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 11 and Enter User Profile View Settings, on page 13.

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.

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.

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 32.

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.
- **Federated Web SSO Configuration** to display the dialog for an administrator who has turned on single sign-on. See, Federated Web SSO Settings.
- **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.
- **WebEx Certificate Management** to display the dialog for an administrator who has turned on single sign-on. See, Configure WebEx Certificate Management.
- **Partner Web SSO Configuration** to display the dialog for an administrator who is “Delegated Authentication”. See, Configure Partner Delegated Authentication.

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 7

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 and Directory Integration Import Process and File Formats.

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 9.

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 11

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.

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 29.

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 17.

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 15.

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.

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 19.
- **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.
- 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.
- **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 29.
- **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 31.

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 20
- Overview of Loosely Coupled Integration, on page 26

  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 23

- Verify the Success of Tightly Coupled Integration for a New Cisco WebEx Messenger Deployment with an Existing Cisco WebEx Meeting Application, on page 24
- Verify the Success of Tightly Coupled Integration for a New Cisco WebEx Meeting Application Deployment with an Existing Cisco WebEx Messenger Deployment, on page 25

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 20.

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 23.

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 24 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 21

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 21

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.
- 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.

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 27
  - Verify the Success of Loosely Coupled Integration for Organizations with Single Sign-on Infrastructure, on page 27
  - Verify the Success of Loosely Coupled Integration for Organizations without Single Sign-on Infrastructure, on page 28

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 26.

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 27.

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 27.

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 20.

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 34.

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 32.

  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.

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

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 4.

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.