Avaya Solution & Interoperability Test Lab

Application Notes for Cyara Platform Virtual Agent with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Cyara Platform Virtual Agent 20.1 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services (AES) 8.1.

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 Platform Virtual Agent 20.1 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services (AES) 8.1. Virtual Agent registered to Communication Manager through Cyara Virtual Endpoint that use H.323 Endpoints emulation which will be covered in Application Notes reference [4].

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 Platform Virtual Agent Service is one of the components of the Cyara Platform that interacts with Telephony Services Application Programming Interface (TSAPI) service on AES to automate agent activities in order to simulate contact center operations. Cyara Platform Virtual Agent Service logs the required agents into the CTI environment and performs the activities specified by the designated behaviors assigned to the agents. The Cyara Virtual Agent also interfaces with the Cyara Database and Web Portal.

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 reference [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. It also includes disrupting the Ethernet connectivity to the Cyara Platform server.

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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and the Cyara Platform did not include use of any specific encryption features as requested by Cyara.

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.
- Agent work mode changes and reason codes.
- Handling of incoming ACD calls.
- Holding and resuming of calls.
- Consult and single step transfers including cancellation.
- Consult and single step conference including cancellation.
- Correct status of agent reflected on the test user interface.
- Proper termination 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. It also includes disrupting the ethernet connectivity to the Cyara Platform server.

2.2. Test Results

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

- Active Campaigns that are running have to be restarted if the CTI link is restarted on Communication Manager.

2.3. Support

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

- Phone: +61-3-9093-0815 (Australia), +44-203-786-5070 (Europe/Middle East/Africa), +1-650-549-8522 (North America/Latin America)
- Email: support@cyara.com
- Web: http://support.cyara.com/

3. Reference Configuration

An on-premises solution is conducted in this compliance testing. **Figure 1** illustrates a sample configuration consisting of Communication Manager, Avaya G430 Media Gateway, AES, Avaya Media Server, Session Manager and System Manager. The System Manager is the administration and management tool for the Avaya Aura® products. Avaya one-X® Communicator is used as utility softphone for initiating calls. Cyara Platform Server is installed on Microsoft Windows 2016 which communicates with the TSAPI Service on the Avaya AES Server. Microsoft SQL 2016 was installed as the database on the same server. Cyara Virtual Endpoint server also installed on Microsoft Windows 2016 provides the virtual H.323 endpoints which will be detailed in another Application Notes reference [4]. A personal computer was used for Cyara Web Portal access. Avaya Session Border Controller for Enterprise was used to complete a SIP trunk connection to simulate a PSTN connection to the Enterprise solution.

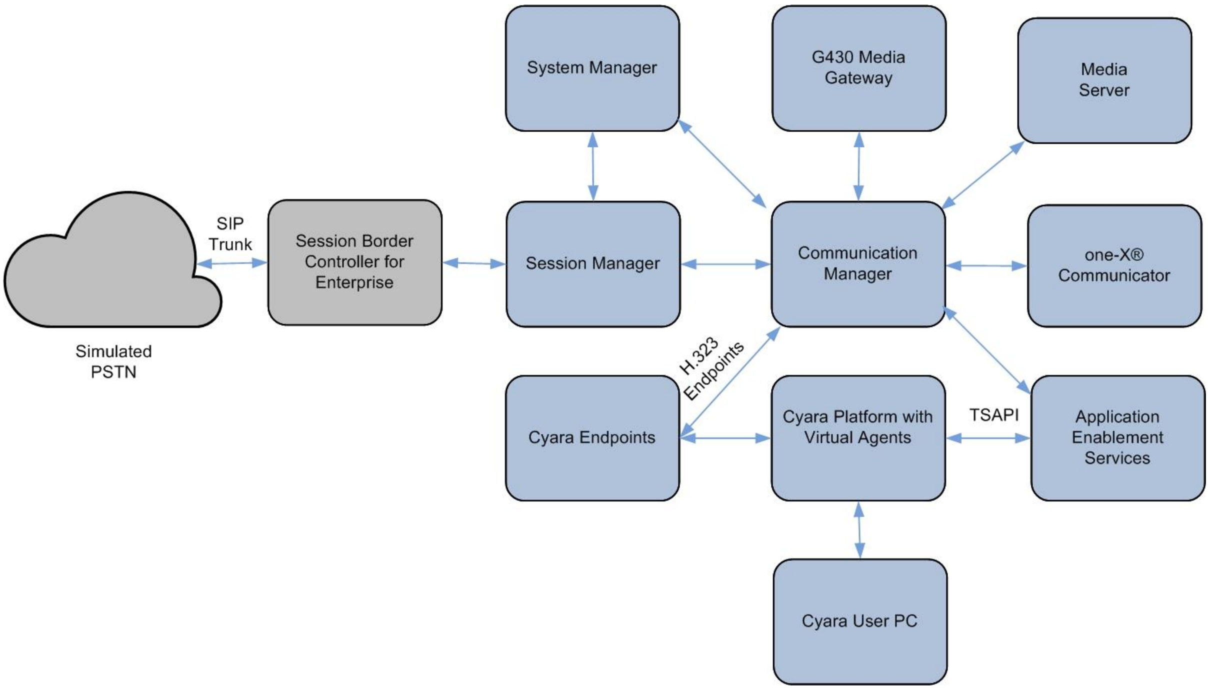


Figure 1: Test Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager Servers	8.1.2.0.0.890.26095
Avaya G430 Media Gateway • MGP	 41.16.0
Avaya Aura® Application Enablement Services	8.1.2.0.0.9-0
Avaya Aura® Media Server	8.0.2.93
Avaya Aura® System Manager	8.1.2.0.0611167
Avaya Aura® Session Manager	8.1.2.0.812033
Avaya one-X® Communicator	6.2.14.4-SP14
Cyara Platform running on Microsoft Windows 2016 • Avaya TSAPI Client	20.1.0 8.0.1-132
Cyara Endpoint running on Microsoft Windows 2016	20.1.0
Dell PC	Microsoft Windows 10 Pro

Table 1: Equipment/Software Validated

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas.

- Verify license
- Administer CTI link
- Configure agent IDs

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.

Setup of VDNs, Hunt Groups and Trunks are assumed to be configured and will not be detailed here. Setup of virtual stations registered to Communication Manager as generic H.323 endpoints will be covered in Application Notes reference [4].

5.1. Verify License

Enter the **display system-parameters customer-options** command. On **Page 4**, verify that **Computer Telephony Adjunct Links** is set to **y**. If not, contact an authorized Avaya account representative to obtain the license.

```
display system-parameters customer-options                     Page   4 of  12
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? y              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
```

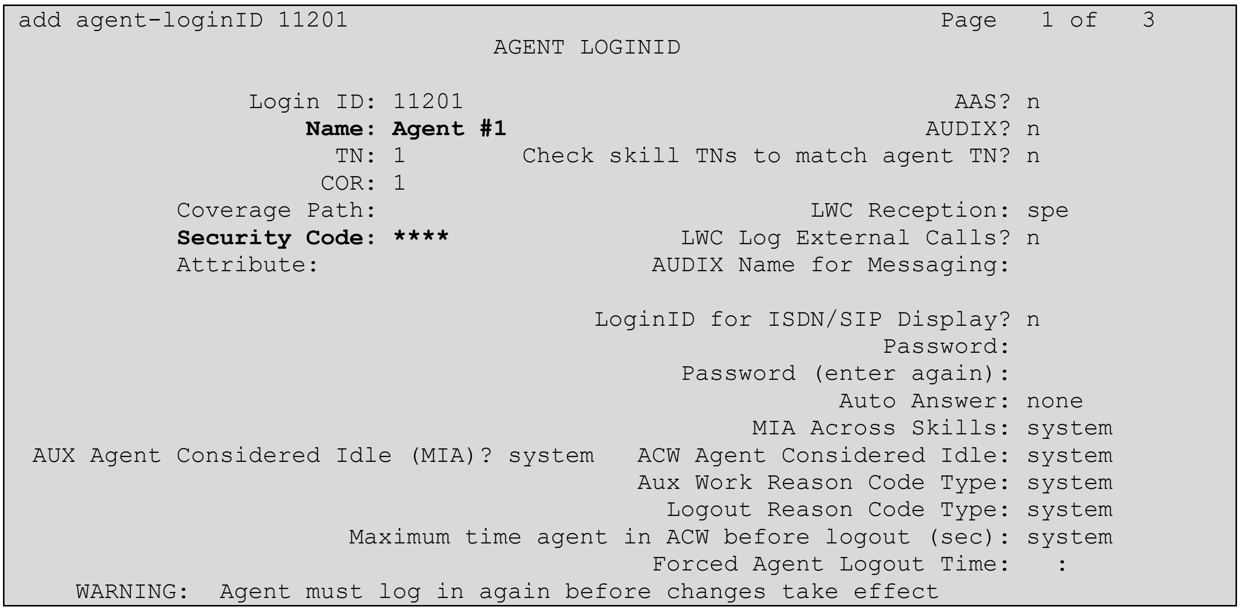
5.2. Administer CTI Link

Enter the **add cti-link m** command, where **m** is a number between 1 and 64, inclusive. Enter a valid **Extension** under the provisioned dial plan in Communication Manager, set the **Type** field to **ADJ-IP**, and assign a descriptive **Name** to the CTI link.

```
add cti-link 3                                                 Page   1 of   3
                                    CTI LINK
 CTI Link: 3
Extension: 10093
     Type: ADJ-IP
                                                                      COR: 1
     Name: TSAPI Service - AES 8x
Unicode Name? n
```

5.3. Configure Agent IDs

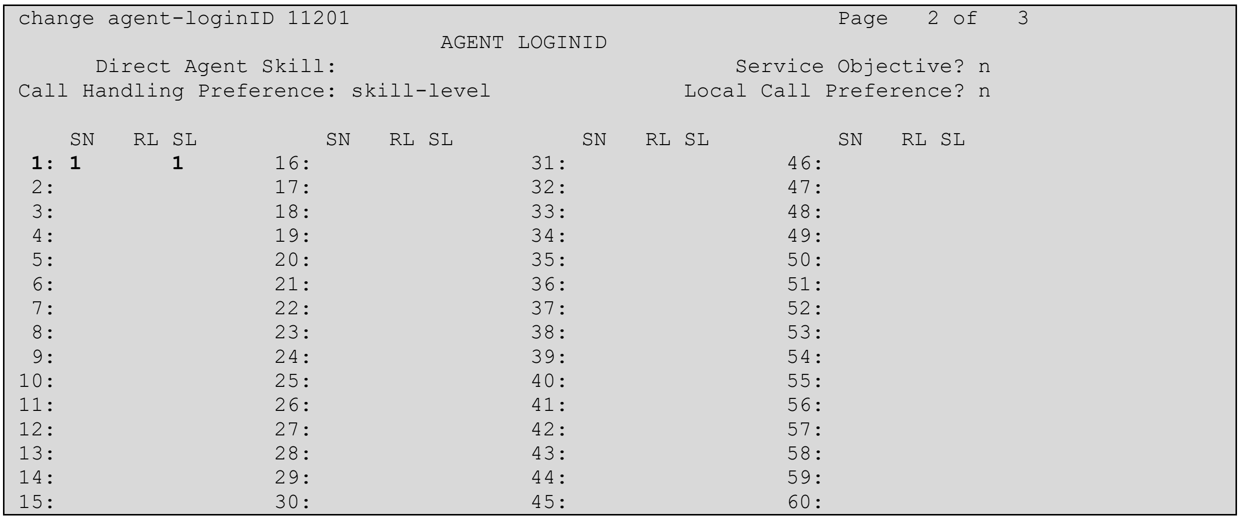
Enter the **add agent-loginID x** command where **x** is a valid agent login ID. On **Page 1**, enter an appropriate **Name** and configure the **Security Code** to desired value.



```
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: ****             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
```

On **Page 2**, configure appropriate Skill **SN** and Skill Level **SL** for testing purpose. Repeat to configure the rest of the agent login IDs required.

In this testing, agent login ID **11201** to **11210** were created which will logon using Virtual Endpoints **10401** to **10410** which are generic H.323 stations where configurations will be covered in Application Notes reference [4].



```
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 Aura® Application Enablement Services

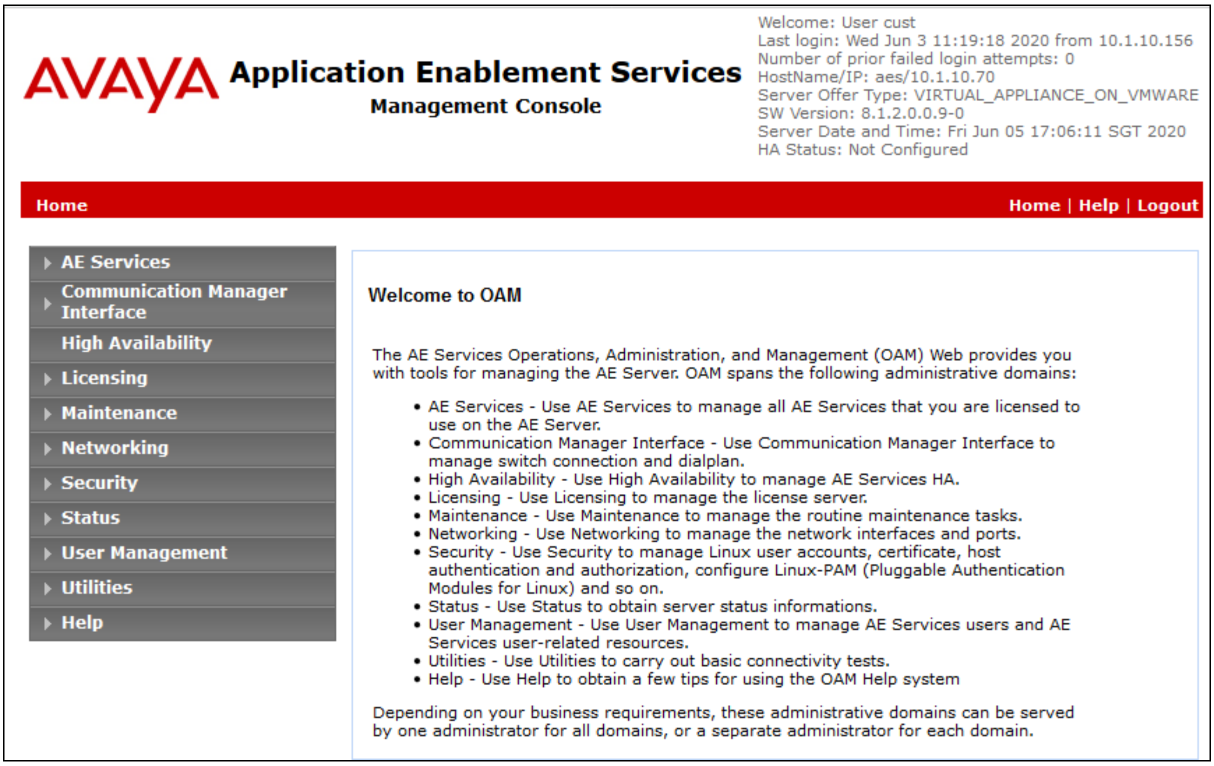
This section provides the procedures for configuring AES. The procedures fall into the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer Cyara user
- Administer security database
- Administer TSAPI ports
- Restart TSAPI service
- Obtain Tlink name

6.1. Launch OAM Interface

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.



Welcome: User cust
Last login: Wed Jun 3 11:19:18 2020 from 10.1.10.156
Number of prior failed login attempts: 0
HostName/IP: aes/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.0.0.9-0
Server Date and Time: Fri Jun 05 17:06:11 SGT 2020
HA Status: Not Configured

Welcome to OAM

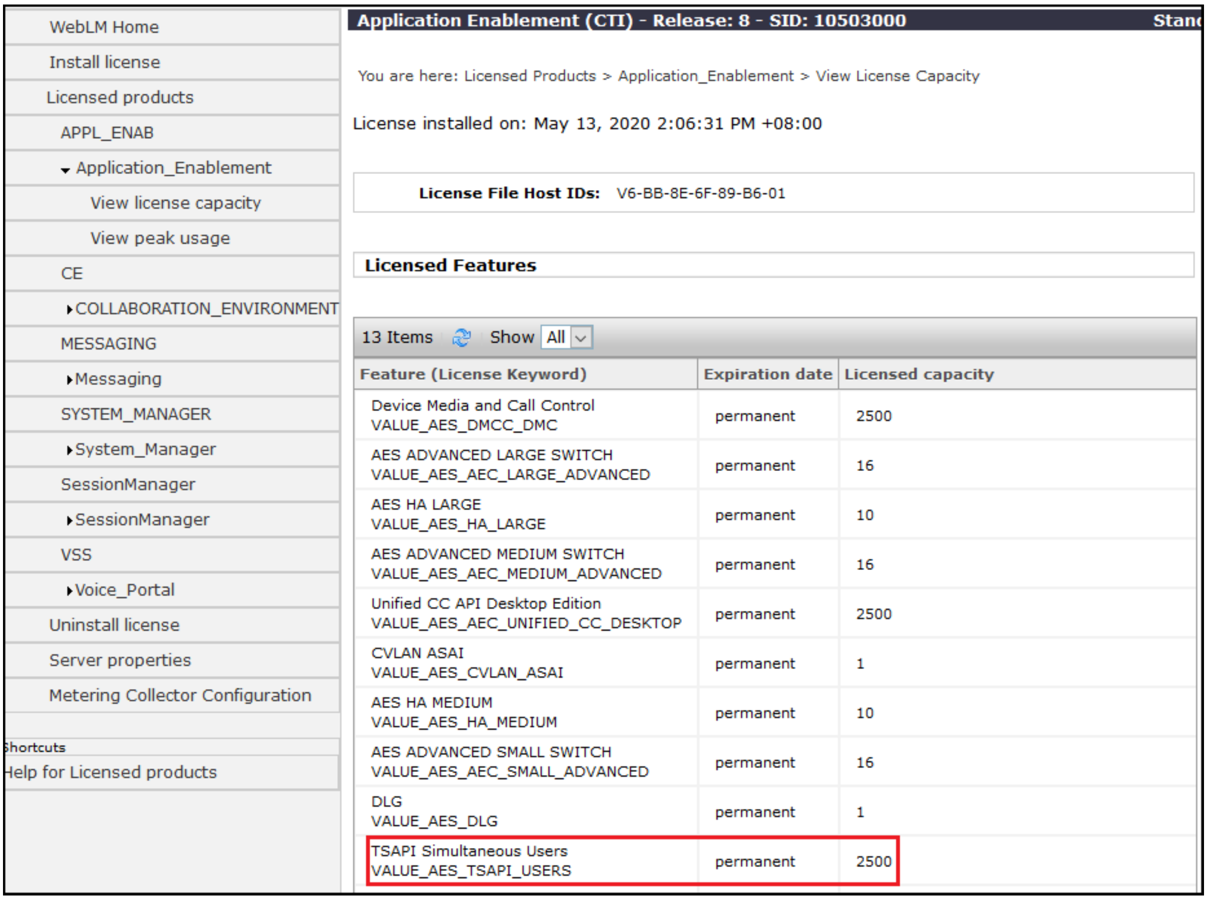
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- 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.

6.2. Verify License

Access the Web License Manager used by the AES server. The **Web License Manager** screen below is displayed. Select **Licensed products → APPL_ENAB → Application_Enablement** in the left pane, to display the **Licensed Features** screen in the right pane. Verify that there are sufficient licenses for **TSAPI Simultaneous Users**, as shown below. If not, consult with your Avaya Account Manager or Business Partner to acquire the proper license for your solution.



Application Enablement (CTI) - Release: 8 - SID: 10503000 Stan

You are here: Licensed Products > Application_Enablement > View License Capacity

License installed on: May 13, 2020 2:06:31 PM +08:00

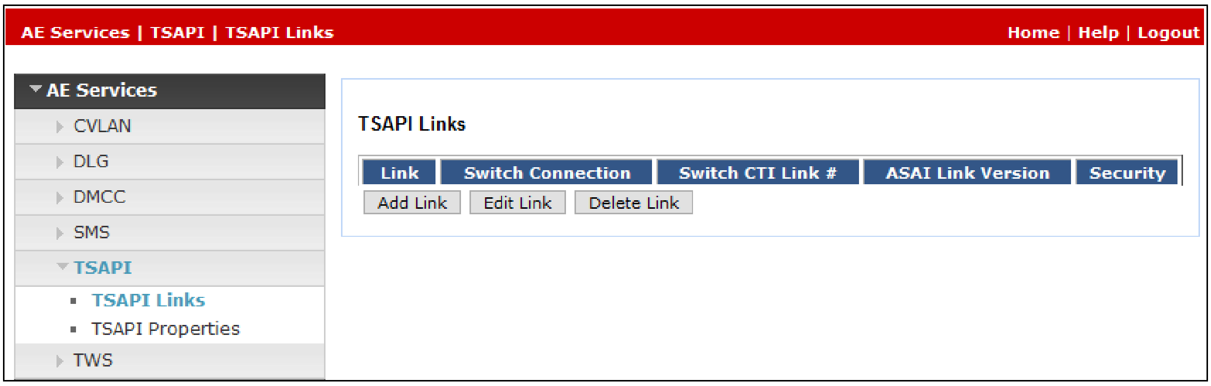
License File Host IDs: V6-BB-8E-6F-89-B6-01

Licensed Features

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	2500
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
AES HA LARGE VALUE_AES_HA_LARGE	permanent	10
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	2500
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	1
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	10
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
DLG VALUE_AES_DLG	permanent	1
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	2500

6.3. Administer TSAPI Link

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

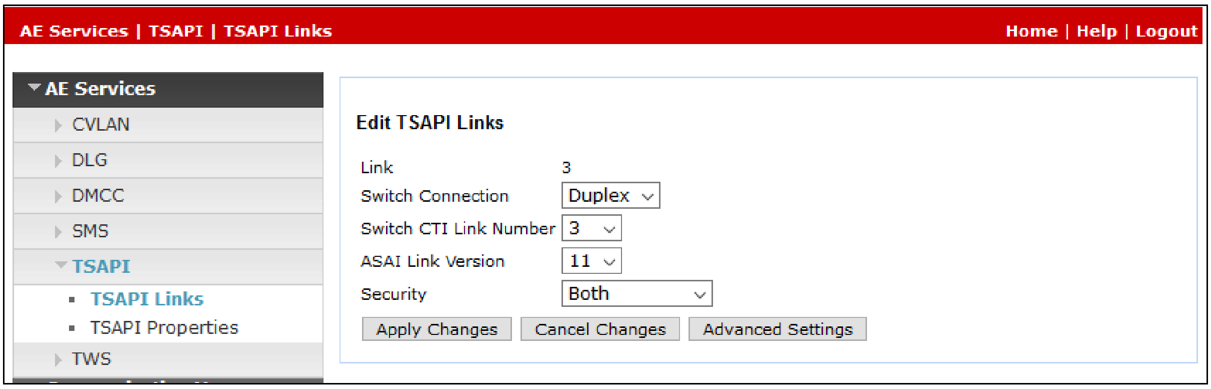


In the **Add TSAPI Links** screen (not shown), select the following values:

- **Link** Select an available Link number from 1 to 16.
- **Switch Connection** Select appropriate switch connection.
- **Switch CTI Link Number** Corresponding CTI link number in **Section 5.2**.
- **ASAI Link Version** Set to the latest version.
- **Security** Select **Both** to allow for encrypted or unencrypted link.

Click **Apply Changes**.

The screenshots below show the settings after changes applied.

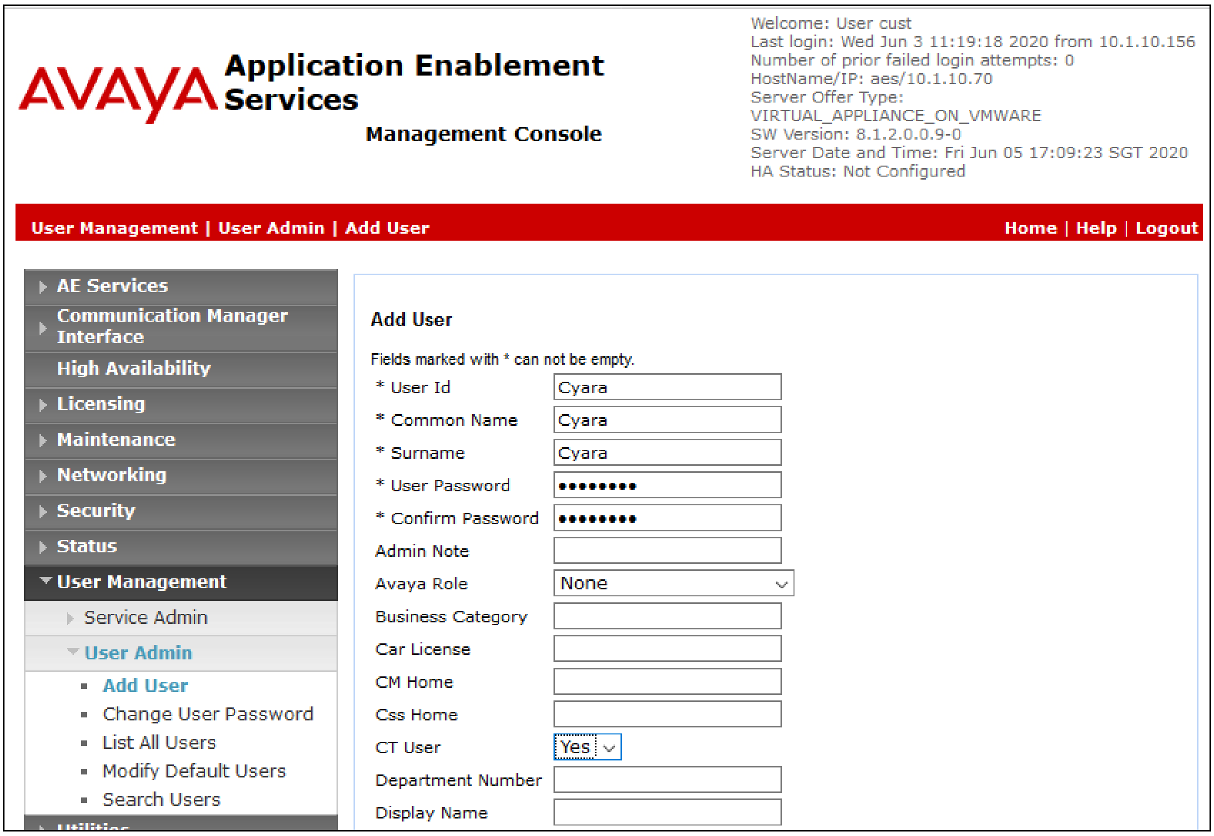


Edit TSAPI Links

Link	3
Switch Connection	Duplex
Switch CTI Link Number	3
ASAI Link Version	11
Security	Both

6.4. Administer Cyara User

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 in **Section 7** to access the TSAPI Service on AES. Scroll down to the bottom of the page and click **Apply** (not shown).



Welcome: User cust
Last login: Wed Jun 3 11:19:18 2020 from 10.1.10.156
Number of prior failed login attempts: 0
HostName/IP: aes/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.0.0.9-0
Server Date and Time: Fri Jun 05 17:09:23 SGT 2020
HA Status: Not Configured

Add User

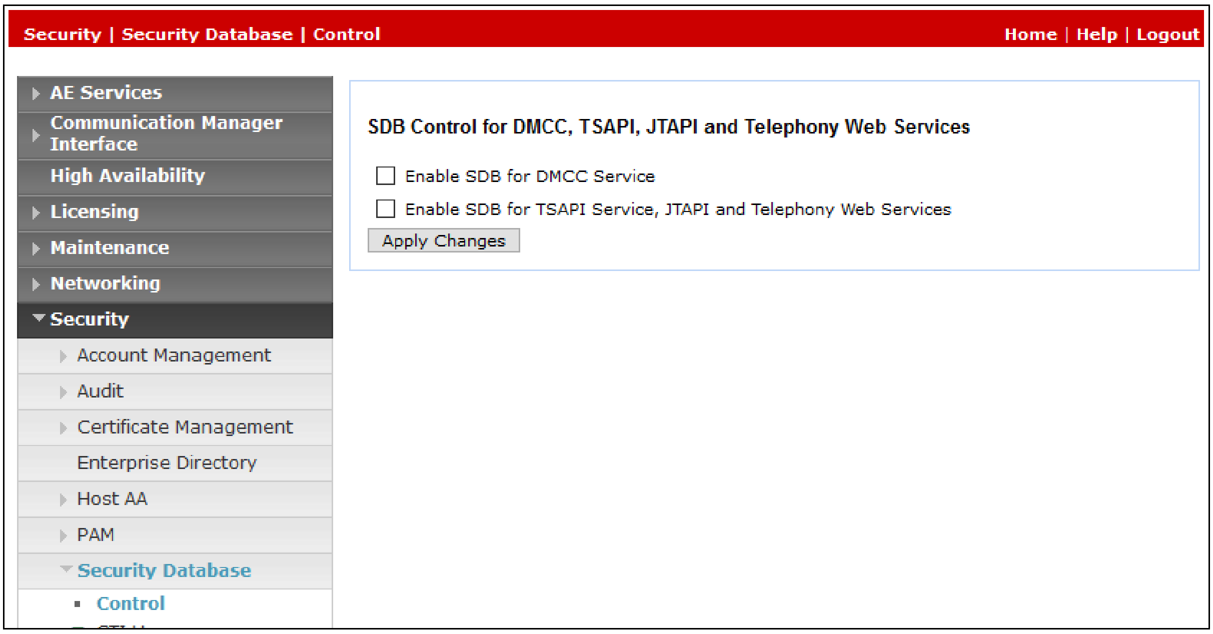
Fields marked with * can not be empty.

* 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
Department Number	
Display Name	

6.5. Verify Security Database

Select **Security → Security Database → Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Make certain both parameters are unchecked, as shown below.

In the event that the security database is used by the customer with parameters already enabled, then follow reference **[2]** to configure access privileges for the Cyara user from **Section 6.4**.



SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

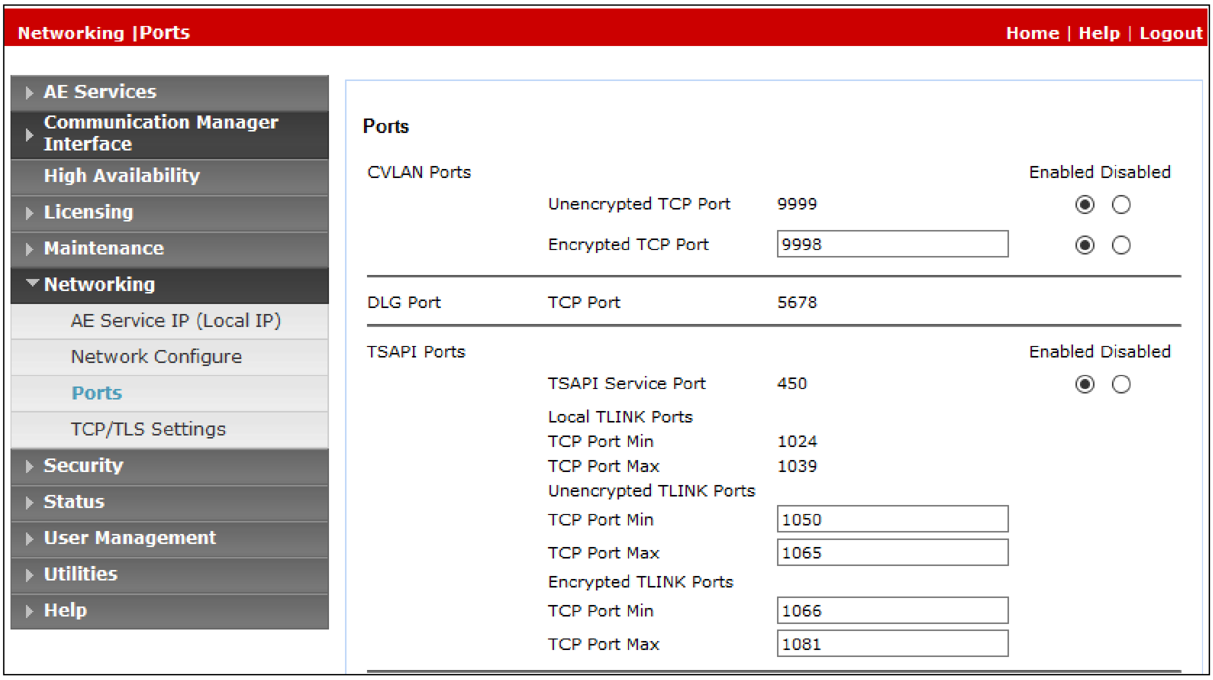
☐ Enable SDB for DMCC Service

☐ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

Apply Changes

6.6. Administer TSAPI Ports

Navigate to the networking ports by **Networking → Ports**. Verify that the default **TSAPI Service Port 450** is **Enabled**.

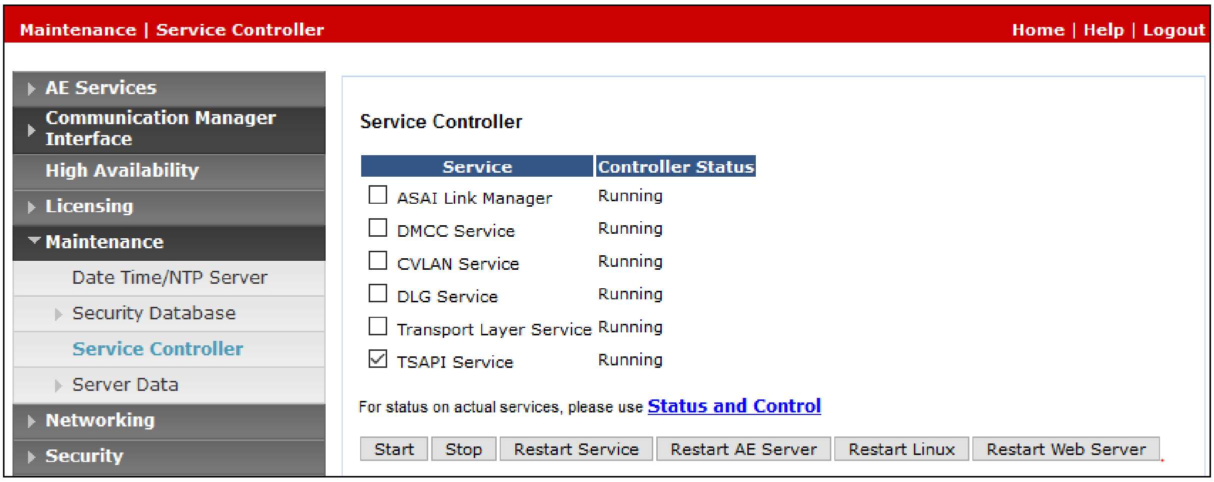


Ports

			Enabled	Disabled
CVLAN Ports				
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports				
	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		

6.7. Restart TSAPI Service

To restart the TSAPI service, select **Maintenance → Service Controller** from the Home menu. Check the **TSAPI Service** checkbox and click **Restart Service**.



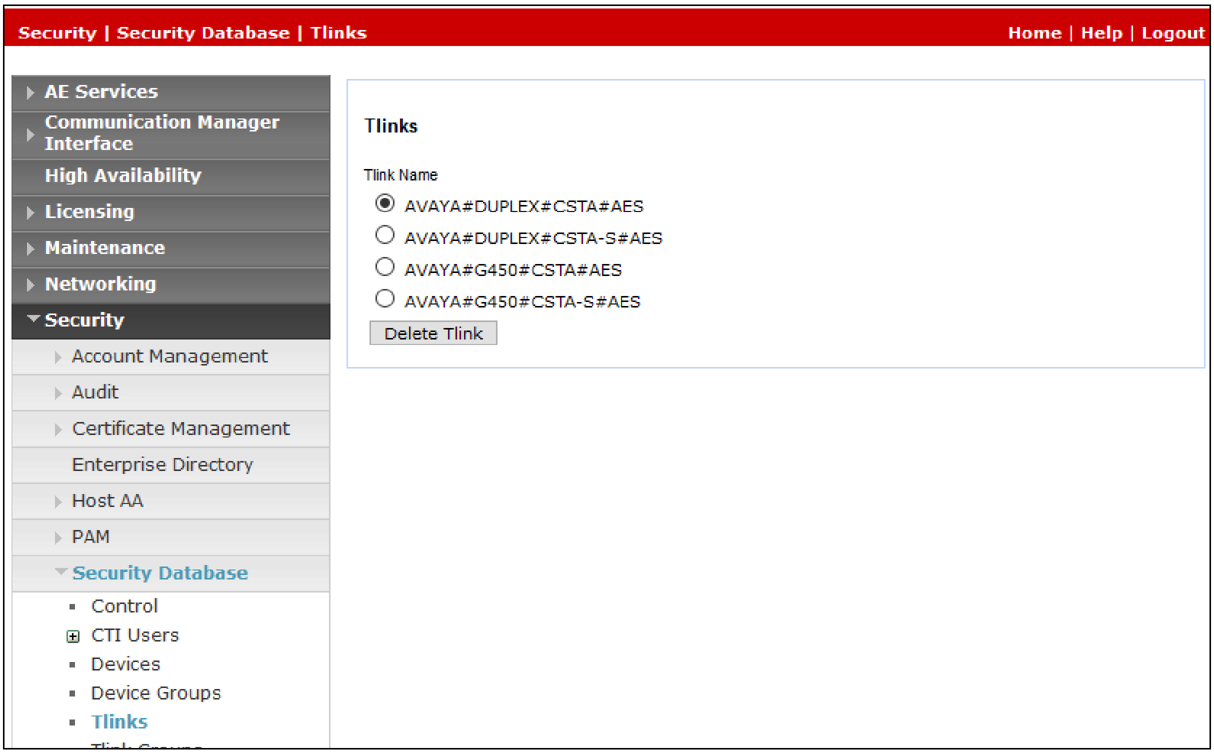
Service Controller

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**

6.8. Obtain Tlink Name

Navigate to the **Tlinks** screen by selecting **Security → Security Database → Tlinks** from the left pane. Note the string of the **Tlink Name**, as this will be needed to configure the Cyara Platform in **Section 7**. In this configuration, the unencrypted string is **AVAYA#DUPLEX#CSTA#AES,** which is automatically assigned by the AES server, is used.



Tlinks

Tlink Name

● AVAYA#DUPLEX#CSTA#AES
○ AVAYA#DUPLEX#CSTA-S#AES
○ AVAYA#G450#CSTA#AES
○ AVAYA#G450#CSTA-S#AES

Delete Tlink

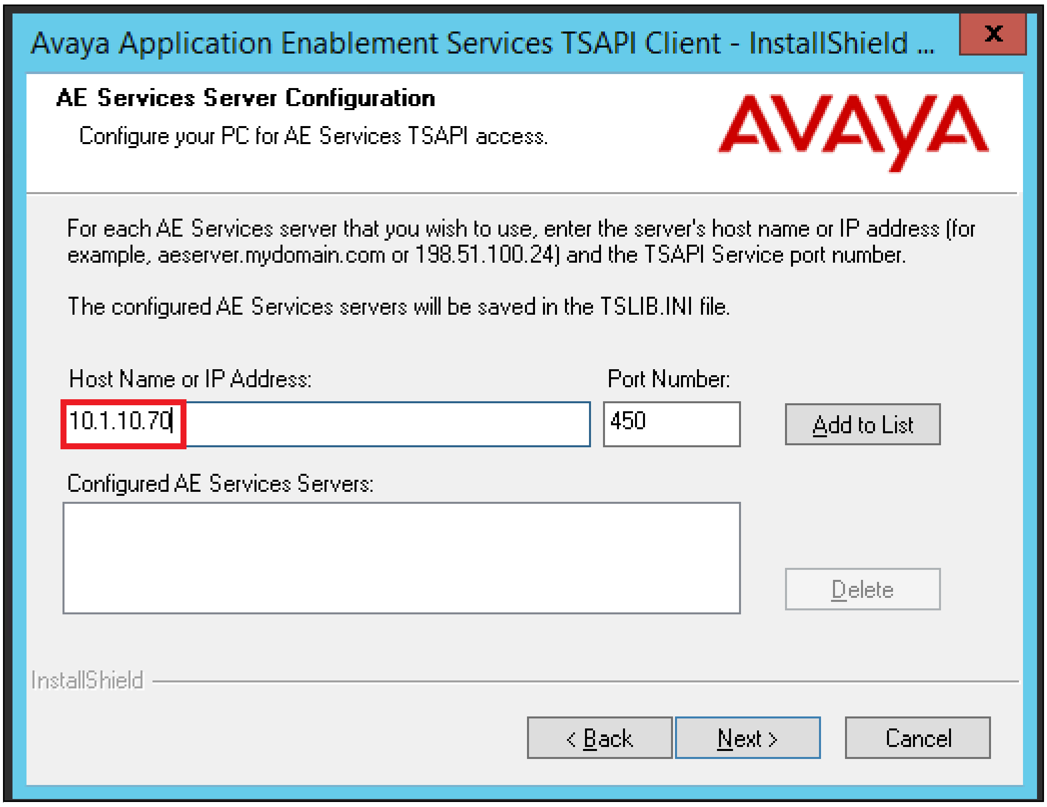
7. Configure Cyara Platform

An on-premises solution is setup for testing. Setup of the Cyara Platform server and Cyara Endpoint Server on Microsoft® Windows 2016 will be done by Cyara engineers and will not be detailed here. Refer to Cyara Deployment Guide reference [5] for details. This section highlights the configuration of Cyara Platform server that interface with AES and it includes the following areas:

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

7.1. Setup TSAPI Client

The TSAPI client is installed with the Avaya AES ip address and Port Number in 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.

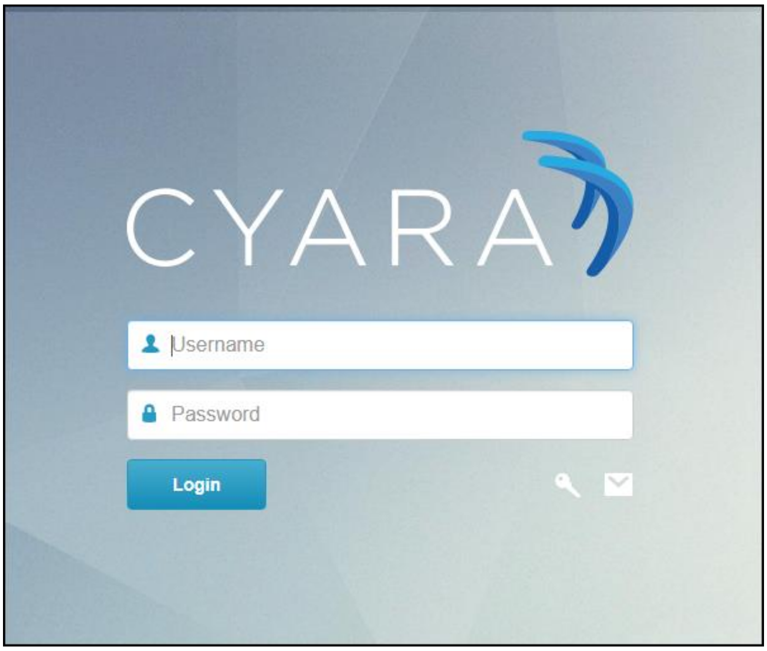
Host Name or IP Address: 10.1.10.70

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**.



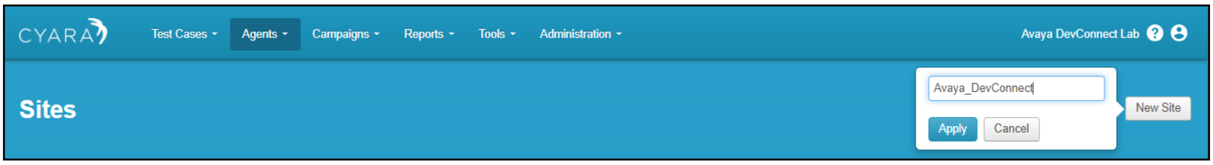
In this compliance testing, **Virtual Agent** and **Outbound** under **Plan Type** are required (not shown). With **Virtual Agent** plan, users can create agent details, define behaviors and assign them to agents, run simulations for teams of agents or entire contact center, and access reports on the outcome of the simulations. **Outbound** plan is simply allowing the dialer to make calls to a simulated environment. The dialer is either using the Call Engine component of the Cyara Platform that makes calls to the Call Center or a separate Outbound dialer system but in our case, this is done manually for testing. If the subscription plans are not available, then contact the Cyara for a proper activation.

7.3. Configure Sites and Environment

The Cyara Platform server provides the test and monitoring platform where Cyara Portal users log into the platform to configure Test cases and campaigns. In this compliance test, the inbound ACD calls were placed manually. Administration, scripting, monitoring and reporting are done via the Cyara Web Portal.

7.3.1. Add Sites

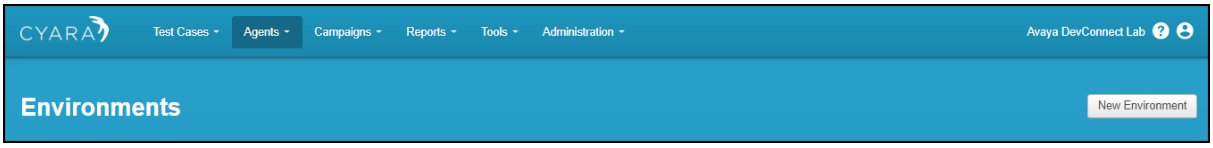
Select **Agents** Tab and from the dropdown menu, click **Sites** (not shown) → **New Site** on the right of the screen. Enter appropriate site name. In this case, **Avaya_DevConnect** is used.



Avaya_DevConnect

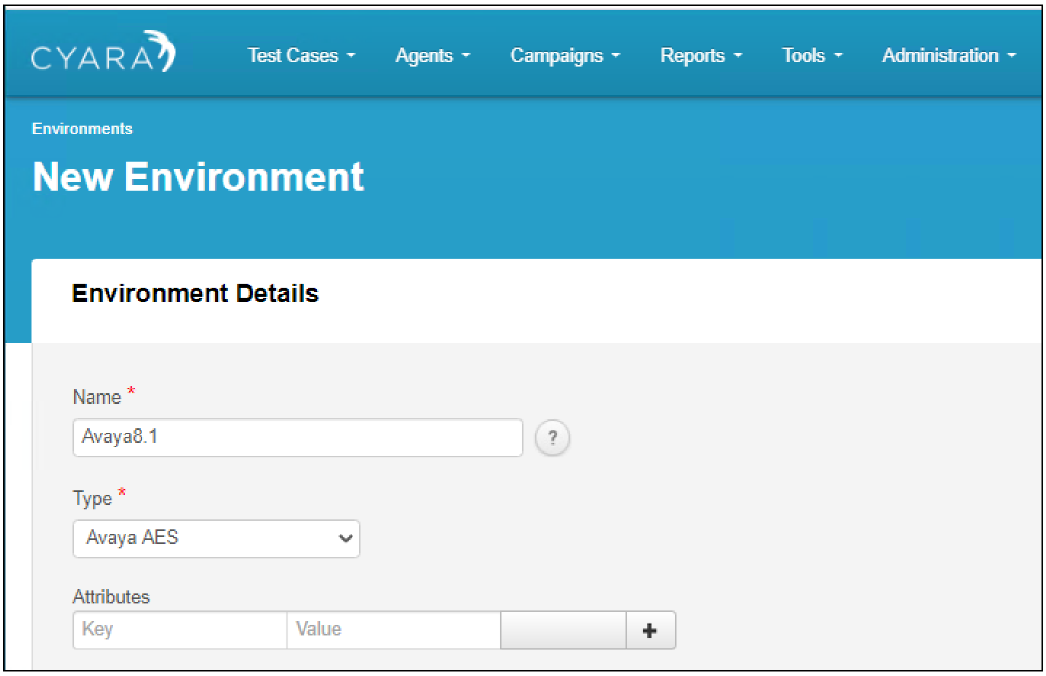
7.3.2. Create Environment

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.



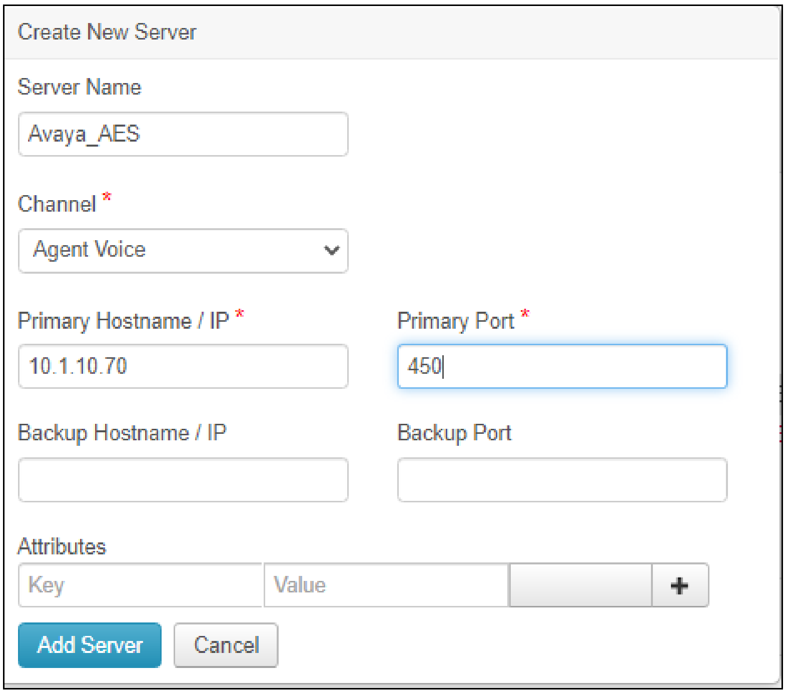
Name * Avaya8.1

Type * Avaya AES

Under header **Environment Servers** below (not shown), click **New Server**.

Enter the following details:

- **Server Name** Enter appropriate name as blanks are not allowed.
- **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 6.6**.



Create New Server

Server Name: Avaya_AES

Channel *: Agent Voice

Primary Hostname / IP *: 10.1.10.70

Primary Port *: 450

Backup Hostname / IP:

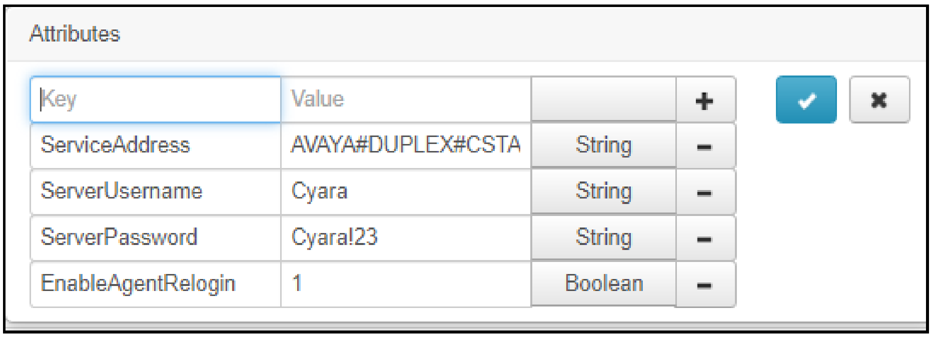
Backup Port:

Attributes

Under **Attributes** in **Create New Server** page, input the following values:

- **ServiceAddress** Enter the Tlink Name as in **Section 6.8**.
- **ServiceUserName** Enter user name created in **Section 6.4**.
- **ServicePassword** Enter user password created in **Section 6.4**.
- **EnableAgentRelogin** Enter “1” to enable**.**

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



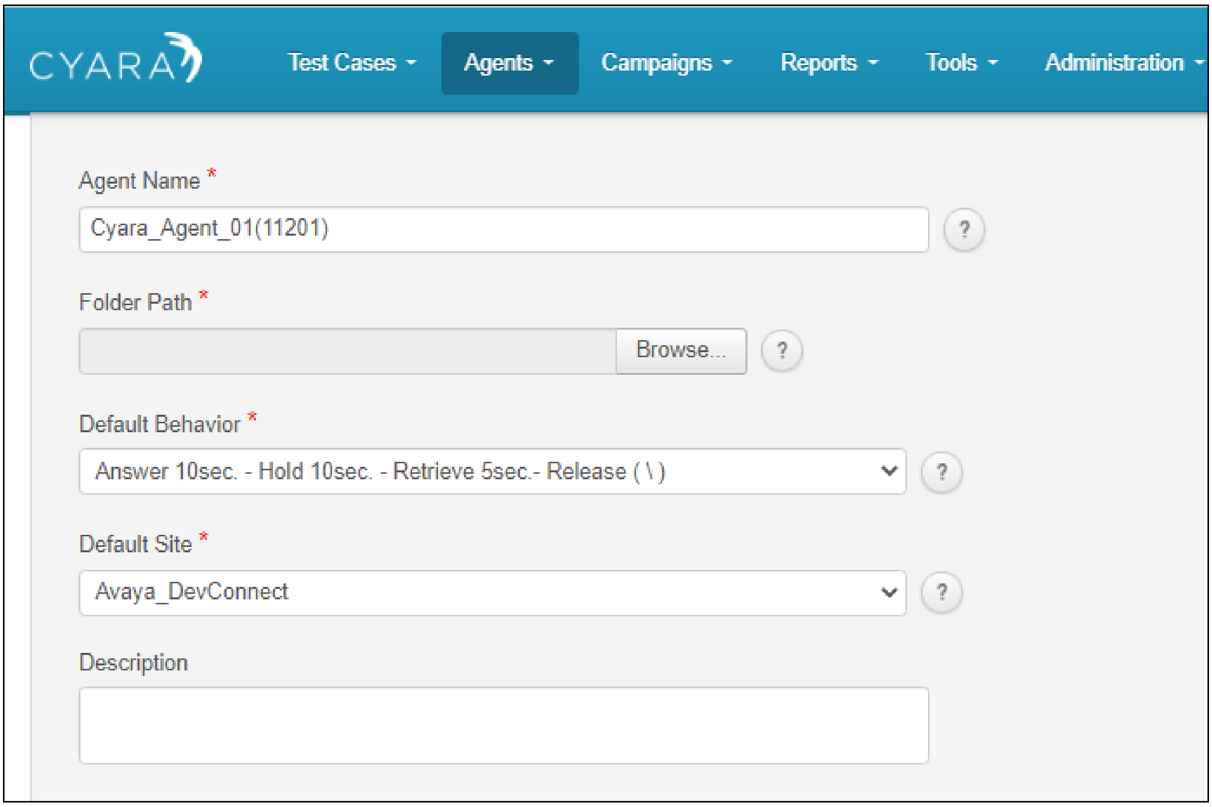
Attributes

Key	Value		
ServiceAddress	AVAYA#DUPLEX#CSTA	String	−
ServerUsername	Cyara	String	−
ServerPassword	Cyara!23	String	−
EnableAgentRelogin	1	Boolean	−

7.4. Configure 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.
- **Default Behavior** Select from a pre-created list of behaviors to be tested.
- **Default Site** Select site created in **Section 7.3.1**.



Agent Name * Cyara_Agent_01(11201)

Folder Path *

Default Behavior * Answer 10sec. - Hold 10sec. - Retrieve 5sec.- Release (\ )

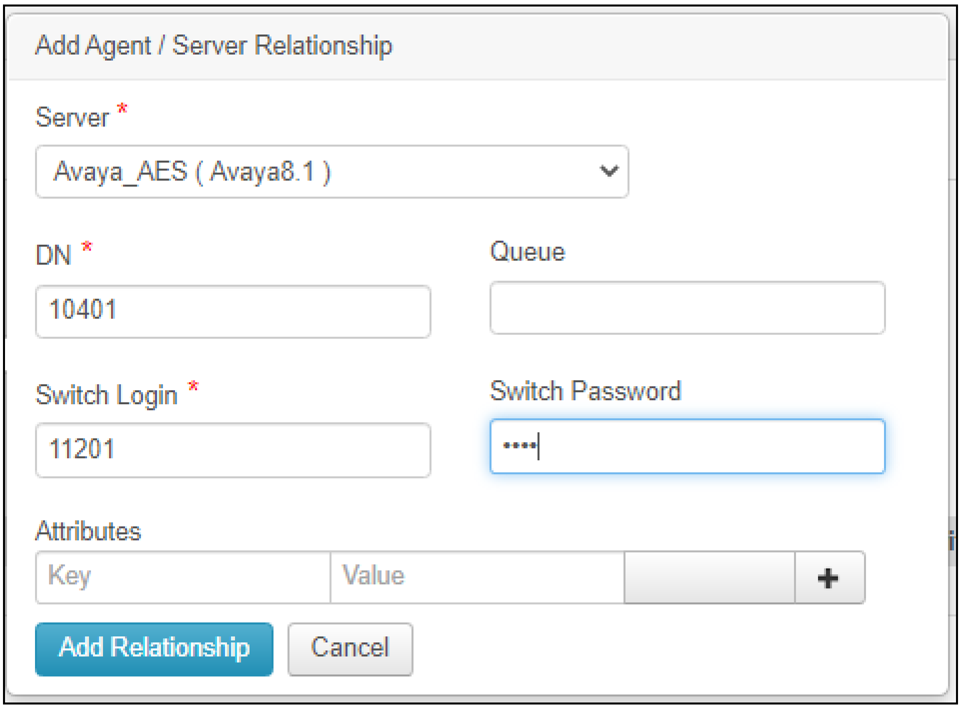
Default Site * Avaya_DevConnect

Description

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 first Virtual Endpoint extension. This is assumed to be created which is detailed in another Application Notes reference **[4]**.
- **Switch Login** Enter first agent loginID created in **Section 5.3**.
- **Switch Password** Enter first agent password created in **Section 5.3**.

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 logins 11201 to 11210 were created.



Add Agent / Server Relationship

Server * Avaya_AES (Avaya8.1)

DN * 10401

Queue

Switch Login * 11201

Switch Password ••••

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 from Cyara engineers.

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, AES and Cyara Platform Virtual Agent.

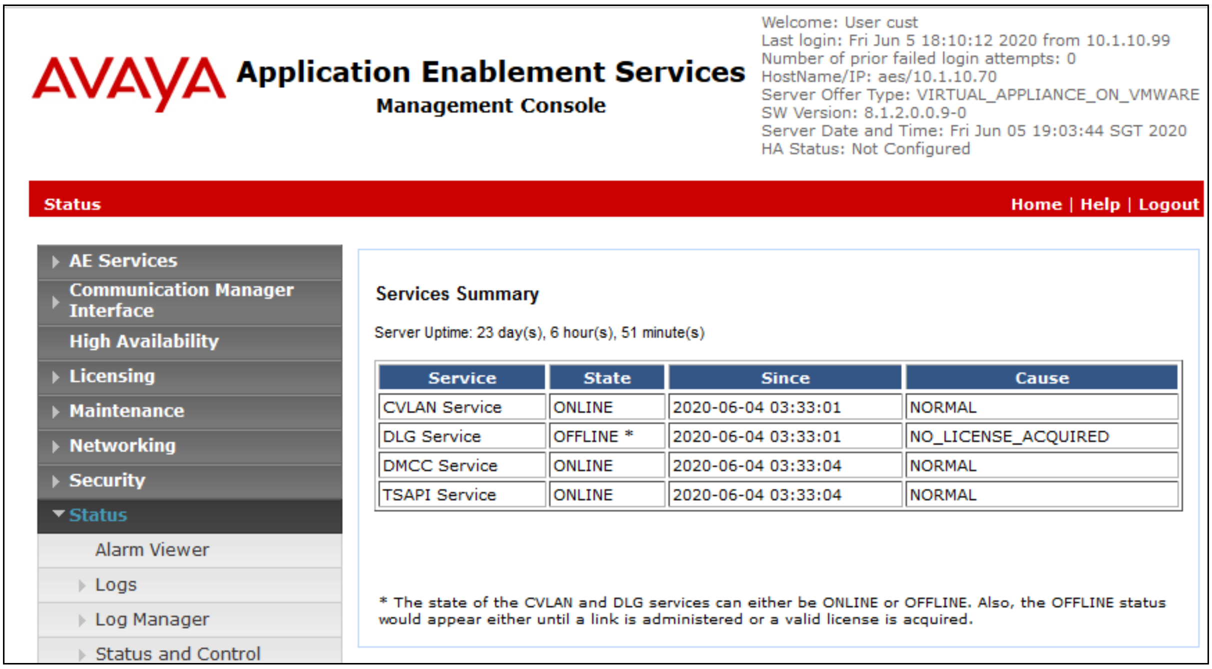
8.1. Verify Avaya Aura® Communication Manager

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
Link           Busy  Server           State         Sent     Rcvd

3     11       no    aes              established   15       15
```

8.2. Verify Avaya Aura® Application Enablement Services

From the Welcome to OAM web pages (not shown), verify the status of the TSAPI service by selecting **Status**. The **State** field for the **TSAPI Service** should display **ONLINE**.



Welcome: User cust
Last login: Fri Jun 5 18:10:12 2020 from 10.1.10.99
Number of prior failed login attempts: 0
HostName/IP: aes/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.0.0.9-0
Server Date and Time: Fri Jun 05 19:03:44 SGT 2020
HA Status: Not Configured

Services Summary

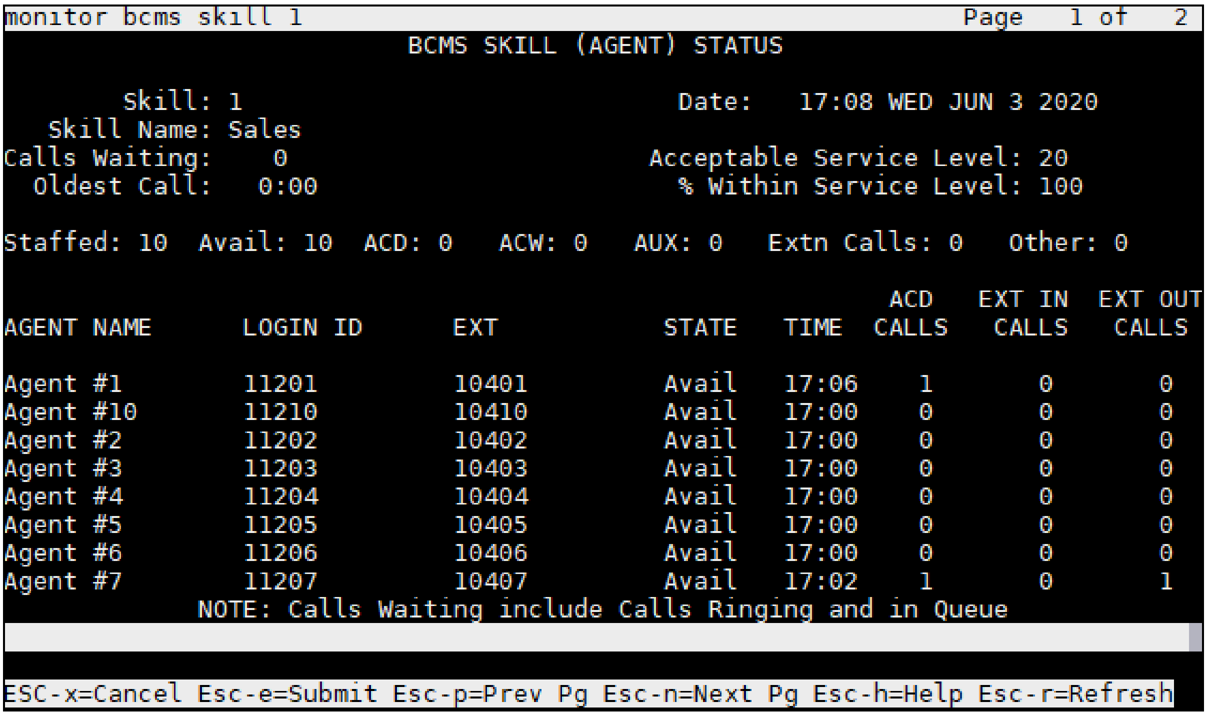
Server Uptime: 23 day(s), 6 hour(s), 51 minute(s)

Service	State	Since	Cause
CVLAN Service	ONLINE	2020-06-04 03:33:01	NORMAL
DLG Service	OFFLINE *	2020-06-04 03:33:01	NO_LICENSE_ACQUIRED
DMCC Service	ONLINE	2020-06-04 03:33:04	NORMAL
TSAPI Service	ONLINE	2020-06-04 03:33:04	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

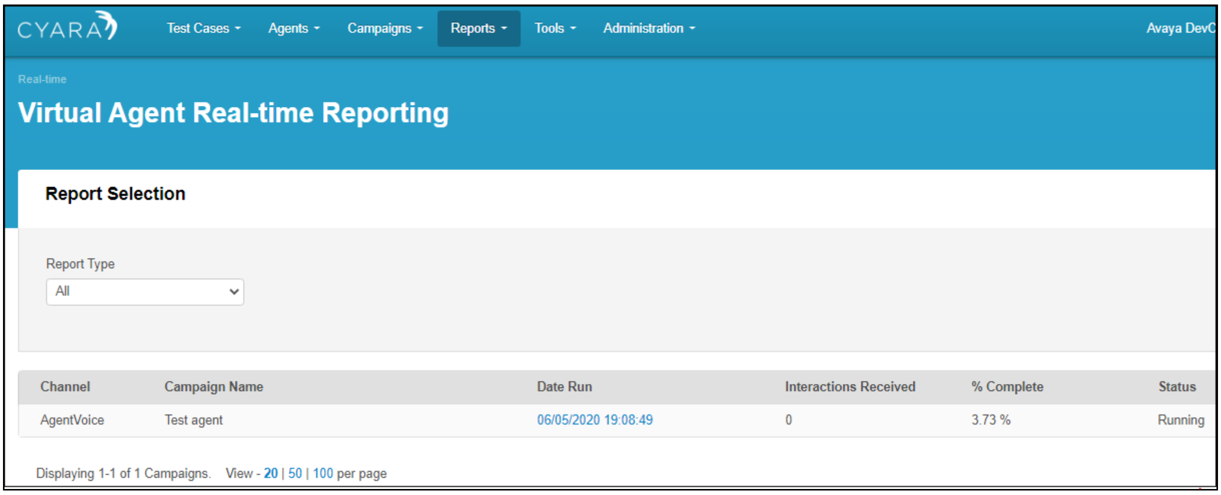
From Communication Manager SAT login, the **monitor bcms** command can be used to verify the agent current state under **STATE** when calls are made, and agent campaigns are run.



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

        Skill: 1                                  Date:   17:08 WED JUN 3 2020
   Skill Name: Sales
Calls Waiting:    0                             Acceptable Service Level: 20
  Oldest Call:   0:00                             % Within Service Level: 100

Staffed: 10  Avail: 10  ACD: 0   ACW: 0   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   17:06    1       0       0
Agent #10       11210         10410         Avail   17:00    0       0       0
Agent #2        11202         10402         Avail   17:00    0       0       0
Agent #3        11203         10403         Avail   17:00    0       0       0
Agent #4        11204         10404         Avail   17:00    0       0       0
Agent #5        11205         10405         Avail   17:00    0       0       0
Agent #6        11206         10406         Avail   17:00    0       0       0
Agent #7        11207         10407         Avail   17:02    1       0       1
             NOTE: Calls Waiting include Calls Ringing and in Queue


ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh
```

8.4. Verify Cyara Virtual Agents

When campaigns are running for the Virtual Agent to be active 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 **Test Agent**.



Virtual Agent Real-time Reporting

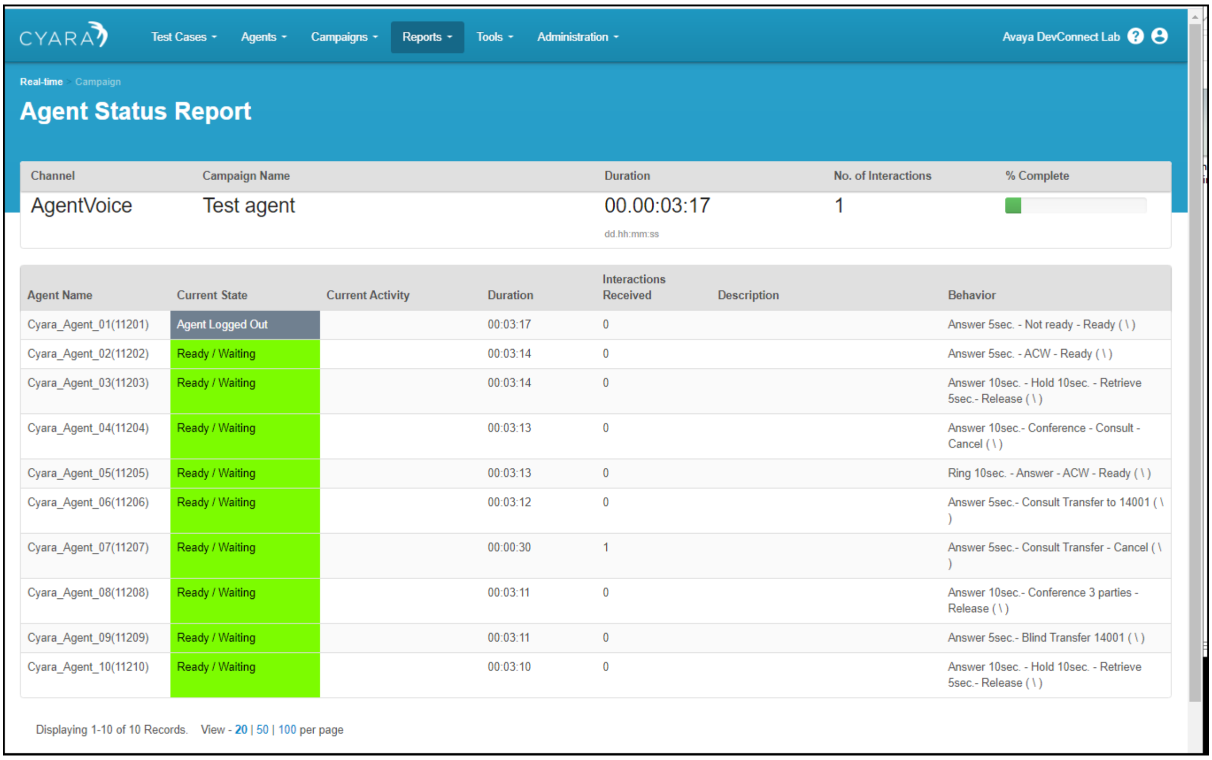
Report Selection

Report Type: All

Channel	Campaign Name	Date Run	Interactions Received	% Complete	Status
AgentVoice	Test agent	06/05/2020 19:08:49	0	3.73 %	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 under **Behavior** column. Manually make inbound calls to the VDN. From here, agents' activities can be monitored to verify correct behavior.



Agent Status Report

Channel	Campaign Name	Duration	No. of Interactions	% Complete
AgentVoice	Test agent	00.00:03:17 dd.hh:mm:ss	1	🟩

Agent Name	Current State	Current Activity	Duration	Interactions Received	Description	Behavior
Cyara_Agent_01(11201)	Agent Logged Out		00:03:17	0		Answer 5sec. - Not ready - Ready (\ )
Cyara_Agent_02(11202)	Ready / Waiting		00:03:14	0		Answer 5sec. - ACW - Ready (\ )
Cyara_Agent_03(11203)	Ready / Waiting		00:03:14	0		Answer 10sec. - Hold 10sec. - Retrieve 5sec.- Release (\ )
Cyara_Agent_04(11204)	Ready / Waiting		00:03:13	0		Answer 10sec.- Conference - Consult - Cancel (\ )
Cyara_Agent_05(11205)	Ready / Waiting		00:03:13	0		Ring 10sec. - Answer - ACW - Ready (\ )
Cyara_Agent_06(11206)	Ready / Waiting		00:03:12	0		Answer 5sec.- Consult Transfer to 14001 (\ )
Cyara_Agent_07(11207)	Ready / Waiting		00:00:30	1		Answer 5sec.- Consult Transfer - Cancel (\ )
Cyara_Agent_08(11208)	Ready / Waiting		00:03:11	0		Answer 10sec.- Conference 3 parties - Release (\ )
Cyara_Agent_09(11209)	Ready / Waiting		00:03:11	0		Answer 5sec.- Blind Transfer 14001 (\ )
Cyara_Agent_10(11210)	Ready / Waiting		00:03:10	0		Answer 10sec. - Hold 10sec. - Retrieve 5sec.- Release (\ )

Displaying 1-10 of 10 Records. View - 20 | 50 | 100 per page

9. Conclusion

These Application Notes describe the configuration steps required for Cyara Platform Virtual Agent 20.1 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 using 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 8.1.x, Issue 3, Mar 2020.
[2] *Administering Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 5, Apr 2020.
[3] *Avaya Aura® Avaya Communication Manager Feature Description and Implementation,* Release 8.1.x, Issue 8, May 2020.
[4] *Application Notes for Cyara Platform with Avaya Aura® Communication Manager using H.323 Endpoints Emulation*.

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.*
[7] *Cyara Platform 20.1.0 Release 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.