Main page: Cisco Unified MeetingPlace, Release 7.1

Navigation: Integration > Integrating with Microsoft Office Communicator

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 Transport Layer Security (TLS) between the Microsoft LCS Server and the Cisco Unified MeetingPlace LCS Gateway to prevent the Cisco Unified MeetingPlace LCS Gateway from receiving and executing malicious requests.

Contents

How to Configure Certificates on the Cisco Unified MeetingPlace LCS Gateway

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

To configure TLS on the Cisco Unified MeetingPlace LCS Gateway with an internal CA, do the following tasks on the Cisco Unified MeetingPlace LCS Gateway in the order presented:

- Downloading the CA Certificate or Certificate Chain
- Installing the CA Certificate or Certificate Chain on the Cisco Unified MeetingPlace LCS Gateway
- Requesting and Installing a Certificate from the CA
- Final Steps of the Configuration

Downloading the CA Certificate or Certificate Chain

Before You Begin

Log in as an administrator to the Cisco Unified MeetingPlace Web Server.

Procedure

1. Choose **Start > Run**.
2. Enter **http://**<*Certification Authority server name*>**/certsrv**, where <*Certification Authority server name*> is the name of the server for the CA.
3. Click **Download a CA Certificate, Certificate Chain, or CRL**.
4. Do one of the following:
   - Click **Download CA Certificate** if you are issuing certificates directly from a root CA.
   - Click **Download CA Certificate Chain** if you are issuing certificates from a subordinate CA.
5. Click **Save** in the File Download window.
6. Save the file to the server.

Installing the CA Certificate or Certificate Chain on the Cisco Unified MeetingPlace LCS Gateway

Procedure

1. Choose **Start > Run**.
2. Enter **mmc** to open the Microsoft Management Console.
3. Choose **File > Add/Remove Snap-in**.
4. Click **Add**.
5. Highlight **Certificates**, then click **Add**.
6. Select **Computer Account**, then click **Next**.
7. Select **Local Computer**.
8. Click **Finish**.
9. Click **Close**, then click **OK**.
10. Expand **Certificates (Local Computer)**.
11. Expand **Trusted Root Certification Authorities**.
12. Right-click **Certificates**.
13. Click **All Tasks > Import**.
14. Click **Next** in the Certificate Import Wizard window.
15. Click **Browse** and browse to the certificate or certificate chain file you saved when you downloaded the CA certificate.
16. Click **Open**, then click **Next**.
17. Accept the default for **Place All Certificates in the Following Store**.
18. Verify that **Trusted Root Certification Authorities** appears under the Certificate store.
19. Click **Next**, then click **Finish**.

Requesting and Installing a Certificate from the CA

Procedure

1. Open a web browser on the Cisco Unified MeetingPlace Web Server.
2. Browse to **http://<Certification Authority server name>/certsrv**.
3. Click **Request a Certificate**.
4. Click **Advanced Certificate Reques**t.
5. Click **Create and Submit a Request to This CA**.
6. Choose **Web Server** for Certificate Template.
7. Enter the DNS name of the Cisco Unified MeetingPlace LCS Gateway.
8. Choose **Microsoft RSA SChannel Cryptographic Provide** for Key Options from the CSP drop-down menu.
9. Check **Store Certificate in the Local Computer Certificate Store**.
10. Click **Submit**.
11. Click **Yes** to accept the potential scripting violation warning.
12. If your CA does not require administrator approval for issuing a certificate:
    1. Click **Install This Certificate**.
    2. Click **Yes** to accept the potential scripting violation warning.
13. If your CA requires administrator approval:
    1. Log in 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**.
    4. Click **Add**.
    5. Highlight **Certification Authority** and click **Add**.
    6. Click **Local Computer**.
    7. Click **Finish**.
    8. Click **Close**.
    9. Click **OK**.
    10. Expand **Certification Authority (Local) > <Certification Authority Server Name>**.
    11. Click **Pending Request**.
    12. Right-click the request ID in the left pane.
    13. Click **All Tasks > Issue**.
    14. Click **Run** on the Cisco Unified MeetingPlace LCS Gateway Windows Start menu.
    15. Enter **http://<Certification Authority server name>/certsrv**.
    16. Click **View the Status of a Pending Certificate Request**.
    17. Click the certificate request.
    18. Click **Install This Certificate**.

Final Steps of the Configuration

- You must add two host authorization entries on the Microsoft LCS Server, one for each of the two hostnames configured on the Cisco Unified MeetingPlace LCS Gateway.
- Enable TLS as the communication protocol on the Cisco Unified MeetingPlace LCS Gateway.

Related Topics

- Configuring the Microsoft LCS Server to Authorize Requests and Responses from the Cisco Unified MeetingPlace LCS Gateway
- Configuring the Cisco Unified MeetingPlace LCS Gateway Parameters