



## **Application Notes for Configuring Trio Enterprise R5.0 from Enghouse Interactive AB with Avaya Aura® Presence Services 6.2.5 – Issue 1.0**

### **Abstract**

These Application Notes describe how to configure an Avaya Aura® Presence Services to interface with Trio Enterprise R5.0. Trio Enterprise display presence status of each monitored phone.

Readers should pay attention to Section 2, in particular the scope of testing as outlined in Section 2.1 as well as the observations noted in Section 2.2, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect Compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

These Application Notes describes how to configure an Avaya Aura® Presence Services to interface with Trio Enterprise R5.0. Trio Enterprise display presence status of each monitored phone.

## 2. General Test Approach and Test Results

The general test approach was to configure Trio Enterprise server connects to Presence Services and display enterprise phones' status on Trio Enterprise Attendant window.

During tests, phones are setup to status such as on hook, off-hook. From the Attendant window, monitor presence status of a user. Change the presence status of the phones. Attendant window displays the new status. Avaya one-X Communicator and Avaya Flare for window were used during compliance test.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

### 2.1. Interoperability Compliance Testing

The compatibility tests included the following.

- Set phone to busy, off-hook.
- Set the phone to available, on hook.

### 2.2. Test Results

Tests were performed to confirm interoperability between the Trio Enterprise and Presence Service. All the test cases passed successfully.

### 2.3. Support

For technical support on Trio products, please use the following web link.

<http://www.trio.com/web/Support.aspx>

Enghouse Interactive AB can also be contacted as follows.

Phone: +46 (0)8 457 30 00

Fax: +46 (0)8 31 87 00

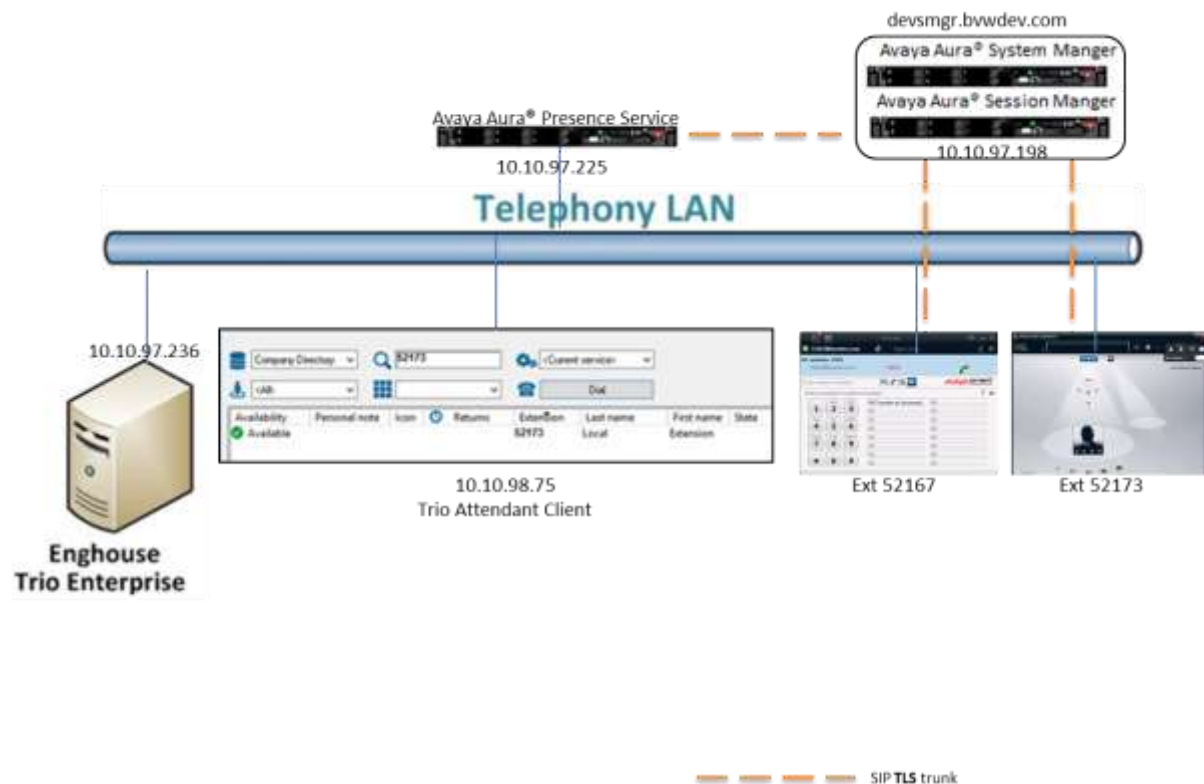
E-mail: [infosweden@enghouse.com](mailto:infosweden@enghouse.com)

### 3. Reference Configuration

**Figure 1** shows the network topology during compliance testing. Trio Enterprise is connected to Presence Services via LAN network. The Presence Services is configured as a SIP Endpoint on Session Manager. System Manager is used to configure user with Presence Services option enabled.

In compliance test, Trio Enterprise monitored subscriber shown in the table below

Device Type	Extension
Avaya one-X Communicator	52167
Avaya Flare Experience	52173



**Figure 1: Configuration for Avaya Presence Services and Trio Enterprise R5.0**

## 4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® Presence Services	6.2.5
Avaya Aura® System Manager	System Manager 6.3 – FP4
Avaya Aura® Session Manager	System Manager 6.3 – FP4
Avaya one-X Communicator	6.2.4.07 FP4
Avaya Flare Experience	1.0.1
Trio Enterprise Running on a Windows 2008 R2 64-bit server.	Version 5.0

## 5. Configure Avaya Aura® Presence Services

This section deals with the configuration of Presence Services. It is assumed that Presence Services server is installed. Presence Services interacts with several external entities like presence sources or user management services in order to gather and provide presence information. During compliance test, Presence Services is connected to System Manager and Session Manager is configured, the steps below will show to verify that the configuration in place is correct.

The configuration management is performed through the **XCP Controller** web-based GUI. Initialize the XCP Controller web interface by browsing to **https:// <ip-address>:7300/admin**, where <ip-address> is the IP address of the Presence Services server and log in with the appropriate credentials. The XCP controller web-based GUI is displayed as shown below.

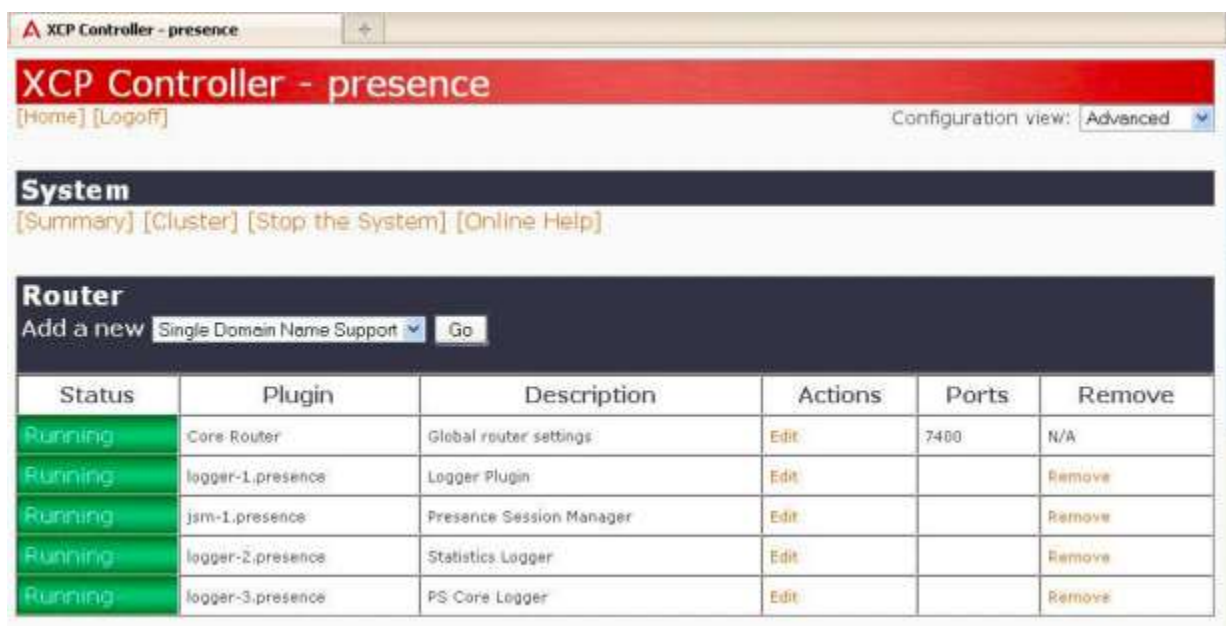
Status	Plugin	Description	Actions	Ports	Remove
Running	Core Router	Global router settings	<a href="#">Edit</a>	7400	N/A
Running	logger-1.presence	Logger Plugin	<a href="#">Edit</a>		<a href="#">Remove</a>
Running	jsm-1.presence	Presence Session Manager	<a href="#">Edit</a>		<a href="#">Remove</a>
Running	logger-2.presence	Statistics Logger	<a href="#">Edit</a>		<a href="#">Remove</a>

## 5.1. Verify Avaya Aura® Session Manager is Configured as Trusted Host on Presence Services

The steps below document how to configure Session Manager as a trusted host on Presence Services. In the **Configuration view**, select **Advanced** to change view.



After setting advanced configuration view, navigate to the **Router** section of the XCP Controller and click the **Edit** action for the **Core Router - Global router settings**.



On the **Global Settings Configuration** page that appears scroll down to display **Mutually Trusted TLS Hostnames**. Ensure that IP address of the virtual SM-100 interface on Session Manager is configured in the **Host Filters**, and if not add that IP address. In this case the IP address of the virtual SM-100 interface is **10.10.97.198** as shown below. Click **Submit** to save changes.

The screenshot shows a web browser window with the URL `https://10.97.225.7300/admin?action=view&xpath=/jabber/global`. The page is titled "Global Settings Configuration" and contains several sections:

- SNMP Configuration**: Includes "Enable SNMP" (set to "Yes") and "Count errors" (set to "No").
- Federation Domains**: Includes a text area for "Federation Domain(s)".
- Avaya Multimedia Messaging Configuration**: Includes a text input for "Avaya Multimedia Messaging Domain".
- Mutually Trusted TLS Hostnames**: Includes a section for "Host Filters" with a text area for "Host(s)".

The "Host(s)" text area contains the following text:

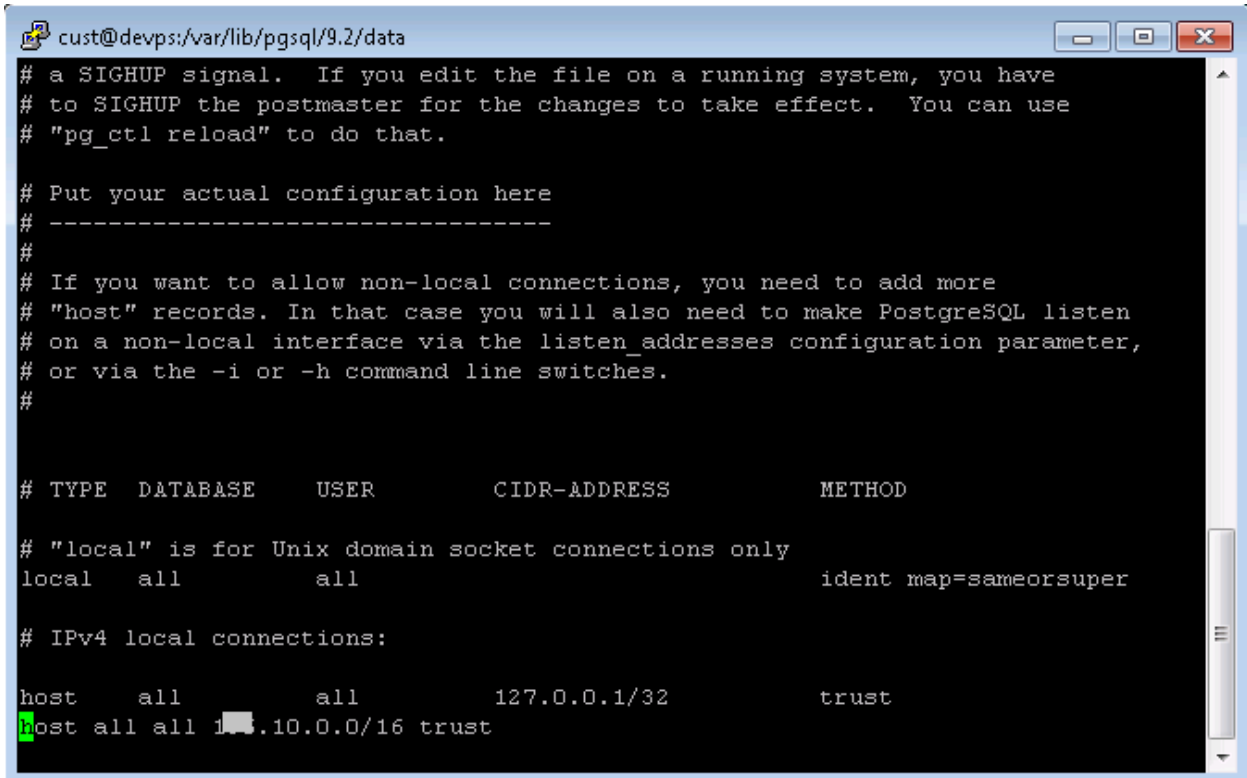
```
devps.bvwdev.com
10.10.97.198
10.10.98.75
```

At the bottom of the page, there are three buttons: "Submit", "Reset", and "Cancel". A green message at the bottom left states: "Fields marked with a \* require values."

## 5.2. Configure Database Engine (Postgres DB) to Accept Connection from Trio Enterprise

Login Presence Services command window with appropriated credential. Add a connection to allow non-local connects (modify the example to fit the environment) by modify **pg\_hba.conf**.

Using command **vi pg\_hba.conf**, scroll to **IPv4 local connection** section modify **host all all 10.10.0.0/16 trust**. Type **:wq** to save changes and quit.



```
cust@devps:/var/lib/pgsql/9.2/data
# a SIGHUP signal.  If you edit the file on a running system, you have
# to SIGHUP the postmaster for the changes to take effect.  You can use
# "pg_ctl reload" to do that.

# Put your actual configuration here
# -----
#
# If you want to allow non-local connections, you need to add more
# "host" records.  In that case you will also need to make PostgreSQL listen
# on a non-local interface via the listen_addresses configuration parameter,
# or via the -i or -h command line switches.
#

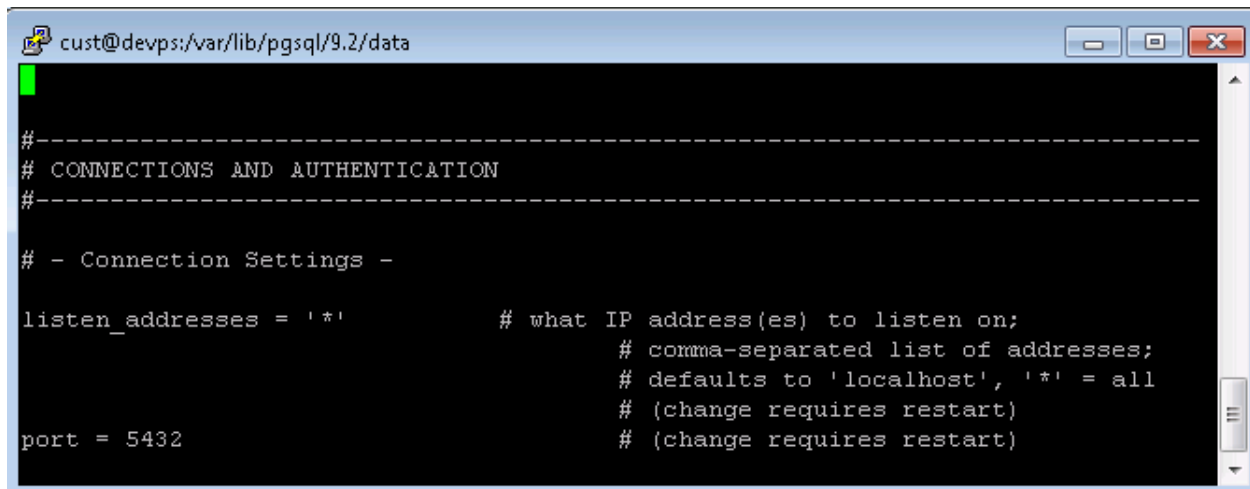
# TYPE      DATABASE      USER      CIDR-ADDRESS      METHOD

# "local" is for Unix domain socket connections only
local      all             all                                     ident map=sameorsuper

# IPv4 local connections:
host       all             all       127.0.0.1/32      trust
host all all 10.10.0.0/16 trust
```



Modify **postgresql.conf** to change **listen\_addresses='\*'** as shown below, type :wq to save changes and quit.



```
cust@devps:/var/lib/pgsql/9.2/data

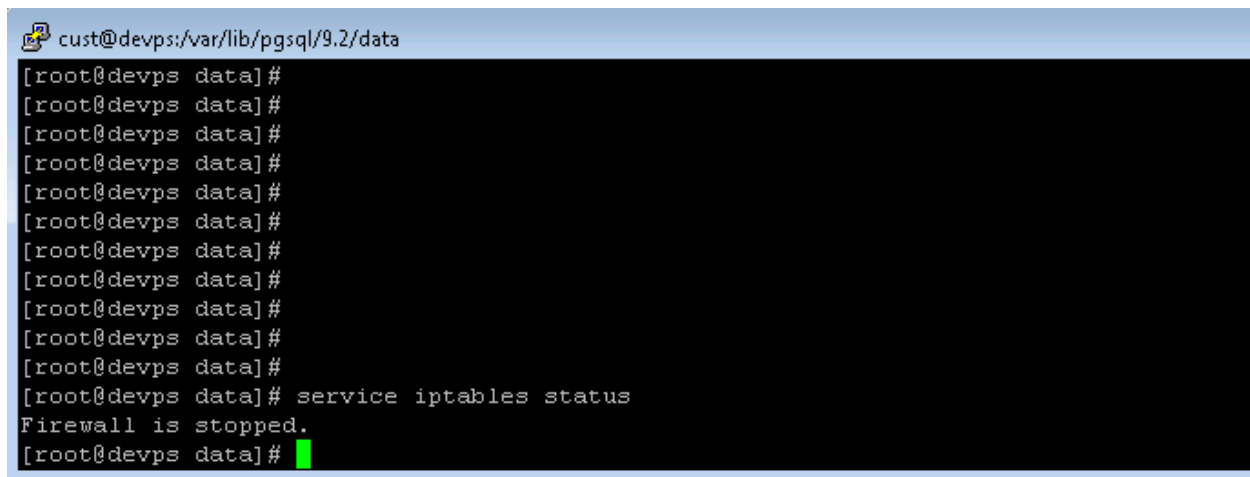
#-----
# CONNECTIONS AND AUTHENTICATION
#-----

# - Connection Settings -

listen_addresses = '*'          # what IP address(es) to listen on;
                                # comma-separated list of addresses;
                                # defaults to 'localhost', '*' = all
                                # (change requires restart)
port = 5432                     # (change requires restart)
```

Restart Presence Services, enter **/etc/init.d/postgresql restart**.

Verify that firewall is disabled using command **service iptables status** (if service is on using command **service iptables stop** to disable firewall).

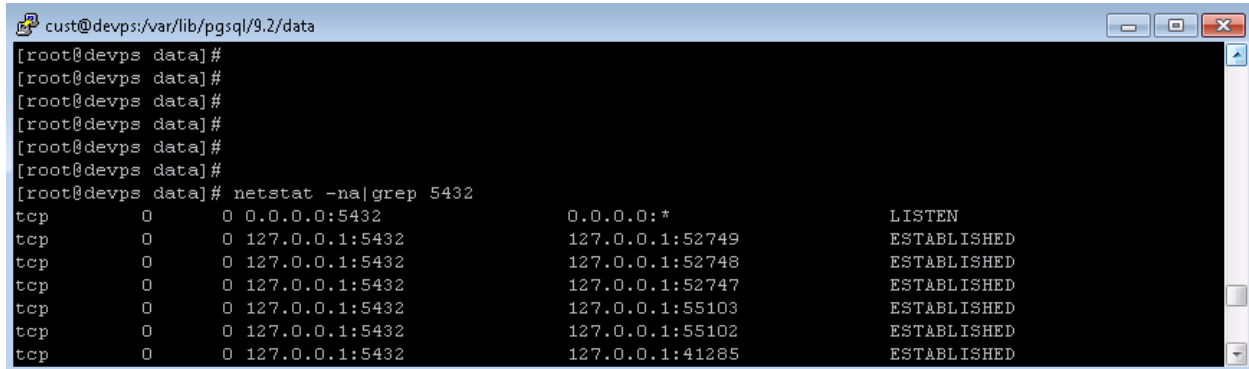


```
cust@devps:/var/lib/pgsql/9.2/data

[root@devps data]#
[root@devps data]#
[root@devps data]#
[root@devps data]#
[root@devps data]#
[root@devps data]#
[root@devps data]#
[root@devps data]#
[root@devps data]#
[root@devps data]#
[root@devps data]#
[root@devps data]# service iptables status
Firewall is stopped.
[root@devps data]#
```

Verify that Presence Services have 5432 port open and listen on all:  
**netstat -na |grep 5432**

Output should include: **tcp 0 0 0.0.0.0:5432 0.0.0.0:\* LISTEN**



A terminal window titled 'cust@devps:/var/lib/pgsql/9.2/data' showing the command 'netstat -na | grep 5432' and its output. The output lists the listening state for port 5432 on all interfaces (0.0.0.0) and several established connections from 127.0.0.1 to the same port.

```
cust@devps:/var/lib/pgsql/9.2/data
[root@devps data]#
[root@devps data]#
[root@devps data]#
[root@devps data]#
[root@devps data]#
[root@devps data]#
[root@devps data]# netstat -na | grep 5432
tcp        0      0 0.0.0.0:5432        0.0.0.0:*           LISTEN
tcp        0      0 127.0.0.1:5432      127.0.0.1:52749     ESTABLISHED
tcp        0      0 127.0.0.1:5432      127.0.0.1:52748     ESTABLISHED
tcp        0      0 127.0.0.1:5432      127.0.0.1:52747     ESTABLISHED
tcp        0      0 127.0.0.1:5432      127.0.0.1:55103     ESTABLISHED
tcp        0      0 127.0.0.1:5432      127.0.0.1:55102     ESTABLISHED
tcp        0      0 127.0.0.1:5432      127.0.0.1:41285     ESTABLISHED
```

## 6. Configure Avaya Aura® Session Manager

### 6.1. Administer Presence Services SIP Entity

A SIP entity must be administered for each SIP-based telephony system that connects to Session Manager. To add a SIP Element, select **Routing** → **SIP Elements** on the left panel menu and then click the **New** button (not shown). Enter the following values when administering Presence Services as a SIP Element:

- **Name:** Enter descriptive name; in this case that is **DevPS**.
- **FQDN or IP Address:** Enter the IP address of the Presence Services server; in this case that is **devps.bvwdev.com**
- **Type:** Enter **Presence Services** for Presence Services
- **Time Zone:** Select appropriate time zone for the location
- **SIP Link Monitoring:** Select **Use Session Manager Configuration** from the drop down list, which is a default value. Click **Commit** to save changes.

The screenshot displays the 'SIP Entity Details' page in the XCP Controller - presence application. The left sidebar shows the 'Routing' menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and 'General'. The form contains the following fields:

- Name:** DevPS
- FQDN or IP Address:** devps.bvwdev.com
- Type:** Presence Services
- Notes:**
- Adaptation:**
- Location:**
- Time Zone:** America/Fortaleza
- SIP Timer B/F (in seconds):** 4
- Credential name:**
- Call Detail Recording:** none

Buttons for 'Commit' and 'Cancel' are visible in the top right corner.

## 6.2. Administer Element Links

To create an Element Link, select **Routing** → **Element Links** on the left panel menu and then click the **New** button (not shown). In the new **Element Links** page that appears, enter the following values when creating the link between Presence Services and Session Manager:

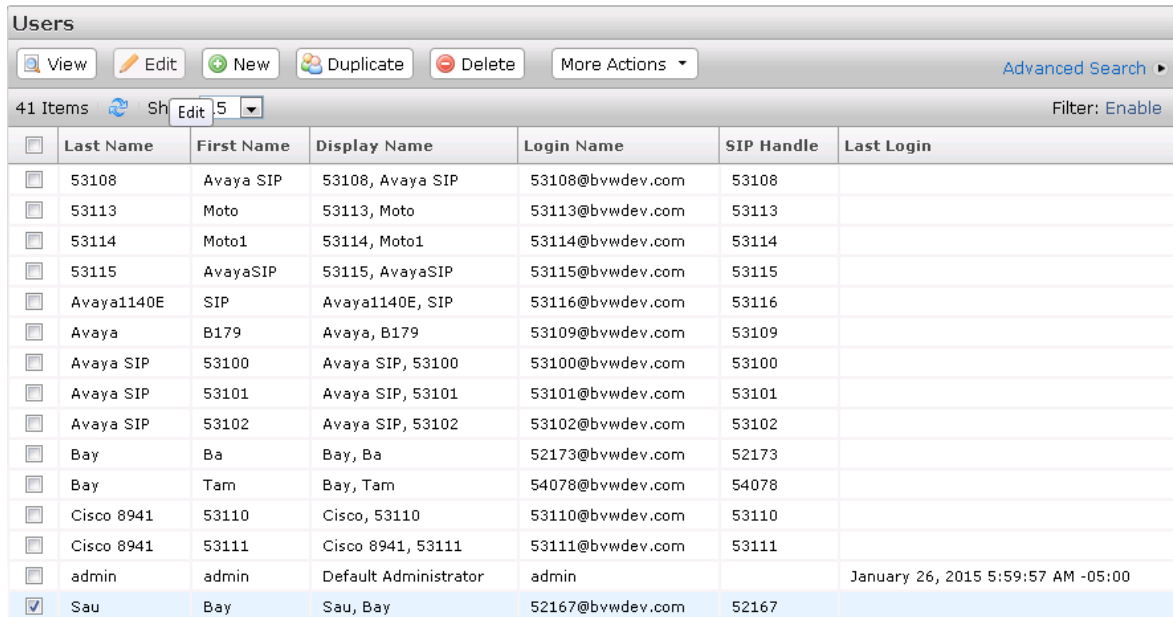
- **Name:** Enter a descriptive name; in this case that is **LinktoPS**.
- **SIP Entity 1:** Select the Session Manager SIP Element from the drop down list configured in this case that is **DevSM**.
- **Protocol:** Enter the transport protocol to be used for SIP requests; in this case that is **TLS**.
- **Port:** Enter port number to which the Presence Services SIP Element sends its SIP requests; in this case that is **5061**.
- **SIP Entity 2:** Enter Presence Services SIP Element created in **Section 6.1**; in this case that is **DevPS**.
- **Port:** Enter the port number on which the Presence Services SIP Element expects to receive SIP requests; in this case that is **5061**.
- **Trusted:** Check the checkbox in order to trust the other system.
- **Notes:** Optional.

Click **Commit** to save changes.



### 6.3. Configure Presence Services for User

To add Presence Service to user, select **Users** → **User Management** → **Manage Users**, select user that need to be modified, in this case user **52167** is selected and click **Edit** button to open user detail page.



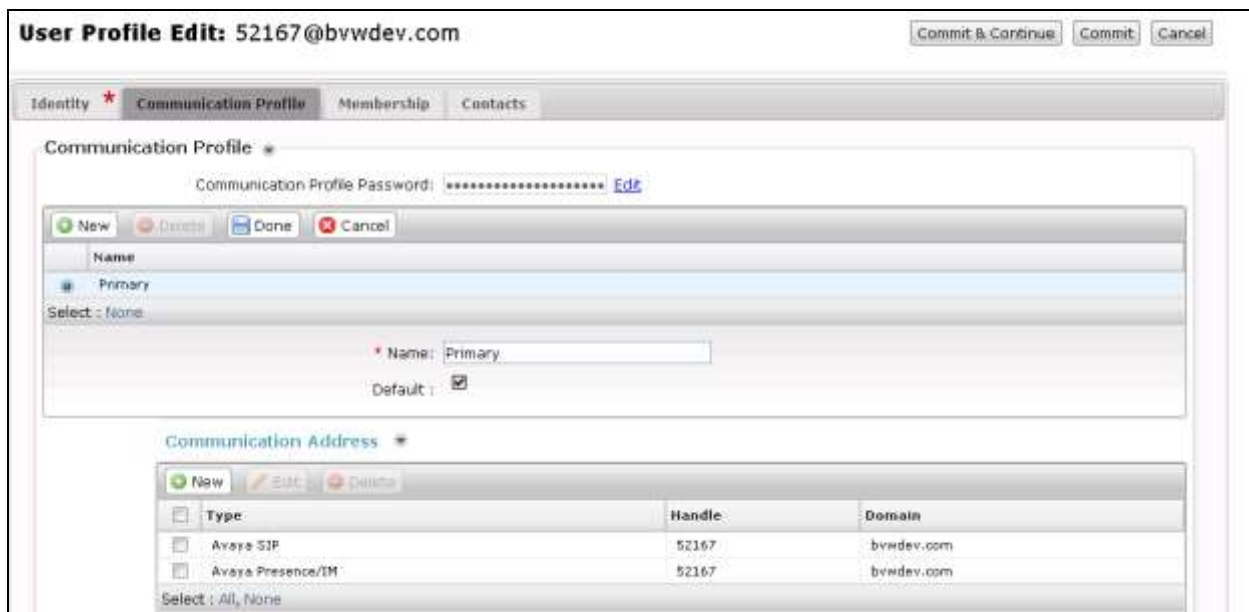
Users

View Edit New Duplicate Delete More Actions Advanced Search

41 Items Show Edit 5 Filter: Enable

	Last Name	First Name	Display Name	Login Name	SIP Handle	Last Login
<input type="checkbox"/>	53108	Avaya SIP	53108, Avaya SIP	53108@bvwddev.com	53108	
<input type="checkbox"/>	53113	Moto	53113, Moto	53113@bvwddev.com	53113	
<input type="checkbox"/>	53114	Moto1	53114, Moto1	53114@bvwddev.com	53114	
<input type="checkbox"/>	53115	AvayaSIP	53115, AvayaSIP	53115@bvwddev.com	53115	
<input type="checkbox"/>	Avaya1140E	SIP	Avaya1140E, SIP	53116@bvwddev.com	53116	
<input type="checkbox"/>	Avaya	B179	Avaya, B179	53109@bvwddev.com	53109	
<input type="checkbox"/>	Avaya SIP	53100	Avaya SIP, 53100	53100@bvwddev.com	53100	
<input type="checkbox"/>	Avaya SIP	53101	Avaya SIP, 53101	53101@bvwddev.com	53101	
<input type="checkbox"/>	Avaya SIP	53102	Avaya SIP, 53102	53102@bvwddev.com	53102	
<input type="checkbox"/>	Bay	Ba	Bay, Ba	52173@bvwddev.com	52173	
<input type="checkbox"/>	Bay	Tam	Bay, Tam	54078@bvwddev.com	54078	
<input type="checkbox"/>	Cisco 8941	53110	Cisco, 53110	53110@bvwddev.com	53110	
<input type="checkbox"/>	Cisco 8941	53111	Cisco 8941, 53111	53111@bvwddev.com	53111	
<input type="checkbox"/>	admin	admin	Default Administrator	admin		January 26, 2015 5:59:57 AM -05:00
<input checked="" type="checkbox"/>	Sau	Bay	Sau, Bay	52167@bvwddev.com	52167	

In **User Profile Edit** page, scroll down to **Communication Address** section, verify there is an **Avaya Presence/IM** item added as shown below for **52167**.



User Profile Edit: 52167@bvwddev.com

Commit & Continue Commit Cancel

Identity \* Communication Profile Membership Contacts

Communication Profile \*

Communication Profile Password: \*\*\*\*\* Edit

New Delete Done Cancel

Name

Primary

Select : None

Name: Primary

Default : ☒

Communication Address \*

New Edit Delete

Type	Handle	Domain
Avaya SIP	52167	bvwddev.com
Avaya Presence/IM	52167	bvwddev.com

Select : All, None

Scroll to **Presence Profile**; verify that Presence system is selected for user as show below. Click **Commit** to save changes.

https://devamp.bwwdev.com/3MGR/

Getting Started | Suggested Sites | Web Slice Gallery

- CS 1000 Endpoint Profile
- Messaging Profile
- CallPilot Messaging Profile
- IP Office Endpoint Profile
- Presence Profile**
  - \* System: DevPS (7)
  - SIP Entity: DevPS
  - \* IM Gateway SIP Entity: DevPS
  - Publish Presence with AES Collector: System Default
- Conferencing Profile
- Work Assignment Profile

\* Required

Commit & Continue | Commit

## 7. Configure TRIO Enterprise for Avaya Aura® Presence Services

This section describes how to integrate Trio Enterprise Presence Services. The installation of the Trio Enterprise software is assumed to be completed and the Trio services are up and running.

### 7.1. Install Java Runtime

Presence connectivity between TE and Avaya is dependent on Java. Java runtime is required on TE server

Download and start the installation of Java runtime environment from [www.java.com](http://www.java.com)



Select **Install**, and unselect installation of ad-ware. Follow instruction on the screen to completed installation process. Select Close when process is completed.

## 7.2. Install Local Presence Service Client

The Java-based Local Presence Service (LPS) client application connects to Presence Services display subscribe and publish presence status information on behalf of one or many users. It is recommended to install LPS client to make sure communication between Avaya systems are working. Unzip file LPS-6.2.4.0-SDK-1.0-SNAPSHOT-39.zip (this file can be obtained on devconnectprogram.com). Open the file lps.properties to modify as below:

```
## SMGR parameters

# Defines presence config service URL. Used for domain conversion
# No conversion is performed if this parameter is empty
# Use host name rather than IP address, especially if it is included in SSL certificate

smgr.host=devsmgr.bvwdev.com

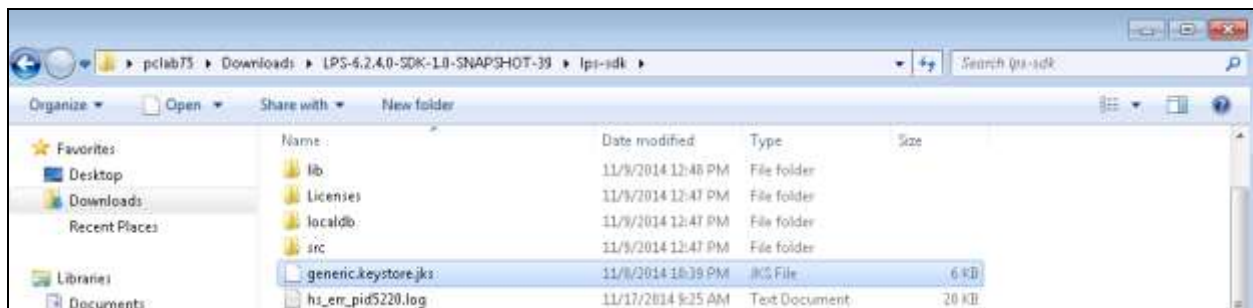
# SMGR naming port. Default value is 1399
#smgr.naming.port=1399

# security parameters. The same values are used for all SMGR services
smgr.username=admin
smgr.password=abc@123

## PS connection parameters
# PS host (required)
# Use host name rather than IP address, especially if it is included in SSL certificate
ps.host=10.10.97.225
```

Leave other sections as default. Save file and close.

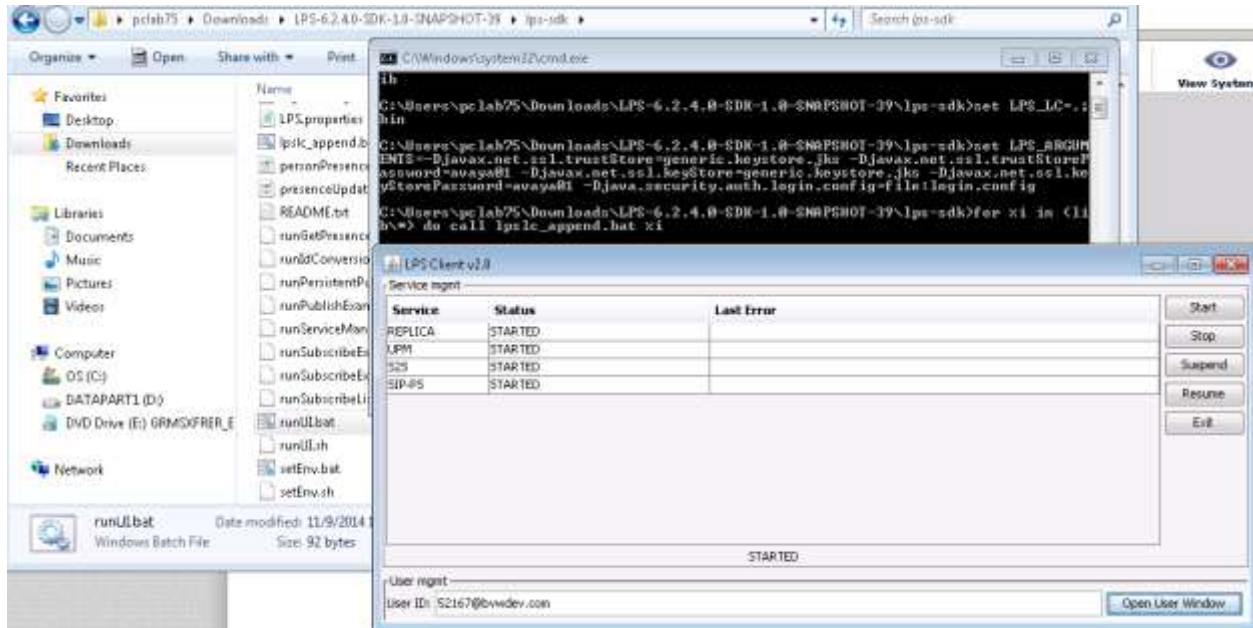
Copy the SSL/TLS certificate file ./opt/Avaya/presence/jabber/xcp/cert/generic.keystore.jks from Presence Services Server and place it in the folder of client application.



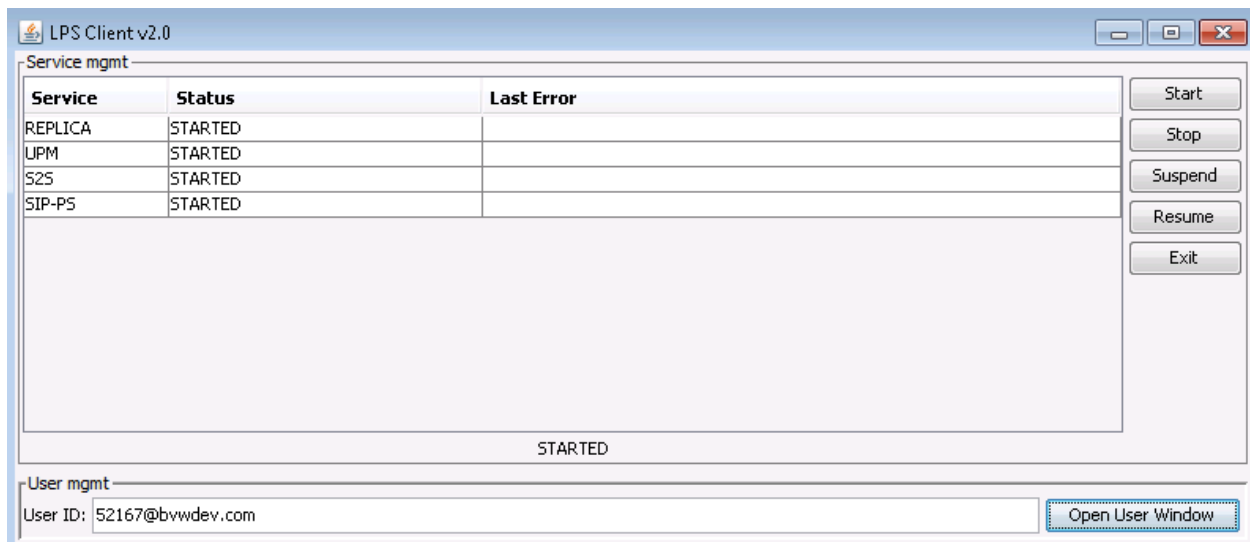


### 7.3. Running Local Presence Service Client

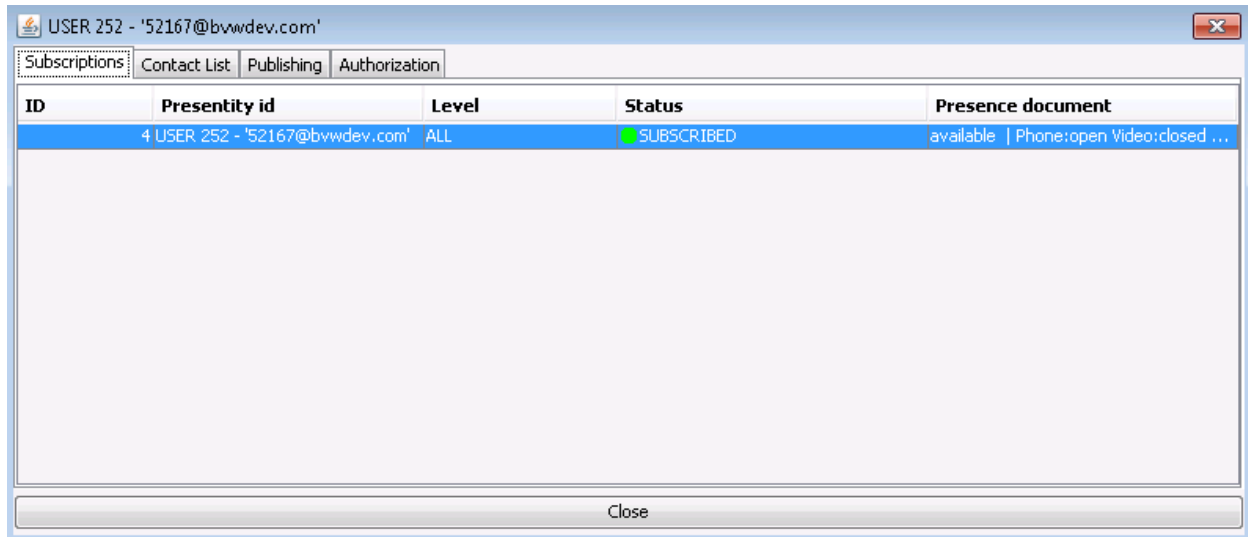
Double click on **runUI.bat** file. Wait for the LPS Client window to appear, verify that all Services status indicators display as “**STARTED**”.



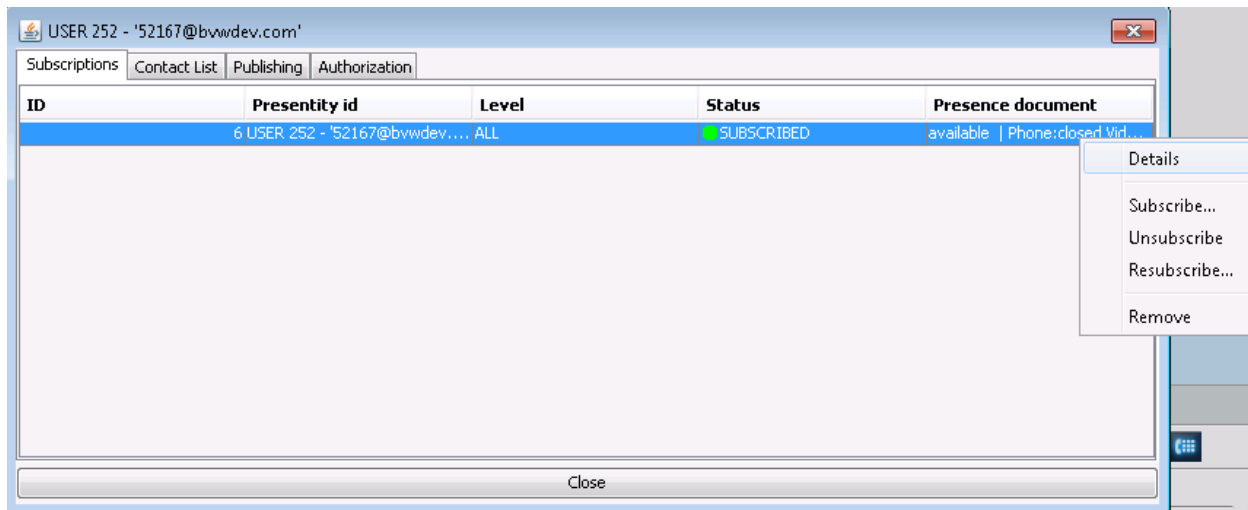
Enter User ID as configured in **Section 6.3** to view its presence status. Click **Open User Window** button to open user detail presence status.



In the Subscriptions tab of selected user, verify that the status is **SUBSCRIBED**, and that presence displays as “**available |Phone:open**”.



Make an outbound call from the monitored user and verify that the phone status is “**Closed**”, since the displayed is the aggregated status, right click on the status to view more detail.



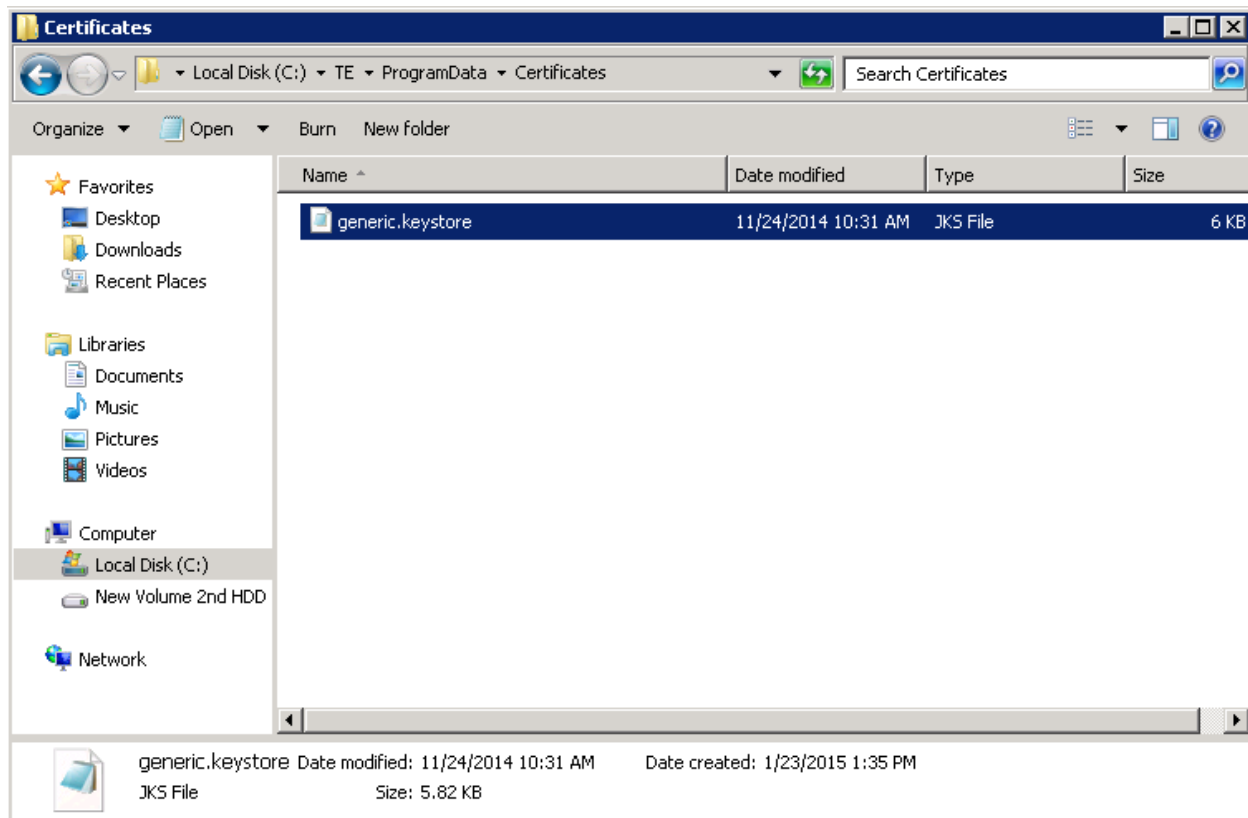
Below is detail show that user “on-the-phone”.



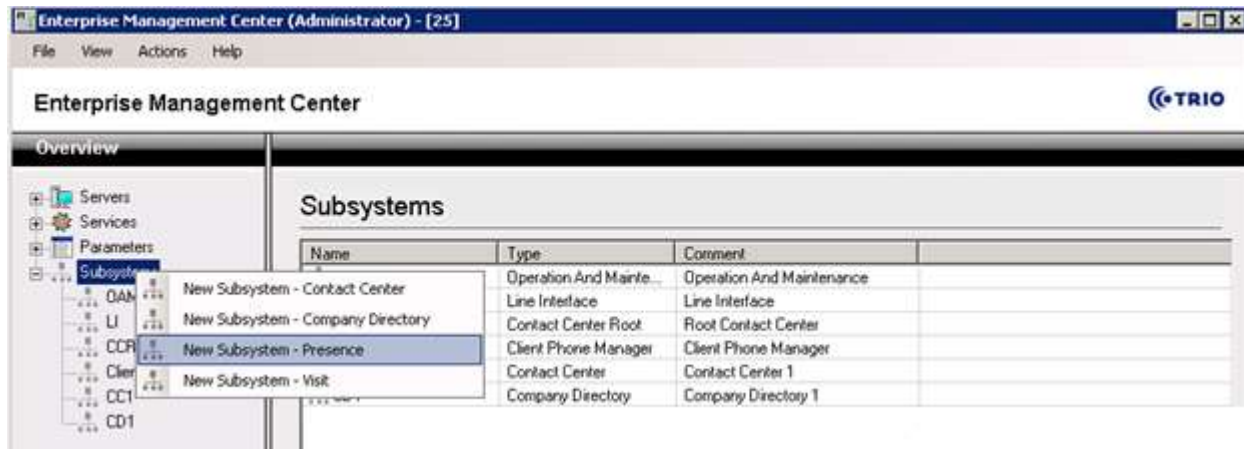
Hang up the call and verify that the status changes back.

## 7.4. Configuring Enterprise Management Center

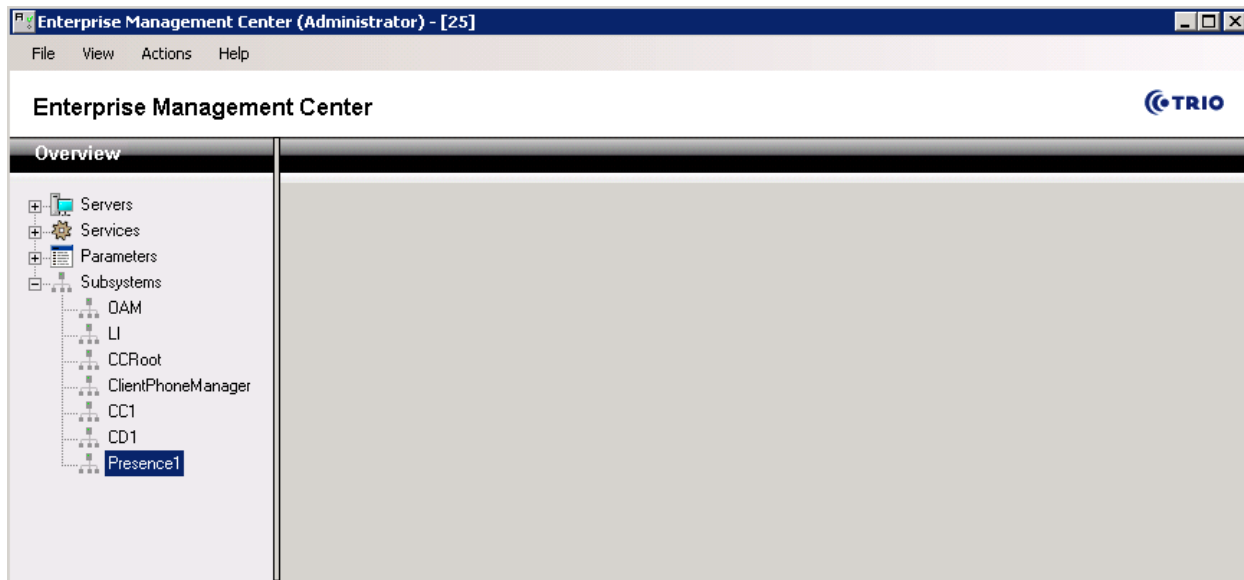
Add the **generickeystore.jks** file in \TE\ProgramData\Certificates.



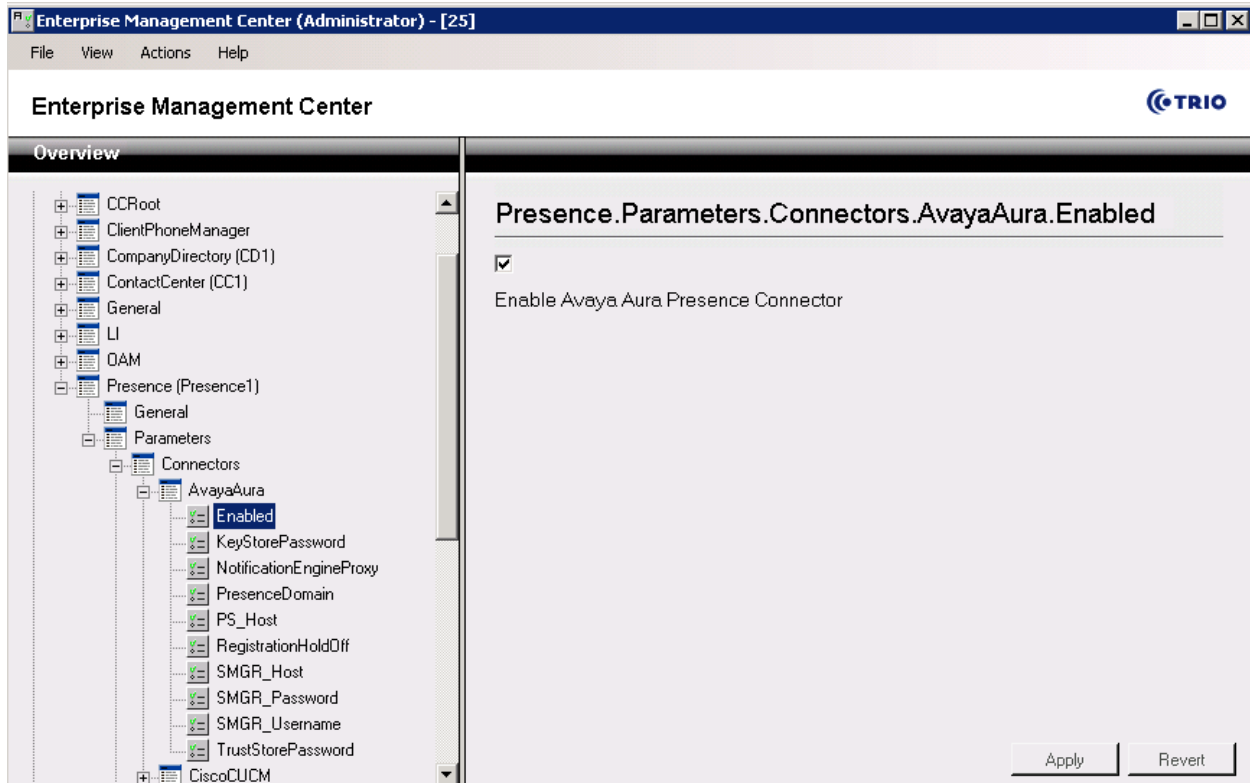
Launch **Enterprise Management** and add a **Presence** subsystem.



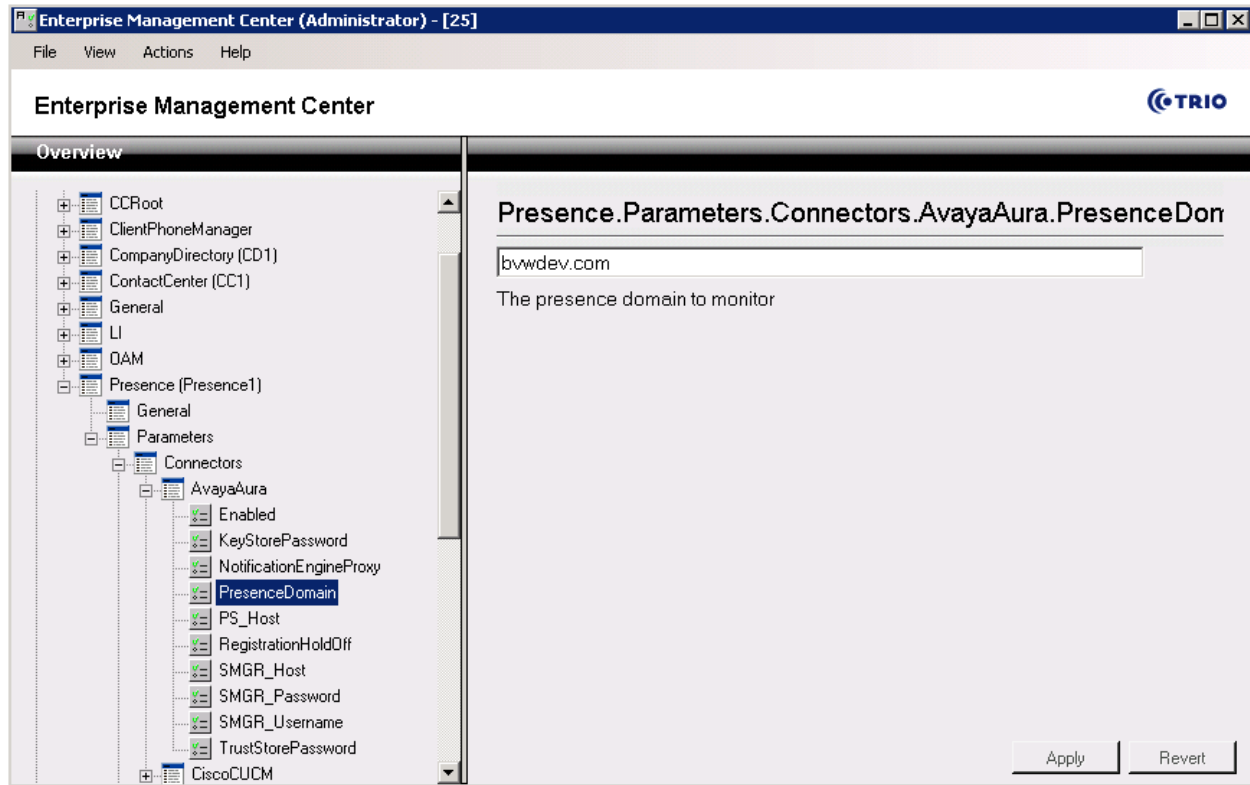
Verify that **Presence1** is added.



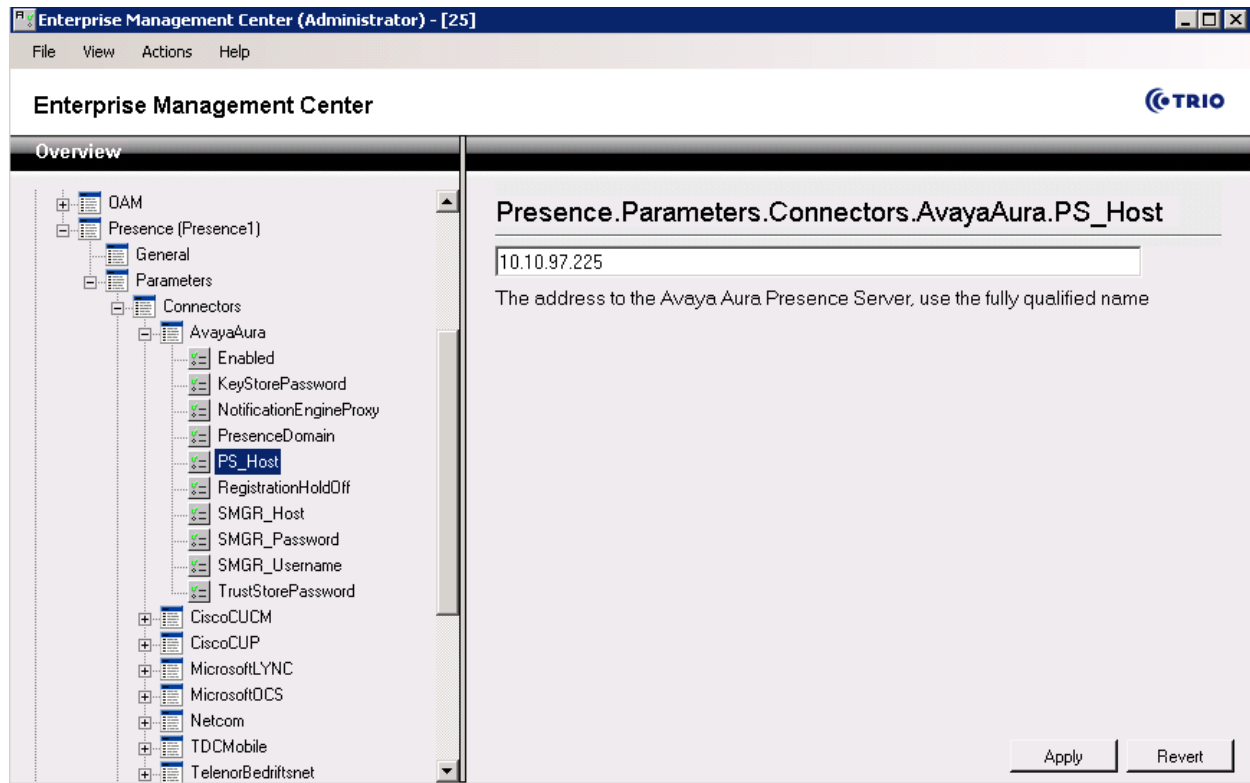
Browse to **Presence (Presence1) → Parameters → Connectors → AvayaAura → Enabled**, verify that **Enable Avaya Aura Presence Services** checkbox is checked. Click Apply to save change.



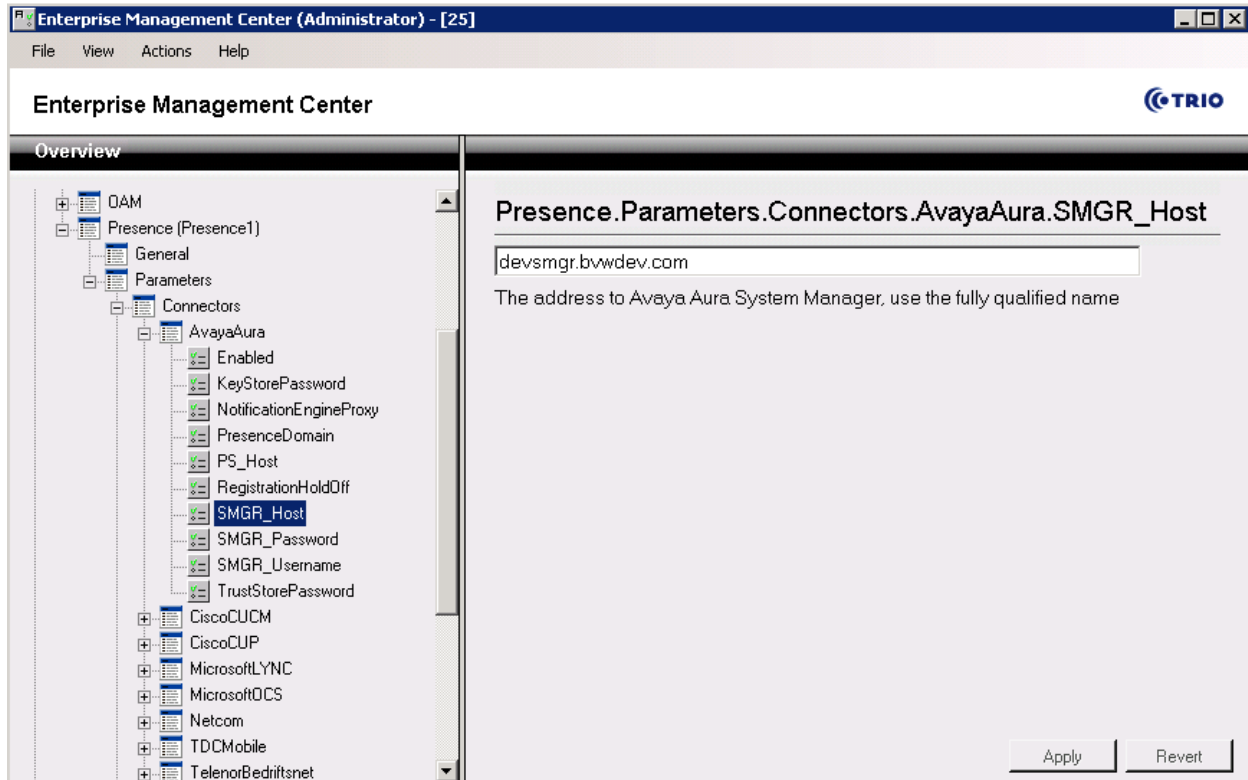
Browse to **PresenceDomain** to enter domain name to monitor, during compliance test **bvwddev.com** is used. Click **Apply** to save change.



Browse to **PS\_Host** to enter the IP address of Presence Services Server, in this case it is **10.10.97.225**.

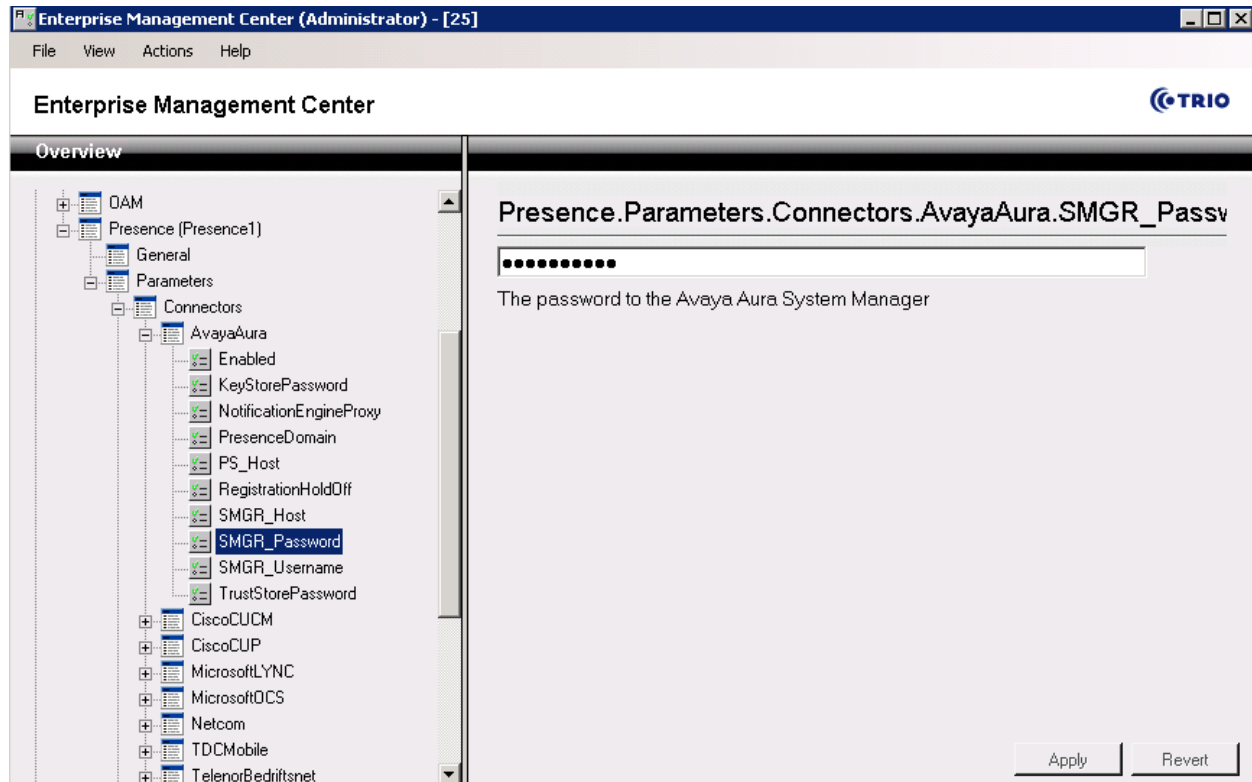


Browse to **SMGR\_Host** to enter address of **System Manager**.

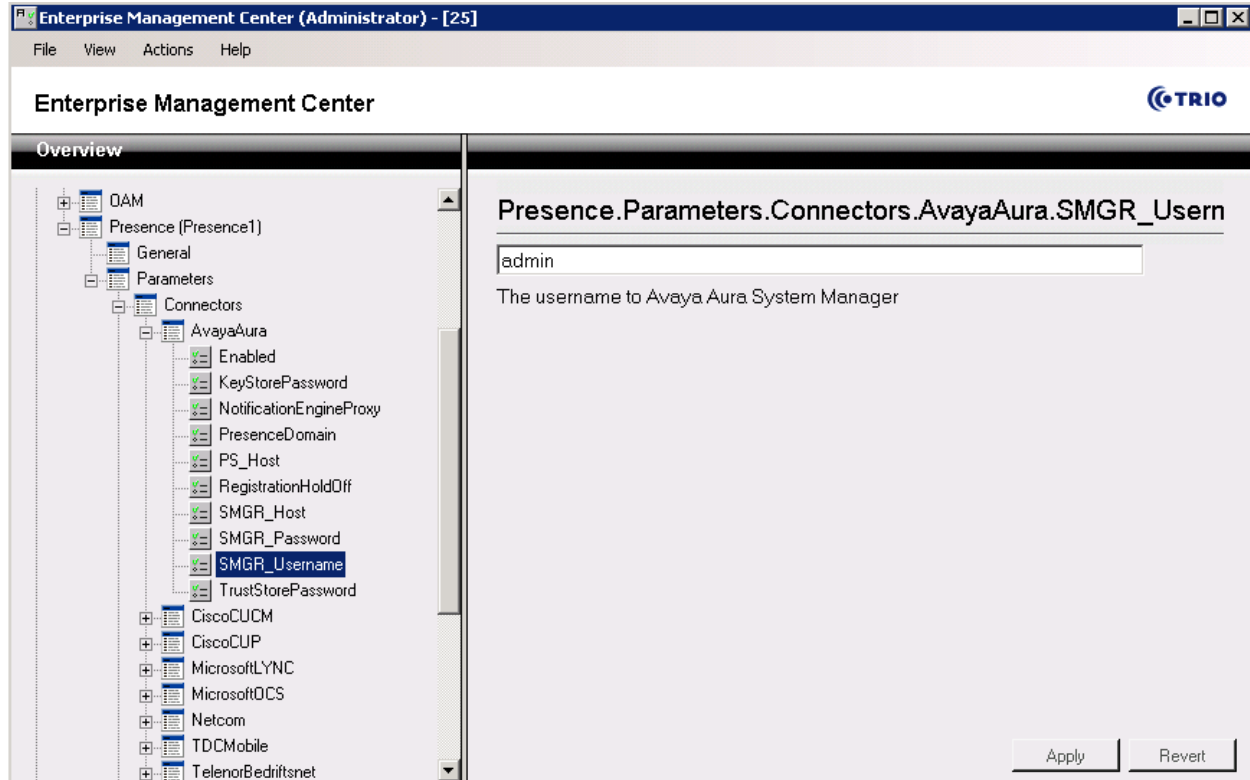




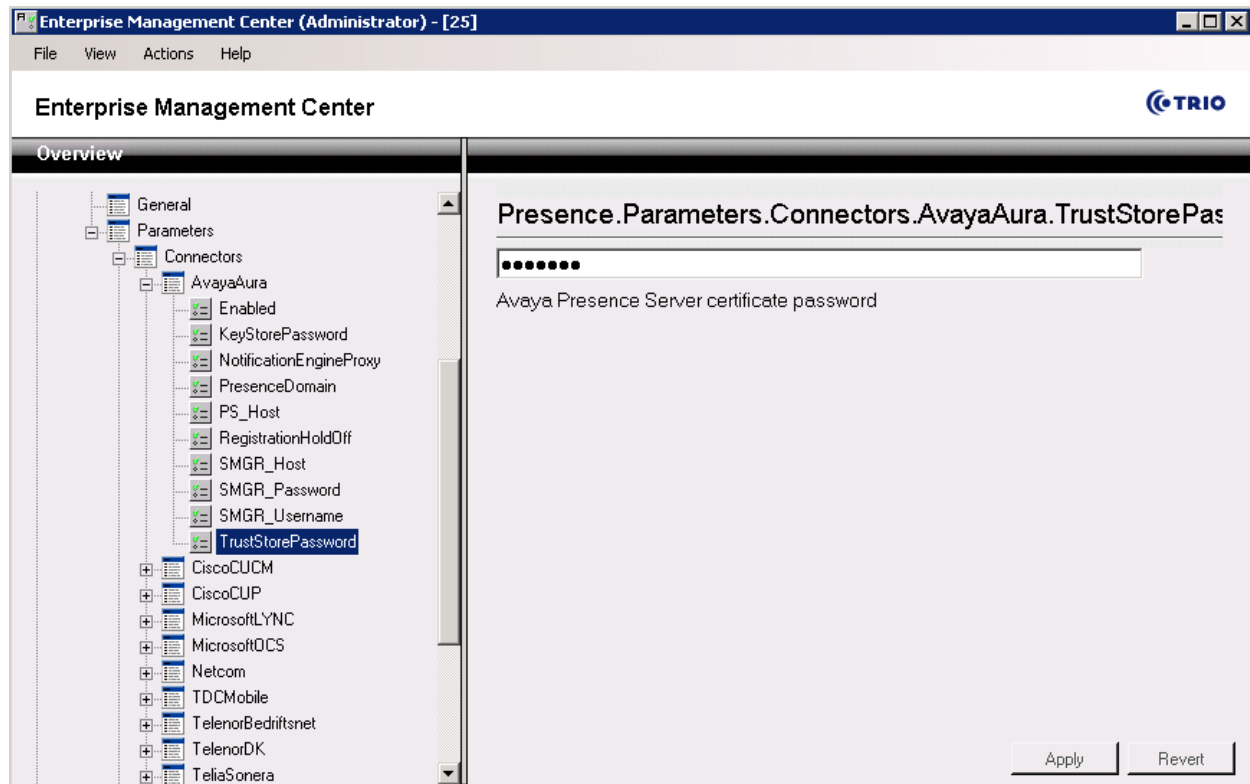
Browse to **SMGR\_Password** to enter System Manager password.



Browse to **SMGR\_UserName** to enter System Manager username.



Browse to **TrustStorePassword** to enter the **Certificate password**.



Verify the setting is corresponding to the screenshot below:

The screenshot shows the Enterprise Management Center (Administrator) interface. The left sidebar displays a tree view of services and parameters. The main pane shows the configuration for 'Presence.Parameters.Connectors.AvayaAura'.

**Enterprise Management Center (Administrator) - [25]**

File View Actions Help

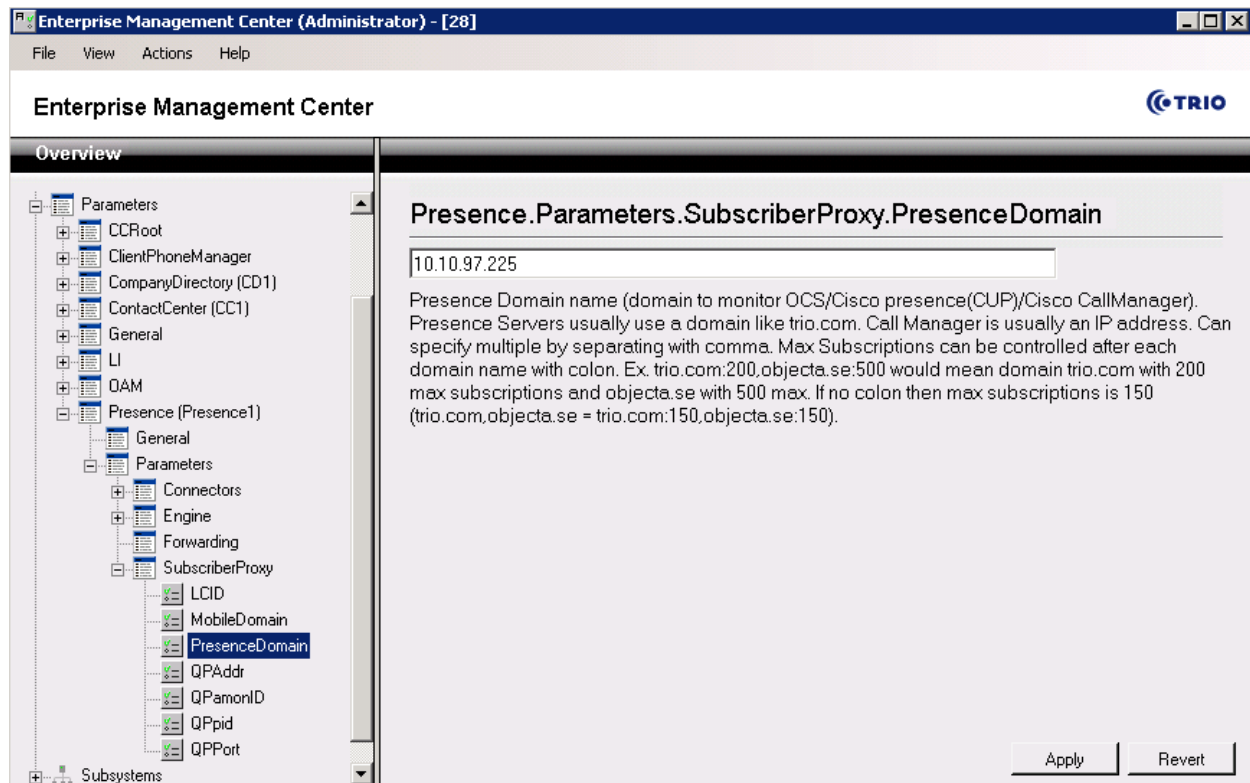
**Enterprise Management Center**

**Overview**

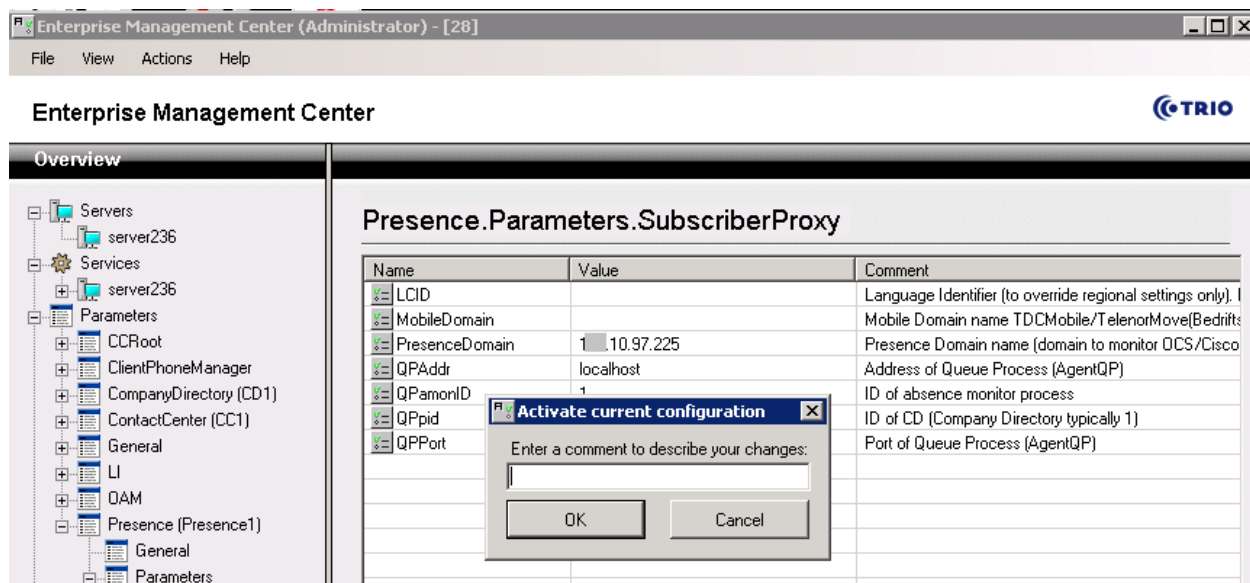
**Presence.Parameters.Connectors.AvayaAura**

Name	Value	Comment
Enabled	true	Enable Avaya Aura Presence Connector
KeyStorePassword		Avaya Presence Server certificate password
NotificationEngineProxy	http://127.0.0.1:31040/NotificationE...	The address to the Notification Engine (Presen
PresenceDomain	bwvdev.com	The presence domain to monitor
PS_Host	10.97.225	The address to the Avaya Aura Presence Serv
RegistrationHoldOff	60	The holdoff period between registrations requ
SMGR_Host	devsmgr.bwvdev.com	The address to Avaya Aura System Manager, u
SMGR_Password		The password to the Avaya Aura System Mana
SMGR_Username	admin	The username to Avaya Aura System Manager
TrustStorePassword		Avaya Presence Server certificate password

Browse to **Presence** → **Parameters** → **SubscriberProxy** → **PresenceDomain** to enter Presence Domain to monitor. Click **Apply** to save change.

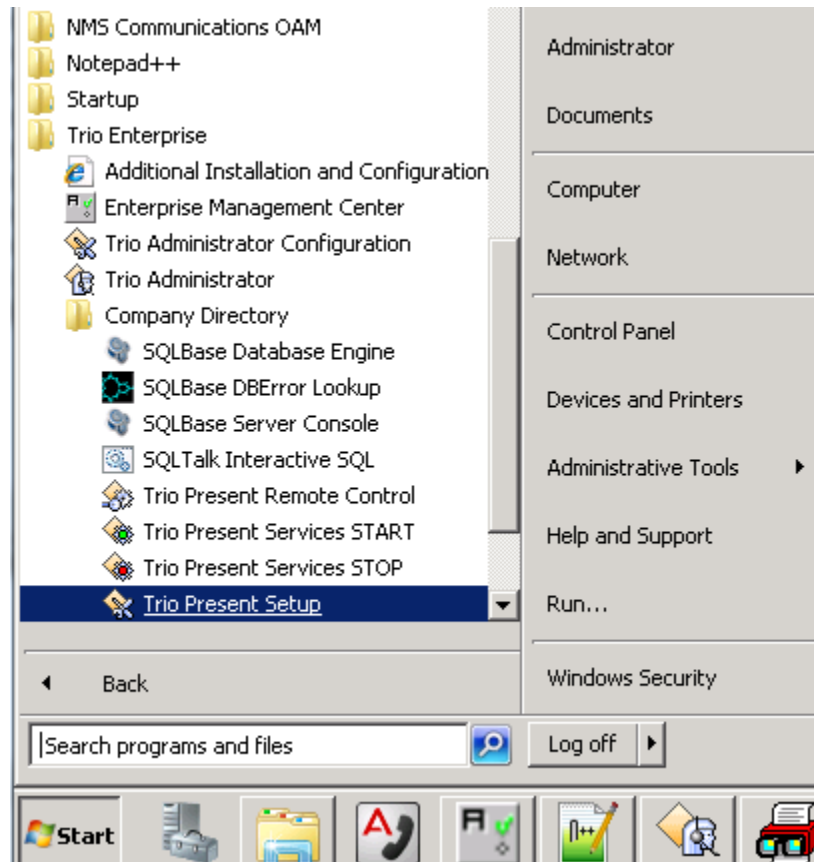


Click on menu **File** → **Activate current Configuration** (not shown). Click **OK** to activate the configuration.

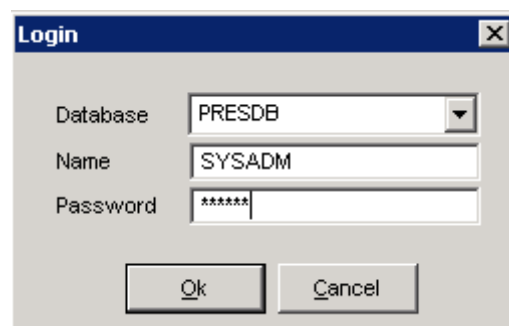


## 7.5. Configure Trio Presence Gateway

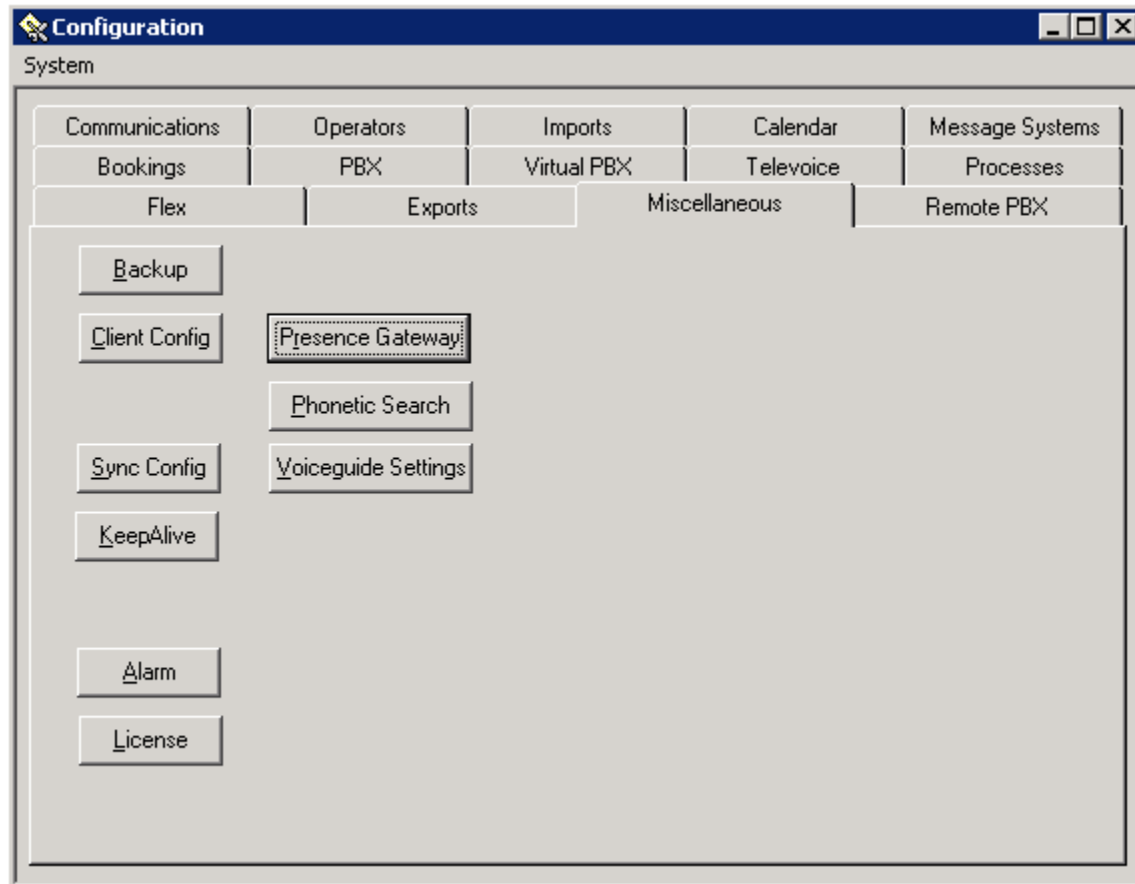
Configure Presence Gateway in Trio setup by click on Window Start button, browse to **Trio Enterprise → Company Directory → Trio Present Setup**.



Enter appropriated credential to login.



In the **Configuration** window, browse to **Miscellaneous** tab and click on **Presence Gateway** button.



In **Presence Gateway** window, set the server to **net.pipe://localhost/Presence1**, set **Presence Domain** to **1**. Make sure the “**Enable connection for monitor of presence or line state**” checkbox is checked. Click **OK** to save changes.

**Presence Gateway**

Server URL:

Present Domain:

☒ Enable connection for monitor of presence or line state

☐ Enable connection to MS OCS

☐ Mobile Line Status

Mobile Domain[s] to subscribe to:

Mobile Prefix:

Mobile in ExtraField:  (1-20)

Browse to Administrator window to restart **Trio Presence1** and **Trio CD1** services. Click on selected service and click **Restart** button.

**Enterprise Management Center (Administrator) - [29]**

File View Actions Help

**Enterprise Management Center**

**Overview**

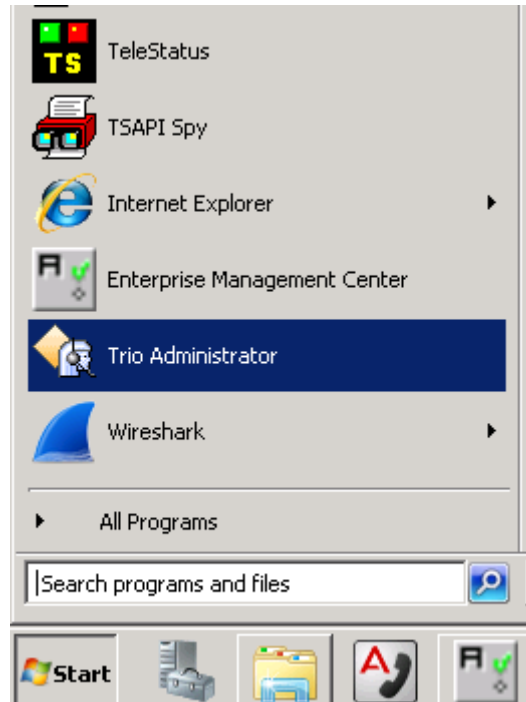
**server236**

Name	Status	Comment
MySQL Service	Running	MySQL Service
World Wide Web Publishing Service	Running	World Wide Web Publishing Service
SQL Server (SQL2008)	Running	SQL Server (SQL2008)
Trio Operations And Maintenance Service	Running	Trio Operations And Maintenance Service
Trio Client Phone Manager	Running	Client Phone Manager Service
Trio CC1	Running	Trio Contact Center CC1
Trio CC1 Mail	Not Active	Trio Contact Center CC1 Mail
Trio CC1 Custom	Running	Trio Contact Center CC1 Custom Service
Trio TeleVoice Service	Running	Trio TeleVoice Service
Trio Unify SQLBase Service	Running	Company Directory Database Engine Service
Trio CD1	Running	Trio Company Directory Service CD1
Trio CD1 Custom	Not Active	Trio Company Directory CD1 Custom Service
<b>Trio Presence1</b>	Running	Trio Presence Service

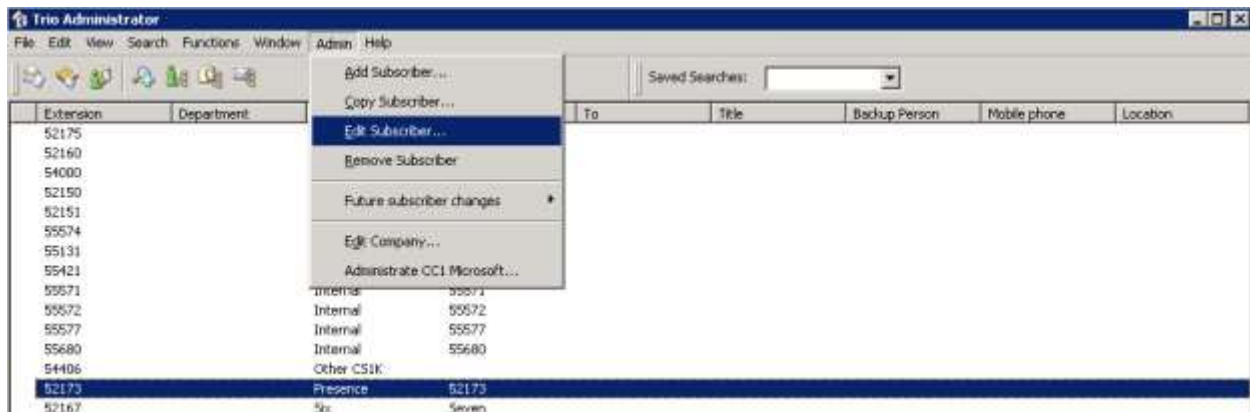


## 7.6. Administer Users

This is assumed that Trio system is already in place with list of current user created and operation. Click on Window Start menu, select **Trio Administrator**.



In **Trio Administrator** window, highlight selected user to edit, browse to menu **Admin → Edit Subscriber...**



In **Subscriber** window, add URI for the user to monitor. Click **OK** to save changes.

Subscriber  
Phone  
Security  
Department  
Skills  
Message Channels  
Schedule  
Extra Fields  
Secretary  
Future Updates

Security

Type of Subscriber

☐ User  
☒ Extension

Communicator

Sign-in address: sip:52173@bvwdev.com

<< >> OK Cancel Apply Help

Open Agent client to verify user's presence status is updated. Click **Start → Programs → Trio Enterprise → Contact Centre → Agent Client**. Enter a valid **User ID** and **Password** (not shown). Attendant performs the search for user [52173@bvwdev.com](mailto:52173@bvwdev.com). Verify the status for user is show as **Available** as below.

Availability	Personal note	Icon	Returns	Extension	Last name	First name	State	T	Q
Available				52173	Local	Extension			

## 8. Verification Steps

This section provides the tests that can be performed to verify correct configuration of Presence Services and System Manager with TRIO Enterprise.

### 8.1. Verify Avaya Aura® System Manager

Verify that link status between Session Manager and Presence Services created in **Section 6.2** is “UP” as shown below.



### 8.2. Verify Avaya Aura® Presence Service

#### 8.2.1. Verify Data Replication from Avaya Aura® System Manager to Avaya Aura® Presence Services

Users created in System Manager as described in **Section 6.3**, are replicated in the presence database of the Presence server. To verify that user data is successfully replicated to the Presence server run following command on the ssh connection to the Presence server:

```
psql -d presence -U postgres -c "select * from csuser"
```

Below is the screen with results showing that users with **loginname 52173@bvwddev.com** and **52167@bvwddev.com** are successfully replicated to Presence server.

id	updatedatetime	version	compassword	encryptionkeyid	isdeleted	isenabled	loginname
tenantid	contactlistdefaultaclid	userdefaultaclid	userstatusid	defaultcommprofilesetid		defaultcontactlistid	
108	2013-04-03 11:25:58	0	MNcJHcSioRmk 7ea36daa-2dc1-4e05-b5b7-3fedd3834891	f	t	52167@bvwddev.com	
50			86	108			58
110	2013-04-09 15:49:25.1	2	8rtrDlct2Szc d8dff78c-70df-412d-afdd-de483950b337	f	t	52173@bvwddev.com	
50			86	110			60

### 8.2.2. Verify User's Presence Data is Obtainable

After a user publishes its presence for the first time, it gets added in the **xcp** Presence database. To verify this, login the user with extension **52173** on a SIP one-X® Communicator. Once user is successfully logged in, the user data is updated in the xcp database. To verify this update is successful run following command on the ssh connection to the Presence server:

```
psql -d xcp -U postgres -c "select * from users"
```

Below is the screen with results showing that user with 52173@bvwdev.com and 52167@bvwdev.com has successfully published its presence.

user_id	jid	auth_pwd	disabled	login_stamp	logout_stamp	auth_count	pwd_stamp	last_status
10209	52173@bvwdev.com	-	F	2014-12-11 19:51:25	2014-12-11 19:51:25	22	2014-11-27	Disconnected.
10207	52175@bvwdev.com	-	F	2015-01-22 01:18:37	2015-01-22 01:18:50	16	2014-11-16	
10211	55016@bvwdev.com	-	F	2015-01-22 01:52:46	2015-01-22 01:52:46	0	2015-01-22	
10206	52161@bvwdev.com	-	F	2014-11-28 17:02:49	2014-11-28 17:02:54	12	2014-11-11	
10210	52167@bvwdev.com	-	F	2015-01-23 13:10:51	2015-01-23 13:10:51	17	2014-12-05	

### 8.3. Verify Presence Status of Monitored User on Trio Enterprise

Confirm a status change is displayed on Attendant window by making an outbound call on monitored phone; verify subscriber's status is changed as shown below



## 9. Conclusion

These Application Notes describe the configuration steps required for Trio Enterprise R5.0 from Enghouse Interactive AB to successfully interoperate with Avaya Aura® Presence Services. Trio Enterprise passed all compliance testing successfully; please see **Section 2.2** of these Application Notes for results and observations.

## 10. Additional References

This section references documentation relevant to these Application Notes. The Avaya product documentation is available at <http://support.avaya.com> where the following documents can be obtained.

1. Installing Avaya Aura® Presence Services
2. Avaya Aura® Presence Services using VMware® in the Virtualized Environment Deployment Guide.
3. Application Notes for Configuring Avaya Aura® Presence Services 6.0 with Avaya Aura® Session Manager 6.0, and Avaya Aura® Communication Manager for one-X® Communicator clients as part of Avaya Unified Communication Mobile Worker Solution – (PS6-1xC.pdf)

All information on the product installation and configuration TRIO Enterprise Server can be found at <http://www.trio.com>

---

**©2015 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 DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).