Configuration Workflows for Partitioned Intradomain Federation

This chapter provides configuration workflows for partitioned intradomain federation with supported Microsoft servers, as well as the workflow for user migration from Skype for Business/Lync/OCS to IM and Presence Service.

Configuration Workflow for Partitioned Intradomain Federation with Skype for Business

Use the following workflow to configure partitioned intradomain federation between IM and Presence Service and Microsoft Skype for Business servers.

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

IM and Presence Service Configuration

1. Verify that the required presence domains are configured on all IM and Presence Service nodes in the cluster. For instructions to view the configured domains on IM and Presence Service and to add new local presence domains, see *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

2. For chat-only deployments with multiple nodes, configure a dedicated routing node, see Configure Routing Node for IM and Presence.

3. Start essential services for cluster nodes, see Start Feature Services for Cluster.

4. Use the Federation wizard to configure federation settings with Skype for Business, including TLS static routes, TLS peers, access control lists, and application listener ports, see Configure Intradomain Federation.

5. Configure CA certificates for IM and Presence Service:

   a. Import root certificate of the Certificate Authority (CA), see Import Root Certificate of Certificate Authority.

   b. Request a CA signed certificate, see Generate Certificate Signing Request for IM and Presence Service.

   c. Import the CA signed certificate, see Import Signed Certificate from CA.

Expressway Gateway Configuration

For chat + calling deployments only. On the Expressway Gateway, configure Microsoft interoperability and enable the SIP broker. For Expressway Gateway configuration details, refer to the **Enable Chat / Presence from Microsoft Clients** section of the *Cisco Expressway with Microsoft Infrastructure Deployment Guide* at:

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/config_guide/X8-11/Cisco-Expressway-Microsoft-Infrastructure-Deployment-Guide-X8-11-1.pdf.

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

Skype for Business Configuration

1. On the Skype for Business servers, set up static routes that point to the IM and Presence Service routing node, see Configure Static Route from Skype for Business.

2. On the Skype for Business server, assign the IM and Presence Service as a trusted application and add the IM and Presence cluster nodes to a trusted servers pool, see Configure Trusted Applications.

3. After you add the IM and Presence Service cluster nodes, publish the Skype for Business topology, see Publish Topology.

4. Exchange certificates between IM and Presence and Skype for Business, see Exchange Certificates.

Configuration Workflow for Partitioned Intradomain Federation with Lync

Use the following workflow to configure partitioned intradomain federation between IM and Presence Service and Microsoft Lync servers.

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

IM and Presence Service Configuration

1. Verify that the required presence domains are configured on all IM and Presence Service nodes in the cluster. For instructions to view the configured domains on IM and Presence Service and to add new local presence domains, see *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

2. For chat-only deployments with multiple nodes, configure a dedicated routing node, see Configure the Routing Node.

3. Start essential services, see Start Feature Services for Cluster.

4. Enable partitioned intradomain federation, see Configure Partitioned Intradomain Federation Options.

5. Configure static routes to Lync deployment, see Configure Static Routes to Microsoft Lync.

6. Configure Access Control Lists for Lync deployment, see Configure an Incoming Access Control List.

7. Configure TLS encryption between the IM and Presence Service and Lync:

    a. Configure application listeners, see Configure Application Listener Ports.
    b. Configure TLS peer subjects, see Configure TLS Peer Subjects.
    c. Configure peer authentication TLS context, see Configure Peer Authentication TLS Context.
    d. Import root certificate of the Certificate Authority (CA), see Import Root Certificate of Certificate Authority.
    e. Request a CA signed certificate, see Generate Certificate Signing Request for IM and Presence Service.
    f. Import the CA signed certificate, see Import Signed Certificate from Certificate Authority.

Note Partitioned intradomain federation only supports back to back federation between IM and Presence Service and Microsoft Lync or OCS. A firewall (ASA) between the federated servers is not supported.

Expressway Gateway Configuration

For chat + calling deployments only. On the Expressway Gateway, configure Microsoft interoperability and enable the SIP broker. For Expressway Gateway configuration details, refer to the *Cisco Expressway with 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.

Lync Configuration

1. Verify that the presence domains for intradomain federation that are configured on the Lync server have matching presence domains configured on the IM and Presence Service nodes. For instructions to view the configured domains on IM and Presence Service and to add new local presence domains, see *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

2. On the Lync servers, configure TLS static routes that point to the Expressway Gateway (for chat+calling) or the IM and Presence Service routing node (for chat-only). For details, see Configure Static Route on Microsoft Lync.

3. Add IM and Presence Service as a trusted application. Add the IM and Presence cluster nodes to a trusted application pool, see Configure Trusted Applications for Lync.

4. Publish the topology, see Publish Topology.

5. Ensure CA root certificates are installed on each Lync server, see Install Certificate Authority Root Certificates on Lync.

6. Ensure all Lync servers have the required signed certificates, see Validate Existing Lync Signed Certificate.

7. Request signed certificate from Certificate Authority, see Request a Signed Certificate from a Certificate Authority for Lync.

8. Download the certificate from the CA server, see Download a Certificate from the CA Server.

9. Import the signed certificate, see Import a Signed Certificate for Lync.

10. Assign the certificate, see Assign Certificate on Lync.

11. Restart services, see Restart Services on Lync Servers.

Tip   Plan the restart of the front-end services during off-peak hours to minimize the impact on users.

After the server is configured, you can proceed to migrate the users.

Configuration Workflow for Partitioned Intradomain Federation with OCS

Use the following workflow to configure partitioned intradomain federation between IM and Presence Service and OCS 2007 R2:

IM and Presence Service Configuration

1. Verify that the required presence domains are configured on all IM and Presence Service nodes in the cluster. For instructions to view the configured presence domains on IM and Presence Service and to add new local presence domains, see *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

2. Select a cluster node to act as the routing node, Configure the Routing Node.

3. Start essential services across the cluster, Start Feature Services for Cluster

4. Enable partitioned intradomain federation, see Configure Partitioned Intradomain Federation Options.

5. Configure static routes to OCS deployment, see Configure Static Routes to Microsoft Lync.

6. Configure Access Control Lists for OCS deployment, see Configure an Incoming Access Control List.

7. (Optional) Configure TLS encryption between IM and Presence Service and OCS:

   a. Configure application listeners, see Configure Application Listener Ports.
   b. Configure TLS peer subjects, see Configure TLS Peer Subjects.
   c. Configure peer authentication TLS context, see Configure Peer Authentication TLS Context.

    d. Import root certificate of the Certificate Authority (CA), see Import Root Certificate of Certificate Authority.

    e. Request a CA signed certificate, see Generate Certificate Signing Request for IM and Presence Service.

    f. Import the CA signed certificate, see Import Signed Certificate from Certificate Authority.

OCS Configuration

1. Verify that the presence domains for intradomain federation that are configured on the OCS server have matching presence domains configured on IM and Presence Service nodes. For instructions to view the configured domains on the IM and Presence Service and to add new local presence domains, see *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

2. Enable port 5060, see Enable Port 5060/5061 on OCS Server.

3. Configure static routes to the IM and Presence Service deployment, see Configure Static Routes on OCS to Point to the IM and Presence Service.

4. Add host authorization for the IM and Presence Service deployment, see Add Host Authorization on OCS for IM and Presence Service.

5. (Optional) Configure TLS encryption between IM and Presence Service and OCS:

    a. Ensure mutual TLS authentication is configured on each OCS server, see Configure Mutual TLS Authentication on OCS.

    b. Ensure CA root certificates are installed on each OCS server, see Install Certificate Authority Root Certificates on OCS.

    c. Ensure all OCS servers have the required signed certificates, see Validate Existing OCS Signed Certificate.

    d. If required, request a newly signed certificate, see Signed Certificate Request from the Certificate Authority for the OCS Server.

6. Restart services, see Restart Services on OCS Front-End Servers.

Tip   Plan the restart of the front-end services during off-peak hours to minimize the impact on users.

After the server is configured, you can proceed to migrate the users.

Configuration Workflow for User Migration from Microsoft Servers to the IM and Presence Service

Use the following workflow to migrate users from Skype for Business/Lync/OCS toIM and Presence Service:

1. Download the user migration tools—see Cisco User Migration Tools.

2. Set unlimited contact list sizes and watcher sizes onIM and Presence Service, see Set Unlimited Contact Lists and Watchers.

3. Enable automatic authorization of subscription requests, see Enable Automatic Authorization of Subscription Requests.

4. Verify the Microsoft server SIP URI format for migrating users, see Verify Microsoft Server SIP URI Format for Migrating Users

5. If applicable, rename contact IDs in the IM and Presence Service contact lists, see Rename Contact IDs in IM and Presence Service Contact Lists

6. Provision migrating users on IM and Presence Service, see Lync/OCS/LCS.

7. Back up Microsoft server data for migrating users, see Lync/OCS/LCS.

8. Export Microsoft server contact lists for migrating users, see Export of Contact Lists for Migrating Users.

9. Disable Microsoft server accounts for migrating users, see Lync/OCS/LCS.

10. Verify that Microsoft server accounts have been disabled for migrating users, see Lync/OCS/LCS.

11. Delete Microsoft server user data for migrating users, see Delete User Data from Database for Migrating Users.

12. Import contact lists into IM and Presence Service for migrating users, see Import Contact Lists for Migrating Users into IM and Presence.

13. Reset the contact list and watcher limits on IM and Presence Service, see Reset Maximum Contact List Size and Maximum Watcher Size.

Configuration Workflow for Integrating IM and Presence with Microsoft Server Interdomain Federation Capability

Note Before you begin this workflow, you must configure partitioned intradomain federation with Skype for Business/Lync/OCS and ensure that it is functioning correctly. See the appropriate workflow for configuring partitioned intradomain federation within your deployment.

1. Configure each federated presence domain on IM and Presence Service—see Remote Domain Setup for Interdomain Federation through Intradomain Federation Connections on Microsoft Servers

2. Configure static routes to each server hosting a remote presence domain on IM and Presence Service—see Configure a Static Route for a Remote Domain