



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Microsoft Office Communicator R2 Client integration with Avaya one-X® Portal and Intelligent Presence Server - Issue 1.0**

### **Abstract**

These Application Notes describe the process of displaying presence information for the Microsoft Office Communicator R2 clients on the Avaya one-X® Portal clients. Presence information is sent to the Avaya one-X® Portal client using the Avaya Intelligent Presence Server (IPS). The configuration described herein uses a Microsoft Edge server deployment for relaying presence between the Microsoft Office Communicator (OCS) R2 clients and the Avaya one-X® Portal clients. Presence notifications from the Microsoft OCS R2 clients are routed through the Microsoft Real Time Communicator (RTC) component; this component is installed on the Microsoft Office Communicator Server (OCS) and subscribes to presence information received by the OCS from the Microsoft Edge server.

Note: The terms user and client are used interchangeably throughout this document and refer to the same entity.

# 1. Introduction

These Application Notes describe the steps involved in displaying presence information between a Microsoft Office Communicator R2 client and Avaya one-X® Portal Clients using an Avaya Intelligent Presence Server. The Microsoft Office Communicator servers and the Avaya components are placed in separate domains. As shown in **Figure 1**, the ‘OCS’<sup>1</sup> domain consists of the Microsoft Office Communicator server, Domain Controller, Microsoft Office Communicator R2 client server and an SQL server. The Domain controller maintains an (Active Directory) list of Microsoft Office Communicator R2 users (clients) and Avaya one-X® Portal clients; these users are collectively grouped under the Enterprise User folder. The list of Enterprise Users is accessed by Avaya one-X® Portal from another domain via a Microsoft Edge server. The Edge server’s internal network interface is added to the Microsoft Office Communicator setup ‘OCS’ domain and the external network interface are configured in the ‘Avaya’<sup>2</sup> domain (Avaya One X Portal and Intelligent Presence server). The Edge server Access Edge service is used to route packets between the internal and external interfaces of the Edge server. Refer to [1] for information on installing a Microsoft Edge server. A Microsoft RTC collector is installed on the Microsoft Office Communications server and subscribes to the Microsoft Office Communicator Server (OCS) via the Microsoft Edge Server for presence notifications of Microsoft Office Communicator (MOC) clients. The RTC collector uses the MS federation protocol to communicate with the Microsoft Office Communication Server via the MS Edge Server. Refer to [2] for information on installing and configuring RTC collector<sup>3</sup> on the Microsoft Office Communication server. The configuration described herein only consists of an Avaya one-X® Portal and Intelligent Presence server in the ‘Avaya’ domain. The Avaya one-X® Portal is configured to access the Enterprise User list mentioned above; a connection to the Intelligent Presence Server is also established to relay presence information between the Microsoft Office Communicator R2 users and Avaya one-X® Portal users. These Application Notes describe the process of displaying presence information from Microsoft Office Communicator R2 users in an Avaya one-X® Portal client for a given user<sup>4</sup>.

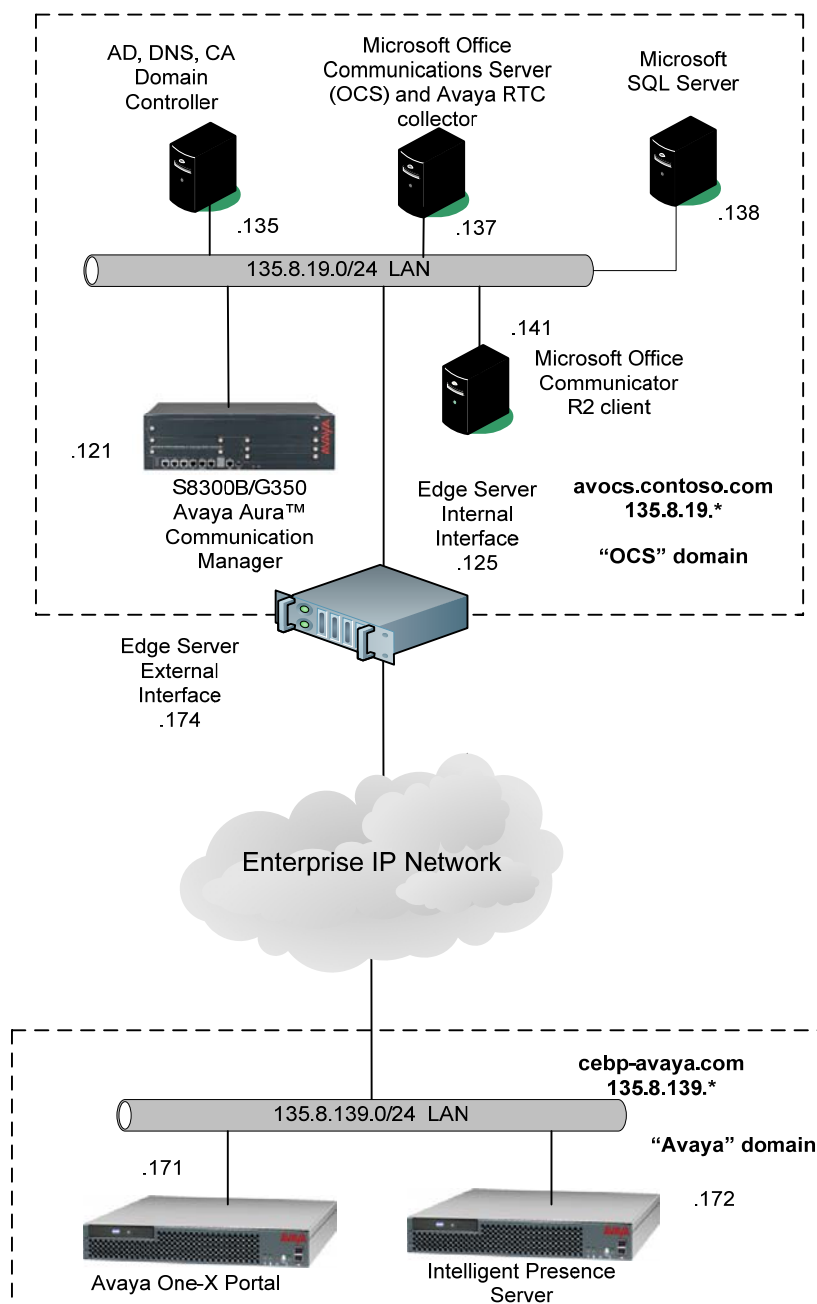
---

<sup>1</sup> The ‘OCS’ domain name used in this document is ‘avocs.contoso.com’

<sup>2</sup> The ‘Avaya’ domain name is ‘cebp-avaya.com’

<sup>3</sup> RTC Collector is provided with the Intelligent Presence Server installation package.

<sup>4</sup> The Intelligent Presence Server does not distribute presence information for Avaya one-X® Portal clients to Microsoft Office Communicator R2 users.



**Figure 1: Network Configuration for Avaya one-X® Portal and Intelligent Presence Server integration with Microsoft Office Communicator (MOC) R2 client**

## 2. Equipment and Software Validated

**Table 2** displays the equipment and software used for the sample configuration provided:

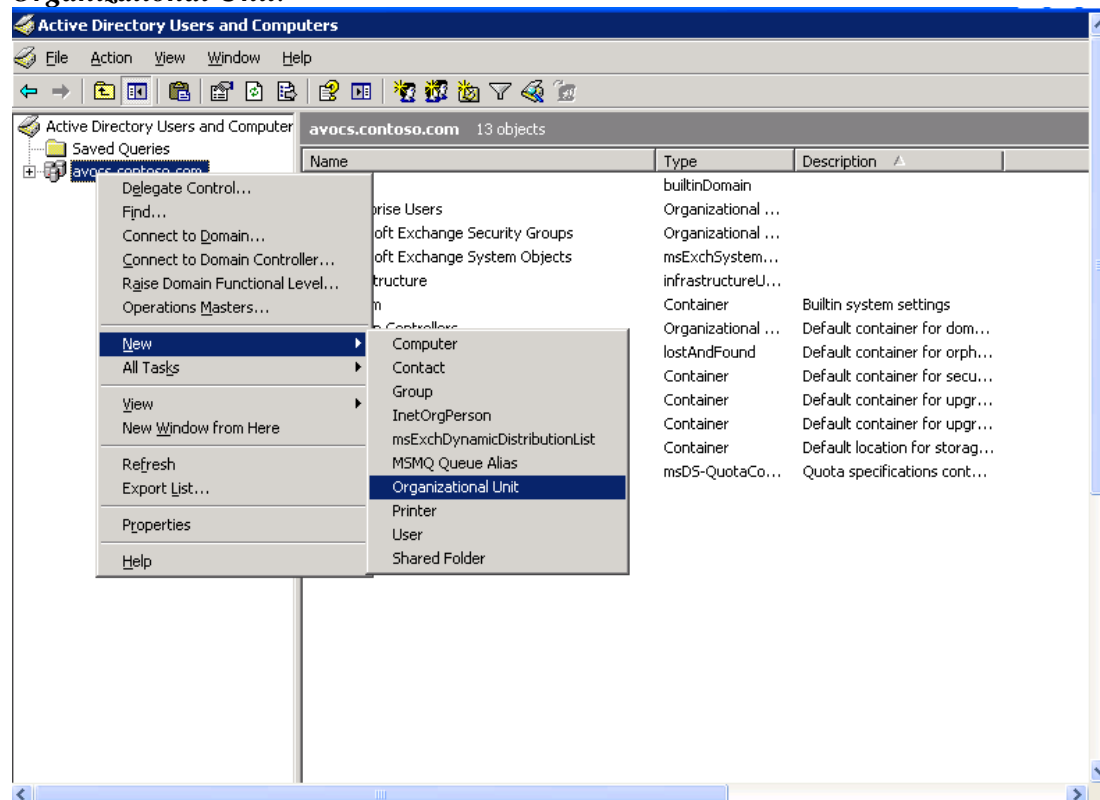
Equipment & Software	Version
Avaya S8300 Server	Avaya Aura™ Communication Manager 5.2 (R015x.02.0.947.3)
Avaya G350 Media Gateway	-
Media Gateway Processor	26.33.0
Avaya 9600 Series H.323 IP Telephones	2.0 (9630) 2.0 (9650)
Avaya 9600 Series SIP IP Telephones	2.0.5 (9640) 2.4.1 (9630)
Microsoft Active Directory, DNS Server, and Certification Authority on Microsoft Windows Server 2003 R2 Enterprise Edition Service Pack 2	5.2.3790.3959
Microsoft Exchange 2007 Server on Microsoft Windows Server 2003 R2 Enterprise x64 Edition Service Pack 2	08.01.0240.006
Microsoft Office Communications Server 2007 on Server 2003 R2 Enterprise Edition Service Pack 2	3.5.6907.0
Microsoft SQL 2005 Server on Microsoft Windows Server 2003 R2 Enterprise Edition Service Pack 2	2005.090.3042.00
Microsoft Mediation Server on Microsoft Windows Server 2003 R2 Enterprise Edition Service Pack 2	3.5.6907.0
Microsoft Office Communicator on Microsoft Windows XP Professional Version 2002 Service Pack 2	2.1.0.70
Avaya one-X® Portal	1.1.0.0.159
Avaya Intelligent Presence Server	1.0

**Table 1 Equipment and software used in the configuration**

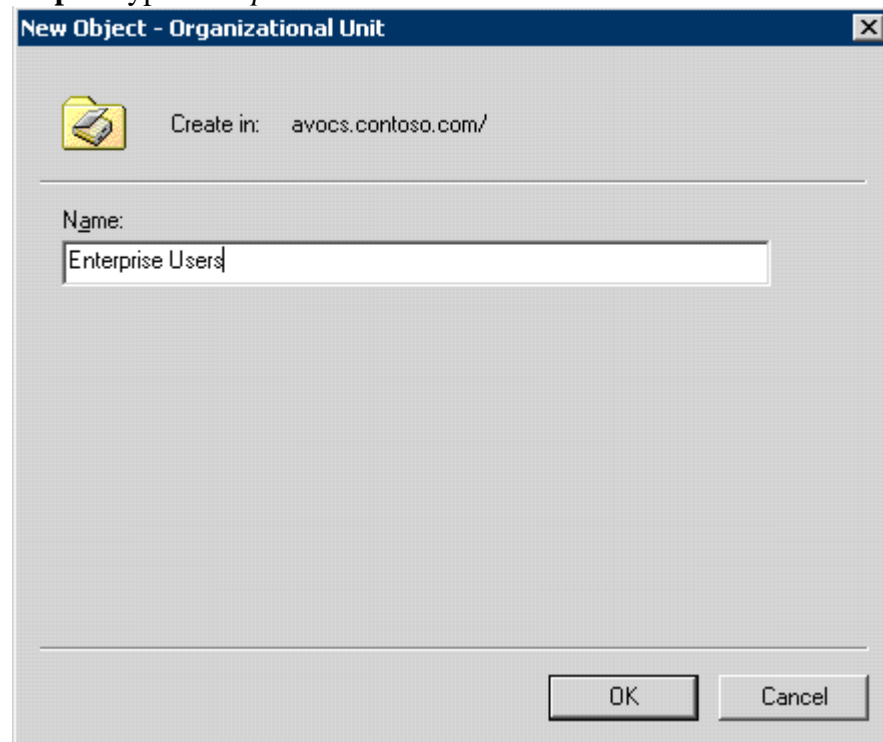
### 3. Assign Enterprise Users in Microsoft Active Directory

These Application Notes assume that basic Microsoft Office Communication Server installation and configuration have already been performed according to the guidelines provided in [3], [4], [5] and [6]. These Application Notes further assume that user accounts have been created in Microsoft Active Directory (Domain Controller) and enabled for Microsoft Office Communication Server.

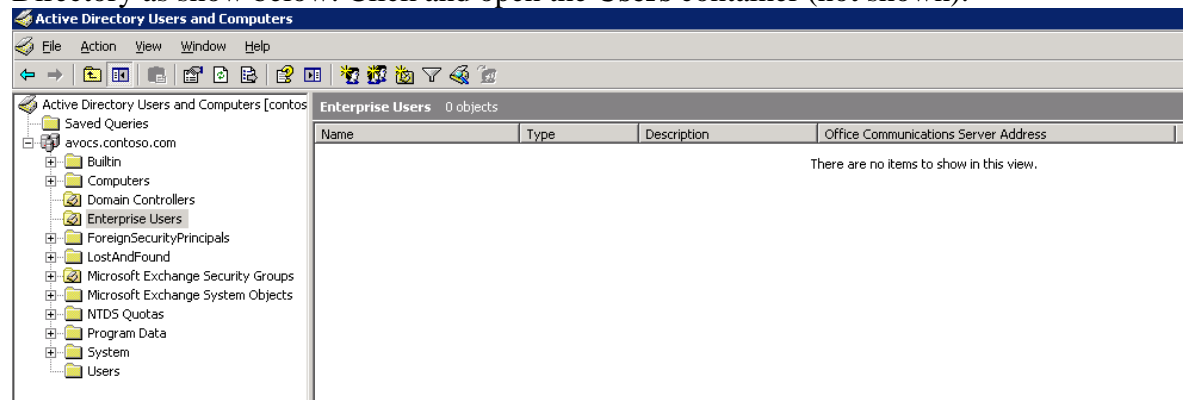
**Step 1. Open Active Directory Users and Computers on the Domain Controller server in the 'OCS' Domain. Right click on the domain name (in the left pane) and select *New* → *Organizational Unit*.**



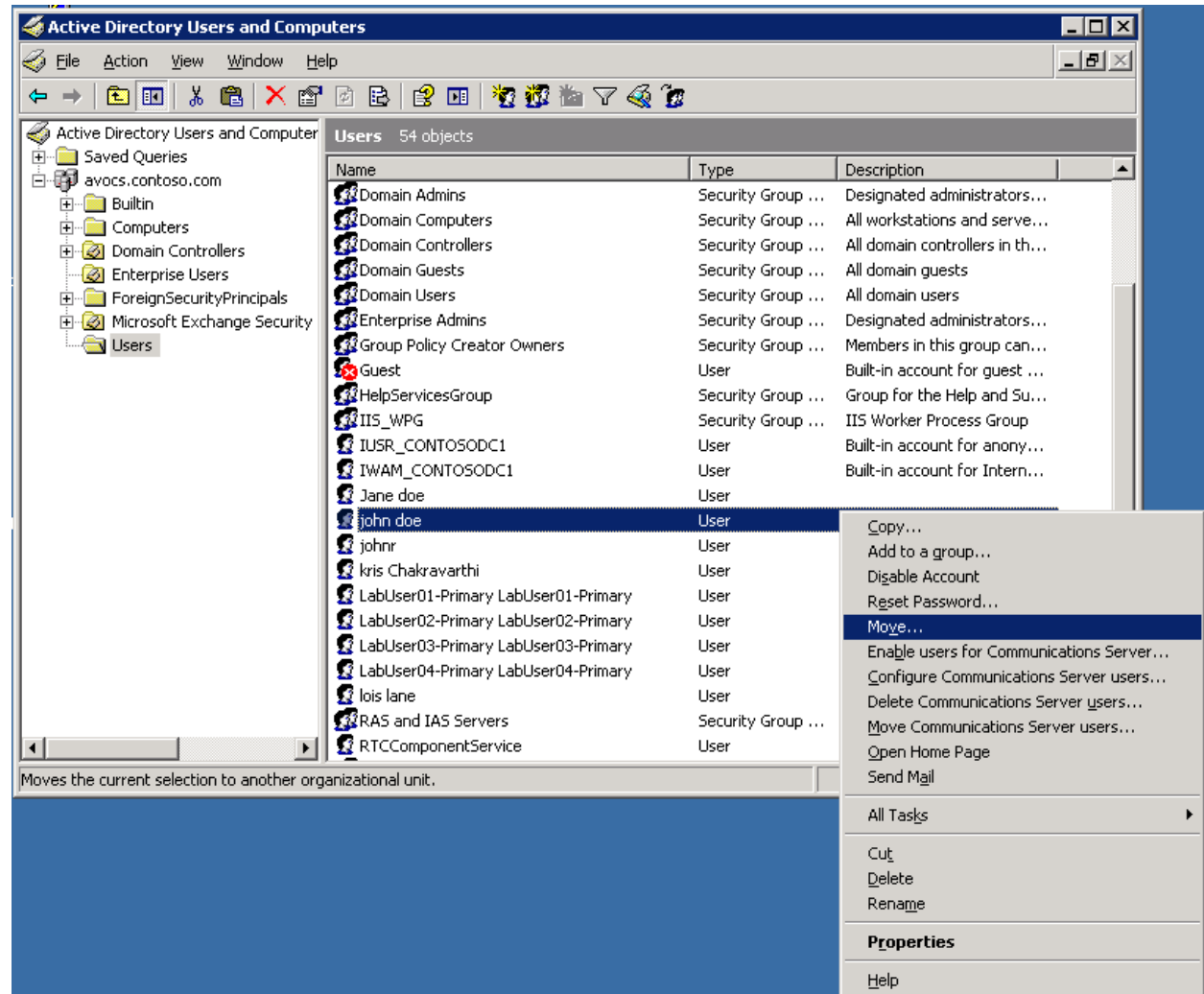
**Step 2.** Type *Enterprise Users* under the **Name:** field and click on the **OK** button.



**Step 3.** Ensure that the **Enterprise Users** Organizational Unit folder is created in the Active Directory as show below. Click and open the **Users** container (not shown).

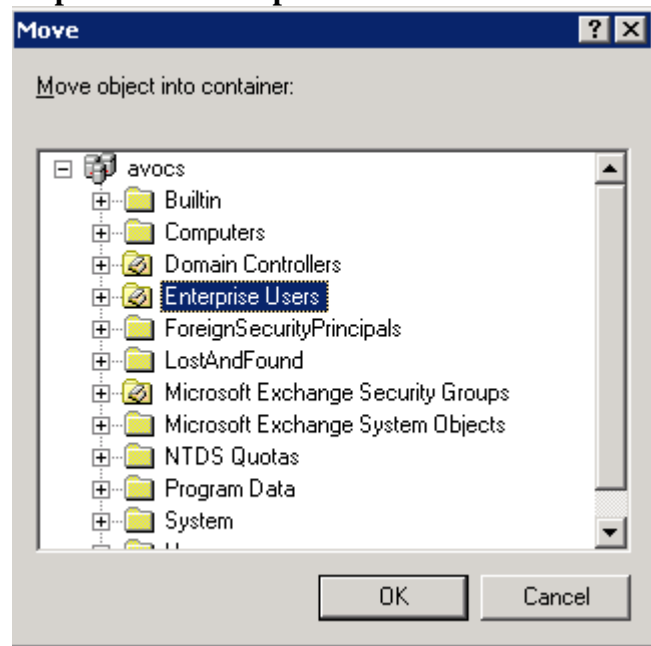


**Step 4.** In the **Users** container, select a Microsoft Office Communicator user<sup>5</sup> and right click to choose **Move** as shown below.



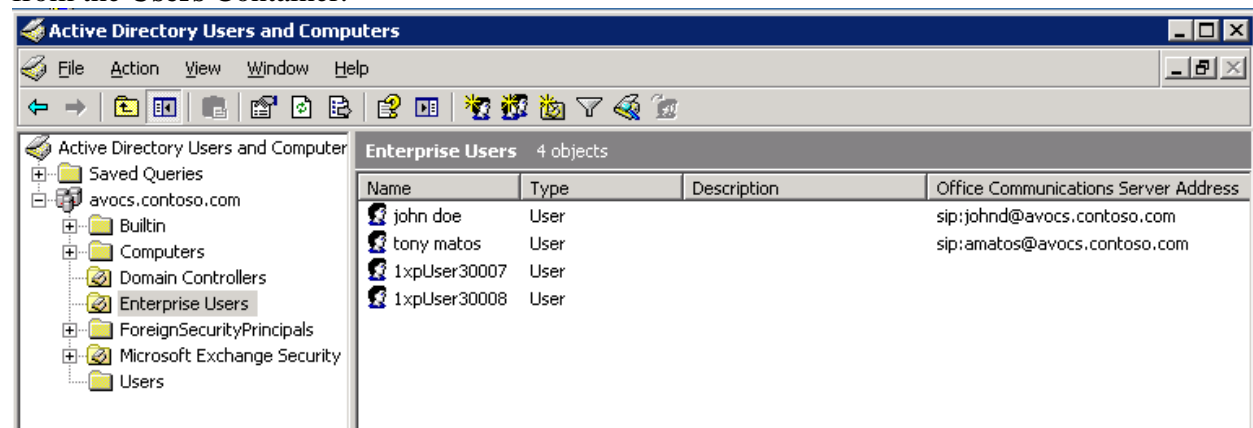
<sup>5</sup> Ensure that the Enable Federation check box is enabled for the user; Right click on a user and select Properties, under the Communications tab for a user click on the Configure button for the Other Setting field; Check the Enable Federation box.

**Step 5.** Select **Enterprise Users** and click **OK**.



Repeat Steps 1 –5 for any Microsoft Office Communicator and Avaya one-X® Portal users to obtain presence information.

**Step 6.** The **Enterprise Users** Organizational Unit folder should contain the list of users moved from the **Users** Container.



The configuration described in this document uses the following user names:

[johnd@avocs.contoso.com](mailto:johnd@avocs.contoso.com) (John Doe) – Microsoft Office Communicator R2 user

[amatos@avocs.contoso.com](mailto:amatos@avocs.contoso.com) (Tony Matos) - Microsoft Office Communicator R2 user

1xpUser30007@ avocs.contoso.com (1xpUser30007) – Avaya one-X® Portal user

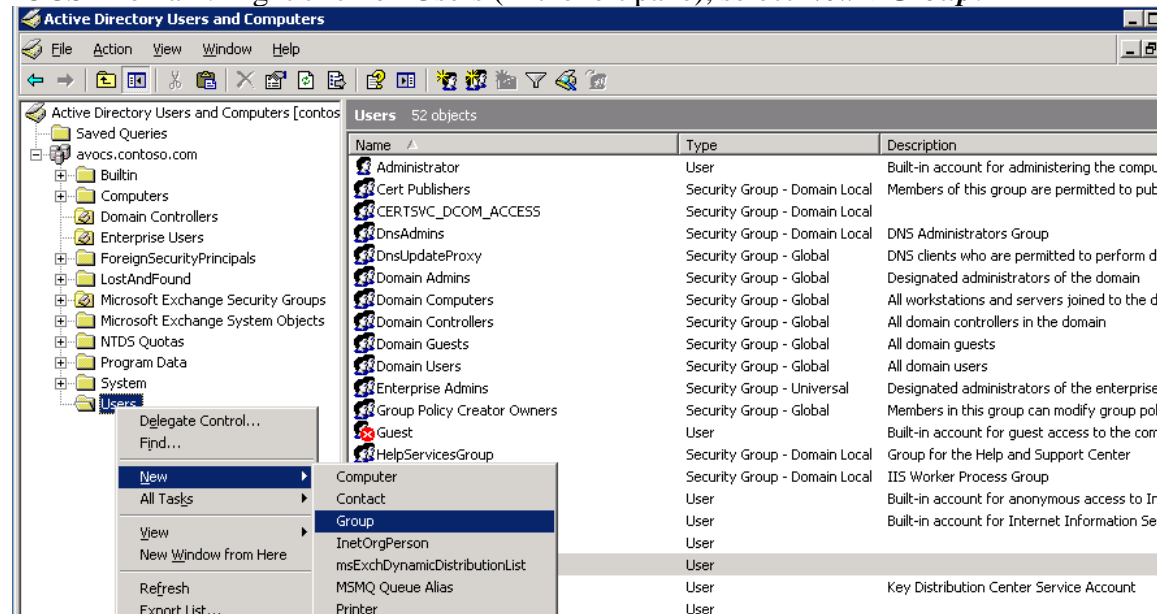
1xpUser30008@ avocs.contoso.com (1xpUser30008) - Avaya one-X® Portal user



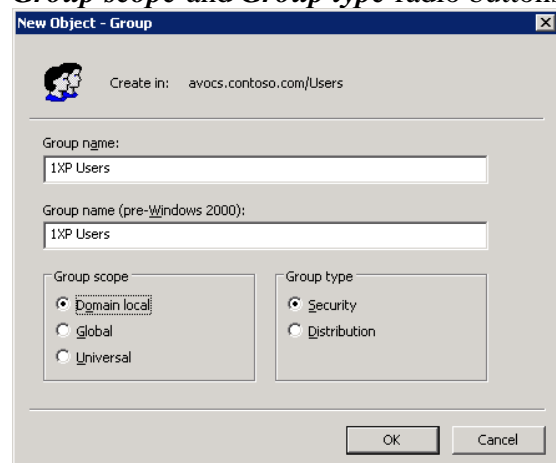
## 4. Create Security Groups for Enterprise Users

The steps described below should be completed prior to installing Avaya one-X® Portal<sup>6</sup>. Refer to [7] for installing and configuring Avaya one-X® Portal.

**Step 1.** Open **Active Directory Users and Computers** on the Domain Controller server in the ‘OCS’ Domain. Right click on **Users** (in the left pane), select **New->Group**.

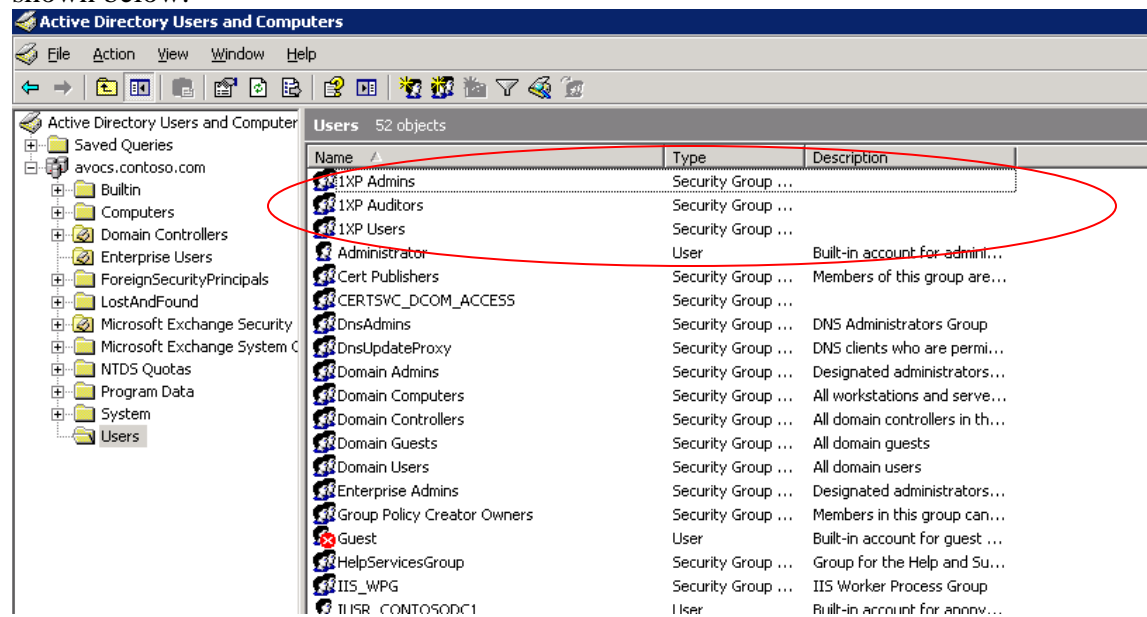


**Step 2.** Enter **1XP Users** in the **Group name** field and select **Domain Local** and **Security** for the **Group scope** and **Group type** radio buttons respectively. Click **OK** to confirm.

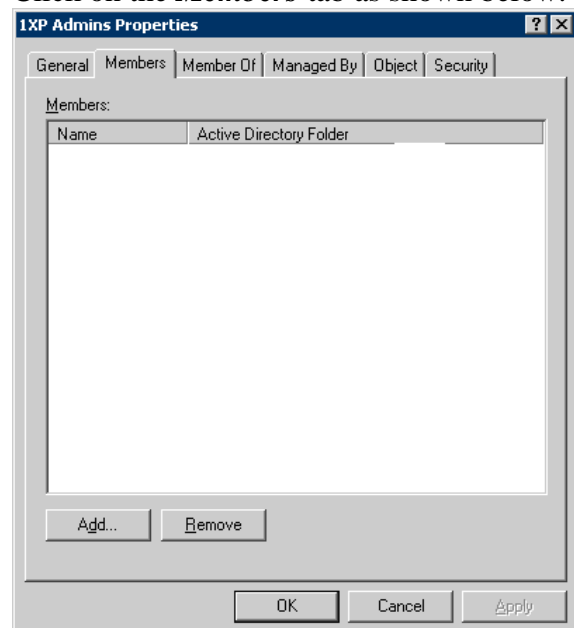


<sup>6</sup> The Avaya one-X® Portal installation prompts for the location of the security groups described in this section.

**Step 3.** Repeat Steps 1 & 2 above and create additional security groups named **1XP Admins** and **1XP Auditors**. All the security groups<sup>7</sup> created should be located in the **Users** container as shown below.



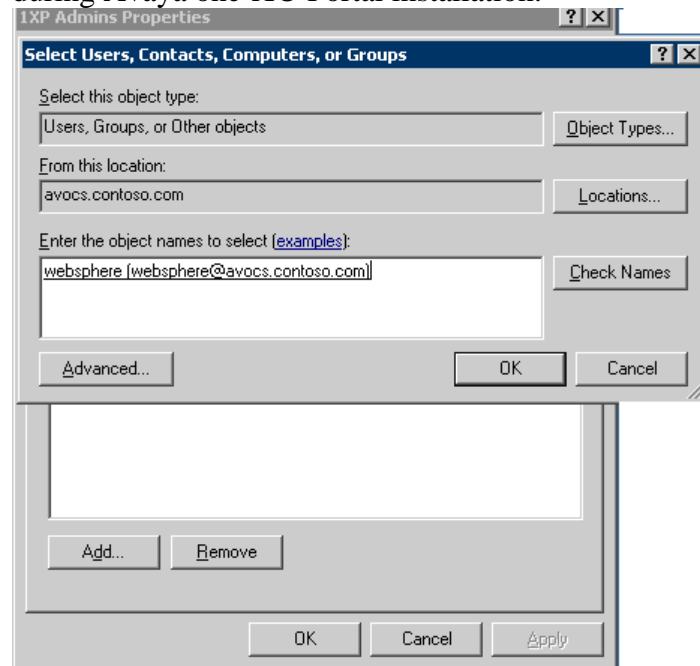
**Step 4.** Select the **1XP Admins** security group; right click and choose **Properties** (not shown). Click on the **Members** tab as shown below. Click on **Add** to add members to this group.



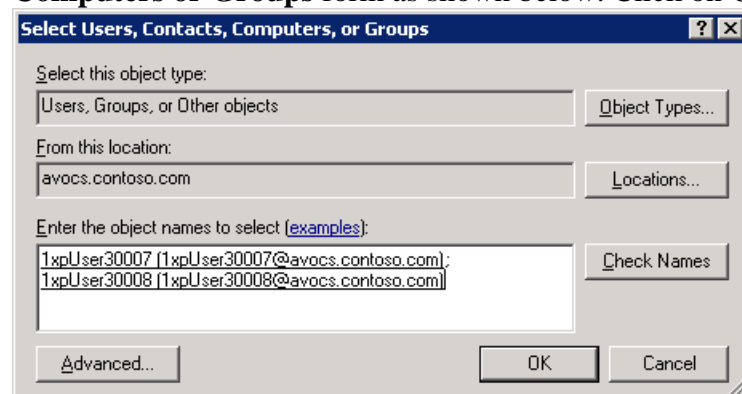
<sup>7</sup> Provide the same security group names created above during the Avaya one-X® Portal installation. The User, Auditor and Admin security groups should be named as **1XP Users**, **1XP Auditors** and **1XP Admins** respectively.

**Step 5.** Enter the username for the Avaya one-X® Portal administrator (use **Check Names** to verify) and click **OK**.

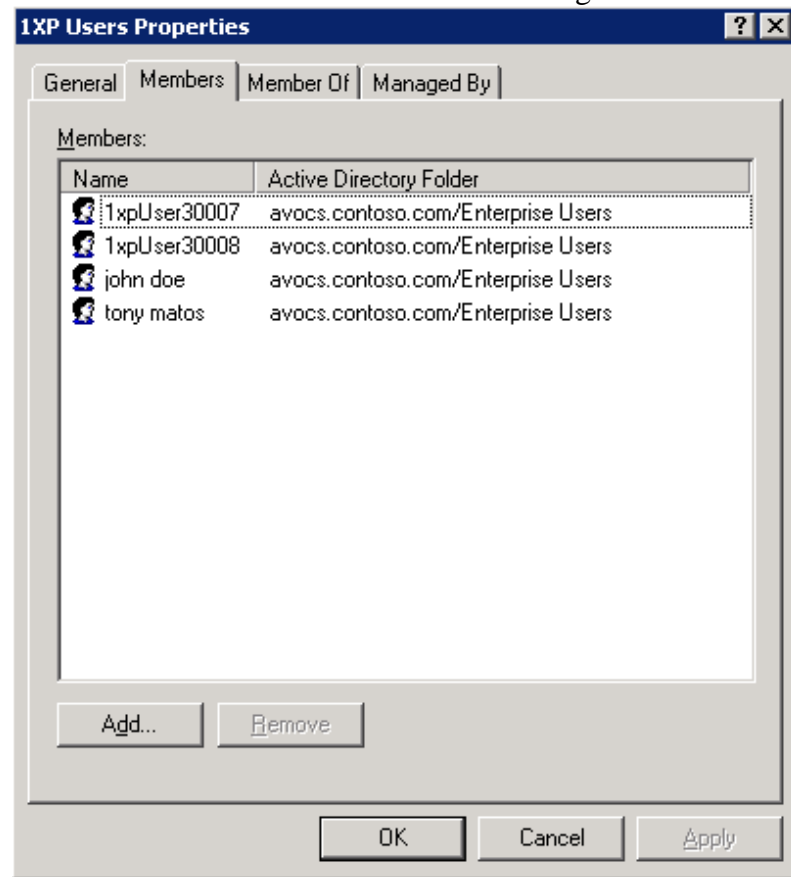
**Note:** The Avaya one-X® Portal configuration described here uses an administrator username of *websphere*. The user *websphere* must be created in the same container (users) as the other Microsoft Office Communicator users (not shown). The same username must also be provided during Avaya one-X® Portal installation.



**Step 6.** Repeat this process and add the necessary users to the **1XP Auditors** security group (not shown). Select the **1XP Users** security group; right click to open the 1XP Admins Properties form and click **Add** on the **Members** tab in the **1XP Admins Properties** form (as shown previously). Enter the Avaya one-X® Portal user names in the **Select Users, Contacts, Computers or Groups** form as shown below. Click on **OK** to confirm.



**Step 7.** Verify that the Avaya one-X® Portal users are added to the **1XP Users** security group as shown below. Click on **OK** to confirm changes.



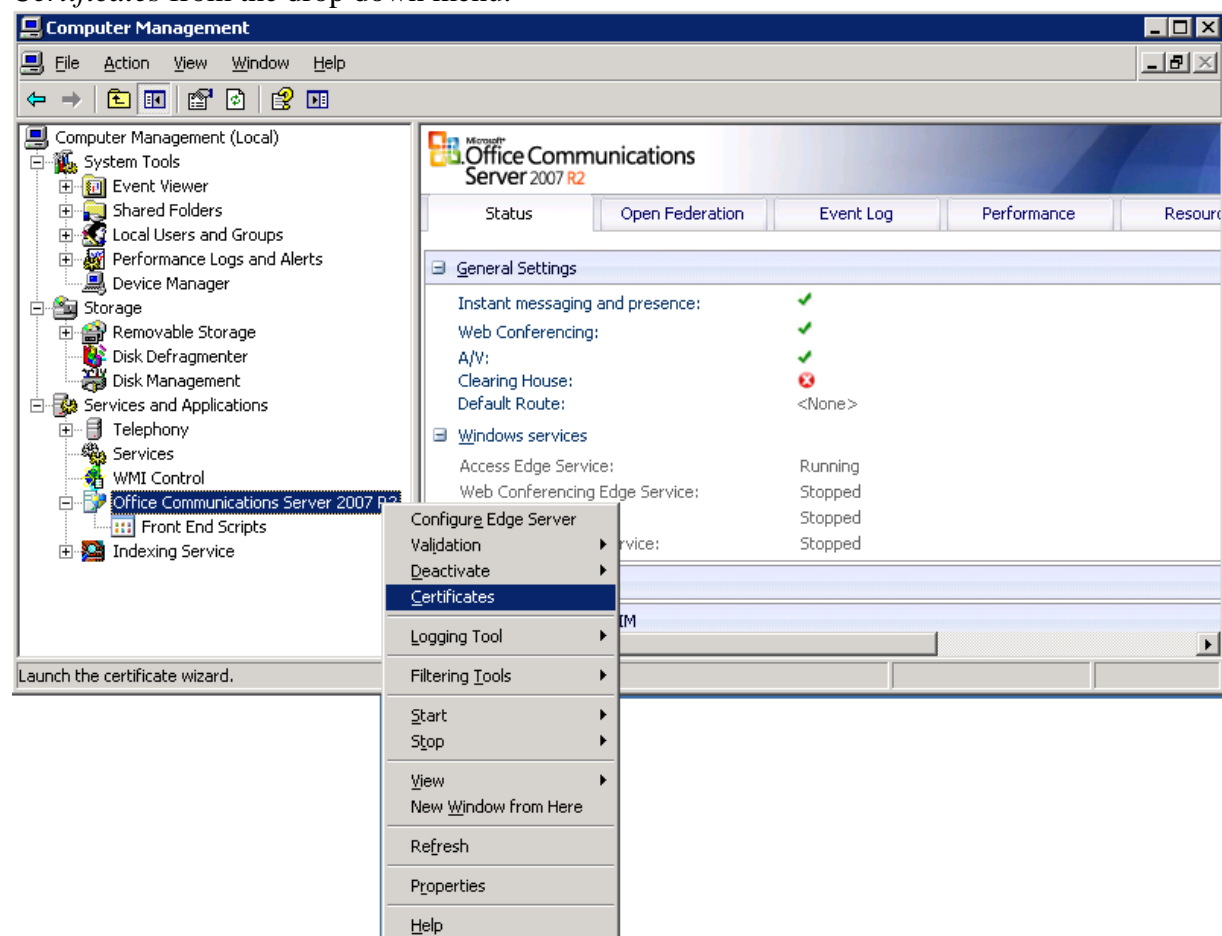
**Note:** The Domain Name Service (DNS) should be configured with the host names and IP addresses (reverse lookup) of the servers in the respective domains.

## 5. Configure Microsoft Edge Server

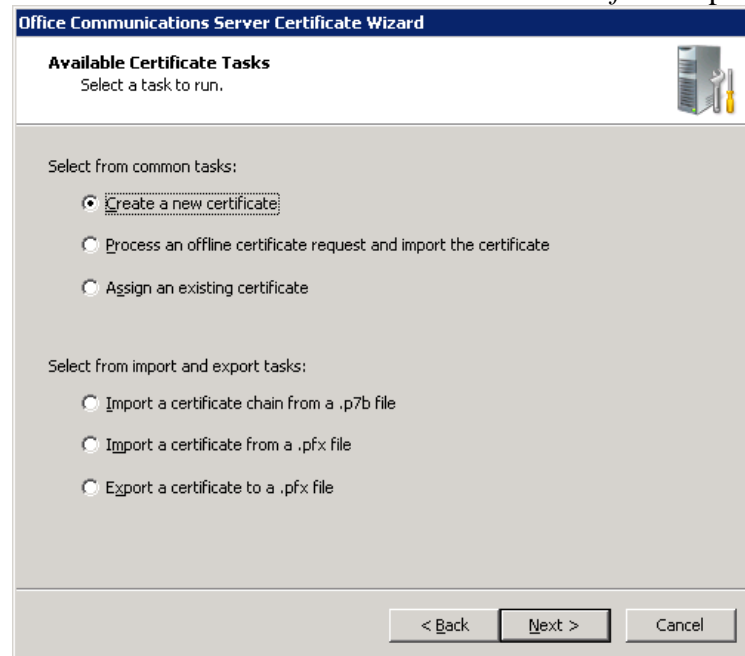
**Note:** Microsoft Edge Server installation is not covered in these Application Notes. Refer to [1] for additional information. The configuration described herein only uses the Access Edge server service; other services i.e: Audio/Video Configuration, Audio/Video Edge and Web Conferencing Edge are not configured or started for this setup.

### 5.1. Assign Certificates to the Microsoft Edge Server Interfaces

**Step 1.** Open Control Panel on the Microsoft Edge Server (not shown) and select **Administrative Tools->Computer Management**. Expand the Services and Applications tree as shown below and right click on Office Communications Server 2007 R2 to view the Edge Server menu. Select **Certificates** from the drop down menu.

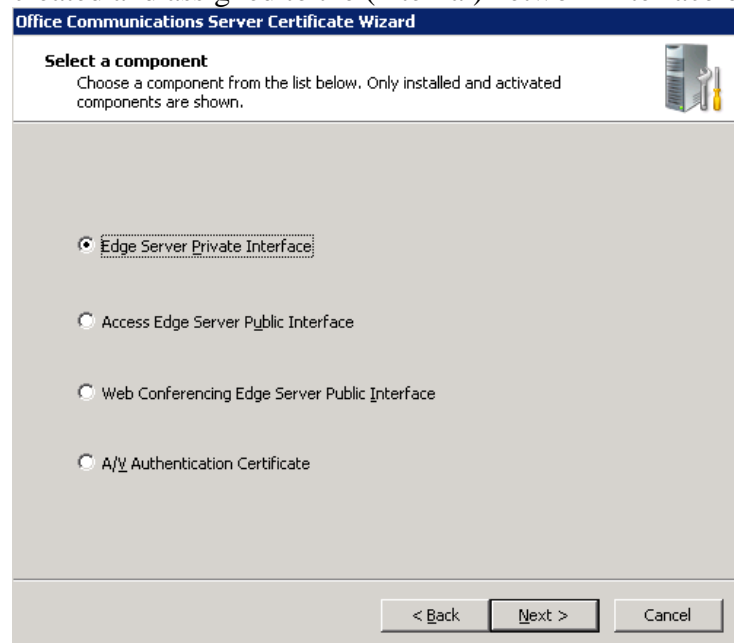


**Step 2.** The **Welcome to the Certificate Wizard** screen will be displayed (not shown), click **Next** to continue. Select the *Create a new certificate* option as shown below and click **Next**.



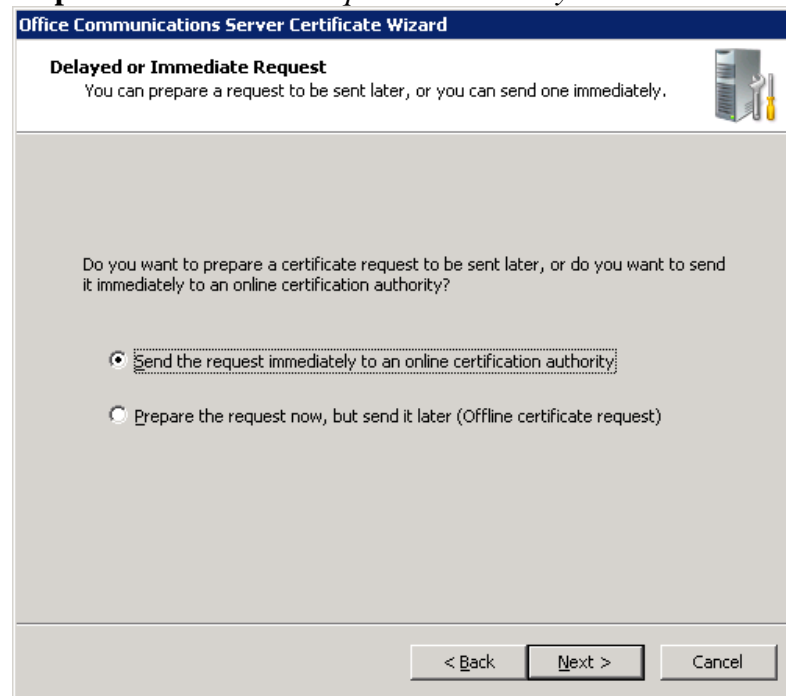
The screenshot shows the 'Office Communications Server Certificate Wizard' window. The title bar is blue with white text. Below the title bar is a header area with the text 'Available Certificate Tasks' and 'Select a task to run.' To the right of this header is an icon of a server rack. The main area of the window is light gray and contains two sections. The first section is titled 'Select from common tasks:' and has three radio button options: 'Create a new certificate' (which is selected and has a dashed border around it), 'Process an offline certificate request and import the certificate', and 'Assign an existing certificate'. The second section is titled 'Select from import and export tasks:' and has three radio button options: 'Import a certificate chain from a .p7b file', 'Import a certificate from a .pfx file', and 'Export a certificate to a .pfx file'. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

**Step 3.** Select *Edge Server Private Interface* and click **Next** to continue. A certificate will be created and assigned to the (internal) network interface of the Edge Server.



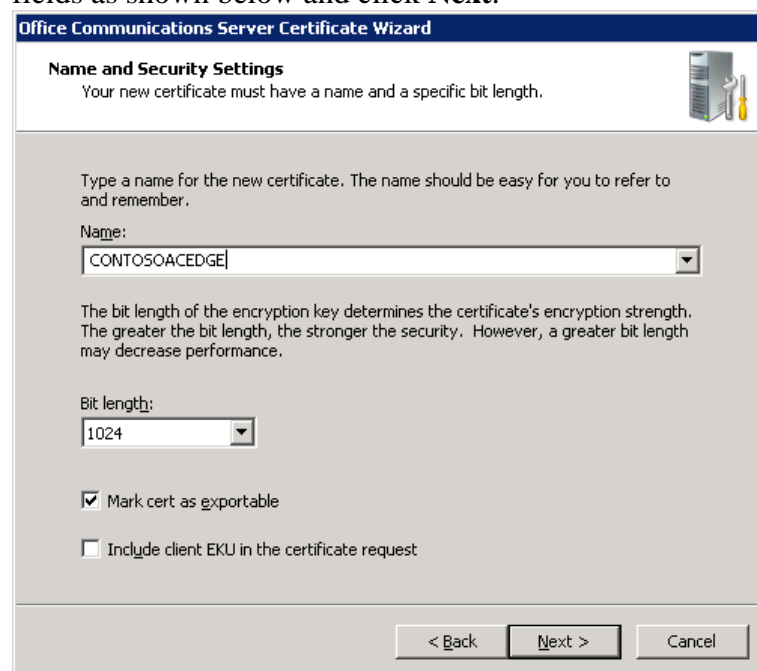
The screenshot shows the 'Office Communications Server Certificate Wizard' window. The title bar is blue with white text. Below the title bar is a header area with the text 'Select a component' and 'Choose a component from the list below. Only installed and activated components are shown.' To the right of this header is an icon of a server rack. The main area of the window is light gray and contains four radio button options: 'Edge Server Private Interface' (which is selected and has a dashed border around it), 'Access Edge Server Public Interface', 'Web Conferencing Edge Server Public Interface', and 'A/V Authentication Certificate'. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

**Step 4.** Select *Send the request immediately to an online certification authority* and click **Next**.



The screenshot shows the 'Office Communications Server Certificate Wizard' window. The title bar is blue with the text 'Office Communications Server Certificate Wizard'. Below the title bar, the section is titled 'Delayed or Immediate Request' with a subtitle 'You can prepare a request to be sent later, or you can send one immediately.' and an icon of a server and a wrench. The main area contains the question 'Do you want to prepare a certificate request to be sent later, or do you want to send it immediately to an online certification authority?'. There are two radio button options: 'Send the request immediately to an online certification authority' (which is selected) and 'Prepare the request now, but send it later (Offline certificate request)'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

**Step 5.** Enter a name for the certificate in the **Name** field; use default values for the remaining fields as shown below and click **Next**.



The screenshot shows the 'Office Communications Server Certificate Wizard' window. The title bar is blue with the text 'Office Communications Server Certificate Wizard'. Below the title bar, the section is titled 'Name and Security Settings' with a subtitle 'Your new certificate must have a name and a specific bit length.' and an icon of a server and a wrench. The main area contains the instruction 'Type a name for the new certificate. The name should be easy for you to refer to and remember.' followed by a 'Name:' label and a text box containing 'CONTOSOACEDGE'. Below this, there is an explanation: 'The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.' followed by a 'Bit length:' label and a dropdown menu showing '1024'. There are two checkboxes: 'Mark cert as exportable' (which is checked) and 'Include client EKU in the certificate request' (which is unchecked). At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

**Step 6.** Enter organizational information in the following form (not shown) and click **Next**. Enter the FQDN<sup>8</sup> of the internal network interface in the **Subject name** field. Click **Next** to continue.

**Office Communications Server Certificate Wizard**

**Your Server's Subject Name**  
 Subject names can contain only alphanumeric characters and a leading wildcard (e.g., sip.contoso.com or \*.contoso.com).

Type the Fully Qualified Domain Name of your server or Select from the list. If the server is part of a Pool, you should use the server's Pool Name. If these names change, you will need a new certificate.

Subject name:

Type any alternate names for your server. Use comma to separate multiple names. Subject Name will be automatically appended if the Alternate Name field is non empty.

Subject Alternate Name:

Specify whether the wizard should automatically add the FQDN of the local computer as an alternate name.

☐ Automatically add local machine name to Subject Alt Name

< Back   Next >   Cancel

**Step 7.** Enter geographical region information in the following screen (not shown) and click **Next**. Click the *Select a Certificate authority from the list detected in your environment* radio button and select the appropriate certificate authority server from the drop down box.

**Note:** In case the Certificate Authority (CA) server is not listed in this drop down box, select the radio button for the **Specify the certificate authority that will be used to request this certificate** and specify the certificate server location as *<FQDN of Certificate Authority server>\<CA instance name>*

**Office Communications Server Certificate Wizard**

**Choose a Certification Authority**  
 Certificate requests are sent to a certification authority available on your network.

Select a certification authority to process your request. Certificate wizard will automatically import the selected CA's certificate chain if necessary.

☒ Select a certificate authority from the list detected in your environment

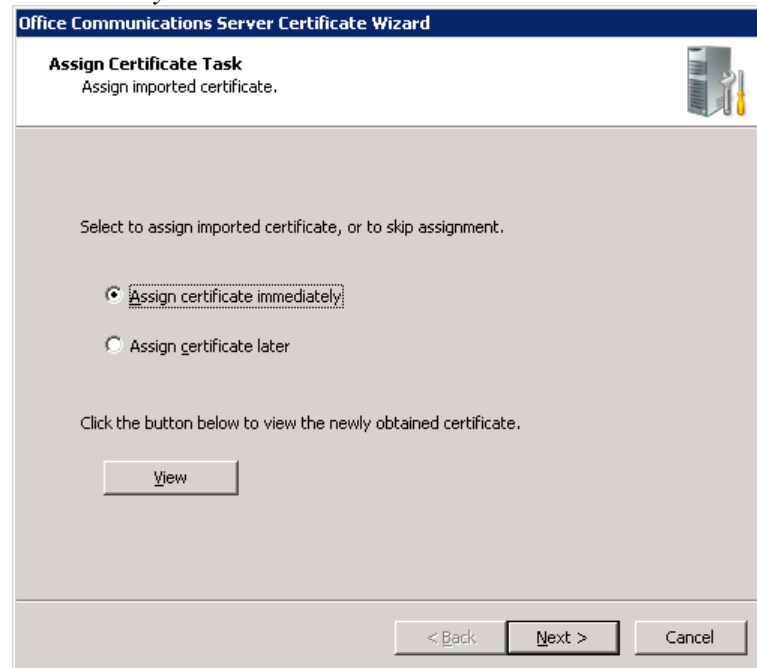
☐ Specify the certificate authority that will be used to request this certificate  
  
 Example: mycaserver.contoso.com\MyCAInstance

< Back   Next >   Cancel

<sup>8</sup> FQDN: Fully Qualified Domain Name

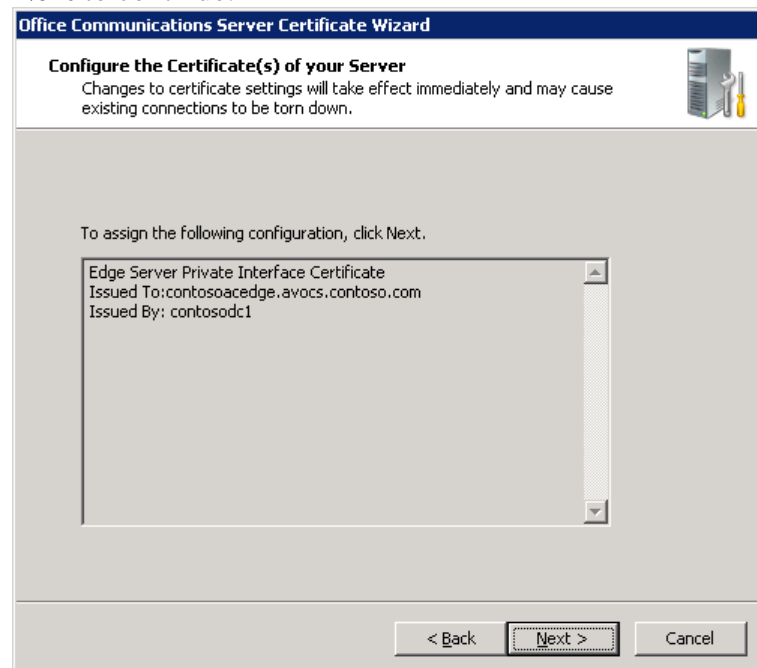


**Step 8.** View the **Request Summary** form (not shown) and click **Next**. Select *Assign certificate immediately* radio button and click **Next** to continue.



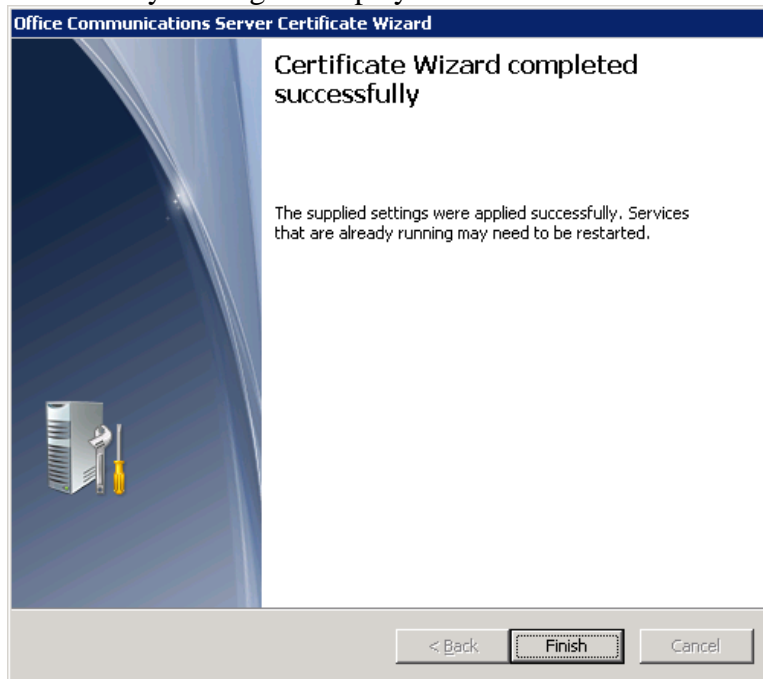
The screenshot shows the 'Assign Certificate Task' window of the Office Communications Server Certificate Wizard. The title bar reads 'Office Communications Server Certificate Wizard'. Below the title bar, the window has a header area with the text 'Assign Certificate Task' and 'Assign imported certificate.' next to a server icon. The main area contains the instruction 'Select to assign imported certificate, or to skip assignment.' followed by two radio buttons: 'Assign certificate immediately' (which is selected) and 'Assign certificate later'. Below these is the text 'Click the button below to view the newly obtained certificate.' and a 'View' button. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

**Step 9.** View the settings in the **Configure the Certificate(s) of your Server** form and click **Next** to continue.

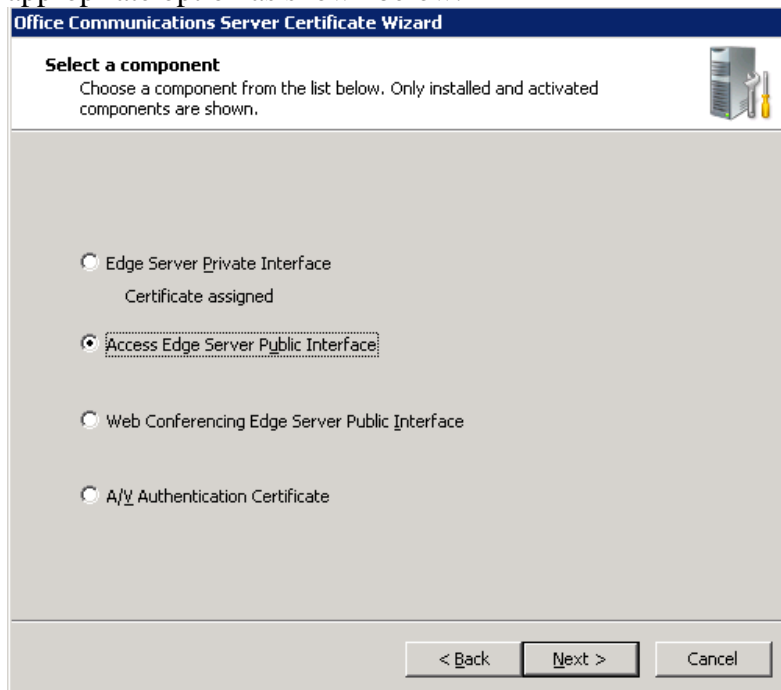


The screenshot shows the 'Configure the Certificate(s) of your Server' window of the Office Communications Server Certificate Wizard. The title bar reads 'Office Communications Server Certificate Wizard'. Below the title bar, the window has a header area with the text 'Configure the Certificate(s) of your Server' and a warning: 'Changes to certificate settings will take effect immediately and may cause existing connections to be torn down.' next to a server icon. The main area contains the instruction 'To assign the following configuration, click Next.' followed by a list box containing the text: 'Edge Server Private Interface Certificate', 'Issued To: contosoacedge.avocs.contoso.com', and 'Issued By: contosodc1'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

**Step 10.** Ensure that the **Office Communications Server Certificate Wizard** completed successfully message is displayed as shown below.



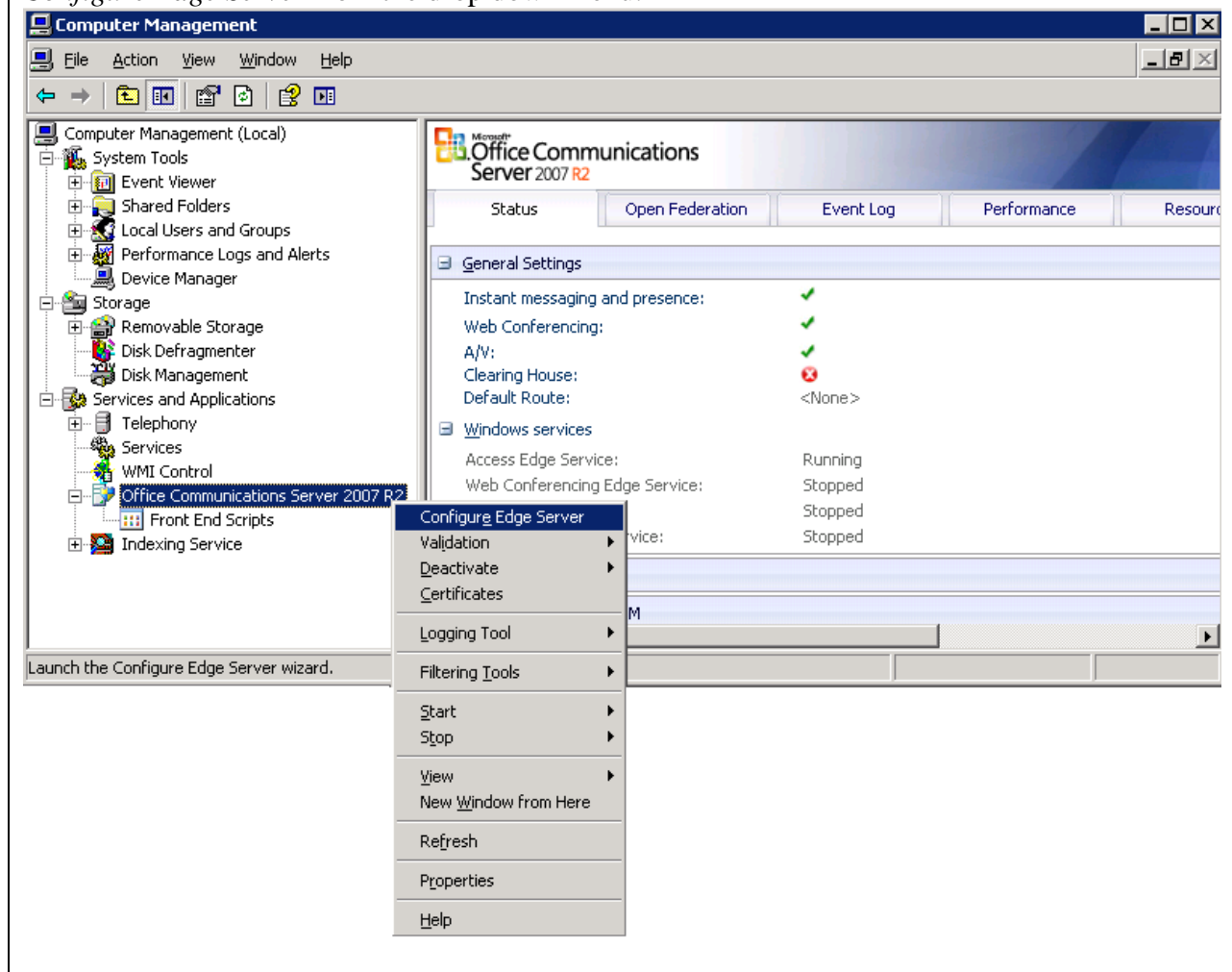
**Step 11.** Repeat the process for installing **Access Edge Server Public Interface** by selecting the appropriate option as shown below.



Repeat Steps 1-11 listed above to generate a certificate for the Access Edge Server Public Interface (external). The configuration in these Application Notes does not require certificates to be installed for the Web Conferencing Edge Server Public Interface and A/V Authentication Certificate. However, the Edge Server validation may fail in the absence of these certificates.

## 5.2. Configure Edge Server Interface

**Step 1.** Open Control Panel on the Microsoft Edge Server (not shown) and select *Administrative Tools->Computer Management*. Expand the Services and Applications tree as shown below and right click on *Office Communications Server 2007 R2* to view the Edge Server menu. Select *Configure Edge Server* from the drop down menu.



**Step 2.** The **Welcome to the Configure Office Communications Server 2007 R2, Edge Server** Wizard screen will be displayed (not shown), click **Next** to continue. Leave the *Import Settings* box unchecked and click **Next**.

The screenshot shows the 'Configure Edge Server Wizard' window. The title bar reads 'Configure Edge Server Wizard'. The main heading is 'Import Settings From a File'. Below this, a sub-heading says 'If you have a configuration file that you want to import, select the check box and provide the file name.' There is an unchecked checkbox labeled 'Import settings:'. Below the checkbox is a text field labeled 'Configuration file name:' and a 'Browse...' button. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

**Step 3.** Select the IP address assigned to the internal Edge Server interface card in the **Internal Interface IP Address** drop down box. Enter the FQDN for the internal interface in the **FQDN for the internal interface** field as shown below. Click **Next** to continue.

The screenshot shows the 'Configure Edge Server Wizard' window. The title bar reads 'Configure Edge Server Wizard'. The main heading is 'Internal Interface'. Below this, a sub-heading says 'Supply the IP address and FQDN used by the internal interface of the Edge Server.' There is a dropdown menu labeled 'Internal Interface IP Address:' with '135.8.19.125' selected. Below this is a text field labeled 'FQDN for the internal interface:' with 'contosoedge.avocs.contoso.com' entered. A note below the text field says: 'Note: If you are using a load balancer, specify the IP address of the local server and the FQDN of the load balancer's VIP.' Below the note is a table of port settings:

Access Edge Server Internal Interface Port:	5061
Web Conferencing Edge Server Internal Interface Port:	8057
A/V Edge Server Internal Interface Port:	443
A/V Edge Server TLS Signaling Port:	5062

Below the table is another note: 'Note: You can change the default port settings using the administrative snap-in.' At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

**Step 4.** In the Access Edge Server section of the screen, select the IP address of the access edge interface in the **IP address** field and enter the FQDN assigned to the access edge interface in the **FQDN** field. Use **5061** as the **Remote user access port**. Click **Next** to continue.

**Note:** The configuration described in this document does not use the Web Conferencing Edge Server or the A/V Edge Server. However, the Configure Edge Server Wizard does not permit leaving these settings blank. Hence dummy settings are used in the **Web Conferencing Edge Server** and **A/V Edge Server** sections below.

**Configure Edge Server Wizard**

**External Interface**

**Access Edge Server**

IP address: 135.8.19.174 FQDN: accessededge.edgeext.avocs.contos

Federation port: 5061

Remote user access port: ☒ 5061 ☐ 443 ☐ Other:

**Web Conferencing Edge Server**

IP address: 135.8.19.174 FQDN: webconfedge.cebp-avaya.com

Port: ☐ 443 ☒ Other: 444

**A/V Edge Server**

IP address: 135.8.19.174 FQDN: avedge.cebp-avaya.com

Port: ☐ 443 ☒ Other: 445

< Back Next > Cancel

**Step 5.** Ensure that the *Enable federation* and the *Allow discovery of federation partners* check boxes are checked. Leave the other boxes unchecked as shown below. Click **Next** to continue.

**Configure Edge Server Wizard**

**Enable Features on Access Edge Server**

**User Access Settings**

☐ Allow remote user access to your network

☐ Allow anonymous user to join meetings.

☐ Allow users to communicate with federated contacts

**Federation Settings**

☒ Enable federation

☒ Allow discovery of federation partners

☐ Federation with selected public IM providers:

☐ MSN ☐ AOL ☐ Yahoo!

Note: If you do not enable automatic discovery of federation partners, you must configure any partners on the Allow tab of the edge server.

< Back Next > Cancel

**Step 6.** Enter the FQDN assigned to the Microsoft Office Communicator pool in the **FQDN of next hop server** field and click **Next** to continue.

The screenshot shows a Windows-style dialog box titled "Configure Edge Server Wizard". The main heading is "FQDN of Internal Next Hop Server". Below the heading is a descriptive text: "Specify the FQDN of the server to which Access Edge Server routes internal traffic. For security and scalability, we recommend that the next hop server be a Director". To the right of this text is a small icon of a server rack. Below the text is a text input field containing the value "contosopool01.avocs.contoso.com". Below the input field is a note: "The FQDN should point to a Standard Edition server, Enterprise pool, a Director or the hardware load balancer used by an array of Standard Edition servers functioning as a Director." At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

**Step 7.** Specify the domain name assigned to servers in the Microsoft Office Communicator R2 domain under the **Specify internal SIP domains within your organization** field. Click **Add** to add the specified domain to the list. Click **Next** to continue.

The screenshot shows a Windows-style dialog box titled "Configure Edge Server Wizard". The main heading is "Authorized Internal SIP Domains". Below the heading is a descriptive text: "Specify internal SIP domains within your organization." To the right of this text is a small icon of a server rack. Below the text is a text input field containing the value "avocs.contoso.com". To the right of the input field are two buttons: "Add" and "Remove". Below the input field is a large empty rectangular box, likely a list of added domains. At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

**Step 8.** Enter the FQDN of the Microsoft Office Communicator R2 server and pool in the **Specify all internal servers that can connect to the Edge Server** field. Click **Add** to add the specified entries to the list. Click **Next** to continue.

The screenshot shows the 'Configure Edge Server Wizard' window, specifically the 'Authorized Internal Servers' step. The window has a title bar 'Configure Edge Server Wizard' and a subtitle 'Authorized Internal Servers'. Below the subtitle is an icon of a server and a screwdriver. The main area contains the text 'Specify all internal servers that can connect to the Edge Server.' Below this is a text input field containing 'contosoocs1.avocs.contoso.com' and an 'Add' button. Below the input field is a list box containing 'contosopool01.avocs.contoso.com' and a 'Remove' button. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

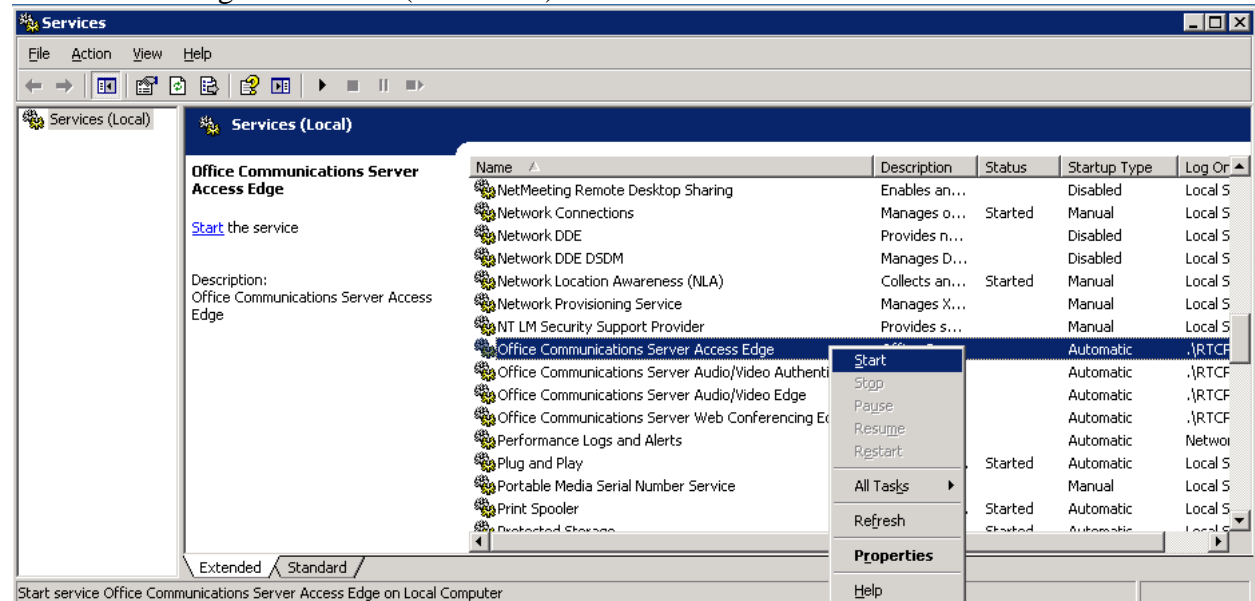
**Step 9.** Review the settings in the form displayed below and click **Next** to start the edge server configuration.

The screenshot shows the 'Configure Edge Server Wizard' window, specifically the 'Configure your Edge Server' step. The window has a title bar 'Configure Edge Server Wizard' and a subtitle 'Configure your Edge Server'. Below the subtitle is an icon of a server and a screwdriver. The main area contains the text 'The wizard has enough information to begin Edge Server configuration.' and 'Please review the settings you have selected below. If you want to change any settings, click Back. Click Next to start.' Below this is a section titled 'Current Settings:' followed by a list of settings: 'Access Edge Server: Activated', 'Web Conferencing Edge Server: Activated', 'A/V Edge Server: Activated', 'Internal interface IP address: 135.8.19.125', 'Internal interface FQDN: contosoacedge.avocs.contoso.com', 'Internal interface port for Access Edge Server: 5061', and 'Internal interface port for Web Conferencing Edge Server: 8057'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

**Step 10.** Ensure that the **Configure Office Communications Server 2007 R2, Edge Server Wizard has completed successfully** message is displayed as shown below. Click **Finish** to exit the wizard.



**Step 11.** Open the **Windows Service Control Manager** on the Edge server (not shown); start the **Office Communicator Server Access Edge** service as shown below. Ensure that the Status for the service changes to *Started* (not shown).

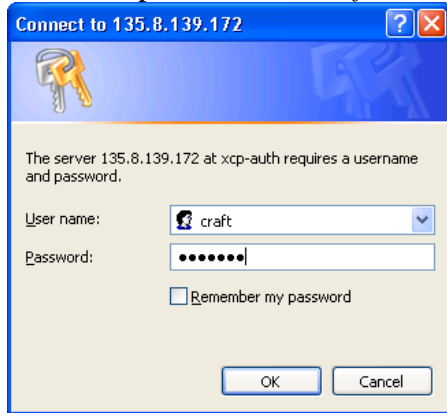




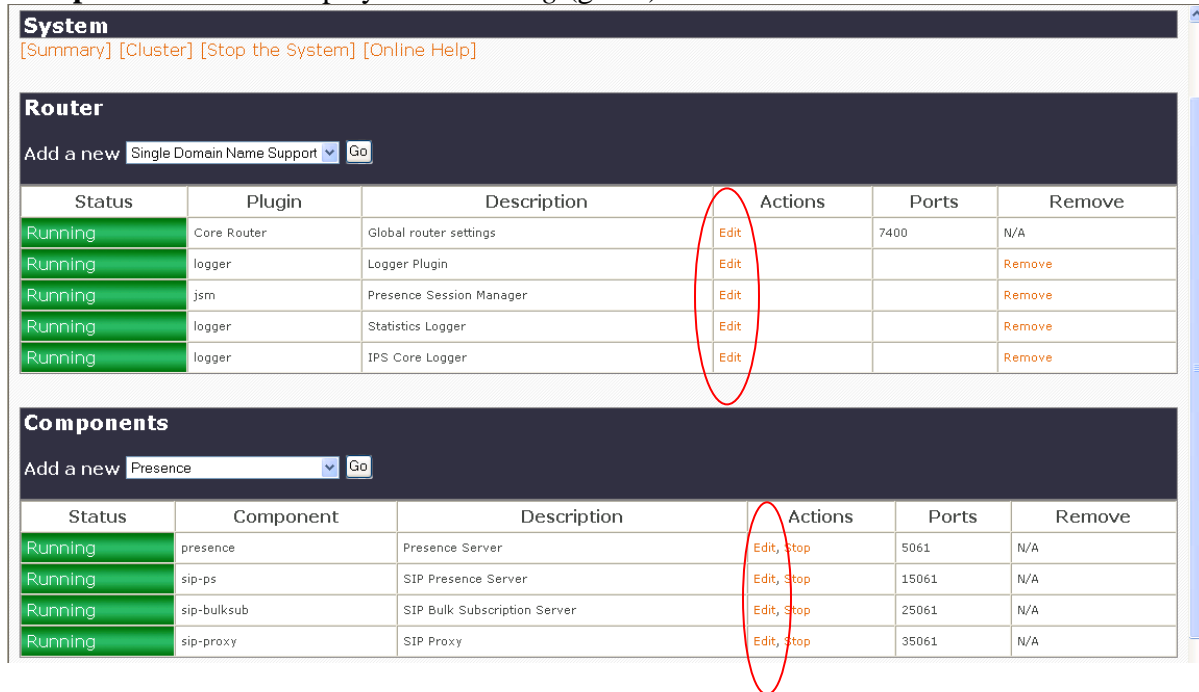
## 6. Configure the Intelligent Presence Server (IPS)

Refer to [2] for instructions on installing an Avaya Intelligent Presence Server. These Application Notes describe configuring the XCP component of an Intelligent Presence server through the web based interface.

**Step 1.** Open a web browser and enter *http://<IP address of an IPS server>:7300/admin* (not shown). Provide appropriate credentials in the authentication box as shown below. Default user name and password are *craft* and *craft01* respectively. Click **OK** to confirm.



**Step 2.** The XCP controller page is displayed as shown below. Verify that the **Plugin** and **Component** status is displayed as *Running* (green).



**System**  
[Summary] [Cluster] [Stop the System] [Online Help]

**Router**  
Add a new Single Domain Name Support Go

Status	Plugin	Description	Actions	Ports	Remove
Running	Core Router	Global router settings	Edit	7400	N/A
Running	logger	Logger Plugin	Edit		Remove
Running	jsm	Presence Session Manager	Edit		Remove
Running	logger	Statistics Logger	Edit		Remove
Running	logger	IPS Core Logger	Edit		Remove

**Components**  
Add a new Presence Go

Status	Component	Description	Actions	Ports	Remove
Running	presence	Presence Server	Edit, Stop	5061	N/A
Running	sip-ps	SIP Presence Server	Edit, Stop	15061	N/A
Running	sip-bulksub	SIP Bulk Subscription Server	Edit, Stop	25061	N/A
Running	sip-proxy	SIP Proxy	Edit, Stop	35061	N/A

**Note:** Select **Advanced** from the **Configuration view** drop down box prior to viewing all the settings for any Plugin or Component page.

### **Core Router (Global router settings):**

**Step 1.** Click on the **Edit** link (Actions Column) for the Global router settings (Step 2 above). Select the **Master Accept Port** check box and enter the IP address of the Intelligent Presence Server in the **Component IP** field. Use default values for the remaining fields in the **Master Accept Port** section.

**XCP Controller**  
[Home] [Logout]  
Help

Configuration view: **Advanced** (selected)  
Basic  
Intermediate  
Advanced

### Global Settings Configuration

Global Settings

Cluster	cluster1
Realm	presence
Enable MDNS	No
Level of information to log	info
Obscure plaintext passwords in log files	Yes
Number of threads devoted to I/O	3
The interval (in seconds) between keepalive packets.	60
Maximum number of bytes per JID resource Do not set this option lower than 18 if using JSM.	
The number of hashtable buckets for JID lookups.	46153
<input checked="" type="checkbox"/> Master Accept Port	
Component IP	135.8.139.172
Port	7400
Password	secret
Buffer size in bytes for outgoing data	65535
Buffer size in bytes for incoming data	65535
<input type="checkbox"/> Start TLS Configuration	

**Step 2.** Scroll down the web page and ensure that the **Database Setup** box is checked. In the edit box for the **host** field enter the FQDN of the one-X Portal server and the Microsoft OCS R2 sub domain name. Leave the other settings unchanged (default values). Click **Submit** to confirm.

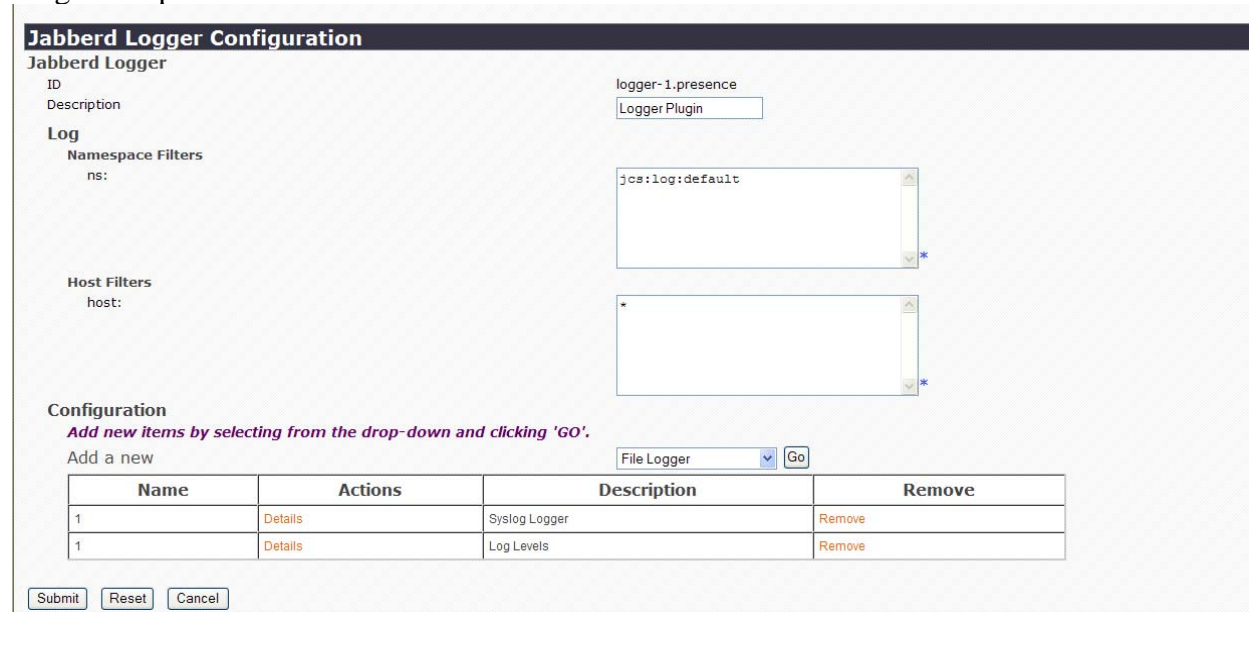
☒ Database Setup

Datasource Name	xcp
Database User Name	xcp_user
Database User's Password	*****
Confirm Password	*****
Database Type	postgresql-odbc
Number of connections to the database	20
Time in seconds between database connection heartbeats	60
Is database debug logging enabled?	0
<input type="checkbox"/> SNMP Configuration	
Enable SNMP	Yes
Count errors	No
Mutually Trusted TLS Hostnames Separate each hostname (or IP address) with a line break.	
Host Filters host:	oneXP171.cebp-avaya.com avocs.contoso.com

Submit Reset Cancel

### **Logger (Logger Plugin):**

**Step 1.** Click on the *Edit* link (Actions Column) for the Logger Plugin (not shown). Use default settings in the Logger page as shown below. No setting changes are required for the Logger Plugin component. Click **Submit** to confirm.



**Jabberd Logger Configuration**

Jabberd Logger

ID: logger-1.presence  
Description: Logger Plugin

**Log**

Namespace Filters  
ns: jcs:log:default

Host Filters  
host: \*

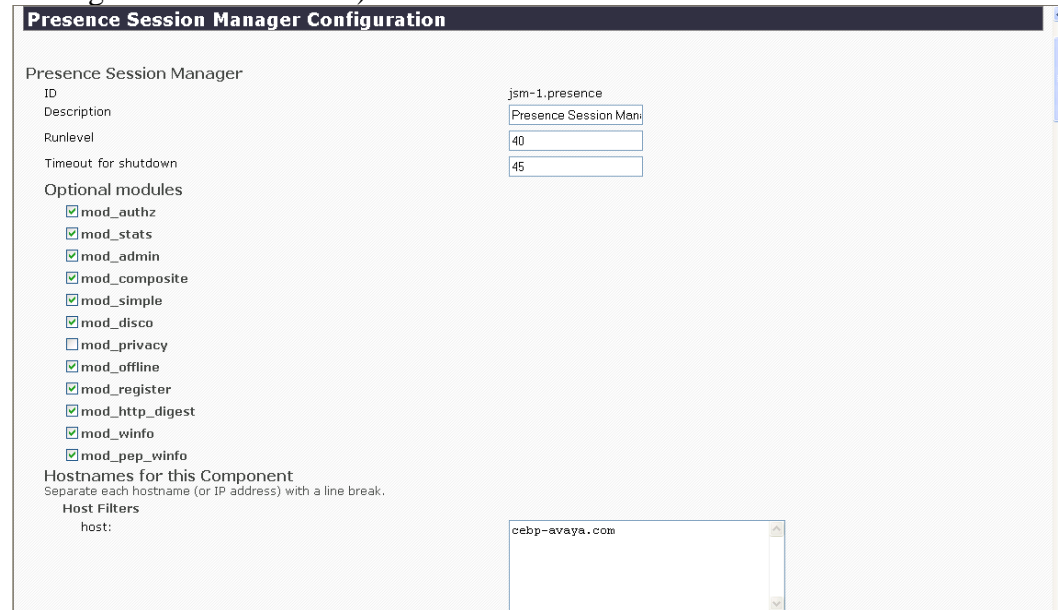
**Configuration**  
Add new items by selecting from the drop-down and clicking 'GO'.  
Add a new: File Logger [Go]

Name	Actions	Description	Remove
1	<a href="#">Details</a>	Syslog Logger	<a href="#">Remove</a>
1	<a href="#">Details</a>	Log Levels	<a href="#">Remove</a>

[Submit] [Reset] [Cancel]

### **JSM (Presence Session Manager):**

**Step 1.** Click on the *Edit* link (Actions Column) for the Presence Session Manager (not shown). Enter the domain name of the network in which the Avaya components (one-X Portal and Intelligent Presence Server) are located in the *host* field. Use default values for other settings.



**Presence Session Manager Configuration**

Presence Session Manager

ID: jsm-1.presence  
Description: Presence Session Manager  
Runlevel: 40  
Timeout for shutdown: 45

**Optional modules**

- ☒ mod\_authz
- ☒ mod\_stats
- ☒ mod\_admin
- ☒ mod\_composite
- ☒ mod\_simple
- ☒ mod\_disco
- ☐ mod\_privacy
- ☒ mod\_offline
- ☒ mod\_register
- ☒ mod\_http\_digest
- ☒ mod\_winfo
- ☒ mod\_pep\_winfo

**Hostnames for this Component**  
Separate each hostname (or IP address) with a line break.

**Host Filters**  
host: cepb-avaya.com

**Step 2.** Scroll down the page and locate the JSM Configuration section. Replace the default domain name for the username jabber with the network domain name in which the Intelligent Presence Server is located. Use default values for the remaining fields in the Presence Session Manager page. Click on the **Submit** button (not shown) at the bottom of the page to confirm changes.

### JSM Configuration

☒ **Presence Administrators**  
Add/remove administrators as needed.  
Administrator(s):

jabber@cebp-avaya.com

sip-ps-1.presence

sip-bulksub-1.presence

☒ **System Limits**  
These options control system usage.  
Maximum number of sessions a single user (JID) can open at a time   
Maximum number of users that can be logged into the server at one time

☒ **System Parameters**  
These options control the XCP server's use of your system's processor.  
Number of threads to use for processing Presence tasks   
Number of worker queues to use for processing Presence tasks   
Closed session cache time (in seconds)   
User session cache time (in seconds)   
Timeout for XDB requests   
Timeout for IQ requests   
Maximum XDB requests to allow   
Resume sockets when XDB requests drop below   
Maximum database requests to allow   
Resume sockets when database requests drop below   
Service ID of identifier mapping component   
Identifier mapping cache age (in seconds)   
Identifier mapping cache cleanup interval (in seconds)

### **Logger (Statistics Logger) settings:**

**Step 1.** Click on the *Edit* link (Actions Column) for the Statistics Logger (not shown). Use default settings in the Logger page as shown below. No setting changes are required for the Statistics Logger component. Click **Submit** to confirm.

**Jabberd Logger Configuration**

Jabberd Logger

ID

logger-2.presence

Description

Statistics Logger

Log

Namespace Filters

ns:

jcs:stats:jsm  
jcs:mod\_log:presence

Host Filters

host:

\*

Configuration

Add new items by selecting from the drop-down and clicking 'GO'.

Add a new

File Logger

Go

Name	Actions	Description	Remove
1	<a href="#">Details</a>	File Logger	<a href="#">Remove</a>

Submit

Reset

Cancel

### **Logger (IPS Core Logger) settings:**

**Step 1.** Click on the *Edit* link (Actions Column) for the IPS Core Logger (not shown). Use default settings in the Logger page as shown below. No setting changes are required for the IPS Core Logger component. Click **Submit** to confirm.

**Jabberd Logger Configuration**

Jabberd Logger

ID

logger-3.presence

Description

IPS Core Logger

Log

Namespace Filters

Namespace(s):

jcs:log:default  
jcs:mod\_log:presence

Host Filters

Host(s):

\*

Configuration

Add new items by selecting from the drop-down and clicking 'GO'.

Add a new

File Logger

Go

Name	Actions	Description	Remove
1	<a href="#">Details</a>	File Logger	<a href="#">Remove</a>
1	<a href="#">Details</a>	Log Levels	<a href="#">Remove</a>

Submit

Reset

Cancel

### **Presence (Presence Server) setting:**

**Step 1.** Click on the *Edit* link (Actions Column) for the Presence Server (not shown). Scroll down the page and locate the **MS RTC Collector Configuration** section. Ensure that the check box for this section is checked as shown below. Enter the network domain name in which the Intelligent Presence Server is located in the **SIP Domain** field. Set the **Transport** drop down box to *tls* and enter *5061* for the **port** field. Define the static route in the following format for the **Define the next hop for a domain (domain next hop next hop port)** field:

*<Domain name of the Microsoft Office Communication R2 server> <IP address of the external interface of the Microsoft Edge server> <TLS Port Number>*

Enter the following values for the respective fields in the UMC to UMS Configuration section: Use default values for the remaining fields in the Presence Server page. Scroll to the bottom of the page and click on the **Submit** button (not shown) to confirm changes.

Field Name	Value
WS Host	<i>IP address of the one-X Portal server</i>
WS Port	<i>9443</i>
WS Service	<i>/ums/services/UserMgmtServicePort</i>
JMS Host	<i>IP address of the one-X Portal server</i>
JMS Port	<i>7286</i>
Login	<i>one-X Portal administrator username</i>
Password	<i>one-X Portal administrator password</i>
Secure Connection	<i>Yes</i>

The screenshot displays two configuration sections. The first section, 'MS RTC Collector Configuration', has a checked checkbox and includes fields for User Name (AveyalPS), SIP Domain (cebp-avaya.com), Transport (tls), Port (5061), Expires (86400), Subscription Failure Retry (3600), and Server Failure Retry (3600). It also features a 'Static Routes' table with one entry: 'avocs.contoso.com' with IP '135.8.19.174' and port '5061'. The second section, 'UMC to UMS Configuration', includes fields for WS Host (135.8.139.171), WS Port (9443), WS Service (/ums/services/UserMgr), JMS Host (135.8.139.171), JMS Port (7286), Login (websphere), Password (Interop123), Secure connection (Yes), Page Size (1000), Resync interval (86400), and Retry interval (180).

<input checked="" type="checkbox"/> MS RTC Collector Configuration	
User Name	AveyalPS
SIP Domain	cebp-avaya.com
Transport	tls
Port	5061
Expires (seconds)	86400
Subscription Failure Retry (seconds)	3600
Server Failure Retry (seconds)	3600
Static Routes	
Define the next hop for a domain (domain next-hop next-hop-port)	avocs.contoso.com 135.8.19.174 5061
UMC to UMS Configuration	
WS Host	135.8.139.171
WS Port	9443
WS Service	/ums/services/UserMgr
JMS Host	135.8.139.171
JMS Port	7286
Login	websphere
Password	Interop123
Secure connection	Yes
Page Size	1000
Resync interval(seconds)	86400
Retry interval(seconds)	180



### Sip-ps (SIP Presence Server) settings:

Click on the **Edit** link (Actions Column) for the SIP Presence Server (Step 2). Ensure that **IPSCCommon** is entered in the host field under the **Host Names** for this component section (not shown). Scroll down the page and locate the table under the **Add a new SIP Transport** section. Click on the first entry under the Actions column as shown below.

SIP Presence Server Configuration

Number of worker queues to use for processing tasks

1100

Server Connection Idle Timeout (seconds)  
-1 = Never; 0 = As last owner disconnects; X = Time in seconds

-1

Max Subscriptions

120000

Max Transactions

50000

Max TCP Connections

2000

Max TLS Sessions

2000

Credentials timeout (in seconds)

300

Realm of the global configuration

presence

Service ID of URI to JID Mapping Component

One session per tuple element in the Publish document?

No

Polite blocking support

No

SIP Stack Configuration Parameters

Add a new SIP Transport

Add new items by selecting from the drop-down and clicking 'GO'.

Add a new

UDP transport

Go

Name	Actions	Description	Remove
1	Details	TLS transport	Remove

☐ Outbound Proxy

Proxy IP address

Proxy Port

Proxy Transport

TCP

Thread count for SIP processing

12

Interval (in seconds) to wait for SIP dialogs to shutdown cleanly before exiting the application

10

**Step 1.** Enter the following values for the respective fields in the TLS transport section as shown above. Use default values for the remaining fields in the TLS transport Configuration page. Click **Submit** to confirm changes and return to the SIP Presence Server page. Use the **Select** button on the SIP Presence Server page (not shown) to accept changes.

Field Name	Value
Hostname of external interface	<i>FQDN of the Intelligent Presence Server</i>
IP address	<i>IP address of the Intelligent Presence Server</i>
Port	<i>15061</i>
Use this transport by default for TLS requests	<i>Yes</i>
Domain used for TLS requests	<i>IPSCCommon</i>
Full path to the certificate file	<i>/opt/IPS/jabber/xcp/certs/IPSCCommon.pem</i>

**TLS transport Configuration**

TLS transport

Hostname of external interface: ips.cebp-aveya.com

IP address: 135.8.139.172

Port: 15061

Use this transport by default for TLS requests: Yes

Domain used for TLS certificate: IPSCCommon

Full path to the certificate file: /opt/IPS/jabber/xcp/cert

Full path to the CA certificate file: /opt/IPS/jabber/xcp/cert

Define an optional external contact for SIP servers to use to contact this transport

External hostname that SIP servers will use for contact:

External port that SIP servers will use for contact:

☐ Routes for this Transport

Add new items by clicking 'GO'.

Add a new Route

Go

Id	Actions	Description	Remove
----	---------	-------------	--------

Submit Reset Cancel

### **Sip-bulksub (SIP Bulk Subscription Server) settings:**

Use default values for the SIP Bulk Subscription Server page. The only exception is to use a value of *25061* for the port field under the TLS transport page.

**Note:** The means of accessing the TLS transport page for the SIP Bulk Subscription Server is the same as described earlier for the SIP Presence Server.

### **SIP-proxy (SIP Proxy) settings:**

Use default values for the SIP Proxy page. The only exception is to use a value of *35061* for the port field under the TLS transport page.

**Note:** The means of accessing the TLS transport page for the SIP Proxy is the same as described earlier for the SIP Presence Server.

Ensure that all the Router and Component elements are started through the XCP Controller page as mentioned in Step 2.



## 7. Configure the Avaya one-X® Portal Server

Refer to [7] for instructions on installing an Avaya one-X® Portal server. These Application Notes only describe configuring the connection to the Intelligent Presence Server. See [8] for documentation on configuring telephony and messaging interfaces on the one-X Portal system.

### 7.1. Install and Configure Presence Security Certificates

Refer to [2] for installing and configuring Intelligent Presence Server certificates on the Avaya one-X® Portal

### 7.2. Configure the Presence Server Component

**Step 1.** Enter the URL: *http://<IPaddress of one-X Portal>/admin* in a web browser and log on to the one-X Portal web interface. Provide an appropriate username and password and click **Logon**.

**Note:** An administrative user (name) must be created on the Microsoft Active Directory service as shown in Section 3. This username must also be provided during Avaya one-X® Portal installation (not shown).



**Step 2.** Click on the *Servers* tab and select the *Presence* link (left hand pane). Click **Add** to add the presence component to the Avaya one-X® Portal configuration.

Avaya one-X Portal Administration

Welcome websphere  
Last login: Monday, December 14, 2009 12:22 PM

Logoff ? Help About

Home Users **Servers** Scheduler System Monitors

Telephony  
Auxiliary Servers  
Voice Messaging  
Conferencing  
**Presence**  
Dial Plan  
Mobility

**Presence Servers**

Server Type: apas 1.0 [Add...](#)

Alias	CN	Extract Certificate
default	oneXP171.cebp-avaya.com	<a href="#">Extract</a>
dummyclientsigner	jclient	<a href="#">Extract</a>
dummyserversigner	jserver	<a href="#">Extract</a>

**Step 3.** Enter the following values in the respective fields for the **View Presence Server** page as shown in the table below. Retain default values for the remaining fields on this page and click on the **Save** button at the bottom of the page (not shown) to confirm the setting changes.

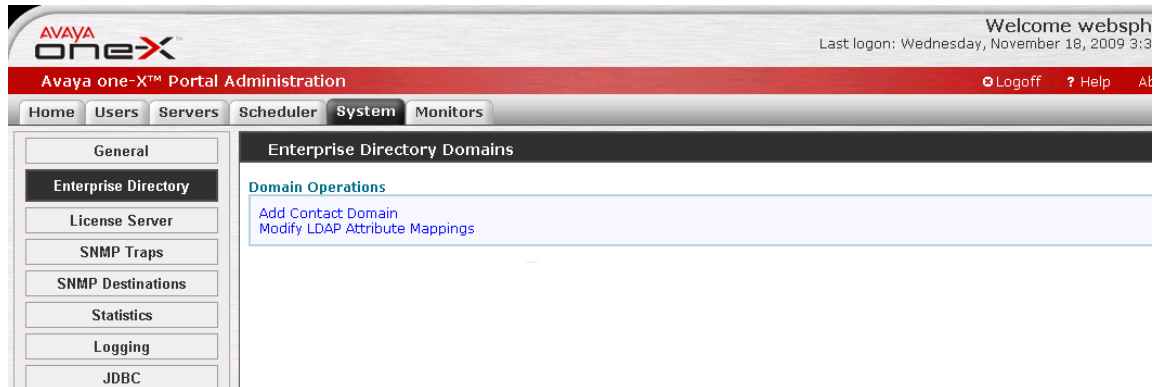
Field Name	Value
Handle	<i>Presencesrv</i>
UMS URL	<i>http://&lt;IP address of the Avaya one-X® Portal server&gt;:9080/ums/services/usermgmtServicePort</i>
Intelligent Presence Server (IPS)	
Host	<i>&lt;IP address of the Intelligent Presence server&gt;</i>
Port	<i>25061</i>
User Management Service (UMS)	
Host	<i>&lt;IP address of the one-X Portal server&gt;</i>
Port	<i>7286</i>
Login	<i>Administrative user name</i>
Passsword (not shown below)	<i>Password for administrative user</i>
Confirm (not shown below)	<i>Confirm password provided above</i>

The screenshot displays the 'Avaya one-X™ Portal Administration' web interface. At the top, there's a header with the Avaya one-X logo and a 'Welcome websphere' message. Below the header is a navigation bar with tabs: Home, Users, Servers, Scheduler, System, and Monitors. The 'Servers' tab is active. On the left, a sidebar contains links to various services: Telephony, Auxiliary Servers, Voice Messaging, Conferencing, Presence (highlighted), Dial Plan, and Mobility. The main area is titled 'View Presence Server' and contains several configuration sections:

- Presence Server Configuration:**
  - Type: apas
  - Version: 1.0
  - \* Handle: presencesrv
  - Description: (empty text box)
  - Enabled: ☒
  - IPS Publish To Port: 15061
  - LPS Consumer Port: 5070
  - LPS Supplier Port: 5060
  - \* UMS URL: http://135.8.139.171:9080/ums/services/UserMgmtServicePort
- Intelligent Presence Server (IPS):**
  - \* Host: 135.8.139.172
  - \* Port: 25061
- User Management Service (UMS):**
  - \* Host: 135.8.139.171
  - \* Port: 7286
  - \* Login ID: websphere

## 7.3. Configure Enterprise Directory

**Step 1.** Click on the **System** tab and select the **Enterprise Directory** link. Click on **Add Contact Domain** to add a Windows based Active Directory server to the configuration.



**Step 2.** Enter the following values in the respective fields for the Add Enterprise Contact Domain page as shown in the table above. Click **OK** to confirm changes.

**Note:** Provide the same administrator user name/password used to log in to the Avaya one-X® Portal web administration interface.

Field Name	Value
Host	<IP Address of the Microsoft Active Directory Server>
Port	389 (default)
Login ID	Administrative user name
Password	Password for administrative user
Base DN	Split the domain name into domain components using Base DN format
Page Size	Use default values shown below
Range Size	Use default values shown below

**Step 3.** The Enterprise Directory Domains page will be updated as shown below.

**Note:** Each Avaya one-X® Portal deployment can authenticate and authorize users from only one Active Directory domain.

Avaya one-X Portal Administration

Welcome Administrator  
Last login: Tuesday, December 1, 2009 11:50 AM

Logoff Help About

Home Users Servers Scheduler System Monitors

General  
Enterprise Directory  
License Server  
SNMP Traps  
SNMP Destinations  
Statistics  
Logging  
JDBC

Enterprise Directory Domains

Domain Operations

Add Contact Domain  
Modify LDAP Attribute Mappings

Domain	Type	Primary Server	Has Backups
avocs.contoso.com	User, Resource, Contact	135.8.19.135	No

**Step 4.** Click on the **Scheduler** tab and select **Enterprise Directory Synchronization** in the left hand pane. Choose **Run Full Sync Now** or **Run Incremental Sync Now** (depending on system usage) to import the users in Microsoft Active Directory Enterprise Users container (See Section 3). If the process is completed successfully then the details are displayed as shown below.

Avaya one-X Portal Administration

Welcome Administrator  
Last login: Tuesday, December 1, 2009 11:50 AM

Logoff Help About

Home Users Servers Scheduler System Monitors

Contact Log Cleanup  
Database Backup  
Enterprise Directory Synchronization  
Modular Messaging Synchronization  
Statistics Cleanup

Enterprise Directory Synchronization

Enabled ☒

Synchronization Schedule Mode: ☐ Daily ☐ Weekly

Incremental Sync Weekly and Full Sync These Weeks of the Month

☐ 1st ☐ 2nd ☐ 3rd ☐ 4th

Day of the Week: Sunday

Time of Day: Hour: 0 Minute: 0

Run Full Sync Now Run Incremental Sync Now

Save Reset

Time	Task ID	Task Type	Task Status
2009-12-01 12:21:42 EST	552	Sync	Task Successful
2009-12-01 12:21:41 EST	552	Sync	Task Started
2009-12-01 11:50:56 EST	551	Sync	Task Successful
2009-12-01 11:50:55 EST	551	Sync	Task Started
2009-12-01 11:43:30 EST	0	Sync	Task Successful
2009-12-01 11:43:29 EST	0	Sync	Task Started
2009-12-01 11:43:29 EST	0	Sync	Task Successful

## 7.4. Configuring Users on the Avaya one-X® Portal Server

**Step 1.** Select the **Users** tab and click on **Portal users** in the left hand pane. Use default values for the drop down boxes shown below and click **Search**. The users added to the 1XP Users security group (see Section 3) are displayed. Select any user under the **User Id** column and click on the user Id (for Example: 1xpUser30007).

The screenshot shows the Avaya one-X Portal Administration interface. The top navigation bar includes 'Home', 'Users', 'Servers', 'Scheduler', 'System', and 'Monitors'. The 'Users' tab is selected, and the 'Portal Users' link is active in the left sidebar. The main content area displays a search results table for Portal Users. The search criteria are: Application: 1XP, Search By: Any, Pattern: \*, Group: Any, Server: Any, Logon: Either. The table lists four users: 1xpUser30007, 1xpUser30008, amatos, and johnd. The '1XP Enabled' column shows 'No' for all users. The user '1xpUser30007' is highlighted.

User Id	First Name	Last Name	Group	Employee Number	1XP Enabled
1xpUser30007	1xpUser30007				No
1xpUser30008	1xpUser30008				No
amatos	tony	matos			No
johnd	john	doe			No

**Step 2.** Click **Enable** for the State field in the View User page. Ensure that the '*user is enabled*' message is displayed (not shown). Select the **Portal Users** link to return to the Portal Users (previous) page and repeat this process for the remaining users.

**Note:** The configuration described in these Application Notes does not require any additional settings to be enabled for the users. Typical Avaya one-X® Portal users might need Telephony settings to function correctly.

The screenshot shows the 'View User' page for user 1xpUser30007. The user's state is 'Disabled', and the 'Enable' button is visible. The 'Group' section shows 'Group Profile <value not set>' with an 'Update...' button. The 'Sessions' section shows 'No Sessions'. The 'Telephony' section shows 'Server' set to 'cmhandle'.

User Id: 1xpUser30007  
First Name: 1xpUser30007  
Last Name:  
Nick Name:  
State: Disabled **Enable**

**Group**  
Group Profile: <value not set>  
**Update...**

**Sessions**  
No Sessions

**Telephony**  
Server: cmhandle

**Step 3.** Select *Enterprise ACL* (in the left hand pane) and click on **Search** in the Browse/Edit watcher list section as shown below. Use default values in the drop down boxes. The list of Microsoft Office Communicator users (added to the 1XP Users security group) is displayed. Ensure that the *Access Status* and *Access Level* for the users are set to *ALLOWED* and *FULL* respectively. Click **Modify** to confirm.

The screenshot shows the Avaya one-X Portal Administration interface. The top navigation bar includes 'Home', 'Users', 'Servers', 'Scheduler', 'System', and 'Monitors'. The left sidebar lists 'Portal Users', 'Unprovisioned Users', 'Prototype Users', 'System Profile', 'Group Profiles', and 'Enterprise ACL' (which is selected). The main content area is titled 'Enterprise ACL' and contains two sections: 'Add watcher' and 'Browse/Edit watcher list'. The 'Add watcher' section has a form with 'Type Watcher Id', 'ALLOWED' (dropdown), 'FULL' (dropdown), and 'Add' and 'Search' buttons. The 'Browse/Edit watcher list' section has a search form with 'Search By' (dropdown), 'Pattern' (dropdown), and a 'Search' button. Below the search form is a table with the following data:

Watcher Id/Uri	Access Status	Access Level	Modify	Remove
johnd	ALLOWED	FULL	Modify	Remove
krisc	ALLOWED	FULL	Modify	Remove

At the bottom of the table, there is a pagination control showing '< << 1 - 2 : 2 >> >'.

## 8. Configuring the Microsoft Real Time Communicator (RTC) service on the Microsoft Office Communicator R2 Server

The Microsoft RTC component must be installed and configured on the Microsoft Office Communicator server. The RTC service enables federating presence with other domains. The Avaya Intelligent Presence Server subscribes to the RTC service via the Microsoft Edge server<sup>9</sup>.

**Note:** The Microsoft RTC service and the Intelligent Presence Server can be configured in the same enterprise domain but must be placed in separate sub domains.

Refer to [2] for instructions on installing and configuring the Microsoft RTC service. Complete the following operations as described in [2].

1. Validate the Edge Server configuration.
2. Open certificate snap in for Microsoft Edge server using MMC snap-in.
3. Check the certificate used by the external interface of the Microsoft Edge server.
4. Generate a certificate with server and client authentication.
5. Download the Certificate Authority (CA) which signed the certificate for the External interface.
6. Add the Certificate Authority (CA) for Microsoft Edge server to Intelligent Presence Server (IPS) trusted list.
7. Generate a self signed certificate for RTC collector to communicate with Microsoft Edge server.
8. Add Intelligent Presence Server (IPS) RTC certificate to Microsoft Edge server trusted root certificates.
9. Configure RTC collector.
10. Add RTC collector as an IM service provider.
11. Add a DNS SRV record for the RTC collector.
12. Restart the Microsoft Edge server service (Access Edge service) after completing changes to the DNS service. (See Step 11, Section 5.2 above)

---

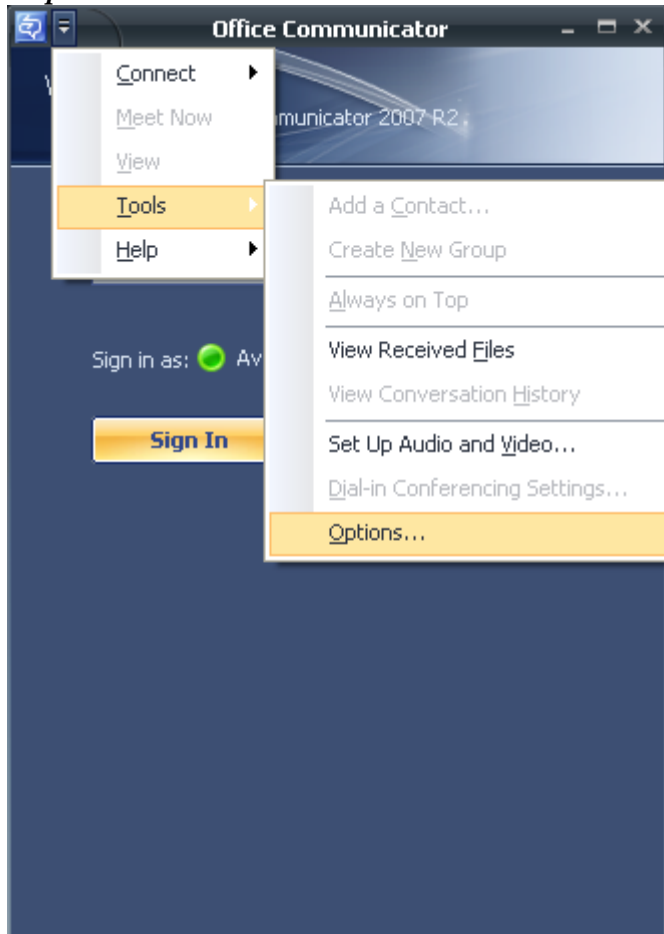
<sup>9</sup> Appropriate certificates must be administered on the Avaya Intelligent Presence server and Microsoft Edge server.



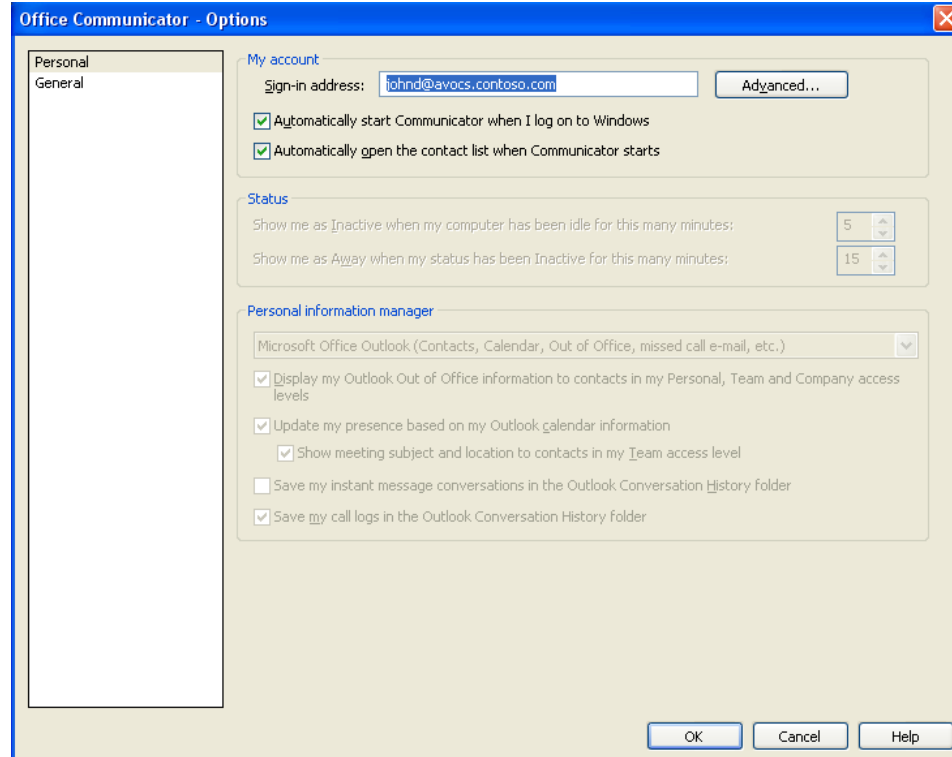
## 9. Configuring Avaya one-X® Portal Users and Microsoft Office Communicator R2 clients for Presence

### 9.1. Microsoft Office Communicator R2 Client Settings

**Step 1.** Open the Microsoft Office Communicator R2 client (not shown) and select **Tools->Options** as shown below.

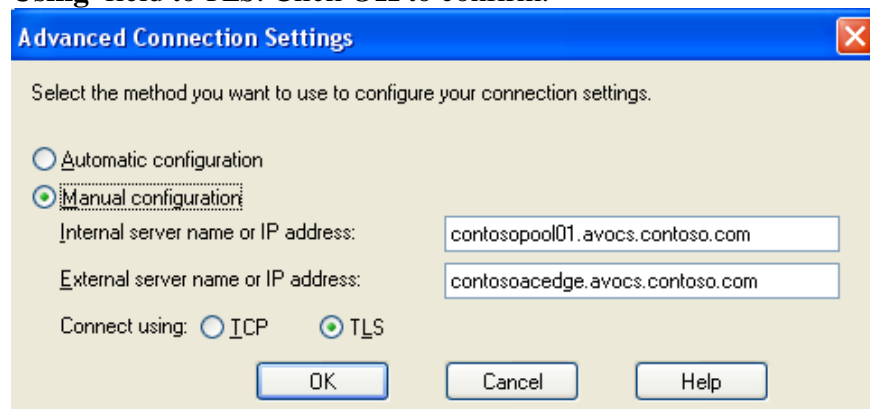


**Step 2.** Enter the user logon name assigned to the Microsoft Office Communicator R2 client in the **sign-in address** field. The user logon name is in the format - <username>@domain name. Check the *Automatically start Communicator when I log on to Windows* and *Automatically open the contact list when Communicator starts* boxes. Click *Advanced...* to continue.



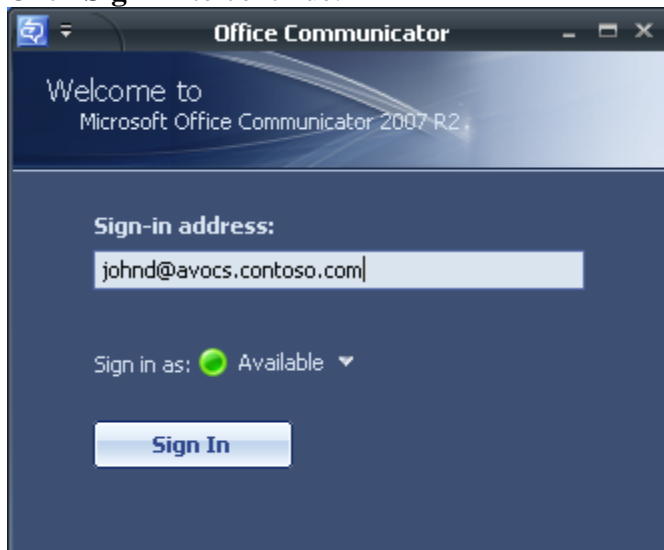
The screenshot shows the 'Office Communicator - Options' dialog box. On the left, the 'Personal' tab is selected. The 'My account' section contains a 'Sign-in address' field with the text 'lohnd@avocs.contoso.com' and an 'Advanced...' button. Below this, two checkboxes are checked: 'Automatically start Communicator when I log on to Windows' and 'Automatically open the contact list when Communicator starts'. The 'Status' section has two spinners: 'Show me as Inactive when my computer has been idle for this many minutes' set to 5, and 'Show me as Away when my status has been Inactive for this many minutes' set to 15. The 'Personal information manager' section has a dropdown menu set to 'Microsoft Office Outlook (Contacts, Calendar, Out of Office, missed call e-mail, etc.)'. Below the dropdown, four checkboxes are present: 'Display my Outlook Out of Office information to contacts in my Personal, Team and Company access levels' (checked), 'Update my presence based on my Outlook calendar information' (checked), 'Show meeting subject and location to contacts in my Team access level' (checked), and 'Save my instant message conversations in the Outlook Conversation History folder' (unchecked). At the bottom, there are 'OK', 'Cancel', and 'Help' buttons.

**Step 3.** Select *Manual configuration*; enter the FQDN of the Microsoft Office Communicator pool in the **Internal server name or IP address** field and the FQDN of the internal interface of the Microsoft Edge server in the **External server name or IP address** field. Set the **Connect Using** field to **TLS**. Click **OK** to confirm.

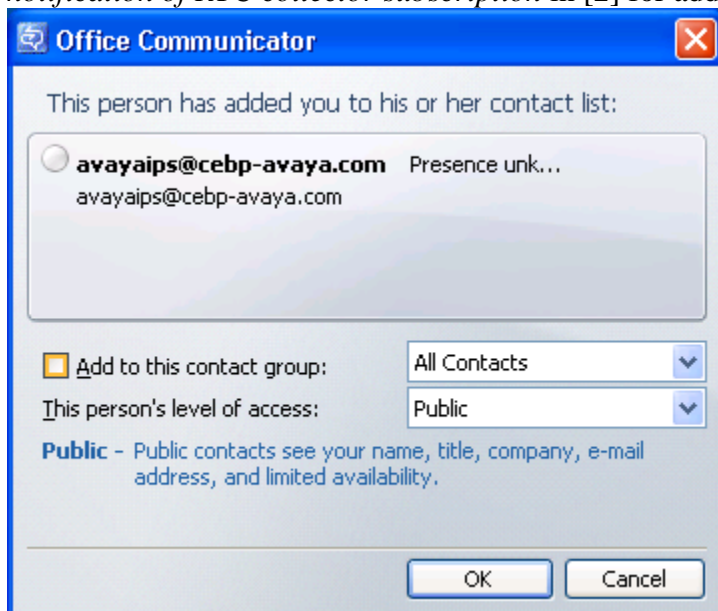


The screenshot shows the 'Advanced Connection Settings' dialog box. It prompts the user to 'Select the method you want to use to configure your connection settings.' There are two radio buttons: 'Automatic configuration' (unselected) and 'Manual configuration' (selected). Below the radio buttons, there are two text fields: 'Internal server name or IP address' with the value 'contosopool01.avocs.contoso.com' and 'External server name or IP address' with the value 'contosoacedge.avocs.contoso.com'. At the bottom, there are two radio buttons for 'Connect using': 'ICP' (unselected) and 'TLS' (selected). At the very bottom, there are 'OK', 'Cancel', and 'Help' buttons.

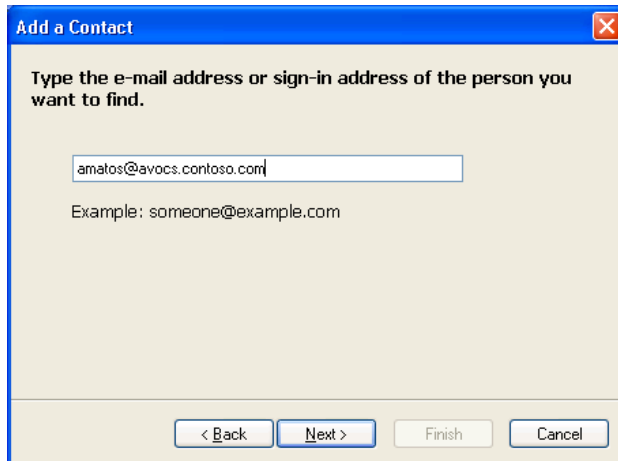
**Step 4.** Ensure that the **sign-in address:** field is populated with the correct user logon name. Click **Sign In** to continue.



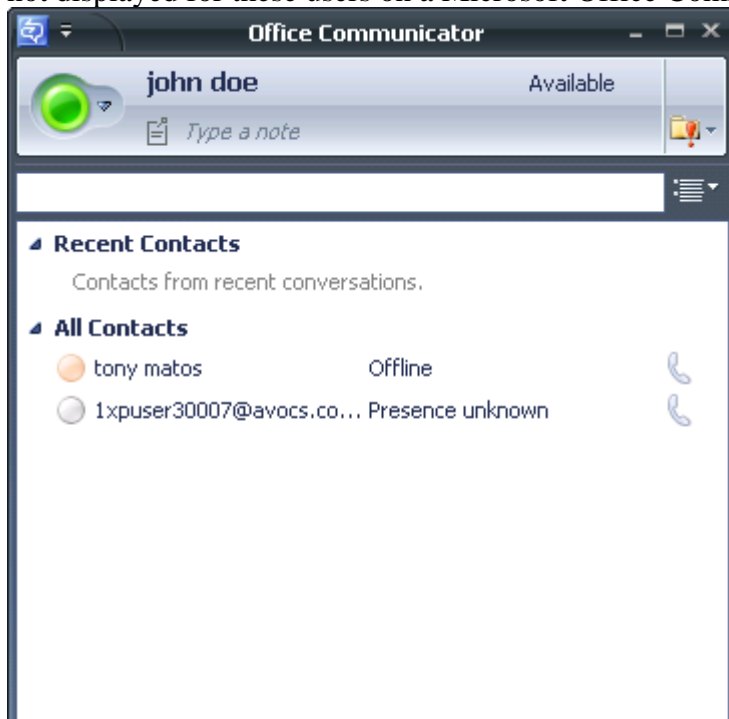
**Step 5.** The Microsoft RTC collector will subscribe to the Microsoft Office Communicator R2 client as shown below. Ensure that the **Add to this contact group** box is unchecked and the **This person's level of access** field is set to *Public* before clicking **OK**. This process is typically done once during initial startup of a Microsoft Office Communicator R2 client. See topic *MOC client notification of RTC collector subscription* in [2] for additional information.



**Step 6.** Click on *Tools* in the top level menu and select *Add a Contact* (not shown). Select Use an e-mail address or sign-in name in the **Add a Contact Wizard** and click **Next** (not shown). Enter the user Id of any user defined in the Microsoft Active Directory Users container and the domain name in the format shown below. Click **Next** to add this user to the contact list of the Microsoft Office Communicator R2 client.



**Step 7.** Contacts for a Microsoft Office Communicator R2 client are displayed below.  
**Note:** Presence information is only displayed for other Microsoft Office Communicator R2 clients. Avaya one-X® Portal users can be added to the Contact List but presence information is not displayed for these users on a Microsoft Office Communicator R2 clients.



## 9.2. Avaya one-X® Portal User Settings

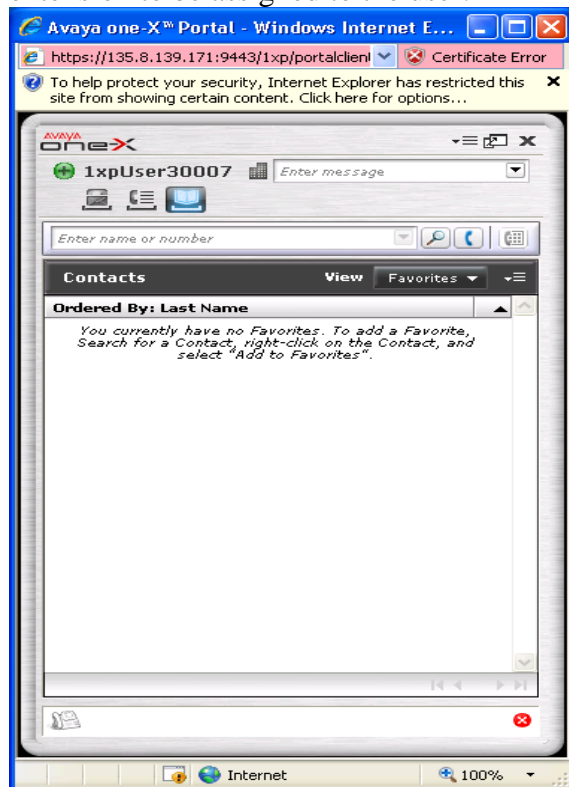
**Step 1.** Enter the URL: *http://<IPaddress of one-X Communicator>/1xp/portalclient* in a web browser and provide an appropriate username and password of an Avaya one-X® Portal User. Click **Log On** to continue.

**Note:** The user must be configured in the Microsoft Active Directory Users Container (See Section 3) and must be enabled as an Avaya one-X® Portal User as described in Section 7.4

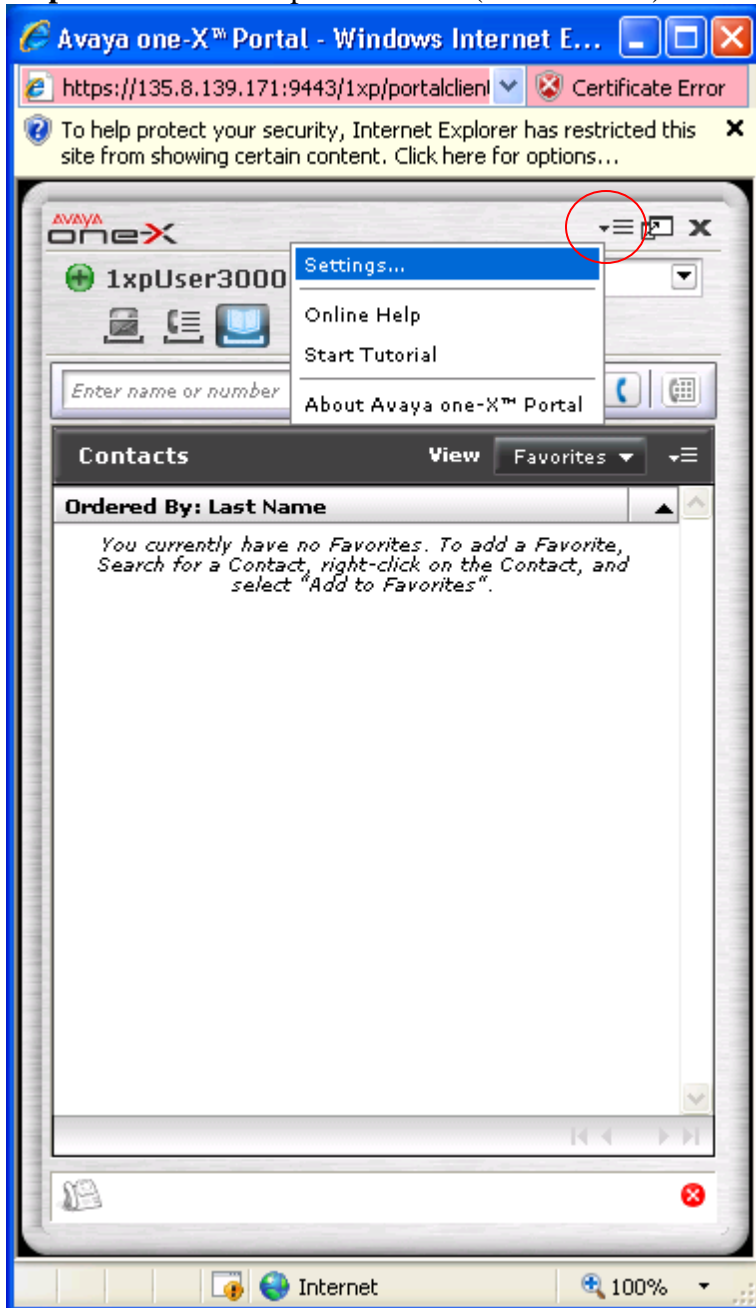


**Step 2.** The Avaya one-X® Portal Client interface for that user is displayed.

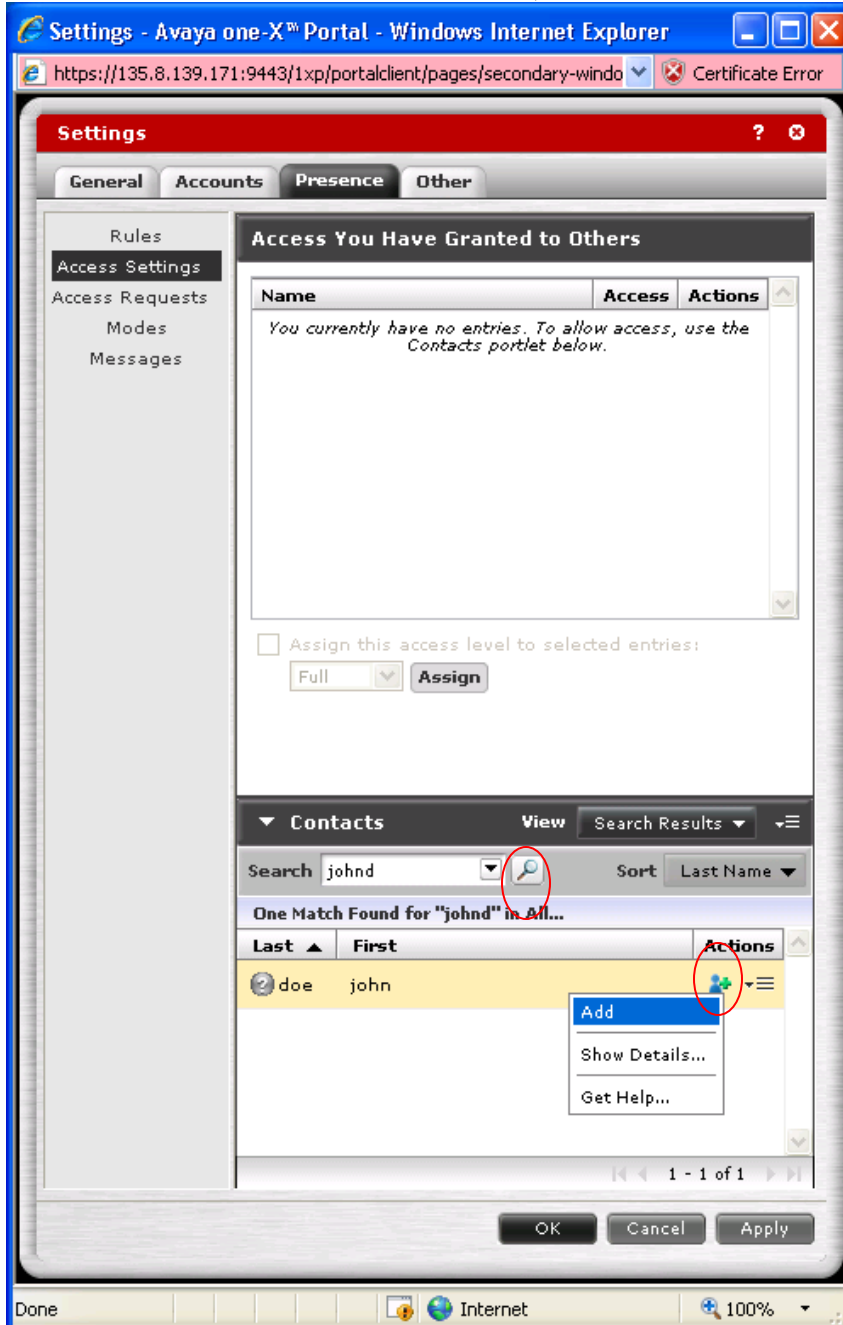
**Note:** An error message might be displayed if no phone extension is configured for the user. The configuration described in this document ignores these messages and does not require an extension to be assigned to the user.



**Step 3.** Access the drop down menu (circled in red) as shown below and select *Settings*.



**Step 4.** Click the **Presence** tab and select **Access Settings** from the left hand pane. Expand the Contacts section and enter the user Id of a Microsoft Office Communicator R2 client (user) in the **Search** field and click the icon (circled) to locate this user. Right click on the icon (circled) under the Actions column and select **Add**; choose **Full** from the subsequent menu (not shown).

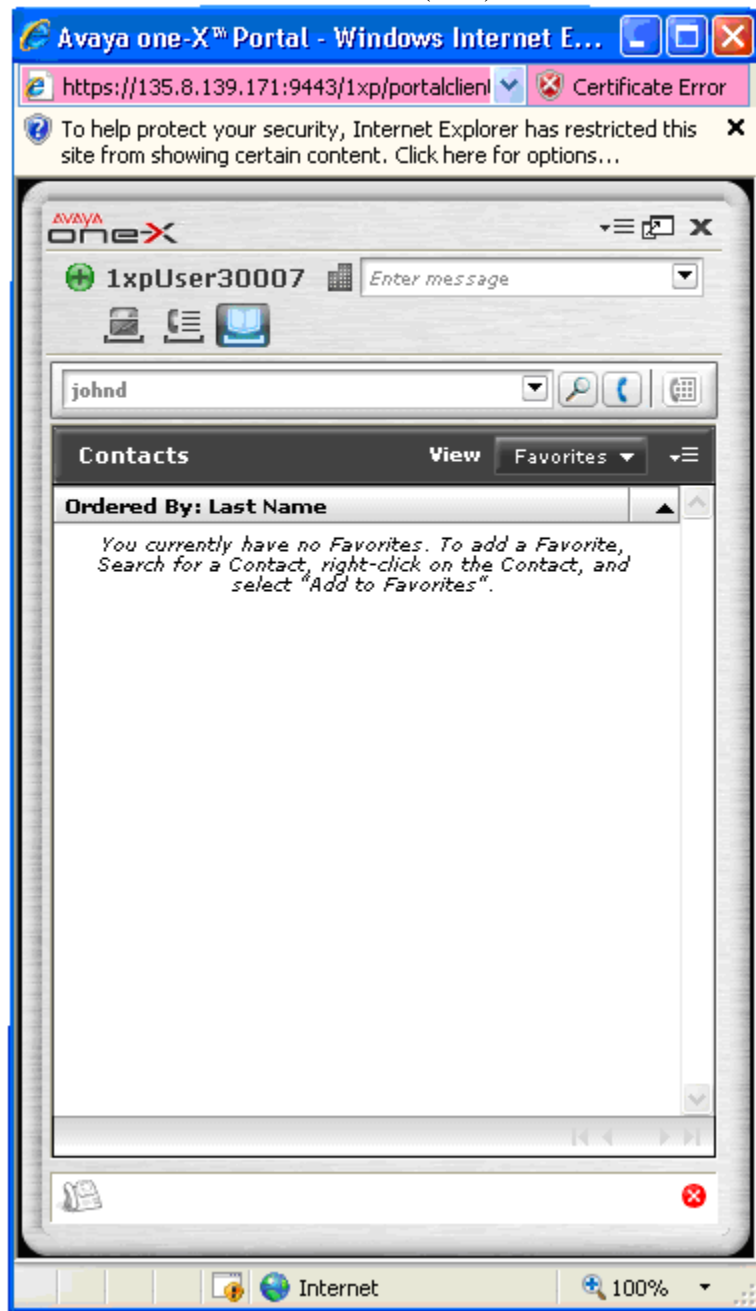


**Step 5.** Ensure that the user has been added to the **Access You Have Granted to Others** section as shown below. The drop down box under the Access column should be set to *Full*. Repeat Steps 1 –5 to add additional users. Click **OK** to confirm changes

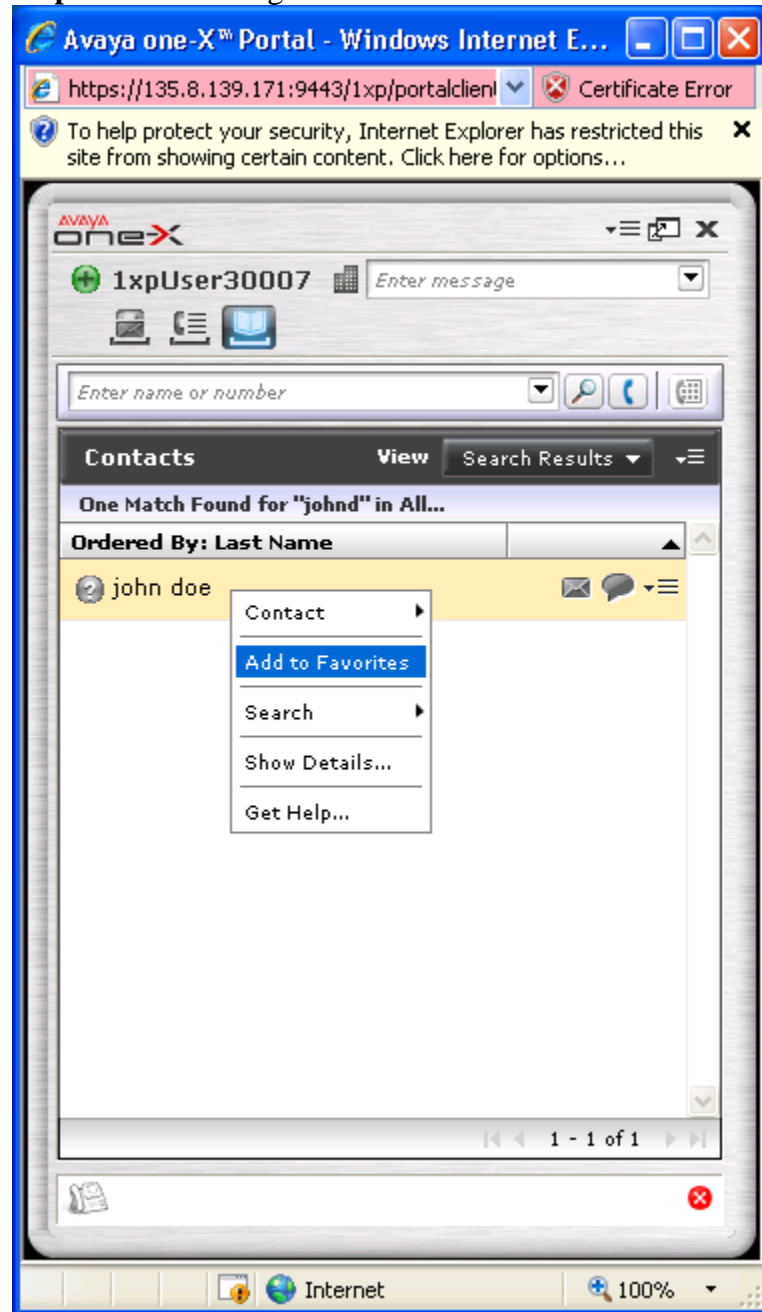




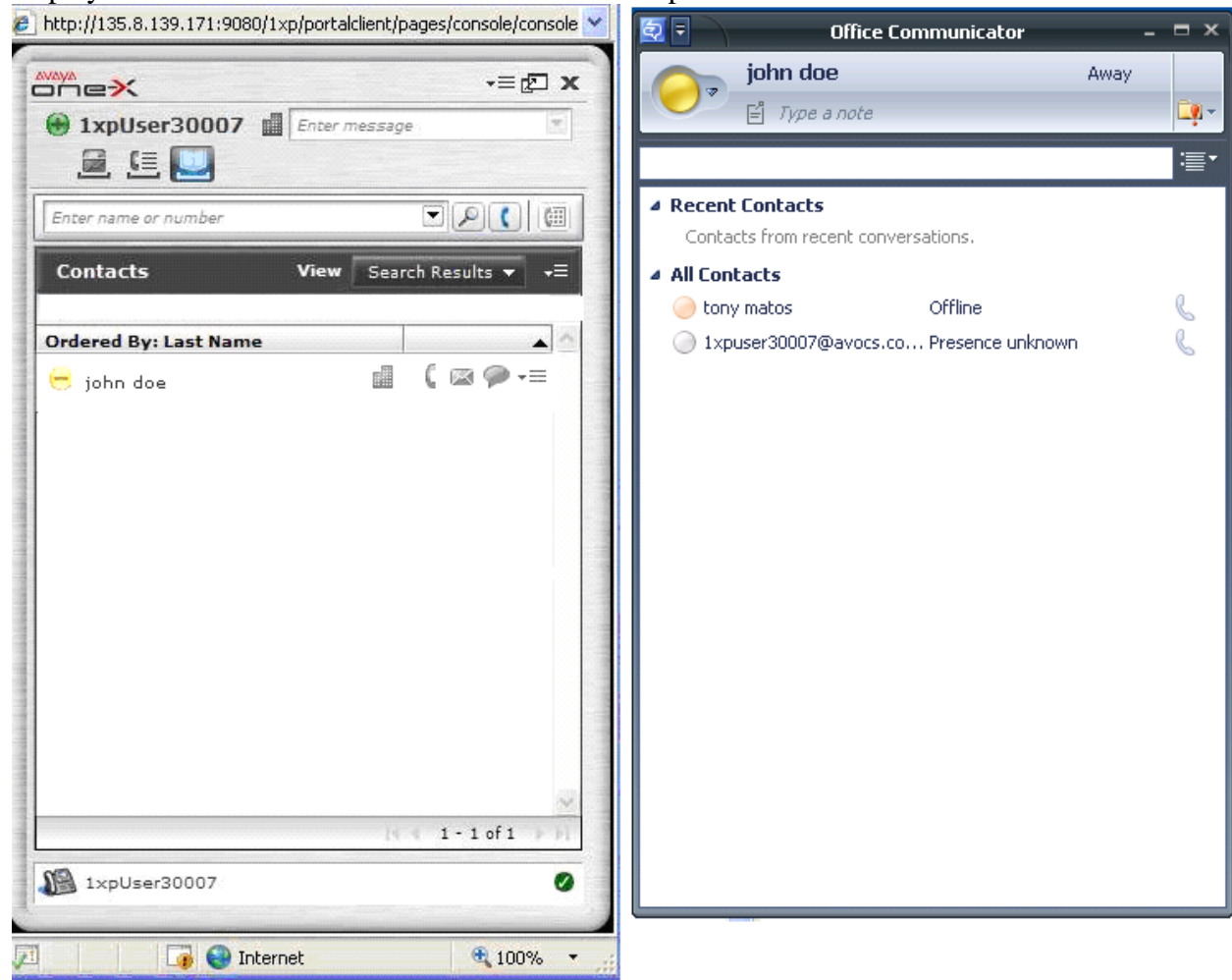
**Step 6.** Select Favorites from the View drop down box and enter the user ID of the Microsoft Office Communicator R2 client (user) in the search field.



**Step 7.** Select and right click on a contact and click **Add to Favorites**.



**Step 8.** Verify that the presence status for Microsoft Office Communicator user John Doe is displayed in the one-X Portal User client for user 1xpUsr30007.



## 10. Verification

This section provides steps involved in verifying presence status, for a Microsoft One-X Communicator R2 user, is updated on a One-X® Portal client.

1. Ensure that Microsoft Office Communicator R2 users and Avaya One-X® portal users are assigned in the Microsoft Active Directory; these users are collectively termed as Enterprise Users.
2. Create security groups in the Microsoft Active Directory and assign enterprise users to appropriate security groups.
3. Install and configure certificates on the Microsoft Edge server and ensure that the Office Communications Service Access Edge service is started on this server.
4. Configure the Intelligent Presence Server plug-in and components; verify that these components are started and in a *running* state.
5. Configure the Presence component on the Avaya One-X® Portal server; update the Enterprise Directory component on the Avaya One-X® portal to download user information from the Microsoft Active Directory server.
6. Install and configure the Microsoft Real Time Collector (RTC) on the Microsoft Office Communication R2 server; ensure that this service is started.
7. Configure the Avaya One-X® Portal clients and Microsoft Office Communicator R2 users; add the Microsoft Office Communicator R2 users to the Avaya One-X® Portal clients and ensure that both entities are online to view presence information.
8. Update presence information for any Microsoft Office Communicator R2 user and verify that the presence status for that user is updated on an Avaya One-X® portal client.

## 11. Conclusion

These Application Notes describe the steps involved in relaying presence information for a Microsoft Office Communicator R2 user to Avaya One-X® Portal clients. The presence status for a Microsoft Office Communicator R2 user is routed through an RTC collector to a Microsoft Edge server; the information is passed from the internal interface of this server to the external interface that is connected to an Avaya One-X portal server. A Presence server connector on the Avaya One-X® Portal server transmits presence data to an Intelligent Presence Server; this server updates presence status for a Microsoft Office Communicator R2 user on the Avaya One-X® portal clients. The configuration can be verified based on the procedure outlined in this document.

## 12. Additional References

- [1] Microsoft Office Communications Server 2007 R2 - Deploying Edge Servers for External User Access; Updated: July 2009
- [2] Intelligent Presence Server (IPS) Installation and Configuration Guide; Version 1.0 SP1, 02-602753, Release 1.0, Issue 1, March 2009
- [3] Microsoft Office Communications Server 2007 Technical Overview; Version 1.1, Oct 2008.
- [4] Microsoft Office Communications Server 2007 Enterprise Edition Deployment Guide; Version 1.1, Oct 2007.
- [5] Microsoft Office Communications Server 2007 Enterprise Voice Planning and Deployment Guide; Version 1.0, Dec 2007.
- [6] Microsoft Office Communications Server 2007 Administration Guide; Version 1.2, July 2008.
- [7] Implementing Avaya one-X® Portal; October 2008
- [8] Sample Configuration for Avaya one-X® Portal – Issue 1.0

---

**©2010 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at [interoplabnotes@list.avaya.com](mailto:interoplabnotes@list.avaya.com)