Integrating Avaya Aura® Presence Services with Microsoft OCS

6.1 Service Pack 5
December 2012

Contents

Chapter 1: Introduction

Overview - OCS/Lync integration

Avaya Aura® Presence Services is a multiprotocol, multifunctional server providing presence and IM services to Avaya Aura® users. Presence Services collects and distributes the communication status of an Avaya Aura® user from the various communication endpoints connected on an enterprise network. Presence Services provides aggregation and composition services in its Event State Compositor (ESC) to create a composite presence document for an Avaya Aura® user. This composite presence document is available to any authorized subscribing enterprise user. A Presence Services server aggregates the presence for an Avaya Aura® user and obtains the presence of a user from the following sources:

- PIDF presence published by Avaya Aura® clients using both SIP and XMPP.
- Collected presence from an integrated enterprise system, for example, telephony presence through AES collection.
- Third-party presence integration such as Microsoft OCS/Lync collects presence.
- Collection of an enterprise user Microsoft OCS/Lync presence that requires the deployment and enabling of the Presence Services RTC Collector component. The collection and aggregation of the Microsoft OCS/Lync presence of an Avaya Aura® user requires the deployment, and enabling of the Presence Services RTC Collector component. The RTC Collector component interacts with an OCS/Lync server through an Edge server and retrieves the Microsoft OCS/Lync presence of an Avaya Aura® user.

Additionally, Presence Services provides IM capabilities to Avaya Aura® users. This capability is achieved using the XMPP protocol support within an Avaya Aura® client. Thus, all Avaya Aura® clients, which are enabled for IM use XMPP for managing their IM conversations. Avaya Aura® users can engage in IM conversations with each other through their Avaya Aura® clients. After enabling the OCS Gateway the scope of this interaction is extended. Thus, an Avaya Aura® user can engage in an IM conversation with another enterprise user, who is using Microsoft Office Communicator (MOC)/Lync clients for their IM communications. Thus, enabling the OSC Gateway within the installation of Presence Services installation supports:

- Avaya Aura® users, using their Avaya Aura® clients, can IM the other enterprise user colleagues who are using Microsoft Office Communicator (MOC)/Lync clients.
- Enterprise users, using MOC/Lync clients, can initiate an IM conversation with their enterprise colleagues who are usingAvaya Aura® clients.

Additionally, an Enterprise user can obtain the overall presence availability of their Aura colleagues by adding the presence handle of an Avaya Aura® user to their buddy list. The MOC/Lync client displays the presence against the contact address of an Avaya Aura® user.

Note:

You can enable RTC Collector and OCS Gateway during the Presence Services installation. But if you decide to enable RTC Collector and OCS Gateway after you have installed Presence Services, see the *Integrating RTC Collector* and *Integrating OCS Gateway* section in this document.

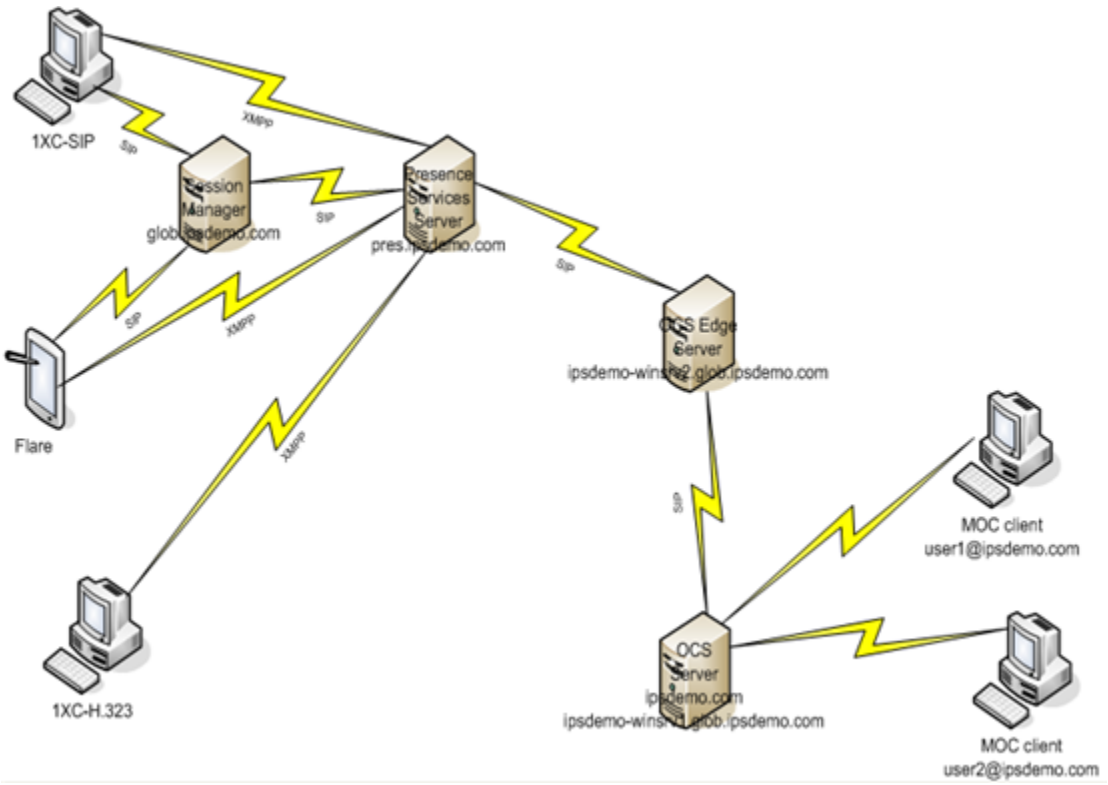
The main purpose of integrating an OCS Gateway with Presence Services is to provide an IM interoperability and presence distribution from Presence Services to the OCS/Lync users. In the latter scenario, an Avaya Aura® user is added to buddy list of an MOC/Lync user, so that you can obtain an overall availability of an Avaya Aura® user. As a result, you have two buddies in your buddy list. This requires that a Presence Services server is configured as a federated IM provider in the deployment of an OCS/Lync Edge server. This federated interworking model requires the management of trust configuration between the two systems, and the setup of network configuration in the form of DNS records (SRV and Host A records).

When you enable and deploy an OCS Gateway in a Presence Services installation, an enterprise user using an MOC/Lync client can engage in IM conversations with a colleague who is using an Avaya Aura® client. Additionally, the enterprise user using the MOC/Lync client can see an overall availability of an Avaya Aura® user, by adding the presence handle of an Aura user to their buddy list.

The Presence Services server and OCS/Lync integration architecture

The following architectural components are involved in the deployment of Presence Services, which is integrated with OCS/Lync for presence and IM:

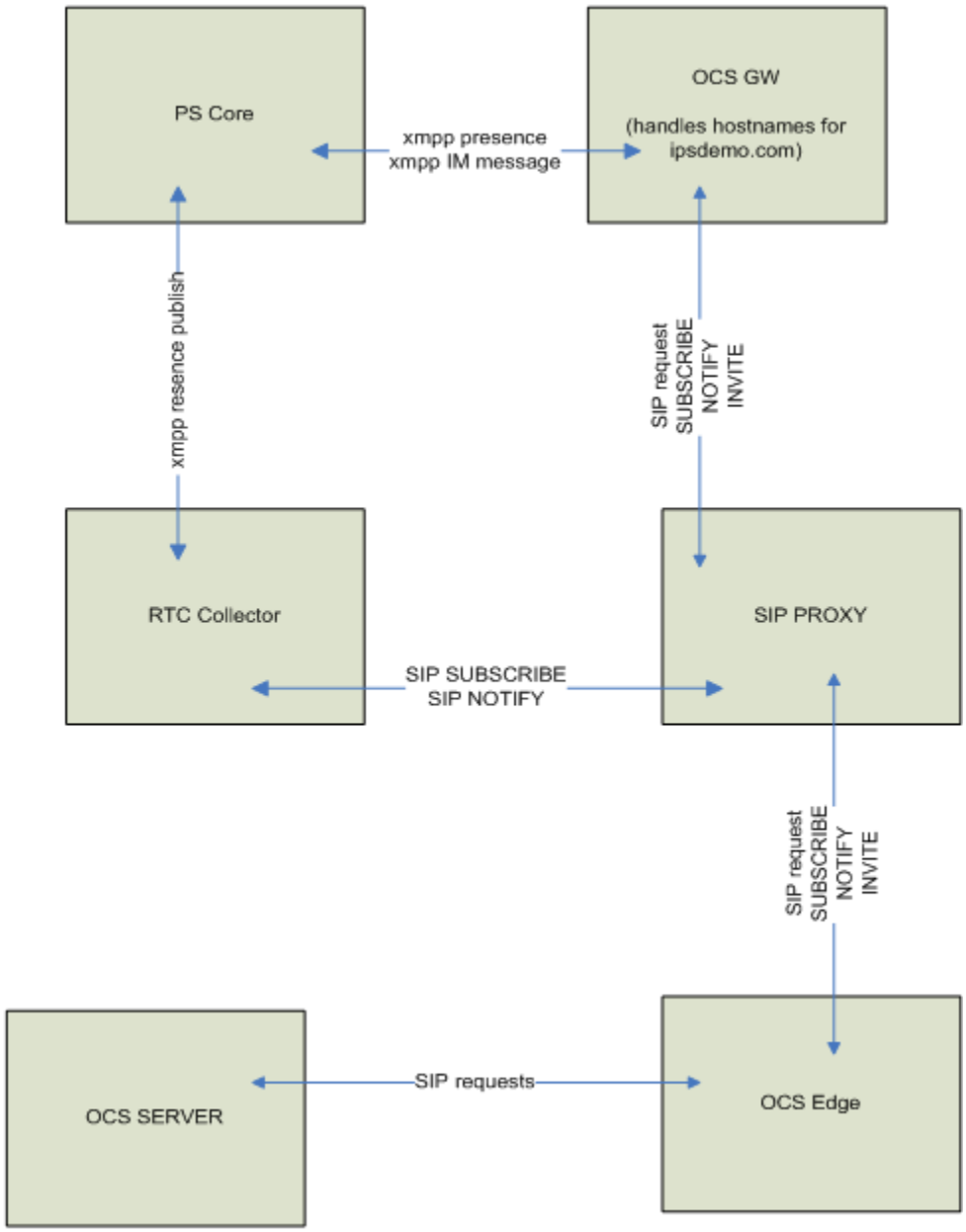
- RTC Collector
- OCS Gateway



In the sample deployment figure, the OCS server resides on the ipsdemo.com domain, Presence Services resides on the pres.ipsdemo.com domain, while the Avaya Aura® domain resides on the glob.ipsdemo.com. Therefore, users provisioned in System Manager will have a domain substitution rule. This substitution rule converts the user name username@glob.ipsdemo.com to a Presence Services user identifier username@pres.ipsdemo.com for provisioned users in System Manager. The FQDN for Presence Services is ipsdemo-ips1.ipsdemo.com, the external FQDN for the OCS server is ipsdemo-winsrv1.glob.ipsdemo.com, and the FQDN for the OCS Edge server is ipsdemo-winsrv2.glob.ipsdemo.com. This sample deployment has been used throughout this guide to help illustrate example configuration input.

For more information on the domain substitution rule, see the *Avaya Aura® Presence Services Implementing guide*.

Within the Presence Services server, there are a number of server components that execute to provide the RTC Collector and OCS Gateway services.



The component view figure shows the Presence Services RTC Collector component and the OCS Gateway component communicating with an OCS Edge server. The SIP requests from the RTC Collector and OCS Gateway to the OCS Edge server are routed through the SIP Proxy of Presence Services, and then through an OCS Edge server.

The Presence Services integration with OCS/Lync is based on a federated interworking deployment between the two systems. You can administer Presence Services as a federated provider on the OCS/Lync environment, which enables the exchange of IM and presence between the two systems. The main components from the Avaya Aura® perspective are:

- Avaya Aura® clients
- Presence Services systems including its RTC Collector component

- The OCS Gateway component
- The SIP Proxy component

The main components involved from an OCS/Lync perspective are:

- OCS/Lync Edge
- OCS/Lync server
- MOC/Lync clients
- DNS server
- Active Directory

Chapter 2: Enabling and Configuring an RTC Collector

Overview - The RTC Collector

The RTC Collector component is part of the ESC functionality of Presence Services. The RTC Collector component is also an integral part of the aggregation and composition functionality within Presence Services. The main purpose of the RTC Collector is to collect and monitor the OCS presence and then feed the ESC of Presence Services for aggregation and composition. In doing so, the RTC Collector sends a SIP SUBSCRIBE for each Avaya Aura®user to the OCS/Lync server. This SIP SUBSCRIBE contains an RTC handle of an Avaya Aura® user as the target of the subscribe request, as specified in the request URI and in the To header field of the SIP request. To facilitate the subscription process, configure the RTC Collector with a system user. This system user is used as the subscribing user for the OCS/Lync subscription. The user name for this system user is specified in the RTC Collector configuration screen that you can gain access to through the XCP Controller Web interface. You can also specify the RTC system user name during the installation of the Presence Services server when you select the RTC Collector..

You must provision the RTC handle associated with an Avaya Aura® user in System Manager to enable the RTC Collector to the presence of an OCS/Lync user. When the system administrator provisions the RTC handles in System Manager, the Avaya Aura® users are propagated to Presence Services by the replication service running on System Manager (DRS).The Presence subscriptions from the RTC Collector are subject to normal authorization control within the OCS/Lync domain. The OCS server must authorize the Presence subscriptions before the OCS/Lync server sends the presence of an MOC/Lync user to the RTC Collector. If this authorization is not in place, then either the RTC Collector receives an error response or the OCS/Lync server executes polite blocking. During polite blocking, a closed presence state is received. An enterprise user logged on the MOC/Lync client receives an authorization request for the user presence from the RTC Collector system user, for example, PSAdmin user, and the user must accept the request to allow the RTC Collector system user to receive their MOC/Lync presence.

RTC Collector parameters

When you are enabling the RTC Collector during the installation, then you must provide the following parameters:

- RTC Collector Username: The federated user name used to make a subscription for the OCS//Lync Presence of an Avaya Aura® user. Note that this appears on the RTC Collector configuration screen as the User Name configuration parameter, for example, PSAdmin. Referred to as the RTC System User.
- RTC SIP Domain: The SIP Domain of the OCS//Lync server. This domain appears on the RTC Collector configuration screen in the Static Routes configuration parameter, for example, ipsdemo.com.
- RTC Collector Port: A default value of 45061 is presented. Accept this value.
- RTC Edge: The external FQDN of the OCS//Lync Edge server.

You must also use the following parameters during the installation and configuration of an RTC Collector:

- Router Service Name: Presence Services Router Service Name. This is the domain name associated with the Presence Services server that will be set at the time of installation. This name appears on the RTC Collector configuration screen as the Presence Services SIP Domain configuration parameter, for example, pres.ipsdemo.com.
- Presence Services IP Address: The IP address of the Presence Services server. Note: The system displays the Presence Services IP address on the RTC Collector configuration screen in the Static Routes parameter, for example, 135.64.22.133.
- Presence Services FQDN: The Fully Qualified Domain Name (FQDN) of the Presence Services server. Note: The system displays the RTC Collector configuration screen as the external host name for a contact parameter, for example, ipsdemo-ips1.ipsdemo.com.

From these installation parameters, the system displays the following configuration parameters on the configuration screen of an RTC Collector:

- User Name: PSAdmin
- PS SIP Domain: pres.ipsdemo.com
- Transport: tls
- Port: 45061
- Expires (seconds): 86400
- Subscription Failure Retry: 3600
- Server Failure Retry: 3600
- Static Routes: ipsdemo.com 135.64.22.133 5061

- External hostname that the server uses for contact: ipsdemo-ips1.ipsdemo.com
- External port that the server uses for contact: 5061

The SIP Proxy plays an integral part in the processing of a SIP SUBSCRIBE that the system sends from the RTC Collector to an OCS//Lync server, and in the processing of a NOTIFY that the system sends from an OCS//Lync server to the RTC Collector system user. You must define routing rules in the SIP Proxy, which routes SIP requests to their appropriate destination servers. The following two rules govern the flow of SIP requests to and from OCS//Lync:

- The outbound SIP SUBSCRIBE requests from Presence Services to OCS//Lync rule: This rule specifies that if the To header is to the OCS//Lync domain and if the From header is from the Presence Services domain, that default SIP routing rules is applicable.
- The inbound SIP NOTIFY request rule: This rule specifies that a SIP NOTIFY method with a To header containing the RTC Collector system user will route to the RTC Collector.
- The default SIP routing rules: This rule determines the destination IP address of the destination server in the target domain. The SIP Host mapping in the Remote Host Configuration of the SIP PROXY assists in resolving the target domain for default SIP routing rule. A SIP Host mapping maps an OCS//Lync domain to the external FQDN of an OCS//Lync Edge server.

Note:

The external FQDN of the OCS//Lync Edger server must be resolvable and requires an entry in the `/etc/hosts` file. Ensure that the `/etc/hosts` file contains an IP address for the external FQDN of the OCS//Lync Edge server.

RTC collector deployment checklist

#	Server	Task	✔
1	Presence Services server	Enable, deploy, and configure RTC Collector in the Presence Services server.	
	Presence Services server	Check that the Presence Services SIP Proxy routing rules and Host mapping configuration has been set for integration with OCS/ Lync. Check that LCS routing compatibility is set to **Yes**.	

#	Server	Task	✔
	OCS/Lync CA and OCS/Lync Edge	Set the server authentication and client authentication properties when you generate a TLS certificate for the OCS/ Lync Edge server'	
	OCS/Lync Edge	Download the CA certificate that the system signs for the external certificate of the Edge server.	
	Presence ServicesPresence Services server	Copy the OCS/Lync Edge server CA certificate to Presence Services.	
	OCS/Lync Edge and Presence Services server	Add the CA certificate for the Edge server to Presence Services to the PS trust store.	
	OCS/Lync Edge server	Upload the Presence Services CA certificate to the OCS/Lync Edge server and add the Presence Services CA certificate to the trust store of the OCS/Lync Edge server. By default, the Presence Services CA certificate is usually the System Manager CA certificate. Use the Presence Services CA certificate to sign the Presence Services TLS certificate.	
	Presence Services server	Verify that the CA certificate that you downloaded exists in trust store, execute the prescert list command.	
	OCS/Lync Edge and Presence Services server	Verify the configuration status for both servers, check trust stores, and DNS configuration on the OCS/Lync Edge server.	

#	Server	Task	✔
	OCS/Lync Edge server	Configure Presence Services as an IM provider on the Edge server.	
	OCS/Lync Active Directory	Configure OCS/Lync users and enable the OCS/Lync users for federated inter-working.	
	System Manager	Add OCS/Lync handles for users on System Manager.	

RTC Collector configuration worksheet

The following table outlines a set of parameters that you must know before enabling an RTC collector:

Configuration parameter Name	Parameter value	Default value presented on the configuration screen
User Name		
PS SIP Domain [1]		The service router name configured during the installation
Transport		Tls
Port		45061
Expires		86400
Subscription Failure retry		3600
Server Failure retry		3600
Static Routes [2]		<OCS Domain><IP address of Presence Services><Port>

[1] The system provides the Presence Services domain by default for this parameter. This equates to the Service Router Name that the system provides at the time of the Presence Services server installation.

[2] The static route configures the next hop destination for the SIP SUBSCRIBE. The next hop should be SIP Proxy. The system presents the IP address of Presence Services and the port 5061 by default for this parameter. The system administrator must complete this static route by preceding these two entry values with the OCS domain, for example, if the IP address of your Presence Services is 135.64.22.133 and the OCS domain is ipsdemo.com, then 135.64.22.133 5061 appears in the static route. Complete the static route by adding ipsdemo.com before the IP address to give a configuration of ipsdemo.com 135.64.22.133 5061.

Configuration parameter Name	Parameter value	Default value presented on the configuration screen
SIP SUBSCRIBE Contact FQDN [3]		-
SIP SUBSCRIBE Contact Port		-

Checklist for adding a new RTC Collector

The system combines the RTC system user name and Presence Services SIP Domain to create the URI of a user who subscribes to an MOC/Lync client on behalf of the RTC Collector. The value of the user name is not important, but you must set the user name to a value that identifies this instance of the RTC Collector. For example, PSAdmin. The OCS/Lync server will then receive subscription requests from sip:PSAdmin@<*PS Domain*>.

Ensure that you know the values for the following parameters:

Component	Description	✔
Router Service name	Ensure that the Presence Services Router Services name is the domain name for the Presence Services server that was set at the time of installation.	
RTC User	The defaulted federated user name used to subscribe to RTC Presence.	
RTC SIP Domain	The SIP domain that the RTC servers use.	
Presence Services IP Address	The IP address of the Presence Services server.	
Presence Services FQDN	The Fully Qualified Domain Name (FQDN) of the Presence Services server.	

[3] Select the “Define an optional external contact for SIP server to contact the RTC Collector” check box and then fill in the two associated configuration parameters: External host name that SIP server uses for contact and External port that SIP server uses for contact, with the FQDN of the Presence Services server and the port 5061 respectively. These values set the Contact header in the SIP SUBSCRIBE, which uses as the request URI in the NOTIFY request sent by the OCS server. The objective is that the system uses Contact address as the NOTIFY R-URI by the OCS server.

Adding and configuring the RTC Collector

Procedure

1. Log in to the Presence Services XCP Controller Web interface.
2. Select the Advanced configuration view, in the Components area, select **RTC Collector** from the **Add a new** drop-down list, and click **Go**.
3. Complete the following settings:
   a. MS RTC Collector Configuration: Select the **MS RTC Collector Configuration** check box.
   b. User Name: Enter the *<RTC User Name>* value.
   c. PS SIP Domain: The system displays the value for this field by default.
   d. Transport: The system displays the value for this field by default.

      Note:

      Accept the default values for other fields.
   e. Define the next hop for a domain: Enter the *<RTC SIP domain><PS IP address>* `5061`.
   f. Select the **Define an optional external contact for SIP servers to use to contact the RTC Collector** check box.
   g. In the **External hostname that SIP servers will use for contact** field, define an optional external hostname that SIP servers use to contact to the RTC Collector: Enter *<PS FQDN>*.
   h. In the **External port that SIP servers will use for contact** field, define an optional external port that SIP servers use to contact to the RTC Collector: Enter `5061`.
4. Click **Submit** to save the changes.

Configuring the SIP Proxy routing rules for RTC Collector

Add the routing rules in the SIP Proxy manually. You must configure the following rules:

- Outbound SIP SUBSCRIBE to OCS
- Inbound SIP NOTIFY from OCS

Note:

The addition of routing rules is linear, that is, a new rule is added directly after the last rule is defined. You must take note of the last rule currently defined, which should be a default

routing rule or catch all, which routes all remaining SIP requests, not covered by the preceding rules, to the SIP Presence server or SIP PS component. Once you record this rule, remove this rule.

Add the two new routing rules for the RTC Collector, and then add the default routing rule.

Before you begin

- The **Add Record-Route header** field is set to **No**.
- The **Enable LCS Routing compatibility** field is set to **Yes**.

Also, consider the possible scenarios:

- RTC Collector is being enabled and deployed and the OCS Gateway is not enabled and deployed.
- RTC Collector is being enabled and deployed and the OCS Gateway has been previously enabled and deployed.

  If the OCS Gateway has already been enabled before the RTC Collector, then a number of relevant routing rules for the RTC Collector will exist.

Procedure

1. On the Presence Services XCP Controller home page, select the **Advanced** configuration view.
2. In the Components area, click **Edit** in the Actions column next to the SIP Proxy component.
3. On the SIP Proxy Configuration page, scroll down to the SIP Proxy Routing Rules section.
4. Review the last routing rule, click details of the last routing rule table entry, and record the details of this rule. The system displays the Routing Rule Configuration page.

   Note:

   This rule specifies the default rule or catch all rule routing SIP requests to SIP Presence Services. If the rule does not specify these details, there is a potential error in your proxy configuration.

Related topics:

Checking and recording a default routing rule on page 19

Checking and recording a default routing rule

Procedure

1. In the Destination Routes section, the system selects the **Use a specific destination for this rule** check box by default. In the **rule-destination** text box, check the entry for rule destination. For example, sip-ps-1. If the system deploys more than one SIP Presence Services, then each of the SIP Presence Services will be listed in the destinations input box.
2. Click **Cancel** and then click **OK** to return to the main configuration page for the SIP Proxy.
3. On the last routing rule, click **Remove** to remove this rule. You can recreate this rule manually after the system adds the RTC Collector routing rules.

Adding the RTC Collector routing rule

While adding the RTC Collector routing rules, consider the following possible scenarios:

- Adding RTC Collector when OCS Gateway is not enabled
- Adding RTC Collector when OCS Gateway is enabled

Note:

In each case, there is a rule to govern the outbound SIP requests (SUBSCRIBE) and the inbound SIP requests (NOTIFY).

Related topics:

Outbound SIP SUBSCRIBE routing rule on page 19
Inbound SIP NOTIFY routing rule on page 20

Outbound SIP SUBSCRIBE routing rule

About this task

The outbound SUBSCRIBE is based on the To and From header field. The From header rule pattern has a domain specified as the Presence Services domain, for example, `pres.ipsdemo.com`. The To header rule pattern specifies the OCS/Lync domain, for example, `ipsdemo.com`.

Procedure

1. On the SIP Proxy Configuration page, scroll down to the SIP Proxy Routing Rules section, and click **GO** to add a new SIP PROXY Routing Rule. The system displays the SIP Proxy Routing Rule Configuration page.
2. Select the **To Hosts** check box.
3. In the input box, enter the OCS/Lync domain. For example, `ipsdemo.com`.
4. Select the **From Hosts** check box.
5. In the input box, enter the PS domain. For example, `pres.ipsdemo.com`.
6. Add the routing destination for this rule.
7. From the Destination Routes section, select **use sip default routing rules**.
8. On the SIP Proxy Routing Rule Configuration page, click **Submit** to save the changes.

Inbound SIP NOTIFY routing rule

About this task

This rule routes NOTIFY requests to the RTC Collector. This rule is based on recognizing the NOTIFY method and filtering on the To header field of this NOTIFY. The To header field will have the RTC Collector user as its target, for example, PSAdmin@pres.ipsdemo.com.

Procedure

1. On the SIP Proxy Routing Rule Configuration page, select the **SIP Methods** check box.
2. Select the **SIP Method** check box and enter `NOTIFY`.
3. Set the **Invert this selection** field to **No**.
4. Select the **Header Rules** check box.
5. Set the **All Headers Must Match?** field to **Yes**.
6. Click **Go** next to **Add a New Header pair**.
7. On the Header Pair Configuration page, do the following:
   a. Set the **Header Name** field to **To**.
   b. In the **Header Value** field, enter the RTC User.

Note:

This user is added as the User Name parameter in the RTC Collector configuration, for example, PSAdmin.

8. On the Header Pair Configuration page, click **Submit**.
9. On the SIP Proxy Routing Rule Configuration page, in the Destination Routes section, select **Use a specific destination for this rule**.

   rule-destination: rtc-collector

   Note:

   The rtc-collector is a routing tag, which is defined in the TLS transport configuration under the SIP Stack Configuration Parameters on the main SIP Proxy configuration page.
10. Set the **Choose destination based on to or from user** field to **To**.
11. On the SIP Proxy Routing Rule Configuration page, click **Submit** to save the changes.

Next steps

You must recreate the default routing rule that you removed in the previous sections. To recreate the default routing rule, perform the following:

1. On the SIP Proxy Configuration page, under the SIP Proxy Configuration section, click **Go** next to **Add a new SIP Proxy Routing Rule**.
2. On the SIP Proxy Routing Rule Configuration page, under the Destination Routes section, select **Use a specific destination for this rule**.
3. In the **IDs of Specific Destinations** text box, enter `sip-ps-1`.
4. From the Choose destination based on to or from user drop-down box, select **from**.
5. To save the routing rule, click **Submit**.

Note:

If a Presence Services installation enables multiple sip Presence Services components, then the original default routing rule will have multiple sip Presence Services entries. Therefore, in recreating the default routing rule, enter the sip PS component id for each sip PS into the **IDs of Specific Destinations** text box.

Adding a new Remote Host

Procedure

1. On the Presence Services XCP Controller home page, select the **Advanced** configuration view.
2. In the Components area, click **Edit** in the Actions column next to the SIP Proxy component.
   The system displays the SIP Proxy Configuration page.
3. Under the Remote Host Configuration section, select **Local Configuration** and then click **Go** next to **Add a new SIP Host**.
   The system displays the SIP Host Configuration page.
4. Under SIP Host, in the **Remote server hostname** text box, enter the external FQDN of the OCS/Lync Edge server. For example, `edger2svext.eu.ocs2adsv.com`.
5. From the **Server Type** drop-down box, select **ocs**.
6. In the **Hostname Mapping** text box, enter the OCS/Lync domain name. For example, `ocsr2adsv.com`.
7. To save the changes, click **Submit**.
   The system take you to the SIP Proxy Configuration page. On the Remote Host Configuration section, under Local Configuration, the system displays the SIP Host entry that you recently created.

Adding a new routing label for the RTC Collector

Procedure

1. On the Presence Services XCP Controller home page, select the **Advanced** configuration view.
2. In the Components area, click **Edit** in the Actions column next to the SIP Proxy component.
   The system displays the SIP Proxy Configuration page.
3. Under the SIP Stack Configuration Parameters section, click **Details** next to the existing transport entry. The existing transport entry must have a name similar to, `sip-proxy-1_tls-transport.presence.`
   The system displays the TLS transport Configuration page.

4. Under the Routes for this Transport section, click **Go**.
   The system displays the Route Configuration page.
5. Enter the details for the following fields:
   - ID, enter the ID. For example, `rtc-collector`.
   - IP address, enter the IP address. For example, `135.60.22.51`.
   - Port, enter the port, `45061`.
6. To save the changes, click **Submit**.

   Note:

   The RTC Collector routing label that you just added here must correspond with the label specified for the RTC Collector inbound routing rule for SIP Proxy.

   The system takes you to the TLS transport Configuration page.
7. On the TLS transport Configuration page, under Routes for this Transport, ensure that the new routes are present.
8. On the SIP Proxy Configuration page, click the **Submit** to save the configured proxy rules that you have recently added.

Next steps

Enable trust management and DNS administration to setup a trust relationship between Presence Services and the RTC Collector. For more information on trust management and DNS administration, see the *Trust Management and DNS Administration* chapter.

Chapter 3: Integrating OCS Gateway

Overview - OCS Gateway

The main purpose of integrating an OCS Gateway with Presence Services is to provide an IM interoperability and presence distribution from Presence Services to the OCS/Lync users. In the latter scenario, an Avaya Aura® user is added to buddy list of an MOC/Lync user, so that the MOC/Lync user can obtain an overall availability of an Avaya Aura® user. This requires that a Presence Services server is configured as a federated IM provider in the deployment of an OCS/Lync Edge server. This federated interworking model requires the management of trust configuration between the two systems, and the setup of network configuration in the form of DNS records (SRV and Host A records).

When you enable and deploy an OCS Gateway in a Presence Services installation, an enterprise user using an MOC/Lync client can engage in IM conversations with a colleague who is using an Avaya Aura® client. Additionally, the enterprise user can also see an overall availability of an Avaya Aura® user, by adding an Aura presence handle to their buddy list.

Note:

You cannot add an OCS/Lync contact directly to the contact list on an Aura client. In order to subscribe for the presence of an OCS/Lync user you must first add an OCS/Lync contact handle to the communication profile of an Aura user in System Manager. Then you add the Aura user as the contact. The addition of an OCS/Lync handle to an Aura user's communication profile handle set allows the RTC Collector to obtain and aggregate OCS/Lync presence for the associated user.

Also, please note that Presence Services does not support ACL=Confirm for Lync.

Related topics:

Inbound requests on page 25
Outbound requests on page 26

Inbound requests

The inbound requests originate from the OCS/Lync and route through the OCS/Lync Edge server and the Presence Services SIP Proxy. The Presence Services SIP Proxy is instrumental in directing SIP requests from the OCS/Lync system to the OCS Gateway. You can achieve this through the routing rules defined in SIP Proxy. Inbound SIP requests are subject to routing rules, which are defined on the To and From header fields of a SIP request. The inbound routing

rules directs certain SIP requests originating from an OCS/Lync system to the OCS Gateway.

Outbound requests

The outbound requests are the SIP requests that the system initiates as a result of Avaya Aura® client initiated requests destined for an OCS/Lync enterprise user. These requests are processed by Presence Services and are routed internally through the OCS Gateway. In the current Presence Services implementation, these requests are XMPP requests that originates from an Aura client.

For example, an Avaya Aura® enterprise user logged on a 1XC-H.323 or 1XC-SIP client can click on a user in their contact list and initiate an IM with that peer enterprise user. The 1XC clients then indicates that the target user has two IM addresses: an Avaya Aura® XMPP handle and an OCS/Lync handle. If the initiating user selects the OCS/Lync handle, then the Avaya Aura® client sends an XMPP IM message to Presence Services and then Presence Services routes this IM message internally through the OCS Gateway. This is because the system configures the OCS Gateway to handle communications with the OCS/Lync domain and the address used in the request contains the OCS/Lync domain.

Outbound SIP requests route through a SIP Proxy of Presence Services, then to the OCS/Lync Edge, and then into the OCS/Lync server. The SIP communication is based on a federated deployment of Presence Services with OCS/Lync. The configuration on OCS/Lync Edge is for federated inter-working. Therefore, you must configure Presence Services for federation as an IM provider on the OCS/Lync Edge server.

Additionally, to establish TLS communications and achieve server authentication, it is necessary that the CA TLS/SSL certificate of the Certificate Authority, which signed the TLS/SSL certificates of Presence Services and OCS/Lync Edge, are imported into each of the trust stores on Presence Services and the OCS/Lync Edge respectively. With the appropriate Presence Server Host records and SRV records configured in the DNS service associated with the OCS/Lync Edge and the OCS/Lync server, you establish this trust relationship.

Use the following domains as an illustration:

- The PS domain is pres.ipsdemo.com
- The OCS/Lync domain is ipsdemo.com
- The PS server FQDN is ipsdemo-ips1.ipsdemo.com
- The OCS/Lync Edge server external FQDN is ipsdemo-winsrv2.glob.ipsdemo.com
- The OCS/Lync server is ipsdemo-winsrv1.glob.ipsdemo.com

If you are enabling the OCS Gateway during installation, then you must know the appropriate values for the following parameters on the Presence Services server:

- OCS/Lync Edge: The external FQDN of the OCS/Lync Edge server, for example, ipsdemo-winsrv2.glob.ipsdemo.com
- OCS/Lync SIP domain: The OCS/Lync domain, for example, ipsdemo.com
- OCS/Lync SIP Port: 65061

These parameters set up the OCS Gateway configuration together with the default settings for non-solicited parameters. You can also use these parameters to configure the OCS Gateway routing rules in the SIP Proxy.

The SIP Proxy plays an integral part in the processing of a SIP request that the system sends to the OCS/Lync server and in handling the SIP requests received from the OCS/Lync server to Presence Services. You must define routing rules in the SIP Proxy, which routes SIP requests to their appropriate destination servers. Two rules govern the flow of SIP requests to and from OCS/Lync:

- The outbound SIP (SUBSCRIBE, INVITE, ACK, NOTIFY) requests from Presence Services to OCS/Lync have a rule which specifies that if the To header is set to the OCS/Lync domain and if the From header is from the Presence Services domain, then you must apply the default SIP routing rule.
- The inbound SIP (SUBSCRIBE, INVITE, ACK, NOTIFY) requests have a rule which specifies that if the To header contains the Presence Services domain and the From header contains the OCS/Lync domain, then the request is to be routed to the OCS Gateway.
- The default SIP routing rules determine the destination IPS address of the target domain. This requires the configuring of a Host mapping in the Proxy. This Host mapping maps an OCS/Lync domain to the external FQDN of the OCS/Lync Edge server. The external FQDN of the OCS/Lync edge server must be resolvable and requires an entry in the /etc/hosts file.

OCS Gateway deployment checklist

This checklist outlines the set of tasks that you must execute to deploy an OCS Gateway and provides cross references to sections of this guide, which provide details of the tasks.

#	Server	Task	✔
	Presence server	Enable, deploy, and configure OCS Gateway in the Presence Server	
	Presence server	Check that the PS SIP Proxy routing rules and Host mapping	

#	Server	Task	✔
		configuration has been set for integration with OCS/Lync.	
	OCS/Lync CA and OCS/Lync Edge	Generate an SSL certificate for use on the OCS/Lync Edge. This requires server authentication and client authentication properties to be set.	
	OCS/Lync Edge	Download the CA which signed the external certificate of the Edge server.	
	Presence Server	Copy the OCS/Lync Edge server CA certificate to Presence server.	
	OCS/Lync Edge and Presence Services server	Add the CA for the Edge server to the Presence Services to the Presence Services trust store.	
	Presence Server	Verify that the downloaded CA certificate exists in the trust store, execute prescert list command.	
	Presence Services server	Restart Presence Services to pick up the new trust store and configurations.	
	OCS/Lync Active Directory	Enable OCS/Lync users for federated inter-working.	
	OCS/Lync Edge server	Upload the Presence Services CA certificate to the OCS/Lync Edge server and add the Presence Services CA certificate to the trust store of the OCS/Lync Edge server. By default, the Presence Services CA certificate is usually	

#	Server	Task	✔
		the System Manager CA certificate. Use the Presence Services CA certificate to sign the Presence Services TLS certificate.	
	OCS/Lync Edge and Presence Services server	Verify the configuration status for both Presence Services and OCS/Lync servers, check trust stores, and DNS configuration on OCS/Lync Edge server.	
	OCS/Lync Edge server	Restart external services to apply the changes.	
	System Manager	Add OCS/Lync handles for users on System Manager.	

OCS Gateway configuration worksheet

The OCS Gateway configuration worksheet identifies the set of configuration parameters that are when you enable an OCS Gateway. It is important that you know the values for the following parameters before starting the configuration process.

Configuration parameter Name	Parameter value	Default valued presented on the configuration screen
OCS Domain		
PS SIP Domain [4]		The service router name configured during installation, for example, pres.ipsdemo.com.
Transport		tls
Port [5]		
Expires		86400

[4] The Service Router Name solicited during the installation process is the Presence Services presence domain.

[5] The system provides a default port, 5061. You must change this port to a free port, typically to 65061. The convention for backend SIP servers is to use 5061 with an integer value from the set 1,2,3,4,5,6 prepended to create the port. Note that any value greater than 6 pushes the port value beyond the acceptable range of TCP ports.

Configuration parameter Name	Parameter value	Default valued presented on the configuration screen
Subscription Failure retry		3600
Server Failure retry		3600
PS IP address		
SIP Proxy Port [6]		
PS server FQDN		
SIP SUBSCRIBE Contact Port [7]		
TLS keystore full file path [8]		
TLS trust store full file path [9]		

Enabling OCS Gateway

You can enable an OCS Gateway in the following scenarios:

- During Presence Services installation
- After Presence Services installation

Related topics:

Enabling OCS Gateway during installation on page 30
Enabling OCS Gateway post installation on page 31

Enabling OCS Gateway during installation

When you select and enable an OCS Gateway at the time of installation, as a part of the installation process, the system requests the following configuration parameters:

[6] The SIP Proxy port is 5061.
[7] The contact port should be that of the SIP Proxy, that is 5061.
[8] Currently, TLS keystore full file path is `/opt/Avaya/Presence/jabber/xcp/certs/generic.pem.jabber`
[9] Currently, TLS trust store full file path is `/opt/Avaya/Presnce/jabber/xcp/certs/generic.trusts`

- OCS/Lync Edge: The external FQDN of the OCS/Lync Edge server, for example, ipsdemo-winsrv2.glob.ipsdemo.com.
- OCS/Lync SIP Domain: The OCS/Lync domain.
- OCS/Lync SIP Port: The TLS port used by the SIP stack.

The system presents a default 65061 port number for the OCS/Lync SIP port. You can accept this value almost invariably. The installer enables the OCS Gateway and sets up its configuration. Additionally, the system configures SIP Proxy with routing route and host mappings for interacting with OCS/Lync.

Enabling OCS Gateway post installation

About this task

The OCS Gateway provides IM and presence interoperability between a Presence Services installation and an OCS/Lync installation. You can achieve this by setting up a federated deployment between OCS/Lync and Presence Services. For this interoperability between the two systems, you must configure Presence Services as an IM provider on the OCS/Lync Edge server on OCS/Lync, and also ensure that the relevant DNS network configuration and trust management is in place.

You can enable an OCS Gateway post installation through the XCP Controller Web interface.

Procedure

1. Log in to the Presence Services XCP Controller Web interface.
2. In the **Components** area, select **Connection Manager** from the **Add a new** drop-down list, and click **Go**. The system displays the Connection Manager Configuration page. By default, the system displays a basic configuration view, but you must switch to the advanced configuration view.

   Tip:

   On the Connection Manager Configuration page, under the Connection Manager section, you can rename the **Description** field to `OCS Connection Manager` for more clarity.
3. Under the Command line to run section, change the text in the **Command line to run** text box to, exec /opt/Avaya/Presence/jabber/xcp/bin/sip_gw -h %i -m %m -n %n -p %p -P /opt/Avaya/Presence/jabber/xcp/var/run/jabberd/%n.pid. The OCS Gateway does not start, unless you make these changes.
4. From the **Add a New Command Processor** drop-down box, select **S2S Command Processor**.
5. Click **GO**. The system displays the S2S Command Processor Configuration page. The initial configuration settings on this page are the default settings for an XMPP

S2S Gateway. You must remove parts of the default configuration and replace with SIP/Simple Gateway configuration.

6. In the Director Configuration section, the system presents two default XMPP directors. Click **Remove** next to each default XMPP directors.
7. To confirm the removal of the XMPP directors, on the **Click 'OK' to confirm removal from the configuration** dialog box, click **OK** for each of the XMPP directors.
8. On the S2S Command Processor Configuration page, under the Director Configuration section, from the **Add a new** drop-down box, select **SIP/SIMPLE Gateway** and then click **Go**.

   The system displays the SIP/Simple Gateway Configuration page. The system requires a number of configuration parameters for the SIP/Simple Gateway, which includes Remote Host Configuration, SIP Stack Configuration, and Outbound Proxy configuration.

Next steps

Configure OCS Gateway.

Configuring OCS Gateway

Overview - Configuring OCS

The SIP/Simple gateway requires the configuration setting of a number of parameters under various categories, which includes SIP Host Configuration and SIP Stack Configuration. To add a SIP Host configuration, perform the following:

- Configure a SIP TLS transport under the SIP Stack Configuration category
- Set the Outbound Proxy
- Modify a number of SIP request timeout parameters

Configuring the SIP Remote Host Configuration parameters

Procedure

1. In the SIP/Simple Gateway Configuration page, scroll to the Remote Host Configuration section and select **Local Configuration**.
2. Click **GO** to add a new SIP Host. The system displays the SIP Host Configuration page. This configuration defines a mapping between the OCS/Lync domain and the OCS/Lync Edge server. For the mapping, you need the following three parameters:
   - Remote server hostname
   - Server Type
   - Hostname mapping
3. In the **Remote server hostname** field, enter the external FQDN of the OCS/Lync Edge server.
4. From the **Server Type** drop-down box, select **ocs**.
5. On the Hostname Mappings section, in the **Hostname(s)** field, enter the OCS/Lync domain. For example, ipsdemo.com.
6. To save the configuration, click **Submit**. The system returns to the SIP/Simple Gateway Configuration page.

Configuring the SIP Stack Configuration parameters for the OCS Gateway

Procedure

1. In the SIP Stack Configuration Parameters section, create and configure TLS transport.
2. From the **Add a new SIP Transport** drop-down box, select **TLS** and click **GO**. The system displays the TLS transport Configuration page. This page provides network and TLS configuration parameters for the selected TLS transport.

Note:

Ensure that the domain that you use for TLS certificate is the FQDN of Presence Services. The full path to the certificate file must be `/opt/Avaya/Presence/`

`jabber/xcp/certs/generic.pem.jabber` and the full path to the CA certificate file should be `/opt/Avaya/Presence/jabber/xcp/certs/generic.trusts`.

3. Accept the default values for the following configuration parameters:
   - Unique identifier for this transport
   - Hostname of external interface
   - IP address

   Note:

   The hostname for external interface is the PS domain name.
4. In the **Port** field, change the value of the port from 5061 to 65061. This is the port configured for the OCS Gateway.
5. In the **Use this transport by default for TLS requests** field, use the default value **Yes**.
6. In the **Domain used for TLS certificate** field, enter the FQDN of Presence Services.
7. Use the following values:
   - The Full path to the certificate file: `/opt/Avaya/Presence/jabber/xcp/certs/generic.pem.jabber`
   - Full path to the CA certificate: `/opt/Avaya/Presence/jabber/xcp/certs/generic.trusts`
8. In the Define an optional external contact for SIP servers to use to contact this transport section, enter the following two configuration parameters:
   - External hostname that SIP servers will use to contact: Enter the FQDN of Presence Services.
   - External port that SIP servers will use for contact: Enter the SIP Proxy port 5061.

   Note:

   These parameters are used to set the Contact header of the outbound SIP requests.
9. Click **Submit** to save the configuration settings. The system displays the SIP/Simple Gateway page again.
10. Configure Outbound Proxy. This forces outbound SIP requests through a next hop processing node. In this case, the next hop processing node is the Presence Services SIP Proxy, where you need to apply the outbound OCS/Lync routing rules.
11. Select the **Outbound Proxy** check box and enter the following parameters:

- Proxy IP address: Presence Services IP address.
- Proxy Port: 5061.
- Proxy Transport: TLS

12. In the list of configuration parameters, set the **TLS connection strict checking of hostname and TLS connection strict certificate usage** parameters value to `No`. Use the default values for the remaining parameters.

    The SIP/Simple Gateway Configuration provides parameters that define how TLS certificates are handled, for example, whether strict host name checking is applied or not.

13. Click **Submit** to save the SIP/Simple Gateway Configuration. The system displays the S2S Command Processor Configuration page. On the S2S Command Processor Configuration page, the system displays an entry for `cm-2_s2scp-1_sipsd-1.presence` SIP/Simple Gateway component in the director configuration table.
14. On the S2S Command Processor Configuration page, on the Outgoing Connection Attempt Rules, the system displays three rules. These rules are applicable to the XMPP S2S directors and are not relevant for the OCS Gateway configuration. Therefore, you must remove the rules.
15. In the table, for each of the existing rules, click **Remove** next to each rule to delete the rule.
16. Create a new dummy rule, Outgoing Connection Attempt Rule. These dummy rules are a form of local SRV DNS lookup and are associated with built-in default rules within OCS Gateway.
17. Prior to creating the dummy rule, take note of the SIP/Simple Gateway identifier. Typically, this is cm-2_s2scp-1_sipsd-1, and you can obtain the value from the director table at the top of this configuration page.
18. To create a dummy rule, click **GO**. The system displays the Rule Configuration page.
19. For example, enter the following:
    - Director ID: cm-2_s2scp-1_sipsd-1. This is the SIP/Simple Gateway component identifier.
    - DNS SRV lookup to use: abcdef.
    - Port to use instead of DNS SRV lookup: Leave this field blank.
20. To save this rule configuration, click **Submit**. The system returns to the S2S Command Processor Configuration page.
21. On the S2S Command Processor Configuration page, click **Submit** to save all configuration inputs. The system displays the Connection Manager Configuration page.

22. On the Connection Manager Configuration page, the system displays a command process `cm-2_s2scp-1.presence` in the command processor table. As a final part of the configuration, enable logging.
23. To enable logging, scroll to Component Logging, and select the **Component Logging** check box.
24. Select the **Logger** check box and then select the **Filtered Syslog Logger** check box.
25. Under the Pipe Level Filter section, accept the default Level at WARNING, and in the **Pipe file** text box, enter the path `/opt/Avaya/Presence/jabber/xcp/var/log/ocs-cm.pipe`. This file is used to dynamically adjust the logging level of the OCS Gateway through the **`/opt/Avaya/Presence/jabber/xcp/bin/updateLogLevel.sh`** script.
26. Under the File Settings section, in the Name and location field, enter the name and location, for example, /var/log/presence/ocsgateway.log.
27. Under the Syslog Settings section, in the **Identity** text box, enter `OCS-CM`.
28. Click **Submit**. The system creates a Connection Manager component containing the OCS Gateway. The system now displays the XCP Controller main page. The system adds an additional connection manager component to the component list.

Next steps

To complete the OCS Gateway setup and integration with OCS/Lync, it is necessary to complete the trust management and DNS administration procedures. For more information, see the *Trust management and DNS Administration* chapter.

Configuring the OCS Gateway Hostname Filter: Open Port component configuration

About this task

You must configure the OCS Gateway in such a way that any presence packets or IM messages destined for the OCS/Lync domain can be routed internally within the Presence Services through the OCS Gateway. For this, you must create an Open Port component that specifies that the OCS Gateway handles packets and message requests destined for the OCS/Lync domain.

Procedure

1. Log in to the XCP Controller Web interface.
2. On the XCP Controller Configuration page, from the **Component** drop-down box, select **Open Port**.

3. Click **GO**. The system displays a pop-up menu, where the system asks you to enter the user input for the name of a component associated with the Open Port component that you want to create.
4. In the enter ID of open port component field, enter the name of the S2SCP which was created while enabling the OCS Gateway. For example, if the name of the Connection Manager was cm-2 and the S2SCP is cm-2_s2scp-1, then enter `cm-2_s2scp-1` as the component ID for the Open Port component.

   Note:

   Ensure that you use the same S2SCP component name, created during the configuration for the OCS Gateway, for the Open Port component name. Also, you must not include ".presence" in the Open port component name.
5. Click **OK**. The system displays the OpenPort Configuration page.
6. On the Hostname for this Component section, in the **Host Filter Host(s)** field, enter the OCS/Lync domain, for example, `ipsdemo.com`.
7. To save the configuration, click **Submit**. This configuration is the only configuration required for the Open Port.

   The main objective of OpenPort configuration is to associate the OCS/Lync domain with the OCS Gateway. This allows any presence packets or IM messages to route internally within Presence Services to the OCS Gateway. The OCS Gateway then converts any presence packets or IM messages to SIP requests. The OCS Gateway then sends these SIP requests to the OCS/Lync server through the SIP Proxy and OCS/Lync Edge server.

Configuring SIP Proxy routing rules for OCS Gateway

You must add the SIP Proxy routing rules manually only after enabling the OCS SIP Gateway. Configure the following rules:

- Outbound SIP requests to OCS
- Inbound SIP requests from OCS

Note:

Note that the addition of routing rules is linear, that is, the system adds a new rule after the last current rule is defined. The last current rule should be a default routing rule or catch all, which routes all remaining SIP requests, not covered by the preceding rules, to the SIP Presence Services. Record the details of the last current rule, after recording the details, remove the rule. It is important that you create the last current rule again after the OCS Gateway routing rules are created. Add the two new routing rules for the OCS Gateway.

This addition should be followed by the readdition of the default or catch all rule to route SIP requests to the SIP Presence Services.

Before you begin

Check that the following configuration parameters are set to the values indicated:

- The Add Record-Route header field is set to `No`.
- The Enable LCS Routing compatibility field is set to `Yes`.

Note:

To check the Add Record-Route header field and Enable LCS Routing compatibility field, see the SIP Proxy settings.

About this task

Also, consider the following possible scenarios:

- OCS Gateway is enabled and deployed and the RTC Collector is not enabled and deployed.
- OCS Gateway is being enabled and deployed and the RTC Collector has been previously enabled and deployed.

Procedure

1. On the Presence Services XCP Controller home page, select the **Advanced** configuration view.
2. In the Components area, click **Edit** in the Actions column next to the SIP proxy component.
3. On the SIP Proxy Configuration page, scroll down to the SIP Proxy Routing Rules section. Review the last routing rule by clicking details of the last routing rule table entry, and record the details of this rule. The system displays the Routing Rule Configuration page. This rule specifies the default or catch all rule routing SIP requests to the SIP Presence server component. If not, then there is a potential error in your proxy configuration. The default routing rule reads as follows: In the Destination Routes section, a use a specific destination for this rule configuration will be set with a routing tag sip-ps-1. If the system deploys more than one SIP Presence server component, then each of these SIP Presence Services is also listed.
4. Click **Cancel** and **OK** to return to the main configuration page for the SIP Proxy.
5. To remove the last routing rule, click **Remove**.

OCS Gateway routing rule

When you add the OCS Gateway routing rules, consider the following possible scenarios:

- Scenario 1: Adding OCS Gateway routing rule without RTC Collector enabled
- Scenario 2: Adding OCS Gateway routing rule with RTC Collector enabled and deployed

In each case, there is a rule to govern the outbound SIP requests (SUBSCRIBE, INVITE, ACK, NOTIFY) and the inbound SIP requests (SUBSCRIBE, INVITE, ACK, NOTIFY). These rules are based on the domains in the To and From headers, such that outbound SIP requests are destined To a user at the OCS domain and will come From a user in the Presence Services domain. For the inbound requests, the system originates these requests From a user in the OCS domain and routes To a user in the Presence Services domain.

Related topics:

Adding a new Remote Host on page 22
Inbound SIP requests routing rule on page 39
Outbound SIP requests routing rule on page 40
Adding a new routing label for the OCS Gateway on page 42

Inbound SIP requests routing rule

About this task

The inbound SIP requests rule is based on the To and From header field. The From header rule pattern specifies the domain as the OCS/Lync domain, for example, ipsdemo.com. The To header rule pattern specifies the Presence Services domain, for example, pres.ipsdemo.com.

Procedure

1. On the SIP Proxy Configuration page, scroll down to the SIP Proxy Routing Rules section. Click **GO** to add a new SIP PROXY Routing Rule. The system displays a SIP Proxy Routing Rule Configuration page.
2. On the SIP Proxy Routing Rule Configuration page, select the **To Hosts** check box.
3. Enter the Presence Services domain, for example, pres.ipsdemo.com.
4. Select the **From Hosts** check box.
5. Enter the OCS/Lync domain, for example, ipsdemo.com.
6. On the SIP Proxy Routing Rule Configuration page, select **Use a specific destination for this rule**.

7. Enter the following:
   - rule-destination: ocs-gw

     Note:

     The ocs-gw is a routing tag. Define this tag in the TLS transport configuration under the SIP Stack Configuration Parameters on the main SIP Proxy configuration page. Additionally, if you enable the OCS Gateway during installation, then the system selects the routing tag as cm2-s2scp-1. This label serves the same purpose as the ocs-gw label. The ocs-gw label is an internal routing label which identifies the network configuration parameters used by the OCS Gateway process, that is, the OCS Gateway IP address and port.

   - Select destination based on to or from user: to
8. On the SIP Proxy Routing Rule Configuration page, click **Submit** to save the changes.

Outbound SIP requests routing rule

About this task

The outbound SIP requests rule is based on the **To** and **From** header field. The From header rule pattern specifies the domain as the Presence Services domain, for example, pres.ipsdemo.com. The To header rule pattern specifies the OCS/Lync domain, for example, ipsdemo.com.

Note:

The outbound routing rule should already exist if you have enabled the RTC Collector prior to enabling an OCS Gateway.

Procedure

1. On the SIP Proxy Routing Rule Configuration page, select the **To Hosts** check box.
2. Enter the OCS/Lync domain, for example,`ipsdemo.com`.
3. Select the **From Hosts** check box.
4. Enter the Presence Services domain, for example, pres.ipsdemo.com. Then add the routing destination for this rule.
5. In the Destination Routes section, select **use sip default routing rules**.

6. On the SIP Proxy Routing Rule Configuration page, click **Submit** to save the changes.

Next steps

You must recreate the default routing rule that you removed in the previous sections. To recreate the default routing rule, perform the following:

1. On the SIP Proxy Configuration page, under the SIP Proxy Configuration section, click **Go** next to **Add a new SIP Proxy Routing Rule**.
2. On the SIP Proxy Routing Rule Configuration page, under the Destination Routes section, select **Use a specific destination for this rule**.
3. In the **IDs of Specific Destinations** text box, enter `sip-ps-1`.
4. From the Choose destination based on to or from user drop-down box, select **from**.
5. To save the routing rule, click **Submit**.

Note:

If a Presence Services installation enables multiple sip Presence Services components, then the original default routing rule will have multiple sip Presence Services entries. Therefore, in recreating the default routing rule, enter the sip PS component id for each sip PS into the **IDs of Specific Destinations** text box.

Adding a new Remote Host

Procedure

1. On the Presence Services XCP Controller home page, select the **Advanced** configuration view.
2. In the Components area, click **Edit** in the Actions column next to the SIP Proxy component.
   The system displays the SIP Proxy Configuration page.
3. Under the Remote Host Configuration section, select **Local Configuration** and then click **Go** next to **Add a new SIP Host**.
   The system displays the SIP Host Configuration page.
4. Under SIP Host, in the **Remote server hostname** text box, enter the external FQDN of the OCS/Lync Edge server. For example, `edger2svext.eu.ocs2adsv.com`.
5. From the **Server Type** drop-down box, select **ocs**.
6. In the **Hostname Mapping** text box, enter the OCS/Lync domain name. For example, `ocsr2adsv.com`.
7. To save the changes, click **Submit**.

The system take you to the SIP Proxy Configuration page. On the Remote Host Configuration section, under Local Configuration, the system displays the SIP Host entry that you recently created.

Adding a new routing label for the OCS Gateway

Procedure

1. On the Presence Services XCP Controller home page, select the **Advanced** configuration view.
2. In the Components area, click **Edit** in the Actions column next to the SIP Proxy component.
   The system displays the SIP Proxy Configuration page.
3. Under the SIP Stack Configuration Parameters section, click **Details** next to the already added TLS transport.
   The system displays the TLS transport Configuration page.
4. Under the Routes for this Transport section, click **Go**.
   The system displays the Route Configuration page.
5. Enter the details for the following fields:
   - ID, enter the ID. For example, `ocs-gw`.
   - IP address, enter the IP address. For example, `135.60.22.51`.
   - Port, enter the port, `65061`.
6. To save the changes, click **Submit**.

   Note:

   The OCS Gateway routing label that you just added here must correspond with inbound routing rule for SIP Proxy, as specified perviously.

   The system takes you to the TLS transport Configuration page.
7. On the TLS transport Configuration page, under Routes for this Transport, ensure that the new routes are present.
8. To save all the newly added SIP Proxy configuration, click **Submit**.

Next steps

Enable trust management and DNS administration to setup a trust relationship between Presence Services and the OCS Gateway. For more information on trust management and DNS administration, see the *Trust Management and DNS Administration* chapter.

Chapter 4: Trust Management and DNS Administration

Overview - Presence Services and OCS Gateway connection

By default, the Edge server external interface uses a server certificate. To enable communication with the OCS Gateway, you must generate a server SSL certificate to act as both the Client certificate and the Server certificate. To verify the certificate in use by the OCS/Lync Edge server external interface, use the OCS/Lync Edge server properties. For more information on verification, see the *OCS 2007 R2 Edge Server Deployment Guide* at: http://www.microsoft.com/download/en/details.aspx?id=24402.

To verify the certificate in use by the Lync Edge server external interface, use the Lync Edge server properties. For more information on verification, see the *Microsoft Lync Server 2010 Edge server Guide* at: http://www.microsoft.com/en-us/download/details.aspx?id=11379.

Checking the certificate used by external interface on server

About this task

By default, the Edge server external interface uses a server certificate. To enable communication with the OCS Gateway, you must configure this server certificate to act as both a Client certificate and Server certificate.

Procedure

To verify the certificate in use by the Edge server external interface, use the Edge server properties. For more information on verification, refer the *OCS 2007 R2 Edge Server Deployment Guide* at: http://www.microsoft.com/download/en/details.aspx?id=24402.

Generating and importing certificate for OCS

Generating a certificate with server and client authentication

About this task

The certificate that the Edge server external interface uses must have server and client authentication. If not, generate a certificate with server and client authentication and assign the certificate to the Edge server external interface.

To create a certificate for external interface using Microsoft Certificate Authority (CA) in a Windows 2003 Enterprise Edition Server running a standalone Microsoft Enterprise CA:

Note:

The procedure may vary depending on the configuration and setup of your Microsoft CA.

Procedure

1. Log on to the Web enrollment page of Certificate Authority at: `http://<CA_Machine>/certsrv/`.
2. On the Web enrollment page, click **Certificate** > **Advanced Certificate Request**.
3. On the **Advanced Certificate Request** dialog box, enter the following details:
   a. Select **Other** from the drop-down menu.
   b. In the **OID** text field, enter `1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2`.
      Separate the two OIDs by a comma but do not add a space.
   c. Click the **Store certificate in the local computer certificate store** check box.
      Leave all other details as is.
   d. Click **Submit**.
4. On the Certificate server perform the following:
   a. To open the mmc of the CertificateAuthority, type `mmc` in the **Run** dialog box, and click **Ok**.
   b. Right-click **Pending Requests**.
      The system displays the certificate request from the Edge server.
   c. Right-click on the certificate request based on request ID, and click **All Tasks** > **Issues**.
5. On the client computer, perform the following:

a. To open the Web enrollment page, click **Certificate** > **Advanced Certificate Request**.
b. Click **View the status of a pending certificate request**.
c. Click the certificate and save the certificate to use as the Certificate for the External Interface on the Edge server.

Importing the System Manager default CA certificate into the OCS Edge Trust Store

Procedure

1. Log in to the System Manager Web interface.
2. Click **Security** > **Certificates** > **Authority**.
3. Click **Download pem file**. Save the pem file with an appropriate name, for example, `default-cacert.pem` and upload to the OCS Edge server.
4. Copy the System Manager CA certificate to the OCS Edge server.
5. On the OCS Edge, run the management console, click **Start** > **Run**.
6. In the **Run** dialog box, enter `mmc` , and click **OK**.
7. On **MMC Console**, select **File** > **Add/Remove Snap-in** to launch the Add/Remove Snap-in wizard.
8. In the **Add/Remove Snap-in** dialog box, click **Add**.
9. On the **Standalone** tab, click **Add**.
10. In the **Add Standalone Snap-in** dialog box, select **Certificates** and then click **Add**.
11. In the **Certificates Snap-in** dialog box, select **Computer Account** and click **Next**.
12. In the **Select Computer** dialog box, select the default setting **Local Computer** and click **Finish**.
13. In the **Add Standalone Snap-in** dialog box, click **Close**. And then in the **Add/Remove Snap-in** dialog box, click **OK**.

    The system takes you to the MMC Console.
14. Click **Console Root**, select **Certificates** > **Trusted Root Certification Authorities**.
15. Select **Trusted Root Certification Authorities**, right-click **Certificates** and select **All Tasks** > **Import**.

The system launches the Certificate Import Wizard. Follow the steps of the wizard and browse for the `default-cacert.pem` file.

16. On the Certificate Import Wizard screen, click **Next**.
17. In the **Open** dialog box, click **Browse** to locate the file and then click **Next**.
18. Retain the default settings and then click **Next**.
19. Click **Finish** to complete the Certificates Import Wizard.
20. Verify the Certificate is in the `Certificates/Trusted Root Certification Authorities/ Certificates` list.
    a. Right-click **Certificates** and select **Refresh** to update the certificates list.

       The system might display the certificate as the default setting.
    b. Verify that the serial number and the expiry date of the System Manager certificate match the serial number and the expiratory date of the new default certificate that appears in the certificate list on the Edge server.
    c. To determine the serial number and expiry date of the System Manager certificate, enter the following command on the Presence Services Server: `openssl x509 -in $PRES_HOME/jabber/xcp/certs/default-cacert.pem -noout -text`.

       The details of this certificate must match the default certificate added to Edge server.
    d. To determine if the certificate was added, double-click the certificate in the list of certificates.

       If the system does not display a default certificate, then the Presence Services CA Certificate has not been added to the OCS Edge server's Trusted Root Certificates.

Note:

The default-cacert.pem is the name given to the System Manager CA certificate when the system downloads the from the System Manager security management page.

Generating and importing certificate for Lync

Generating a Web server certificate with server and client authentication

About this task

The certificate that the Edge server external interface uses must have server and client authentication. If not, generate a certificate with server and client authentication and assign the certificate to the Edge server external interface.

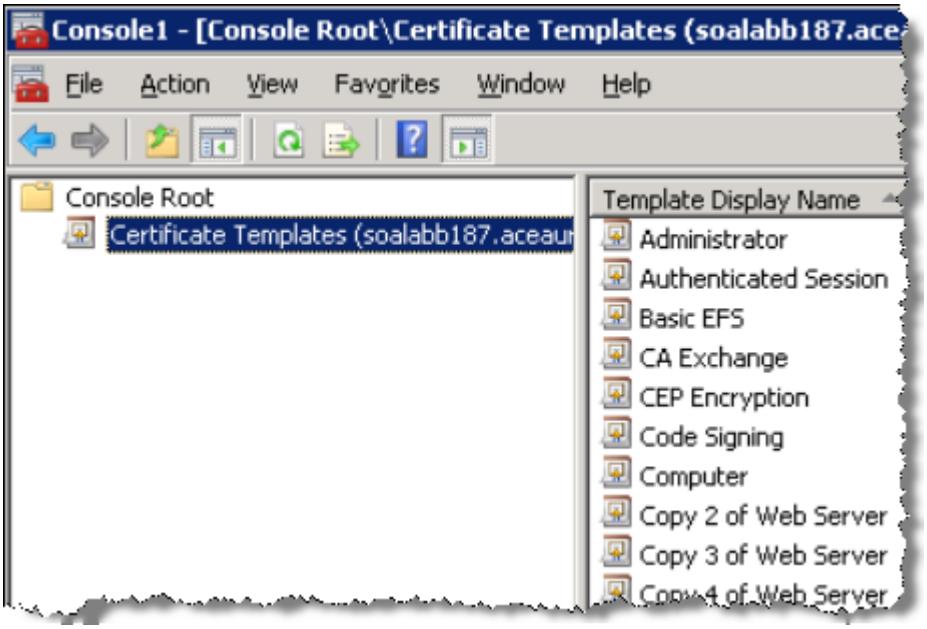
To create a certificate for external interface using Microsoft Certificate Authority (CA) in a Windows 2008 Enterprise Edition Server running a standalone Microsoft Enterprise CA:

Note:

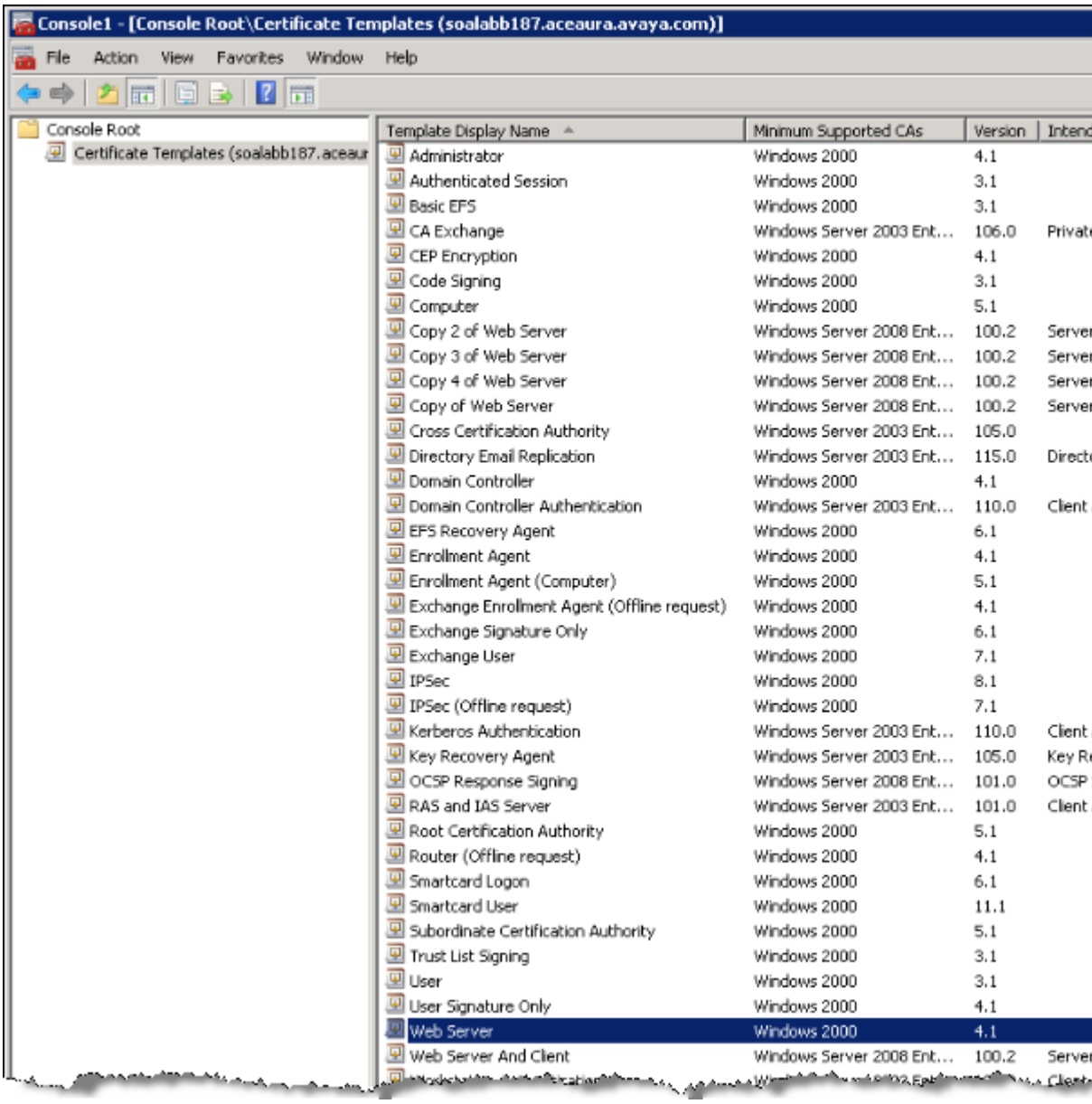
The procedure may vary depending on the configuration and setup of your Microsoft CA.

Procedure

1. Expand **Console Root** and click **Certificate Templates**. The system displays a list of template display names.



2. From the Template Display Name list, right-click **Web Server** and then click **Duplicate Template**.

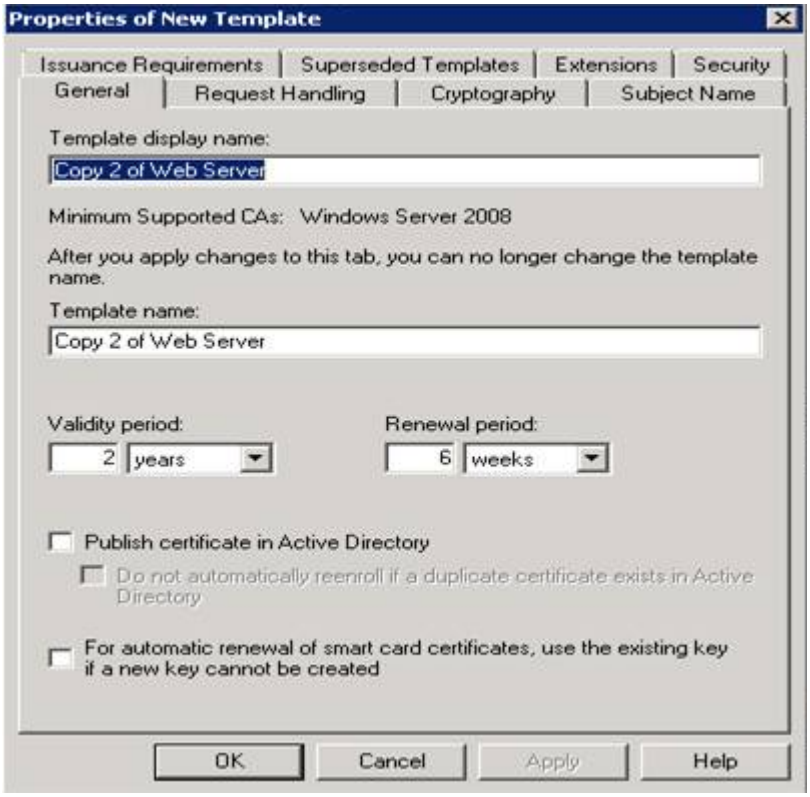


The system displays the Duplicate Template dialog box.

3. On the Duplicate Template dialog box, select the **Windows Server 2008, Enterprise Edition** option.

The system displays the Properties of New Template dialog box.

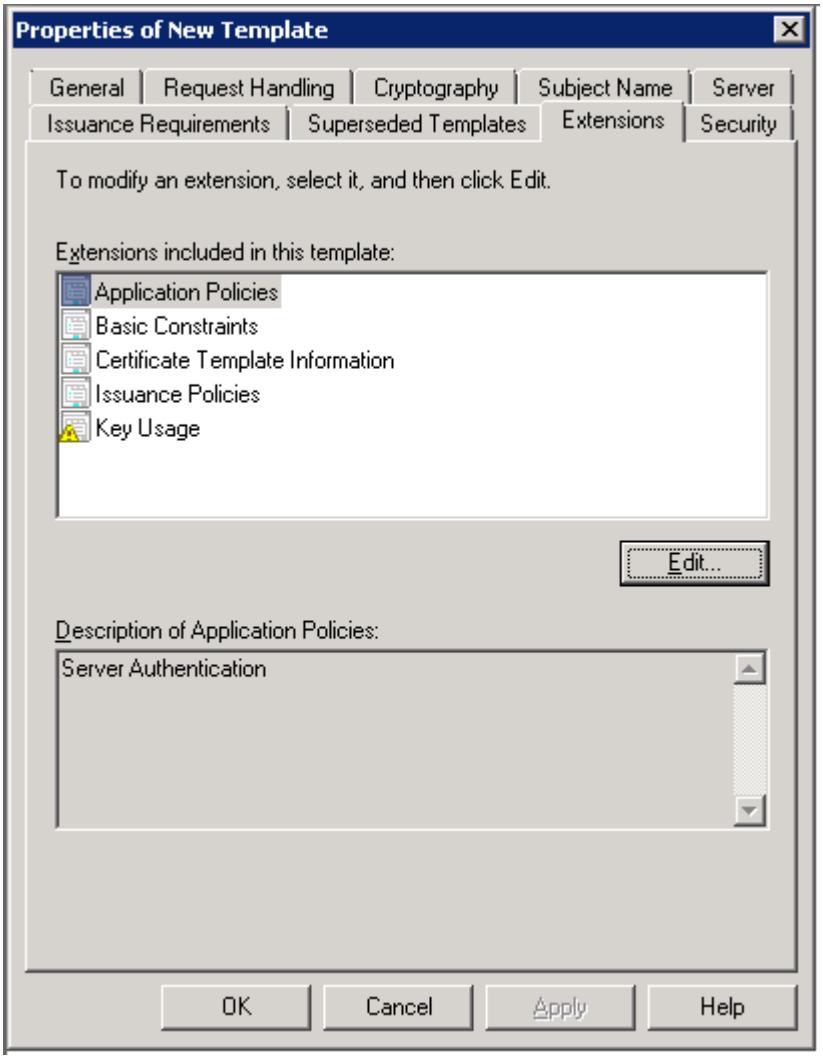
4. In the Properties of New Template dialog box, on the **General** tab, in the **Template display name** and **Template name** field, enter a display name for the template.



Note:

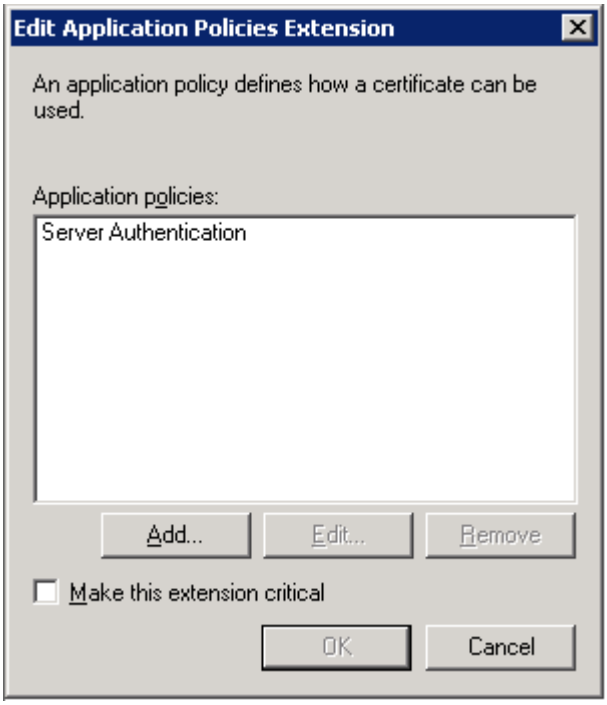
You must use the default entry for the Template name field.

5. On the **Extensions** tab, under the **Extensions included in this template** list, select **Application Policies**, and then click **Edit**.



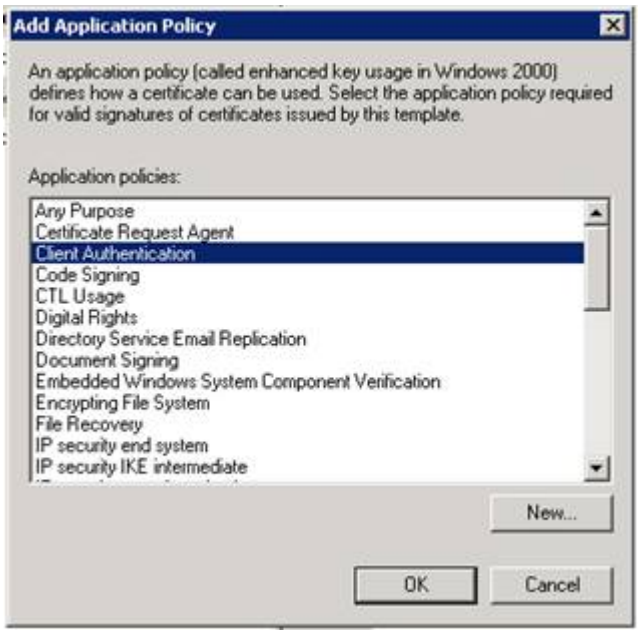
The system displays the Edit Application Policies Extension dialog box.

6. On the Edit Application Policies Extension dialog box, click **Add**.



The system displays the Add Application Policy dialog box.

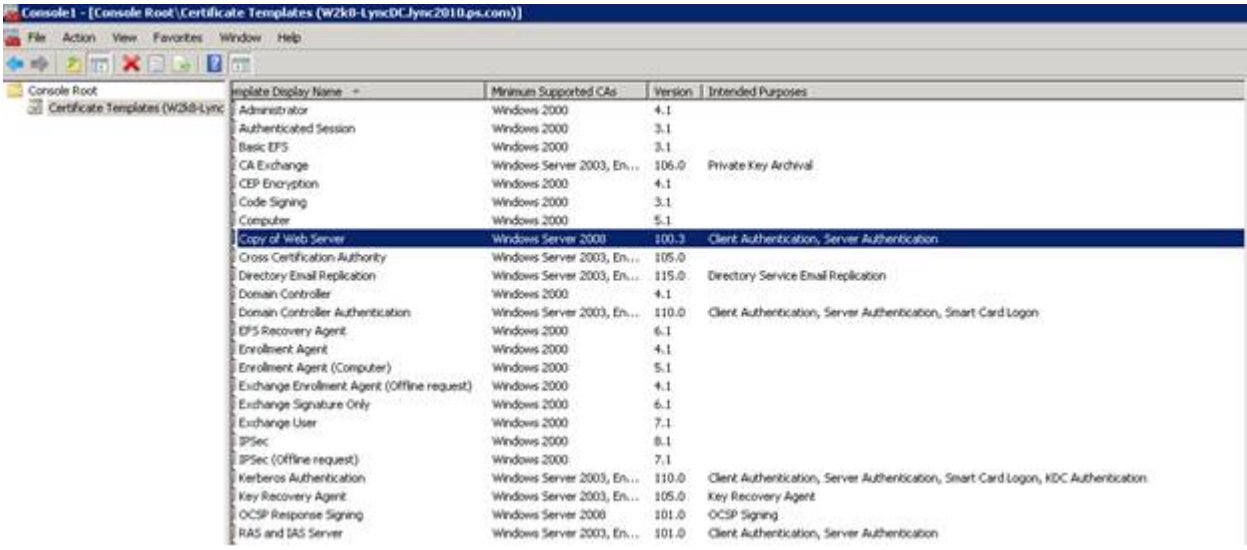
7. On the Add Application Policy dialog box, from the Application policies list, select **Client Authentication**, and then click **OK**.



8. Click **Apply**, and then click **OK**.

Next steps

Verify the newly added duplicate Web server certificate in the Certificate Templates list.



Importing the System Manager default CA certificate into the Lync Edge Trust Store

Procedure

1. Log in to the System Manager Web interface.
2. Click **Security** > **Certificates** > **Authority**.
3. Click **Download pem file**. Save the pem file with an appropriate name, for example, `default-cacert.pem` and upload to the Lync Edge server.
4. Copy the System Manager CA certificate to the Lync Edge server.
5. On the Lync Edge, run the management console, click **Start** > **Run**.
6. In the **Run** dialog box, enter `mmc` , and click **OK**.
7. On **MMC Console**, select **File** > **Add/Remove Snap-in** to launch the Add/Remove Snap-in wizard.
8. In the **Add/Remove Snap-in** dialog box, click **Add**.
9. On the **Standalone** tab, click **Add**.

10. In the **Add Standalone Snap-in** dialog box, select **Certificates** and then click **Add**.
11. In the **Certificates Snap-in** dialog box, select **Computer Account** and click **Next**.
12. In the **Select Computer** dialog box, select the default setting **Local Computer** and click **Finish**.
13. In the **Add Standalone Snap-in** dialog box, click **Close**. And then in the **Add/ Remove Snap-in** dialog box, click **OK**.

    The system takes you to the MMC Console.
14. Click **Console Root**, select **Certificates** > **Trusted Root Certification Authorities**.
15. Select **Trusted Root Certification Authorities**, right-click **Certificates** and select **All Tasks** > **Import**.
    The system launches the Certificate Import Wizard. Follow the steps of the wizard and browse for the `default-cacert.pem` file.
16. On the Certificate Import Wizard screen, click **Next**.
17. In the **Open** dialog box, click **Browse** to locate the file and then click **Next**.
18. Retain the default settings and then click **Next**.
19. Click **Finish** to complete the Certificates Import Wizard.
20. Verify the Certificate is in the `Certificates/Trusted Root Certification Authorities/ Certificates` list.
    a. Right-click **Certificates** and select **Refresh** to update the certificates list.

       The system might display the certificate as the default setting.
    b. Verify that the serial number and the expiry date of the System Manager certificate match the serial number and the expiratory date of the new default certificate that appears in the certificate list on the Edge server.
    c. To determine the serial number and expiry date of the System Manager certificate, enter the following command on the Presence Services Server: `openssl x509 -in $PRES_HOME/jabber/xcp/certs/default-cacert.pem -noout -text`.

       The details of this certificate must match the default certificate added to Edge server.
    d. To determine if the certificate was added, double-click the certificate in the list of certificates.

       If the system does not display a default certificate, then the Presence Services CA Certificate has not been added to the Lync Edge server's Trusted Root Certificates.

Note:

The default-cacert.pem is the name given to the System Manager CA certificate when the system downloads the from the System Manager security management page.

DNS Administration

Adding a DNS SRV record for the OCS Gateway

On the DNS for the Microsoft domain, which is the DNS server that Edge server uses, the FQDN of the Presence Services specified in the network address in the IM provider section must be resolvable. You must also add a DNS SRV record for the Presence Services server (OCS Gateway).

You must create the DNS records that meet the following criteria:

1. When Presence Services contacts Edge server, Presence Services provides a certificate that contains the Presence Services FQDN. Ensure that this FQDN is resolvable in the DNS of the OCS.
2. The Edge server performs a DNS lookup on the Presence Services FQDN. The Edge server rejects the TLS connection request with Presence Services if the DNS server does not return the same FQDN as in the certificate.
3. The Edge server performs a reverse DNS lookup on the IP address of Presence Services. The Edge server rejects TLS connection request with Presence Services if the DNS server does not return the same IP address as in the certificate.
4. The OCS Edge server performs a SRV DNS lookup for the SRV record `_sipfederationtls._tcp.<PS domain>`. The PS domain is also referred to as the Router Service Name. PS domain is the domain part of the SIP URI in a SIP request originating from the Presence Services server. It gets the SIP domain from the name of the Presence Services user requesting the subscription. In this case, the SIP domain is the Presence ID domain of the Presence Services server.

   Note:

   If the firewall on Microsoft Edge server is on, update the firewall so that the Presence Services server can gain access to port 5061 on the Edge server.

   For examples on creating the required DNS entries, see *Example DNS SRV settings with Windows*.

Adding New Host (A)

Procedure

1. On the OCS DNS server, right-click the domain that you just created and select **New Host (A)**.
2. In the New Host dialog box, enter the Presence Services server name and IP address. For example, `ipsdemo-ips1.ipsdemo.com`.
3. Click **Add Host** > **Done**.

Note:

When you add New Host (A) in DNS, check the associated pointer. This associated pointer may eliminate the need to add the machine name to the Reverse Lookup Zone if that zone already exists.

Adding a new reverse pointer

Procedure

1. On the OCS DNS server, in the left navigation pane, select **Reverse Lookup Zones** > **New Zone**.
2. To add a new zone, on the **Action** menu, click **New Zone** > **Next**.
3. Select **Primary zone** and **Store the zone in Active Directory**.
4. Click **Next**.
5. Select **To all DNS servers in the Active Directory domain ...**.
6. Click **Next**.
7. Enter the `Network ID` corresponding to the Presence Services server, and click **Next**.
8. Select **Allow both non-secure and secure dynamic updates**, and click **Next**.
9. Click **Finish**.
10. Right-click on the new zone you just created and select **New Pointer (PTR)...**.
11. In the **Host IP number** field, enter the Host IP number of the Presence Services server.
12. In the **Host Name** field, enter the Host Name of the Presence Services server.

13. Click **OK**.

Adding OCS Gateway as an IM service provider for Microsoft OCS

Procedure

1. Click **Start** > **All Programs** > **Administrative Tools** > **Computer Management**.
   The system displays the Computer Management window.
2. In the left navigation pane, expand **Services and Applications** and then select **Microsoft Office Communications 2007**.
3. Right-click **Microsoft Office Communications 2007** > **Properties**.
4. On the **IM Provider** tab, click **Add**.
   Enter details in the following fields:
   - **IM service provider name**: This name must match the Presence ID domain name used by the Presence Services server. For example, `ipsdemo.com`
   - **Network address of the IM service provider Access Edge**: This address must match the hostname of the Presence Services server. For example, `ipsdemo-ips1.ipsdemo.com`.
   - **This is a public IM service provider**: Do not clear this field.
   - **Allow all communications from this provider**: Select this option for filtering incoming communication.
5. Click **OK**.

Adding OCS Gateway as an IM service provider for Lync

Procedure

1. On the Lync Front End Server, click **Start** > **All Programs** > **Microsoft Lync Server 2010** > **Micrsoft Lync Server Control Panel**.
2. Log in as a user from Active Directory, who is a member of the CSAdministrator group. (The user account cannot be the local administrator of the server running Lync Server 2010, Standard Edition) You may need to add a user to the CSAdministrator group, and if that user is currently logged on, log them off and on again to register the group membership update.
3. Under External User Access, click **Provider**.

4. Click **New** > **Public Provider**.
5. Ensure that you select the Enable communications with this provider check box.
6. Specify the JID domain name that the Presence server uses for Provider and the Presence Server FQDN for the Access Edge (FQDN).
7. Click **External User Access** > **External Access Policy**.
8. Select the global policy and click **Edit**.
9. Ensure that you select the following:
    - Enable communications with federated users
    - Enable communications with remote users
    - Enable communications with public users
10. Ensure that you select the following:
    - Enable federation
    - Enable partner domain discovery
    - Enable remote user access

Enabling an OCS user for remote access and federation

Procedure

1. Click **Start** > **All Programs** > **Administrative Tools** > **Microsoft Office Communications Server 2007 R2**.
2. Right-click **Forest** and select **Properties** > **Global Properties**.
   The system displays the **Office Communications Server Global Properties** dialog box.
3. On the **Federation** tab, select **Enable Federation and Public IM connectivity**.
4. In the **FQDN** field, enter the external FQDN of the OCS Edge server.
5. In the **Port** field, enter `5061`.
6. Click **Start** > **All Programs** > **Administrative Tools** > **Active Directory Users and Computer**.
7. In the left navigation pane, click **Users**.
8. Double-click an enterprise user.
   The system displays the **Properties** dialog box of the selected user.
9. In the **Properties** dialog box of the user, click the **Communications** tab, and then click **Configure…** next to Other settings.

10. In the **Other Options** dialog box:
    a. Select **Enable federation**
    b. Select **Enable remote user access**
    c. Select **Enable public IM connectivity**
    d. Click **OK**
    e. Click **OK**
11. Repeat the steps for all other OCS users.

Enabling a Lync user for remote access and federation

Procedure

1. On the Lync Front End Server, click **Start** > **All Programs** > **Microsoft Lync Server 2010** > **Lync Server Control Panel** and gain access as a CSAdministrator group user.
2. In the left navigation pane, click **Users**.
3. In the **Provided Search Filter** field, enter all or part of the name of an Active Directory user that you want to enable for Lync.
4. In the search results displayed, select a user you want to enable and click **Edit**.
5. Ensure that you select **Enable for Lync Server** check box, and in the **SIP address** field, enter the login handle for the user, selecting the enterprise SIP domain from the drop-down.
6. Ensure that system defaults the Registrar pool field to the Lync Front End pool.
7. For Telephony, select **PC-to-PC only**.
8. For External Access Policy, select from the following choices:
    - Global: Ensure this policy is correctly set to allow federation as described in an earlier section.
    - Custom policy: Ensure that you enable Federation, Public, and Outside Access.
9. For all other policy fields, select **Automatic**.
10. Repeat the steps for all other users you want to enable for Lync remote access and federation.

Restarting the Edge server service after completing changes to DNS

About this task

The Edge server hold a cache of DNS information. Restart Edge server if you have entered an incorrect DNS entry. You must recreate the entry to prevent Edge server from storing the incorrect DNS records.

Procedure

1. On the Microsoft Edge Server, click **Start** > **Administrative Tools** > **Services**.
2. Locate the Office Communications Server Access Edge service.
3. Right-click **Office Communications Server Access Edge** service and select **Start** > **Start all stopped Services**.

Presence Services Trust Management for OCS integration

Downloading the CA that signed the certificate for the External Interface of the Edge server

About this task

You must add the CA, which signed the certificate that the External Interface of the Edge server uses, to the Presence Services list of trusted CAs. Download the CA from a standalone Microsoft Enterprise Certificate Authority and convert the CA to a format that you can use on Presence Services.

Procedure

1. From a Microsoft server, enter `http://<CA_Machine>/certsrv/` in the address bar.
   The system displays the Web enrollment page of the Certificate Authority.
2. On the Web enrollment page, click **Download a CA certificate, certificate chain, or CRL** > **Download CA certificate chain** > **Save**.
3. In Windows Explorer, double-click the `filename.p7b` file.
   The system displays a Certificates window.
4. In the left pane of the Certificates window, click the file name.

5. Click the **Certificates** folder.
   The system displays a list of certificates.
6. Select a certificate to convert to the PEM format.
7. Right-click the certificate, then select **All Tasks** > **Export** to display the Certificate Export wizard.
8. On the Certificate Export wizard, click **Next**.
9. Select the **Base-64 encoded X.509 (.CER)** option.
10. Click **Next**.

    Base-64 encoded is the PEM format.
11. In the **File name** field, enter a name for the converted digital certificate.
12. Click **Next**.
13. Copy the Microsoft root CA to any location on Presence Services. For example, `/opt/Avaya/Presence/jabber/xcp/certs` or `$JABBER_HOME/certs`.
14. Run **dos2unix <msroot>.cer**.
15. Run **$PRES_HOME/presence/bin/prescert addTrusted pem<msroot>.cer alias <optional name>**.

Adding a SIP Gateway domain to the Presence Services Global Router Configuration

About this task

When the Presence Services server receives presence subscriptions from the OCS domain, the subscriptions are subject to authorization rules, and the Presence Services server applies the ACL controls to the subscription. As the subscribing user is effectively an external user that is external to Avaya Aura® and external to Presence Services, by default, the system treats the authorization as a CONFIRM ACL. To apply this CONFIRM policy, Presence Services server must recognize the OCS domain. Therefore, you must add the OCS domain to the SIP Gateway Domain list in the Presence Services global router configuration.

Procedure

1. Log in to the XCP Controller Web interface.
2. On the home page, scroll to the Core Router and click the **Edit** link. The system displays the Global Settings Configuration page.
3. In the SIP Gateway Domains section, select the **SIP Gateway Domain(s)** check box, if not already selected, and add the OCS domain to the SIP Gateway Domain.

Stopping the Presence Services server

Avaya recommends that you use a script instead of the Presence Services Web GUI to stop the entire Presence Services system.

Before you begin

Before you stop Presence Services, you must have an instance of Presence Services running on your server.

About this task

The purpose of this task is to terminate the activity of Presence Services.

Procedure

To stop Presence Services, run **`/opt/Avaya/Presence/presence/bin/stop.sh`**

Note:

You can use this script to stop jadderd.

Starting the Presence Services server

Avaya recommends that you use a script instead of the Presence Services Web GUI to start the entire Presence Services system.

Before you begin

Before you start Presence Services, you must have an instance of Presence Services on your server that is not currently running.

About this task

The purpose of this task is to start or restart the activity of Presence Services.

Procedure

To start Presence Services, run **`/opt/Avaya/Presence/presence/bin/start.sh`**

Note:

You can use this script to start jadderd.

Verifying the trust configuration

Procedure

1. Log in to the OCS Edge server.
2. On the prompt, run `nslookup <FQDN of Presence Services>`. The system returns the IP address of the Presence Services server.
3. Run nslookup <IP Address of Presence Services>. The system returns the FQDN of the Presence Services machine and port 5061.
4. Log in to the Presence Services server and use the presstatus tool, which is located in the /opt/Avaya/Presence/presence/bin directory, to see the status of the Microsoft Office Communications Server Integration component.
5. Run the /opt/Avaya/Presence/presence/bin/prescert list command and ensure that the OCS CA certificate is in the trust store.
6. On the Presence Services server, enable the logging for RTC Collector in /opt/Avaya/Presence/presence/lib/path/log4j.xml and look into the output log file at /var/log/presence/presence-container-1.presence_local.log. For more information on disabling the logging for RTC Collector, see the *Troubleshooting Avaya Aura® Presence Services 6.1 guide*.

Adding Microsoft OCS SIP user handles or RTC handles to System Manager

Procedure

1. Log in to the System Manager Web interface as an administrator.
2. On the System Manager Dashboard, click **User Management** > **Manage Users**.
3. On the User Management page, select the relevant user and click **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. On the Communication Profile page, click **New** in the Communication Address section.
6. From the **Type** drop-down list box, select **Microsoft OCS SIP**.
7. In the **Fully Qualified Address:** field, enter the handle and domain details.

   For example, in the **Handle** field, enter `sip:handle` and in the **Domain** field, enter `ocsdomain.com`.

8. Click **Add**.

Changing the Cipher Suite Order

An issue was identified in Windows Server 2008 while establishing a communication between the Lync Edge and an external provider through Public Internet Cloud (PIC). The initial SSL dialog established between the Presence server and Lync Edge needs to use a different cipher suite in place of the default cipher suite in Windows Server 2008. This requires modifying the Cipher Suite Ordering on the Windows Server on which you deploy the Lync Edge. You must use the `TLS_RSA_WITH_RC4_128_MD5` cipher suite.

Procedure

1. On the Windows Server 2008 (x64) Edge server, click **Start** > **Run** > **gpedit.msc** > **OK**.
2. In the Group Policy Object Editor, click **Computer Configuration** > **Administrative Templates** > **Network**.
3. Under Network, click **SSL Configuration**, and then double-click **SSL Cipher Suite Order** (by default, the SSL Cipher Suite Order is set to **Not Configured**)
4. Select the **Enable** radio button.
5. From the SSL Cipher Suites text box, copy the entire text from the SSL Cipher Suites text box to a Notepad. It should look like the following:
   TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA ,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TL S_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256,TLS_ECDHE_ECDSA_ WITH_AES_128_CBC_SHA_P384,TLS_ECDHE_ECDSA_WITH_AES_128_CB C_SHA_P521,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256,TLS_E CDHE_ECDSA_WITH_AES_256_CBC_SHA_P384,TLS_ECDHE_ECDSA_WIT H_AES_256_CBC_SHA_P521,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA _P256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,TLS_ECDHE_RS A_WITH_AES_128_CBC_SHA_P521,TLS_ECDHE_RSA_WITH_AES_256_CBC _SHA_P256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,TLS_ECDH E_RSA_WITH_AES_256_CBC_SHA_P521,TLS_DHE_DSS_WITH_AES_128_C BC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_ 3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_MD5,SSL_CK_RC4_128_ WITH_MD5,SSL_CK_DES_192_EDE3_CBC_WITH_MD5,TLS_RSA_WITH_NU LL_MD5,TLS_RSA_WITH_NULL_SHA

   You must move the `TLS_RSA_WITH_RC4_128_MD5` value to the beginning of the list.

6. In your Notepad, where you have copied the text from the SSL Cipher Suites text box, search for the `TLS_RSA_WITH_RC4_128_MD5` value and move it to the beginning of the list. It should look like the following:
   TLS_RSA_WITH_RC4_128_MD5,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P521,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P521,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA,SSL_CK_RC4_128_WITH_MD5,SSL_CK_DES_192_EDE3_CBC_WITH_MD5,TLS_RSA_WITH_NULL_MD5,TLS_RSA_WITH_NULL_SHA
7. Copy the recently formatted list back into the SSL Cipher Suites text field, click **OK**.
8. For the changes to take effect, restart the Windows Server 2008 (x64) Edge server.

Chapter 5: Troubleshooting

Enabling logging for RTC Collector

Procedure

1. Log in to the Presence Services server.
2. Make changes to the `/opt/Avaya/Presence/presence/lib/path/log4j.xml` file.
3. To enable the RTC Collector logs, enable the relevant section and change the level as required in log4j.xml.

   <logger

   name="events.operational.com.avaya.presence.server.RTCCollector">

   <level

   value="FINEST#com.avaya.common.logging.client.LogLevel"/>

   </logger>

Enabling logging for OCS Gateway

Procedure

1. Log in to the Presence Services server.
2. Once logged in, type the following command to log in as the root user: **su root**
3. Check the current log level, type `/opt/Avaya/Presence/jabber/xcp/bin/updateLogLevel.sh cm-2 –c`.

   Note:

   OCS Gateway logging is typically set at the WARN level. To diagnose any issue, you must increase the logging level to DEBUG.

4. To increase the logging level, type the following command until you reach the DEBUG level, `/opt/Avaya/Presence/jabber/xcp/bin/updateLogLevel.sh cm-2 –i`.
5. Check the filtering level of the syslog logger in the /etc/syslog.conf file.
6. Restart the logging service, type `Service syslog retstart` to restart service logging.

Note:

Service syslog sends the OCS Gateway logging to the /var/log/messages file. You can recognize the OCS Gateway records by the logging tag OCS_GW in each of the associated log output entries from the OCS Gateway. The system sends the debug level logging messages from the OCS Gateway to /var/log/messages and extracts these messages to assist in diagnosing any problems that you might encounter.

Changing the default logging level

Procedure

1. Log in to the Presence Services server.
2. Make changes to the `/opt/Avaya/Presence/presence/lib/path/log4j.xml` file.
3. Enable the relevant section and change the level as required.

```
    <logger name="events.operational">
        <level
    value="WARN#com.avaya.common.logging.client.LogLevel"/
    >
        </logger>
to, for example,
    <logger name="events.operational">
        <level
    value="INFO#com.avaya.common.logging.client.LogLevel"/
    >
        </logger>
```

Note:

The system generates more log records if you set a level lower. Do not set a low level for a long period of time. If you do, you will have to navigate through unwieldy log files. Set a lower log level for individual components as opposed to changing the default for the whole Presence server.

Note:

If the log level of a component is increased to the DEBUG level then you must change it back to the ERROR level as soon as the required debug logs are collected for debugging.

OCS server side logging

Starting SIP logging on OCS Edge

Procedure

1. Click **Start** > **Control Panel** > **Administrative Tools**.
2. Double-click **Computer Management**. The system displays the Computer Management page.
3. Click **Services and Applications** and then select **Microsoft Office Communications Server**.
4. Right-click **Microsoft Office Communications Server** and select **Logging Tool** > **New Debug**. The system displays the Microsoft Office Communications Server 2007 Logging Tool page.
5. From the Components list, select **SIPStack**.
6. Click **Start Logging**.

Starting SIP logging on OCS Server

Procedure

1. Click **Start** > **Control Panel** > **Administrative Tools**.
2. Double-click **Microsoft Office Communications Server 2007**. The system displays the Microsoft Office Communications Server 2007 page.
3. Click **Enterprise pools**.
4. Right-click **Pools** > **New Debug Session**.
5. From the **Components** list, select **SIPStack**.

6. Click **Start Logging**.

Enabling logging on the OCS server

Procedure

1. On the Microsoft Office Communications Server 2007 Logging Tool page, click **Stop Logging**.
2. Click **Analyze Log Files** or **View Log Files**.

   Note:

   - When you click **View Log Files**, the system displays the trace in the text mode.
   - When you click **Analyze Log Files**, the system displays the trace in the GUI mode.
3. In the Snooper GUI, check all the SIP trace messages.

Lync server side logging

Starting SIP trace on Lync Edge

Procedure

1. Click **Start** > **Microsoft Lync Server 2010** > **Lync Server Logging Tool**.
   The system displays the logging properties page, where you can select components and flags for the logging sessions.
2. From the Components list, select **SIPStack**.
3. Click **Start Logging**.

Starting SIP trace on Lync server

Procedure

1. Click **Start** > **Microsoft Lync Server 2010** > **Lync Server Logging Tool**.
   The system displays the logging properties page, where you can select components and flags for the logging sessions.
2. From the Components list, select **SIPStack**.
3. Click **Start Logging**.

Checking the SIP trace

Procedure

1. On the Microsoft Office Communications Server 2007 Logging Tool page, click **Stop Logging**.
2. Click **Analyze Log Files** or **View Log Files**.

   Note:

   - When you click **View Log Files**, the system displays the trace in the text mode.
   - When you click **Analyze Log Files**, the system displays the trace in the GUI mode.
3. In the Snooper GUI, check all the SIP trace messages.

Appendix A: Sample deployment configurations

RTC Collector configuration worksheet

The following table outlines a set of parameters that you must know before enabling an RTC collector:

Configuration parameter Name	Parameter value	Default value presented on the configuration screen
User Name		
PS SIP Domain [10]		The service router name configured during the installation
Transport		Tls
Port		45061
Expires		86400
Subscription Failure retry		3600
Server Failure retry		3600
Static Routes [11]		<OCS Domain><IP address of Presence Services><Port>
SIP SUBSCRIBE Contact FQDN [12]		-

[10] The system provides the Presence Services domain by default for this parameter. This equates to the Service Router Name that the system provides at the time of the Presence Services server installation.

[11] The static route configures the next hop destination for the SIP SUBSCRIBE. The next hop should be SIP Proxy. The system presents the IP address of Presence Services and the port 5061 by default for this parameter. The system administrator must complete this static route by preceding these two entry values with the OCS domain, for example, if the IP address of your Presence Services is 135.64.22.133 and the OCS domain is ipsdemo.com, then 135.64.22.133 5061 appears in the static route. Complete the static route by adding ipsdemo.com before the IP address to give a configuration of ipsdemo.com 135.64.22.133 5061.

[12] Select the “Define an optional external contact for SIP server to contact the RTC Collector” check box and then fill in the two associated configuration parameters: External host name that SIP server uses for contact and External port that SIP server uses for contact, with the FQDN of the Presence Services server and the port 5061 respectively. These values set the Contact header in the SIP SUBSCRIBE, which uses as the request URI in the NOTIFY request sent by the OCS server. The objective is that the system uses Contact address as the NOTIFY R-URI by the OCS server.

Configuration parameter Name	Parameter value	Default value presented on the configuration screen
SIP SUBSCRIBE Contact Port		-

OCS Gateway configuration worksheet

The OCS Gateway configuration worksheet identifies the set of configuration parameters that are when you enable an OCS Gateway. It is important that you know the values for the following parameters before starting the configuration process.

Configuration parameter Name	Parameter value	Default valued presented on the configuration screen
OCS Domain		
PS SIP Domain [13]		The service router name configured during installation, for example, pres.ipsdemo.com.
Transport		tls
Port [14]		
Expires		86400
Subscription Failure retry		3600
Server Failure retry		3600
PS IP address		
SIP Proxy Port [15]		
PS server FQDN		
SIP SUBSCRIBE Contact Port [16]		
TLS keystore full file path [17]		

[13] The Service Router Name solicited during the installation process is the Presence Services presence domain.

[14] The system provides a default port, 5061. You must change this port to a free port, typically to 65061. The convention for backend SIP servers is to use 5061 with an integer value from the set 1,2,3,4,5,6 prepended to create the port. Note that any value greater than 6 pushes the port value beyond the acceptable range of TCP ports.

[15] The SIP Proxy port is 5061.

[16] The contact port should be that of the SIP Proxy, that is 5061.

[17] Currently, TLS keystore full file path is `/opt/Avaya/Presence/jabber/xcp/certs/generic.pem.jabber`

Configuration parameter Name	Parameter value	Default valued presented on the configuration screen
TLS trust store full file path [18]		

[18] Currently, TLS trust store full file path is `/opt/Avaya/Presnce/jabber/xcp/certs/generic.trusts`

Appendix B: Process flow of a SIP Subscribe from the RTC Collector to Presence Services

Initiating a SIP subscribe from the RTC Collector to an OCS server

During the Presence Services installation, the Presence Services server interacts with System Manager to retrieve users and system level data. This data is stored in a local database, known as presence database. The user data that the Presence Services system retrieves from the presence database includes the communication handle of a user. For the RTC Collector to monitor and retrieve the OCS IM communication status of a user, then an RTC handle associated with an Aura user should be provisioned in System Manager. The RTC handle is instrumental in the retrieval of the OCS presence state of a user. When you enable and activate an RTC Collector, the RTC Collector obtains RTC handles provisioned for Presence Services users. The system then subscribes for the user's OCS presence using this handle. The following flow describes a successful subscribe request:

- RTC Collector is activated.
- RTC Collector reads configuration.
- RTC Collector initializes SIP stack.
- RTC Collector sets up RTC Subscriber User (RTC User and Presence Services SIP Domain parameters).
- RTC Collector creates presence fragment initialized to unknown presence.
- RTC Collector publishes initial presence fragment to ESC for aggregation and composition.
- RTC Collector creates SIP SUBSCRIBE using To address equal to RTC Handle of the user.
- RTC Collector sends SUBSCRIBE.
- SIP Proxy receives outbound SIP SUBSCRIBE to OCS.
- SIP Proxy applies SIP routing rules to ocs-domain from ps-domain.
- SIP Proxy resolves ocs-domain to OCS Edge server.

- SIP Proxy sends SIP SUBSCRIBE to OCS Edge server.
- OCS Edge server authenticates PS server and resolves OCS server for the OCS user.
- OCS server receives SIP SUBSCRIBE and sends a response.
- RTC Collector receives response and updates the subscribe state.
- OCS server delivers SUBSCRIBE request to a MOC user.
- MOC user authorizes request. OCS server sends SIP NOTIFY to OCS Edge server.
- OCS Edge server sends SIP NOTIFY to Presence Services SIP Proxy.
- SIP Proxy applies route rules for NOTIFY and To RTC Collector system user.
- RTC Collector receives NOTIFY.
- RTC Collector processes OCS PIDF body of NOTIFY extracts status, activities and publishes to ESC for aggregation.
- Presence Services Compositor creates a new composite PIDF presence document and applies Availability Calculation for a user.
- Presence Services distributes new composite PIDF presence document to authorized watchers.
- Presence Services sends SIP NOTIFY to SIP based watcher clients.
- Presence Services sends XMPP presence with embedded PIDF presence document to XMPP based watcher clients.

The presence that the system obtains from OCS through the RTC Collector is aggregated as a part of a composite presence for an Avaya Aura® user. This presence is made available to any authorized Avaya Aura® subscribing user or watcher. Aura users make a subscription for presence by subscribing to their resource list. This occurs when an Avaya Aura® user adds another Avaya Aura® user as a (user level) contact and sets the buddy flag for the contact. This flag indicates that the owner of the contact wishes to make a presence subscription to this contact. Once the system authorizes the subscription, the Presence Services server sends the composite presence for that contact to the subscribing user in a SIP NOTIFY. The composite presence document contains OCS presence of the contact user.

The SIP OCS Gateway component

Inbound requests

The inbound requests originate from the OCS/Lync and route through the OCS/Lync Edge server and the Presence Services SIP Proxy. The Presence Services SIP Proxy is instrumental in directing SIP requests from the OCS/Lync system to the OCS Gateway. You can achieve this through the routing rules defined in SIP Proxy. Inbound SIP requests are subject to routing

rules, which are defined on the To and From header fields of a SIP request. The inbound routing rules directs certain SIP requests originating from an OCS/Lync system to the OCS Gateway.

Outbound requests

The outbound requests are the SIP requests that the system initiates as a result of Avaya Aura® client initiated requests destined for an OCS/Lync enterprise user. These requests are processed by Presence Services and are routed internally through the OCS Gateway. In the current Presence Services implementation, these requests are XMPP requests that originates from an Aura client.

For example, an Avaya Aura® enterprise user logged on a 1XC-H.323 or 1XC-SIP client can click on a user in their contact list and initiate an IM with that peer enterprise user. The 1XC clients then indicates that the target user has two IM addresses: an Avaya Aura® XMPP handle and an OCS/Lync handle. If the initiating user selects the OCS/Lync handle, then the Avaya Aura® client sends an XMPP IM message to Presence Services and then Presence Services routes this IM message internally through the OCS Gateway. This is because the system configures the OCS Gateway to handle communications with the OCS/Lync domain and the address used in the request contains the OCS/Lync domain.

Outbound SIP requests route through a SIP Proxy of Presence Services, then to the OCS/Lync Edge, and then into the OCS/Lync server. The SIP communication is based on a federated deployment of Presence Services with OCS/Lync. The configuration on OCS/Lync Edge is for federated inter-working. Therefore, you must configure Presence Services for federation as an IM provider on the OCS/Lync Edge server.

Additionally, to establish TLS communications and achieve server authentication, it is necessary that the CA TLS/SSL certificate of the Certificate Authority, which signed the TLS/SSL certificates of Presence Services and OCS/Lync Edge, are imported into each of the trust stores on Presence Services and the OCS/Lync Edge respectively. With the appropriate Presence Server Host records and SRV records configured in the DNS service associated with the OCS/Lync Edge and the OCS/Lync server, you establish this trust relationship.

Use the following domains as an illustration:

- The PS domain is pres.ipsdemo.com
- The OCS/Lync domain is ipsdemo.com
- The PS server FQDN is ipsdemo-ips1.ipsdemo.com
- The OCS/Lync Edge server external FQDN is ipsdemo-winsrv2.glob.ipsdemo.com
- The OCS/Lync server is ipsdemo-winsrv1.glob.ipsdemo.com

If you are enabling the OCS Gateway during installation, then you must know the appropriate values for the following parameters on the Presence Services server:

- OCS/Lync Edge: The external FQDN of the OCS/Lync Edge server, for example, ipsdemo-winsrv2.glob.ipsdemo.com
- OCS/Lync SIP domain: The OCS/Lync domain, for example, ipsdemo.com
- OCS/Lync SIP Port: 65061

These parameters set up the OCS Gateway configuration together with the default settings for non-solicited parameters. You can also use these parameters to configure the OCS Gateway routing rules in the SIP Proxy.

The SIP Proxy plays an integral part in the processing of a SIP request that the system sends to the OCS/Lync server and in handling the SIP requests received from the OCS/Lync server to Presence Services. You must define routing rules in the SIP Proxy, which routes SIP requests to their appropriate destination servers. Two rules govern the flow of SIP requests to and from OCS/Lync:

- The outbound SIP (SUBSCRIBE, INVITE, ACK, NOTIFY) requests from Presence Services to OCS/Lync have a rule which specifies that if the To header is set to the OCS/Lync domain and if the From header is from the Presence Services domain, then you must apply the default SIP routing rule.
- The inbound SIP (SUBSCRIBE, INVITE, ACK, NOTIFY) requests have a rule which specifies that if the To header contains the Presence Services domain and the From header contains the OCS/Lync domain, then the request is to be routed to the OCS Gateway.
- The default SIP routing rules determine the destination IPS address of the target domain. This requires the configuring of a Host mapping in the Proxy. This Host mapping maps an OCS/Lync domain to the external FQDN of the OCS/Lync Edge server. The external FQDN of the OCS/Lync edge server must be resolvable and requires an entry in the /etc/hosts file.

Initiating a SIP SUBSCRIBE from the OCS server to Presence Services

A SIP SUBSCRIBE is initiated from the OCS server to an Avaya Aura® user when the OCS user adds the presence handle of an Avaya Aura® user to their buddy list. Following are the possible scenarios:

- Scenario 1: Avaya Aura® user is logged on the SIP client and the pending subscription notified in watcher information.
- Scenario 2: Avaya Aura® user is logged on an XMPP client (1XC-H323), and the pending subscription delivered in an XMPP subscribe packet.
- Scenario 3: Avaya Aura® user is logged on a legacy phone, and the pending subscription remains pending as the end user will not receive a notification of the pending subscription.

Avaya Aura® user is logged on the SIP 1XC client

- MOC/Lync user adds a presence handle of an Avaya Aura® user to the buddy list. The handle contains the Presence Services domain.
- OCS server sends SIP SUBSCRIBE from an OCS user to the presence handle of the Avaya Aura® user.
- DNS resolution routes the SIP SUBSCRIBE to OCS Edge server.
- OCS Edge server resolves the Presence Services domain to the Presence Services server host.
- OCS Edge sends SIP SUBSCRIBE to the Presence Services server (SIP Proxy).
- SIP Proxy authenticates the OCS Edge server during the TLS session creation.
- SIP Proxy receives SIP SUBSCRIBE from OCS-domain to Presence Services-domain.
- SIP Proxy applies routing rules and forwards SIP SUBSCRIBE to OCS Gateway.
- OCS Gateway sets up SIP session and sends 200 OK response.
- OCS Gateway internalizes the SIP SUBSCRIBE to an internal XMPP subscribe.
- Presence Services processes subscribe and sets up pending roster subscription.
- Authorization Manager checks ACLs, but as the From address is not an Avaya Aura® user, Authorization Manager checks the SIP Gateway Domain configuration. Subscribe is treated as CONFIRM and requires explicit user authorization.
- SIP Presence Services sends NOTIFY presence.winfo to Avaya Aura® SIP client with pending subscription.
- SIP Presence Services sends NOTIFY through Session Manager, using the Route Set created.
- SIP clients authorizes the subscribe using PUBLISH presence.wauth.
- SIP Presence Services sends a subscribed packet to authorize internal roster subscription.
- XMPP Roster is updated from pending to FROM.
- OCS Gateway receives subscribed packet and creates a 200 OK response.
- OCS Gateway sends 200 OK response to OCS Edge server through the SIP Proxy.
- SIP Proxy receives 200 OK response and forwards to OCS Edge on an existing connection.
- OCS Gateway creates NOTIFY status pending empty body.

- OCS Gateway sends NOTIFY to OCS Edge through SIP Proxy.
- SIP Proxy applies Outbound routing rules To OCS-domain From Presence Services-domain.
- SIP Proxy resolves OCS-domain to the OCS Edge server.
- SIP Proxy sends NOTIFY to the OCS Edge server.
- Composite presence of Aura user (subscriber) is generated for the OCS user.
- Composite presence sent to OCS Gateway.
- OCS gateway applies composite presence mapping policy and maps the Aura user's overall presence. This is the first activities element in the composite PIDF's person element into a single tuple PIDF document.
- OCS Gateway sends NOTIFY to the OCS user through a SIP Proxy, as per outbound proxy configured in OCS Gateway.
- SIP Proxy receives NOTIFY and applies routing rule: To OCS-domain From Presence Services-domain and routes request to OCS edge.
- OCS Edge resolves the NOTIFY and forward to the OCS server of the user.
- OCS server delivers presence to the MOC/Lync client of the user.

Internally, the SIP SUBSCRIBE for presence from OCS is managed as an XMPP Roster subscription, which is a permanent subscription. This remains extant until the subscription is explicitly removed, for example, a SIP SUBSCRIBE with a value, expires = 0. This value is translated internally to unsubscribe the request, and the XMPP roster subscription of the OCS user is removed.

Note:

The presence NOTIFY from the OCS Gateway is routed through the SIP Proxy. Ordinarily, this does not happen, but for the OCS Gateway, the outbound proxy configuration is set to create a next hop node as the SIP Proxy. An Aura SIP client is informed about a pending subscription through a watcher information notification. The authorization of the subscription is performed by sending a SIP PUBLISH on the presence.wauth package.

Avaya Aura® user is logged on the XMPP 1XC-H323 client

- MOC user adds a presence handle of an Avaya Aura® user to the buddy list. The handle contains the Presence Services domain.
- OCS server sends SIP SUBSCRIBE from an OCS user to the presence handle of the Avaya Aura® user.
- DNS resolution routes the SIP SUBSCRIBE to OCS Edge server.
- OCS Edge server resolves the Presence Services domain to the Presence Services server host.
- OCS Edge sends SIP SUBSCRIBE to the Presence Services server (SIP Proxy).
- SIP Proxy authenticates the OCS Edge server during the TLS session creation.
- SIP Proxy receives SIP SUBSCRIBE from OCS-domain to Presence Services-domain.
- SIP Proxy applies routing rules and forwards SIP SUBSCRIBE to OCS Gateway.

- OCS Gateway sets up SIP session and sends 200 OK response.
- OCS Gateway internalizes the SIP SUBSCRIBE to an internal XMPP subscribe.
- Presence Services processes subscribe and sets up pending roster subscription.
- Authorization Manager checks ACLs, but as the From address is not an Avaya Aura® user, Authorization Manager checks the SIP Gateway Domain configuration. Subscribe is treated as CONFIRM and requires explicit user authorization.
- Presence Services sends XMPP subscribe packet to XMPP client of the Avaya Aura®.
- Aura XMPP clients authorizes the subscribe sending an XMPP subscribed.
- XMPP Roster is updated from pending to FROM.
- OCS Gateway receives subscribed packet and creates a 200 OK response.
- OCS Gateway sends 200 OK response to OCS Edge server through the SIP Proxy.
- SIP Proxy receives 200 OK response and forwards to OCS Edge on an existing connection.
- OCS Gateway creates NOTIFY status pending empty body.
- OCS Gateway sends NOTIFY to OCS Edge through SIP Proxy.
- SIP Proxy applies Outbound routing rules To OCS-domain From Presence Services-domain.
- SIP Proxy resolves OCS-domain to the OCS Edge server.
- SIP Proxy sends NOTIFY to the OCS Edge server.
- Composite presence is generated for the OCS user.
- Composite presence sent to OCS Gateway.
- OCS Gateway applies composite presence mapping policy and maPresence Services Enterprise IM presence tuple to OCS PIDF. MaPresence Services highest priority tuple from composite PIDF.
- OCS Gateway sends NOTIFY to the OCS user through a SIP Proxy, outbound proxy configured in OCS Gateway.
- SIP Proxy receives NOTIFY and applies routing rule: To OCS-domain From Presence Services-domain and routes request to OCS edge.
- OCS Edge resolves the NOTIFY and forward to the OCS server of the user.
- OCS server delivers presence to the MOC client of the user.

Note:

The main difference between this flow and the SIP flow is that the subscribe packet is delivered to the Avaya Aura® XMPP client to indicate a pending subscribe. In the SIP case, the watcher information informs the client about a pending subscription.

Avaya Aura® user logged on a legacy phone

The subscription remains pending. The subscription is not authorized until the user logs on another device which can support the explicit authorization of the pending subscription.

Initiating an IM conversation from Presence Services to the OCS server

An Avaya Aura® user can initiate an IM conversation with another enterprise user by adding the user as a contact and then clicking on the IM icon on the Avaya Aura® client interface. This action renders the IM contact addresses for that contact user. If the system provisions an OCS handle for the Avaya Aura® user, then the system initiates an IM conversation using the OCS contact address. The flow of such an IM conversation is as follows:

- Avaya Aura® user clicks on the IM icon of the contact user and then selects an OCS handle.
- Avaya Aura® user types a message and presses Enter to send the message.
- Avaya Aura® client sends XMPP message from an Avaya Aura® presence handle to an OCS handle.
- Presence Services Connection Manager receives message and routes the message to the OCS Gateway.
- OCS Gateway sets up a SIP session.
- OCS Gateway sends an invite to an OCS user handle from the presence handle.
- SIP Proxy receives an invite and applies outbound routing rule To OCS-domain From PS-domain.
- SIP Proxy sends invite to the OCS Edge server.
- The OCS Edge server resolves the OCS user address and sends an invite to the OCS server.
- The OCS server sends an invite to the MOC/Lync client of an OCS user.
- The system accepts an IM conversation and sends 200 OK response to OCS Gateway through the OCS Edge server and SIP Proxy.
- OCS Gateway sends ACK to complete the offer/answer exchange.
- The system converts XMPP IM message into SIP MESSAGE.
- The system sends SIP MESSAGE to SIP Proxy.
- SIP Proxy applies outbound routing rules and sends SIP MESSAGE to the OCS Edge server.
- OCS Edge routes MESSAGE to the OCS server.
- The OCS server delivers MESSAGE to MOC/Lync client.

Initiating an IM conversation from the OCS server to Presence Services

A user on a MOC/Lync client can initiate an IM conversation with another Avaya Aura® user by using the presence handle of the Avaya Aura® user.

- MOC/Lync user clicks the Avaya Aura® presence user handle on the buddy list.
- MOC/Lync user types a message and presses Enter to send the message.
- MOC/Lync client sends SIP INVITE from the OCS user handle to the presence user handle.
- OCS Edge resolves the Presence Services domain to the Presence Services server host.
- OCS Edge sends SIP INVITE to SIP Proxy.
- SIP Proxy receives SIP INVITE and applies inbound routing rule To PS-domain From OCS-domain and sends SIP INVITE to OCS Gateway.
- OCS Gateway creates SIP session and sends 200 OK to complete the dialog.
- The OCS Edge server forwards ACK to SIP Proxy.
- SIP Proxy receives ACK and applies inbound routing rule To PS-domain From OCS-domain and sends SIP ACK to OCS Gateway.
- OCS Gateway receives ACK.
- The OCS Edge server forwards SIP INFO with a typing status to SIP Proxy
- SIP Proxy receives SIP INFO and applies inbound routing rule To PS-domain From OCS-domain and sends SIP INFO to OCS Gateway.
- OCS Gateway receives SIP INFO.
- OCS Gateway converts SIP INFO into XMPP message with chat state notification is composing.
- OCS Gateway sends an XMPP message to an Avaya Aura® user XMPP IM session.
- Presence Services Connection Manager forwards XMPP is composing message to the client of the Avaya Aura® user.
- OCS Edge server forwards SIP MESSAGE to SIP Proxy.
- SIP Proxy receives SIP MESSAGE and applies inbound routing rule To PS-domain From OCS-domain and sends SIP MESSAGE to OCS Gateway.
- OCS Gateway receives SIP MESSAGE.
- OCS Gateway converts the SIP MESSAGE to an XMPP message.

- OCS Gateway sends an XMPP IM message to the XMPP IM session of the Avaya Aura® user.
- Presence Services Connection Manager forwards XMPP is composing message to the client of the Avaya Aura® user.

Index

R

S

T

U

V

W