Microsoft Office Communications Server Configuration for Partitioned Intradomain Federation

Microsoft Office Communications server configuration for partitioned intradomain federation applies only to Microsoft Office Communications Server (OCS) 2007 R2.

Domain Verification for OCS Servers

Before you proceed to set up IM and Presence Service for partitioned intradomain federation, verify that there are matching domains configured on the Microsoft OCS servers and all nodes in the IM and Presence Service cluster.

Use the **Cisco Unified CM IM and Presence Administration** user interface to verify local domains that are configured on the IM and Presence Service, as well as the system-managed domains that are configured on external servers.

Enable Port 5060/5061 on OCS Server

To use unencrypted TCP connections for SIP traffic between IM and Presence Service and OCS, configure the OCS server to listen on TCP SIP port 5060. For federated TLS connections, configure the OCS server to listen on TLS port 5061.

Note

- For Standard Edition, you must complete this procedure on all Standard Edition servers.
- For Enterprise Edition, you must complete this procedure on all front-end servers.

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Office Communications Server 2007 R2**.

Step 2 Right-click the FQDN of the Standard Edition or Enterprise Edition front-end server and choose **Properties** > **Front End Properties**.

Step 3 Click the **General** tab.

Step 4 If port 5060 or 5061 is not listed under Connections, click **Add**.

Step 5 Choose **All** as the IP Address Value.

Step 6 Enter the Transport and Port values.

- For TCP, enter **TCP** as the Transport Value and **5060** as the Port Value.
- For TLS, enter **TLS** as the Transport Value and **5061** as the Port Value.

Step 7 Click **OK** to close the **Add Connection** window. The port value should now be listed under the Connections list.

Step 8 Click **OK** again to close the **Front End Server Properties** window.

What to Do Next

Configure static routes on the OCS server to point to the IM and Presence Service.

Related Topics

Integration Troubleshooting

Federated Link to Microsoft OCS Server Configuration Task List

The following table provides an overview of the steps to configure federated links between IM and Presence Service and Microsoft OCS servers.

If you are using direct federation from IM and Presence Service to OCS without the Access Edge server or Cisco Adaptive Security Appliance, you must configure a TLS or TCP static route for each domain on the OCS server. These static routes are to point to an IM and Presence Service node. The Cisco Adaptive Security Appliance or the Microsoft Access Edge are not required.

- For Standard Edition, you must you must configure static routes on all Standard Edition servers.
- For Enterprise Edition, you must you must configure static routes on all pools.

Table 1: Task List for End-to-End Configuration of Federated Links to Microsoft OCS Server

Step	Description
Configure a static route on IM and Presence Service	TLS or TCP is supported. For TLS, select TLS as the Protocol Type and 5061 as the Next Hop Port number. For TCP, select TCP as the Protocol Type and 5060 as the Next Hop Port number.
Configure a static route on OCS for IM and Presence Service	TLS or TCP is supported. For TLS, the static route port should be 5061 For TCP, the static route port should be 5060. **Important** When using TLS with static routes on OCS, you must specify the FQDN of the IM and Presence Service node, rather than an IP address. Verify the Peer Auth Listener port is configured as 5061 and change Server Auth Listener port. Log in to **Cisco Unified CM IM and Presence Administration**, choose **System** > **Application Listeners**. • Verify that the Peer Auth Listener port is 5061. • If the Server Auth Listener port is configured as 5061, you must change it to another value, for example 5063.
Configure a host authorization entry for the IM and Presence Service	This procedure applies to TLS and TCP. For TLS, you must add two host authorization entries for each IM and Presence Service node, one entry using the IP address of the IM and Presence Service node, and the second entry using the IM and Presence Service FQDN. For TCP, only one host authorization entry using the IM and Presence Service IP address needs to be added for each IM and Presence Service node.
Configure the certificates on OCS	This procedure is only for TLS. To retrieve the CA root certificate and the OCS signed certificate, perform the following steps: • Download and install the CA certificate chain. • Request a certificate from the CA server • Download the certificate from the CA server In the OCS Front End Server Properties, ensure the TLS listener for port 5061 on OCS is configured. (The transport can be MTLS or TLS). From the OCS Front End Server Properties, choose the Certificates tab, and click **Select Certificate** to choose the OCS signed certificate.

Step	Description
Configure OCS to use FIPS (TLSv1 rather than SSLv3), and import the CA root certificate.	This procedure is only for TLS. **1** Open the Local Security Settings on OCS. **2** In the console tree, choose **Local Polices.** **3** Choose **Security Options**. **4** Double-click **System Cryptography:Use FIPS Compliant algorithms for encryption, hashing and signing**. **5** Enable the security setting. **6** Click **OK**. **Note** You may need to restart OCS for this to take effect. **7** Import the CA root certificate for the CA that signs the IM and Presence Service certificate. Import the CA root certificate in to the trust store on OCS using the certificate snap-in.
Configure the certificates on IM and Presence Service	This procedure is only for TLS. You must upload the root certificate for the CA that signs the OCS server certificates to IM and Presence Service. As well, generate a CSR for IM and Presence Service and have it signed by the CA. Then upload the CA-signed certificate to IM and Presence Service. You must then add a TLS peer subject on IM and Presence Service for the OCS Server. See topics related to setting up certificates for detailed instructions.

Configure Static Routes on OCS to Point to the IM and Presence Service

To allow OCS to route requests to IM and Presence Service for direct federation, you must configure a TLS or TCP static route on the OCS server for each IM and Presence Service domain. These static routes are to point to an IM and Presence Service node.

Note

- For Standard Edition, you must complete this procedure on all Standard Edition servers.
- For Enterprise Edition, you must complete this procedure on all pools.

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Office Communications Server 2007 R2**.

Step 2 Right-click the Enterprise Edition pool name or the Standard Edition server name, as appropriate.

Step 3 Choose **Properties** > **Front End Properties**.

Step 4 Choose the **Routing** tab and click **Add**.

Step 5 Enter the domain for the IM and Presence Service node, for example, foo.com.

Step 6 Ensure that the check box for **Phone URI** is unchecked.

Step 7 Set the next hop transport, port, and IP address/FQDN values:

- For TCP, choose **TCP** as the Next Hop Transport value and enter a Next Hop Port value of **5060**. Enter the IP address of the IM and Presence Service node as the Next Hop IP Address.
- For TLS, choose **TLS** as the Next Hop Transport value and enter a Next Hop Port value of **5061**. Enter the IP address of the IM and Presence Service node as the FQDN.

Note
- The port used for the TLS static route must match the Peer Auth Listener port that is configured on the IM and Presence Service node.
- The FQDN must be resolvable by the OCS server. Ensure that the FQDN resolves to the IP address of the IM and Presence Service node.

Step 8 Ensure that the check box for **Replace host in request URI** is unchecked.

Step 9 Click **OK** to close the **Add Static Route** window. The new static route should appear in the Routing list.

Step 10 Click **OK** again to close the **Front End Server Properties** window.

What to Do Next

See Verify Peer Authentication Listener in the Interdomain Federation for IM and Presence Service on Cisco Unified Communcations Manager guide.

Add Host Authorization on OCS for IM and Presence Service

To allow OCS to accept SIP requests from IM and Presence Service without being prompted for authorization, you must configure Host Authorization entries on OCS for each IM and Presence Service node.

For TCP, only one host authorization entry using the IM and Presence Service IP address needs to be added for each IM and Presence Service node.

If you are configuring TLS encryption between OCS and IM and Presence Service, you must add two Host Authorization entries for each IM and Presence Service node, as follows:

- The first entry must contain the FQDN of the IM and Presence Service node.
- The second entry must contain the IP address of the IM and Presence Service node.

If you are not configuring TLS encryption, then you add only one Host Authorization entry for each IM and Presence Service node. This host authorization entry must contain the IP address of the IM and Presence Service node.

The following procedure describes how to add the required Host Authorization entries.

Note

- For Standard Edition, you must complete this procedure on all Standard Edition servers.
- For Enterprise Edition, you must complete this procedure on all pools.

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Office Communications Server 2007 R2**.

Step 2 Right-click the Enterprise Edition pool name or the Standard Edition server name, as appropriate.

Step 3 Choose **Properties** > **Front End Properties**.

Step 4 Choose the **Host Authorization** tab and click **Add**.

Step 5 If you are entering an FQDN, choose **FQDN** and enter the FQDN of the IM and Presence Service node. For example, imp1.foo.com.

Step 6 If you are entering an IP address, choose **IP Address** and enter the IP address of the IM and Presence Service node. For example, 10.x.x.x.

Step 7 Ensure that the **Outbound Only** check box is unchecked.

Step 8 Check the **Throttle as Server** check box.

Step 9 Check the **Treat as Authenticated** check box.

Step 10 Click **OK** to close the **Add Authorized Host** window.

Step 11 Repeat Step 4 to Step 10 for each IM and Presence node.

Step 12 After you add all the Host Authorization entries, click **OK** to close the **Front End Server Properties** window.

What to Do Next

Restart Services on OCS Front-End Servers, on page 6

Related Topics

Integration Troubleshooting

Restart Services on OCS Front-End Servers

After you complete all the configuration steps on OCS, you must restart the OCS services to ensure that the configuration takes effect.

Note

- Cisco recommends that you perform this procedure during a scheduled maintenance window.
- For Standard Edition, you must follow this procedure on all Standard Edition servers.
- For Enterprise Edition, you must follow this procedure on all front-end servers.

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Office Communications Server 2007 R2**.

Step 2 Right-click the FQDN of the Standard Edition server or Enterprise Edition front-end server and choose **Stop** > **Front End Services** > **Front End Service**.

Step 3 After the services stop, right-click the FQDN of the Standard Edition server or Enterprise Edition front-end server and choose **Start** > **Front End Services** > **Front End Service**.

Related Topics

Integration Troubleshooting

TLS Encryption Configuration

You must complete the procedures in this section to configure TLS encryption between IM and Presence Service and OCS.

After the TLS configuration is complete, you must restart services on OCS servers. See Restart Services on OCS Front-End Servers, on page 6.

Enable Federal Information Processing Standard Compliance on OCS

To support TLS encryption between IM and Presence Service and OCS, you must enable TLSv1 on OCS servers. TLSv1 is included as part of the Federal Information Processing Standard (FIPS) compliance on Windows servers. The following procedure describes how to enable FIPS compliance.

Note

- For Standard Edition, you must perform this procedure on all Standard Edition servers.
- For Enterprise Edition, you must perform this procedure on all front-end servers.

Procedure

Step 1 On the OCS server, choose **Start** > **Programs** > **Administrative Tools** > **Local Security Policy**.

Step 2 From the console tree, choose **Local Policies**.

Step 3 Choose **Security Options**.

Step 4 Double-click **System Cryptography: Use FIPS Compliant algorithms for encryption, hashing and signing**.

Step 5 Enable the security setting.

Step 6 Click **OK**.

Step 7 Close the Local Security Settings window.

What to Do Next

Configure Mutual TLS Authentication on OCS, on page 8

Related Topics

Integration Troubleshooting

Configure Mutual TLS Authentication on OCS

To configure TLS encryption betweenIM and Presence Service and OCS, you must configure port 5061 on the OCS servers for Mutual TLS authentication. The following procedure describes how to configure port 5061 for Mutual TLS authentication.

Note

- For Standard Edition, you must perform this procedure on all Standard Edition servers.
- For Enterprise Edition, you must perform this procedure on all front-end servers.

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Office Communications Server 2007 R2**.

Step 2 Right-click the FQDN of the Standard Edition server or Enterprise front-end server and choose **Properties** > **Front End Properties**.

Step 3 Choose the **General** tab.

Step 4 If the Transport associated with Port 5061 is **MTLS**, go to Step 8.

Step 5 If the Transport associated with Port 5061 is not **MTLS**, click **Edit**.

Step 6 From the Transport drop-down list, choose **MTLS**.

Step 7 Click **OK** to close the **Edit Connection** window. The Transport associated with Port 5061 should now be **MTLS**.

Step 8 Click **OK** to close the **Properties** window.

What to Do Next

Install Certificate Authority Root Certificates on OCS, on page 8

Related Topics

Integration Troubleshooting

Install Certificate Authority Root Certificates on OCS

To support TLS encryption between IM and Presence Service and OCS, each OCS server must have a signed security certificate. This signed certificate, along with the root certificate of the Certificate Authority (CA) that signed the certificate, must be installed on each OCS server.

Cisco recommends that OCS and IM and Presence Service nodes share the same CA. If not, the root certificate of the CA that signed the IM and Presence Service certificates must also be installed on each OCS server.

Generally, the root certificate of the OCS CA is already installed on each OCS server. Therefore, if OCS and IM and Presence Service share the same CA, there may be no need to install a root certificate. However, if a root certificate is required, see the following details.

If you are using Microsoft Certificate Authority, refer to the following procedures in the *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager* for information about installing the root certificate from the Microsoft Certificate Authority onto OCS:

- Downloading the CA Certification Chain
- Installing the CA Certification Chain

If you are using an alternative CA, the following procedure is a generic procedure for installing root certificates onto OCS servers. The procedure for downloading the root certificate from the CA differs depending on your chosen CA.

Before You Begin

Download the root certificate or certificate chain from your CA and save it to the hard disk of your OCS server.

Procedure

Step 1 On your OCS server, choose **Start** > **Run**.

Step 2 Enter `mmc` and click **OK**.

Step 3 From the File menu, choose **Add/Remove Snap-in**.

Step 4 From the Add/Remove Snap-in dialog box, click **Add**.

Step 5 From the list of Available Standalone Snap-ins, choose **Certificates**, and then click **Add**.

Step 6 Choose **Computer Account**, and then click **Next**.

Step 7 In the Select Computer dialog box, check the check box for **<Local Computer> (the computer this console is running on)**, and then click **Finish**.

Step 8 Click **Close**, and then click **OK**.

Step 9 In the left pane of the Certificates console, expand **Certificates (Local Computer)**.

Step 10 Expand **Trusted Root Certification Authorities**.

Step 11 Right-click **Certificates**, and choose **All Tasks**.

Step 12 Click **Import**.

Step 13 In the **Import** wizard, click **Next**.

Step 14 Click **Browse** and navigate to where you saved the root certificate or certificate chain.

Step 15 Choose the file and click **Open**.

Step 16 Click **Next**.

Step 17 Leave the default value **Place all certificates in the following store** and ensure that **Trusted Root Certification Authorities** appears under the Certificate store.

Step 18 Click **Next**, and then click **Finish**.

Step 19 Repeat Step 11 to Step 18 as necessary for other CAs.

Note The *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager* document refers to the Access Edge Server. For partitioned intradomain federation, you can replace references to the Access Edge Server with OCS Standard Edition server or Enterprise Edition front-end server.

What to Do Next

Validate Existing OCS Signed Certificate, on page 10

Related Topics

Integration Troubleshooting
Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager

Validate Existing OCS Signed Certificate

To support TLS encryption between IM and Presence Service and OCS, each OCS server must have a signed security certificate that supports Client Authentication. If a signed certificate is already installed on the OCS server, the following procedure describes how to check if that existing signed certificate supports Client Authentication.

Note
- For Standard Edition, you must perform this procedure on all Standard Edition servers.
- For Enterprise Edition, you must perform this procedure on all front-end servers.

Procedure

Step 1 On your OCS server, choose **Start** > **Run**.
Step 2 Enter `mmc` and click **OK**.
Step 3 From the File menu, choose **Add/Remove Snap-in**.
Step 4 From the Add/Remove Snap-in dialog box, click **Add**.
Step 5 From the list of Available Standalone Snap-ins, choose **Certificates** and click **Add**.
Step 6 Choose **Computer Account** and click **Next**.
Step 7 In the Select Computer dialog box, check the **<Local Computer> (the computer this console is running on)** check box and click **Finish**.
Step 8 Click **Close**, and then click **OK**.
Step 9 In the left pane of the Certificates console, expand **Certificates (Local Computer)**.
Step 10 Expand **Personal** and choose **Certificates**.
Step 11 Find the signed certificate currently used by OCS in the right pane.
Step 12 Ensure that **Server and Client Authentication** is listed in the Intended Purposes column.

What to Do Next

Signed Certificate Request from the Certificate Authority for the OCS Server, on page 11

Related Topics

Integration Troubleshooting

Signed Certificate Request from the Certificate Authority for the OCS Server

This section describes how to install a signed certificate on a Microsoft Office Communicator Server (OCS) and how to choose the installed certificate for TLS negotiation.

Note The procedures in this topic are only necessary if no signed certificate exists on an OCS or the existing certificate does not support Client Authentication.

To support TLS encryption between IM and Presence Service and OCS, each OCS must have a signed security certificate that supports Client Authentication. If that is not the case on any OCS, the following procedures outline how to request a newly signed certificate from the Certificate Authority and install it onto that specific OCS.

The Subject Common Name (CN) used in Certificate Signing Requests (CSR) from the OCS differs depending on the OCS deployment:

- For Standard Edition servers, use the FQDN of the Standard Edition server as the Subject CN.
- For Enterprise Edition front-end servers, use the FQDN of the pool to which the front-end server belongs as the Subject CN.

Standalone Microsoft Certificate Authority

If you are using a Standalone Microsoft Certificate Authority, see the following procedures in the *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager* to request a signed certificate from the CA for the OCS:

- Requesting a Certificate from the CA Server
- Downloading the Certificate from the CA Server

Note This document refers to the Access Edge Server. For Partitioned Intradomain Federation, you can replace references to the Access Edge Server with an OCS Standard Edition or Enterprise Edition front-end server.

Enterprise Microsoft Certificate Authority

If you are using an Enterprise Microsoft Certificate Authority, see the following procedures in the *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager* to generate the required template on the CA and request a signed certificate from the CA for the OCS:

- Creating a Custom Certificate for Access Edge Using an Enterprise Certificate Authority

- Requesting the Site Server Signing Certificate

Alternative Certificate Authority

If you are using an alternative CA, the following is a generic procedure for installing signed certificates onto the OCS. The procedure for requesting a signed certificate differs depending on your chosen CA.

Related Topics

Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager

Install Signed Certificate on the OCS Server

Before You Begin

Download the signed certificate from your CA and save it to the hard disk of your OCS server.

Procedure

Step 1 On your OCS server, choose **Start** > **Run**.
Step 2 Enter **mmc** and click **OK**.
Step 3 From the File menu, choose **Add/Remove Snap-in**.
Step 4 From the Add/Remove Snap-in dialog box, click **Add**.
Step 5 From the list of Available Standalone Snap-ins, choose **Certificates** and click **Add**.
Step 6 Choose **Computer Account** and click **Next**.
Step 7 In the Select Computer dialog box, check the **<Local Computer> (the computer this console is running on)** check box and click **Finish**.
Step 8 Click **Close**, and then click **OK**.
Step 9 In the left pane of the Certificates console, expand **Certificates (Local Computer)**.
Step 10 Expand **Personal**.
Step 11 Right-click **Certificates**, and then choose **All Tasks**.
Step 12 Click **Import**.
Step 13 In the **Import** wizard, click **Next**.
Step 14 Click **Browse** and navigate to where you saved the signed certificate.
Step 15 Choose the file and click **Open**.
Step 16 Click **Next**.
Step 17 Leave the default value **Place all certificates in the following store** and ensure that **Personal** appears under the Certificate store.
Step 18 Click **Next**, and then click **Finish**.

What to Do Next

Select Installed Certificate for TLS Negotiation, on page 13

Related Topics

Integration Troubleshooting

Select Installed Certificate for TLS Negotiation

Regardless of which CA is used, after the signed certificate is installed onto the OCS server, you must perform the following procedure to select the installed certificate for use by OCS in TLS negotiation withIM and Presence Service.

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Office Communications Server 2007 R2**.

Step 2 Right-click the FQDN of the Standard Edition server or Enterprise Edition front-end server and choose **Properties** > **Front End Properties**.

Step 3 Choose the **Security** tab and choose **Select Certificate**.

Step 4 From the list of installed certificates, choose the newly signed certificate and click **OK** to close the **Select Certificate** window.

Step 5 Click **OK** to close the **Properties** window.

What to Do Next

Restart Services on OCS Front-End Servers, on page 6

Related Topics

Integration Troubleshooting