IM and Presence Service Node Configuration for Partitioned Intradomain Federation

- Domain Configuration for Partitioned Intradomain Federation, page 1
- IM and Presence Configuration Task Flow for Federation, page 2

Domain Configuration for Partitioned Intradomain Federation

Before you proceed to set up IM and Presence Service for partitioned intradomain federation, verify that all required presence domains are configured on all nodes in the IM and Presence Service cluster. Ensure that there are matching presence domains configured on the Lync/OCS servers. If necessary, use the **Cisco Unified IM and Presence Administration** user interface to add or update local presence domains on the nodes in the cluster.

Multiple presence domains are supported in the IM and Presence Service cluster when Directory URI is configured as the IM address scheme. All nodes in the cluster must support Directory URI to use Directory URI as the IM address scheme.

For information to set up the Directory URI IM address scheme for the cluster, see *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

For information to set up multiple domains for Interdomain Federation, see *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager Guide*.

View IM Address Domains

All system-managed and administrator-managed presence domains across the IM and Presence Service deployment are displayed in the **Presence > Domains> Find and List Domains** window. A check mark in one of the information fields indicates if a domain is associated with the local cluster and/or with any peer clusters. The following information fields are displayed for administrator-managed presence domains:

- Domain
- Configured on Local Cluster
- Configured on Peer Cluster(s)

The following information fields are displayed for system-managed presence domains:

- Domain
- In use on Local Cluster
- In use on Peer Cluster(s)

Procedure

Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Domains**. The **Find and List Domains** window appears.

IM and Presence Configuration Task Flow for Federation

Before You Begin

Verify that all required presence domains are configured on all nodes in the IM and Presence Service cluster. For details, see Domain Configuration for Partitioned Intradomain Federation, on page 1.

Procedure

	Command or Action	Purpose
Step 1	Configure the Routing Node, on page 3	(Optional) If you have a chat-only deployment with multiple nodes, select a dedicated routing node, and deactivate nonessential services on the routing node. **Note** For chat+calling deployments or single node deployments, you do not need a dedicated routing node and can skip this task.
Step 2	Start Feature Services for Cluster, on page 4	Start essential services on your IM and Presence Service cluster nodes.
Step 3	Configure Partitioned Intradomain Federation Options, on page 5	Enable partitioned intradomain federation and routing options on IM and Presence Service.
Step 4	Configure Static Routes to Microsoft Lync, on page 6	Configure static routes to Lync/OCS deployment, **Note** For Lync, create TLS static routes. For OCS, you can create TLS or TCP routes.
Step 5	Configure an Incoming Access Control List, on page 7	Configure an incoming access control list on IM and Presence so that Lync/OCS servers can access IM and Presence without authentication.
Step 6	Configure Application Listener Ports, on page 9	On the IM and Presence Service, change the Default Cisco SIP Proxy TLS Listener port values for both server authentication and peer authentication.
Step 7	Configure TLS Peer Subjects, on page 10	Configure TLS peer subjects for the Lync/OCS servers and the Expressway Gateway (chat + calling scenarios).

	Command or Action	Purpose
Step 8	Configure Peer Authentication TLS Context, on page 12	Configure peer authentication.
Step 9	Import Root Certificate of Certificate Authority, on page 13	Upload the root certificate of the CA into the IM and Presence Service trust store.
Step 10	Generate Certificate Signing Request for IM and Presence Service, on page 13	Request a CA signed certificate
Step 11	Import Signed Certificate from Certificate Authority, on page 14	Generate and download a CSR from IM and Presence Service.
Step 12	Configure Expressway Gateway, on page 15	(Optional) For chat + calling Federation with Lync, deploy the Expressway Gateway. **Note** There is no need to deploy an Expressway Gateway in chat-only deployments, or when configuring Federation with OCS.

Configure the Routing Node

For multi-node chat-only deployments, choose an IM and Presence Service cluster node to act as the routing node. To provide extra capacity for routing, there should be no users assigned to the routing node. The routing node acts as a front-end server, accepting inbound SIP requests from Lync/OCS and routing those requests to the appropriate cluster node that homes the recipient.

Note For chat+calling deployments with Lync, and for single-node deployments, you can skip this procedure as there is no need to configure a routing node.

Procedure

Step 1 From the Cisco Unified IM and Presence Serviceability user interface, choose **Tools** > **Service Activation**.

Step 2 From the **Server** drop-down menu, choose the cluster node that you want to designate as the routing node. The routing node should have no users assigned.

Step 3 Check the **Cisco SIP Proxy** feature service.

Step 4 Uncheck the following feature services:

- Cisco Presence Engine
- Cisco XCP Text Conference Manager
- Cisco XCP Web Connection Manager
- Cisco XCP Connection Manager
- Cisco XCP SIP Federation Connection Manager

- Cisco XCP XMPP Federation Connection Manager
- Cisco XCP Message Archiver
- Cisco XCP Directory Service
- Cisco XCP Authentication Service

Step 5 Click **Save**.

Step 6 Confirm that the **CIsco XCP Router** network service is running. Because the service is a network service it is running by default, unless you previously disabled it.

a) Choose **Tools** > **Control Center – Network Services**.
b) From the **Server** drop-down menu, select the routing node and click **Go**.
c) If the **CIsco XCP Router** service is not running, check the corresponding radio button, and click **Start**.

What to Do Next

Start Feature Services for Cluster, on page 4

Start Feature Services for Cluster

Start essential feature services for your IM and Presence Service cluster nodes. If you have a multi-node chat-only deployment, complete this task for all nodes except the routing node. Otherwise, complete this task for all cluster nodes.

Procedure

Step 1 From the Cisco Unified IM and Presence Serviceability interface, choose **Tools** > **Service Activation**.

Step 2 From the **Server** menu, choose the cluster node and click **Go**.

Step 3 Check the following services:

- **Cisco SIP Proxy**
- **Cisco XCP SIP Federation Connection Manager**

Step 4 Click **Save**.

Step 5 Confirm that the **CIsco XCP Router** network service is running. Because the service is a network service it is running by default, unless you previously disabled it.

a) Choose **Tools** > **Control Center – Network Services**.
b) From the **Server** drop-down menu, select the routing node and click **Go**.
c) If the **CIsco XCP Router** service is not running, check the corresponding radio button, and click **Start**.

Step 6 Repeat this procedure for all cluster nodes, except the routing node.

What to Do Next

Configure Partitioned Intradomain Federation Options, on page 5

Configure Partitioned Intradomain Federation Options

The following procedure describes how to enable partitioned intradomain federation on IM and Presence Service and choose a routing mode.

If you have a multicluster deployment, you must perform this procedure on each cluster. When you enable partitioned intradomain federation or choose a routing mode, these settings are enabled cluster-wide; therefore you only need to enable them on the IM and Presence Service publisher node within any given cluster.

Caution Email Address for Federation is not supported in deployments where Partitioned Intradomain Federation is configured. Email Address for Federation is also not supported for Interdomain Federation if your deployment uses the interdomain federation capabilities of Lync/OCS. Confirm that Email Address for Federation is not enabled anywhere in the deployment in these deployment scenarios and ensure that the **Enable use of Email Address when Federating** option is not checked for the clusters.

Procedure

Step 1 Log in to the **Cisco Unified Communications Manager IM and Presence Administration** user interface. Choose **Presence** > **Settings> Standard Configuration**.

Step 2 Check the **Enable Partitioned Intradomain Federation with LCS/OCS/Lync** check box.

Step 3 Read the warning message and click **OK**.

Step 4 Choose one of the following from the partitioned intradomain federation Routing Mode drop-down list:

- **Basic Routing Mode (default)** when you have unlicensed IM and Presence Service request recipients within the IM and Presence Service domain. In Basic Routing mode, the IM and Presence Service routes requests for these recipients to the Microsoft server.
- **Advanced Routing Mode** when you have request recipients within the IM and Presence Service domain who are licensed and have a valid Microsoft Lync or Microsoft Office Communicator SIP address stored in the IM and Presence Service database. Choose Advanced Routing only if Cisco Unified Communications Manager synchronizes users from the same Active Directory that the Microsoft server uses.

  Note The list of users synchronized from Active Directory must include all Microsoft Lync or Microsoft Office Communicator users.

Step 5 Click **Save**.

Step 6 After you enable partitioned intradomain federation or choose a routing mode, you must restart the Cisco XCP Router on all IM and Presence Service nodes in the cluster. To restart the Cisco XCP Router, log in to the **Cisco Unified IM and Presence Serviceability** user interface and choose **Tools** > **Control Center – Network Services**. Click the appropriate IM and Presence Service node, scroll down and select Cisco XCP Router, and click restart.

Note You are prompted to restart the SIP proxy when you enable partitioned federation.

What to Do Next

Configure Static Routes to Microsoft Lync, on page 6

Related Topics

IM and Presence to Microsoft Server Request Routing

Configure Static Routes to Microsoft Lync

The following procedure describes how to configure static routes to enable partitioned intradomain federation routing between the IM and Presence Service and Lync/OCS. You must add an individual static route for each Microsoft server presence domain. Static routes can have a common next hop address. See topics related to IM and Presence Service to Microsoft server request routing, and basic and advanced routing modes for more information.

Note If you are integrating partitioned intradomain federation with the interdomain federation capabilities of Microsoft servers, then you must configure static routes on the IM and Presence Service for each remote domain. For more information, see topics related to configuring static routes for remote domains.

Note Perform this procedure for each Microsoft server presence domain.

For the Microsoft server presence domain static route, note the following:

- For Standard Edition Microsoft servers, the static route must point to the IP address of a specific Standard Edition server.
- For Enterprise Edition Microsoft servers, to route federation traffic from the IM and Presence Service cluster directly to one of the front-end Microsoft servers, the static route must point to the IP address of that front-end server

See the following URL for a list of approved load balancers: http://technet.microsoft.com/en-us/office/ocs/cc843611. It is your responsibility to ensure that those load balancers are deployed and managed correctly.

Note Cisco does not support the configuration of static routes to point to load balancers. Cisco recommends that you configure static routes to bypass the front-end load balancer.

For high availability purposes, you can configure additional backup static routes for each Microsoft server presence domain.

The backup route has a lower priority and is used only if the next hop address of the primary static route is unreachable.

Note If you have a multicluster deployment, you must perform this procedure on each cluster. These settings are cluster-wide; therefore you need to set them only on the IM and Presence Service database publisher node within any given cluster.

Procedure

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 is reversed. For example, if the domain is `domaina.com`, the Destination Pattern value must be `.com.domaina`

Step 4 In the **Next Hop** field, enter the IP address of the Microsoft server.

Step 5 Choose **domain** for the Route Type.

Note The default setting for Route Type is user.

Step 6 Set the **Next Hop Port** and **Protocol Type** values according to the protocol that you want to use:

- For TCP——Choose **TCP** as the **Protocol Type** and **5060** as the **Next Hop Port**.
- For TLS—Choose **TLS** as the **Protocol Type** and **5061** as the **Next Hop Port**.

Note For static routes to Lync, you must configure TLS routes. For static routes to OCS, you can configure TLS or TCP.

Step 7 Enter the Priority value as follows:

- For primary static routes, enter the default Priority value of **1**.
- For backup static routes, enter a Priority value of greater than 1. (The lower the value, the higher the priority of the static route).

Step 8 Leave the default values for all other parameters.

Step 9 Click **Save**.

Step 10 Create an additional static route with the Destination Pattern FQDN in reverse order and with the Next Hop the Microsoft Lync server IP address. For example, if the domain is lyncserver.domaina.com, the Destination Pattern value must be .com.domaina.lyncserver.

What to Do Next

Configure an Incoming Access Control List, on page 7

Configure an Incoming Access Control List

The following procedure describes how to configure entries in the Incoming Access Control List (ACL) to ensure that Lync/OCS servers can access the IM and Presence Service server without authentication.

Note If you have a multicluster deployment, you must perform this procedure on each cluster. These settings are cluster-wide; therefore you need to set them only on the IM and Presence Service publisher node within any given cluster.

How you configure the Incoming ACLs depends on how strictly you wish to control access to IM and Presence Service:

- To allow open access to IM and Presence Service, you can add an entry with an address pattern of **All**.
- To allow access to IM and Presence Service from specific DNS domains, you can add entries with an address pattern matching the specific DNS domain. For example, to allow access from any server within the foo.com DNS domain, enter **foo.com** as the address pattern.
- To allow access to IM and Presence Service from specific servers, add ACL entries that have an address pattern matching the IP address and the FQDN of those servers. You must create two ACL entries for each server: one entry for the IP address and another entry for the FQDN. For example, to allow access from the server ocs1.foo.com (10.1.10.100) enter **ocs1.foo.com** as the address pattern in one ACL entry, and enter **10.1.10.100** as the address pattern in another ACL entry.

For partitioned intradomain federation, if you decide to restrict access to IM and Presence Service for certain Microsoft server FQDNs or IP addresses only, you must add ACL entries for the following entities:

- Each Microsoft server Enterprise Edition front-end or Standard Edition server
- Each Microsoft server pool FQDN (Enterprise Edition only)
- Gateway Expressway FQDN (chat + calling scenarios only)

If you choose to restrict access using the FQDN of the server, then you need to also add an ACL entry for any other DNS records that resolve to the same IP address as any of the front end servers or pools. For example, you can create a DNS record, such as admin.lync.com, on the Lync server to access the Lync control panel and which resolves to the same IP address as one of the Lync front end servers.

Caution If you choose to enter a specific server FQDN or IP address for your ACL entries, failure to create all the required ACL entries as described may cause stability issues with the Lync 2013 client.

Procedure

Step 1 Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **System** > **Security** > **Incoming ACL**.

Step 2 Click **Add New**.

Step 3 In the **Description** field, enter a description of the entry. For example, Lync Server.

Step 4 Enter the address pattern in the **Address Pattern** field. You have the following options:

- Enter **Allow from all** to allow open access to IM and Presence Service.
- Enter a specific network domain name. For example, **Allow from foo.com**.
- Enter a specific IP address. For example, **Allow from 10.1.10.100**.
- Enter a specific FQDN. For example, **Allow from admin.lync.com**.

Note If you do not enter **Allow from All** as the address pattern, then you must create at least two ACL entries: one for the IP address of the server and another one for the FQDN of the server. Entering a domain name is optional.

Step 5 Click **Save**.

Step 6 Restart the SIP Proxy by doing the following:

a) Choose **Presence** > **Routing** > **Settings**

b) Click the **Restart All Proxy Services** button.

What to Do Next

Configure Application Listener Ports, on page 9

TLS Encryption Configuration

You must complete the procedures in this section to configure TLS encryption between IM and Presence Service and Lync/OCS. TLS encryption is mandatory for partitioned intradomain federation with Lync servers.

Note If you have a multicluster deployment, you must perform each of these procedures on each cluster. These settings are cluster-wide; therefore you need to set them only on the IM and Presence Service publisher node within any given cluster.

Configure Application Listener Ports

You must change the Default Cisco SIP Proxy TLS Listener port values for both server authentication and peer authentication.IM and Presence Service performs peer (mutual) TLS authentication on port 5062 by default. You must modify this default setting so that peer TLS authentication takes place on port 5061 and configure the server TLS authentication port value to 5062.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Administration** user interface. Choose **System** > **Application Listeners**.

Step 2 If they are not already displayed, click **Find** to display all application listeners.

Step 3 Choose **Default Cisco SIP Proxy TLS Listener – Server Auth**.

Step 4 Change the Port value to **5063**.

Step 5 Click **Save** and click **OK** on the pop-up window that appears.

Step 6 From the Related Links drop-down list, choose **Back to Find/List** and click **OK** to return to the Application Listeners list.

Step 7 Choose **Default Cisco SIP Proxy TLS Listener – Peer Auth**.

Step 8 Change the Port value to **5061**.

Step 9 Click **Save** and click **OK** on the dialog-box that appears.

Step 10 From the Related Links drop-down list, choose **Back to Find/List** and click **OK** to return to the Application Listeners list.

Step 11 Choose **Default Cisco SIP Proxy TLS Listener – Server Auth**.

Step 12 Change the Port value from **5063** to **5062**.

Step 13 Click **Save**.

Step 14 Restart the SIP Proxy service on all IM and Presence Service nodes in the cluster. To restart the SIP Proxy service, Log in to the **Cisco Unified IM and Presence Serviceability** user interface, choose **Tools** > **Control Center – Feature Services**.

What to Do Next

Configure TLS Peer Subjects, on page 10

Related Topics

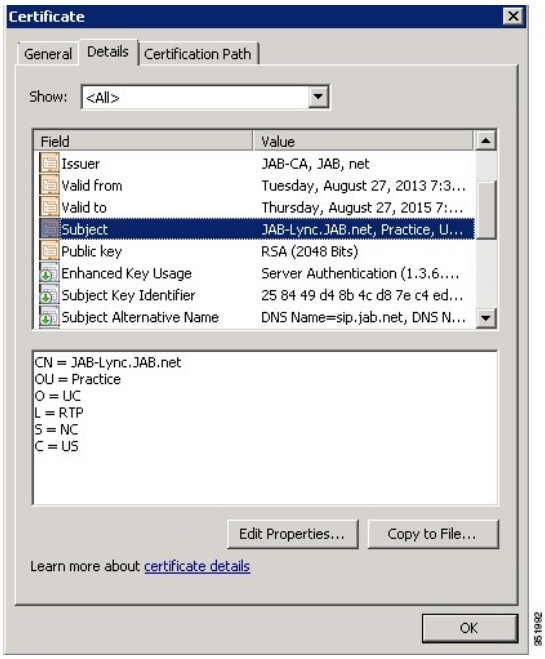
Integration Troubleshooting

Configure TLS Peer Subjects

For Peer TLS authentication, IM and Presence Service requires that the Subject Common Name (CN) from the security certificate that is presented by the peer is included in a TLS Peer Subject list. Use the **Cisco Unified IM and Presence Administration** user interface to add a Subject CN to this list.

Include only the Subject CN in the TLS Peer Subject list. Do not include Subject Alternative Name (SAN) entries in the TLS Peer Subject list. The following figure shows an example of a Subject CN certificate with the Subject CN highlighted.

Figure 1: Subject Common Name Certificate



For partitioned intradomain federation, add a TLS Peer Subject for whichever of the following entities you are deploying:

- Each Lync/OCS Enterprise Edition front-end or Standard Edition server
- Each Lync/OCS pool Fully Qualified Domain Name (FQDN) (Enterprise Edition only)
- Expressway Gateway FQDN (for chat + calling scenarios only)

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Administration** user interface. Choose **System** > **Security** > **TLS Peer Subjects**.

Step 2 Click **Add New**.

Step 3 Enter the Peer Subject Name.

- For a Microsoft server Enterprise Edition front-end or Standard Edition server, enter the FQDN of the server.
- For a Microsoft server pool Fully Qualified Domain Name (FQDN), enter the subject CN of the certificate that is presented to the IM and Presence Service.
- Enter the FQDN of the Expressway Gateway (for chat + calling scenarios only)

Step 4 In the **Description** field, enter a description of the subject, for example, OCS Server.

Step 5 Click **Save**.

Step 6 Restart the Cisco SIP Proxy service on all IM and Presence Service nodes in the cluster. To restart the Cisco SIP Proxy service, log in to the **Cisco Unified IM and Presence Serviceability** user interface and choose **Tools** > **Control Center - Feature Services**. Click the CUCM IM and Presence Server, select **SIP Proxy** and click **Restart**.

What to Do Next

Configure Peer Authentication TLS Context, on page 12

Related Topics

Integration Troubleshooting

Configure Peer Authentication TLS Context

To support TLS encryption between IM and Presence Service and Lync/OCS, you must modify Peer Authentication TLS Context configuration on IM and Presence Service.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Administration** user interface. Choose **System** > **Security** > **TLS Context Configuration**.

Step 2 Click **Find**.

Step 3 Click the link for **Default Cisco UP SIP Proxy Peer Auth TLS Context**.

Step 4 Ensure that the check box for **Disable Empty TLS Fragments** is checked.

Step 5 In the TLS Cipher Mapping area list of Available TLS Ciphers, choose all of the ciphers and click the **Move Right** arrow to move these ciphers to the Selected TLS Ciphers list.

Step 6 In the TLS peer Subject Mapping area list of Available TLS Peer Subjects, choose the TLS peer subject that you configured in Configure TLS Peer Subjects, on page 10 and click the **Move Right** arrow to move this TLS peer subject to the Selected TLS Peer Subjects list.

Step 7 Click **Save**.

Step 8 Restart the Cisco SIP Proxy service on all IM and Presence Service nodes in the cluster. To restart the Cisco SIP Proxy service, log in to the **Cisco Unified IM and Presence Serviceability** user interface and choose **Tools** > **Control Center – Feature Services**. Click the CUCM IM and Presence Service server, select **Cisco SIP Proxy** and click **Restart**.

What to Do Next

Import Root Certificate of Certificate Authority, on page 13

Related Topics

Integration Troubleshooting

Import Root Certificate of Certificate Authority

All Lync/OCS security certificates are generally signed by a Certificate Authority (CA). The IM and Presence Service certificates should also be signed by the same Certificate Authority used by the Microsoft server. In order for the IM and Presence Service to use a certificate signed by the Microsoft server CA, and to accept Microsoft server certificates signed by that same CA, the root certificate of the CA must be uploaded into the IM and Presence Service trust store.

Before You Begin

Before importing the root certificate, retrieve the certificate from the certificate authority and copy it to your local computer.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence OS Administration** user interface. Choose **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate/ Certificate Chain**.

Step 3 For the Certificate Purpose drop-down list, choose **cup-trust**.

Step 4 In the Description (friendly name) field, enter a description for the certificate, for example, Certificate Authority Root Certificate.

Step 5 Click **Browse** to find the root certificate on your local computer.

Step 6 Click **Upload** to upload the certificate to the IM and Presence Service node.

Step 7 Restart the Cisco SIP Proxy service on all IM and Presence Service nodes in the cluster. To restart the Cisco SIP Proxy service, log in to the Cisco Unified IM and Presence Serviceability user interface and choose **Tools** > **Control Center – Feature Services**. Click the CUCM IM and Presence Service server, select **Cisco SIP Proxy** and click **Restart**.

What to Do Next

Generate Certificate Signing Request for IM and Presence Service, on page 13

Related Topics

Integration Troubleshooting

Generate Certificate Signing Request for IM and Presence Service

IM and Presence Service certificates should be signed by the same Certificate Authority (CA) that is used by Lync/OCS. You must complete the following two-step process to obtain a CA-signed certificate:

1 Generate an IM and Presence Service Certificate Signing Request (CSR).

2 Upload the CA signed certificate onto IM and Presence Service.

The following procedure describes how to generate and download a CSR from IM and Presence Service. IM and Presence Service CSRs are 2048 bit in size.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Administration** user interface. Choose **Security** > **Certificate Management** on IM and Presence Service.

Step 2 Click **Generate CSR**.

Step 3 From the Certificate Purpose drop-down list, choose **cup**.

Step 4 Click **Generate CSR**.

Step 5 When the Status shows "Success: Certificate Signing Request Generated" click **Close**.

Step 6 Click **Download CSR**.

Step 7 From the Certificate Name drop-down list, choose **cup**.

Step 8 Click **Download CSR** to download the certificate to your local computer.

Step 9 After the certificate has downloaded, click **Close**.

What to Do Next

After you download the CSR, you can use it to request a signed certificate from your chosen CA. This can be a well-known public CA or an internal CA.

Import Signed Certificate from Certificate Authority, on page 14

Related Topics

Integration Troubleshooting

Import Signed Certificate from Certificate Authority

The following procedure describes how to upload the CA signed certificate to IM and Presence Service.

Before You Begin

Generate and download a CSR from IM and Presence Service. See Generate Certificate Signing Request for IM and Presence Service, on page 13.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Administration** user interface. Choose **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate/Certificate chain** and the Upload Certificate/Certificate chain dialog box opens.

Step 3 From the Certificate Name drop-down list, choose **cup**.

Step 4 In the Description (friendly name) field, enter a description of the certificate, for example, CA Signed Certificate.

Step 5 Click **Browse** to find the certificate file on your local computer.

Step 6 Click **Upload** to upload the certificate to the IM and Presence Service node.

Step 7 After the certificate has uploaded, restart the Cisco SIP Proxy service on all IM and Presence nodes in the cluster. To restart the Cisco SIP Proxy service, log in to the **Cisco Unified IM and Presence Serviceability**

user interface. Choose **Tools** > **Control Center – Feature Services**. Click the Cisco Unified IM and Presence Service server, select **Cisco SIP Proxy** and click **Restart**.

What to Do Next

For chat+calling Federation with Lync, Configure Expressway Gateway, on page 15

Otherwise, for chat-only, go to one of the following chapters:

- Microsoft Lync Configuration for Partitioned Intradomain Federation
- Microsoft Office Communications Server Configuration for Partitioned Intradomain Federation

Related Topics

Integration Troubleshooting

Configure Expressway Gateway

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

Microsoft Lync Configuration for Partitioned Intradomain Federation