2.0 is displayed each time the **Federated Web SSO Configuration** window opens.

Step 4 **Select Import SAML Metadata** to open the **Federated Web SSO Configuration - SAML Metadata** dialog box.

Step 5 Perform one of the following:

- Navigate to and import the SAML Metadata file to autofill the federated Web authentication fields.
- Select **Import**, **Back** to complete the import. Imported metadata fields include:
  - AuthnRequestSigned Destination
  - Issuer for SAML (Idp ID)
  - Customer SSO Service Login URL
- Enter the appropriate information for each field.
  See the Related Topics section.

Step 6 After the SAML Metadata file has been successfully imported, verify that the relevant fields in the **Federated Web SSO Configuration** window have been populated.

Related Topics

Federated Web SSO Settings, on page 58

Federated Web SSO Settings

Field	Description
SSO Profile	SP Initiated - When a user visits a service provider (SP) site and first accessing resources that do not require special authentication or authorization. In an SAML-enabled deployment, when they subsequently attempt to access a protected resource at the SP, the SP will send the user to the IdP with an authentication request in order to permit the user to sign in. AuthnRequest Signed Destination - When selected, a WebEx certificate and destination must be specified. This destination address must match the authnRequest signed configuration in the IAM.
	IdP Initiated Target page URL Parameter - If the user visits Cisco WebEx service (SP), SP sends the user to IDP without an authentication request.
WebEx SAML Issuer (SP ID)	The URI identifies the Cisco WebEx Messenger service as an SP. The configuration must match the settings in the customer Identity Access Management. The default value is http://www.webex.com.
Issuer For SAML (IdP ID)	A URI uniquely identifies the IdP.The configuration must match the settings in the customer IAM.
Customer SSO Service Login URL	URL for your enterprise's single sign-on service. Users in your enterprise will typically sign in via this URL.
You can export an SAML metadata WebEx SP configuration file: Exported metadata fields include: • AuthnRequestSigned Destination • Issuer for SAML (Idp ID) • Customer SSO Service Login URL	
NamedID Format	This field must match the IAM configuration. The following formats are supported: • Unspecified (default) • Email address • X509 Subject Name • Entity Identifier • Persistent Identifier
AuthnContextClassRef	The SAML statement that describes the act of authentication at the identity provider.This field must match the IAM configuration.

Field	Description
Default WebEx Target page URL	Optional. Upon authentication, displays a target page assigned for the web application only. The request does not contain a RelyState parameter.
Single Logout for Web Client	Check to require a sign out and set the log out URL. **Note:** This option is only applicable to the web IM application.
Auto Account Creation	Select to create a user account. UID, email, and first and last name fields must be present in the SAML assertion.
Auto Account Update	Specify the "updateTimeStamp" attribute in the SAML assertion and check this field to update an existing user account. The "updateTimeStamp" value is the last update time of a user's profile in the customer's Identity store. For example, in Active Directory, the "whenChanged" attribute has this value. If "updateTimeStamp" is not in the attribute, the user profile would not be updated since the last update. It updates the first time when the user profile is updated via Auto Account Update or Auto Account Creation. Unchecked indicates no updates will occur.
Remove uid Domain Suffix for Active Directory UPN	The Active Directory domain part will be removed from the UPN when selected. Cisco WebEx Messenger uid's require the email domain; therefore, when this field is checked, it will cause an error. In this case, use "ssoid" to identify the user. The default is unchecked for SAML 2.0 and WS-Federation 1.0.

Configure WS Federation

After the SAML Metadata file has been successfully imported, verify the relevant fields in the **Federated Web SSO Configuration** dialog box have been populated.

Procedure

Step 1 From the **Federation Protocol** drop down list, select the federation protocol **WS-Federation 1.0**. The fields displayed in the **Federated Web SSO Configuration** dialog box vary based on the selected federation protocol.

Step 2 Enter the following additional information:

- WebEx Service URI: The URI identifies the Cisco WebEx Service relying party.
- Federation Service URI: The URI identifies the enterprise's single sign-on service (IdP).

- Customer SSO Service Login URL: URL for your enterprise's single sign-on service. Users in your enterprise will typically sign in via this URL. Depending on the single sign-on Profile, the IdP-Initiated login URL and SP-Initiated sign in URL would be set accordingly to match IdP settings.

Step 3 Select **Save** to save the Federated Web single sign-on Configuration details and return to the **SSO Related Options** window.

Configure Organization Certificate Management

Procedure

Step 1 Select **Organization Certificate Management** to display the available certificates.
Certificates are limited to a maximum of three and only one can be active at any given time. Previously imported X.509 certificates are displayed.

Step 2 Select a certificate link in the **Certificate Alias** column to view certificate details and, optionally, select **Remove** to remove the certificate.

Step 3 Select **Import New Certificate**.
The **Organization Certificate Management** window appears.

Step 4 In the **Organization Certificate Management** window, enter your company's Cisco WebEx Organization name in the **Alias** field.

Step 5 Select **Browse** to navigate to the X.509 certificate.
The certificate should be in a cer or crt file format. Only certificates with 1024, 2048 or 4096 encryption bits and RC4-MD5 algorithms are supported.

Step 6 Select **Import** to import the certificate.
If the certificate is not according to the format specified for an X.509 certificate, an error is displayed.

Step 7 Select **Close**.

Step 8 Select **Save** to save your newly imported organization certificate and return to the **SSO Related Options** screen.

Configure WebEx Certificate Management

Procedure

Step 1 Select **WebEx Certificate Management** to display previously generated Cisco WebEx certificates.

Step 2 To generate a new certificate, select **Generate New Certificate**.
New certificates are typically generated when an existing certificate is about to expire.

Step 3 In the **WebEx Certificate Management** window, enter the following information:

- **Alias:** An alias that identifies the WebEx Certificate.
- **Val:** The number of days the WebEx Certificate is valid. A WebEx Certificate is valid for a minimum of 90 days and maximum of 3652 days.

Step 4 Select a Certificate Alias to view the complete details of the generated certificate.

Step 5 In the generated certificate screen, select:

- **Remove**: to delete the certificate. Active certificates cannot be removed.
- **Export**: to export and save the certificate as a .cer file to your computer.

Step 6 Select **Close** to return to the **WebEx Certificate Management** window.

Step 7 Select the **Active** option to apply this (newly-generated) WebEx Certificate as the active certificate for single sign-on related authentication purposes.

Step 8 Select **Save** to save your WebEx Certificate changes and return to the **SSO Related Options** window.

Step 9 Import the active Cisco WebEx certificate to the IdP.

Partner Delegated Authentication

Partner delegation allows administrators to setup up a single user name and password authentication sign on page for partner applications. Administrators should use this functionality to increase security and reduce multiple sign on and password requirements, eliminating the need for users to track multiple sign on credentials.

Requirements for partner delegated authentication

A trust must be established between a customer and a partner. The partner acts on behalf of its customer's user to log on to the Cisco WebEx service via the partner route. Partner Delegated Authentication consists of the following attributes used to build trusted and consented relationships:

- Customer and Cisco WebEx service (trust)
- Partner and Cisco WebEx service (trust)
- Customer and Partner (trust and consent)

Configure Partner Delegated Authentication

Procedure

Step 1 Use **WebEx Certificate Management** to upload the certificate.

Step 2 Use **Partner Web SSO Configuration** to configure SAML 2.0 settings.

Step 3 Select **Partner Delegated Authentication** to display the dialog for an administrator whose organization is not “Delegated Authentication”.

Step 4 Trust the partner to act as member or member plus an organization administrator

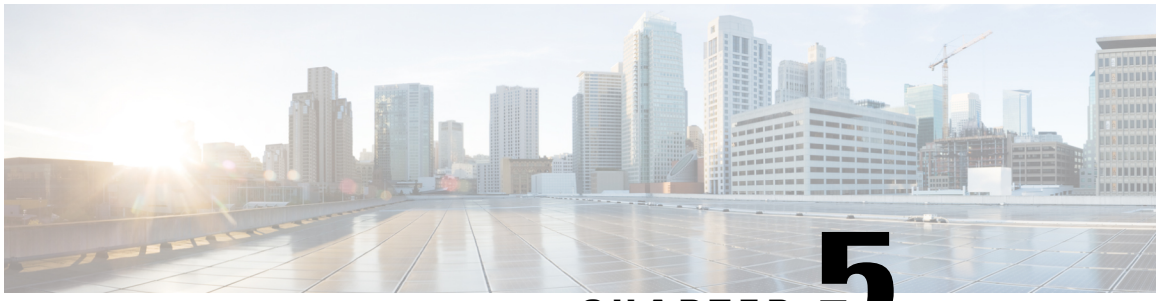
Step 5 Set the corresponding **NameID field**.

Configure Partner Web Single Sign-on

Procedure

Step 1 Select **Partner Web SSO Configuration**.

Step 2 If you have not imported SAML configurations, select **Import SAML Metadata** to open the Partner Web Single sign-on configuration - SAML metadata dialog box.
For more information, see Configure Federated Web SSO, on page 57



CHAPTER 5

Cisco Unified Communications Integration with Cisco WebEx

Overview

The Cisco Unified Communications (UC) integration with Cisco WebEx (Click-to-Call) enables you to create and configure new clusters for each of the following types of Cisco UC integration available for Cisco WebEx:

- Cisco WebEx Click-to-Call
- Cisco UC Integration with Cisco WebEx
- Cisco UC Manager Express Integration with Cisco WebEx

It is recommended that the following topics be reviewed prior to proceeding:

- Set Up Cisco Unified Communications Manager for Click-to-Call, on page 71
- Unified Communications, on page 64
- *Cisco Unified Communications Manager Express* documentation available at http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmeadm.html

Typically, an enterprise is comprised of several Cisco Unified Communications Manager (Unified Communications Manager) clusters. Each of these clusters can be a Cisco WebEx Click-to-Call cluster or Cisco UC integration with Cisco WebEx cluster. Users are assigned to a Unified Communications Manager cluster based on certain predefined grouping criteria. A typical example of a grouping criterion is to assign users to a CUCM cluster based on their phone numbers.

Cisco Unified Communications Integration (Click-to-Call)

Cisco Unified Communications Integration settings work only for users on Cisco WebEx application versions 6.x or earlier. Cisco Unified Communications Integration enables you to use Cisco WebEx to make calls to another computer or phone. You can specify the settings for a specific Click-to-Call cluster or use the default settings provided for the entire organization. For more information, see Configure Cisco Unified Communication for Click-to-Call, on page 68.

Cisco UC Integration (Unified Communications Manager) Cisco WebEx

The Cisco UC Integration for Cisco WebEx adds a phone tab to Cisco WebEx. This new space turns your computer into a full-featured phone, permitting you to place, receive, and manage calls. The Cisco UC Integration with Cisco WebEx comprises these following broad steps:

- Configuring the Unified Communications Manager with the Device Type, and setting dial rules. For more information, see the *CUCI-Connect Configuration Guide* available at http://www.cisco.com/en/US/products/ps10627/products_installation_and_configuration_guides_list.html.
- Specifying the Cisco UC Integration with Cisco WebEx settings in the Cisco WebEx Administration Tool. For more information, see Configure Cisco Unified Communication for Click-to-Call, on page 68.
- Visual Voicemail is available with only Cisco WebEx application version 7 or later. Visual Voicemail is an alternative to the audio voicemail service. For more information, see Configure Visual Voicemail, on page 66.

Cisco UC Call Manager Express (CME) Integration with Cisco WebEx

For more information, see the *Cisco Unified Communications Manager Express* documentation available at http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmeadm.html.

Unified Communications

integration with Cisco WebEx includes specifying configuration options for these components:

- Cisco Unified Communications Integration (Click-to-Call)
- Cisco UC Integration for Cisco WebEx
- Cisco UC Manager Express Integration for Cisco WebEx

  You can configure these components either at your Cisco WebEx organization level or by creating a cluster for each component.

  To open the **Unified Communications** window, select the **Configuration tab** > **Unified Communications**.

  The three tabs available are:

- **General tab**: Used to specify Cisco WebEx Click-to-Call settings and the URL to download the Cisco UC Integration for Cisco WebEx Setup Program. For more information, see Cisco WebEx Click-to-Call, on page 65.

Note Applies only to Cisco WebEx 6.x.

- **Voicemail tab**: Used to specify Visual Voicemail settings. For more information, see Configure Visual Voicemail, on page 66.
- **Clusters tab**: Used to create, modify and delete Cisco Unified Communications Clusters.

Cisco WebEx Click-to-Call

Cisco WebEx Click-to-Call settings work only for users on Cisco WebEx application versions 6.x. The configuration settings apply only to users in your Cisco WebEx organization that do not belong to any cluster. For more information about creating Cisco Unified Communications Clusters, see Create Unified Communications Clusters, on page 67.

Refer to the following for more information:

-
- Configure Click to Call Task Flow, on page 72
- Cisco Unified Communications Manager, on page 71
- Configure Cisco Unified Communication Manager Integration with Cisco WebEx Messenger, on page 68
- *CUCI-Connect Configuration Guide* available at http://www.cisco.com/en/US/products/ps10627/products_installation_and_configuration_guides_list.html

Configure Cisco WebEx Click-to-Call

Procedure

Step 1 To configure Cisco WebEx Click-to-Call, select the **Configuration tab**.
The **System Settings** window opens.

Step 2 Select **IM** .
The **General IM** window opens.

Step 3 Select **Unified Communications** .
The **Unified Communications** window opens.

Step 4 Under **Cisco WebEx Click-to-Call Settings**:

- Select **Enable Cisco WebEx Click-to-Call by default** to enable Click-to-Call integration for your organization by default. This option enables Click-to-Call integration for your organization whether or not you have created a separate Click-to-Call cluster.
- In the **Cisco Unified Communications Manager (CUCM)** box, enter the IP address or server name for the Cisco Unified Communications Manager server configured for your Cisco WebEx Organization.

  Note Unless you select **Enable Cisco WebEx Click-to-Call by default,** you will be unable to enter settings for Cisco Unified Communications Manager.

- Select **Allow user to enter manual settings** to permit the users of your Cisco WebEx Organization to manually specify Click-to-Call settings. If you select this option, the user-entered settings will override the default Click-to-Call settings entered by the Organization Administrator.

Step 5 Under **Cisco UC Integration for Cisco WebEx Settings**, enter the URL for **Cisco UC Integration for Cisco WebEx Setup Download URL**. This URL enables your Cisco WebEx Organization's users to download the Setup program, which installs the Cisco Unified Communications Integration (CUCI) feature on the Cisco WebEx application.

Step 6 Select **Save**.

Visual Voicemail

Visual Voicemail is available with only Cisco WebEx application version 7 or later. The Visual Voicemail application is an alternative to the audio voicemail service. With Visual Voicemail, you can use the screen on your phone to work with your voice messages. You can view a list of your messages and play your messages from the list. You can also compose, reply to, forward, and delete messages.

Note Cisco UC Integration for Cisco WebEx must also be configured to use this service.

When you enable the integration of Cisco WebEx with Visual Voicemail, you can directly view your Visual Voicemail from within the Cisco WebEx application. Before enabling the integration of Cisco WebEx with Visual Voicemail, we recommend reading the following documentation:

- *Planning to Install Visual Voicemail* available at http://www.cisco.com/en/US/docs/voice_ip_comm/cupa/visual_voicemail/7.0/english/install/guide/plan.pdf
- *Installation and Configuration Guide for Visual Voicemail* available at http://www.cisco.com/en/US/docs/voice_ip_comm/cupa/visual_voicemail/7.0/english/install/guide/Installation_and_Configuration_Guide_for_Visual_Voicemail_Release_70.pdf
- *CUCI Connect Configuration Guide* available at http://www.cisco.com/en/US/products/ps10627/products_installation_and_configuration_guides_list.html

Note The settings entered are the default visual voicemail settings for clusters and are not configured for a specific server. Additionally, each cluster must be individually enabled. For more information, see Create Unified Communications Clusters, on page 67

Configure Visual Voicemail

Procedure

Step 1 To configure Visual Voicemail, select the **Configuration tab** > **Unified Communications**.

The **Unified Communications** window opens.

Step 2 Select **Voicemail** to open the **Default settings for Visual Voicemail for CUCI** screen.
Unity Connection customers should enter the Unity Connection server IP Address or DNS name into the "Voicemail Server" and "Mailstore Server" fields. It is recommended that all other settings remain as the defaults.

Step 3 To enable Visual Voicemail, select **Enable Visual Voicemail**.

Step 4 If you want to manually enter the Visual Voicemail settings, select **Allow user to enter manual settings**.

Step 5 Enter the following information:

- **Voicemail Server**: Name of the Visual Voicemail server with which the Cisco WebEx application should communicate for retrieving voicemail.
- **Voicemail Protocol**: Protocol used for communicating with the Visual Voicemail server. You can select HTTPS or HTTP.
- **Voicemail Port**: Port associated with the Visual Voicemail server.
- **Mailstore Server**: Name of the mailstore server.
- **Mailstore Protocol**: Protocol used by the mailstore server. You can select TLS or Plain.
- **Mailstore Port:** Port associated with the mailstore server.
- **IMAP IDLE Expire Time**: Time (in minutes) after the expiry of which the server stops automatically checking for voicemail.
- **Mailstore Inbox Folder Name**: Name of the inbox folder configured at the mailstore server.
- **Mailstore Trash Folder Name**: Name of the trash folder (typically, the deleted items folder) configured at the mailstore server.

Step 6 Select **Save**.

Create Unified Communications Clusters

Complete the procedures for following Cisco Unified Communications components to configure Cisco Jabber:

- Cisco Unified Communication settings for Click-to-Call
- Cisco Unified Communication Manager integration with Cisco Jabber
- Cisco Unified Communication Manager Express integration with Cisco Jabber
- Cisco TelePresence Video Communication Server

Because the configuration steps vary between these UC components, the configuration instructions are explained in multiple parts. Refer to the following documentation:

- *CUCI-Connect Configuration Guide* available at http://www.cisco.com/en/US/products/ps10627/products_installation_and_configuration_guides_list.html.
- *Cisco Unified Communications Manager Express* documentation available at http://cisco.com/en/US/docs/voice_ip_comm/cucme_webex/configuration/guide/webexconnect_cme.html

Configure Cisco Unified Communication for Click-to-Call

Organization administrators should contact their customer support representative for CUCI provisioning

Procedure

Step 1 Select the **Configuration tab** > **Additional Services > Unified Communications**.

Step 2 Select **Clusters**.
Previously created clusters are displayed.

Step 3 Select **Add**.

Step 4 Enter a name for the new cluster in the **Cluster Name** box.

Step 5 If it is not already selected, select **Enable Cisco WebEx Connect Click-to-Call**.

Step 6 Select **Allow user to enter manual settings** to permit all users belonging to this cluster to specify their Cisco Unified Communication Manager settings.

Note When you enable this option, user-entered settings will override the default or global Click-to-Call settings specified for the Cisco WebEx organization.

Step 7 In the **Cisco Unified Communications Manager** box, enter the IP Address of Unified Communication Manager configured for your Cisco WebEx organization. Ensure that your Unified Communication Manager includes a Device Type called **Client Services Framework** (CSF).

Step 8 Select **Save** to save the Click-to-Call cluster settings and return to the **Unified Communications** screen.
For more information on configuring your Unified Communication Manager to work with CSF, refer to the section titled Preparing Cisco Unified Communications Manager in the *CUCI-Connect Configuration Guide* available at
http://www.cisco.com/en/US/products/ps10627/products_installation_and_configuration_guides_list.html.

The new Click-to-Call cluster is now displayed under **Cisco Unified Communications Clusters.**

Configure Cisco Unified Communication Manager Integration with Cisco WebEx Messenger

Procedure

Step 1 Select the **Configuration tab** > **Additional Services > Unified Communications** .

Step 2 Select the **Clusters** tab and select**Add** .

Step 3 Select **Enable Cisco UC Manager integration with Cisco WebEx Connect**.

Step 4 Select **Allow user to enter manual settings** to permit users to change the Primary Server values in basic mode or the TFTP/CTI/CCMCIP Server values in advance mode.

Note When this option is enabled, the user-entered settings will override the default or global Unified Communications Manager settings specified for the Cisco WebEx organization.

Step 5 Under **Cisco Unified Communications Manager Server Settings**, select:

- **Basic Server Settings**: to enter the basic settings for the Unified Communications Manager server.

- **Advanced Server Settings**: to enter advanced or more detailed settings for the Unified Communications Manager server.

Note The Server configuration options changes based on: Basic or Advanced.

Step 6 Enter the following values for **Basic Server Settings**:

- **Primary Server**: Enter the IP address of the primary Unified Communications Manager server. This server is configured with TFTP, CTI, and CCMCIP settings.
- **Backup Server**: Enter the IP address of the backup Unified Communications Manager server. This server is configured with TFTP, CTI, and CCMCIP settings and provides failover support in case the primary Unified Communications Manager server fails.

Step 7 If you have selected **Advanced Server Settings**, specify each setting for TFTP (Trivial File Transfer Protocol), CTI (Computer Telephony Integration), and CCMCIP (Cisco Unified Communications Manager IP Phone) servers.

Step 8 Enter the IP address for each of the following servers:

Note You can specify up to two backup servers for the TFTP server and one backup server each for the CTI and CCMCIP servers. Enter the appropriate IP addresses for each Backup Server.

- **TFTP Server**
- **CTI Server**
- **CTI Server**

Step 9 In the **Voicemail Pilot Number** box, enter the number of the voice message service in your Cisco Unified Communications system.
The Organization Administrator typically provides a default voice message number for your entire Cisco WebEx organization. However, you can select the **Allow user to enter manual settings** check box to enable users of the cluster to override this default voice message number.

Step 10 Enter the **LDAP Server Settings** information if you Cisco WebEx organization is set up with Directory Integration.
To obtain LDAP server settings, contact your company or Organization's IT administrator. LDAP server settings are applicable only for users on Cisco WebEx client versions 6.x or earlier.

Step 11 Select **Voicemail**.

Step 12 Select **Enable Visual Voicemail**.
The Visual Voicemail settings entered here are applicable only to the users belonging to this cluster.

Step 13 In the **Clusters** tab, select **Specific voicemail server for this cluster** to specify a voicemail server, which is different from the voicemail server settings provided for the entire organization.

Step 14 Select **Allow user to enter manual settings** to permit users to manually enter Visual Voicemail settings for this cluster.
For information on entering specific Visual Voicemail settings, see Configure Visual Voicemail, on page 66

Step 15 Select **Save** to save the Unified Communications configuration.
For detailed information about the TFTP, CTI, and CCMCIP servers, see CUCI-Connect Configuration Guide located at
http://www.cisco.com/en/US/products/ps10627/products_installation_and_configuration_guides_list.html.

Configure Cisco Unified Communication Manager Express Integration with Cisco WebEx Messenger

Procedure

Step 1 Select the **Configuration tab** > **Additional Services > Unified Communications**.

Step 2 Select the **Clusters tab** > **Add** .
The **New Cluster** page opens.

Step 3 Select **Enable Cisco UC Manager Express integration with Cisco WebEx Connect**.

Step 4 Select the **Download** link to obtain and download the latest software release.
The Cisco Unified CME integration download server settings are not auto populated. The download should be considered a plugin for Cisco WebEx Messenger.

Step 5 Select **Allow user to enter manual settings** to permit organization administrators to provide default values and permit users to modify their Primary Server values.

Step 6 Select **Save**.

Configure Cisco TelePresence Video Communication Server

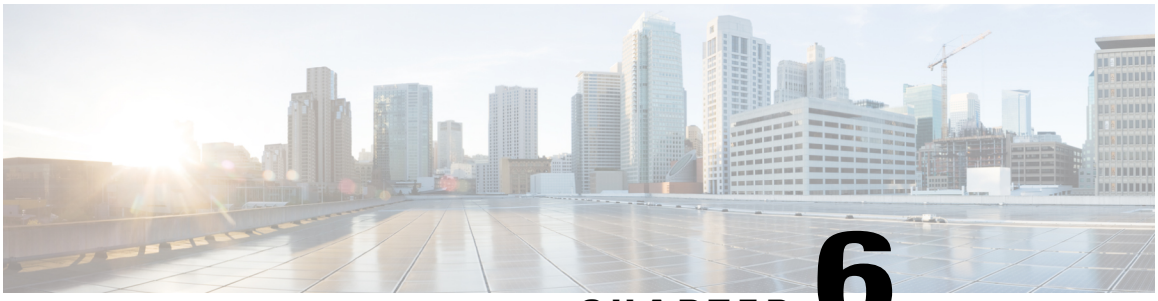
Procedure

Step 1 Select the **Configuration tab** > **Additional Services > Unified Communications**.

Step 2 Select the **Clusters** tab and select **Add**.

Step 3 Select **Enable Cisco TelePresence Video Communication Server**.

Step 4 Select **Allow user to enter manual settings** to permit organization administrators to provide default values but allow users to modify their Internal/External Server and SIP Domain values.



CHAPTER 6

Set Up Cisco Unified Communications Manager for Click-to-Call

Overview

Cisco's call-processing software, telephones, and endpoint devices allows your company or organization to efficiently run voice, data, and video communications over a single, converged network.

Cisco provides call-processing solutions for organizations of all sizes and types. These industry-leading IP private-branch-exchange (PBX) solutions manage voice, video, mobility, and presence services between IP phones, media processing devices, voice-over-IP (VoIP) gateways, mobile devices, and multimedia applications. Cisco call-processing solutions include the Cisco Unified Communications Manager.

The Cisco Unified Communications Manager Click-to-Call service is an optional feature and not available in Cisco WebEx by default. Click-to-Call is offered as a free service. However, your Organization Administrator needs to enable it. Contact your Cisco sales representative for more information.

Cisco Unified Communications Manager

This enterprise IP telephony call-processing system is the core of Cisco Unified Communications. It provides voice, video, mobility, and presence services to IP phones, media-processing devices, VoIP gateways, mobile devices, and multimedia applications. This powerful call processing solution can help:

- **Build productivity** with feature-rich unified communications that help workers spend less time chasing people, and more time being productive.
- **Enable mobility** with software that has embedded unified mobility capabilities so mobile workers can remain productive wherever they are.

Cisco Unified Communications Manager creates a unified workspace that supports a full range of communications features and applications with a solution that is highly:

- **Scalable:** Each Cisco Unified Communications Manager cluster can support up to 30,000 users and scale to support up to 1 million users at up to 1000 sites.
- **Distributable:** For scalability, redundancy, and load balancing.
- **Available:** Support business continuity and improve collaboration with high availability that provides a foundation for multiple levels of server redundancy and survivability.

Configure Click to Call Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Cisco Unified IP Phones, on page 72	Use to add and configure an IP Phone to Cisco Unified Communications Manager.
Step 2	Add a Directory Number to the Phone, on page 73	Use to add a directory number to the IP Phone.
Step 3	Activate Cisco WebDialer on Cisco Unified Communications Manager, on page 73	Use to activate Cisco WebDialer on Cisco Unified Communications Manager.
Step 4	Verify the CTI Manager is Running on Cisco Unified Communications Manager, on page 74	Use to verify the CTI Manager is Running on Cisco Unified Communications Manager.
Step 5	Verify the CCMCIP Service is Running on Cisco Unified Communications Manager, on page 74	Use to verify the CCMCIP Service is Running on Cisco Unified Communications Manager.
Step 6	Verify the Correct Phone Devices are Associated with the User, on page 75	Use to verify the Correct Phone Devices are Associated with the User.

Configure Cisco Unified IP Phones

Before a Cisco Unified IP Phone can be used, you must use this procedure to add the phone to Cisco Unified Communications Manager. You can also configure third-party phones that are running SIP, H.323 clients, CTI ports, the Cisco ATA 186 Telephone Adaptor, or the Cisco IP Communicator.

Procedure

Step 1 Select **Device** > **Phone > Add New**.

Step 2 From the **Phone Type** list, select the appropriate phone type or device and select **Next**.
After you select a phone type, you cannot modify it.

Step 3 If the **Select the device protocol** list is displayed, choose the appropriate protocol of the device and select **Next.**
The **Find and List Phones** window is displayed.

Step 4 Enter the appropriate settings. For more information see, *Cisco Unified Communications Administration Guide*.

Step 5 Select **Save**.

What to Do Next

Add a Directory Number to the Phone, on page 73

Add a Directory Number to the Phone

When a pattern is used as a directory number, the display on the phone and the caller ID that displays on the dialed phone will both contain characters other than digits. To avoid this, Cisco recommends that you provide a value for Display (Internal Caller ID), Line text label, and External phone number mask.

Before You Begin

Configure Cisco Unified IP Phones, on page 72

Procedure

Step 1 To add a directory number to the phone, select one of the line links, such as **Line [1] - Add a new DN**, in the **Association Information** section that displays on the left side of the window.

Step 2 Enter a valid phone number. The directory number that you enter can appear in more than one partition.

Step 3 Select **Save.**

Step 4 Select **Reset Phone.**

Note Restart devices as soon as possible. During this process, the system may drop calls on gateways.

For more information, see the *Cisco Unified Communications Administration Guide*.

What to Do Next

Activate Cisco WebDialer on Cisco Unified Communications Manager, on page 73

Activate Cisco WebDialer on Cisco Unified Communications Manager

Cisco Unified Communications Integration (Click-to-Call) uses the SOAP interface to interact with the WebDialer servlet on Cisco Unified Communications Manager. Because Click-to-Call does not use the HTTP interface, the application does not interact with the Redirector servlet.

Before You Begin

Add a Directory Number to the Phone, on page 73

Procedure

Step 1 Select **Cisco Unified Communications Manager Serviceability** > **Tools > Service Activation**.
Step 2 Select the **Cisco Unified Communications Manager** server from the server drop-down list.
Step 3 In CTI Services, check **Cisco WebDialer Web Service**.
Step 4 Select **Save**.

What to Do Next

Verify the CTI Manager is Running on Cisco Unified Communications Manager, on page 74

Verify the CTI Manager is Running on Cisco Unified Communications Manager

The CTI Manager must be running on Cisco Unified Communications Manager for Cisco Unified Communications Integration (Click-to-Call) to function properly.

Before You Begin

Activate Cisco WebDialer on Cisco Unified Communications Manager, on page 73

Procedure

Step 1 Select **Cisco Unified Communications Manager Serviceability** > **Tools > Control Center > Feature Services**.
Step 2 Select the Cisco Unified Communications Manager server from the server drop-down list.
Step 3 In Call Manager Services, verify **Cisco CTIManager** is running.

What to Do Next

Verify the CCMCIP Service is Running on Cisco Unified Communications Manager, on page 74

Verify the CCMCIP Service is Running on Cisco Unified Communications Manager

Cisco Unified Communications Integration (Click-to-Call) retrieves the phone type for the user from the CCMCIP (Cisco CallManager Cisco IP Phone Services) service, and displays the phone type on the **Phone Preferences** screen in Click-to-Call. Because the CCMCIP service only runs on Cisco Unified Communications Manager release 6.x or later, this procedure is only applicable if you are running this Cisco Unified Communications Manager release.

Before You Begin

Verify the CTI Manager is Running on Cisco Unified Communications Manager, on page 74

Procedure

Step 1 Select **Cisco Unified Communications Manager Serviceability** > **Tools > Control Center - Network Services**.

Step 2 Select the Cisco Unified Communications Manager server from the server drop-down list.

Step 3 In CM Services, verify **Cisco CallManager Cisco IP Phone Services** is running.

What to Do Next

Verify the Correct Phone Devices are Associated with the User, on page 75

Verify the Correct Phone Devices are Associated with the User

You need to verify that the correct phone devices are associated with the user on Cisco Unified Communications Manager. If not, the phone is not listed on the **Phone Preferences** screen in Click-to-Call.

Before You Begin

Verify the CCMCIP Service is Running on Cisco Unified Communications Manager, on page 74

Procedure

Step 1 Select **Cisco Unified Communications Manager Administration** > **User Management > End User**.

Step 2 Select **Find**.

Step 3 Select the appropriate user ID.

Step 4 In the **Device Association** section, verify the correct devices are listed in the **Controlled Devices** window.

Note If you need to associate a phone device with the user, select Device Association. Consult the Cisco Unified Communications Manager Online Help for further information.

Configure Application Dial Rules

You can configure dial rules for applications that automatically strip numbers from, or add numbers to, a telephone number that a user dials. For example, you can use dial rules to automatically prefix a digit to a telephone number to provide access to an outside line.

You configure application dial rules on Cisco Unified Communications Manager from **Cisco Unified Communications Manager Administration > Call Routing > Dial Rules > Application Dial Rules**.

This section provides a brief description of application dial rules. For detailed information on configuring the application dial rules on Cisco Unified Communications Manager, refer to the following:

- The Application Dial Rules Configuration section in the *Cisco Unified Communications Manager Administration Guide*

- The Dial Plans section in the *Cisco Unified Communications Manager Administration Guide*
- Sample Application Dial Plan, on page 76
- Configure Cisco WebDialer to Automatically Use Application Dial Rules on Cisco Unified Communications Manager, on page 77

Sample Application Dial Plan

Name/Description	Number Begins With	Number of Digits	Total Digits to be Removed	Prefix with Pattern
International 12 Digit	+	12	1	9011
International 13 Digit	+	13	1	9011
International 14 Digit	+	14	1	9011
International 15 Digit	+	15	1	9011
Local 7 Digit XXX-XXXX		7		9
Local 10 Digit (510) XXX-XXXX	510	10	3	9
National 10 Digit (XXX) XXX-XXXX		10		91
National 11 Digit 1(XXX) XXX-XXXX		11		9

In the sample application dial plan above, 9 represents the off-net access code for outside dialing. For domestic calls, you append the appropriate quantity of digits to the off-net access code to call either a local number or a national (long-distance) number. In each international dial rule, you replace the "+" with the off-net access code and the appropriate international dialing access code.

These application dial rules are configured in the sample dial plan above:

- Any international number, the application dial rule removes "+" from the number, and prepends the off-net access code 9 and the international dialing access code 011 to the remaining digits.
- Any local seven digit number, the application dial rule prepends the off-net access code 9.
- Any local ten digit number that begins with 510, the application dial rule removes 510 from the number and prepends the off-net access code 9 to the remaining digits.

- Any national ten digit number, the application dial rule prepends the digits 91.
- Any national eleven digit number beginning with 1, the application dial rule prepends the off-net access code 9.

If the **Number Begins With** field is blank, you leave the number of initial digits open that you wish to apply to the dial rule. For example, the initial digits 1, 1408, or 1408526 will each match the dialed number 14085264000.

You must configure the application dial rule list in order of priority.
Cisco Unified Communications Manager applies the *first* dial rule match that it finds for the dialed number in the dial rule list; it does not attempt to find the best match in the list. For example, if you configure the dial rule conditions listed below, on receipt of the dialed number 14085264000, Cisco Unified Communications Manager ignores dial rule 1, and applies dial rule 2 as it is the first match. Although dial rule 3 is the best match, Cisco Unified Communications Manager ignores any subsequent rules in the list after finding the first match.

1 Begins with 9 and is 8 digits long, then do X.

2 Begins with 1 and is 11 digits long, then do Y.

3 Begins with 1408 and is 11 digits long, then do Z.

Note You can also configure directory lookup rules on Cisco Unified Communications Manager. Directory lookup rules transform the number the user dials into a directory number. For further information, refer to the Directory Lookup dial Rules Configuration in the *Cisco Unified Communications Manager Administration Guide*.

Configure Cisco WebDialer to Automatically Use Application Dial Rules on Cisco Unified Communications Manager

Procedure

Step 1 Select **Cisco Unified Communications Manager Administration** > **System > Service Parameters**.

Step 2 Select the Cisco Unified Communications Manager server from the **Server** menu.

Step 3 Select **Cisco WebDialer Web Service** from the **Service** menu.

Step 4 Select **True** for the **Apply Application Dial Rules on Dial** parameter.

Step 5 If you are running Cisco Unified Communications Manager release 6.x or 7.x, select **True** for the **Apply Application Dial Rules on SOAP Dial** parameter.

Step 6 Restart the Cisco WebDialer service.

Troubleshooting

The following topics provide troubleshooting information when you encounter problems when using Cisco Unified Communications Manager:

- Click-to-Call log files and configuration files
- Click-to-Call Log Files
- Error Messages, on page 78

Error Messages

This table provides a list of error messages that can appear in the Cisco Unified Communications Integration (Click-to-Call) application and describes a recommended action for each error message.

Error message	Problem and recommended action
A connection error occurred. Verify Click-to-Call is running	• A call was attempted using the Click-to-Call functionality when the Click-to-Call application is not running. • Ask the end user to restart the Click-to-Call application.
A directory error occurred. Contact your phone administrator	• The Cisco Unified Communications Manager directory service may be down. • Allow a short time lapse and retry your connection. If the error occurs again, contact your Cisco Unified Communications Manager system administrator.
A service error occurred. Retry the call. If the problem persists, contact your phone administrator	• An internal error occurred in the WebDialer application. • Contact your Cisco Unified Communications Manager system administrator.
Cannot make call. Verify Click-to-Call is running	• Ask the end user to restart the Click-to-Call application.
Click-to-Call cannot find Cisco IP Communicator. Verify it is running or select another phone	• Ask the end user to verify that their Cisco IP Communicator soft phone is running properly or to select a phone to use with the Click-to-Call application.

Error message	Problem and recommended action
Click-to-Call is not fully configured	• One or more mandatory fields in the sign in screen have been left blank. • Ask the end user to enter the missing information on the sign in screen and retry.
Destination cannot be reached	• The end user dialed the wrong number or you have not applied the correct dial rules. • Check that the Cisco WebDialer service is configured to use the application dial rules on Cisco Unified Communications Manager.
Login failed. Verify your user name and password are correct	• Provide the end user with the correct username and password for the Cisco Unified Communications Manager server. • Ask the end user to enter the username and password at the sign in screen and retry.
No phone is available. Verify contact your phone administrator	• Ask the end user to verify and refresh the phone preferences in the Phones screen of the Click-to-Call Preferences.
No phone has been selected for use with Click-to-Call. Select a phone	• The end user has no phone selected to use with the Click-to-Call application. • Ask the end user to select a phone to use with the application from the Click-to-Call application.
Proxy authentication rights could not be found. Contact your phone administrator	• Cisco WebDialer service sends this error. Contact your Cisco Unified Communications Manager system administrator.
Service is temporarily unavailable. Retry the call. If the problem persists, contact your phone administrator	• The Cisco Unified Communications Manager service is overloaded. It has reached its limit of two concurrent sessions. • Allow a short time lapse and retry your connection. If the error occurs again, contact your Cisco Unified Communications Manager system administrator.

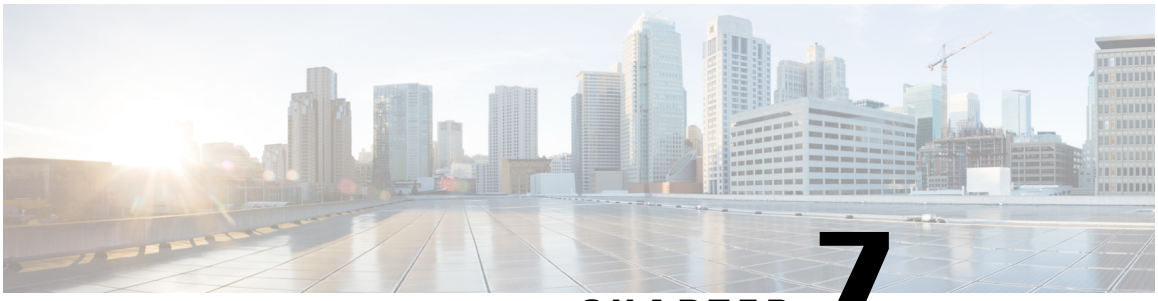
Error message	Problem and recommended action
The service is overloaded. Retry the call. If the problem persists, contact your phone administrator	• The Cisco Unified Communications Manager service is overloaded. It has reached its limit of two concurrent sessions. • Allow a short time lapse and retry your connection. If the error occurs again, contact your Cisco Unified Communications Manager system administrator.
The URL you requested is not available. Contact your phone administrator	• Provide the end user with the correct Cisco Web Dialer and/or Device Query service IP address. • Ask the end users to enter this information in the sign in screen and retry.
The XML command is not available in the request. Contact your phone administrator	• This is an error sent from the Cisco WebDialer service. Contact your Cisco Unified Communications Manager system administrator.
<*Number*> cannot be converted to a valid phone number	• The phone number the end user has entered is invalid. • Ask the end user to edit the phone number and retry the call.
The maximum phone number length is 32 digits	• The phone number the end user has entered is too long. • Ask the end user to edit the phone number and retry the call.
Invalid XML command. Contact your phone administrator	• Cisco WebDialer service sends this error. Contact your Cisco Unified Communications Manager system administrator.
Cisco WebDialer service cannot be found. Verify the address	• Provide the end user with the correct Webdialer server address. • Ask the end user to enter this server address on the sign in screen and retry.

Error message	Problem and recommended action
The call failed. Verify you are logged into your Extension Mobility device. If the problem persists contact your phone administrator	• A call request is already in progress or the Cisco WebDialer service could not get a line on the phone device from the CTI. • Wait a few moments and then retry your connection. If the error occurs again, contact your Cisco Unified Communications Manager system administrator.

This table provides a list of error messages that can appear in the Phone tab (Cisco Unified Communications Manager integration) of the Cisco Jabber application and describes a recommended action for each error message.

Error message	Problem and recommended action
If you still have problems, contact your system administrator.	• An error was encountered when retrieving account or device information. • If the end user has an account, a retry button is displayed.
Client tried to register with invalid credentials.	• The end user has entered an invalid username or password. • Ask the end user to register again using a valid username and password.
Unable to connect to backend server; your call cannot be completed. Please try again.	• The connection to the backend Cisco Unified Communications Manager server failed. • The Cisco Unified Communications Manager address may be invalid. Check the address and retry the connection.
The requested feature/capability is not currently available.	• The deskphone service was shut down by the server. • Contact your Cisco Unified Communications Manager system administrator.
Could not connect to CCMCIP.	• The softphone service was disconnected by the server. • Contact your Cisco Unified Communications Manager system administrator.

Error message	Problem and recommended action
Unable to select this device. Please choose a different device and try again.	• The selected device is unknown or has been removed. • Select a different device and try to connect again.
Failed to hold a call.	• An error was encountered when a call hold was requested. • Try to hold the call again by pressing the **Hold** button. If the problem persists, restart the client application.
Failed to merge calls.	• An error was encountered when a call merge was requested. • Try to merge the calls again. If the problem persists, restart the client application.
Max Call Limit exceeded.	• The maximum number of lines allowed has been reached. No more calls can be made.
No device selected. Please select the device you want to use and try again.	• The timeout for selecting a device has been reached. • Select the device and try connecting again.
Unable to access the default line. Please contact your administrator.	• The timeout for selecting the default line has been reached. • Contact your Cisco Unified Communications Manager system administrator.
Due to temporary restrictions, you cannot make calls now. Please wait a few moments and try again.	• Calls cannot be made. This may be due to service failover or fallback. • Allow a short time lapse and then try to make the call again.



CHAPTER 7

Policy Editor

Overview

Cisco WebEx provides a Policy Editor to define and apply policies for your groups. Policies can be used to enable or disable features such as file transfer, desktop sharing, archiving IM sessions, and automatically upgrading Cisco WebEx. You can apply policies for all the users within your Cisco WebEx organization or to a specific groups of users.

You cannot apply policies to an individual.

Policies and Policy Actions

A policy is a set of rules that includes actions which determine the Cisco WebEx features available to groups of users or to an entire Cisco WebEx organization. Thus, a policy can include multiple actions which are enabled, disabled, or available for advanced configuration. For example, a customer who wants to restrict certain Cisco WebEx capabilities for New Employees can create a policy named **New Employee Policy** and associate various actions with that policy.

An action is a Cisco WebEx capability that can be regulated via policies. For example, the **External File Transfer** action corresponds to the capability of exchanging files with users outside the Cisco WebEx organization.

Defining and Applying Policies

It is important to understand the difference between Organization level policies and group level policies.

When you create new users in your Cisco WebEx organization, they do not belong to any groups by default. All default policy actions therefore apply to your entire Cisco WebEx organization. This is because the top-level group, typically created at the time of provisioning includes all the users of the Cisco WebEx organization.

When the Organization Administrator creates groups and applies specific policies to these groups, the group-level policies override the organization-level policies. Users belonging to these groups are now be governed by the group-level policies instead of the organization-level policies. For example, if the Organization Administrator applies a policy that prohibits external VOIP communications for a particular group, users of that group are unable to communicate using VOIP. However, external VOIP communications may still be enabled for all other users in the organization.

You can apply policies at the Organization level or to specific groups. However, if there is a conflict in policy settings between the organization level and group level (or between a parent group and its sub-groups), the most restrictive actions take effect. For example, if VOIP capability is turned on (**Enabled**) at the organization level, but turned off (**Disabled**) at the group level, VOIP capability for all users within the group is disabled. However, if VOIP capability is turned off at the organization level but the group has enabled it, VOIP capability is still disabled for the users of the group.

The Policy Editor

Use the Cisco WebEx Administration Tool to set policies. You can set different policies for each group and make changes to your policies at any time. If your Cisco WebEx organization is newly provisioned, all capabilities are enabled for all users by default, except the capability that requires users to use AES encryption.

Note If you have modified or updated any policy, you need to first sign out of Cisco WebEx and then sign in again for the updated policy to take effect.

To learn how to apply policies to your groups, see Assign Policies to a Group, on page 95.

Add a Policy

Procedure

Step 1 Select the **Policy Editor** tab.
The **Policy List** appears to the left and the **Action List** appears at the right of the **Policy** screen.

Step 2 Under **Policy List**select **Add**.
The new policy appears at the top of the list of existing policies.

Step 3 Enter a unique name for the policy.

What to Do Next

To add actions for this policy, see Add Actions to a Policy, on page 85

Add Actions to a Policy

Procedure

Step 1 Select the **Policy Editor** tab.
The **Policy List** appears to the left and the **Action List** appears at the right of the **Policy Editor** screen.

Step 2 Under **Policy Name** select the policy to which you want to add actions.

Step 3 To add actions, select **Add** under **Action List** on the right of the screen.
The **Action Editor** screen appears.

Step 4 Select a policy action from the **Action Tag Name** list.
For more information on these actions, see Policies and Policy Actions, on page 83

Step 5 Select **Save**.

Step 6 Repeat Steps 3-5 until all of your policies have actions assigned to them.

Policy Actions Available in Cisco WebEx

This section describes the policy actions available in Cisco WebEx. The description also includes information about the impact a policy action has on the features that it controls. This enables you to set the most appropriate policies on the groups that you administer. For information on how to view and set policy actions, see Add Actions to a Policy, on page 85.

By default, a newly provisioned Cisco WebEx organization has all the capabilities granted to all the users. This means all Cisco WebEx features are available to all users by this default policy action.

Note Only the end-to-end encryption policy is not enabled by default. The Organization Administrator needs to explicitly enable this policy. Administrators then need to create policies only if specific capabilities for all the users or specific groups of users need to be disabled.

Policy actions cannot be enforced on users using third-party XMPP IM applications.

No more than 10 VoIP conference attendees can be connected to the same VoIP conference simultaneously.

External users are users who do not belong to the Cisco WebEx organization but can still use Cisco WebEx to communicate with users who belong to the Cisco WebEx organization.

Policy Action	Description	Impact	Default Value
External File Transfer	Controls file transfer in an IM session between organization users and users outside the organization.	Setting this policy action to **Disabled** will stop all file transfers between the organization users and external users, including multi-party IM sessions with at least one external user.	**Enabled**

Policy Action	Description	Impact	Default Value
Internal File Transfer	Controls file transfer in an IM session between users within the organization.	Setting this policy action to **Disabled** will stop all internal file transfers. When this policy action is not explicitly set to **Disabled**, all the users within the organization will have the ability to exchange files with the internal users.	**Enabled**
External IM	Controls IM sessions between users in the organization and users outside the organization.	Setting this policy action to **Disabled** will stop all IM sessions between users in the organization and users outside the organization. This will also stop all dependent services like voice, video, and VOIP.	**Enabled**
External VOIP	Controls VOIP communications in IM sessions between users in the organization and users outside the organization	Setting this policy action to **Disabled** will stop all VOIP communications in IM sessions between users in the organization and users outside the organization. However, other services like text-based IM sessions and file transfers will be available	**Enabled**
Internal VOIP	Controls VOIP communications in IM sessions between users within the organization.	Setting this policy action to **Disabled** will stop all VOIP communications in IM sessions between users within the organization. However, other services like text-based IM sessions and file transfers will be available. When this policy action is not explicitly set to **Disabled**, all the users within the organization will have the ability to use VOIP communications in IM sessions.	**Enabled**
External Video	Controls video services in IM sessions between users in the organization and users outside the organization	Setting this policy action to **Disabled** will stop all video services in IM sessions between users within the organization and users outside the organization. However, other services like text-based IM sessions and file transfers will be available.	**Enabled**
Internal Video	Controls video services in IM sessions between users within the organization.	Setting this policy action to **Disabled** will stop all video services in IM sessions between users within the organization. However, other services like text-based IM sessions and file transfers will be available. When this policy action is not explicitly set to **Disabled**, all the users within the organization will have the ability to use video communications in IM sessions.	**Enabled**

Policy Action	Description	Impact	Default Value
Local Archive	Controls the ability of the user to locally archive IM text messages.	Starting with the 7.1 application, previous stored local history will be deleted when this policy is set to **Disabled**. In the Cisco WebEx application, the following option is disabled: **Edit > Settings > General IM > Message Archive**. If you are upgrading from Cisco WebEx version 5.x to 6.x, the chat history archive stored on the users' local computers will be deleted and cannot be recovered. It is recommended that the Organization Administrator communicates this to all Cisco WebEx organization users. Additionally, users need to backup their individual chat archives before Cisco WebEx is upgraded to a newer version. Beginning with 7.1, local history will be deleted when this policy is set to **Disabled**.	**Enabled**
Join Workspace			**Enabled**
Join External Workspace			**Enabled**
External Desktop Share	Controls the ability of users within the organization to share their desktop with users outside the organization.	Setting this policy action to **Disabled** prevents users within the organization from sharing their (local) desktop with users outside the organization. When this policy action is not explicitly set to **Disabled**, users can share their (local) desktop with users outside the organization.	**Enabled**
Internal Desktop share	Controls the ability of users within the organization to share their desktop with other users within the organization.	Setting this policy action to Unchecked prevents users within the organization from sharing their desktop with other users within the organization. When this policy action is not explicitly set to **Disabled**, users can share their desktop with other users inside the organization.	**Enabled**
Workspace Feature			**Enabled**

Policy Action	Description	Impact	Default Value
Invite Users to Workspace			**Enabled**
Invite Users External Workspace			**Enabled**
Support End-to-End Encryption For IM	Enables users to specify support for end-to-end Encryption for IM sessions.	Setting this policy action to **Enabled** will allow support for end-to-end Encryption for IM sessions. If a user is designated to be logged, the end-to-end encryption policy setting will be overridden to be FALSE. End-to-end encryption is not supported for logged users. For more information, see Overview of IM Logging and Archiving, on page 47.	**Disabled**
Support NO Encoding For IM	Controls whether applications with end-to-end encryption enabled can initiate an IM session with applications that do not have end-to-end encryption enabled or with 3rd party applications that do not support end-to-end encryption.	Setting this policy to **Disabled** prevents applications with end-to-end encryption enabled from initiating an IM session with applications that do not have end-to-end encryption enabled or with 3rd party applications that do not support end-to-end encryption. **Note** If the Support End-to-End Encryption For IM is set to **Enabled**, the encryption level negotiated is the highest level that the other party supports. For more information about encryption levels, see Encryption Levels, on page 90.	**Enabled**
Internal IM (including White Listed domains)	Controls IM communication between users within the organization and specific domains on the white list.	Setting this policy action to **Disabled** will prevent users within the organization from being able to IM users within the domains specified in the white list. However, users within the domain will continue to be able to IM each other. Setting this policy action to **Disabled** will also disable other dependent services such as VOIP, Video and FileTransfer.	**Enabled**
Upload Widgets			**Enabled**

Policy Action	Description	Impact	Default Value
Allow user to edit profile	Controls the ability to restrict users from editing their profile information.	Setting this policy action to **Disabled** will prevent users from editing their profile information. This policy action impacts the settings in the **Profile Settings** screen under the **Configuration** tab.	**Enabled**
Allow user to edit the view profile setting	Controls the ability to restrict groups of users from changing their user profile view settings.	Setting this policy action to **Disabled** prevents users from changing their user profile view settings. This policy action impacts the **Allow users to change their profile view settings** check box in the **Profile Settings** screen under the **Configuration** tab. When this policy action is set to **Disabled**, the **Allow users to change their profile view settings** check box will have no impact even if it is selected.	**Enabled**
Internal Screen Capture	Controls users' ability to send a screen capture to users within the organization.	Setting this policy action to **Disabled** prevents users within the organization from sending screen captures within the organization.	**Enabled**
External Screen Capture	Controls users' ability to send a screen capture to users outside of the organization.	Setting this policy action to **Disabled** prevents users within the organization from sending screen captures outside of the organization.	**Enabled**
Send Internal Broadcast Message	Controls users' ability to send broadcast messages to users within the organization.	Setting this policy action to **Disabled** prevents users within the organization from sending broadcast messages inside the organization.	**Enabled**
Send External Broadcast Message	Controls users' ability to send broadcast messages to users outside of the organization.	Setting this policy action to **Disabled** prevents users within the organization from sending broadcast messages outside of the organization.	**Enabled**
Allow user to send broadcast to a directory group	Controls users' ability to send broadcast messages to a directory group within the organization.	Setting this policy action to **Disabled** prevents users within the organization from sending broadcast messages to a directory group within the organization.	**Enabled**

Policy Action	Description	Impact	Default Value
HD Video	Controls the HD Video feature on computer to computer calls when External Video or Internal Video policies are enabled	Setting this policy action to **Disabled** will prevent HD Video for all computer to computer calls.	**Enabled**

Organization Administrators who want to disable the following policy actions for all users should set their value to FALSE:

- Internal VoIP
- External VoIP
- Internal Video
- External Video
- Internal File Transfer
- External File Transfer
- Internal Desktopshare
- External Desktopshare

Encryption Levels

Typically, all IM communication between Cisco WebEx applications are encrypted both within the Cisco WebEx organization and outside of it. The IM communication is encrypted at the originating Cisco WebEx application and decrypted at the destination application. This encryption applies to all forms of IM communication including text, desktop (and application) sharing, file transfer, VOIP, and video.

Cisco WebEx provides three levels of encryption:

- **256-bit Advanced Encryption Standard (AES)/End-to-End encryption**: Provides an additional layer of security, where data is encrypted using AES at the application and decrypted only at its destination.
- **128-bit Secure Sockets Layer (SSL)**: Connectivity between an application and the SSL termination point in the data center is encrypted. In Cisco WebEx version 6 or later, Cisco WebEx applications always use SSL (Secure Sockets Layer) to connect to Cisco WebEx Data Centers.
- **No encryption**: The data is not encrypted, but connectivity maybe SSL (for Cisco WebEx version 5.x). For Cisco WebEx version 6 or later, connectivity is always SSL.

  The level of encryption depends on the policy set by the Organization Administrator. The Organization Administrator can apply the encryption policy either across the Cisco WebEx organization or to specific groups.

  The Cisco WebEx application automatically determines its encryption level from the policy applicable to the user logged into the application. Therefore, if a Cisco WebEx organization's policy settings do not allow a particular encryption level, the IM session will be disallowed and the applicable error message will be displayed to all applications in the IM session.

Note In a group IM scenario, the encryption level will be negotiated between all the users when the initial invite is sent out. After the IM session is established, subsequent attendees will need to support the negotiated encryption level to be able to participate.

The following example explains a typical encryption policy for IM sessions.

An organization that chooses to adopt end-to-end encryption can choose from these policy options:

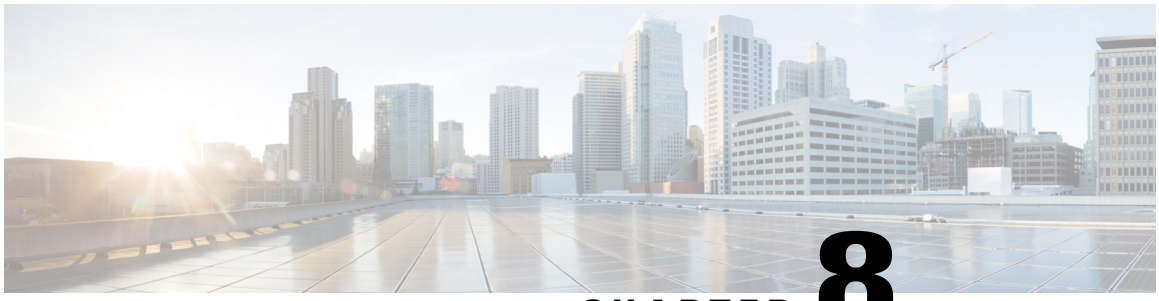
- Allow only end-to-end encryption. Do not set end-to-end encryption exclusively if you have users that you need to log IMs for. This is because IM logging will take precedence over end-to-end encryption.
- Allow both end-to-end encryption and SSL encryption. This option is applicable if you are using Cisco WebEx version 5.x.
- Allow end-to-end encryption, SSL encryption, and no encryption.

  In the Action Editor, you need to set **Enabled** or **Disabled** for each of these encryption levels based on the policy option you choose.

The following table illustrates the impact of these policy options.

Application A Policies	**Application B Encryption Level**		
	End-to-end encryption	**SSL**	**SSL**
Only end-to-end encryption	End-to-end encryption	Don't allow	Don't allow
End-to-end encryption or SSL	End-to-end encryption	SSL	Don't allow
End-to-end encryption or SSL or no encryption	End-to-end encryption	SSL	No encryption

In the Action Editor, you need to set **Enabled** or **Disabled** for each of these encryption levels based on the policy option you choose.



CHAPTER 8

Cisco WebEx Messenger Groups

Overview

The Cisco WebEx Messenger organizes users into groups (or policy groups). The Organization Administrator can:

- Create a new group
- Assign group policies
- Edit groups
- Delete groups
- Organize groups

The groups are assigned group policies to determine what actions are applied to users belonging to a particular group. Users can be members of one or more groups. Assigning a policy to a group involves selecting the group and the policy that you want to apply. You can assign multiple policies to a group. If a group contains child groups, the policies you assign to the parent group also apply to the child groups. However, the policies that you assign to a child group do not apply to the parent group. For more information about policies, see Policies and Policy Actions, on page 83.

A group can only be deleted if the group is empty with no associated users. However, if a group is not empty, you can delete any users that belong to multiple groups. You cannot delete the top-level group, which was created when your Cisco WebEx Messenger organization was provisioned.

A top-level group, named with your company, or organization's name is created when your Cisco WebEx Messenger organization is provisioned. The Organization Administrator role can only be assigned to users who are members of the top level group.

As the Organization Administrator you can organize groups in a hierarchical manner by creating parent and child groups. The topmost group in the groups hierarchy is always the top-level group created when your Cisco WebEx Messenger organization is provisioned. You cannot create another parent group above the top-level group. You can create any number of parent and child groups under this top-level group.

Note Cisco WebEx Messenger sees a personal library appear as a group associated with a user, but this group cannot be modified.

To view the **Group** window, select the **Group** tab in to the Cisco WebEx Messenger Administration Tool.

Note The following options are not available when your Cisco WebEx Messenger organization is set up with Directory Integration and single sign-on integration:

- Creating new groups
- Editing existing groups
- Deleting existing groups

Create a New Group

Procedure

Step 1 To create a new group, select the **Group tab** > **Add**.
The name of the **Parent Group** is always displayed at the top of this dialog box.

Step 2 Select to open the **Add Group** dialog box.

Step 3 In the **Group Name** field, enter a name for the group.

Step 4 Select **OK** .

Edit a Group

Editing a group involves only renaming it.

Procedure

Step 1 To edit a group, select the **Group** tab.

Step 2 In the **Search** field, enter at least one letter of the group that you want to edit and select **Search**.

Step 3 Choose the group and select **Rename**.

Step 4 In the **Group Name** field, enter the new name for the group and select **OK** .
Your renamed group is now visible in the **Group** screen.

Delete a Group

Procedure

Step 1 To delete a group, select the **Group** tab.

Step 2 In the Search field, enter at least one letter of the group that you want to delete and select **Search**.

Step 3 Choose the group and select **Delete**.

Step 4 Select **OK** in the message box to delete the selected group.
You cannot retrieve a deleted group.

Assign Policies to a Group

Procedure

Step 1 To assign policies to a group, select the **Group** tab.

Step 2 In the **Search** field, enter at least one letter of the group for which you want to assign policies and select **Search.**

Step 3 In the list of groups that match your search term, select the group for which you want to assign policies.

Step 4 In the **Policy Assignment** frame, select the policies you want to apply.
You can select one policy at a time. A brief pause indicates that your policy is being assigned.

Step 5 To unassign a policy, clear the check box next to the appropriate policy.

View Top Level, Parent, and Child Groups

Procedure

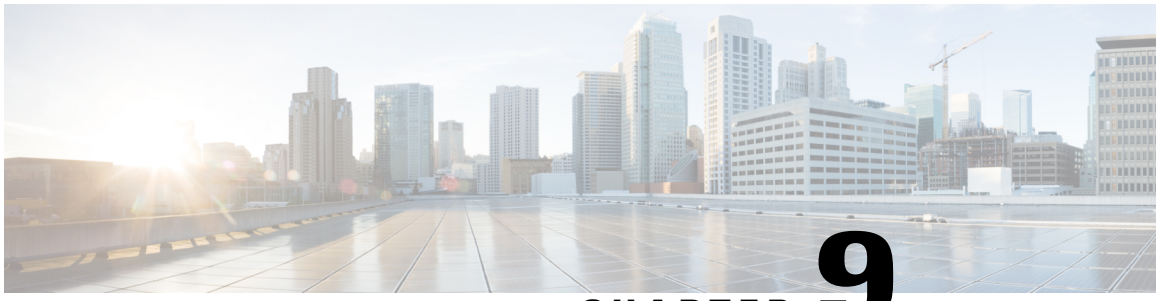
Step 1 To view top-level, parent and child groups, select the **Group** tab.

Step 2 In the **Search** field, enter at least one letter of the group whose parent or child groups you want to view and select **Search**.

Step 3 Choose the group and select **More Actions.**

Step 4 From the **More Actions** list, select one of the following as required:

- **View Group Users:** to view the list of users belonging to the selected group. The list of users is displayed in the **User** screen under the **User** tab.
- **Top Level Group:** to view the top level group of the selected group. The top level group is always the group created when your Cisco WebEx Messenger organization was provisioned.
- **View Child Groups:** to view the child groups of the selected group.
- **View Parent Group:** to view the parent group of the selected group.



CHAPTER 9

Directory Integration

Overview

With Directory Integration, the following are enabled for your Cisco WebEx organization:

- Automating user provisioning and de-provisioning.
- Keeping user profile information in the Cisco WebEx Administration Tool updated with the information from the corporate directory.
- Exposing groups (for example, distribution lists) to users in Cisco WebEx so that users can add Groups to their contact list without having to add individual members directly.
- Categorizing users into Policy groups. For information about applying policies to groups, see Assign Policies to a Group, on page 95.
- If your Cisco WebEx organization is enabled with directory integration, users cannot edit the directory information in their profiles. Users need to contact the Organization Administrator for updates to their profiles.
- If your Cisco WebEx organization is enabled with directory integration, you can deactivate users manually in case a user's account needs to be deactivated immediately.

Directory Integration Import Process and File Formats

Note: Organization Administrators and User Administrators cannot be created using the Directory Integration process.

Cisco WebEx customers who plan to enable Directory Integration for their organizations must:

- Contact your Cisco CSM or representative to request Directory Integration.
- Sign in to the Cisco WebEx Administration Tool to configure Directory Integration settings with the credentials and other settings provided by Cisco.
- Develop and run a script or tool to do the following:
- Extract the relevant pieces of information from the directory.
- Convert the extracted information to a CSV file. For information about CSV files, see Group File Formats, on page 104.

Note

- You can use tab, or comma-separated CSV files.
- Ensure that your CSV file is encoded in the ISO-8859-1 format.
- You must upload four CSV files before you begin Directory Integration; userInactivation_xxx.csv, userFile_xxx.csv, groupFile_xxx.csv, groupDeletion_xxx.csv.
- Upload the CSV file to Cisco's Secure FTP server.

Job Scheduling uses CRON expressions. For more information, see CRON Expressions, on page 99.

Configure Directory Integration

Procedure

Step 1 Select the **Configuration tab** > **System Settings > Directory Settings**.

Step 2 In the **Job Scheduling** field, enter the schedule at which the job runs.

Step 3 Under **SFTP Server**, enter the details in each field.
See the Related Topics section for more information about the fields.

The SFTP server is hosted by Cisco, which provides access to customers for uploading and downloading CSV files in a secure manner.

Step 4 Select **Save**.

Note The job running time must be rescheduled if the person that originally scheduled it has left the organization. When a Cisco WebEx Messenger account is disabled or deleted scheduled jobs automatically stop.

You can reschedule the job running time by clearing the existing schedule in the **Job Scheduling** field and entering a new scheduling time. Select **Save** after clearing the existing schedule and after entering the new one.

This ensures that the scheduling change is applied whether the Messenger service is running in primary or backup mode.

Directory Integration Settings

Field	Description
Server Address	IP address of the SFTP server.
Port	Port number of the SFTP server. Typically, the default port number of an SFTP server is 22.
User ID	ID of the person who has access to the SFTP server. This is typically an administrator of the customer's Cisco WebEx organization.
Password	Password associated with the user ID.
Input Folder Path	Path of the folder on the SFTP server where the administrator will download the input CSV files. The default folder name is **Input**and is case sensitive.
Output Folder Path	Path of the folder on the SFTP server where the administrator will download the input CSV files. The default folder name is **Output** and is case sensitive.
Error Folder Path	Path of the folder on the SFTP server where any errors in the output file are stored. The default folder name is **error** and is case sensitive.
File Password	If encrypting the input CSV files, enter the password for the CSV file. Cisco WebEx supports the standard gpg encryption system. For more information about gpg, see http://www.gnupg.org/. Alternatively, field can be left blank. In such a case, input CSV files will be treated as plain text.

CRON Expressions

The job schedule time expression, see Directory Integration Import Process and File Formats, on page 98, is a string comprised of six or seven fields separated by white space that represents a set of times, normally

as a schedule to execute some routine. Fields can contain any of the allowed values, along with various combinations of the allowed special characters.

CRON jobs are run in the GMT time zone

The CRON expression fields are as follows:

Field Sequence	Field Name	Mandatory	Allowed Values	Allowed Special Characters
1st	Seconds		0-59	, - * /
2nd	Minutes	YES	0-59	, - * /
3rd	Hours	YES	0-23	, - * /
4th	Day of Month	YES	1-31	, - * ? / L W
5th	Month	YES	1-12 or JAN-DEC	, - * /
6th	Day of Week	YES	0-7 or SUN-SAT	, - * ? / L #
7th	Year	NO	empty, 1970-2099	, - * /

Special characters

- * ("all values") - used to select all values within a field. For example, "" in the minute field means *"every minute".
- ? ("no specific value") - used to specify something in one of the two fields in which the character is allowed, but not the other. For example, to schedule a job to run on a particular day of the month, but any day of the week, enter "10" in the day-of-month field, and "?" in the day-of-week field. See the examples below for clarification.
- - - used to specify ranges. For example, "8-10" in the hour field means "the hours 8, 9 and 10".
- , - used to specify additional values. For example, "JAN,MAR,MAY" in the month field means "the months January, March, and May".
- / - used to specify increments of ranges. For example, 5-59/30 in the 1st field (minutes) indicate the fifth minute of the hour and every thirty minutes thereafter. You can also specify '/' after the " character - in this case " is the equivalent of '0' before the '/'. '1/5' in the day-of-month field indicates that the job is scheduled every five days starting on the first day of the month.
- L ("last") - performs differently in each of the two fields in which it is allowed. For example, the value "L" in the day-of-month field indicates "the last day of the month" - day 31 for January, day 28 for February on non-leap years. If entered as a standalone special character in the day-of-week field, it indicates "7" or "SAT". When entered in the day-of-week field, you can specify schedules such as "the last Friday" ("5L") of a given month. When using the 'L' option, do not specify lists, or ranges of values.
- W ("weekday") - used to specify the weekday (Monday-Friday) nearest the given day. For example, entering "20W" in the day-of-month field, indicates "the nearest weekday to the 20th of the month". If the 20th is a Wednesday, the job will run on Wednesday the 20th. However, if the 20th is a Saturday, the job will run on Friday the 19th. Similarly, if the 20th is a Sunday, the job will run on Monday the

21st. However, if you enter "1W" as the value for day-of-month, and the 1st is a Saturday, the job will run on Monday the 3rd, as it will not 'jump' over the boundary of a month's days. The 'W' character can only be specified when the day-of-month is a single day, not a range or list of days.

The 'L' and 'W' characters can also be combined in the day-of-month field. 'LW', indicates the *"last weekday of the month"*.

- # - used to specify "the nth" XXX day of the month. It can be entered in the day-of-week field, and must be followed by a number between one and five. It allows you to specify, for example, "the first Monday" of a given month "2#1" or "4#5", the fifth Wednesday of the month. However, if you specify "#5" and there is not 5 of the given day-of-week in the month, the job will not run that month.
- Note: The characters and the names of months and days of the week are not case sensitive. MON is the same as mon.

Examples

Expression	Meaning
0 0 12 * * ?	Scheduled for 12pm (noon) every day.
0 30 11 ? * *	Scheduled for 11:30am every day.
0 30 11 * * ?	Scheduled for 11:30am every day.
0 30 11 * * ? *	Scheduled for 11:30am every day.
0 * 14 * * ?	Scheduled for every minute starting at 2pm and ending at 2:59pm, every day.
0 0/5 14 * * ?	Scheduled for every 5 minutes starting at 2pm and ending at 2:55pm, every day.
0 0/5 14,18 * * ?	Scheduled for every 5 minutes starting at 2pm and ending at 2:55pm, AND run every 5 minutes starting at 6pm and ending at 6:55pm, every day.
0 0 12 1/5 * ?	Scheduled for 12pm (noon) every 5 days every month, starting on the first day of the month.

Note We do not currently support specifying both a day-of-week and a day-of-month value. You must enter the '?' character in one of these fields.

Be aware of "daylight savings" time when scheduling jobs to run between mid-night and 1:00 AM. The change in the hour causes a skip or a repeat depending on whether the time is adjusted forward or back.

User File Formats

The directory information for users and groups is imported using files with the following formats. User and group data is imported in separate files. Files need to be saved in ISO-8859-1 format.

User file name format: userFile_yyyy-mm-dd_n.csv

Format	Description
yyyy-mm-dd	The date on which the job is run. The date is based on the GMT time zone.
n	The job instance number for that particular day.

Example

If the job is scheduled to run four times a day, and the job was running on 28th July 2008, the files would be named

```
userFile_2008-07-28_1.csv, userFile_2008-07-28_2.csv,
userFile_2008-07-28_3.csv, userFile_2008-07-28_4.csv
```

User Inactivation File Name Format

userInactivation_yyyy-mm-dd_n.csv

A header record should not be present in the file.

User inactivation file format: userSSOID

Note If Single sign-on (SSO) is not enabled, you must enter the email address of the user you want to deactivate or delete in the userSSOID field.

This file contains only userSSOIDs whose record must be either deactivated or deleted.

Format	Description
yyyy-mm-dd	The date on which the job is run. The date is based on the GMT time zone.
n	The job instance number for that particular day.

Important If the user is an Organization Administrator, all jobs scheduled by them are blocked when they are deleted from the system. In this case, contact the Cisco WebEx Messenger Service Engineer team (connectteam@cisco.com) for assistance.

User file format

A header record should not be present in the file. The file format is:

```
userSSOId,displayName,firstName,lastName,email,jobTitle,address1,city,state,zip,
country,phoneOffice,phoneCell,homeGroupSSOId,homeGroupName,businessUnit,userProfilePhotoURL,
address2,storageAllocated,CUCMClusterName,IMloggingEnable,EndPointName,autoUpgradeSitName,
center,TC1,TC2,TC3,TC4,TC5,TC6,TC7,TC8,TC9,TC10
```

Format	Description
userSSOId	*Mandatory* The userSSOID used internally by the Cisco WebEx organization. This is the main field used to determine the record to be updated. If users with the same userSSOID already exist in the Cisco WebEx database, then such users' details are updated. If not, a new user is provisioned for the Cisco WebEx organization with all the details.
displayName	User's display name on the Cisco WebEx client.
firstName	*Mandatory* The user's first name.
lastName	*Mandatory* The user's last name.
email	*Mandatory* The user's email address. Whenever the address is updated or changed, the username, login and IM contact list are automatically migrated from the old username to the new username. All the user's contacts automatically receive a new presence subscription request with the new username.
jobTitle	*Optional* The user's job title.
address1	*Optional* The user's mailing address.
city	*Optional* City where the user resides.
state	*Optional* State where the user resides.
zip	*Optional* ZIPcode of the user's city.
country	*Optional* Country where the user resides.
phoneOffice	*Optional* The user's work phone number.
phoneCell	*Optional* The user's cell phone number.
homeGroupSSOId	*Optional* Used internally by an organization to identify a group. It determines whether a group has already been created in Cisco WebEx. If it has, the group information is updated. If it has not, a new group is created. If a value is present, the user is associated with that group.
homeGroupName	*Optional* The name for the group. If a name is not provided, the homeGroupSSOID itself is used.
businessUnit	*Optional* If present this information is placed in the user's profile area.
userProfilePhotoURL	*Optional* A URL where the user's profile photo is provided. This URL is used as-is by the Cisco WebEx application to display the photo.
address2	*Optional* The user's alternate mailing address if any.

Format	Description
storageAllocated	*Optional* The amount of storage allocated (in Mb) to the user in Cisco WebEx.
CUCMClusterName	*Optional* Name of the CUCM cluster to which the user is assigned if any.
IMLoggingEnable	*Optional* The value of this field can be either **True** or **False**. **Note** This value can be used in conjunction with the **EndPointName** field described below.
EndPointName	*Optional* Name of the IM archiving endpoint if any, configured for the user. **Note** If no endpoint is configured for the user and if **IMLoggingEnable** is set to **True**, the user's endpoint can be set to the Cisco WebEx organization's default endpoint.
autoUpgradeSiteName	*Optional*
center	*Optional* The user's Cisco WebEx Meetings account if an account has been created.
TC	*Optional* Tracking code for the user's Cisco WebEx Meetings account when Cisco WebEx and Cisco WebEx Meetings are integrated. **Note** The tracking codes range from TC1 - TC10.

Group File Formats

The directory information for users and groups is imported using files with the following formats. User and group data is imported in separate files. Files need to be saved in ISO-8859-1 format.

Group file name format

Group file name format: groupFile_yyyy-mm-dd_n.csv

Format	Description
yyyy-mm-dd	The date on which the job is run. The date is based on the GMT time zone.
n	The job instance number for that particular day.

Group file format

A header record should not be present in the file.

The group file contains three different types of records—Group Information, Child group information and Member information. Each of these types of records are differentiated by providing a recIndicator (Record Indicator).

- Group Information record the record indicator— **g**

- Child group record the record indicator is **— gg**
- Group members record the record indicator is **— gu**

Group Records

The following table lists the group information records.

recIndicator,ssoGroupId,groupName,groupType

Format	Description
SSOGroupID	This field is used to determine if a group has been created in Cisco WebEx Messenger. If already created, the group information is updated. Otherwise, a new group is created.
groupType	*Optional*. If present, it needs to have a numeric value. groupType can take on the following values: • 0 - Normal. Typically, most groups belong to this type. • 4 - Presence. These groups will be available for searching on the Cisco Jabber application. If groupType is not specified, the value defaults to 0.

Child Group Records

The child group record fields are:

recIndicator,ssoGroupId,RECURRING_subGroupSSOID

For example, the subgroupSSOIDs are provided in a comma separated format after the parent record indicator and parent group id to which they belong to.

Group Member Records

The group member record fields are:

recIndicator,ssoGroupId,RECURRING_memberSSOID

The member SSOIDs are provided after the record indicator and group ID to which they belong.

The group file can have many types of records, in any order. This example contains records of all three types in any order.

g, groupSSOID1, Group SSO Name1

g, groupSSOID2, Group SSO Name2

g, groupSSOID3, Group SSO Name3

gu,groupSSOID2,userSSOId6, userSSOId7

g, groupSSOID4, Group SSO Name4

g, groupSSOID5, Group SSO Name5

gg, groupSSOID3, groupSSOID10

gu,groupSSOID1,userSSOId1,userSSOId2,userSSOId3, userSSOId4

gg, groupSSOID1, groupSSOID2, groupSSOID3, groupSSOID4, groupSSOID5

gg, groupSSOID2, groupSSOID3, groupSSOID4

Group Deletion file name format

Group deletion file name format: groupDeletion_yyyy-mm-dd_n.csv

A header record should not be present in the file.

Group deletion file format: SSOGroupID.

Note If Single sign-on (SSO) is not enabled, you must enter the name of the group you want to delete in the SSOGroupID field.

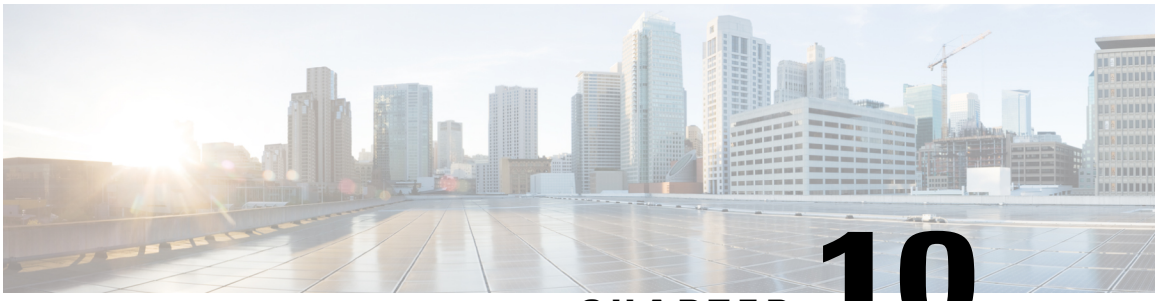
This file contains only SSOGroupIDs whose record must be deleted.

Format	Description
yyyy-mm-dd	The date on which the job is run. The date is based on the GMT time zone.
n	The job instance number for that particular day.

Sign in to a Cisco WebEx Organization Enabled with Directory Integration

After directory integration has been enabled, a welcome email is sent to users who are provisioned in the Cisco WebEx organization. However, if your Cisco WebEx organization is also enabled with Single Sign-on integration, no welcome email is sent.

Users of a Directory Integration-enabled Cisco WebEx organization can sign in to the Cisco Jabber application and change their sign in password. Additionally, the Cisco WebEx organization administrator can reset the password for the entire Cisco WebEx organization.



CHAPTER 10

Reports

Overview

You can generate reports to track and measure activities and usage of the Cisco Jabber application. You can only run reports for the previous 13 months. Generating a report is a two-step process of selecting the type of report to generate and then generating it. Each report displays the time stamp using the Greenwich Mean Time (GMT) as the time zone.

Many reports can be run in 15, 30, and 60 minute intervals.

The Cisco WebEx Messenger Organization Administrator can generate the following reports:

- Messenger User Report, on page 108
- Messenger Widget Report, on page 109
- Messenger Activity, on page 110
- Messenger User Activity, on page 111
- Audit Trail Report, on page 112

  You can run only one report at a time. A progress indicator shows the status of the report generation. A completed status indicates that your report was successfully generated. You can directly view the report or save it to your computer as a CSV file. Reports are saved for 7 days from the date the report is generated.

Generate a Report

Procedure

Step 1 To generate a report, select the **Report** tab.

Step 2 From the **Report Type** drop down list, select the type of report that you want to generate.

Step 3 (Optional) Select the **Interval** for the report.
The **Interval** option is available only for the following reports:

- **Messenger Activity:** Select **Interval, Month,** or **Year**.
- **Messenger User Activity:** Select **Month** or **year**

Step 4 Select **Generate Report**.
The **Status** column shows a **Running** status indicating the progress of the report generation. After it is successfully generated, the **Status** column shows **Completed**. Additionally, you also receive an email that contains instructions to download the report.

Step 5 Select the name of the report link to open or save the report.

Note To cancel the report generation at any time when the **Running** status is showing, select **Cancel the Progress**. A **Stopped** status indicates that the report generation has been canceled.

Messenger User Report

The Messenger User Report includes the following columns (listed below in the order they appear from left to right in the report):

Column	Description
User Name	The user's sign in name.
User Status	Displays the user as activated/deactivated. A deactivated user cannot sign into the Cisco Jabber application.
Total Storage Used(MB)	The total megabytes of storage used.
Total Allocated Storage (MB)	The total megabytes of storage limit allocated for the user.
Total Number of Spaces Owned	The total number of spaces owned by the user.
Total Number Of Spaces as Member	The total number of spaces in which the user has the role of member.

Column	Description
Logged User	Displays if the user's IMs are signed in via IM Logging and Archiving. (true/false).
Archiving Endpoint	The endpoint where the user's IMs are being archived. If the Logged User is set to true, then this value is set to the default. The value is shown as **Default** if the user's IM's are archived to the endpoint which has been designated as is the default archiving endpoint. For more information, see Set Up IM Archiving, on page 50.
Number of Users in roster (excluding Directory Groups)	Displays the number of contacts in the user's contact list. Does not include those in Directory groups. For more information, see Directory Integration, on page 97.
Number of Personal Groups in roster	Displays the number of contacts in the users contact list. This number excludes those that are part of the Directory Group. For more information, see Directory Integration, on page 97.
Number of Directory Groups in roster	Directory Groups are groups whose membership is pre-determined. Users can add groups to their contact list but cannot alter the members in the group. This feature is only available if the customers using the Directory Integration feature

Messenger Widget Report

The Messenger Widget Report displays details about widgets created in your Cisco WebEx Messenger Organization. This report is only useful if your organization uses the Spaces feature in Cisco WebEx Messenger. The Messenger Widget Report includes the following columns (listed below in the order they appear from left to right in the report):

Column	Description
Widget Name	The name of the widget.
Company Name	The name of the company in which the widget is created.
Creator Name	Name of the person (user) who created the widget.
Version Number	The version number of the widget.
Used in Spaces	The number of spaces where this widget is used.

Messenger Activity

The Messenger Activity report displays details of various activities in your Cisco WebEx Messenger organization for a particular month. This report displays the following data for the month for which you have generated the report.

Column	Description
Date	Displays the date data as YYYY/MM/DD. This is the date that data collection began.
Time	Displays the time data. This is the time that data collection began and was collected and aggregated up to the specified aggregation intervals of 15, 30, and 60 minute.
Number of Concurrent Users	Displays the number of simultaneous users signed into the Cisco Jabber application. **Note** The metric is calculated as: Number of Concurrent Users = Number of users signed in (beginning of interval) + Number of users signed in (during time interval) – Number of users signed out (during time interval). Negative numbers are permitted.
Aggregate Number of Logins/Logouts	Displays the number of sign in/sign outs. **Note** This is the Number of Concurrent Users (current interval) – the Number of Concurrent Users (previous interval).
Number of IM's	Displays the number of outgoing instant messages.
Number of Meetings Hosted	Displays the number of meetings hosted from the Cisco Jabber application.
Number of Meetings Joined	Displays the number of meetings joined from the Cisco Jabber application.
Number of Desktop Share Sessions	Displays the number of desktop share sessions initiated from the Cisco Jabber application.
Number Telephony of Calls	Displays the number of conference calls initiated from the Cisco Jabber application.
Number of Click-to-Call Calls	Displays the number of calls initiated from the Cisco Jabber application using the Cisco Unified Communication Integration.
Number of Video Calls	Displays the number of outgoing video calls.
Number of PC-to-PC Calls	Displays the number of outgoing VOIP calls.

Messenger User Activity

The Messenger User Activity report displays details of activities that users of your Cisco WebEx Messenger organization have performed for a particular month. This report displays the following data for the month for which you have generated the report.

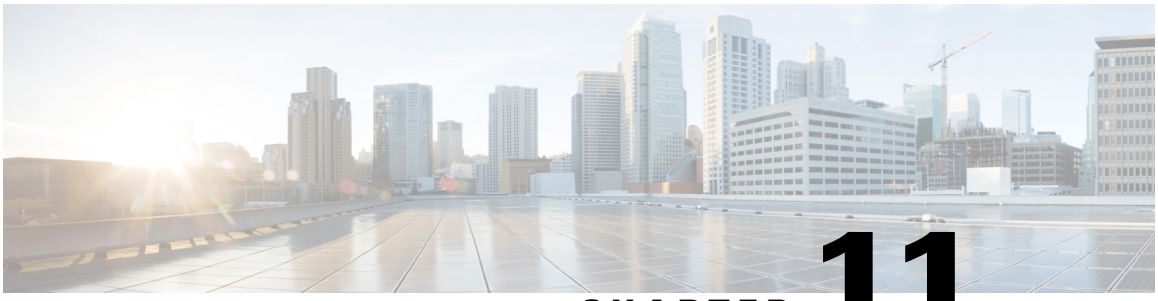
Column	Description
User Name	Displays the name (sign in name) of the user.
Number of Logins	Displays the number of times the user signs in into the Cisco Jabber application.
Number of New Spaces Owned	Displays the number of new spaces created during the month. This includes the two spaces (MyWebex and Developer Sandbox) that are automatically created when the user signs in for the first time.
Number of New Spaces Joined	Displays the number of new spaces that users have joined with the member role during the month. This number excludes the number of spaces that users have created.
Number of Meetings Hosted	Displays the number of meetings hosted from the Cisco Jabber application.
Number of Meetings Joined	Displays the number of meetings joined from the Cisco Jabber application.
Number of IMs	Displays the number of outgoing IMs.
Number of Telephony Calls	Displays the number of conference calls initiated by users from the Cisco Jabber application.
Number of Click-to-Call Calls	Displays the number of Click-to-Call calls initiated by users from the Cisco Jabber application using the Cisco Unified Communication Integration.
Number of Desktop Share Sessions	Displays the number of desktop sharing sessions initiated by users from the Cisco Jabber application.
Additional Storage Used (MB)	Displays the amount of additional storage (in MB) used. This metric is calculated as follows: Additional Storage Used = Storage Used – Storage Freed Up. This can be a negative number.
Last Login	Displays the last time the user signed in and the type/version used.
Number of Video Calls	Displays the number of video calls made by the user (outgoing calls).
Number of PC-to-PC Calls	Displays the number of VOIP calls initiated from the Cisco Jabber application.

Audit Trail Report

The Audit Trail report displays a list of all the actions performed by the Cisco WebEx Messenger Organization Administrator. Every action that the Organization Administrator performs within Cisco WebEx Messenger Administration Tool is logged by the tool and displayed in the Audit Trail report. This includes actions such as signing into the Cisco WebEx Messenger Administration Tool, clicking various tabs on the interface, changing configuration settings and generating the Audit Trail report itself.

The Audit Trail report is available as a CSV file and includes the following details:

Column	Description
Administrator	Sign in ID of the Organization Administrator whose actions are logged and captured in this report.
Timestamp	Timestamp of each individual action performed by the Organization Administrator.
Category	Category to which the action belongs. Typical categories include sign in, configuration, policy management, and report management.
Sub Category	Sub category to which the action belongs. Typical sub categories include meetings, XMPP IM clients, policy action addition and removal, auto upgrade and unified communications.
Details	Details of the action. For instance, when the Organization Administrator changes Unified Communication settings, the corresponding details will include the following wording: Changed the Org-Level settings for all clusters.



CHAPTER 11

CSV File Format

Overview

You use CSV files to import users into your organization. Every CSV file needs to adhere to a specific format in order for the import to be successful. Before you import, it is useful to review the following guidelines about creating CSV files.

Important If it is not the first time importing users from a CSV file, it is vital that you first export your users. This is to ensure you have the latest information in the CSV file as details such as phone numbers may have been updated. You can then edit this latest CSV file with any new information or users, save it as an UTF-8 or UTF-16LE Encoded spreadsheet, and import back into your Cisco WebEx Messenger organization.

- The CSV file supports both UTF-8 and UTF-16LE formats
- Every column in the CSV file should have a header with a valid name. For more information about valid column names, see CSV Fields, on page 114.
- If you do not want to enter information into a field, you can enter the character "-" and it is imported into the database as an empty field. You can only do this for optional fields. If you input - in a mandatory field, an error is reported on import. Do not use the value N/A.
- The name of a column should typically correspond to the name of a field in the user's profile. For example, the **First Name** field in the user profile dialog box should have a corresponding column named **firstName** in the CSV file.
- You can have optional or invalid column names in your CSV file. However, these columns are skipped or re-ordered during the import process.

- The status of the import is reported in the CSV file that replicates all the information from the input file, with a specific column indicating the status.
- If a user with the same email address is already in Cisco WebEx, the existing record in the database is overwritten with the value in the CSV file.
- Updates replaces the previous settings. For example, if new roles are specified for the user, the previous roles are replaced.
- The import process runs in the background. This enables you to continue performing other Cisco WebEx Administration tasks, such as configuration.
- After the import is complete, a confirmation email is sent to the person who initiated it. The notification includes a summary of the import results.
- The Organization Administrator can cancel an import process that is in progress.

Note Information is imported as provided in the CSV file. It is vital to ensure all information is correct. For example, if a phone number is provided without the country code, auto call-out in IM or meeting will not occur. You must then modify the CSV file providing the correct country code and import the CSV file again.

CSV Fields

Note: Organization Administrators and User Administrators cannot be created using the CSV Import process.

The following fields (in no specific order) should be included in the CSV file prior to importing users into Cisco WebEx. Some fields are mandatory, you must enter information into them, and some are optional.

Note: If you do not want to enter information into a field, you can enter the character "-" and it is imported into the database as an empty field. You can only do this for optional fields. If you input "-" in a mandatory field, an error is reported on import. Do not use the value N/A.

Field Name	Description
employeeID	*Mandatory (only SSO enabled)* Enter the user's ID.
displayName	*Optional* Enter the user's display name.
firstName	*Mandatory* Enter the user's first name.
lastName	*Mandatory* Enter the user's last name.
email	*Mandatory* Enter the user's email address.
userName	*Mandatory* Enter the user's username in the user@email.com format.
jobTitle	*Optional* Enter the user's job title or designation.
address1	*Optional* Enter the first line of the user's address. The Organization Administrator can configure this field so that it is mandatory for users.

Field Name	Description
address2	*Optional* Enter the second line of the user's address. The Organization Administrator can configure this field so that it is mandatory for users.
city	*Optional* Enter the city in which the user lives. The Organization Administrator can configure this field so that it is mandatory for users.
state	*Optional* Enter the state in which the user lives. The Organization Administrator can configure this field so that it is mandatory for users.
zipCode	*Optional* Enter the user's ZIP code. The Organization Administrator can configure this field so that it is mandatory for users.
ISOcountry	*Optional* Enter the two letter country code, for example IN, US, CN, in which the user lives. For more information see http://www.iso.org/iso/country_codes/iso_3166_code_lists/country_names_and_code_elements.htm. The Organization Administrator can configure this field so that it is mandatory for users.
phoneBusinessISOCountry	*Optional* Enter the country code, for example IN, US, CN, for the user's business phone number. The Organization Administrator can configure this field so that it is mandatory for users.
phoneBusinessNumber	*Optional* Enter the user's business phone number. The Organization Administrator can configure this field so that it is mandatory for users.
phoneMobileISOCountry	*Optional* Enter the country code, for example IN, US, CN, for the user's mobile phone number. The Organization Administrator can configure this field so that it is mandatory for users.
phoneMobileNumber	*Optional* Enter the user's mobile phone number. The Organization Administrator can configure this field so that it is mandatory for users.
fax	*Optional* Enter the user's fax number.
policyGroupName	*Optional* Enter the default policy group to which the user belongs.
userProfilePhotoURL	*Optional* Enter the URL where the user's profile picture can be accessed.
activeConnect	*Optional* Indicate whether the user's status is **active** in Cisco WebEx. Enter **Yes** to indicate an **active** status and **No** to indicate an **inactive** status.
center	*Optional* Used to assign (Yes) or remove (No) the center account for the Cisco Jabber application user. Only one center can be specified.
storageAllocated	*Optional* Enter the storage allocated to the user in Megabytes. This must be a numerical value

Field Name	Description
CUCMClusterName	*Optional* Enter the name of the Cisco Unified Communications Manager cluster that the user belongs to.
businessUnit	*Optional* Enter the business unit or department of the user. The Organization Administrator can configure this field so that it is mandatory for users.
IMLoggingEnable	*Optional* Indicate if IM logging is enabled for this user. Enter **True** to indicate an **enabled** status and **False** to indicate a **disabled** status.
endpointName	*Optional* Enter the endpoint name configured for logging IMs.
autoUpgradeSiteName	*Optional* Enter the upgrade site name.

Note You can use tab, or comma-separated CSV files. Ensure that your CSV file is encoded in either UTF-8 or UTF16-LE formats.

Select UTF-8 as the Encoding Format

Procedure

Step 1 In Microsoft Excel select **File > Save As**.
Step 2 In the **Save As** dialog box, select **Tools and Web Options**.
Step 3 In the **Web Options** dialog box, select the **Encoding** tab.
Step 4 From the **Save this document as** list, **select UTF-8**.
Step 5 Select **OK** to return to the **Save As** dialog box.
Step 6 From the **Save as type** list, select **CSV (Comma delimited) (*.csv)**.
Step 7 In the **File Name** field, type a name for the CSV file and select **Save**.

Workaround to Resolve a Potential Import Issue

In some cases, you might encounter an error when importing users via a CSV file. This is caused when the Organization Administrator has set the Country field as mandatory. To work around this issue, follow one of the following solutions.

Solution 1:

Procedure

Step 1 Select the **Configuration tab** > **System Settings > User Provisioning**.
The **User Provisioning** window opens.

Step 2 Under **Set Mandatory Fields for User Profile**, clear the **Country** field.

Step 3 Run the CSV import process again.

Solution 2:

Procedure

Step 1 Open the CSV file and locate the field titled **ISOCountry**.

Step 2 Enter the ISO Country Code for each user as appropriate.

Step 3 Save the CSV file.

Step 4 Run the CSV import process again.

Solution 3:

Procedure

Step 1 Open the CSV file and locate the field titled **ISOCountry**.

Step 2 Delete the **ISOCountry** field if your organization does not use it.

Step 3 Save the CSV file.

Step 4 Run the CSV import process again.

Solution 3:

CHAPTER 12

Library Management

Overview

The Library (Application) Management application allows users to manage applications (**widgets** and **templates**) for an organization, such as uploading applications to a library, moving applications between libraries, and deleting applications.

Note The workspaces feature in Cisco WebEx Messenger is at end-of-life and is no longer offered.

Users can upload applications to any library for which they have permission. In addition, users can copy applications from one library to another, and delete applications from a library. The user must have write permissions to the library in order to copy applications. If the user does not have permissions to a library, the user can send a notification to the Organization Administrator to copy the application.

For more information on using the Cisco WebEx Messenger product and the Library Management widget, refer to the Cisco WebEx Messenger Help and search for **Library Management**.

Application Management

A regular Cisco Jabber application user and the Organization Administrator can add applications using the Library Management Widget. Regular users can only add or manage applications to their own personal libraries. The Organization Administrator can also manage applications in the public library.

If a user does not have permission to a library, an error message is displayed asking whether the user wants to send a request to the Organization Administrator. The user can select **Yes** or **No**. If the user selects **Yes**, a notification email is sent to the Organization Administrator.

When the Organization Administrator signs in to Cisco WebEx Messenger and opens the Library Management widget, the list of applications under the **Pending Approval** displays. The Organization Administrator can use the mouse to hover over the widget to see details and **Approve** or **Deny** the request. For more information on approving requests to add applications, see Approve a Request to Add Application to Public Library, on page 120.

If the request is approved, it appears in the public library. If the request is denied, it is removed from the Pending Approval list and a notification is sent to the user.

Note For more details on adding applications (widgets) to a library, refer to Cisco Jabber application Help.

Copy an Application to a Library

This is for regular Cisco Jabber application users and Organization Administrators.

Procedure

Step 1 To copy application from one library to another, navigate to the applications in your personal or public library.

Step 2 Select an application from the list of applications and select **Copy widget to** ….

Step 3 Select **Public** or **Personal** from the drop down list and select **OK**.

Approve a Request to Add Application to Public Library

This is for users with Organization Administrator privileges only. The Organization Administrator receives an email notification each time a user requests a widget/template to be copied to the public library. The email has a title such as, **Request to copy application to the Public Library**.

Procedure

Step 1 Sign in to MyWebEx and navigate to the library management widget.
A list of applications in the **Pending Approval** list displays.

Step 2 Hover over the widget to see details (pop-up similar to the "Get More Apps" pop-up), and **Accept** or **Deny** the request.
If the request is approved, it appears in the public library. If the request is denied, it is removed from the **Pending Approval** list and a notification is sent to the user.

Remove an Application from a Library

This is for regular Cisco Jabber application users and Organization Administrators.

Procedure

Step 1 Navigate to the applications in the personal library (personal and public for organization administrator user).

Step 2 Select an application from the list of applications and select **Remove The Widget...**.

Step 3 To confirm deleting the widget, select **OK**.
The application is removed from the user's personal library and added to the Recycle Bin.

Restore an Application to a Library

This is for Cisco Jabber application users and Organization Administrators.

Procedure

Step 1 Navigate to the **Recycle Bin** list.

Step 2 Select an application from the list of applications and select **Restore**.
The application is restored to the library it was originally removed from and is removed from the **Recycle Bin**.