Configuration Workflows for Interdomain Federation

This section explains the Configuration Workflows for Interdomain Federation.

Office 365 Workflow (Business to Business via Expressway)

The IM and Presence Service supports interdomain SIP federation with Office 365 via Cisco Expressway session classification in a business to business configuration. With this integration, Office 365 hosts the Skype for Business deployment.

Note For interdomain federation with Skype for Business without Office 365, see Skype for Business Workflow, on page 2.

IM and Presence Service Configuration

1. Start Federation services. See Turn on Federation Services.
2. Configure a public DNS SRV record for the IM and Presence domain. The SRV should resolve to the Expressway-E IP address. See Add DNS SRV Record for the IM and Presence Service.
3. In the IM and Presence Service, add the Office 365 domain entry. See Add Office 365 Domain to IM and Presence Service.

4. In the IM and Presence Service, configure a TLS static route to Expressway-C. See Configure Static Route to Office 365.
5. In the IM and Presence Service, assign Expressway-C as a TLS peer. See Add Expressway as TLS Peer.
6. In the IM and Presence Service, add the Expressway-E server to the inbound access control list. See Add Expressway to Access Control List.
7. Restart the Cisco XCP Router on all IM and Presence Service nodes. See Restart Cisco XCP Router.
8. 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. See Exchange Certificates.

Cisco Expressway Configuration

After interdomain federation is configured on the IM and Presence Service, set up Cisco Expressway for 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

Skype for Business Workflow

The IM and Presence Service supports SIP federation with Skype for Business via Expressway in the following integrations:

- Business to Business via Expressway—Federation with a remote Skype for Business server that is located in another company's network.
- Single Enterprise Network—Federation with an on-premise Skype for Business server that is located in the same enterprise network as the IM and Presence Service, but which is in a different domain.

Note Skype for Business can also be hosted by Office 365. For Office 365 deployments, see Office 365 Workflow (Business to Business via Expressway), on page 1.

Following is an overview of the configuration process. For a detailed task flow, see Skype for Business Federation Task Flow.

IM and Presence Service Configuration

1. Turn on Federation Services. See Turn on Federation Services.
2. Configure a DNS SRV record for the IM and Presence domain. See Assign DNS SRV for IM and Presence.
   - In business to business federations, it should be a public DNS SRV that points to Expressway-E.
   - For interdomain federation within a single enterprise, it can be an internal DNS SRV that points to Expressway-C.

Note You can still configure interdomain federation without the DNS SRV record, but you will have to add the route manually on the Skype for Business server.

3. In the IM and Presence Service, add the Skype for Business domain entry. See Add Federated Domain to IM and Presence.
4. In the IM and Presence Service, configure a TLS static route to Expressway. See Configure Static Route on IM and Presence.
5. In the IM and Presence Service, assign Expressway-C as a TLS peer. See Add Expressway as a TLS Peer.
6. In the IM and Presence Service, add the Expressway-C server to the inbound access control list. See Add Expressway to Access Control List.
7. Restart the Cisco XCP Router service on all IM and Presence nodes. See Restart Cisco XCP Router.
8. Exchange certificates between the servers in your deployment. See Exchange Certificates.

Expressway Configuration

Configure Expressway for interdomain federation with Skype for Business. For Expressway configuration details, see the *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.

Additional Configuration Details

Note For a more detailed view of the configuration tasks for Skype for Business, see Skype for Business Federation Task Flow.

Microsoft Lync Workflow (Intracompany via Expressway)

Complete the following tasks to set up interdomain federation between IM and Presence Service and Microsoft Lync via Expressway in an intracompany scenario.

This configuration supports both chat-only and chat+calling deployments.

IM and Presence Service Configuration

1. 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. See Add a Microsoft Lync Domain Within Enterprise.
2. 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. See Configure Static Routes from IM and Presence to Lync.

Note You must configure TLS static routes. TCP is not supported for federation with Microsoft Lync.

3. 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. See Set up Certificates on IM and Presence for Federation with Lync.

Expressway Configuration

For chat+calling deployments only, add an Expressway Gateway. On the gateway, configure Microsoft interoperability and the SIP broker. For Expressway configuration, go to Configure Expressway Gateway for Microsoft Lync Federation.

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

For chat+calling deployments that use Expressway Gateway's SIP Broker, support is limited to intracompany scenarios only. Business to Business is not supported.

Lync Configuration

1. On the Lync server, configure TLS static routes using one of the following procedures:
   a. If you have a chat+calling deployment, Configure a Static Route from Lync to IM and Presence
   b. If you have a chat-only deployment, Configure Static Route from Lync to Expressway Gateway
2. 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. See Configure Trusted Applications on Lync Server.
3. On the Lync server, commit the topology. See Publish Topology.

Microsoft Lync Workflow (Business to Business via Expressway)

Note This deployment is supported for intracompany deployments only. Federation via Expressway Gateway SIP broker is not supported for business to business federation.

Complete the following tasks to set up interdomain federation between IM and Presence Service and Microsoft Lync in a business to business deployment via Expressway's session classification method.

This configuration supports both chat-only and chat+calling deployments.

Note The minimum IM and Presence Service release for this configuration is 11.5(1)SU2.

IM and Presence Service Configuration

1. 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. See Add a Microsoft Lync Domain Within Enterprise.
2. 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. See Configure Static Routes from IM and Presence to Lync.

Note You must configure TLS static routes. TCP is not supported for federation with Microsoft Lync.

3. 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. See Set up Certificates on IM and Presence for Federation with Lync.

Expressway Configuration

Configure Cisco Expressway session classification. Refer to your Cisco Expressway configuration documentation at https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html. For Release X8.9.2, refer to *Cisco Expressway Options with Cisco Meeting Server and/or Microsoft Infrastructure*.

Microsoft Lync Workflow (Business to Business via ASA)

- Configure a federated domain on the IM and Presence Service for Microsoft Lync federation, see Add a SIP Federated Domain.
- Configure the DNS SRV records, see DNS Configuration for SIP Federation.
- Configure the routing on the IM and Presence Service for Microsoft Lync federation, see Routing Configuration on IM and Presence Service
- (Optional) Configure the email address for federation feature, see Turn On Email for Federation
- Configure the TLS security settings on the IM and Presence Service, see Configuration of Security Settings on IM and Presence Service
- Configure the Cisco Adaptive Security Appliance for Microsoft Lync federation, see Cisco Adaptive Security Appliance for SIP Federation Workflow and TLS Proxy Configuration on the Cisco Adaptive Security Appliance.
- Configure certificate exchange for Microsoft Lync federation, see Security Certificate Configuration on Lync Edge Server for TLS Federation.

- Configuration of Lync Server 2010 and Edge servers for interdomain federation differs from that outlined within this guide for OCS. For information on configuring the Lync enterprise for interdomain federation with the IM and Presence Service, see Microsoft documentation.

Microsoft OCS Workflow (Direct Federation)

Complete the following tasks to set up interdomain federation between IM and Presence Service and Microsoft OCS. This configuration is for SIP Federation inside an enterprise, and without an ASA firewall.

IM and Presence Service Configuration

1. 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. See Add a Microsoft OCS Domain Within Enterprise.
2. 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. See Configure Static Route on IM and Presence Service for Microsoft Servers.

Note For OCS, you can choose either TCP or TLS as the protocol type.

Microsoft OCS Configuration

1. 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. See Configure Static Routes on OCS to Point to the IM and Presence Service.
2. 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. See Verify Peer Authentication Listener.
3. 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 node IP address, and one entry with the FQDN. See Adding a Host Authorization Entry for the IM and Presence Service Node on OCS.
4. If you have TLS configured between OCS to IM and Presence Service, configure certificates on OCS for interdomain federation with IM and Presence Service. If you are not using TLS, you can skip this step. See Configure Certificates on OCS for Interdomain Federation.
5. On the OCS server, confirm the listener ports for TLS (The transport can be MTLS or TLS) or TCP are configured. For TLS, use port 5061. For TCP, use port 5060. See Enable Port 5060/5061 on the OCS Server.
6. If you are using TLS, configure OCS to use FIPS. See Configure OCS to use FIPS.
7. If you are using TLS, upload the root certificate for the CA that signs the OCS server certificates to IM and Presence Service. See Set Up Certificates on the IM and Presence Service Node for Federation with Microsoft Server over TLS.

Microsoft OCS Workflow (Business to Business via ASA)

- Configure a federated domain on the IM and Presence Service for Microsoft OCS federation, see Add a SIP Federated Domain.
- Configure the DNS SRV records, see DNS Configuration for SIP Federation.
- Configure the routing on the IM and Presence Service for Microsoft OCS federation, see Routing Configuration on IM and Presence Service.
- (Optional) Configure the email address for federation feature, see Turn On Email for Federation.
- Configure the TLS security settings on the IM and Presence Service, see Configuration of Security Settings on IM and Presence Service.
- Configure the Cisco Adaptive Security Appliance for Microsoft OCS federation, see Cisco Adaptive Security Appliance for SIP Federation Workflow and TLS Proxy Configuration on the Cisco Adaptive Security Appliance.
- Configure certificate exchange for Microsoft OCS federation, see SIP Federation Security Certificate Configuration with Cisco Adaptive Security Appliance.
- Configure the Microsoft OCS server, see External Server Component Configuration for SIP Federation.
- (Optional) Configure a load balancer for redundancy, see Load Balancer Configuration for Redundancy for SIP Federation.
- For troubleshooting information on Microsoft OCS federation, see Troubleshooting a SIP Federation Integration.

Cisco Adaptive Security Appliance for SIP Federation Workflow

- Configure certificates between the Cisco Adaptive Security Appliance and the IM and Presence Service (inside interface), see Security Certificate Exchange Between IM and Presence Service and Cisco Adaptive Security Appliance.
- Configure certificates between the Cisco Adaptive Security Appliance and the federated domain (outside Interface), see Security Certificate Exchange Between Cisco Adaptive Security Appliance and Microsoft Access Edge (External Interface) with Microsoft CA.
- Configure PAT rules for private to public messaging, see Port Address Translation (PAT).
- Configure static PAT for public to private messaging, see Sample Static PAT Commands.
- Configure the required access lists, see Access List Configuration Requirements.
- Configure the TLS proxy instances, see Configure TLS Proxy Instances.
- Associate the access lists with the TLS proxy, see Associate Access List with TLS Proxy Instance Using Class Maps.

Configuration Workflow for SIP Federation with AOL

- Establish an AOL license to enable AOL Federation, see License Requirements for AOL Federation, AOL Routing Information Requirements and AOL Provisioning Information Requirements.
- Configure federated domains on the IM and Presence Service for AOL federation, see Add a SIP Federated Domain.
- Configure DNS SRV records, see DNS Configuration for SIP Federation. If you are not using DNS, see the next step).
- Configure the routing for AOL federation, see Configure Static Routes Using TLS.
- (Optional) Verify and configure the Default Federation Routing Domain for AOL hosted domains.
- (Optional) Configure the email address for federation feature, see Turn On Email for Federation.
- Configure the TLS security settings and certificates on the IM and Presence Service, see Configuration of Security Settings on IM and Presence Service and Security Certificate Exchange Between Cisco Adaptive Security Appliance and the AOL SIP Access Gateway.
- Configure the Cisco Adaptive Security Applicance for AOL, see AOL SIP Access Gateway for information on AOL FQDN, server port, and the public IP address.
- (Optional) Configure a load balancer for redundancy, see Load Balancer Configuration for Redundancy for SIP Federation.

XMPP Federation Workflow

Note Follow this workflow for WebEx, IM and Presence Service and IBM Sametime.

- Configure the IM and Presence Service for XMPP federation, see IM and Presence Service Configuration for XMPP Federation.
- Configure security for XMPP federation, see Security Certificate Configuration for XMPP Federation.
- (Optional) Configure the email address for federation feature, see Turn On Email for Federation.
- Turn on the XMPP Federation service, see Turn On XMPP Federation Service.
- Configure the Cisco Adaptive Security Appliance for XMPP federation, see Configure the Cisco Adaptive Security Appliance for XMPP Federation.
- For troubleshooting information on XMPP federation, see Troubleshooting an XMPP Federation Integration