# Microsoft Lync Configuration for Partitioned Intradomain Federation

To configure Microsoft Lync for partitioned Intradomain federation, you must complete the following procedures in the order they are presented. After the configuration is complete, you must restart services on Lync servers.

**Note** You must configure TLS for Partitioned Intradomain Federation with Lync. TCP is not supported by Lync.

## Domain Verification for Lync Servers

Before you proceed to set up IM and Presence Service for partitioned intradomain federation, verify that there are matching presencer domains configured on the Microsoft Lync servers and all nodes in the IM and Presence Service cluster.

On the **Cisco Unified CM IM and Presence Administration** user interface, go to **Presence** > **Domains** > **Find** to verify local presence domains that are configured on the IM and Presence Service, as well as the system-managed presence domains that are configured on external servers.

## Lync Federation Configuration Task Flow

Complete these tasks to set up Microsoft Lync for Partitioned Intradomain Federation.

### Before You Begin

IM and Presence Configuration Task Flow for Federation

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Configure Static Route on Microsoft Lync, on page 2 | On the Lync servers, set up a TLS static route that points to either Expressway Gateway (for chat+calling deployments) or the IM and Presence Service routing node (for chat-only deployments). |
| **Step 2** | Configure Trusted Applications for Lync, on page 3 | On the Lync servers, add the IM and Presence Service as a trusted application and add your IM and Presence cluster nodes to a trusted application server pool. |
| **Step 3** | Publish Topology, on page 5 | On the Lync servers, commit the topology. |
| **Step 4** | Configure Certificates on Lync, on page 6 | Set up certificates on your Lync servers. |

## Configure Static Route on Microsoft Lync

You must create a TLS static route on the Lync servers that points to one of the following destinations:

- For chat + calling deployments, configure a static route to the Expressway Gateway
- For chat-only deployments, configure a static route to the IM and Presence Service routing node

**Note** When using TLS, the FQDN used in the destination pattern of the static route must be resolvable from the Lync front-end server. Ensure that the FQDN resolves to the IP address of the Expressway Gateway or IM and Presence Service routing node.

The Lync FQDN cannot match the IM and Presence Service domain that is used for partitioned intradomain federation.

### Procedure

**Step 1** Log in to a computer as the domain administrator, for example, where Lync Server Management Shell is installed.

**Tip** You must log in as a member of the RTCUniversalServerAdmins group or a role-based access control (RBAC) role to which you have assigned the **New-CsStaticRoute** cmdlet.

**Step 2** Choose **Start** > **All Programs** > **Microsoft Lync Server 2010** > **Lync Server Management Shell**.

**Step 3** Enter the following command to define a TLS route:

```
$tlsRoute = New-CsStaticRoute -TLSRoute -Destination fqdn_of_imp_routing_node -Port
listening_port_imp_routing_node -usedefaultcertificate $true -MatchUri domain_imp
```

where:

| Parameter | Description |
|---|---|
| -Destination | The FQDN of the Expressway Gateway (chat+calling) or the FQDN or IP address of the IM and Presence Service routing node (chat-only). For example, `expGateway.example,com` or `impNode.example.com.` |
| -Port | The listening port of the Expressway Gateway (default port is 65072) or the listening port of the IM and Presence Service routing node (default port is 5061). |
| -MatchUri | The domain for the Expressway Gateway domain (chat+calling) or IM and Presence Service (chat-only). For example, `example.com`. |

**Example:**

```
$tlsRoute = New-CsStaticRoute -TLSRoute -Destination impNode.example.com -Port 5061
-usedefaultcertificate $true -MatchUri example.com
```

**Note**

- To match child domains of a domain, you can specify a wildcard value in the **`-MatchUri`** parameter, for example, *.sip.com. That value matches any domain that ends with the suffix sip.com.
-

**Step 4** Make the newly created static route persistent in the Central Management store. Enter the following command:

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

**Note** Perform this step only for the routing IM and Presence Service node.

**Step 5** If you made the new static route persistent, verify that the command was successful. Enter the following command:

```
Get-CsStaticRoutingConfiguration | select-object -ExpandProperty Route
```

**Step 6** Open the Lync control panel. In the **External User Access** area:

a) Click **New** and create a Public Provider for the domain that Lync is federating with (your IM and Presence Service domain) and the FQDN of the VCS Expressway Gateway.

b) In the new Public Provider, configure the Verification level of your users to Allow all communications with this provider.

### What to Do Next

Configure Trusted Applications for Lync, on page 3

## Configure Trusted Applications for Lync

On the Lync server, add the IM and Presence Service as a trusted application and add each IM and Presence cluster node to a trusted application server pool. This procedure applies for both Enterprise Edition and Standard Edition Lync deployments.

### Procedure

**Step 1** Create a trusted application server pool for the IM and Presence Service deployment using the following commands:

**Tip** You can enter `Get-CsPool` to verify the FQDN value of the Registrar service for the pool.

```
New-CsTrustedApplicationPool -Identity trusted_application_pool_name_in FQDN_format -Registrar
Lync_Registrar_service_FQDN -Site ID_for_the_trusted_application_pool_site
-TreatAsAuthenticated $true -ThrottleAsServer $true -RequiresReplication $false -OutboundOnly
$false -Computerfqdn first_trusted_application_computer
```

**Example:**

```
New-CsTrustedApplicationPool -Identity trustedpool.sip.com -Registrar lyncserver.synergy.com
-Site 1 -TreatAsAuthenticated $true -ThrottleAsServer $true -RequiresReplication $false
-OutboundOnly $false -Computerfqdn impserverPub.sip.com
```

where:

| Parameter | Description |
|---|---|
| -Identity | Enter the name of the trusted application pool for the IM and Presence Service deployment. This must be in FQDN format. For example: `trustedpool.sip.com`.<br>**Tip** Ignore warning messages regarding the machine not found in Active Directory and proceed to apply the changes. |
| -Registrar | The service ID or FQDN of the Registrar service for the pool. For example: `lyncserver.synergy.com`.<br>You can check this value using the command **Get-CsPool**. |
| -Site | The numeric value of the site where you want to create the trusted application pool.<br>**Tip** Use the **Get-CsSite** Management Shell command. |
| -Computerfqdn | The FQDN of the IM and Presence Service routing node. For example: `impserverPub.sip.com`.<br>• impserverPub = the IM and Presence Service hostname.<br>• sip.com = the IM and Presence Service domain. |

**Step 2** For each IM and Presence Service node, enter the following commands to add the FQDN of the node as a trusted application computer to the new application pool:

```
New-CsTrustedApplicationComputer -Identity imp_FQDN -Pool new_trusted_app_pool_FQDN
```

**Example:**

```
New-CsTrustedApplicationComputer -Identity impserver2.sip.com -Pool trustedpool.sip.com
```

where:

| Parameter | Description |
|---|---|
| -Identity | The FQDN of the IM and Presence Service node. For example: `impserver2.sip.com`.<br>**Note** Do not add the IM and Presence Service routing node as a trusted application computer using this command. |
| -Pool | The FQDN of the trusted application pool that is used for the IM and Presence Service deployment. For example: `trustedpool.sip.com`. |

**Step 3** Enter the following command to create a new trusted application and add it to the new application pool:

```
New-CsTrustedApplication -ApplicationID new_application_name -TrustedApplicationPoolFqdn
new_trusted_app_pool_FQDN -Port 5061
```

**Example:**

```
New-CsTrustedApplication -ApplicationID imptrustedapp.sip.com -TrustedApplicationPoolFqdn
trustedpool.sip.com -Port 5061
```

where:

| Parameter | Description |
|---|---|
| -ApplicationID | The name of the application. This can be any value. For example: imptrustedapp.sip.com. |
| -TrustedApplicationPoolFqdn | The FQDN of the trusted application pool server for the IM and Presence Service deployment. For example: `trustedpool.sip.com`. |
| -Port | The SIP listening port of the IM and Presence Service node. For TLS the port is 5061. |

### What to Do Next

Publish Topology, on page 5

# Publish Topology

The following procedure describes how to commit the topology.

### Procedure

**Step 1** Log in to the Lync Server Management Shell.

**Step 2** Enter the **Enable-CsTopology** command to enable the topology.

### What to Do Next

Configure Certificates on Lync, on page 6

# Configure Certificates on Lync

Complete the following tasks to install and set up certificates on your Lync servers for partitioned intradomain federation with IM and Presence Service.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Install Certificate Authority Root Certificates on Lync, on page 6 | To support TLS encryption between IM and Presence Service and Lync, each Lync server must have a signed security certificate. |
| **Step 2** | Validate Existing Lync Signed Certificate, on page 8 | To support TLS encryption between IM and Presence Service and Lync, each Lync server must have a signed security certificate that supports Client Authentication. |
| **Step 3** | Request a Signed Certificate from a Certificate Authority for Lync, on page 9 | Request a newly signed certificate from the Certificate Authority (CA) and install it onto a Lync server. |
| **Step 4** | Download a Certificate from the CA Server, on page 10 | Download the newly signed certificate from the CA server. |
| **Step 5** | Import a Signed Certificate for Lync, on page 10 | Import the newly signed certificate into Lync. |
| **Step 6** | Assign Certificate on Lync, on page 11 | On the Lync server, assign the newly signed certificate. |
| **Step 7** | Restart Services on Lync Servers, on page 12 | Restart the Lync front-end services to ensure that the configuration takes effect. |

## Install Certificate Authority Root Certificates on Lync

TLS configuration must be used for partitioned intradomain federation between the IM and Presence Service and Lync servers. TCP cannot be used. To support TLS encryption between IM and Presence Service and Lync, each Lync server must have a signed security certificate. This signed certificate, along with the root certificate of the Certificate Authority (CA) that signed the certificate, must be installed on each Lync server.

Cisco recommends that Lync and IM and Presence Service servers share the same CA. If not, the root certificate of the CA that signed the IM and Presence Service certificates must also be installed on each Lync server.

Generally, the root certificate of the Lync CA is already installed on each Lync server. Therefore, if Lync and IM and Presence Service share the same CA, there may be no need to install a root certificate. However, if a root certificate is required, see the following details.

If you are using Microsoft Certificate Authority, refer to the following procedures in the *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager* for information about installing the root certificate from the Microsoft Certificate Authority onto Lync:

- Downloading the CA Certification Chain
- Installing the CA Certification Chain

If you are using an alternative CA, the following procedure is a generic procedure for installing root certificates onto Lync servers. The procedure for downloading the root certificate from the CA differs depending on your chosen CA.

**Note** The *Integration Guide for Configuring IM and Presence Service for Interdomain Federation* document refers to the Access Edge Server. For partitioned intradomain federation, you can replace references to the Access Edge Server with Lync Standard Edition server or Enterprise Edition front-end server.

**Before You Begin**

Download the root certificate or certificate chain from your CA and save it to the hard disk of your Lync server.

### Procedure

**Step 1** On your Lync server, choose **Start** > **Run**.

**Step 2** Enter mmc and click **OK.**

**Step 3** From the **File** menu, choose **Add/Remove Snap-in**.

**Step 4** From the **Add/Remove Snap-in** dialog box, click **Add**.

**Step 5** From the list of Available Standalone Snap-ins, choose **Certificates** and click **Add**.

**Step 6** Choose **Computer Account**, and then click **Next**.

**Step 7** In the **Select Computer** dialog box, check the **<Local Computer> (the computer this console is running on)** check box and click **Finish**.

**Step 8** Click **Close**, and then click **OK**.

**Step 9** In the left pane of the Certificates console, expand **Certificates (Local Computer)**.

**Step 10** Expand **Trusted Root Certification Authorities**.

**Step 11** Right-click **Certificates** and choose **All Tasks**.

**Step 12** Click **Import.**

**Step 13** In the Import Wizard, click **Next**.

**Step 14** Click **Browse** and navigate to where you saved the root certificate or certificate chain.

**Step 15** Choose the file and click **Open**.

**Step 16** Click **Next**.

**Step 17** Leave the default value **Place all certificates in the following store** and verify that **Trusted Root Certification Authorities** appears under the Certificate store.

**Step 18** Click **Next** and then click **Finish**.

**Step 19** Repeat Step 11 to Step 18 as necessary for other CAs.

### What to Do Next

Validate Existing Lync Signed Certificate, on page 8

### Related Topics

Integration Troubleshooting

## Validate Existing Lync Signed Certificate

To support TLS encryption between IM and Presence Service and Lync, each Lync server must have a signed security certificate that supports Client Authentication. If a signed certificate is already installed on the Lync server, the following procedure describes how to check if that existing signed certificate supports Client Authentication.

Verify that the certificate is assigned one of the following OID values:

- If the certificate is configured for both server and client authentication, the OID value is “1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2”
- If the certificate is configured for server authentication only, the OID value is “1.3.6.1.5.5.7.3.1”

**Note**

- For Standard Edition, you must perform this procedure on all Standard Edition servers.
- For Enterprise Edition, you must perform this procedure on all front-end servers.

### Procedure

**Step 1** On your Lync server, choose **Start** > **Run**.

**Step 2** Enter mmc and click **OK**.

**Step 3** From the File menu, choose **Add/Remove Snap-in**.

**Step 4** From the **Add/Remove Snap-in** dialog box, click **Add**.

**Step 5** From the list of Available Standalone Snap-ins, choose **Certificates** and click **Add**.

**Step 6** Choose **Computer Account** and click **Next**.

**Step 7** In the **Select Computer** dialog box, check the **<Local Computer> (the computer this console is running on)** check box and click **Finish**.

**Step 8** Click **Close**, and then click **OK**.

**Step 9** In the left pane of the Certificates console, expand **Certificates (Local Computer)**.

**Step 10** Expand **Personal** and choose **Certificates**.

**Step 11** Find the signed certificate currently used by Lync in the right pane.

**Step 12** Verify that **Client Authentication** is listed in the Intended Purposes column.

### What to Do Next

Request a Signed Certificate from a Certificate Authority for Lync, on page 9

### Related Topics

Integration Troubleshooting

## Request a Signed Certificate from a Certificate Authority for Lync

To support TLS encryption between IM and Presence Service and Lync, each Lync server must have a signed security certificate that supports Client Authentication and Server Authentication. The following procedure outlines how to request a newly signed certificate from the Certificate Authority (CA) and install it onto a Lync server.

The following procedure is based on a Windows Server 2003 certification authority. The procedure may be slightly different on other Windows server versions.

**Note** The CA must have a certificate template that supports client authentication and server authentication Extended Key Usage (EKU), and this template must be used to sign the certificate.

Verify that the certificate is assigned one of the following OID values before you install the certificate onto a Lync server:

- If the certificate is configured for both server and client authentication, the OID value is “1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2”
- If the certificate is configured for server authentication only, the OID value is “1.3.6.1.5.5.7.3.1”

**Tip** If a specific template type is not specified when you generate the Certificate Signing Request (CSR), a default template format is used. The template type that you specify during the certificate enrollment process must match the template type that is specified in the certificate, otherwise the certificate enrollment process fails.

### Procedure

**Step 1** In the Lync Server Management Shell enter the following command to create the CSR file:

```
Request-CsCertificate -New -Type Default -Output filename -ClientEku $true
```

**Note** If you want to create a specific request for an internal or external certificate, use the `-Type Internal` or `-Type External` parameters instead of `-Type Default`.

If you are using a custom certificate template on your CA to sign the certificate, add the `-Template` *`template_name`* parameter to the command string.

**Step 2** Log in to the Lync server and open a web browser.

**Step 3** Open the following URL: `http://ca_server_IP_address/certsrv` (If it is SSL encrypted, use https instead of http.)

**Step 4** Click **Request a Certificate** and then click **Advanced Certificate Request**.

**Step 5** Choose **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 request file you created using a text editor.

**Step 7** Select and copy all of the text from the request file and paste it into the browser in the field **Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7)**:

**Step 8** Click **Submit**.

### What to Do Next

Download a Certificate from the CA Server, on page 10

## Download a Certificate from the CA Server

Complete the following procedure to download the certificate from the CA server.

### Procedure

**Step 1** Log into the CA server.

**Step 2** Choose **Start** > **Administrative Tools** > **Certificate Authority** to launch the CA console.

**Step 3** Click **Pending Requests**.

**Step 4** From the right pane, right-click on the certificate request that you submitted and choose **All Tasks** > **Issue**.

**Step 5** Log into the Lync server and open a web browser.

**Step 6** Open the following URL: `http://ca_server_IP_address/certsrv` (If it is SSL encrypted, use https instead of http.)

**Step 7** From **View the Status of a Pending Certificate Request**, choose your certificate request.

**Step 8** Download the certificate.

### What to Do Next

Import a Signed Certificate for Lync, on page 10

## Import a Signed Certificate for Lync

Complete the following procedure to import the signed certificate.

### Before You Begin

**Note** Verify that the certificate is assigned one of the following OID values:

- If the certificate is configured for both server and client authentication, the OID value is “1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2”
- If the certificate is configured for Server Authentication only, the OID value is “1.3.6.1.5.5.7.3.1”

### Procedure

In the Lync Server Management Shell, enter the following command to import the signed certificate:

```
Import-CsCertificate -Path "signed_certificate_path" -PrivateKeyExportable $false
```

**Note** If the certificate contains a private key, use the `-PrivateKeyExportable $true` parameter.

### What to Do Next

Assign Certificate on Lync, on page 11

### Related Topics

Integration Troubleshooting

## Assign Certificate on Lync

Complete the following procedure to assign the certificate.

### Procedure

**Step 1** Choose **Start** > **Lync Server Deployment Wizard**.

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

**Step 3** Click **Run Again** to Request, Install or Assign Certificates.

**Step 4** On the Certificate Wizard window, choose the default certificate.

**Step 5** Click **Assign**.

**Step 6** On the Certificate assignment window, click **Next**.

**Step 7** Choose the imported certificate in the certificate store window and click **Next**.

**Step 8** In the certificate assignment summary window click **Next**.

**Step 9** On the executing commands window, wait for the task status to report **Completed** and then click **Finish**.

**Step 10** Close the certificate wizard window.

### What to Do Next

Restart Services on Lync Servers, on page 12

## Restart Services on Lync Servers

After you complete all the configuration steps on Lync, you must restart the Lync front-end services to ensure that the configuration takes effect.

**Note**

- Cisco recommends that you perform this procedure during a scheduled maintenance window.
- For Standard Edition, you must perform this procedure on all Standard Edition servers.
- For Enterprise Edition, you must perform this procedure on all front-end servers.

### Procedure

**Step 1** Choose **Start** > **Programs** > **Administrative Tools** > **Services**.

**Step 2** Right-click the service **Lync front end server** and choose **Restart**.

### Related Topics

Integration troubleshooting