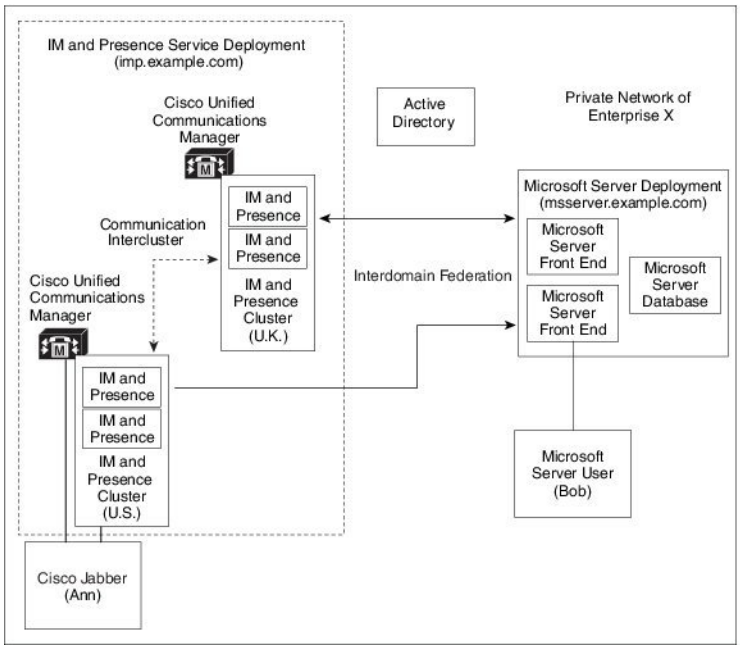
Interdomain Federation to Microsoft OCS

This section explains the Interdomain Federation to Microsoft OCS.

Interdomain Federation to Microsoft OCS 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 OCS Federation

Complete the following tasks to set up federated links between IM and Presence Service and Microsoft OCS.

If you are using direct federation from IM and Presence Service to OCS without the Access Edge server or Cisco Adaptive Security Appliance, you must configure a TLS or TCP static route for each domain on the OCS server. These static routes point to an IM and Presence Service node. The Cisco Adaptive Security Appliance or the Microsoft Access Edge are not required.

- For Standard Edition, configure static routes on all Standard Edition servers.
- For Enterprise Edition, configure static routes on all pools.

Procedure

	Command or Action	Purpose
Step 1	Add a Microsoft OCS Domain Within Enterprise, on page 3	In the IM and Presence Service, add a federated domain entry for the Microsoft OCS domain. The IM and Presence Service automatically adds the incoming ACL for the federated domain entry.
Step 2	Configure Static Route on IM and Presence Service for Microsoft Servers, on page 4	In the IM and Presence Service, configure an individual static route for each Microsoft OCS server domain. Each route should point to a specific Microsoft front end server. **Note** For OCS, you can choose either TCP or TLS as the protocol type.
Step 3	Configure Static Routes on OCS to Point to the IM and Presence Service, on page 4	On the OCS server, configure TCP or TLS static routes that point to the IM and Presence Service domain. Each route must point to a specific IM and Presence Service node.
Step 4	Verify Peer Authentication Listener, on page 5	Verify that on the IM and Presence Service the Peer Auth Listener is configured as port 5061 and the Server Auth Listener is not port 5061.
Step 5	Adding a Host Authorization Entry for the IM and Presence Service Node on OCS, on page 6	On the OCS server, configure host authorization entries for each IM and Presence Service node. With TLS encryption, you must add two entries for each IM and Presence node: • one entry with the IM and Presence node IP address • one entry with the IM and Presence node FQDN If you are not using TLS encryption, configure one host authorization entry for each IM and Presence Service node with the node IP address.
Step 6	Configure Certificates on OCS for Interdomain Federation, on page 7	If you have TLS configured between OCS to IM and Presence Service, configure certificates on OCS for interdomain federation with IM and Presence Service.

	Command or Action	Purpose
		Note If you are not using TLS, you can skip this step.
Step 7	Enable Port 5060/5061 on the OCS Server, on page 7	On the OCS server, confirm the listener ports for TLS (The transport can be MTLS or TLS) or TCP are configured. . • For TLS static routes to the OCS server, use port 5061. • For TCP static routes to the OCS server, use port 5060.
Step 8	Configure OCS to use FIPS, on page 8	If you are using TLS, configure OCS to use FIPS.
Step 9	Set Up Certificates on the IM and Presence Service Node for Federation with Microsoft Server over TLS , on page 8	If you are using TLS, upload the root certificate for the CA that signs the OCS server certificates to IM and Presence Service.

Add a Microsoft OCS Domain Within Enterprise

When you configure a federated domain entry for an OCS 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.

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 Route on IM and Presence Service for Microsoft Servers, on page 4

Configure Static Route on IM and Presence Service for Microsoft Servers

To configure the IM and Presence Service to use TLS when exchanging IM and availability with a federated Microsoft server domain, or to use TCP for an OCS domain, you must configure a static route on IM and Presence Service that points to the Microsoft server and not the external edge of Microsoft Access Edge.

You must add an individual static route for each Microsoft server domain. The Microsoft server domain static route should point to the IP address of a specific Microsoft server 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.

Step 1 Log in to the **Cisco Unified CM IM and Presence Administration** user interface. 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.*` as the Destination Pattern value.

Step 4 Enter the remaining parameters as follows:

a) Enter the Next Hop, the value is the Microsoft server IP address or FQDN.

b) Choose the Next Hop Port number and Protocol Type value.

- For TCP — from the drop-down list, choose **TCP** as the Protocol Type and **5060** as the Next Hop Port number.
- For TLS — from the drop-down list, choose **TLS** as the Protocol Type and **5061** as the Next Hop Port number.

Note Microsoft OCS servers support federation over TCP or TLS.

c) From the Route Type drop-down list, choose Domain.

Step 5 Click **Save**.

What to do next

Configure Static Routes on OCS to Point to the IM and Presence Service, on page 4

Configure Static Routes on OCS to Point to the IM and Presence Service

To allow OCS to route requests to IM and Presence Service for direct federation, you must configure a TLS or TCP static route on the OCS server for each IM and Presence Service domain. These static routes are to point to an IM and Presence Service node.

Note

- For Standard Edition, you must complete this procedure on all Standard Edition servers.
- For Enterprise Edition, you must complete this procedure on all pools.

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Office Communications Server 2007 R2**.

Step 2 Right-click the Enterprise Edition pool name or the Standard Edition server name, as appropriate.

Step 3 Choose **Properties** > **Front End Properties**.

Step 4 Choose the **Routing** tab and click **Add**.

Step 5 Enter the domain for the IM and Presence Service node, for example, foo.com.

Step 6 Ensure that the check box for **Phone URI** is unchecked.

Step 7 Set the next hop transport, port, and IP address/FQDN values:

- For TCP, choose **TCP** as the Next Hop Transport value and enter a Next Hop Port value of **5060**. Enter the IP address of the IM and Presence Service node as the Next Hop IP Address.
- For TLS, choose **TLS** as the Next Hop Transport value and enter a Next Hop Port value of **5061**. Enter the IP address of the IM and Presence Service node as the FQDN.

Note
- The port used for the TLS static route must match the Peer Auth Listener port that is configured on the IM and Presence Service node.
- The FQDN must be resolvable by the OCS server. Ensure that the FQDN resolves to the IP address of the IM and Presence Service node.

Step 8 Ensure that the check box for **Replace host in request URI** is unchecked.

Step 9 Click **OK** to close the **Add Static Route** window. The new static route should appear in the Routing list.

Step 10 Click **OK** again to close the **Front End Server Properties** window.

What to do next

See Verify Peer Authentication Listener in the Interdomain Federation for IM and Presence Service on Cisco Unified Communcations Manager guide.

Verify Peer Authentication Listener

Verify that the peer authentication listener is configured correctly on the IM and Presence Service.

Step 1 From Cisco Unified CM IM and Presence Administration, choose**System** > **Application Listener**.

Step 2 Click **Find**.
The list of configured application listener ports displays. The default peer auth listener port and server auth listener ports also display.

Step 3 Confirm that the **Default Cisco SIP Proxy TLS Listener - Peer Auth** port is 5061.

Step 4 Confirm that the **Default Cisco SIP Proxy TLS Listener - Server Auth** port is not 5061. If this port is configured as 5061, you must change it to another value. For example, 5063.

What to do next

Adding a Host Authorization Entry for the IM and Presence Service Node on OCS, on page 6

Adding a Host Authorization Entry for the IM and Presence Service Node on OCS

To allow OCS to accept SIP requests from the IM and Presence Service without being prompted for authorization, you must configure host authorization entries on OCS for each IM and Presence Service node.

If you are configuring TLS encryption between OCS and the IM and Presence Service, you must add two Host Authorization entries for each IM and Presence Service node, as follows:

- The first entry must contain the FQDN of the IM and Presence Service node.
- The second entry must contain the IP address of the IM and Presence Service node.

If you are not configuring TLS encryption, then you add only one host authorization entry for eachIM and Presence Service node. This host authorization entry must contain the IP address of the IM and Presence Service node.

The following procedure describes how to add the required host authorization entries.

Note

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

Step 1 Choose the **Host Authorization** tab on OCS.

Step 2 Perform one of the following steps:

a) Enter the IP address of the authorized host if you configured a static route on OCS that specifies the next hop computer by its IP address.

b) Enter the FQDN of the authorized host if you configured a static route on OCS that specifies the next hop computer by its FQDN.

Step 3 Click **Add**.

Step 4 Choose **IP.**

Step 5 Enter the IP address of the IM and Presence Service node.

Step 6 Check the **Throttle as Server** check box.

Step 7 Check the **Treat as Authenticated** check box.

Note Do not check the **Outbound Only** check box.

Step 8 Click **OK**.

What to do next

Configure Certificates on OCS for Interdomain Federation, on page 7

Configure Certificates on OCS for Interdomain Federation

If you have TLS configured between OCS to IM and Presence Service, configure certificates on OCS for interdomain federation with IM and Presence Service.

Note If you aren't using TLS, you can skip this procedure.

Step 1 Retrieve the CA root certificate and the OCS signed certificate by completing the following steps:

a) Download and install the CA certificate chain.
b) Request a certificate from the CA server.
c) Download the certificate from the CA server.

Step 2 From the OCS Front End Server Properties, choose the **Certificates** tab, and click **Select Certificate** to choose the OCS signed certificate.

What to do next

Enable Port 5060/5061 on the OCS Server, on page 7

Enable Port 5060/5061 on the OCS Server

For TCP static routes to the OCS server, use port 5060.

For TLS static routes to the OCS server, use port 5061.

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Microsoft Office Communicator Server 2007** on OCS.

Step 2 Right-click on the FQDN of Front End server.

Step 3 Choose **Properties** > **Front End Properties** and choose the **General** tab.

Step 4 If port 5060 or 5061 is not listed under Connections, click **Add**.

Step 5 Configure port value as follows:

a) Choose **All** as the IP Address Value.
b) Choose the Port Value.
   - For TCP, choose **5060** as the Port Value.
   - For TLS, choose **5061** as the Port Value.
c) Choose the Transport value.
   - For TCP, choose **TCP** as the Transport Value.
   - For TLS, choose **TLS** as the Transport Value.

Step 6 Click **OK**.

What to do next

Configure OCS to use FIPS, on page 8

Configure OCS to use FIPS

Configure FIPS on the OCS server. Complete this procedure only if you are using TLS only (TLSv1 rather than SSLv3).

Step 1 Open the **Local Security Settings** on OCS.

Step 2 In the console tree, choose **Local Polices**.

Step 3 Choose **Security Options**.

Step 4 Double-click **System Cryptography:Use FIPS Compliant** algorithms for encryption, hashing and signing.

Step 5 Enable the security setting.

Step 6 Click **OK**.

Note You may need to restart OCS for this to take effect.

Step 7 Import the CA root certificate for the CA that signs the IM and Presence Service certificate. Import the CA root certificate in to the trust store on OCS using the certificate snap-in.

What to do next

Set Up Certificates on the IM and Presence Service Node for Federation with Microsoft Server over TLS , on page 8

Set Up Certificates on the IM and Presence Service Node for Federation with Microsoft Server over TLS

This procedure applies only if you have set up TLS static routes between IM and Presence Service and Microsoft servers.

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. 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