Before you begin the configuration, Cisco Unified MeetingPlace for Jabber must be installed on a Jabber server. (See Installing or Upgrading Cisco Unified MeetingPlace for Jabber.)

To complete the configuration after installation, do the following procedure by using the Jabber server XCP Controller web interface.

Contents

- 1 To Configure Cisco Unified MeetingPlace for Jabber on the Jabber Server
- 2 Configuring SSL (Optional)
  - 2.1 To Enter the Web Conferencing Server Certificate Files in the Jabber Server Keystore
  - 2.2 To Configure Cisco Unified MeetingPlace for Jabber on the Jabber Server

To Configure Cisco Unified MeetingPlace for Jabber on the Jabber Server

1. Log on to the Jabber XCP Controller web interface. Refer to the Jabber documentation for information on how to access this interface.
2. In the Components section, from the Add a New drop-down list, choose **Cisco External Command Interface**, then click **Go**.
3. On the Cisco External Command Interface Configuration page, scroll down to the Cisco Unified MeetingPlace Command Configuration section, and enter a value in the **MeetingPlace Web Server Hostname or IP Address** field.
4. In the MeetingPlace Server Type drop-down list, choose **MeetingPlace**.
5. Click **Submit**.
6. From the XCP Controller home page, in the Components section, locate the Cisco External Command Interface component you just added. In the Actions column, click **Start**.

Configuring SSL (Optional)

You can implement security between the Cisco Unified MeetingPlace Web Conferencing server and the Jabber server by using the Secure Sockets Layer (SSL) protocol. SSL provides secure transmission of data across the network through the use of public/private key encryption.

For information on configuring SSL on the Web Conferencing server, see How to Configure Secure Sockets Layer.

After SSL has been configured on the Web Conferencing server, and a certificate has been procured or generated, do the following tasks to set up secure communication on the Jabber server:

1. Copy the certificate files from the Web Conferencing server to the Jabber server. There are two certificate files-one for Hostname [Home Page] and one for Hostname [Web Conferencing]. The certificate file names end in .cer.
2. Add the certificates to the keystore on the Jabber server. Do the To Enter the Web Conferencing Server Certificate Files in the Jabber Server Keystore.
3. Configure the keystore properties in the Jabber XCP web interface. Do the To Configure Cisco Unified MeetingPlace for Jabber on the Jabber Server.

To Enter the Web Conferencing Server Certificate Files in the Jabber Server Keystore

1. Log in to the Jabber server as root.
2. At the command line, enter: **keytool -import -alias "CiscoMeetingPlaceHomePage" -file <Certificate File for Hostname [Home Page]> -keystore <Keystore Location>** and press **Enter**.
   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. You will need to know the full path to the keystore file to configure the Jabber security settings in the next procedure.
3. When prompted, enter a password for the keystore.
4. At the command line, enter: **keytool -import -alias "CiscoMeetingPlaceWebConferencing" -file <Certificate File for Hostname [Web Conferencing]> -keystore <Keystore Location>** and press **Enter**.
   Note: The value for the -keystore parameter must match the value you used in Step 2.
5. When prompted, enter a password for the keystore.

To Configure Cisco Unified MeetingPlace for Jabber on the Jabber Server

1. Log on to the Jabber XCP Controller web interface.
2. From the Jabber XCP Controller home page, in the Components section, locate the **Cisco External Command Interface** component.
3. In the Actions column, click **Edit**.
4. On the Cisco External Command Interface Configuration page, from the Configuration View drop-down list, choose **Intermediate**.
5. In the External Command Integration Configuration section, under Cisco Unified MeetingPlace Command, check the **SSL Configuration** check box.
6. In the **Full Path to SSL Key File** field, enter the path to the keystore that you configured in Step 2 of the To Enter the Web Conferencing Server Certificate Files in the Jabber Server Keystore procedure.
7. In the **Password for SSL Key File** field, enter the password that you configured in Step 3 of the To Enter the Web Conferencing Server Certificate Files in the Jabber Server Keystore.
8. Click **Submit**.
9. From the XCP Controller home page, in the Components section, locate the Cisco External Command Interface component you just added. In the Actions column, click **Start**.