Configure Microsoft Office Communications Server for Partitioned Intradomain Federation

Note The procedures in this chapter apply only to Microsoft Office Communications Server (OCS) 2007 R2.

Domain verification for OCS servers

Before you proceed to set up Cisco Unified Presence for Partitioned Intradomain Federation, verify that there are matching domains configured on the Microsoft OCS servers and all nodes in the Cisco Unified Presence cluster.

Enable Port 5060/5061 on the OCS Server

For TCP static routes to the OCS server, use port 5060.

For TLS static routes to the OCS server, use 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 Select **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 select **Properties > Front End Properties**.

Step 3 Select the **General** tab.

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

Step 5 Configure the IP address, port, and transport values as follows:

a. Select **All** as the IP Address Value.

b. Select the Port Value.

- For TCP, select **5060** as the Port Value.
- For TLS, select **5061** as the Port Value.

c. Select **TCP** as the Transport Value.

- For TCP, select **TCP** as the Transport Value.
- For TLS, select **TLS** as the Transport Value.

Step 6 Select **OK** to close the Add Connection window. Port 5060 should now be listed under the Connections list.

Step 7 Select **OK** again to close the Front End Server Properties window.

Related Topic

Troubleshooting Partitioned Intradomain Federation, page 11-1

What To Do Next

Configure OCS Static Route to Point to Cisco Unified Presence, page 7-2

Configure OCS Static Route to Point to Cisco Unified Presence

To allow OCS to route requests to Cisco Unified Presence, you must configure a static route on OCS servers. The static route points to a Cisco Unified Presence server. The following procedure describes how to configure the required static route.

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 Select **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 Select **Properties > Front End Properties**.

Step 4 Select the **Routing** tab and select **Add**.

Step 5 Enter the domain for the Cisco Unified Presence server, for example, foo.com.

Step 6 Ensure that **Phone URI** is unchecked.

Step 7 Enter the IP address of the Cisco Unified Presence server as the Next Hop IP address.

Step 8 Select one of the following for the Next Hop Transport and port values:

- Select **TCP** as the Next Hop Transport value, and enter a Next Hop Port value of **5060**.
- Select **TLS** as the Next Hop Transport value, and enter a Next Hop Port value of **5061**.

Note

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

Step 9 Ensure that **Replace host in request URI** is unchecked.

Step 10 Select **OK** to close the Add Static Route window. The new static route should appear in the Routing list.

Step 11 Select **OK** again to close the Front End Server Properties window.

Related Topics

Troubleshooting Partitioned Intradomain Federation, page 11-1

What To Do Next

Add Host Authorization on OCS for Cisco Unified Presence, page 7-3

Add Host Authorization on OCS for Cisco Unified Presence

To allow OCS to accept SIP requests from Cisco Unified Presence without being prompted for authorization, you must configure Host Authorization entries on OCS for each Cisco Unified Presence server.

If you are configuring TLS encryption between OCS and Cisco Unified Presence, you must add two Host Authorization entries for each Cisco Unified Presence server, as follows:

- The first entry must contain the FQDN of the Cisco Unified Presence server.
- The second entry must contain the IP address of the Cisco Unified Presence server.

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

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 Select **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 Select **Properties > Front End Properties**.

Step 4 Select the **Host Authorization** tab and select **Add**.

Step 5 If you are entering an FQDN, select **FQDN** and enter the FQDN of the Cisco Unified Presence server. For example, cup1.foo.com.

Step 6 If you are entering an IP address, select **IP Address** and enter the IP address of the Cisco Unified Presence server. For example, 10.x.x.x.

Step 7 Ensure that **Outbound Only** is unchecked.

Step 8 Check **Throttle as Server**.

Step 9 Check **Treat as Authenticated**.

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

Step 11 Repeat Step 4 to Step 10 for each Cisco Unified Presence server.

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

Related Topic

Troubleshooting Partitioned Intradomain Federation, page 11-1

What To Do Next

Restart Services on OCS Front-End Servers, page 7-4

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 Select **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 select **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 select **Start > Front End Services > Front End Service**.

Related Topic

Troubleshooting Partitioned Intradomain Federation, page 11-1

Configure TLS Encryption

You must complete the following procedures to configure TLS encryption between Cisco Unified Presence and OCS:

- Configure Mutual TLS Authentication on OCS, page 7-5
- Install Certificate Authority Root Certificates on OCS, page 7-6
- Validate Existing OCS Signed Certificate, page 7-7
- Request Signed Certificate from Certificate Authority, page 7-8

After the TLS configuration is complete, you must restart services on OCS servers. See Restart Services on OCS Front-End Servers, page 7-4.

Configure Mutual TLS Authentication on OCS

To configure TLS encryption between Cisco Unified Presence 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 Select **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 select **Properties > Front End Properties**.

Step 3 Select the **General** tab.

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

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

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

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

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

Related Topic

Troubleshooting Partitioned Intradomain Federation, page 11-1

What To Do Next

Install Certificate Authority Root Certificates on OCS, page 7-6

Install Certificate Authority Root Certificates on OCS

To support TLS encryption between Cisco Unified Presence 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 Cisco Unified Presence servers share the same CA. If not, the root certificate of the CA that signed the Cisco Unified Presence 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 Cisco Unified Presence 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 *Integration Guide for Configuring Cisco Unified Presence for Interdomain Federation* 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, select **Start > Run**.

Step 2 Enter **mmc** and select **OK**.

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

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

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

Step 6 Select **Computer Account** and select **Next**.

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

Step 8 Select **Close**, and then **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 select **All Tasks**.

Step 12 Select **Import**.

Step 13 In the Import Wizard, select **Next**.

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

Step 15 Select the file and select **Open**.

Step 16 Select **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 Select **Next** and **Finish**.

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

Related Topics

- *Integration Guide for Configuring Cisco Unified Presence for Interdomain Federation:*

  http://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html

Note The *Integration Guide for Configuring Cisco Unified Presence for Interdomain Federation* 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.

- Troubleshooting Partitioned Intradomain Federation, page 11-1

What To Do Next

Validate Existing OCS Signed Certificate, page 7-7

Validate Existing OCS Signed Certificate

To support TLS encryption between Cisco Unified Presence 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, complete the following procedure to check whether the 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, select **Start > Run**.

Step 2 Enter **mmc** and select **OK**.

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

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

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

Step 6 Select **Computer Account** and select **Next**.

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

Step 8 Select **Close**, and then **OK**.

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

Step 10 Expand **Personal** and select **Certificates**.

Step 11 Find the signed certificate that is currently used by OCS in the right pane.

Step 12 Ensure that **Server and Client Authentication** is listed in the Intended Purposes column.

Related Topic

Troubleshooting Partitioned Intradomain Federation, page 11-1

What To Do Next

Request Signed Certificate from Certificate Authority, page 7-8

Request Signed Certificate from Certificate Authority

This section describes the following procedures:

- Install Signed Certificate on OCS Server, page 7-9
- Select Installed Certificate for TLS Negotiation, page 7-10

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

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

The Subject Common Name (CN) used in Certificate Signing Requests (CSR) from OCS differs depending on 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 *Integration Guide for Configuring Cisco Unified Presence for Interdomain Federation* to request a signed certificate from the CA for the OCS server:

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

Note You can find the *Integration Guide for Configuring Cisco Unified Presence for Interdomain Federation* here:
http://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html
This 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.

Enterprise Microsoft Certificate Authority

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

- 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 OCS servers. The procedure for requesting a signed certificate differs depending on your chosen CA.

Install Signed Certificate on 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, select **Start > Run**.

Step 2 Enter **mmc** and select **OK**.

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

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

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

Step 6 Select **Computer Account** and select **Next**.

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

Step 8 Select **Close**, and then **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 select All Tasks.

Step 12 Select **Import**.

Step 13 In the Import Wizard, select **Next**.

Step 14 Select **Browse** and navigate to where you saved the signed certificate.

Step 15 Select the file and select **Open**.

Step 16 Select **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 Select **Next** and **Finish**.

Related Topic

Troubleshooting Partitioned Intradomain Federation, page 11-1

What To Do Next

Select Installed Certificate for TLS Negotiation, page 7-10

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 with Cisco Unified Presence.

Procedure

Step 1 Select **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 select **Properties > Front End Properties**.

Step 3 Select the **Security** tab and select **Select Certificate**.

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

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

Related Topic

Troubleshooting Partitioned Intradomain Federation, page 11-1

What To Do Next

Restart Services on OCS Front-End Servers, page 7-4