

Main page: [Cisco Unified MeetingPlace, Release 7.0](#)

Up one level: [Integration](#)

This section describes how to configure Jabber with Cisco Unified MeetingPlace on a Jabber XCP server so that users can initiate Cisco Unified MeetingPlace meetings from a Jabber Messenger client. You have the option to configure Secure Sockets Layer (SSL) to implement security between the Cisco Unified MeetingPlace Web Server and the Jabber XCP server. Use SSL to provide secure transmission of data across the network through the use of public or private key encryption.

Contents

- [1 Configuring Jabber](#)
 - ◆ [1.1 Before You Begin](#)
 - ◆ [1.2 Procedure](#)
- [2 \(Optional\) How to Configure SSL](#)
 - ◆ [2.1 Entering the Cisco Unified MeetingPlace Web Server Certificate Files in the Jabber Server Keystore](#)
 - ◇ [2.1.1 Before You Begin](#)
 - ◇ [2.1.2 Procedure](#)
 - ◆ [2.2 Configuring SSL for Cisco Unified MeetingPlace on the Jabber Server](#)
 - ◇ [2.2.1 Before You Begin](#)
 - ◇ [2.2.2 Procedure](#)

Configuring Jabber

You must configure Jabber so that users can initiate Cisco Unified MeetingPlace meetings.

Before You Begin

- Install Jabber. See [How to Install the Jabber with Cisco Unified MeetingPlace Integration](#).
- Obtain the hostname or IP address of the Cisco Unified MeetingPlace Web Server.
- Log in to the Jabber XCP Controller web interface. See the Jabber documentation for information about how to access the Jabber XCP Controller web interface.

Procedure

1. Locate the Components section.
2. Locate the **Add a New** list.
3. Click **Cisco External Command Interface**.
4. Click **Go**.

The system displays the Cisco External Command Interface Configuration window.
5. Scroll to the Cisco Unified MeetingPlace Command Configuration section.
6. Enter the hostname or IP address of the Cisco Unified MeetingPlace Web Server.
7. Choose **MeetingPlace** from the MeetingPlace Server Type list.

8. Click **Submit**.
9. Locate the Cisco External Command Interface component that you added.
10. Locate the Actions column.
11. Click **Start**.

(Optional) How to Configure SSL

Entering the Cisco Unified MeetingPlace Web Server Certificate Files in the Jabber Server Keystore

Before You Begin

- Log in to the Jabber XCP server as root.
- Configure SSL on the Cisco Unified MeetingPlace Web Server. See [Configuring Cisco Unified MeetingPlace Web Conferencing Security Features](#).
- Copy the certificate files from the Cisco Unified MeetingPlace Web Server to the Jabber XCP server. There are two certificate files—one for Hostname [Home Page] and one for Hostname [web conferencing]. The certificate file names end in .cer.
- Obtain the hostname or IP address of the Cisco Unified MeetingPlace Web Server.
- Log in to the Jabber XCP Controller web interface. See the Jabber documentation for information about how to access the Jabber XCP Controller web interface.

Procedure

1. Open a command line interface.
2. Enter **keytool -import -alias "CiscoMeetingPlaceHomePage" -file <Certificate File for Hostname [Home Page]> -keystore <Keystore Location>**, where *<Certificate File for Hostname [Home Page]>* is the name of the certificate file for the *Hostname [HomePage]* and *<Keystore Location>* is the value for the -keystore parameter.

Note: The -keystore parameter specifies a file that holds the keystore. If you do not specify a full path, the keystore is created in the directory in which you run the keytool command.
3. Enter **keytool -import -alias "CiscoMeetingPlaceWebConferencing" -file <Certificate File for Hostname [Web Conferencing]> -keystore <Keystore Location>** where *<Certificate File for Hostname [Web Conferencing]>* is the name of the certificate file for the *Hostname [Web Conferencing]* and *<Keystore Location>* is the value for the -keystore parameter you set in [Step 2](#).
4. Enter a password for the keystore.

Configuring SSL for Cisco Unified MeetingPlace on the Jabber Server

Before You Begin

Log in to the Jabber XCP Controller web interface.

Procedure

Procedure

1. Locate the Cisco External Command Interface component.
2. Click **Edit**.
The system displays the Cisco External Command Interface Configuration page.
3. Choose **Intermediate** from the Configuration View list box.
4. Locate the Cisco Unified MeetingPlace Command area.
5. Click **SSL Configuration** in the External Command Integration Configuration area.
6. Enter the information from Step 2 of [Entering the Cisco Unified MeetingPlace Web Server Certificate Files in the Jabber Server Keystore](#) in **Full Path to SSL Key File**.
7. Enter the information from Step 3 of [Entering the Cisco Unified MeetingPlace Web Server Certificate Files in the Jabber Server Keystore](#) in **Password for SSL Key File**.
8. Click **Submit**.
9. Go to the Jabber XCP Controller home page.
10. Locate the Components area.
11. Locate the Cisco External Command Interface component that you just added.
12. Click **Start**.