Skype for Business Configuration for Partitioned Intradomain Federation

Skype for Business Intradomain Federation

To configure Microsoft Skype for Business for partitioned Intradomain federation, you must complete the following procedures in the order they are presented.

Skype for Business Intradomain Federation Task Flow

Complete these tasks to set up intradomain federation with Skype for Business.

Procedure

	Command or Action	Purpose
Step 1	Configure Routing Node for IM and Presence, on page 2	Select an IM and Presence node to act as the routing node. The routing node routes traffic to and from Skype for Business. There should be no users assigned to the routing node.
Step 2	Start Feature Services for Cluster, on page 3	Start essential feature services for your IM and Presence Service cluster nodes. Complete this task on all nodes except the routing node.
Step 3	Configure Intradomain Federation, on page 3	Use the Federation wizard to configure partitioned intradomain federation with Skype for Business. The wizard configures items such as TLS static routes, TLS peers, access control lists, and application listener ports.
Step 4	Configure CA Certificates for IM and Presence, on page 4	Complete these tasks to set up CA certificates for IM and Presence Service.

	Command or Action	Purpose
Step 5	Configure Static Route from Skype for Business, on page 7	On the Skype for Business servers, set up static routes that point to the IM and Presence Service routing node.
Step 6	Configure Trusted Applications, on page 8	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.
Step 7	Publish Topology, on page 9	After you add the IM and Presence Service cluster nodes, publish the Skype for Business topology.
Step 8	Exchange Certificates, on page 10	Exchange certificates between IM and Presence and Skype for Business.

Configure Routing Node for IM and Presence

For multi-node IM and Presence Service deployments, select an IM and Presence routing node. There should be no users assigned to the routing node. The routing node routes traffic to and from the Skype for Business server.

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 3

Start Feature Services for Cluster

Start essential feature services for your IM and Presence Service cluster nodes. Complete this task for all nodes except the routing node.

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 Intradomain Federation, on page 3

Configure Intradomain Federation

Use the wizard to set up partitioned intradomain federation with Skype for Business.

Before you begin

Make sure that you know your Skype for Business deployment details.

Procedure

Step 1 From Cisco Unified CM IM and Presence Administration, choose **Presence** > **Intradomain Federation Setup**.
The wizard launches.

Step 2 Select **Skype for Business** and click **Next**.

Step 3 Enter the following details for your Skype for Business deployment:

- Skype for Business Version—Enterprise Edition or Standard Edition
- Pool FQDN—If Skype for Business is using a pool of front-end servers for load balancing, enter the pool FQDN.
- Load Balancer—Select Yes or No to indicate if you are using a load balancer.
- Load Balancer IP Address—The IP address of the load balancer.
- Register ID—The FQDN of the Skype for Business registration server. You can use the **Get-CsPool** command in Skype for Business to get this value.
- Site ID—The Site ID FQDN. You can use the **Get-CsSite** command in Skype for Business to get this value.

Step 4 Click **Next**.

Step 5 Enter the Skype for Business front end server FQDN and IP address. Click **Add** if you need to enter additional servers.

Step 6 Click **Next**.

Step 7 Enter your **Presence Domains** and click **Next**.

Step 8 Review your configuration.

Step 9 Click **Next**.

Step 10 When you are done, click **Finish**.

The wizard sets up intradomain federation with TLS static routes, application listener ports, and access control lists.

What to do next

After setting up partitioned intradomain federation, the wizard provides general instructions on additional configuration tasks, such as configuring certificates on IM and Presence Service and setting up static routes on the Skype for Business server. For detailed procedures, see:

- To configure CA certificates on IM and Presence Service, go to Configure CA Certificates for IM and Presence, on page 4
- To proceed with the Skype for Business setup, go to Configure Static Route from Skype for Business, on page 7

Configure CA Certificates for IM and Presence

Complete these tasks to set up CA certificates for the IM and Presence Service.

Procedure

	Command or Action	Purpose
Step 1	Import Root Certificate of Certificate Authority	Upload the root certificate of the CA into the IM and Presence Service trust store.
Step 2	Generate Certificate Signing Request for IM and Presence Service	Request a CA-signed certificate.
Step 3	Import Signed Certificate from CA, on page 6	Generate and download a CSR from IM and Presence Service.

Import Root Certificate of Certificate Authority

All Skype for Business 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

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 Skype for Business. 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. For details, see Import Signed Certificate from CA, on page 6.

Import Signed Certificate from CA

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

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

Configure Static Route from Skype for Business, on page 7

Configure Static Route from Skype for Business

On the Skype for Business server, configure TLS static routes that point to the IM and Presence Service routing node.

Procedure

Step 1 Log in to the Skype for Business command shell interface.

Step 2 Enter the following command to define a TLS route:

```
$tlsRoute = New-CsStaticRoute -TLSRoute -Destination fqdn_of_imp_routing_node -Port
listening_port_imp_routing_node -usedefaultcertificate $true -MatchUri domain_imp
```

where:

Parameter	Description
-Destination	The fully qualified domain name of the IM and Presence Service routing node. For example, `impNode.example.com`.
-Port	The listening port of the IM and Presence Service routing node (default port is 5061).
-MatchUri	The domain for the lM and Presence Service. For example, `example.com`.

Note
- To match child domains of a domain, you can specify a wildcard value in the **`-MatchUri`** parameter, for example, *.sip.com. That value matches any domain that ends with the suffix sip.com.
- If you are using IPv6, the * wildcard option is not supported in the **`-MatchUri`** parameter.

Step 3 Make the newly created static route persistent in the Central Management store. Enter the following command:

```
Set-CsStaticRoutingConfiguration -Route @{Add=$tlsRoute}
```

Note Perform this step only for the IM and Presence Service routing node.

Step 4 If you made the new static route persistent, verify that the command was successful. Enter the following command:

```
Get-CsStaticRoutingConfiguration | select-object -ExpandProperty Route
```

What to do next

Configure Trusted Applications, on page 8

Configure Trusted Applications

On the Skype for Business server, assign the IM and Presence Service as a trusted application and add all IM and Presence cluster nodes to a trusted server pool.

Procedure

Step 1 Log in to the Skype for Business command shell.

Step 2 Run the following command to create a trusted application server pool on the Skype for Business server:

Tip You can enter **Get-CsPool** to verify the FQDN value of the Registrar service for the pool

```
New-CsTrustedApplicationPool -Identity trusted_application_pool_name_in FQDN_format -Registrar
S4B_registrar_service_FQDN -Site ID_for_the_trusted_application_pool_site
-TreatAsAuthenticated $true -ThrottleAsServer $true -RequiresReplication $false -OutboundOnly
$false -Computerfqdn first_trusted_application_computer
```

where:

Parameter	Description
-Identity	Enter the name of the trusted application pool for the IM and Presence Service deployment. This must be in FQDN format. For example: `trustedpool.sip.com`. **Tip** Ignore warning messages regarding the machine not found in Active Directory and proceed to apply the changes.
-Registrar	The service ID or FQDN of the Registrar service for the pool. For example: `s4b.synergy.com`. You can check this value using the command **Get-CsPool**.
-Site	The numeric value of the site where you want to create the trusted application pool. **Tip** Use the **Get-CsSite** Management Shell command.
-Computerfqdn	The FQDN of the IM and Presence Service routing node. For example: `impserverPub.sip.com`. • impserverPub = the IM and Presence Service hostname. • sip.com = the IM and Presence Service domain.

Step 3 Run the following command to add your IM and Presence Service cluster nodes to the trusted application pool. You must run this command for each IM and Presence node, except the routing node.

```
New-CsTrustedApplicationComputer -Identity imp_FQDN -Pool new_trusted_app_pool_FQDN
```

where:

Parameter	Description
-Identity	The FQDN of the IM and Presence Service node. For example: `impserver2.sip.com`. **Note** Do not add the IM and Presence Service routing node as a trusted application computer using this command.
-Pool	The FQDN of the trusted application pool that is used for the IM and Presence Service deployment. For example: `trustedpool.sip.com`.

Step 4 Enter the following command to create a new trusted application for the IM and Presence Service and add it to the new application pool:

`New-CsTrustedApplication -ApplicationID` *`new_application_name`* **`-TrustedApplicationPoolFqdn`** *`new_trusted_app_pool_FQDN`* **`-Port 5061`**

where:

Parameter	Description
-ApplicationID	The name of the application. This can be any value. For example: `imptrustedapp.sip.com`.
-TrustedApplicationPoolFqdn	The FQDN of the trusted application pool server for the IM and Presence Service deployment. For example: `trustedpool.sip.com`.
-Port	The SIP listening port of the IM and Presence Service node. For TLS the port is 5061.

What to do next

Publish Topology, on page 9

Publish Topology

Procedure

Step 1 Log in to the Skype for Business PowerShell.

Step 2 Run the following command: **Enable-CsTopology**.

What to do next

Exchange Certificates, on page 10

Exchange Certificates

To deploy Intradomain Federation, you must follow this process to exchange CA-signed certificates between the IM and Presence Service deployment and the Skype for Business deployment.

Procedure

Step 1 Download CA-signed certificates from IM and Presence Service.

Step 2 Download CA-signed certificates from the Skype for Business edge server.

Step 3 Upload Skype for Business certificates to the IM and Presence Service.

Step 4 Upload IM and Presence certificates to the Skype for Business edge server.

Certificate Notes

- For IM and Presence Service, you can download and upload certificates from the **Certificate Management** window of 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 Skype for Business certificates, you can use the Skype for Business Deployment Wizard to install or download certificates. Run the wizard and select the **Request, Install or Assign Certificates** option. For details, see your Microsoft Skype for Business documentation.