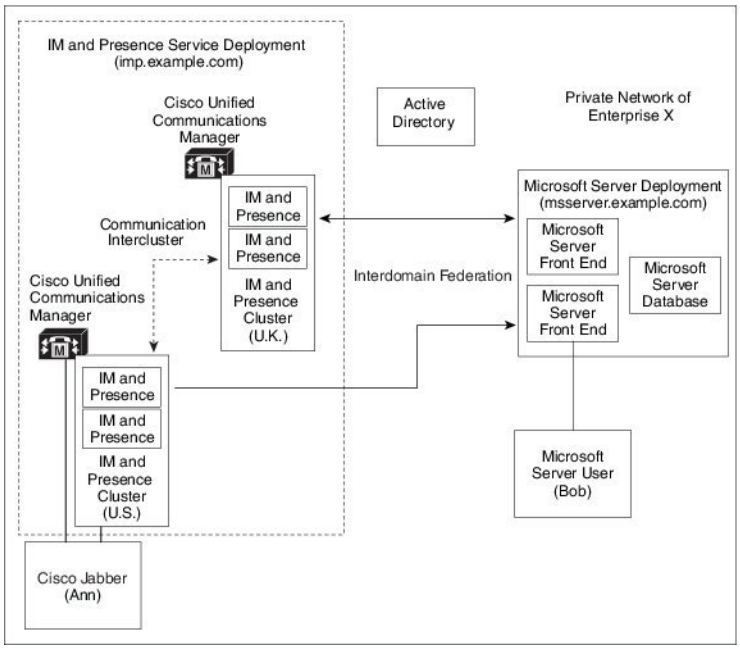
Interdomain Federation to Microsoft Lync

This section explains the Interdomain Federation to Microsoft Lync.

Interdomain Federation to Microsoft Lync within an Enterprise

Figure 1: Interdomain Federation to Microsoft Server within an Enterprise



When the Microsoft server and IM and Presence Service domains are different, you can configure federation within the enterprise. You do not have to use subdomains; separate domains are equally applicable. See topics related to federation and subdomains for more information.

Configuration Task Flow for Microsoft Lync Federation

Complete the following tasks to set up federation between IM and Presence Service and Microsoft Lync. This configuration supports both chat-only deployments and chat+calling deployments.

Note Interdomain federation via Expressway Gateway's SIP Broker is supported for single enterprise networks only (intracompany). For Business to Business, you must use Expressway Traffic Classification or the ASA.

Procedure

	Command or Action	Purpose
Step 1	Add a Microsoft Lync Domain Within Enterprise, on page 3	In the IM and Presence Service, add a federated domain entry for the Microsoft Lync domain. The IM and Presence Service automatically adds the incoming ACL for the federated domain entry.
Step 2	Configure Static Routes from IM and Presence to Lync, on page 3	In the IM and Presence Service, configure an individual TLS static route for each Microsoft Lync server domain. Each route should point to a specific Microsoft front end server. **Note** You must configure TLS static routes. TCP is not supported for federation with Microsoft Lync.
Step 3	Configure Expressway Gateway for Microsoft Lync Federation, on page 4	**Optional**. For chat+calling deployments only, add an Expressway Gateway. On the gateway, configure Microsoft interoperability and the SIP broker. **Note** For chat-only deployments, you do not need the Expressway Gateway.
Step 4	On the Lync server, configure TLS static routes using one of the following procedures: • Configure Static Route from Lync to Expressway Gateway, on page 4 • Configure a Static Route from Lync to IM and Presence, on page 6	If you have a chat+calling deployment, configure the TLS static route to the Expressway Gateway. If you have a chat-only deployment, configure the TLS static route to the IM and Presence Service routing node.
Step 5	Configure Trusted Applications on Lync Server, on page 8	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.

	Command or Action	Purpose
Step 6	Publish Topology, on page 10	On the Lync server, commit the topology.
Step 7	Set up Certificates on IM and Presence for Federation with Lync, on page 10	In the IM and Presence Service, upload the root certificate for the CA that signs the Lync server certificates to IM and Presence Service. Also, set up TLS Peer subjects.

Add a Microsoft Lync Domain Within Enterprise

When you configure a federated domain entry for a Lync server, the IM and Presence Service automatically adds the incoming ACL for the federated domain entry. You can see the incoming ACL associated with a federated domain on IM and Presence Administration, but you cannot modify or delete it. You can only delete the incoming ACL when you delete the (associated) federated domain entry.

Procedure

Step 1 Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Presence** > **Inter-Domain Federation** > **SIP Federation**.

Step 2 Click **Add New**.

Step 3 Enter the federated domain name in the Domain Name field.

Step 4 Enter a description that identifies the federated domain in the Description field.

Step 5 Choose **Inter-domain to OCS/Lync**.

Step 6 Check the **Direct Federation** check box.

Step 7 Click **Save**.

Step 8 After you add, edit, or delete a SIP federated domain, restart the Cisco XCP Router. Log in to the **Cisco Unified IM and Presence Service Serviceability** user interface. Choose **Tools** > **Control Center - Network Services**. When you restart the Cisco XCP Router, it causes a restart of all XCP services on the IM and Presence Service.

Note A restart of the Cisco XCP Router is required on all IM and Presence Service nodes within the cluster.

What to do next

Configure Static Routes from IM and Presence to Lync, on page 3

Configure Static Routes from IM and Presence to Lync

Use this procedure to configure TLS static routes on the IM and Presence Service that point to the Microsoft Lync server domain. You must add an individual static route for each Microsoft server domain. Each static route that you set up should point to a specific Microsoft Lync Enterprise Edition front-end server or Standard Edition server.

For high availability purposes, you can configure additional backup static routes to each Microsoft server domain. The backup route has a lower priority and is used only if the next hop address of the primary static route is unreachable.

Procedure

Step 1 From Cisco Unified CM IM and Presence Administration, choose **Presence** > **Routing** > **Static Routes**.

Step 2 Click **Add New**.

Step 3 Enter the **Destination Pattern** value so that the domain or FQDN is reversed. For example, if the domain is `domaina.com`, enter `.com.domaina.*`.

Step 4 In the **Next Hop** field, enter the Microsoft Lync server IP address or FQDN.

Step 5 In the **Next Hop Port** field enter **5061**.

Step 6 From the **Route Type** drop-down list, choose **Domain**.

Step 7 From the **Protocol Type** drop-down list box, select **TLS**.

Step 8 Click **Save**.

What to do next -

Fo chat+calling deployments, Configure Expressway Gateway for Microsoft Lync Federation, on page 4

For chat-only deployments, Configure a Static Route from Lync to IM and Presence, on page 6

Configure Expressway Gateway for Microsoft Lync Federation

Chat + calling deployments only. On the Expressway Gateway, configure Microsoft interoperability and enable the SIP broker. For Expressway Gateway configuration, see the *Cisco Expressway and Microsoft Lync Deployment Guide* at:

http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html.

Note For chat-only deployments, you do not need to deploy the Expressway Gateway.

What to do next

Configure Static Route from Lync to Expressway Gateway, on page 4

Configure Static Route from Lync to Expressway Gateway

For chat + calling deployments only. On the Lync servers, configure TLS static routes that point to the Expressway Gateway fully qualified domain name (FQDN).

Note Make sure that the FQDN in the static route is resolvable from the Lync front-end server and that it resolves to the correct IP address for the Expressway Gateway.

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**.

Tip Navigate to either Microsoft Lync Server 2010 or 2013, depending on your Microsoft Lync Server version.

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

```
$tlsRoute = New-CsStaticRoute -TLSRoute -Destination expresswayGateway_fqdn -Port
expresswayGateway_TLS_listening_port -usedefaultcertificate $true -MatchUri
expresswayGateway_domain
```

where:

Parameter	Description
-Destination	The fully qualified domain name (FQDN) of the Expressway Gateway. For example, `expGateway.sip.com`
-Port	The TLS listening port on Expressway Gateway. The default listening port is `65072`.
-MatchUri	The domain for the Expressway Gateway. For example, `sip.com`.

Example:

```
$tlsRoute = New-CsStaticRoute -TLSRoute -Destination expGateway.sip.com -Port 65072
-usedefaultcertificate $true -MatchUri sip.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.
- If you are using IPv6 with a Microsoft Lync server 2013, the * wildcard option is not supported in the **-MatchUri** parameter.
- If you set **-usedefaultcertificate** to false, you must specify the TLSCertIssuer and TLSCertSerialNumber parameters. These parameters indicate the name of the certificate authority (CA) that issues the certificate used in the static route and the serial number of the TLS certificate, respectively. See the Lync Server Management Shell for more information about these parameters.

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

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

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 Expressway Gateway domain) and the FQDN of the 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 on Lync Server, on page 8

Configure a Static Route from Lync to IM and Presence

If you have a chat-only deployment, on the Lync server, configure a TLS static route to the IM and Presence Service routing node. It is not necessary to create static routes to subscriber nodes, nor any intercluster peer nodes even if your IM and Presence Service deployment has multiple clusters.

However, a static route is required for each IM and Presence Service domain.

The following table lists the sample configuration parameters that are used in this procedure.

Table 1: Sample Parameters for TLS Static Route on Microsoft Lync

Description	Sample Parameters
IM and Presence Service node FQDN (routing IM and Presence Service node) Ensure the FQDN can resolve to the correct IP address.	impserverPub.sip.com
IM and Presence Service node IP address (routing IM and Presence Service node)	10.10.1.10
IM and Presence Service node TLS port The TLS port value must match what is configured in the user interface. To check the value, log in to the **Cisco Unified CM IM and Presence Administration** user interface and choose **System** > **Application Listeners** > **Default Cisco SIP Proxy TLS Listener - Peer Auth**. **Note** Cisco recommends port 5061; however, you can use port 5062.	5061
IM and Presence Service node domain	sip.com
Lync Registrar server	lyncserver.synergy.com

Note

- When using Transport Layer Security (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 IM and Presence Service node to which the static route points.
- 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**.

Tip Navigate to either Microsoft Lync Server 2010 or 2013, depending on your Microsoft Lync Server version.

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 destination_domain
```

Example:

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

where:

Parameter	Description
-Destination	The FQDN of the IM and Presence Service routing node.
-Port	The listening port of the IM and Presence Service routing node.
-MatchUri	The destination IM and Presence Service domain.

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.
- If you are using IPv6 with a Microsoft Lync server 2013, the * wildcard option is not supported in the **-MatchUri** parameter.
- If you set **-usedefaultcertificate** to false, you must specify the TLSCertIssuer and TLSCertSerialNumber parameters. These parameters indicate the name of the certificate authority (CA) that issues the certificate used in the static route and the serial number of the TLS certificate, respectively. See the Lync Server Management Shell for more information about these parameters.

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 IM and Presence Service node.

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 on Lync Server, on page 8

Configure Trusted Applications on Lync Server

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`. **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`. 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. **Tip** Use the **Get-CsSite** Management Shell command.
-Computerfqdn	The FQDN of the IM and Presence Service routing node. For example: `impserverPub.sip.com`. • impserverPub = the IM and Presence Service hostname. • 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`. **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. 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 10

Publish 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

Set up Certificates on IM and Presence for Federation with Lync, on page 10

Set up Certificates on IM and Presence for Federation with Lync

Use this procedure to set up certificates on your IM and Presence Service nodes for Federation with Microsoft Lync.

Procedure

Step 1 On the IM and Presence Service, upload the root certificate for the CA that signs the Microsoft server certificate.

- Upload the certificate as a cup-trust certificate.
- Leave the **Root Certificate** field blank.
- Import the self-signed certificate onto the IM and Presence Service.

Step 2 Generate a CSR for the IM and Presence Service so that the certificate can be signed by a CA. Upload the CSR to the CA that signs your certificate.

Important
- The CA must sign the certificate so that it has "Enhanced Key Usage" with both "Server Authentication" and "Client Authentication".
- If this is Microsoft Windows Server CA, it must use a certificate template that has "Server Authentication" and "Client Authentication".

Step 3 When you have retrieved the CA-signed certificate and the CA root certificate, upload the CA-signed certificate and the root certificate to the IM and Presence Service node.

- Upload the root certificate as a cup-trust certificate.
- Upload the CA-signed cup certificate. Specify the root certificate .pem file as the root certificate.

Step 4 Add a TLS Peer subject on IM and Presence Service for the Microsoft server. Use the FQDN of the Microsoft server.

Step 5 Add the TLS Peer to the Selected TLS Peer Subjects list.

- Make sure that the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher is chosen for the TLS Context Configuration.
- Make sure that you disable empty TLS fragments.

What to do next

Set up certificates on the Microsoft Lync server that have "Enhanced Key Usage" with "Server Authentication" and "Client Authentication" values. For details, see:

- Request Certificate from CA Server
- Microsoft TechNet Library, Windows Server — Implementing and Administering Certificate Templates at http://technet.microsoft.com/en-us/library/cc731256(v=ws.10).aspx.