Application Notes for Cyara CX Automated Test and Monitoring Virtual Agent with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Cyara CX Automated Test and Monitoring Virtual Agent to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services (AES).

The Cyara Platform is an automated testing products and services platform that provides scripting, reporting, administration, collaboration, and management portal for contact center testing. The Cyara Virtual Agent Service is one of the components of the Cyara Platform that interacts with contact center Computer Telephony Integration (CTI) environments to automate agent activities in order to simulate contact center operations. Virtual Agent logs the required agents into the CTI environment and performs the activities specified by the designated behaviors assigned to the agents. The Virtual Agent interfaces with the Cyara Database and Web Portal.

Readers should pay attention to **section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any 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 describe the configuration steps required for Cyara CX Automated Test and Monitoring Virtual Agent to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services (AES).

2. General Test Approach and Test Results

The feature test cases were performed manually. Campaigns are run from the Cyara Web Portal to handle inbound calls routed to the Virtual Agent. In this testing, voice is answered by Virtual Endpoint registered to Communication Manager as generic H.323 endpoint which will be covered in Application Notes **[4]**.

The serviceability test cases were also performed manually by restarting the Telephony Services Application Programming Interface (TSAPI) service on AES server as well as the CTI link on Communication Manager.

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.

This test was conducted in a lab environment simulating a basic customer enterprise network environment. The testing focused on the standards-based interface between the Avaya solution and the third party solution. The results of testing are therefore considered to be applicable to either a premise-based deployment or to a hosted or cloud deployment where some elements of the third party solution may reside beyond the boundaries of the enterprise network, or at a different physical location from the Avaya components.

Readers should be aware that network behaviors (e.g., jitter, packet loss, delay, speed, etc.) can vary significantly from one location to another, and may affect the reliability or performance of the overall solution. Different network elements (e.g., session border controllers, soft switches, firewalls, NAT appliances, etc.) can also affect how the solution performs.

If a customer is considering implementation of this solution in a cloud environment, the customer should evaluate and discuss the network characteristics with their cloud service provider and network organizations, and evaluate if the solution is viable to be deployed in the cloud.

The network characteristics required to support this solution are outside the scope of these Application Notes. Readers should consult the appropriate Avaya and third party documentation for the product network requirements. Avaya makes no guarantee that this solution will work in all potential deployment configurations.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying Cyara Virtual Agent which includes the following:

- Agent in login mode, logout scenarios.
- Handling of incoming calls.
- Holding and resuming of calls.
- Consult and single step voice transfers including cancellation.
- Consult and single step voice conference including cancellation.
- Correct status of Agent reflected on the test user interface.
- Proper hang up of calls including call hold, transfer and conference.

The serviceability testing focused on verifying the ability of Cyara Virtual Agent to recover from adverse conditions such as restarting of the TSAPI service on the Avaya AES server and CTI link on the Communication Manager.

2.2. Test Results

All feature test cases were successfully completed with the following observation:

- Agent ready status was not reflected on the web portal user interface after TSAPI link is restarted from AES or Communication Manager.

2.3. Support

Technical support on Cyara Platform can be obtained through the following:

- Phone: +61-3-90930815 (Australia), +44-203-356-9775 (Europe/Middle East/Africa), +1-844-204-2359 (North America/Latin America)
- Email: support@cyarasolutions.com
- Web: http://cyara.com/services/support/

3. Reference Configuration

An on-premises solution is conducted in this compliance testing. **Figure 1** illustrates a sample configuration consisting of a duplex pair of Communication Manager, Avaya G430 Media Gateway, Avaya AES Server, Avaya Media Server and System Manager. 96x1 H.323 IP Telephones are used as utility phones for initiating calls. Cyara Platform Server is installed on Microsoft Windows 2012 R2 which communicates with the TSAPI Service on the Avaya AES Server. Microsoft SQL 2012 was installed as the database on the same server. Cyara Endpoint Server also installed on Microsoft Windows 2012 R2 provides the virtual H.323 endpoint which will be detailed in another Application Notes **[4]**. The Avaya 4548GT-PWR Converged Stackable Switch provides ethernet connectivity to the servers and IP telephones. A personal computer was used for Cyara Web Portal access.

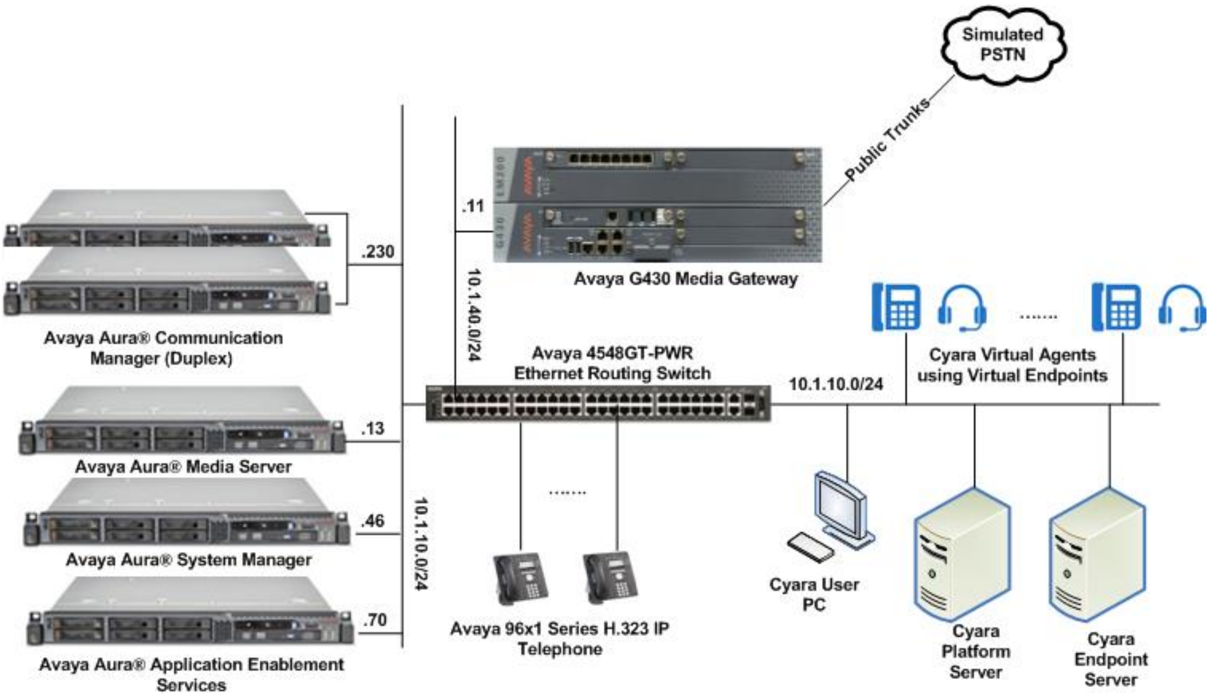

Simulated PSTN
Public Trunks
.11
10.1.40.0/24
Avaya G430 Media Gateway
.230
Avaya Aura® Communication Manager (Duplex)
Avaya 4548GT-PWR Ethernet Routing Switch
10.1.10.0/24
Cyara Virtual Agents using Virtual Endpoints
.13
Avaya Aura® Media Server
.46
Avaya Aura® System Manager
10.1.10.0/24
.70
Avaya Aura® Application Enablement Services
Avaya 96x1 Series H.323 IP Telephone
Cyara User PC
Cyara Platform Server
Cyara Endpoint Server

Figure 1: Test Configuration

4. Equipment and Software Validated

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

Equipment/Software	Version
Avaya Aura® Communication Manager Duplex Servers	7.0.1.0.0-FP1 (7.0.1.0.0.441.23012)
Avaya G430 Media Gateway • MGP	37.38.0
Avaya Aura® Application Enablement Services	7.0.1.0.2.15-0
Avaya Aura® Media Server	7.7.0.19
Avaya Aura® System Manager	7.0.1.1.065378
96x1 Series (H.323) IP Telephones	6.6029
Cyara Platform Server running on Microsoft Windows 2012 R2	6.4
Cyara Endpoint Server running on Microsoft Windows 2012 R2	6.4
Dell PC	Microsoft Windows 10 Pro

Table 1: Equipment/Software Validated

5. Configure Communication Manager

This section provides the procedures for configuring Computer Telephony Integration (CTI) links on Communication Manager. Setup of Agent Stations, Agent Login ID, VDNs, Hunt Groups, Trunks and Call Center features is assumed to be configured and will not be detailed here.

All the configuration changes in Communication Manager are performed through the System Access Terminal (SAT) interface. The highlights in the following screens indicate the values used during the compliance test.

5.1. Configure AES and CTI Links

Avaya AES server forwards CTI requests, responses, and events between Cyara Platform Server and Communication Manager. Avaya AES server communicates with Communication Manager over an AES link. Within the AES link, CTI links may be configured to provide CTI services to CTI applications such as Cyara Virtual Agent. The following steps demonstrate the configuration of the Communication Manager side of the AES and CTI links.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>Enter the <b>display system-parameters customer-options</b> command. On <b>Page 4</b>, verify that <b>Computer Telephony Adjunct Links</b> is set to <b>y</b>. If not, contact an authorized Avaya account representative to obtain the license.</td></tr>
<tr><td></td><td><pre>
display system-parameters customer-options   Page   4 of   12
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y   Audible Message Waiting? y
        Access Security Gateway (ASG)? n   Authorization Codes? y
        Analog Trunk Incoming Call ID? y   CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y   CAS Main? n
Answer Supervision by Call Classifier? y   Change COR by FAC? n
                                  ARS? y Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n   DCS (Basic)? y
          ASAI Link Core Capabilities? y   DCS Call Coverage? y
          ASAI Link Plus Capabilities? y   DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n   Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n   DS1 MSP? y
                                 ATMS? y   DS1 Echo Cancellation? y
                  Attendant Vectoring? y

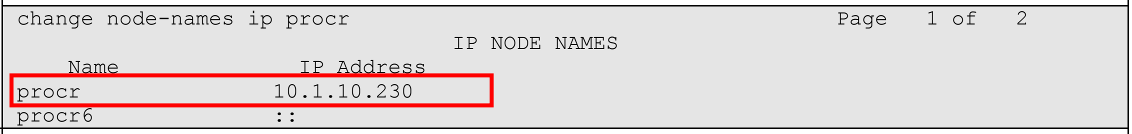
        (NOTE: You must logoff & login to effect the permission changes.)
</pre></td></tr>
<tr><td>2.</td><td>Enter the <b>add cti-link m</b> command, where <b>m</b> is a number between 1 and 64, inclusive. Enter a valid <b>Extension</b> under the provisioned dial plan in Communication Manager, set the <b>Type</b> field to <b>ADJ-IP</b>, and assign a descriptive <b>Name</b> to the CTI link.</td></tr>
<tr><td></td><td><pre>
add cti-link 3   Page   1 of   3
                                    CTI LINK

 CTI Link: 3
Extension: 10093
     Type: ADJ-IP
                                                                        COR: 1

     Name: TSAPI Service - AES7x
</pre></td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.</td><td>

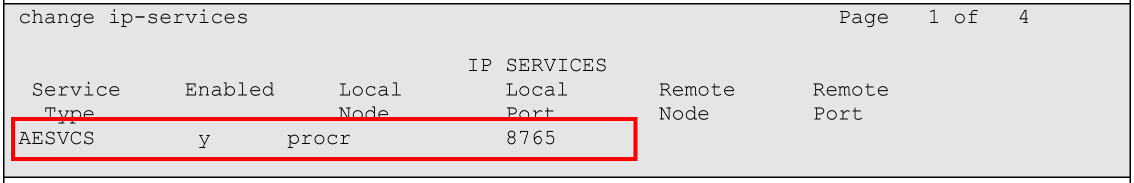
Enter the **change node-names ip procr** command. In the compliance-tested configuration, the processor of the communication manager with the node-name **procr** was utilized for connectivity to Avaya AES server.



```
change node-names ip procr                                      Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
procr                   10.1.10.230
procr6                  ::
```

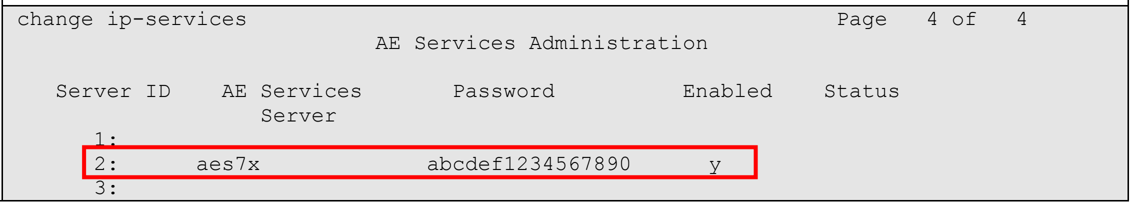
</td></tr>
<tr><td>4.</td><td>

Enter the **change ip-services** command. On **Page 1**, configure the **Service Type** field to **AESVCS** and the **Enabled** field to **y**. The **Local Node** field should be set to the **procr** that was noted previously in **Step 3**. During the compliance test, the default port was utilized for the **Local Port** field.



```
change ip-services                                              Page   1 of   4

                                   IP SERVICES
 Service      Enabled      Local         Local        Remote       Remote
  Type                     Node          Port         Node         Port
AESVCS         y       procr            8765
```

On **Page 4**, enter the hostname of the Avaya AES server for the **AE Services Server** field. The server name may be obtained by logging in to the Avaya AES server using Secure Shell (SSH) and running the **uname -a** command. Enter an alphanumeric password for the **Password** field and set the **Enabled** field to **y**. The same password will be configured on Avaya AES server in **Section 6.3 Step 2**.



```
change ip-services                                              Page   4 of   4
                            AE Services Administration

   Server ID    AE Services        Password          Enabled    Status
                   Server
       1:
       2:      aes7x             abcdef1234567890       y
       3:
```

</td></tr>
</table>

5.2. Configure agent IDs

Step	Description
1.	Enter the **add agent x** command where **x** is a valid agent loginID. On **Page 1**, enter an appropriate **Name** and configure the **Security Code** to **0000**.

```
add agent-loginID 11201                                         Page   1 of   3
                                 AGENT LOGINID

                Login ID: 11201                                      AAS? n
                    Name: Agent #1                                 AUDIX? n
                      TN: 1        Check skill TNs to match agent TN? n
                     COR: 1
           Coverage Path:                                 LWC Reception: spe
           Security Code: 0000                    LWC Log External Calls? n
           Attribute:                           AUDIX Name for Messaging:

                                        LoginID for ISDN/SIP Display? n
                                                                Password:
                                                   Password (enter again):
                                                             Auto Answer: none
                                                       MIA Across Skills: system
 AUX Agent Considered Idle (MIA)? system   ACW Agent Considered Idle: system
                                           Aux Work Reason Code Type: system
                                             Logout Reason Code Type: system
                        Maximum time agent in ACW before logout (sec): system
                                               Forced Agent Logout Time:   :
    WARNING:  Agent must log in again before changes take effect
```

Step	Description
2.	On **Page 2**, configure appropriate Skill **SN** and Skill Level **SL** for testing purpose. Repeat **Step 1-2** for more agent loginIDs to be created. Repeat to configure the rest of the agent loginIDs required. In this testing, agent loginID **11201** to **11210** were created which will logon using Virtual Endpoints **10401** to **10410**.

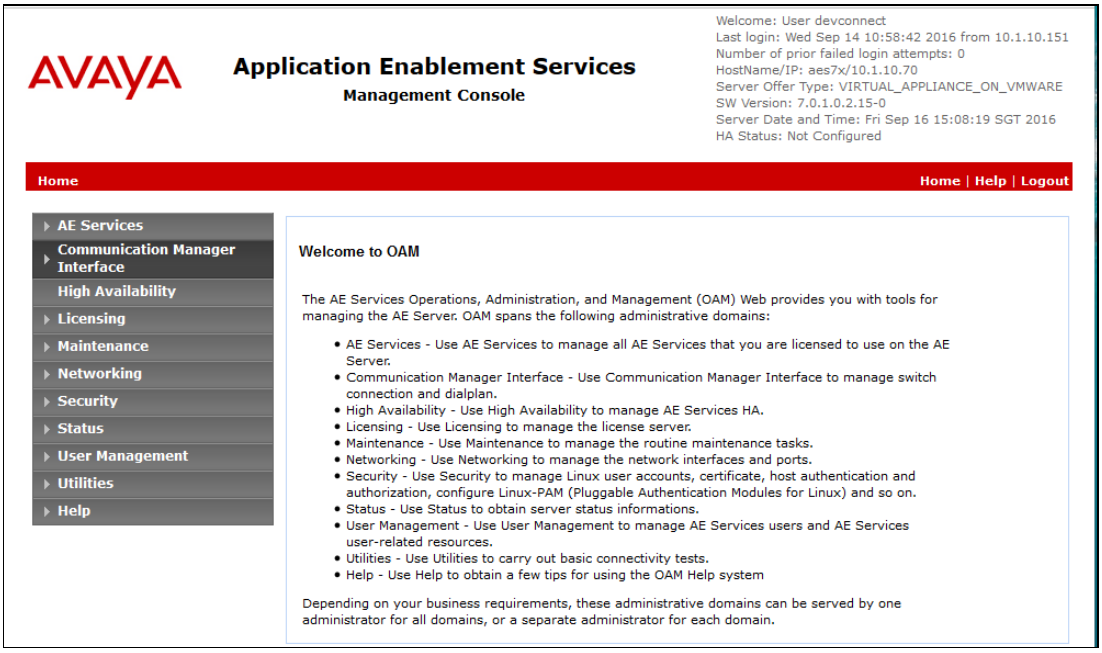
```
change agent-loginID 11201                                      Page   2 of   3
                                 AGENT LOGINID
      Direct Agent Skill:                               Service Objective? n
Call Handling Preference: skill-level                 Local Call Preference? n

    SN    RL  SL          SN    RL  SL          SN    RL  SL          SN    RL  SL
 1: 1          1     16:                   31:                   46:
 2:                  17:                   32:                   47:
 3:                  18:                   33:                   48:
 4:                  19:                   34:                   49:
 5:                  20:                   35:                   50:
 6:                  21:                   36:                   51:
 7:                  22:                   37:                   52:
 8:                  23:                   38:                   53:
 9:                  24:                   39:                   54:
10:                  25:                   40:                   55:
11:                  26:                   41:                   56:
12:                  27:                   42:                   57:
13:                  28:                   43:                   58:
14:                  29:                   44:                   59:
15:                  30:                   45:                   60:
```

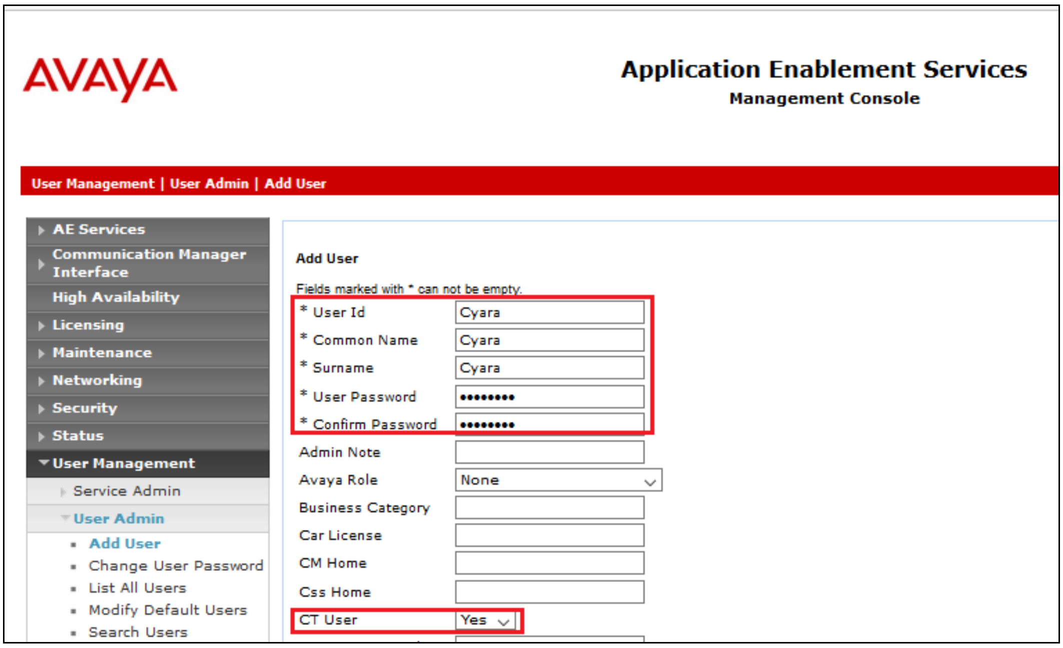
6. Configure Avaya Application Enablement Services

This section provides the procedures for configuring Avaya Application Enablement Services. The procedures fall into the following areas:

- Administer CTI User
- Verify Avaya AES License
- Administer Switch Connection
- Administer TSAPI link and Verify TSAPI Service Port
- Administer CTI user permission

6.1. Administer CTI User

Step	Description
1.	Launch a web browser and enter **https://<IP address of Avaya AES server>** to access the AES Management Console web based interface. Log in to AES Management Console using an administrative login and password (not shown) and the **Welcome To OAM** screen will be displayed.  Application Enablement Services Management Console Home Home | Help | Logout AE Services Communication Manager Interface High Availability Licensing Maintenance Networking Security Status User Management Utilities Help Welcome: User devconnect Last login: Wed Sep 14 10:58:42 2016 from 10.1.10.151 Number of prior failed login attempts: 0 HostName/IP: aes7x/10.1.10.70 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE SW Version: 7.0.1.0.2.15-0 Server Date and Time: Fri Sep 16 15:08:19 SGT 2016 HA Status: Not Configured Welcome to OAM The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains: • AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server. • Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan. • High Availability - Use High Availability to manage AE Services HA. • Licensing - Use Licensing to manage the license server. • Maintenance - Use Maintenance to manage the routine maintenance tasks. • Networking - Use Networking to manage the network interfaces and ports. • Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on. • Status - Use Status to obtain server status informations. • User Management - Use User Management to manage AE Services users and AE Services user-related resources. • Utilities - Use Utilities to carry out basic connectivity tests. • Help - Use Help to obtain a few tips for using the OAM Help system Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

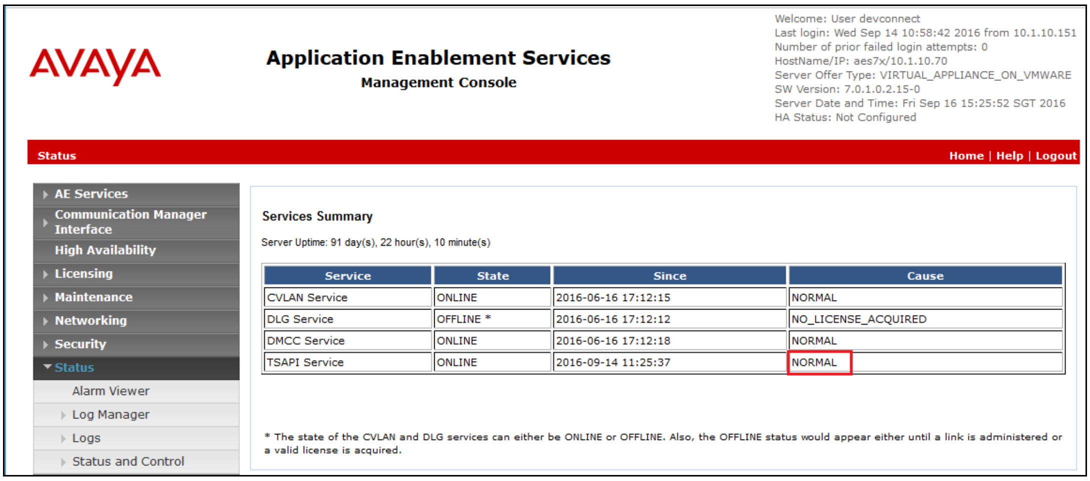
Step	Description
2.	Select **User Management** → **User Admin** → **Add User** in the left pane. Specify a value for **User Id**, **Common Name**, **Surname**, **User Password** and **Confirm Password**. Set **CT User** to **Yes**. Use the values for **User Id** and **User Password** to configure Cyara Platform Server in **Section 7** to access the TSAPI Service on Avaya AES server. Scroll down to the bottom of the page and click **Apply** (not shown). 

Add User

Fields marked with * can not be empty.

Field	Value
* User Id	Cyara
* Common Name	Cyara
* Surname	Cyara
* User Password	••••••••
* Confirm Password	••••••••
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes

6.2. Verify Avaya AES License

Step	Description
1.	Select **Status f**rom the Welcome to OAM Screen page. Verify that Avaya AES license has proper permissions for the features illustrated in these Application Notes by ensuring the TSAPI service is licensed. If the TSAPI service is not licensed, then contact the Avaya sales team or business partner for a proper license file. 

Welcome: User devconnect
Last login: Wed Sep 14 10:58:42 2016 from 10.1.10.151
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Fri Sep 16 15:25:52 SGT 2016
HA Status: Not Configured

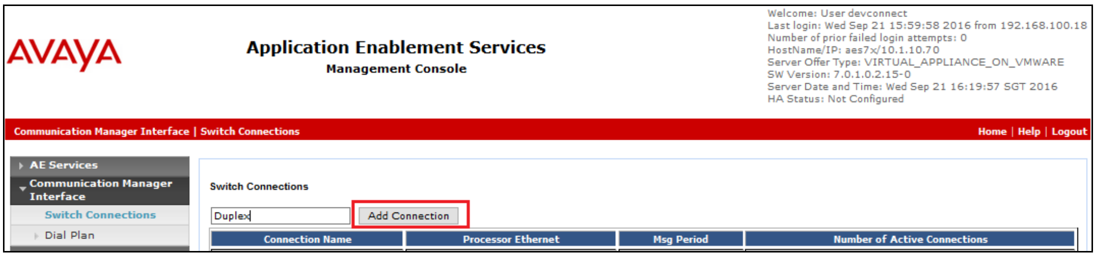
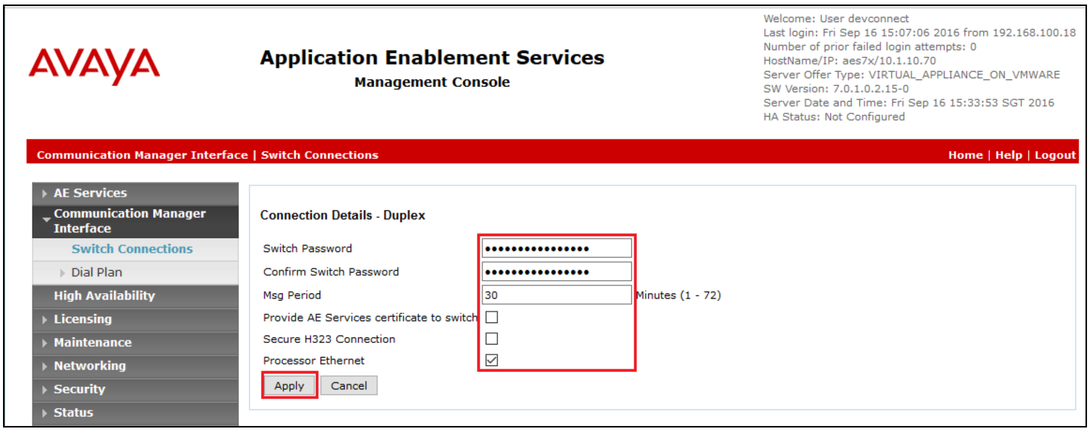
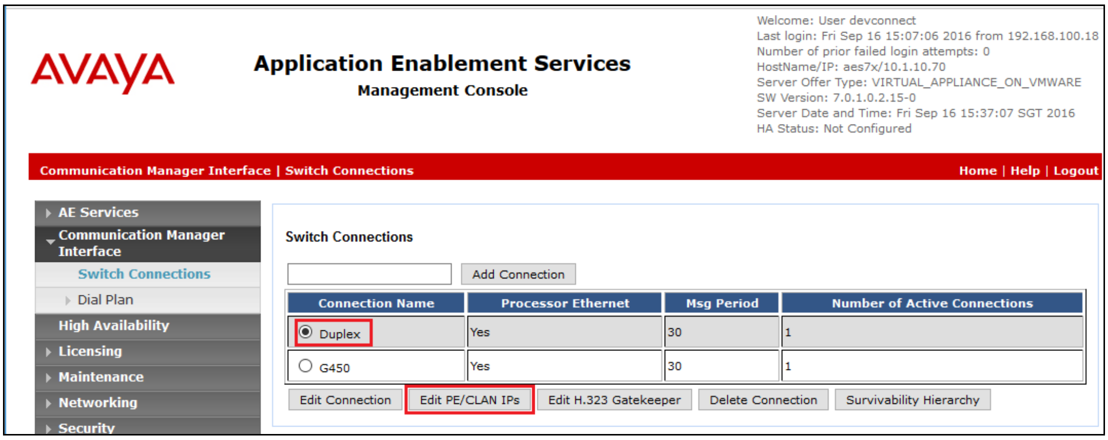
Services Summary

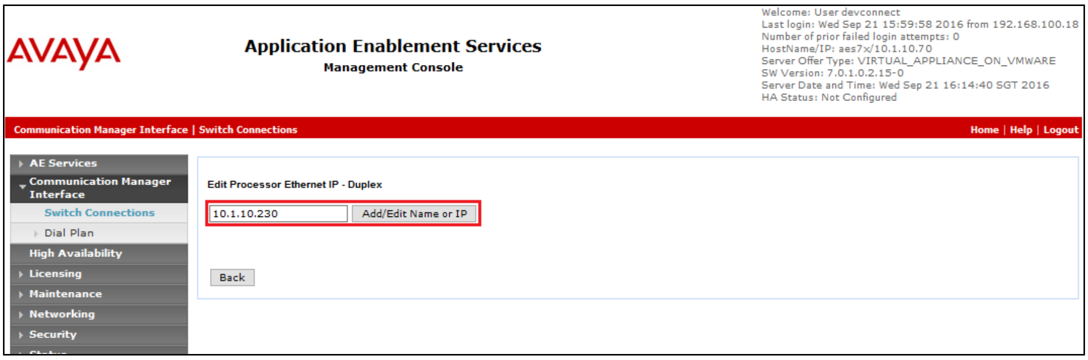
Server Uptime: 91 day(s), 22 hour(s), 10 minute(s)

Service	State	Since	Cause
CVLAN Service	ONLINE	2016-06-16 17:12:15	NORMAL
DLG Service	OFFLINE *	2016-06-16 17:12:12	NO_LICENSE_ACQUIRED
DMCC Service	ONLINE	2016-06-16 17:12:18	NORMAL
TSAPI Service	ONLINE	2016-09-14 11:25:37	NORMAL

* The state of the CVLAN and DLG services can either be ONLINE or OFFLINE. Also, the OFFLINE status would appear either until a link is administered or a valid license is acquired.

6.3. Administer Switch Connection

Step	Description
1.	From the Home menu, select **Communication Manager Interface → Switch Connections**. Enter a descriptive name for the switch connection and click **Add Connection**. In this configuration, **Duplex** is used.  Welcome: User devconnect Last login: Wed Sep 21 15:59:58 2016 from 192.168.100.18 Number of prior failed login attempts: 0 HostName/IP: aes7x/10.1.10.70 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE SW Version: 7.0.1.0.2.15-0 Server Date and Time: Wed Sep 21 16:19:57 SGT 2016 HA Status: Not Configured Application Enablement Services Management Console Communication Manager Interface | Switch Connections Switch Connections Duplex [Add Connection] Connection Name | Processor Ethernet | Msg Period | Number of Active Connections AVAYA Home | Help | Logout AE Services Communication Manager Interface Switch Connections Dial Plan
2.	The **Connection Details – Duplex** screen is displayed. For the **Switch Password** and **Confirm Switch Password** fields, enter the password that was administered in Communication Manager using the IP Services form in **Section 5.1 Step 4**. Here we are using the **Processor Ethernet** as well for connection and the field needs to be checked. Click on **Apply** to effect changes.  Welcome: User devconnect Last login: Fri Sep 16 15:07:06 2016 from 192.168.100.18 Number of prior failed login attempts: 0 HostName/IP: aes7x/10.1.10.70 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE SW Version: 7.0.1.0.2.15-0 Server Date and Time: Fri Sep 16 15:33:53 SGT 2016 HA Status: Not Configured Application Enablement Services Management Console Communication Manager Interface | Switch Connections Connection Details - Duplex Switch Password: •••••••••••••••• Confirm Switch Password: •••••••••••••••• Msg Period: 30 Minutes (1 - 72) Provide AE Services certificate to switch: □ Secure H323 Connection: □ Processor Ethernet: ☑ [Apply] [Cancel] AVAYA Home | Help | Logout AE Services Communication Manager Interface Switch Connections Dial Plan High Availability Licensing Maintenance Networking Security Status
3.	The Switch Connections screen is displayed. Select the newly added switch connection name and click **Edit PE/CLAN IPs**.  Welcome: User devconnect Last login: Fri Sep 16 15:07:06 2016 from 192.168.100.18 Number of prior failed login attempts: 0 HostName/IP: aes7x/10.1.10.70 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE SW Version: 7.0.1.0.2.15-0 Server Date and Time: Fri Sep 16 15:37:07 SGT 2016 HA Status: Not Configured Application Enablement Services Management Console Communication Manager Interface | Switch Connections Switch Connections [Add Connection] Connection Name | Processor Ethernet | Msg Period | Number of Active Connections ● Duplex | Yes | 30 | 1 ○ G450 | Yes | 30 | 1 [Edit Connection] [Edit PE/CLAN IPs] [Edit H.323 Gatekeeper] [Delete Connection] [Survivability Hierarchy] AVAYA Home | Help | Logout AE Services Communication Manager Interface Switch Connections Dial Plan High Availability Licensing Maintenance Networking Security

Step	Description
5.	In the **Edit Processor Ethernet IP – Duplex** screen, enter the host name or IP address of the PE/C-LAN used for AES connectivity. In this case, **10.1.10.230** is used, which corresponds to the **procr** address of the Communication Manager in **Section 5.1 Step 3**. Click **Add/Edit Name or IP** 

Welcome: User devconnect
Last login: Wed Sep 21 15:59:58 2016 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Wed Sep 21 16:14:40 SGT 2016
HA Status: Not Configured

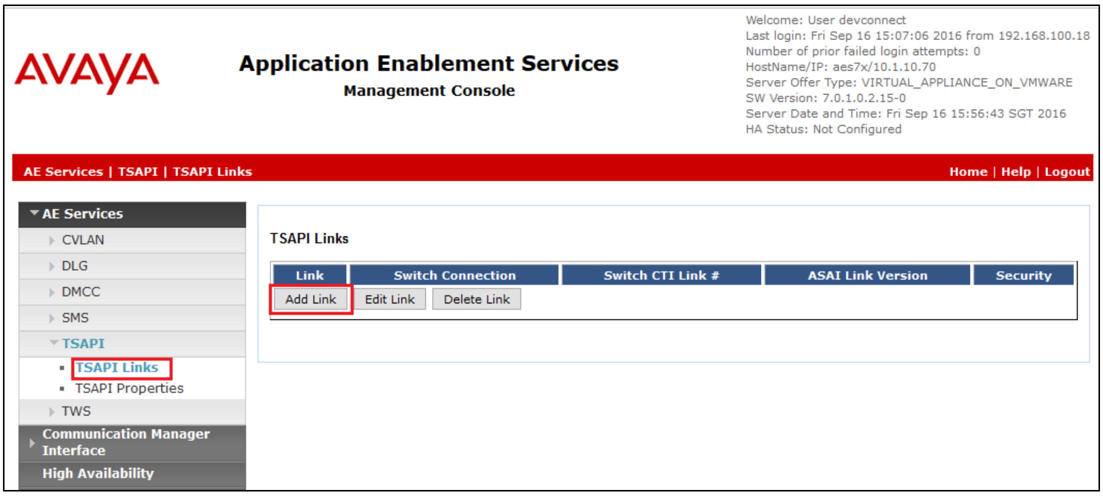
Edit Processor Ethernet IP - Duplex

10.1.10.230

6.4. Administer TSAPI Link and Verify TSAPI Service Port

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>

To administer a TSAPI link on AES, select **AE Services → TSAPI → TSAPI Links**. Click **Add Link**.



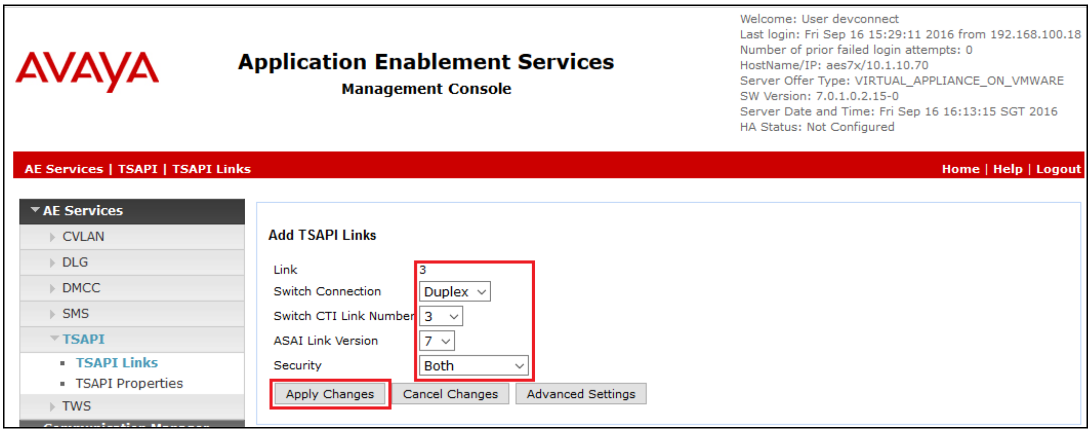
Welcome: User devconnect
Last login: Fri Sep 16 15:07:06 2016 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Fri Sep 16 15:56:43 SGT 2016
HA Status: Not Configured

</td></tr>
<tr><td>2.</td><td>

In the **Add TSAPI Links** screen, select the following values:

- **Link:** Select an available Link number from 1 to 16.
- **Switch Connection:** Administered switch connection in **Section 6.3 Step 1**.
- **Switch CTI Link Number:** Corresponding CTI link number in **Section 5.1 Step2**.
- **ASAI Link Version:** Set to **7** for the latest version.
- **Security:** Select **Both** to allow for encrypted or unencrypted link.

Click **Apply Changes**.

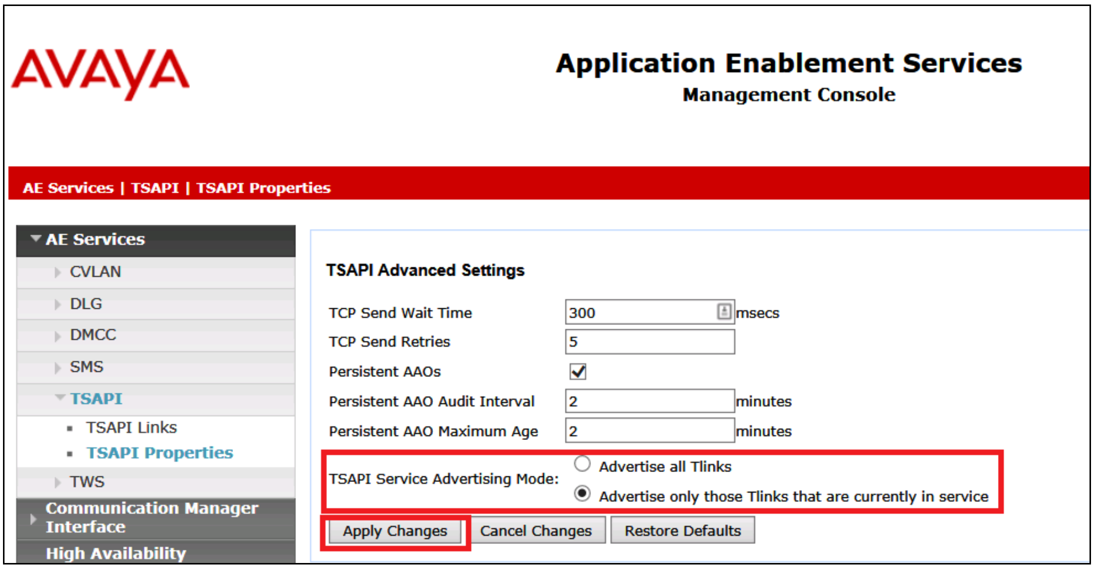
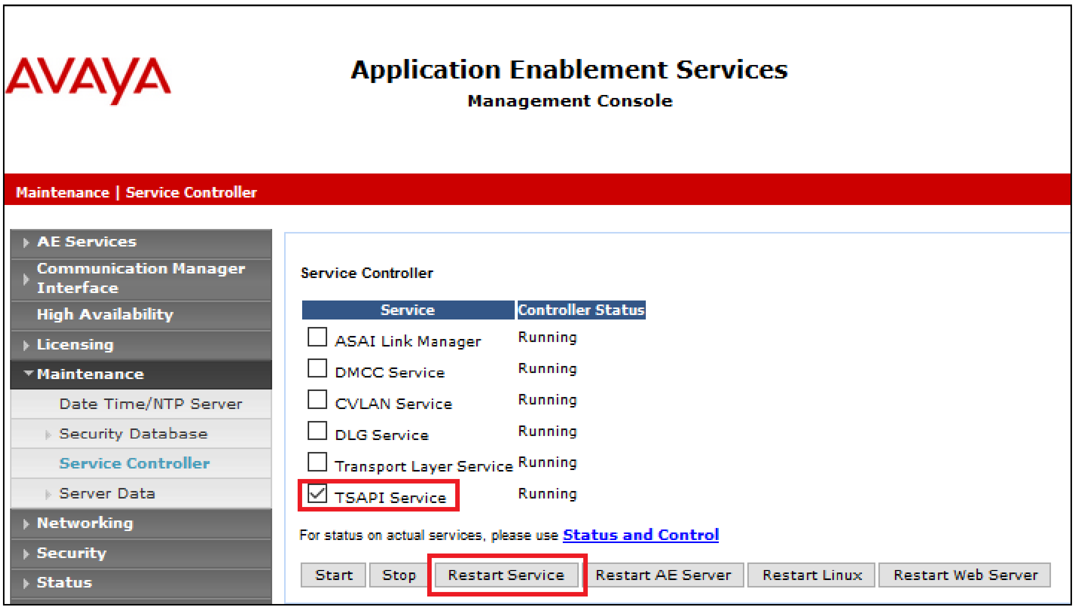


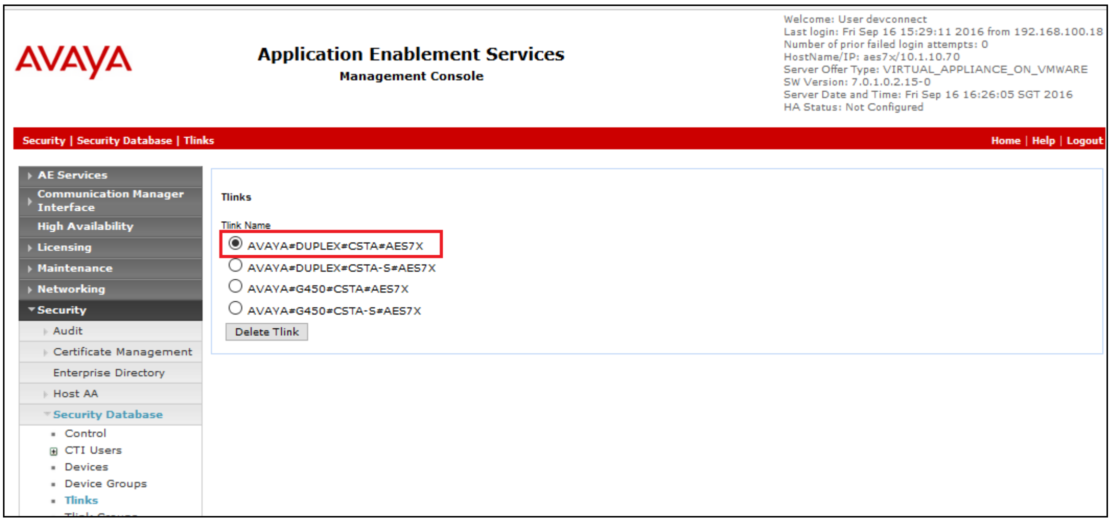
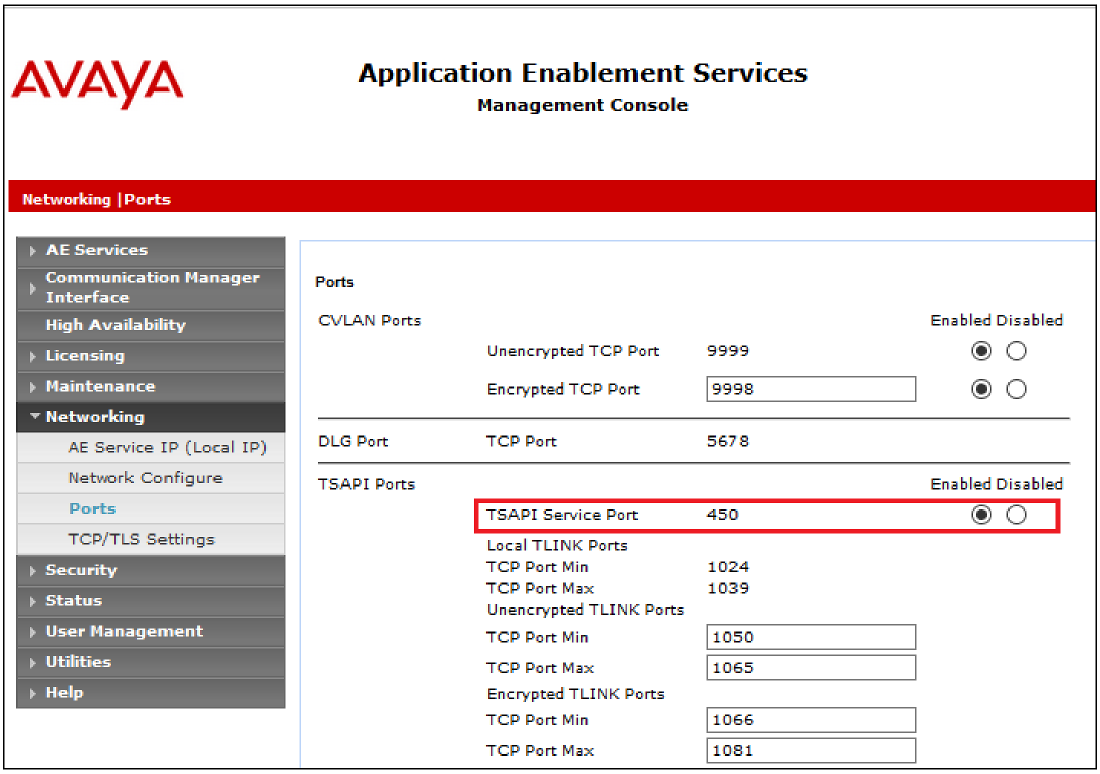
Welcome: User devconnect
Last login: Fri Sep 16 15:29:11 2016 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Fri Sep 16 16:13:15 SGT 2016
HA Status: Not Configured

Add TSAPI Links

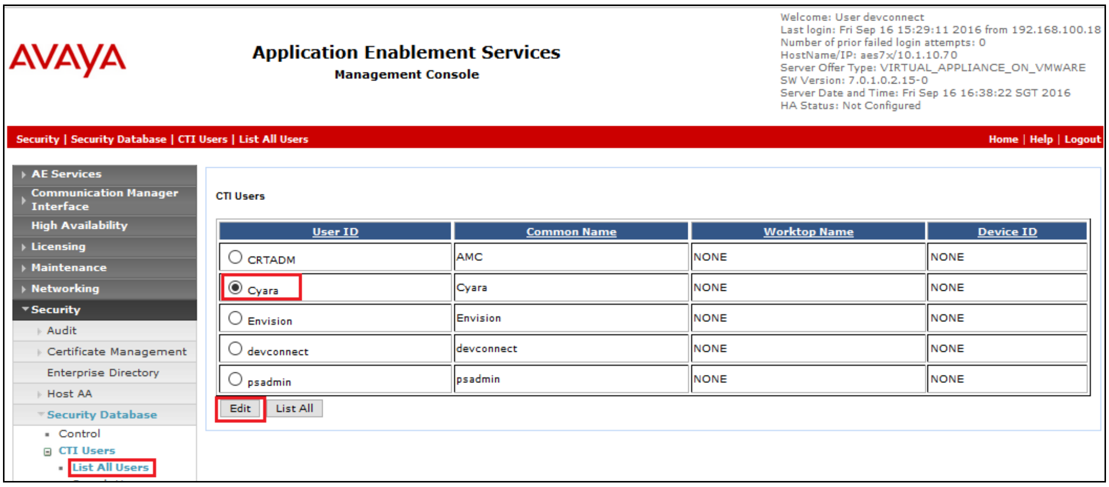
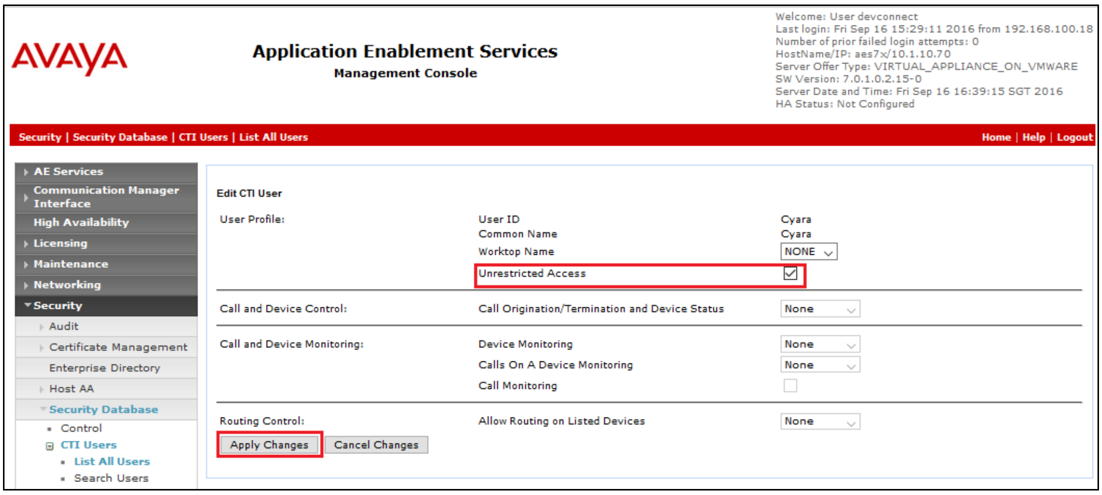
Link: 3
Switch Connection: Duplex
Switch CTI Link Number: 3
ASAI Link Version: 7
Security: Both

</td></tr>
</table>

Step	Description
3.	From the home screen, select **AE Services → TSAPI → TSAPI Properties**. Select the button on **Advertise only those Tlinks that are currently in service**. This will have the effect that only those Tlinks that are in service will be available to TSAPI applications. Any Tlinks that are not in service will **not** be available to TSAPI applications.  AVAYA Application Enablement Services Management Console AE Services | TSAPI | TSAPI Properties AE Services CVLAN DLG DMCC SMS TSAPI TSAPI Links TSAPI Properties TWS Communication Manager Interface High Availability Apply Changes Cancel Changes Restore Defaults TSAPI Advanced Settings TCP Send Wait Time: 300 msecs TCP Send Retries: 5 Persistent AAOs: ☑ Persistent AAO Audit Interval: 2 minutes Persistent AAO Maximum Age: 2 minutes TSAPI Service Advertising Mode: ○ Advertise all Tlinks ● Advertise only those Tlinks that are currently in service
4.	To restart the TSAPI Service, select **Maintenance → Service Controller** from the Home menu. Check the **TSAPI Service** checkbox and click **Restart Service**.  AVAYA Application Enablement Services Management Console Maintenance | Service Controller AE Services Communication Manager Interface High Availability Licensing Maintenance Date Time/NTP Server Security Database Service Controller Server Data Networking Security Status Start Stop Restart Service Restart AE Server Restart Linux Restart Web Server Service Controller Service — Controller Status □ ASAI Link Manager — Running □ DMCC Service — Running □ CVLAN Service — Running □ DLG Service — Running □ Transport Layer Service — Running ☑ TSAPI Service — Running For status on actual services, please use Status and Control

Step	Description
5.	Navigate to the Tlinks screen by selecting **Security → Security Database → Tlinks** from the Welcome to OAM home menu. Note the string of the **Tlink Name**, as this will be needed to configure the Cyara Platform Server in **Section 7**. In this configuration, the unencrypted string is **AVAYA#DUPLEX#CSTA#AES7X,** which is automatically assigned by the Avaya AES server, is used.  Application Enablement Services Management Console Security | Security Database | Tlinks Home | Help | Logout AE Services Communication Manager Interface High Availability Licensing Maintenance Networking Security Audit Certificate Management Enterprise Directory Host AA Security Database Control CTI Users Devices Device Groups Tlinks Welcome: User devconnect Last login: Fri Sep 16 15:29:11 2016 from 192.168.100.18 Number of prior failed login attempts: 0 HostName/IP: aes7x/10.1.10.70 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE SW Version: 7.0.1.0.2.15-0 Server Date and Time: Fri Sep 16 16:26:05 SGT 2016 HA Status: Not Configured Tlinks Tlink Name ● AVAYA#DUPLEX#CSTA#AES7X ○ AVAYA#DUPLEX#CSTA-S#AES7X ○ AVAYA#G450#CSTA#AES7X ○ AVAYA#G450#CSTA-S#AES7X Delete Tlink
6.	Navigate to the networking ports by **Networking → Ports**. Verify that the default **TSAPI Service Port 450** is **Enabled**.  Application Enablement Services Management Console Networking |Ports AE Services Communication Manager Interface High Availability Licensing Maintenance Networking AE Service IP (Local IP) Network Configure Ports TCP/TLS Settings Security Status User Management Utilities Help Ports CVLAN Ports — Enabled Disabled Unencrypted TCP Port 9999 ● ○ Encrypted TCP Port 9998 ● ○ DLG Port — TCP Port 5678 TSAPI Ports — Enabled Disabled TSAPI Service Port 450 ● ○ Local TLINK Ports TCP Port Min 1024 TCP Port Max 1039 Unencrypted TLINK Ports TCP Port Min 1050 TCP Port Max 1065 Encrypted TLINK Ports TCP Port Min 1066 TCP Port Max 1081

6.5. Administer CTI User Permission

Step	Description
1.	Select **Security → Security Database → CTI Users → List All Users** from the AES Management Console Home menu. Select the **User ID** created in **Section 6.1 Step 2** and click **Edit**. 
2.	Tick the **Unrestricted Access** box. Click **Apply Changes**. 

Step 1 screenshot:

AVAYA

Application Enablement Services
Management Console

Welcome: User devconnect
Last login: Fri Sep 16 15:29:11 2016 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Fri Sep 16 16:38:22 SGT 2016
HA Status: Not Configured

Security | Security Database | CTI Users | List All Users

Home | Help | Logout

CTI Users

User ID	Common Name	Worktop Name	Device ID
○ CRTADM	AMC	NONE	NONE
● Cyara	Cyara	NONE	NONE
○ Envision	Envision	NONE	NONE
○ devconnect	devconnect	NONE	NONE
○ psadmin	psadmin	NONE	NONE

Step 2 screenshot:

AVAYA

Application Enablement Services
Management Console

Welcome: User devconnect
Last login: Fri Sep 16 15:29:11 2016 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Fri Sep 16 16:39:15 SGT 2016
HA Status: Not Configured

Security | Security Database | CTI Users | List All Users

Home | Help | Logout

Edit CTI User

User Profile:	User ID	Cyara
	Common Name	Cyara
	Worktop Name	NONE
	Unrestricted Access	☑
Call and Device Control:	Call Origination/Termination and Device Status	None
Call and Device Monitoring:	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	□
Routing Control:	Allow Routing on Listed Devices	None

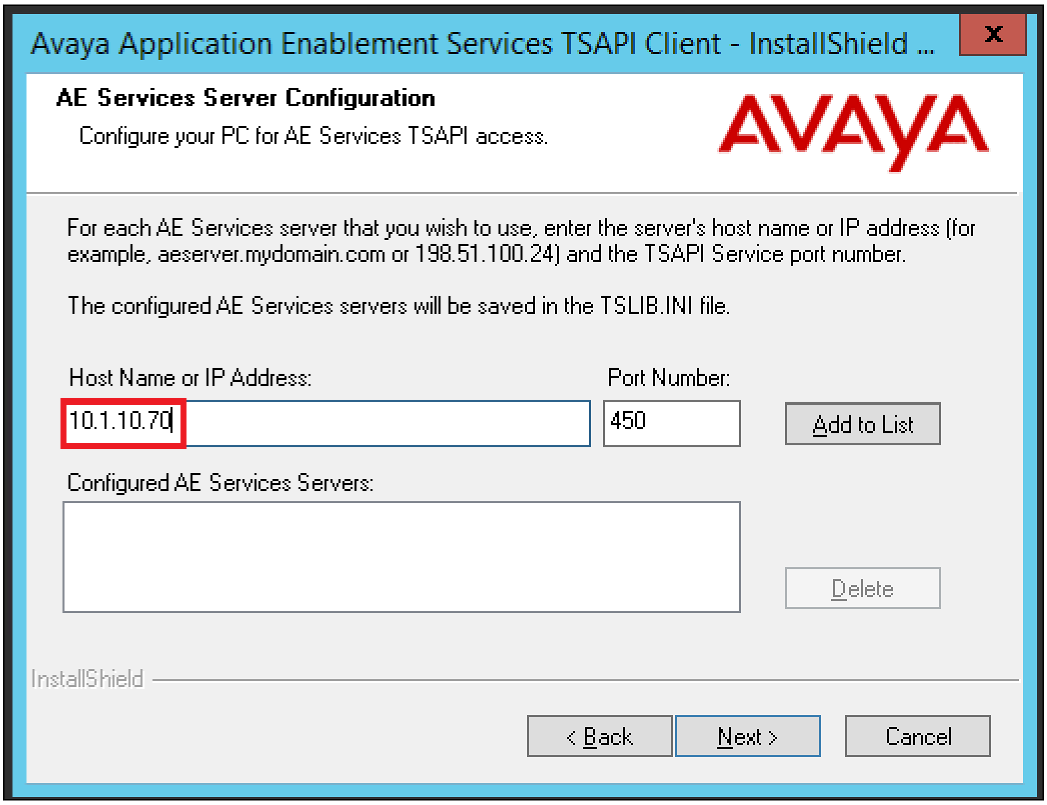
7. Configure Cyara Platform

An on-premises solution is setup for testing. Setup of the Cyara Platform server and Cyara Endpoint Server on Microsoft® Windows 2012 R2 will be done by Cyara engineers and will not be detailed here. Refer to Cyara Deployment Guide **[5]** for details. This section highlights the configuration of Cyara Server that interface with Avaya AES and it includes the following areas:

- Setup Avaya AES Client
- Verify Subcription Plans
- Configure Sites and Environment
- Configure Agents and Agents/Server Relationship
- On Test Cases, Behaviors and Campaigns

7.1. Setup Avaya AES Client

The Avaya AES client is installed with the Avaya AES ip address and Port Number in **Section 6.4 Step 6** are configured under **Host Name or IP Address** and **Port Number** during installation.



Avaya Application Enablement Services TSAPI Client - InstallShield ...

AE Services Server Configuration

Configure your PC for AE Services TSAPI access.

For each AE Services server that you wish to use, enter the server's host name or IP address (for example, aeserver.mydomain.com or 198.51.100.24) and the TSAPI Service port number.

The configured AE Services servers will be saved in the TSLIB.INI file.

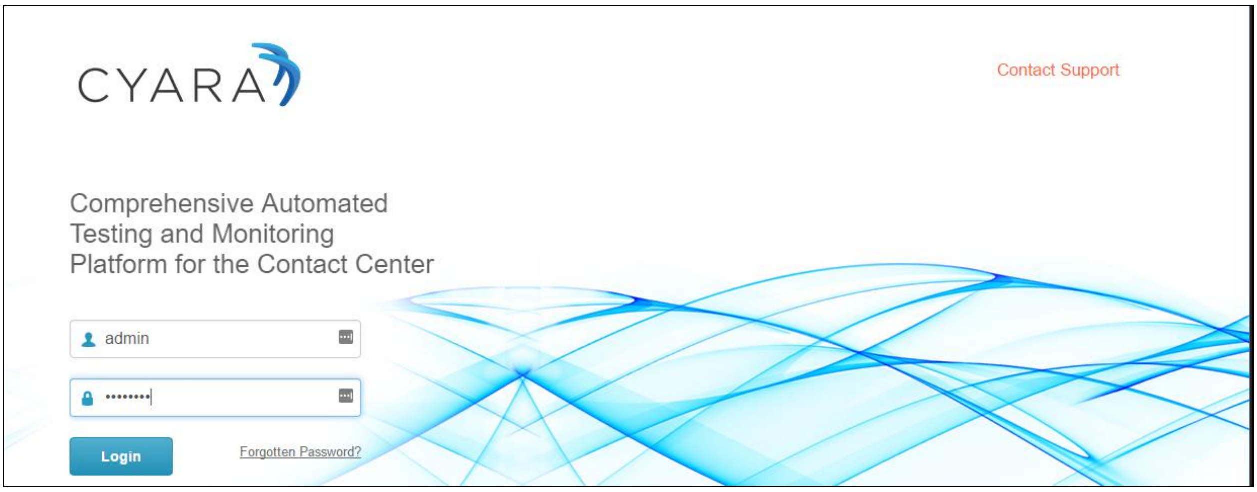
Host Name or IP Address: 10.1.10.70

Port Number: 450

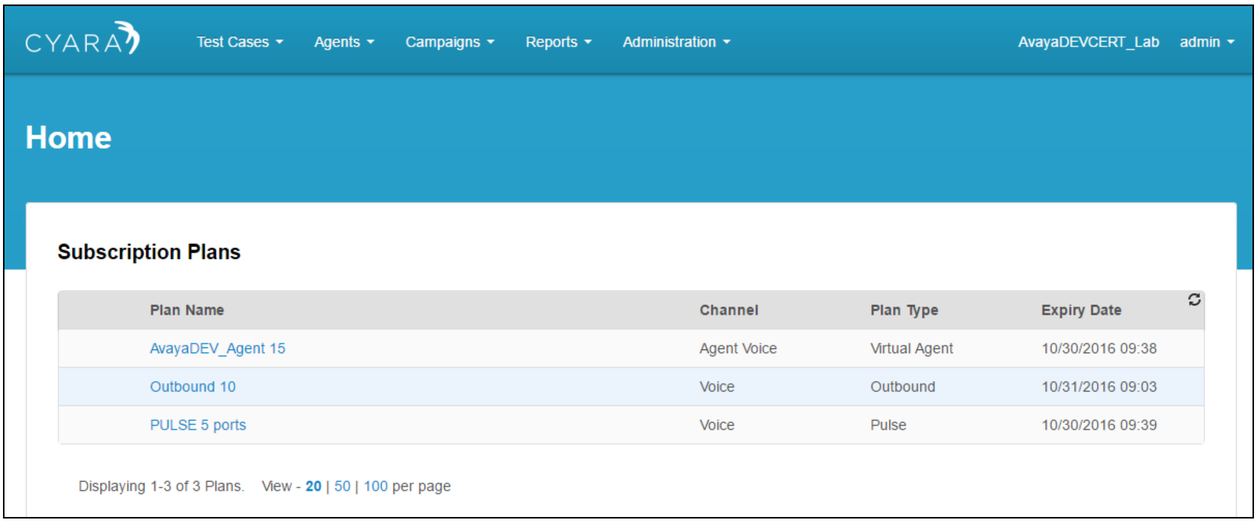
Configured AE Services Servers:

7.2. Verify Subscription Plans

Enter on a web browser **http://<IP address of Cyara Platform Server>/CyaraWebPortal** to access the system. Log in with an appropriate **Username** and **Password**.



In this compliance testing, **Virtual Agent** and **Outbound** under **Plan Type** are required. With **Virtual Agent** plan, users can create agent details, define behaviors and assign them to agents, run simulations for teams of agents or entire contact centers, and access reports on the outcomes of the simulations. **Outbound** plan is simply allowing the dialer to make calls to a simulated environment. If the subscription plans are not available, then contact the Cyara for a proper activation.



Home

Subscription Plans

Plan Name	Channel	Plan Type	Expiry Date
AvayaDEV_Agent 15	Agent Voice	Virtual Agent	10/30/2016 09:38
Outbound 10	Voice	Outbound	10/31/2016 09:03
PULSE 5 ports	Voice	Pulse	10/30/2016 09:39

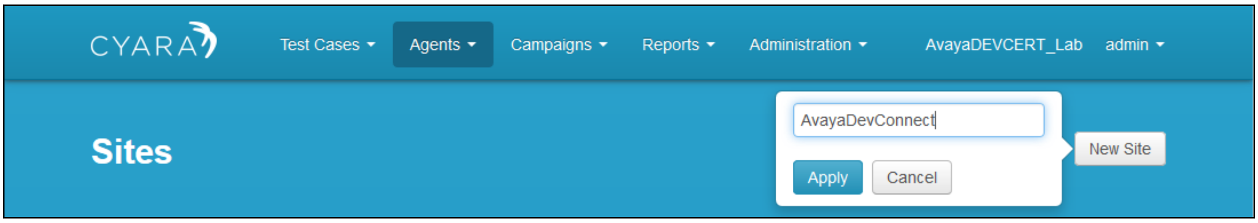
Displaying 1-3 of 3 Plans. View - 20 | 50 | 100 per page

7.3. Configure Sites and Environment

The Cyara Platform Server provides the test and monitoring platform where user emulates real callers. Normally, calls are placed into IVR at regular intervals and results are monitored in real time and stored. In this compliance test, we manually place test calls. Administration, scripting, monitoring and reporting are done via the Cyara Web Portal.

7.3.1. Add Sites

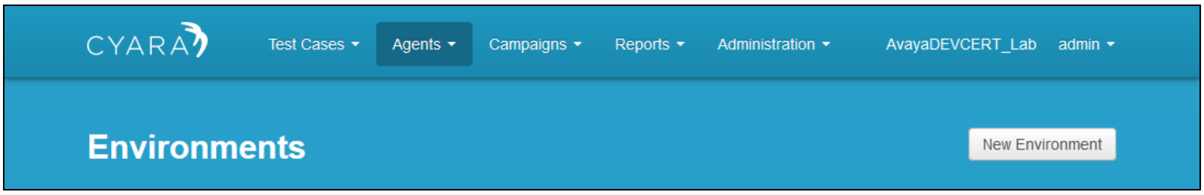
Select **Agent** Tab and from the dropdown menu, click **Sites** (not shown)→ **New Site** on the right of the screen. Enter appropriate site name. In this case, **AvayaDevConnect** is used.



AvayaDevConnect

7.3.2. Create Environment

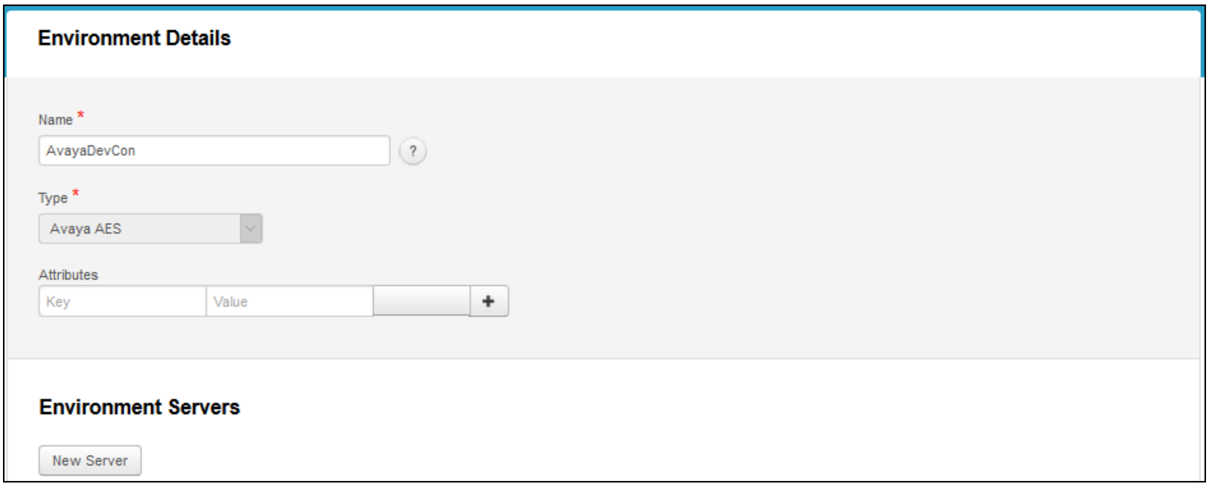
Select **Agent** Tab and from the drop down menu, click **Environments** (not shown). Select **New Environment** on the right of the screen.



Enter the following details:

- **Name** Enter appropriate name.
- **Type** Select **Avaya AES** from the drop down menu.

Under header **Environment Servers** below, click **New Server**.

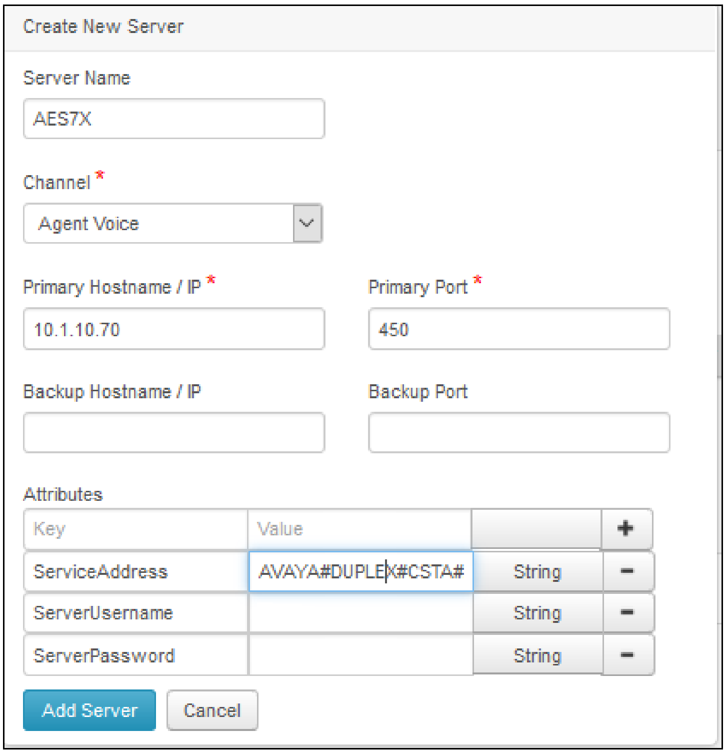


Name * AvayaDevCon

Type * Avaya AES

Enter the following details:

- **Server Name** Enter appropriate name.
- **Channel** Select Agent Voice from the drop down menu.
- **Primary Hostname/IP** Enter ip address of AES i.e., **10.1.10.70**
- **Primary Port** Enter default port as configured in **Section 6.4 Step 6**.



Create New Server

Server Name: AES7X

Channel *: Agent Voice

Primary Hostname / IP *: 10.1.10.70

Primary Port *: 450

Backup Hostname / IP:

Backup Port:

Attributes

Key	Value		+
ServiceAddress	AVAYA#DUPLEX#CSTA#	String	−
ServerUsername		String	−
ServerPassword		String	−

From previous page, under **Attributes**, input the following values:

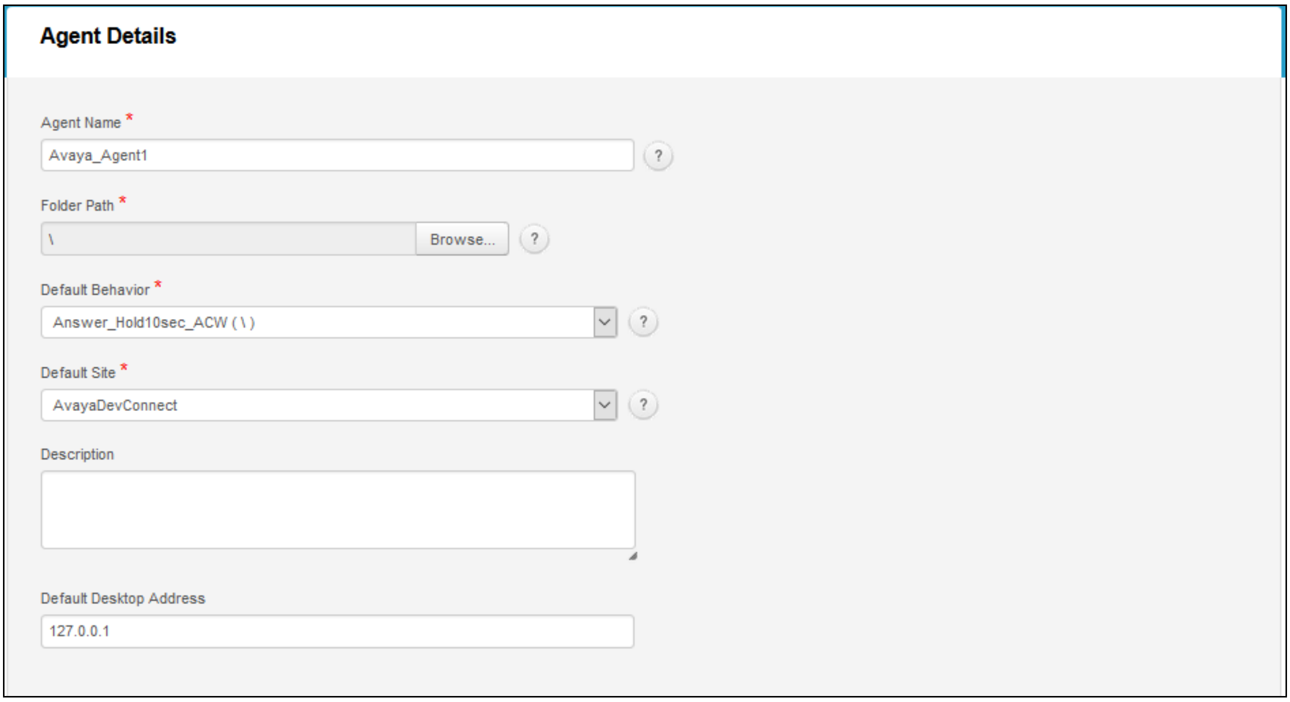
- **ServiceAddress** Enter the Tlink Name as in **Section 6.4 Step 5**.
- **ServiceUserName** Enter User name created in **Section 6.1 Step 2**.
- **ServicePassword** Enter User password created in **Section 6.1 Step 2**.

Click **Add Server** and after all details are entered for the new Environment, click **Save Details** (not shown).

7.4. Create Agents and Agents/Server Relationship

Select **Agent** Tab and from the drop down menu, click **New Agent** (not shown). Complete the following:

- **Agent Name** Enter appropriate agent name say **Avaya_Agent1**.
- **Default Behavior** Select say **Answer_Hold10sec_ACW (\)** which is pre-created from a list of behaviors to be tested.
- **Default Site** Select site created in **Section 7.3.1**.
- **Default Desktop Address** Enter **127.0.0.1** for the localhost.



Agent Details

Agent Name * Avaya_Agent1

Folder Path * \

Default Behavior * Answer_Hold10sec_ACW (\ )

Default Site * AvayaDevConnect

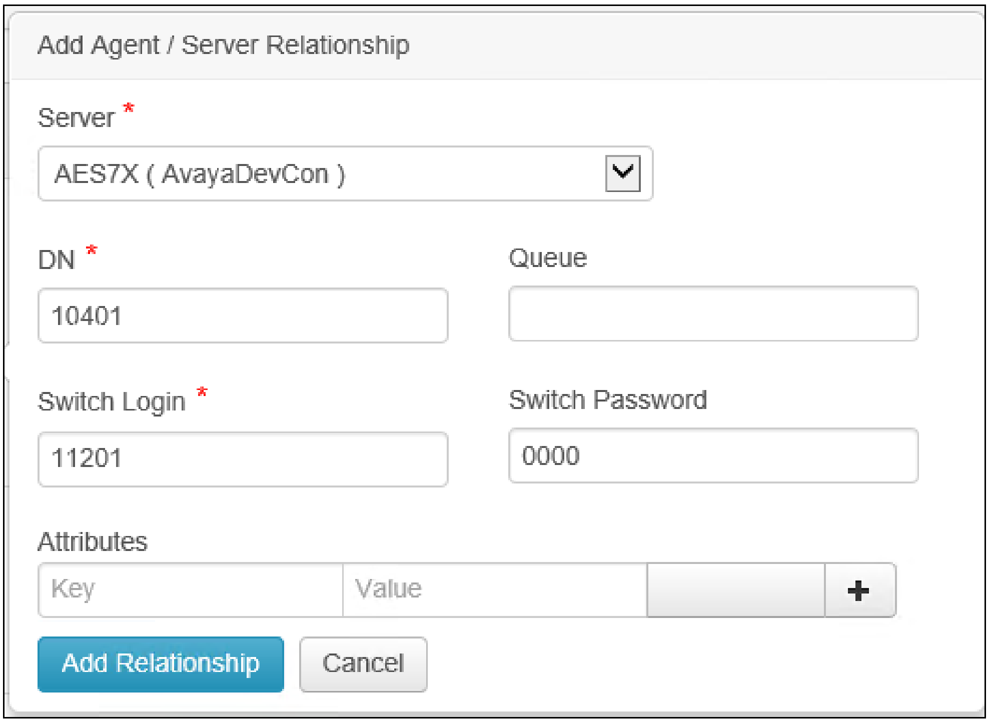
Description

Default Desktop Address 127.0.0.1

Scroll down below, under **Agent Servers** click **Add Agent / Server Relationship** (not shown) which will pop up. Complete the following:

• **Server**	Select the server created in **Section 7.3.2**.
• **DN**	Enter the Virtual Endpoint extensions. This is assumed to be created which is detailed in another Application Notes **[4]**.
• **Switch Login**	Enter agent loginID created in **Section 5.2**.
• **Switch Password**	Enter agent password created in **Section 5.2**.

Leave the rest as default and click **Add Relationship**. On completion, click **Save Details** (not shown). Repeat this for agents to be created. In this compliance test, agent loginIDs 11201 to 11210 were created.


Add Agent / Server Relationship

Server * AES7X (AvayaDevCon)

DN * 10401

Queue

Switch Login * 11201

Switch Password 0000

Attributes

7.5. Test Cases, Agent Behaviors and Campaigns

Test cases, Agent Behaviors and Campaigns created for this testing will not be elaborated here as it depends on the desired agent behaviors and test scenarios. User guide can be obtained online from the Cyara Web Portal **[6]** or from Cyara engineers.

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Avaya AES and Cyara Web Portal.

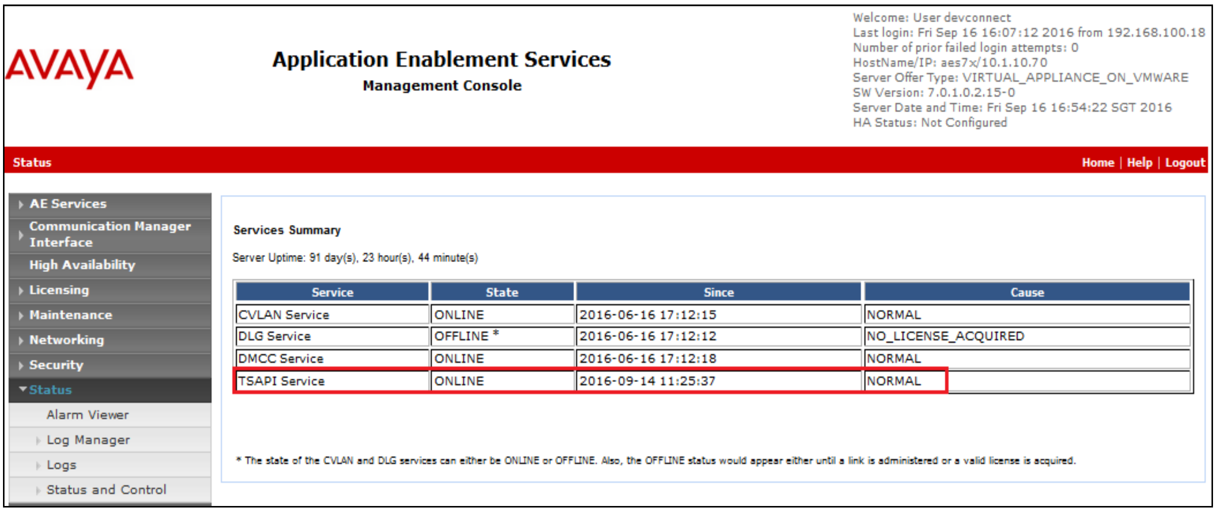
8.1. Verify Communication Manager

Verify the status of the administered TSAPI CTI link by using the **status aesvcs cti-link** command. The **Service State** field should display **established**.

```
status aesvcs cti-link

                           AE SERVICES CTI LINK STATUS

CTI   Version  Mnt   AE Services      Service       Msgs     Msgs
Link           Busy  Server           State         Sent     Rcvd

3     7        no    aes7x            established   15       15
4     7        no    aes7x            established   98       98
```

8.2. Verify Avaya Application Enablement Services

From the Welcome to OAM web pages, verify the status of the TSAPI Service by selecting **Status**. The **State** field for the **TSAPI Service** should display **ONLINE**.



Welcome: User devconnect
Last login: Fri Sep 16 16:07:12 2016 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Fri Sep 16 16:54:22 SGT 2016
HA Status: Not Configured

Services Summary

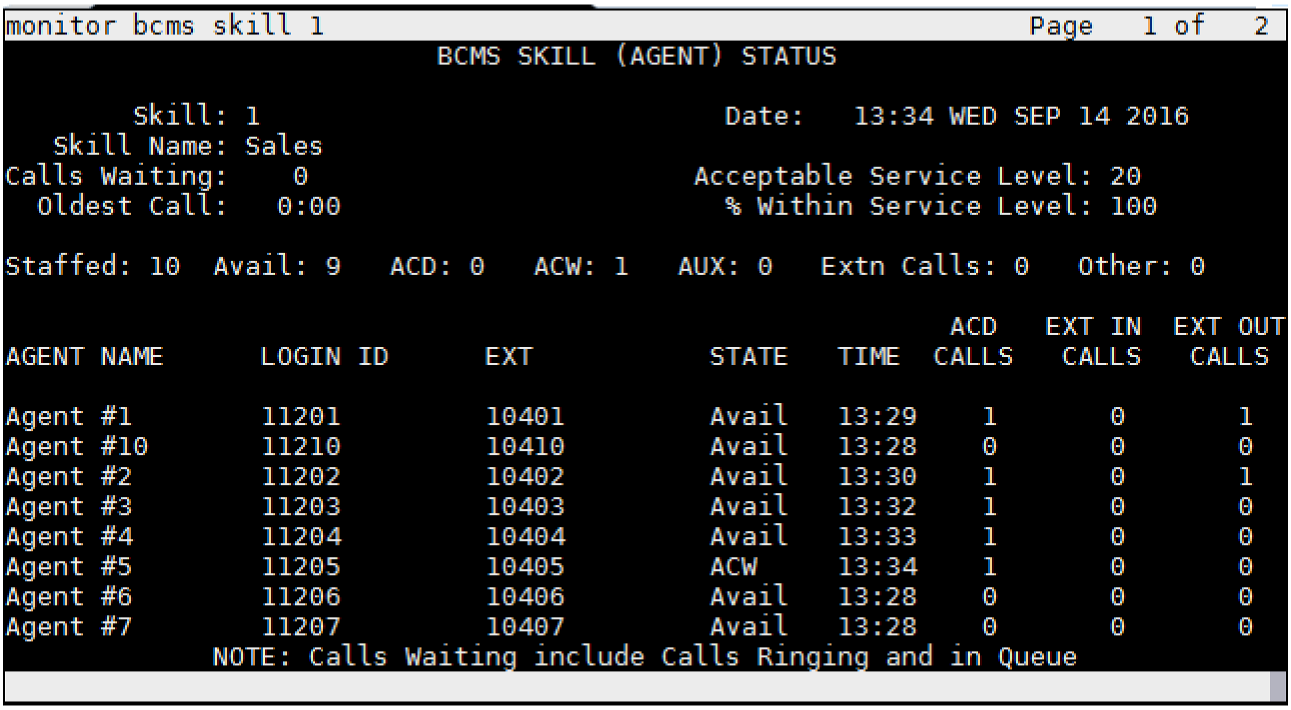
Server Uptime: 91 day(s), 23 hour(s), 44 minute(s)

Service	State	Since	Cause
CVLAN Service	ONLINE	2016-06-16 17:12:15	NORMAL
DLG Service	OFFLINE *	2016-06-16 17:12:12	NO_LICENSE_ACQUIRED
DMCC Service	ONLINE	2016-06-16 17:12:18	NORMAL
TSAPI Service	ONLINE	2016-09-14 11:25:37	NORMAL

* The state of the CVLAN and DLG services can either be ONLINE or OFFLINE. Also, the OFFLINE status would appear either until a link is administered or a valid license is acquired.

8.3. Verify Agent States

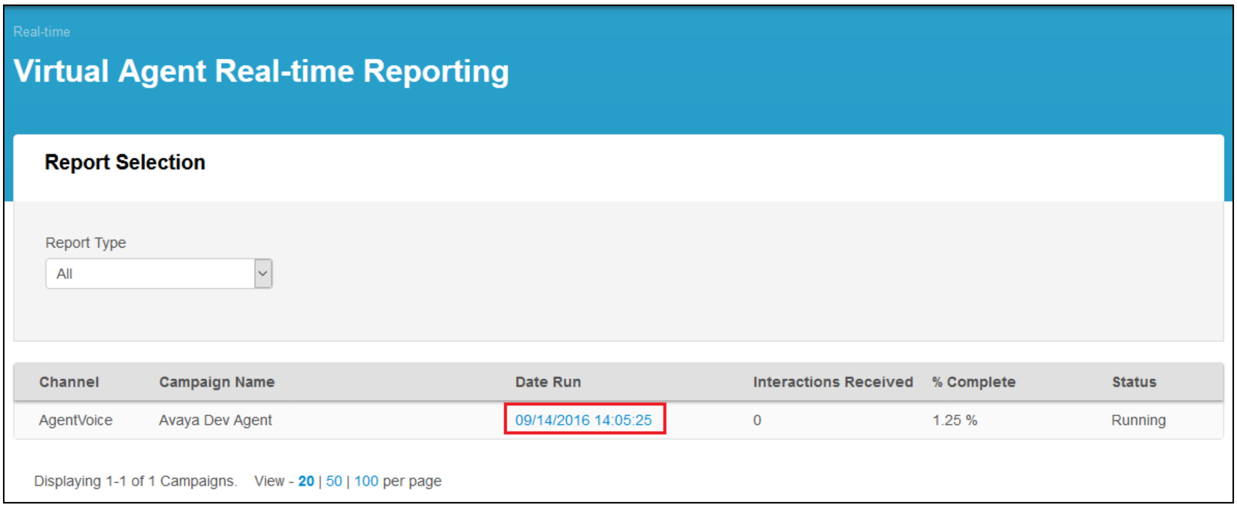
From Communication Manager SAT login, the **monitor bcms** command can be used to verify the agent current state under **STATE** when calls are made and agent campaigns are run.



```
monitor bcms skill 1                                            Page   1 of   2
                           BCMS SKILL (AGENT) STATUS

        Skill: 1                                    Date:   13:34 WED SEP 14 2016
   Skill Name: Sales
Calls Waiting:    0                               Acceptable Service Level: 20
  Oldest Call:   0:00                               % Within Service Level: 100

Staffed: 10  Avail: 9   ACD: 0   ACW: 1   AUX: 0   Extn Calls: 0   Other: 0

                                                                ACD   EXT IN  EXT OUT
AGENT NAME      LOGIN ID      EXT           STATE   TIME   CALLS   CALLS   CALLS

Agent #1        11201         10401         Avail   13:29    1       0       1
Agent #10       11210         10410         Avail   13:28    0       0       0
Agent #2        11202         10402         Avail   13:30    1       0       1
Agent #3        11203         10403         Avail   13:32    1       0       0
Agent #4        11204         10404         Avail   13:33    1       0       0
Agent #5        11205         10405         ACW     13:34    1       0       0
Agent #6        11206         10406         Avail   13:28    0       0       0
Agent #7        11207         10407         Avail   13:28    0       0       0
             NOTE: Calls Waiting include Calls Ringing and in Queue
```

8.4. Verify Cyara Virtual Agents

When campaigns are running for the Virtual Agent to be active and the Virtual Station to answer incoming calls, select **Reports** Tab and from the drop down menu, click under **Agent**, **Real Time**. Below shows the campaign running for the Virtual Agent. Click on the highlighted for the campaign **Date Run** column for the **Avaya Dev Agent**.



Real-time

Virtual Agent Real-time Reporting

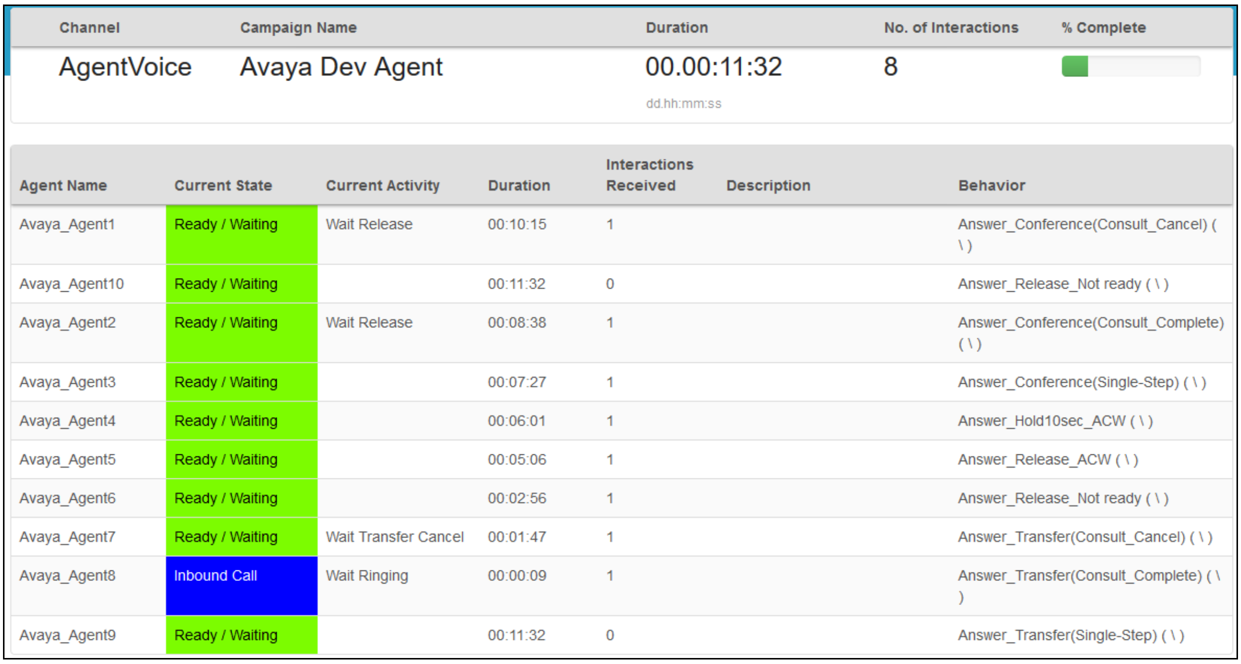
Report Selection

Report Type: All

Channel	Campaign Name	Date Run	Interactions Received	% Complete	Status
AgentVoice	Avaya Dev Agent	09/14/2016 14:05:25	0	1.25 %	Running

Displaying 1-1 of 1 Campaigns. View - 20 | 50 | 100 per page

Below shows a list of 10 Virtual Agents associated with different behaviors. Manually make calls using the utility phones to the VDN. From here, agents' activities can be monitored to verify correct behavior.



Channel	Campaign Name	Duration	No. of Interactions	% Complete
AgentVoice	Avaya Dev Agent	00.00:11:32 dd.hh:mm:ss	8	🟩

Agent Name	Current State	Current Activity	Duration	Interactions Received	Description	Behavior
Avaya_Agent1	Ready / Waiting	Wait Release	00:10:15	1		Answer_Conference(Consult_Cancel) (\ )
Avaya_Agent10	Ready / Waiting		00:11:32	0		Answer_Release_Not ready (\ )
Avaya_Agent2	Ready / Waiting	Wait Release	00:08:38	1		Answer_Conference(Consult_Complete) (\ )
Avaya_Agent3	Ready / Waiting		00:07:27	1		Answer_Conference(Single-Step) (\ )
Avaya_Agent4	Ready / Waiting		00:06:01	1		Answer_Hold10sec_ACW (\ )
Avaya_Agent5	Ready / Waiting		00:05:06	1		Answer_Release_ACW (\ )
Avaya_Agent6	Ready / Waiting		00:02:56	1		Answer_Release_Not ready (\ )
Avaya_Agent7	Ready / Waiting	Wait Transfer Cancel	00:01:47	1		Answer_Transfer(Consult_Cancel) (\ )
Avaya_Agent8	Inbound Call	Wait Ringing	00:00:09	1		Answer_Transfer(Consult_Complete) (\ )
Avaya_Agent9	Ready / Waiting		00:11:32	0		Answer_Transfer(Single-Step) (\ )

9. Conclusion

These Application Notes describe the configuration steps required for Cyara Platform Virtual Agent to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using the Telephony Services Application Programming Interface (TSAPI). All feature test cases were completed successfully with observations in **Section 2.2**.

10. Additional References

This section references the Avaya and Cyara documentations that are relevant to these Application Notes.

The following Avaya product documentations can be found at http://support.avaya.com.
[1] *Deploying Avaya Aura® Application Enablement Services in Virtualized Environment,* Release 7.0.1, Issue 3, Aug 2016
[2] *Administering and Maintaining Avaya Aura® Application Enablement Services*, Release 7.0.1, Issue 2, Aug 2016.
[3] *Avaya Aura® Avaya Communication Manager Feature Description and Implementation*, Document Number 555-245-205, Release 7.0.1, Issue 3, Sep 2016.
[4] *Application Notes for Cyara CX Automated Test and Monitoring Virtual Endpoint with Avaya Aura® Communication Manager 7.0*

The following Cyara product documentation is obtained is either obtained directly from member or available online.
[5] Cyara Platform Deployment Guide
[6] Cyara User Guide available online at https://www.cyaraportal.com/CyaraWebPortal

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.