Security between IM and Presence Service and Microsoft Lync Setup

This chapter is only applicable if you require a secure connection between the IM and Presence Service and Microsoft Lync.

- Security Certificate for Microsoft Lync Setup, on page 1
- Verify Certificate Setup for Server and Client Authentication, on page 5
- TLS Route for Microsoft Lync Setup, on page 6
- Set Up Microsoft Lync for TLSv1, on page 10
- Create New TLS Peer Subject for Microsoft Lync, on page 10
- Add TLS Peer to TLS Peer Subjects List, on page 11

Security Certificate for Microsoft Lync Setup

Download CA Certification Chain

Complete the following procedure to download the CA certification chain.

Procedure

Step 1 Select **Start** > **Run**.

Step 2 Enter `http://<name of your Issuing CA Server>/certsrv` and select **OK**.

Step 3 From **Select a task**, select Download a CA certificate, certificate chain, or CRL .

Step 4 Select **Download CA certificate chain**.

Step 5 Select **Save** in the **File Download** dialog box.

Step 6 Save the file on a hard disk drive on your server.

Note The certificate file has an extension of .p7b. If you open this .p7b file, the chain will have the following two certificates:

- name of Standalone root CA certificate
- name of Standalone subordinate CA certificate (if any)

What to do next

Install CA Certification Chain, on page 2

Install CA Certification Chain

Complete the following procedure to install the CA certification chain.

Before you begin

Download the CA certification chain.

Procedure

Step 1 Select **Start** > **Run**.

Step 2 Enter `mmc` and select **OK**.

Step 3 Select **File** > **Add/Remove Snap-in**.

Step 4 Select **Add** in the **Add/Remove Snap-in** dialog box.

Step 5 Select **Certificates** in the list of **Available Standalone Snap-ins** and select **Add**.

Step 6 Select **Computer account** and select **Next**.

Step 7 In the **Select Computer** dialog box, ensure Local computer: (the computer this console is running on) is selected.

Step 8 Select **Finish**, select **Close**, and then select **OK**.

Step 9 Expand **Certificates** (Local Computer) in the left pane of the Certificates console.

Step 10 Expand **Trusted Root Certification Authorities** and right-click **Certificates**.

Step 11 Point to **All Tasks** and select **Import**.

Step 12 Select **Next** in the **Import Wizard**.

Step 13 Select **Browse** and locate the certificate chain on your computer.

Step 14 Select **Open** and select **Next**.

Step 15 Leave the default value Place all certificates in the following store selected.

Step 16 Ensure **Trusted Root Certification Authorities** appears under the Certificate store.

Step 17 Select **Next** and select **Finish**.

What to do next

Submit Certificate Request on CA Server, on page 3

Related Topics

Download CA Certification Chain, on page 1

Submit Certificate Request on CA Server

Complete the following procedure to submit the certificate request on the CA server.

Before you begin

Install the CA Certification Chain.

Procedure

Step 1 Select **Start** > **All Programs** > **Microsoft Lync Server** > **Lync Server Management Shell**.

Step 2 Enter the following command to create a certificate request for Microsoft Lync Server:

```
Request-CsCertificate -New -Type Default -DomainName <FQDN of Lync Server> -Output c:\cert.csr
-ClientEku $true
```

Step 3 From Microsoft Lync Server, enter the URL `http://<name of your Issuing CA server>/certsrv`.

Step 4 Select **Request a Certificate** and then select **Advanced certificate request**.

Step 5 Select **Submit** a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Step 6 Open the file cert.csr from Step 2, on page 3 and copy all information in the file to the clipboard.

Step 7 Paste the information from the file cert.csr to the **Saved Request** box in the certificate authority server and select **Submit**.

What to do next

Approve and Import Certificate, on page 3

Related Topics

Install CA Certification Chain, on page 2

Approve and Import Certificate

Complete the following procedure to approve and import the certificate.

Before you begin

Submit the Certificate Request on the CA Server.

Procedure

Step 1 From the Certificate Authority Server, select **Administrative Tools** > **Certificate Authority**.

Step 2 Select **Pending Requests** and find the new certificate in the list.

Step 3 Right-click on the new certificate and select **All Tasks** > **Issue Certificate**.

Step 4 From Microsoft Lync Server, enter the URL `http://<name of your Issuing CA server>/certsrv`.

Step 5 Select **View** the status of a pending certificate request.

Step 6 Select **Base 64 encoded** and download the certificate as a cer file extension to the Microsoft Lync server local drive.

Step 7 Sign in as a member of the Administrators group to the same Microsoft Lync Server on which you created the certificate request.

Step 8 Start the Lync Server Deployment Wizard and select **Install** or **Update** Lync Server System.

Step 9 Select **Run Again** (beside Step 3: Request, Install, or Assign Certificates).

Step 10 From the **Available Certificate Tasks** page, select **Import** a certificate from a .p7b, pfx or .cer file.

Step 11 In the **Import Certificate** page, enter the full path and filename of the certificate that you retrieved from the Certificate Authority in Step 6, on page 4. Alternatively, you can select **Browse** to locate and select the file.

What to do next

Assign Imported Certificate, on page 4

Related Topics

Submit Certificate Request on CA Server, on page 3

Assign Imported Certificate

Complete the following procedure to assign the imported certificate.

Before you begin

Approve and import the Certificate.

Procedure

Step 1 From Microsoft Lync Server start the Lync Server Deployment Wizard.

Step 2 Select **Install** or **Update** Lync Server System.

Step 3 Select **Run Again** in Step 3: Request, Install or Assign Certificates.

Step 4 From the **Available Certificate Tasks** page, select **Assign an existing certificate**.

Step 5 From the **Certificate Assignment** page, select **Next**.

Step 6 From the **Advanced Certificate Usages** page, select all checkboxes to assign the certificate for all usages.

Step 7 From the **Certificate Store** page, select the certificate that you requested and imported.

Step 8 In the **Certificate Assignment Summary** page, review your settings, and select **Next** to assign the certificates.

Step 9 From the wizard completion page, select **Finish**.

Step 10 Open the Certificate snap-in on each server, select **Certificates (Local computer)** > **Personal** > **Certificates**, and verify that the certificate is listed in the **Details** pane.

What to do next

Verify Certificate Setup for Server and Client Authentication, on page 5

Related Topics

Approve and Import Certificate, on page 3

Verify Certificate Setup for Server and Client Authentication

Complete the following procedure to verify that the certificate is properly configured for server and client authentication.

Procedure

Step 1 From Microsoft Lync Server, start the Lync Server Deployment Wizard.

Step 2 Select **Install** or **Update** Lync Server System.

Step 3 Select **Run Again** in Step 3: Request, Install or Assign Certificates.

Step 4 In the **Certificate Wizard** screen, highlight the Default certificate and select **View**.

Step 5 In the **View Certificate** screen, select **View Certificate Details**.

Step 6 In the **Certificate** screen, select the **Details** tab.

Step 7 From the **Show** drop-down list, select **Extensions Only**.

Step 8 Select **Enhanced Key Usage** and verify that the following are listed: Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)

Step 9 Select **Start** > **All Programs** > **Microsoft Lync Server** > **Lync Server Management Shell**.

Step 10 Enter the following command to view the certificate from Microsoft Lync Server: `Get-CsCertificate`

Step 11 Verify that the Default certificate is present and similar to the following:

```
Issuer    : CN=ne001a-lynccaNotAfter
NotAfter         : 6/16/2012 2:18:20 PM
NotBefore        : 6/16/2011 2:08:20 PM
SerialNumber     : 152E466D00000000000C
Subject          : CN=pool1.rcdnlync.com
AlternativeNames : {sip.rcdnlync.com, ne011a-lyncent.rcdnlync.com, pool1.rcdnlync.com}
Thumbprint       : 84BED88F2BFBB463CB4CBC328DAA6FD3A5E0677B
Use              : Default
```

What to do next

TLS Route for Microsoft Lync Setup, on page 6

TLS Route for Microsoft Lync Setup

Set up the following items to configure a TLS route for IM and Presence Service on Microsoft Lync:

- static routes
- application pools
- Microsoft Remote Call Control (RCC) application

After you set up a TLS route for IM and Presence Service on Microsoft Lync, commit the topology and restart the front-end service.

Set Up Static Route

Complete the following procedure to configure the static route.

Procedure

Step 1 Select **Start** > **All Programs** > **Microsoft Lync Server** > **Lync Server Management Shell**.

Step 2 If there is a TCP route, remove it with the following command:

```
Remove-CsStaticRoutingConfiguration -Identity Global
```

Step 3 Enter the following command to create a static TLS route:

```
$tlsRoute = New-CsStaticRoute -TLSRoute -Destination <FQDN CUP Server> -Port 5062 -MatchUri
*.rcdnlync.com -UseDefaultCertificate $true
```

Step 4 At the prompt, enter the following command to load the static route into the Lync server.

```
Set-CsStaticRoutingConfiguration -Route @{Add=$tlsRoute}
```

Step 5 Verify the new system configuration by entering the following command:

```
Get-CsStaticRoutingConfiguration
```

The following table describes the parameters that you use to insert a new static route for Lync server.

Table 1: Static route parameters

Parameter	Description
$tlsRoute	The name of the variable. It can be named anything but it must begin with a `$` and mach the reference in the Set command.
New-CsStaticRoute	The internal command that populates the static route to a variable.
-TLSRoute	This parameter configures the route as TLS.
-Destination	The FQDN of theIM and Presence Service node.

Parameter	Description
-Port	The port to which the IM and Presence Service node listens. For TLS, the port is 5062.
-MatchUri	This value is a wildcard, denoted by an asterisk (*), followed by a domain. It is compared to the Line Server URI value that is specified for each user in the Lync Control Panel. See Enable Users in Lync Server Control Panel.
-UseDefaultCertificate	This value is set to True to instruct the static route to use the default certificate.
-CsStaticRoutingConfiguration	The internal command to move parameter values to the routing database.
-Route	This parameter takes the parameters in the variable and adds the static route.

What to do next

Set Up Application Pool, on page 7

Set Up Application Pool

The following procedure sets up an application pool that is referenced by the Lync server (registrar). It also links the site information to this pool.

Procedure

Step 1 Select **Start** > **All Programs** > **Microsoft Lync Server** > **Lync Server Management Shell**.

Step 2 Enter the following command to remove any existing TCP application pool:

```
Remove-CsTrustedApplicationPool -Identity TrustedApplicationPool:<IP_Address_CUPserver>
```

Step 3 Enter the following command to create the application pool:

```
New-CsTrustedApplicationPool -Identity <FQDN CUP Server> -Registrar <FQDN of Pool> -site 1
-ThrottleAsServer $true -TreatAsAuthenticated $true
```

Step 4 Select Y at the prompt.

Step 5 Verify the new system configuration by entering the following command:

```
Get-CsTrustedApplicationPool
```

The following table describes the parameters that you use to configure the application pool.

Table 2: Application pool parameters

Parameter	Description
New-CsTrustedApplicationPool	The internal command that adds the application pool.
-Identity	The FQDN of the IM and Presence Service node.
-Registrar	The reference name of the pool. It can also be the FQDN of the Lync server.
-Site	The numeric value of the site. **Tip** You can find the site ID with the Get-CsSite Management Shell command.
-TreatAsAuthenticated	Always set this value to `$True`
-ThrottleAsServer	Always set this value to `$True`

What to do next

Set Up RCC Application, on page 8

Set Up RCC Application

The following procedure adds the Microsoft Remote Call Control (RCC) application to the pool.

Procedure

Step 1 Select **Start** > **All Programs** > **Microsoft Lync Server** > **Lync Server Management Shell**.

Step 2 Enter the following command to remove any existing TCP application:

```
Remove-CsTrustedApplication -Identity <FQDN of IM and Presence server>/urn:application:rcc
```

Step 3 Enter the following command to add the RCC application to the pool:

```
New-CsTrustedApplication -ApplicationID RCC -TrustedApplicationPoolFqdn <FQDN of IM and
Presence server> -Port 5062
```

Step 4 Select **Y** at the prompt.

Step 5 Verify the new system configuration by entering the following command:

```
Get-CsTrustedApplication
```

The following table describes the parameters that you use to configure the application pool.

Table 3: Application configuration parameters

Parameter	Description
New-CsTrustedApplication	The internal command that adds the RCC application.

Parameter	Description
-ApplicationID	The name of the application, for example, RCC.
-TrustedApplicationPoolFQDN	The FQDN of the IM and Presence Service node.
-Port	The SIP TLS listening port of the IM and Presence Service node. For TLS, the port is 5062.

What to do next

Commit Lync Server Setup, on page 9

Commit Lync Server Setup

This procedure describes how to commit the topology and restart the front-end service.

Procedure

Step 1 In the Lync Server Management Shell enter the following command to enable the topology:

```
Enable-CsTopology
```

Step 2 Enter the following command to output the topology to an XML file called rcc.xml and save it to the C drive:

```
Get-CsTopology -AsXml | Out-File C:\rcc.xml
```

Note You can select any name and location to output the topology information.

Step 3 Open the rcc.xml file.

Step 4 In the **Cluster Fqdn** section, change the IPAddress parameter from “<0.0.0.0>” to the IP Address of the IM and Presence Service node.

Step 5 Save the rcc.xml file.

Step 6 Enter the following command in the Lync Server Management Shell:

```
Publish-CsTopology -FileName C:\rcc.xml
```

Step 7 Enter the following command to restart the front-end service:

```
Restart-Service RtcSrv
```

What to do next

Set Up Microsoft Lync for TLSv1, on page 10

Set Up Microsoft Lync for TLSv1

IM and Presence Service only supports TLSv1 so you must configure Microsoft Lync to use TLSv1. This procedure describes how to configure FIPS-compliant algorithms on Microsoft Lync to ensure that Microsoft Lync sends TLSv1 with TLS cipher TLS_RSA_WITH_3DES_EDE_CBC_SHA.

Procedure

Step 1 Select **Start** > **Administrative Tools** > **Local Security Policy**.

Step 2 Select **Security Settings** in the console tree.

Step 3 Select **Local Policies**.

Step 4 Select **Security Options**.

Step 5 Double-click the FIPS security setting in the **Details** pane and modify the security setting.

Step 6 Select **OK**.

Step 7 Restart the Windows Server for the change to the FIPS security setting to take effect.

What to do next

Create New TLS Peer Subject for Microsoft Lync, on page 10

Create New TLS Peer Subject for Microsoft Lync

Complete the following procedure to create a new TLS Peer Subject for Microsoft Lync on IM and Presence Service.

Procedure

Step 1 Select **Cisco Unified CM IM and Presence Administration** > **IM and Presence** > **Security** > **TLS Peer Subjects**.

Step 2 Select **Add New**.

Step 3 In the **Peer Subject Name** field, enter the subject CN of the certificate that Microsoft Lync presents.

Step 4 In the **Description** field, enter the name of the Microsoft Lync server.

Step 5 Select **Save**.

What to do next

Add TLS Peer to TLS Peer Subjects List, on page 11

Add TLS Peer to TLS Peer Subjects List

Complete the following procedure to add the TLS Peer to the selected TLS Peer Subjects list on IM and Presence Service.

Before you begin

Create a new TLS Peer Subject for Microsoft Lync on IM and Presence Service.

Procedure

Step 1 Select **Cisco Unified CM IM and Presence AdministrationSystemSecurityTLS Context Configuration**.

Step 2 Select **Find**.

Step 3 Select **Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context**.

The TLS Context Configuration window displays.

Step 4 From the list of available TLS ciphers, select **TLS_RSA_WITH_3DES_EDE_CBC_SHA**.

Step 5 Select the right arrow to move this cipher to **Selected TLS Ciphers**.

Step 6 Check **Disable Empty TLS Fragments**.

Step 7 From the list of available TLS peer subjects, select the TLS peer subject that you configured.

Step 8 Select the right arrow to move it to **Selected TLS Peer Subjects**.

Step 9 Select **Save**.

What to do next

Lync Remote Call Control Installation