Contents

- 1 Configuring Cisco Unified MeetingPlace LCS Gateway Parameters
  - 1.1 To Configure Cisco Unified MeetingPlace LCS Gateway Parameters
- 2 Configuring Cisco Unified MeetingPlace Web Conferencing Single Sign-On Parameters
  - 2.1 To Configure Single Sign-On Parameters
- 3 Configuring Cisco Unified MeetingPlace Web Conferencing to Trust Web Server Authentication
  - 3.1 To Configure Web Conferencing to Trust Web Server Authentication
- 4 Configuring LCS to Route Conference Requests to the Cisco Unified MeetingPlace LCS Gateway
  - 4.1 To Configure LCS to Route Conference Requests to the Cisco Unified MeetingPlace LCS Gateway
- 5 Configuring LCS to Authorize Requests from the Cisco Unified MeetingPlace LCS Gateway
  - 5.1 To Configure LCS to Authorize Requests from the Cisco Unified MeetingPlace LCS Gateway
- 6 Configuring Cisco Unified MeetingPlace for Office Communicator End Users
  - 6.1 Adding Cisco Unified MeetingPlace Profiles for Office Communicator Users
    - 6.1.1 To Add a Cisco Unified MeetingPlace Profile
  - 6.2 Configuring Cisco Unified MeetingPlace Profiles for Office Communicator Users
  - 6.3 Enabling Conference Settings on the Office Communicator Client
  - 6.4 Configuring Conference Settings on the Office Communicator Client
    - 6.4.1 To Configure Conference Settings on the Office Communicator Client
- 7 Configuring Transport Layer Security (Optional)
  - 7.1 Prerequisites
  - 7.2 Tasks
  - 7.3 Configuring Certificates on the Cisco Unified MeetingPlace LCS Gateway
    - 7.3.1 To Download the CA Certificate or Certificate Chain
    - 7.3.2 To Install the CA Certificate or Certificate Chain on the Cisco Unified MeetingPlace LCS Gateway
    - 7.3.3 To Request and Install a Certificate from the CA
  - 7.4 Configuring LCS to Authorize Requests from the Cisco Unified MeetingPlace Gateway by Hostname
    - 7.4.1 To Configure LCS to Authorize Requests from the Cisco Unified MeetingPlace LCS Gateway by Hostname
  - 7.5 Enabling TLS on the Cisco Unified MeetingPlace LCS Gateway
    - 7.5.1 To Enable TLS on the Cisco Unified MeetingPlace LCS Gateway

Configuring Cisco Unified MeetingPlace LCS Gateway Parameters

You configure settings on the Cisco Unified MeetingPlace LCS Gateway by using the MeetingPlace Gateway Configurations utility. These settings determine how the Cisco Unified MeetingPlace LCS Gateway will communicate with the Microsoft LCS server, how to authenticate users, and what level of information to log.

Note: We recommend that you configure TCP as the transport protocol while bringing up the Cisco Unified

MeetingPlace for Office Communicator system for the first time, verify that Office Communicator clients can initiate and attend meetings, and then configure TLS. For TLS configuration instructions, see the Configuring Transport Layer Security (Optional).

To Configure Cisco Unified MeetingPlace LCS Gateway Parameters

1. Open the MeetingPlace Gateway Configurations utility by right-clicking the Cisco Unified MeetingPlace icon (orange door) located in the system tray.
2. Click the **LCS Gateway** tab.
   Note: The LCS Gateway tab is displayed in the Gateway Configurations utility only after the Cisco Unified MeetingPlace LCS Gateway has been installed on the server.
3. In the **IP Address** field, enter the primary IP address of the server on which the Cisco Unified MeetingPlace LCS Gateway is installed.
   Note: If you do not enter an IP address, the system displays the following message: "The Cisco Unified MeetingPlace LCS Gateway Service on Local Computer started and then stopped. Some services stop automatically if they have no work to do, for example, the Performance Logs and Alerts services." To resolve this issue, enter a valid IP address.
4. Configure the transport protocol based on your LCS server configuration:
   - If your LCS server is configured to use TCP, click **TCP** and enter the TCP port to use. Port 5060 is the default port for TCP.
   - If your LCS server is configured to use TLS, click **TLS** and enter the TLS port to use. Port 5061 is the default port for TLS.
     Note: If your deployment includes the Cisco Unified MeetingPlace H.323/SIP Gateway, it may be configured to use TCP ports 5060 and 5061. In this case, choose a different port between 5062 and 5069.
     Note: If Cisco Security Agent for Cisco Unified MeetingPlace is running on the Cisco Unified MeetingPlace LCS Gateway server, it will only allow conference request traffic to be exchanged on TCP ports 5060 through 5069. Configuring a port outside of this range while Cisco Security Agent is enabled will cause Office Communicator clients to time out while attempting to initiate conferences.
5. Configure user authentication:
   - If your deployment does not include a Cisco Unified MeetingPlace Directory Services server, click **AD** to use Active Directory authentication, and accept the default value for the attribute to search (msRTCSIP-PrimaryUser). This instructs the LCS Gateway to perform an LDAP search using the SIP username it receives from the LCS server (in a format such as user@domain.com).
   - If your deployment includes a Cisco Unified MeetingPlace Directory Services server, click **MPDS**.
6. Choose a log level to determine the type of information written to the Cisco Unified MeetingPlace Eventlog application:
   - **Error**-Only error conditions are logged.
   - **Warning**-Error conditions and warning of potential problems are logged.
   - **Informational**-Errors, warnings, and internal state information are logged. This is the default level.
   - **Verbose**-All of the above plus additional troubleshooting details are logged.
7. Click **Apply** to save changes.
8. Click **OK** to close the window.
9. After changing any Cisco Unified MeetingPlace LCS Gateway parameters, stop the Cisco Unified MeetingPlace LCS Gateway service, restart the Cisco Unified MeetingPlace Web Conferencing service, then start the Cisco Unified MeetingPlace LCS Gateway service:

1. From the Windows Start menu, choose **Settings > Control Panel > Administrative Tools > Services**.
2. Right-click **Cisco Unified MeetingPlace LCS Gateway** and choose **Stop**.
3. Right-click**Cisco Unified MeetingPlace Web Conferencing** and choose **Stop**.
4. Right-click **Cisco Unified MeetingPlace Web Conferencing** and choose **Start**.
5. Right-click **Cisco Unified MeetingPlace LCS Gateway** and choose **Start**.
6. Close the Services control panel.

Configuring Cisco Unified MeetingPlace Web Conferencing Single Sign-On Parameters

After installing Cisco Unified MeetingPlace for Office Communicator, you must configure the Cisco Unified MeetingPlace Web Conferencing single sign-on service to look up directory information for a user and return the user name to the Cisco Unified MeetingPlace LCS Gateway.

Note: Although not required, we strongly recommend that your deployment include a Cisco Unified MeetingPlace Directory Services server configured to synchronize user profiles from Active Directory.

To Configure Single Sign-On Parameters

1. Open the MeetingPlace Gateway Configurations utility by right-clicking the Cisco Unified MeetingPlace icon (orange door) located in the system tray.
2. Click the **Single Sign-On** tab.
   Note: The Single Sign-On tab is displayed in the Gateway Configurations utility only after the Cisco Unified MeetingPlace LCS Gateway has been installed on the server.
3. On the Single Sign-On tab, configure either Active Directory (AD) authentication or Cisco Unified MeetingPlace Directory Services (MPDS) authentication, depending on the type you selected in Step 5 of the To Configure Cisco Unified MeetingPlace LCS Gateway Parameters:
   - For AD authentication, configure the following fields with information about your AD deployment:

AD Server	Enter the name of the primary AD server.
Account Name	Enter the full LDAP name of the AD account to use to authenticate to your AD server, for example, **CN=Administrator,CN=Users,DC=mycompany,DC=com**.
Password	Enter the password for the AD account.
Base DN	Enter the starting point for searching the AD hierarchy, for example, **OU=Users,DC=mycompany,DC=com**.
Retrieve	Use the default value, **sAMAccountName**. This ensures that the username required to match the Cisco Unified MeetingPlace user profile is retrieved as a result of a search on the msRTCSIP-PrimaryUser attribute that was specified on the LCS Gateway tab in the To Configure Cisco Unified MeetingPlace LCS Gateway Parameters.
Query Scope	Check **Subtree** to search the Base DN by subtree (or multiple levels). The default behavior is to search one level only.

   - For MPDS authentication, configure the following fields with information about your MPDS server:

MPDS Server	Enter the name of the MPDS server.
Account Name	Enter the full LDAP name of the account to use to authenticate to the MPDS server, for example, **CN=Administrator,O=mycompany.com**.
Password	Enter the password for the account.
Search	Enter the custom parameter for Directory Services to use to get username information from the LDAP server-when configuring single sign-on for the Cisco Unified MeetingPlace LCS Gateway, this parameter should be set to **Custom2**, to search based on the SIP username (username@domain.com) from the LCS server.

4. Check the **Verbose Logging** check box if you want troubleshooting information logged to the Cisco Unified MeetingPlace Eventlog application.

5. When finished, close the MeetingPlace Gateway Configurations utility.

Configuring Cisco Unified MeetingPlace Web Conferencing to Trust Web Server Authentication

You configure Cisco Unified MeetingPlace Web Conferencing on the Cisco Unified MeetingPlace LCS Gateway to trust web server authentication so that users who sign in to the MOC client do not need to sign in separately to initiate or join a Cisco Unified MeetingPlace audio conference.

To Configure Web Conferencing to Trust Web Server Authentication

1. From a web browser, sign in to Cisco Unified MeetingPlace Web Conferencing.
2. From the Welcome page, click **Admin**, then click **Web Server**.
3. From the bottom section of the page, click the name of the web server on which the Cisco Unified MeetingPlace LCS Gateway is installed. This populates the top section of the page with predefined settings.
4. For Trust Web Server Authentication, choose **Yes**.
5. Click **Submit** to save the change.

Configuring LCS to Route Conference Requests to the Cisco Unified MeetingPlace LCS Gateway

You must configure the LCS server to route conferencing requests to the Cisco Unified MeetingPlace LCS Gateway. Conference requests are sent as SIP messages.

To Configure LCS to Route Conference Requests to the Cisco Unified MeetingPlace LCS Gateway

1. Log in to the LCS server.
2. On the Windows Start menu, click **Programs > Administrative Tools > Live Communications Server 2005**.
3. On the left side panel, click **Forest > Domains > Live Communication Server and Pools**.
4. Right-click the LCS server name and click **Properties**.
5. Click the **Routing** tab, then click **Add**. The Edit Static Route window appears.
6. In the User field, enter ***.
7. In the Domain field, enter the domain of the Cisco Unified MeetingPlace LCS Gateway.
8. For Next Hop, click **IP Address** and enter the primary IP address of the Cisco Unified MeetingPlace LCS Gateway. This IP address must match the value that you configured in Step 3 of the To Configure Cisco Unified MeetingPlace LCS Gateway Parameters.
9. For Transport, choose the protocol to transport requests-TCP or TLS; then enter the port to use for the requests. The protocol and port must match the values that you configured in Step 4 of the To Configure Cisco Unified MeetingPlace LCS Gateway Parameters.

   Note: If Cisco Security Agent for Cisco Unified MeetingPlace is running on the Cisco Unified MeetingPlace LCS Gateway server, it will only allow conference request traffic to be exchanged on TCP ports 5060 through 5069. Configuring a port outside of this range while Cisco Security Agent is enabled will cause Office Communicator clients to time out while attempting to initiate conferences.
10. Click **OK** to close the Edit Static Route window.
11. In the Properties window, click **Apply**, then click **OK** to close the window.

Configuring LCS to Authorize Requests from the Cisco Unified MeetingPlace LCS Gateway

You must configure the LCS server to authorize conference status updates from the Cisco Unified MeetingPlace LCS Gateway. Conference status updates are sent as SIP-CX NOTIFY messages.

Note: The Cisco Unified MeetingPlace Web Conferencing software on the Cisco Unified MeetingPlace LCS Gateway uses two IP addresses. If you do not configure the LCS server to authorize updates from both of these IP addresses, Office Communicator clients may appear to hang while waiting for conference status updates.

To Configure LCS to Authorize Requests from the Cisco Unified MeetingPlace LCS Gateway

1. Log in to the LCS server.
2. On the Windows Start menu, click **Programs > Administrative Tools > Live Communications Server 2005**.
3. On the left side panel, click **Forest > Domains > Live Communication Server and Pools**.
4. Right-click the LCS server name and click **Properties**.
5. Click the **Host Authorization** tab.
6. Click **Add**.
7. On the Add Authorized Host window, do one of the following:
   - If you are using TLS as the protocol between the LCS server and Cisco Unified MeetingPlace LCS Gateway, click **Network Address** and enter the primary hostname of the

Cisco Unified MeetingPlace LCS Gateway.
- If you are using TCP as the protocol between the LCS server and Cisco Unified MeetingPlace LCS Gateway, click **IP Address** and enter the primary IP Address on the Cisco Unified MeetingPlace LCS Gateway.

8. Check the **Throttle as Server** and **Treat as Authenticated** check boxes.
9. Click **OK**.
10. Repeat Step 6 through Step 9 for the secondary hostname or IP address on the Cisco Unified MeetingPlace LCS Gateway.
11. In the Properties window, click **Apply**, then click **OK** to close the dialog box.

Configuring Cisco Unified MeetingPlace for Office Communicator End Users

In order to initiate Cisco Unified MeetingPlace audio conferences, an Office Communicator end user must have a Cisco Unified MeetingPlace profile, and must have conferencing settings configured in his or her Office Communicator client.

Do the following tasks in the order listed to configure end-user clients for Cisco Unified MeetingPlace conferencing:

1. If Office Communicator users do not have Cisco Unified MeetingPlace profiles, add them. See the Adding Cisco Unified MeetingPlace Profiles for Office Communicator Users.
2. Review the configuration of user profiles to determine the type of meeting that will be launched by Office Communicator users, and change it if applicable. See the Configuring Cisco Unified MeetingPlace Profiles for Office Communicator Users.
3. Enable the configuration of conference settings on end-user client machines. See the Enabling Conference Settings on the Office Communicator Client.
4. Configure the conference settings on end-user client machines. See the Configuring Conference Settings on the Office Communicator Client.

Adding Cisco Unified MeetingPlace Profiles for Office Communicator Users

Note: If you are using Cisco Unified MeetingPlace Directory Services, the user information from your corporate directory is propagated automatically to the Cisco Unified MeetingPlace system. We recommend that you do not add new profiles directly to the Cisco Unified MeetingPlace system. For more information, see the information about Cisco Unified MeetingPlace Directory Services, Release 6.1.

If your deployment does not include Cisco Unified MeetingPlace Directory Services, you must manually add user profiles for Office Communicator users to the Cisco Unified MeetingPlace database. To add new user profiles through Cisco Unified MeetingPlace Web Conferencing, do the following procedure. (Further customization of user profiles requires that you access the profile through MeetingTime. For additional details on configuring user profiles in MeetingTime, see Deploying and Using MeetingTime.)

To Add a Cisco Unified MeetingPlace Profile

1. Sign in to Cisco Unified MeetingPlace Web Conferencing.
2. From the Welcome page, click **Admin**, then click **Profiles**.
3. Fill in the parameters as indicated in the following table:

User ID	Enter a unique alphanumeric string of 3 to 17 characters that identifies the user when the user accesses Cisco Unified MeetingPlace from a workstation. **Recommended:** The Active Directory user name.
User ID Password	Enter an alphanumeric password of 3 to 11 characters that authenticates the user when the user accesses Cisco Unified MeetingPlace from a workstation. **Note:** This is a temporary password. Users are prompted to change this password the first time they log in.
Confirm Password	Enter the user ID password again.
Profile Number	Enter a unique numeric string of 3 to 17 digits that identifies the user when the user accesses Cisco Unified MeetingPlace through the phone interface. Do not set the user ID and profile number to the same value. **Recommended**: The phone number, extension, or voice mailbox of the user.
Profile Password	Enter an alphanumeric password of 3 to 11 characters that authenticates the user when the user accesses Cisco Unified MeetingPlace from the phone. **Note:** This is a temporary password. Users are prompted to change this password the first time they log in.
Confirm Password	Enter the profile password again.
First Name	(Optional) Enter the first name of the user.
Last Name	(Optional) Enter the last name of the user.
E-Mail Address	(Optional) Enter the primary e-mail address of the user. Cisco Unified MeetingPlace will direct meeting notifications to this e-mail address.
Phone Number	(Optional) Enter the phone number of the user.
Time Zone	(Optional) Choose the local time zone of the user. If this user profile will be part of a group, click **Group Default (Localtime)**.

4. Click **Add**.

Configuring Cisco Unified MeetingPlace Profiles for Office Communicator Users

When an Office Communicator user initiates a Cisco Unified MeetingPlace meeting, the type of meeting that is initiated depends on the value selected for the Use Reservationless attribute in the user profile. If Use Reservationless is set to Yes, meetings that the user initiates from Office Communicator will be created as reservationless meetings. This approach has the advantage of providing users with a meeting ID they are

familiar with (their reservationless ID), which they can easily distribute to others so that they can dial in to the meeting. If Use Reservationless is set to No, meetings that the user initiates from Office Communicator will be created as immediate meetings with random unique meeting IDs.

The Use Reservationless setting can be configured by using MeetingTime. For instructions on configuring user profiles in MeetingTime, see Deploying and Using MeetingTime.

Enabling Conference Settings on the Office Communicator Client

In order to configure the conference settings required for initiating Cisco Unified MeetingPlace meetings, you must set the EnableConferencingService group policy setting on user machines, either by using the administrative template (.adm) file provided with your Microsoft LCS server software, or by running a script on the client machine (for example, when installing Office Communicator) to set the policy setting in the registry. To enable the settings via the registry, create and run a .reg file containing the following two lines:

[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Communicator]

"EnableConferencingService"=dword:00000001

For more information on deploying group policy settings, refer to the Microsoft Office Communicator and Live Communications Server documentation.

Configuring Conference Settings on the Office Communicator Client

Conferencing information must be configured in the Office Communicator client to initiate Cisco Unified MeetingPlace meetings. This procedure assumes that the Office Communicator clients have already been configured to communicate with the LCS server. End-users can refer to this procedure in the *Quick Start Guide*: *Cisco Unified MeetingPlace for Office Communicator*, available at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_user_guide_list.html.

To Configure Conference Settings on the Office Communicator Client

1. In Microsoft Office Communicator, click **Actions > Options**.
2. Click the **Accounts** tab.
3. In the Conferencing Information section, enter values for the following fields:

Conference ID	This field must be unique for this user across your organization, in order to avoid conflicts when users initiate meetings, and should be entered in the format **+<numeric code>.<numeric code>**. We recommend using +<Cisco Unified MeetingPlace Profile ID>.<Cisco Unified MeetingPlace Profile ID> (for example, +5551212.5551212).
Leader Code	This field must be unique for this user across your organization. We recommend using the Cisco Unified MeetingPlace profile ID.

Participant Code	The participant code must match the digits after the period in the Conference ID field. This field must be unique for this user across your organization. We recommend using the Cisco Unified MeetingPlace profile ID.
Domain	Enter the domain of the Cisco Unified MeetingPlace server. This value must match the value you configured in Step 7 of the To Configure LCS to Route Conference Requests to the Cisco Unified MeetingPlace LCS Gateway.

4. Click **OK** twice to exit the client configuration.

Configuring Transport Layer Security (Optional)

The Cisco Unified MeetingPlace LCS Gateway and the Microsoft LCS server communicate by using SIP messages, which can be easily spoofed. We highly recommend that you configure TLS between the servers to prevent the Cisco Unified MeetingPlace LCS Gateway from receiving and executing malicious requests.

Prerequisites

- You must have access to a certificate authority (either internal or external).
- The LCS server must be configured for TLS (certificates must be installed, and TLS must be enabled). Refer to the Microsoft LCS documentation for instructions.
- End-user Microsoft Office Communicator clients must be properly configured for TLS; you should verify that end-users can sign on to the LCS server from their MOC clients and chat with other users.
- You must already have configured your Cisco Unified MeetingPlace LCS Gateway and Web Conferencing single-sign on for proper authentication, configured routing on your LCS server, and configured Cisco Unified MeetingPlace for Office Communicator end-users. We recommend that you configure TCP while bringing up the Cisco Unified MeetingPlace for Office Communicator system for the first time, verify that Office Communicator clients can initiate and attend meetings, and then configure TLS.

Tasks

1. Configure certificates on the Cisco Unified MeetingPlace LCS Gateway. See the Configuring Certificates on the Cisco Unified MeetingPlace LCS Gateway.
2. Configure the LCS Server to authorize requests from the Cisco Unified MeetingPlace LCS Gateway by hostname. See the Configuring LCS to Authorize Requests from the Cisco Unified MeetingPlace Gateway by Hostname.
3. Enable TLS on the Cisco Unified MeetingPlace LCS Gateway. See the Enabling TLS on the Cisco Unified MeetingPlace LCS Gateway.

Configuring Certificates on the Cisco Unified MeetingPlace LCS Gateway

Note: If you are using an external certificate authority, refer to the certifier's instructions for requesting and installing certificates.

To configure TLS on the Cisco Unified MeetingPlace LCS Gateway with an internal certificate authority, do

the following tasks on the Cisco Unified MeetingPlace LCS Gateway in the order presented.

1. Download the certificate or certificate chain for the Certificate Authority (CA). See the To Download the CA Certificate or Certificate Chain.
2. Install the CA certificate or certification chain. See the To Install the CA Certificate or Certificate Chain on the Cisco Unified MeetingPlace LCS Gateway.
3. Request a certificate for the Cisco Unified MeetingPlace LCS Gateway from the CA, and install the certificate. See the To Request and Install a Certificate from the CA.

To Download the CA Certificate or Certificate Chain

1. Log on to the Cisco Unified MeetingPlace LCS Gateway.
2. On the Windows Start menu, click **Run**.
3. In the Open field, type **http://<Certification Authority server name>/certsrv** and press **Enter**.
4. Click **Download a CA Certificate, Certificate Chain, or CRL**.
5. Do one of the following:
   - If you are issuing certificates directly from a root CA, click **Download CA Certificate**.
   - If you are issuing certificates from a subordinate CA, click **Download CA Certificate Chain**.
6. In the File Download window, click **Save** and save the file to a location on the server.

To Install the CA Certificate or Certificate Chain on the Cisco Unified MeetingPlace LCS Gateway

1. On the Windows Start menu, click **Run**, enter **mmc** and press **Enter**.
2. Choose **File > Add/Remove Snap-In**. The Add/Remove Snap-In dialog box opens.
3. Click **Add**.
4. Click **Certificates**, then click **Add**.
5. Click **Computer Account**, then click **Next**.
6. In the Select Computer dialog box, click **Local Computer**, then click **Finish**.
7. Click **Close**.
8. Click **OK** to close the Add/Remove Snap-In dialog box.
9. In the left pane of the console, expand **Certificates (Local Computer)**.
10. Expand **Trusted Root Certification Authorities**.
11. Right-click **Certificates** and click **All Tasks > Import**. The Certificate Import Wizard opens.
12. Click **Next**.
13. Click **Browse** and browse to the certificate or certificate chain file you saved in Step 6 of the To Download the CA Certificate or Certificate Chain, then click **Open**.
14. Click **Next**.
15. Accept the default for **Place All Certificates in the Following Store** and verify that **Trusted Root Certification Authorities** appears under the Certificate store, then click **Next**.
16. Click **Finish**.

To Request and Install a Certificate from the CA

1. Open a web browser on the Cisco Unified MeetingPlace LCS Gateway and browse to **http://<Certification Authority server name>/certsrv**.
2. Click **Request a Certificate**.

3. Click **Advanced Certificate Request**.
4. Click **Create and Submit a Request to This CA**.
5. For Certificate Template, choose **Web Server**.
6. In the Name field, enter the DNS name of the Cisco Unified MeetingPlace LCS Gateway.
7. For Key Options, in the CSP drop-down menu, choose **Microsoft RSA SChannel Cryptographic Provide**.
8. Check the **Store Certificate in the Local Computer Certificate Store** check box.
9. Click **Submit**.
10. Click **Yes** to accept the potential scripting violation warning.
11. If your CA does not require administrator approval for issuing a certificate, click **Install This Certificate**, then click **Yes** to accept the potential scripting violation warning. If your CA requires administrator approval, do the following sub-steps:
    1. Log on to the CA server by using an account that is a member of the Domain Admins group.
    2. On the Windows Start menu, click **Run**, then enter **mmc** and press **Enter**.
    3. Choose **File > Add/Remove Snap-In**. The Add/Remove Snap-In dialog box opens.
    4. Click **Add**.
    5. Click **Certification Authority**, then click **Add**.
    6. In the Select Computer dialog box, click **Local Computer**, then click **Finish**.
    7. Click **Close**, then click **OK** to close the Add/Remove Snap-In dialog box.
    8. In the left pane, expand **Certification Authority (Local) > <Certification Authority Server Name>**, and click **Pending Request**.
    9. In the left pane, right-click the request ID and click **All Tasks > Issue**.
    10. On the Cisco Unified MeetingPlace LCS Gateway, on the Windows Start menu, click **Run**.
    11. Enter **http://<Certification Authority server name>/certsrv** and press **Enter**.
    12. Click **View the Status of a Pending Certificate Request**.
    13. Click the certificate request, then click **Install This Certificate**.

Configuring LCS to Authorize Requests from the Cisco Unified MeetingPlace Gateway by Hostname

TLS uses hostnames rather than IP addresses for secure communications between servers. When you configure TLS, you must add two host authorization entries on the LCS server, one for each of the two hostnames configured on the Cisco Unified MeetingPlace LCS Gateway.

Note: The Cisco Unified MeetingPlace Web Conferencing software on the Cisco Unified MeetingPlace LCS Gateway uses two hostnames. If you do not configure the LCS server to authorize updates from both of these hostnames, Office Communicator clients may appear to hang while waiting for conference status updates.

To Configure LCS to Authorize Requests from the Cisco Unified MeetingPlace LCS Gateway by Hostname

1. Log in to the LCS server.
2. On the Windows Start menu, click **Programs > Administrative Tools > Live Communications Server 2005**.
3. On the left side panel, click **Forest > Domains > Live Communication Server and Pools**.
4. Right-click the LCS server name and click **Properties**.
5. Click the **Host Authorization** tab.
6. Click **Add**.

7. On the Add Authorized Host window, click **Network Address** and enter the primary hostname of the Cisco Unified MeetingPlace LCS Gateway.
8. Check the **Throttle as Server** and **Treat as Authenticated** check boxes.
9. Click **OK**.
10. Repeat Step 6 through Step 9 for the secondary hostname on the Cisco Unified MeetingPlace LCS Gateway.
11. In the Properties window, click **Apply**, then click **OK** to close the dialog box.

Enabling TLS on the Cisco Unified MeetingPlace LCS Gateway

Use the following procedure to enable TLS as the communication protocol on the Cisco Unified MeetingPlace LCS Gateway.

To Enable TLS on the Cisco Unified MeetingPlace LCS Gateway

1. Open the MeetingPlace Gateway Configurations utility by right-clicking the Cisco Unified MeetingPlace icon (orange door) located in the system tray.
2. Click the **LCS Gateway** tab.
3. Click **TLS** and enter the TLS port to use. Port 5061 is the default port for TLS.
   Note: If your deployment includes the Cisco Unified MeetingPlace H.323/SIP Gateway, it may be configured to use TCP ports 5060 and 5061. In this case, choose a different port between 5062 and 5069.
   Note: If Cisco Security Agent for Cisco Unified MeetingPlace is running on the Cisco Unified MeetingPlace LCS Gateway server, it will only allow conference request traffic to be exchanged on TCP ports 5060 through 5069. Configuring a port outside of this range while Cisco Security Agent is enabled will cause Office Communicator clients to time out while attempting to initiate conferences.
4. Click **Apply** to save changes.
5. Click **OK** to close the window.
6. After changing any Cisco Unified MeetingPlace LCS Gateway parameters, stop the Cisco Unified MeetingPlace LCS Gateway service, restart the Cisco Unified MeetingPlace Web Conferencing service, then start the Cisco Unified MeetingPlace LCS Gateway service:
   1. From the Windows Start menu, choose **Settings > Control Panel > Administrative Tools > Services**.
   2. Right-click **Cisco Unified MeetingPlace LCS Gateway** and choose **Stop**.
   3. Right-click **Cisco Unified MeetingPlace Web Conferencing** and choose **Stop**.
   4. Right-click **Cisco Unified MeetingPlace Web Conferencing** and choose **Start**.
   5. Right-click **Cisco Unified MeetingPlace LCS Gateway** and choose **Start**.
   6. Close the Services control panel.