# Interdomain Federation with Office 365

This section provides information on Interdomain Federation with Office 365.



# Office 365 Interdomain Federation Overview

The IM and Presence Service supports business to business interdomain federation with an Office 365 deploymnet. With this integration, Office 365 hosts a Skype for Business server, which handles instant messaging and presence for the Office 365 users.

**Note** With this integration, Office 365 hosts a Skype for Business server within the cloud. You can also federate with:

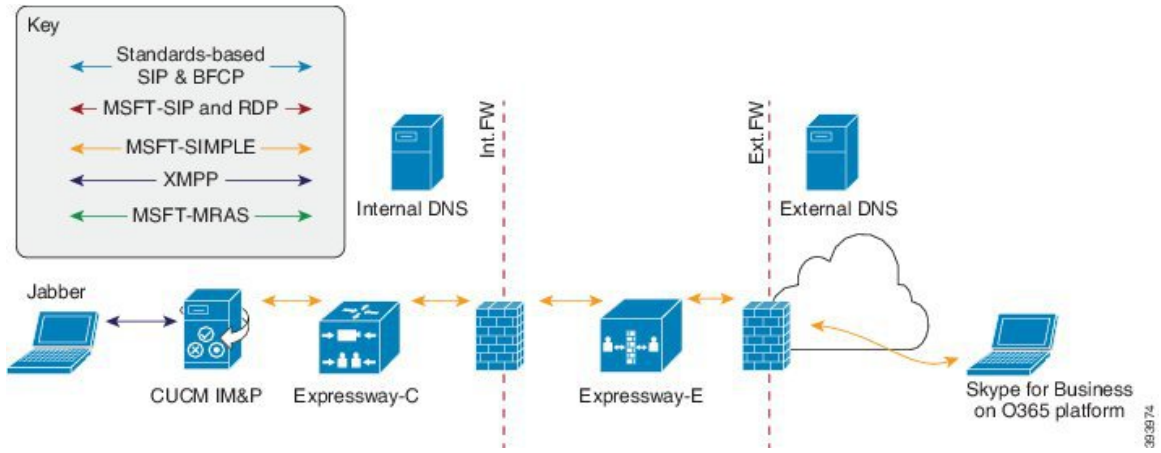
- A remote Skype for Business server in another company's network (Business to Business)
- An on-premise Skype for Business server in a different domain, but the same enterprise network as the IM and Presence Service (Single Enterprise Network)

For these Skype for Buisness federations, see Interdomain Federation with Skype for Business.

### Office 365 Federation Example

The following image illustrates Business to Business federation with an Office 365-hosted Skype for Business server. Communication between the IM and Presence Service and Office 365 must cross a company firewall and go to the cloud. You must deploy Expressway-C in the internal network and Expressway-E in the DMZ of the company firewall in order to guard traffic that enters and leaves the enterprise network.

*Figure 1: Office 365 Federation Example*




# Office 365 Interdomain Federation Task Flow

Complete these tasks on the IM and Presence Service to configure business to business interdomain federation with an Office 365 deployment.

### Before you begin

By default, the Federation routing parameter is set to the database publisher node FQDN upon installation. If you want to reset this value, go to Configure Federation Routing Parameters.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Turn on Federation Services , on page 3 | Turn on the Cisco XCP SIP Federation Connection Manager service. |
| **Step 2** | Add DNS SRV Record for the IM and Presence Service, on page 3 | Configure a public DNS SRV record for the IM and Presence domain. The SRV should resolve to the Expressway-E IP address |
| **Step 3** | Add Office 365 Domain to IM and Presence Service , on page 3 | In the IM and Presence Service, add the Office 365 domain entry. |
| **Step 4** | Configure Static Route to Office 365, on page 4 | In the IM and Presence Service, configure a TLS static route to Expressway-C. |
| **Step 5** | Add Expressway as TLS Peer, on page 4 | In the IM and Presence Service, assign Expressway-C as a TLS peer. |
| **Step 6** | Add Expressway to Access Control List, on page 5 | In the IM and Presence Service, add the Expressway-E server to the inbound access control list. |
| **Step 7** | Restart Cisco XCP Router, on page 6 | Restart the Cisco XCP Router on all IM and Presence Service nodes. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | Exchange Certificates, on page 6 | Exchange certificates between the servers in your deployment. For the IM and Presence Service, you will need to upload the Expressway-C certificate chain to the cup-trust store. |
| **Step 9** | Configure Expressway for Federation with Office 365, on page 7 | Configure Expressway for interdomain federation with Office 365. |

# Turn on Federation Services

Turn on the **Cisco XCP SIP Federation Connection Manager** service. This turns on the SIP Federation feature for each user that you provision. You must complete this task on each node in the cluster.

**Step 1** Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools** > **Service Activation**.

**Step 2** Fom the **Server** drop-down, choose an IM and Presence node and click **Go**.

**Step 3** Under **IM and Presence Services**, make sure that the adjacent radio button to the **Cisco XCP SIP Federation Connection Manager** service is checked.

**Step 4** Click **Save**.

**Step 5** The Cisco SIP Proxy service must be running for SIP federation to work. Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools** > **Feature Services** and verify that the Cisco SIP Proxy service is running.

# Add DNS SRV Record for the IM and Presence Service

Configure a public DNS SRV record that points to the IM and Presence Service. Office 365 uses this record to route traffic to the IM and Presence Service. The record must point to the Expressway-C servers as in the following example, where `expwye` represents the Expressway-E domain.

```
nslookup
set type=srv
_sipfederationtls._tcp.expwye
```

**Note** You can still configure interdomain federation without the DNS SRV record, but Office 365 will need to be configured manually with a route to the IM and Presence Service.

### What to do next

Add Office 365 Domain to IM and Presence Service , on page 3

# Add Office 365 Domain to IM and Presence Service

On the IM and Presence Service, add the Office 365 domain as a federated domain.

**Step 1** From Cisco Unified CM IM and Presence Administration, choose **Presence** > **Inter-Domain Federation** > **SIP Federation**.
**Step 2** Click **Add New**.
**Step 3** In the **Domain Name** field, enter the Office 365 domain.
**Step 4** Enter a **Description** of the domain. For example, `Office 365 federated domain`.
**Step 5** From the **Integration Type** drop-down, select **Inter-domain to OCS/Lync/S4B**.
**Step 6** Click **Save**.

### What to do next

Configure Static Route to Office 365, on page 4

# Configure Static Route to Office 365

On the IM and Presence Service, configure a TLS static route to Office 365 via Expressway-C.

**Step 1** From Cisco Unified CM IM and Presence Administration, choose **Presence** > **Routing** > **Static Routes**.
**Step 2** Click **Add New**.
**Step 3** In the **Destination Pattern** field, enter the Office 365 FQDN in a reversed format. For example, if the domain is `office365.com`, enter `.com.office365.*`.
**Step 4** In the **Next Hop** field, enter the Expressway-C 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

Add Expressway as TLS Peer, on page 4

# Add Expressway as TLS Peer

Use this procedure in the IM and Presence Service to add Expressway as a TLS peer subject.

**Step 1** Add Expressway-C as a TLS peer subject:
a) From Cisco Unified CM IM and Presence Administration, choose **System** > **Security** > **TLS Peer Subjects**.
b) Click **Add New**.
c) In the **Peer Subject Name** field, enter the Expressway-C fully qualified domain name of the Expressway-C.
d) Enter a **Description**.
e) Click **Save**.
**Step 2** Create a TLS Context that includes the Expressway TLS peer subject that you configured:

a) From Cisco Unified CM Administration, choose **System** > **Security** > **TLS Context Configuration**
b) Click **Find**.
c) Select **Default_Cisco_UP_SIP_Proxy_Peer_Auth_TLS_Context**.
d) Under **TLS Cipher Mapping**, use the arrows to move the desired TLS ciphers to the **Selected TLS Ciphers** box. However, leaving this at the default settng should be sufficient in most cases.
e) Under **TLS Peer Subject Mapping**, use the arrows to move the TLS peer subject that you created to the **Selected TLS Peer Subjects** list box.
f) Click **Save**.

### What to do next

Add Expressway to Access Control List, on page 5

# Add Expressway to Access Control List

On the IM and Presence Service, add inbound access control list (ACL) entries for the Expressway-C server so that Expressway-C can access the IM and Presence Service without authentication. For multicluster deployments, complete this procedure on each cluster.

**Note** If you have an ACL that provides global access (`Allow from all`), or an ACL which provides access to the domain on which the Expressway-C server resides (for example, `Allow from company.com`) then you do not need to add ACL entries for the Expressway-C server.

**Step 1** Log in to the IM and Presence Service publisher node.

**Step 2** From Cisco Unified CM IM Administration, choose **System** > **Security** > **Incoming ACL**.

**Step 3** Create your ACL entries:

a) Click **Add New**.
b) Enter a **Description** for the new ACL entry. For example, `Skype for Business Federation via Expressway-C`.
c) Enter an **Address Pattern** that provides access to the Expressway-C IP address or FQDN. For example, `Allow from 10.10.10.1` or `Allow from expwyc.company.com`.
d) Click **Save**.
e) Repeat this set of steps to create another ACL entry. To provide server access, you need two entries: an ACL with the server IP address, and an ACL with the server FQDN.

**Step 4** Restart Cisco SIP Proxy services:

a) Choose **Presence** > **Routing** > **Settings**.
b) Click **Restart All Proxy Services**.

### What to do next

Restart Cisco XCP Router, on page 6

# Restart Cisco XCP Router

After completing your configurations, restart the **Cisco XCP Router**.

**Step 1** From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Network Services**.

**Step 2** From the **Server** drop-down list box, choose the IM and Presence database publisher node and click **Go**.

**Step 3** Under **IM and Presence Services**, select the **Cisco XCP Router** service.

**Step 4** Click .

**Step 5** Repeat this procedure for all IM and Presence Service cluster nodes.

### What to do next

**Restart**

Configure Static Route to Office 365, on page 4

# Exchange Certificates

Exchange certificates among the servers in your deployment.

**Step 1** Download certificates from each system in the deployment:

- IM and Presence Service (internal certificate can be self-signed)
- Expressway-C (internal certificate can be self-signed)
- Expressway-E (external certificate must be CA-signed)
- Office 365 server (external certificate must be CA-signed)

**Step 2** On the IM and Presence Service, upload the Expressway-C certificate chain to the **cup-trust** store.

**Step 3** On the Expressway-C, upload the IM and Presence Service certificate.

**Step 4** On the Expressway-E, upload the Office 365 certificate.

**Note** For business to business Federation, the other company must upload the Expressway-E certificate to the Office 365 server.

### Certificate Notes

- For IM and Presence Service, you can download and upload certificates from the **Certificate Management** window in Cisco Unified IM OS Administration (choose **Security** > **Certificate Management**). For detailed procedures, see the "Security Configuration" chapter of the *Configuration and Administration Guide for IM and Presence Service* at http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html.

- For Expressway certificate management, see the *Cisco Expressway Administrator Guide* at http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-maintenance-guides-list.html.

### What to do next

Configure Expressway for Federation with Office 365, on page 7

# Configure Expressway for Federation with Office 365

After interdomain federation is configured on the IM and Presence Service, set up Cisco Expressway for business to business interdomain federation with Office 365. For Expressway configuration details, see *Chat and Presence XMPP Federation and Microsoft SIP Federation using IM and Presence or Expressway* at:

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

**Note** Make sure that your Expressway-C zone configuration points to the port that is associated with TLS Peer Authentication on the IM and Presence Service. You can confirm the correct port on Cisco Unified CM IM and Presence Administration by going to **System** > **Application Listeners** and confirming the port associated to **Default Cisco SIP Proxy TLS Listener - Peer Auth**. The default is **5062**.

### What to do next

For business to business Federation to work, the other company must configure their Office 365 deployment to federate with the IM and Presence Service.