



## Avaya Solution & Interoperability Test Lab

# **Application Notes for Configuring Pronet Dynamic IVR R1 with Avaya Experience Portal R8.0, Avaya Aura® Communication Manager R8.1 and Avaya Aura® Application Enablement Services R8.1 using AES Connector - Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps for Pronet Dynamic IVR R1 to interoperate with Avaya Experience Portal R8.0, Avaya Aura® Communication Manager R8.1 and Avaya Aura® Application Enablement Services R8.1 using AES Connector. Pronet Dynamic IVR utilizes Avaya AES Connector to connect with the Telephony Server Application Programming Interface on Avaya Aura® Application Enablement Services to monitor and control IVR ports on Avaya Aura® Communication Manager.

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 describe the configuration steps for Pronet Dynamic IVR R1 to interoperate with Avaya Experience Portal R8.0, Avaya Aura® Communication Manager R8.1 and Avaya Aura® Application Enablement Services R8.1 using AES Connector. The IVR ports are H.323 virtual endpoints used by Avaya Experience Portal for incoming calls from Avaya Aura® Communication Manager. The application utilizes the Telephony Server Application Programming (TSAPI) Link on Avaya Aura® Application Enablement Services (AES) to monitor and control these IVR ports on Avaya Aura® Communication Manager. Note that the AES Connector only works with H.323 connection.

The scope of testing excluded the middleware and any CRM (Customer Relationship Management) applications on client side for self-service transaction. Pronet applications were developed using Avaya Aura® Orchestration Designer (AAOD) and run on Avaya Experience Portal. The applications point to the Pronet Application Server running in Tomcat on Windows Server 2016 and utilizes the Avaya AES Connector to establish contact and pass values with Avaya Aura® Application Enablement Services. AES Connector is an Avaya developed connector used in AAOD applications which is developed by Pronet to interface with AES.

## 2. General Test Approach and Test Results

The general test approach was to configure the Pronet Dynamic IVR to communicate with Communication Manager via Application Enablement Services (AES). See **Figure 1** for network diagram. The interoperability compliance test included both feature functionality and serviceability tests.

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 Pronet Dynamic IVR did not include use of any specific encryption features as requested by Pronet.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing. The scope of testing includes the feature functionality testing below:

- Monitoring of calls.
- Transfer of calls.
- Codec that includes G.711 and G.729.
- Announcement provided on the applications.

The serviceability testing focused on verifying the ability of Pronet Dynamic IVR to recover from LAN disconnection and reconnection and also between application server and Avaya solutions.

## 2.2. Test Results

All functionality and serviceability test cases were completed successfully.

## 2.3. Support

Technical support on Pronet Dynamic IVR can be obtained through the following:

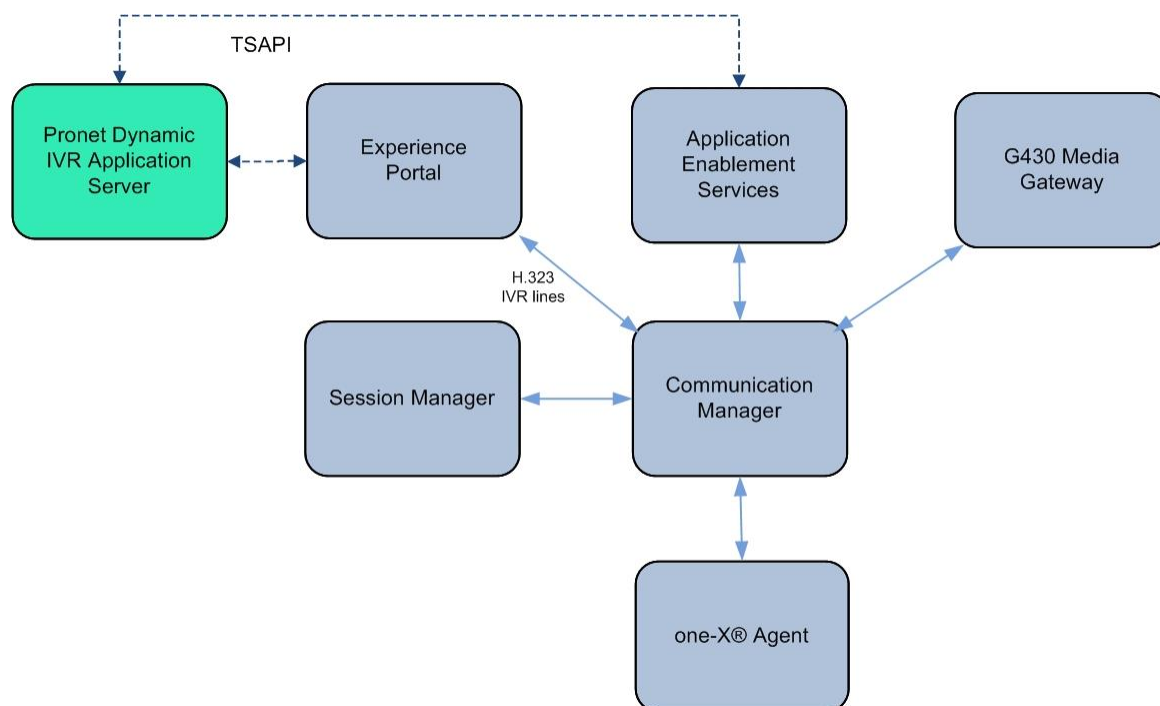
**Phone:** +92 (21) 582 2401-4

**Email:** [info@pronet-tech.net](mailto:info@pronet-tech.net)

**Web :** <https://pronet-tech.net>

### 3. Reference Configuration

The configuration shown in **Figure 1** was used during the compliance test of Pronet Dynamic IVR with Experience Portal, Communication Manager and Application Enablement Services. Pronet Dynamic IVR utilizes AES TSAPI Link to monitor and control IVR ports on Communication Manager. In this configuration, Avaya one-X® Agent is used as Elite agent for compliance testing.



**Figure 1: Compliance Testing Configurations**

## 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 running on Virtual Server           | 8.1.3<br>(8.1.3.2.0.890.26989) |
| Avaya Aura® Application Enablement Services running on Virtual Server | 8.1.3<br>(8.1.3.2.0.4-0)       |
| Avaya G430 Media Gateway  | N/A                            |
| Avaya Experience Portal   | 8.0<br>(8.0.0.0.1483)          |
| Avaya one-X® Agent (H.323)  | 2.5.60624.0                    |
| Pronet Application Server running on Windows Server 2016              | R1<br>Standard                 |
| Apache Tomcat   | 8.5                            |
| AES Connector   | 8.1.0.0.0.9                    |
| Database Server   | SQL 2012                       |

## 5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration of vdn, vectors, routing, skill hunt groups etc., are not the focus of these Application Notes and will not be described.

The configuration operations described in this section can be summarized as follows:

- Verify system parameters customer options
- Configure virtual stations for the IVR ports
- Configure interface to AES

### 5.1. Verify System Parameters Customer Options

Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 4**, ensure that **Computer Telephony Adjunct Links** is set to **y** as shown below.

```
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
```

(NOTE: You must logoff & login to effect the permission changes.)

## 5.2. Configure Virtual Stations for the IVR ports

Use the **add station** command to configure a station for each of the virtual stations to be used for the IVR ports. Enter station **Type** as **7434D** and **Port** as **IP**. Enter a descriptive **Name** and **Security Code** for each one. Set **IP Softphone** to **y**. Repeat these steps for all the virtual stations to be used. Below is the configured sample station 250. In this compliance testing, 2 ports are created i.e., 250 and 251.

|                           |  |             |
|---------------------------|--|-------------|
| add station 250           |  | Page 1 of 6 |
| STATION                   |  |             |
| Extension: 250            | Lock Messages? n                             | BCC: 0      |
| <b>Type: 7434D</b>        | <b>Security Code: ****</b>                   | TN: 1       |
| <b>Port: IP</b>           | Coverage Path 1:                             | COR: 1      |
| <b>Name: IVR Port 1</b>   | Coverage Path 2:                             | COS: 1      |
| Unicode Name? n           | Hunt-to Station:                             |             |
| STATION OPTIONS           |  |             |
| Time of Day Lock Table:   |  |             |
| Loss Group: 2             | Personalized Ringing Pattern: 1              |             |
| Data Module? n            | Message Lamp Ext: 2200                       |             |
| Display Module? y         |  |             |
| Display Language: english | Coverage Module? n                           |             |
| Survivable COR: internal  | Media Complex Ext:                           |             |
| Survivable Trunk Dest? y  | <b>IP SoftPhone? y</b>                       |             |
|                           | Remote Office Phone? n                       |             |
|                           | IP Video Softphone? n                        |             |
|                           | Short/Prefixed Registration Allowed: default |             |

### 5.3. Configure Interface to AES

In order for Communication Manager to establish a connection to Application Enablement Services, administer the CTI Link as shown below. Add an available cti-link number which in this case is **1**. Specify an available **Extension** number, set the **Type** as **ADJ-IP**, which denotes that this is a link to an IP connected adjunct, and name the link for easy identification.

|                        |             |
|------------------------|-------------|
| <b>add cti-link 1</b>  | Page 1 of 3 |
| CTI LINK               |             |
| CTI Link: <b>1</b>     |             |
| Extension: <b>2000</b> |             |
| Type: <b>ADJ-IP</b>    |             |
|                        | COR: 1      |
| Name: <b>aes8</b>      |             |
| Unicode Name? n        |             |



## 6. Configure Avaya Aura® Application Enablement Services

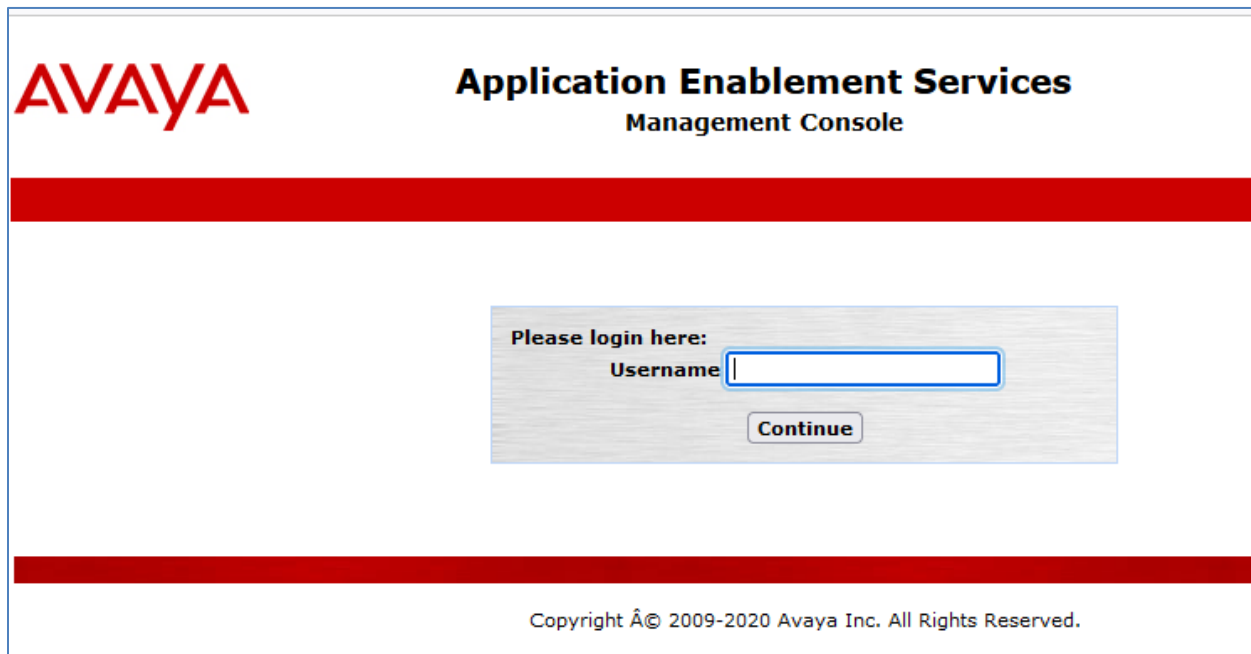
This section provides the procedures for configuring Application Enablement Services. For other provisioning information such as initial installation and configuration of switch connections and the TSAPI link etc., are not the focus of these Application Notes and will not be described. In any case, the switch connections will need to be verified.

The configuration operations described in this section can be summarized as follows:

- Launch OAM interface
- Verify License
- Create CTI User
- Administer Security Database
- Add Devices
- Restart Services
- Check TSAPI status and Tlink name

### 6.1. Launch OAM interface

To access the AES Management Console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the IP address of AES. At the login screen displayed, log in with the appropriate credentials and then select the **Login** button.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo in red. To its right, the text "Application Enablement Services" is displayed in bold black, with "Management Console" below it in a smaller font. A thick red horizontal bar spans the width of the page below the header. In the center, there is a light gray rectangular box containing the text "Please login here:" followed by "Username" and a text input field. Below the input field is a "Continue" button. Another thick red horizontal bar is located at the bottom of the page, above the footer text "Copyright © 2009-2020 Avaya Inc. All Rights Reserved."

The **Welcome to OAM** screen is displayed next.

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message with user information: "Welcome: User cust", "Last login: Wed Sep 29 13:35:57 2021 from 192.168.0.97", "Number of prior failed login attempts: 0", "HostName/IP: aes8/192.168.10.21", "Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE", "SW Version: 8.1.3.2.0.4-0", "Server Date and Time: Wed Sep 29 13:39:02 PKT 2021", and "HA Status: Not Configured". The left sidebar contains a navigation menu with options: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled "Welcome to OAM" and contains a paragraph: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:" followed by a bulleted list of domains and their functions. The list includes: AE Services (manage all AE Services), Communication Manager Interface (manage switch connection and dialplan), High Availability (manage AE Services HA), Licensing (manage the license server), Maintenance (manage routine maintenance tasks), Networking (manage network interfaces and ports), Security (manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM), Status (obtain server status information), User Management (manage AE Services users and AE Services user-related resources), Utilities (carry out basic connectivity tests), and Help (obtain a few tips for using the OAM Help system). A final paragraph states: "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

Select **Licensing** → **WebLM Server Access** in the left pane, to display the applicable WebLM server log in screen (not shown). Log in using the appropriate credentials and navigate to display installed licenses (not shown).

The screenshot shows the Avaya Application Enablement Services Management Console Licensing page. The top header includes the title "Licensing" and navigation links: "Home | Help | Logout". The left sidebar contains a navigation menu with options: AE Services, Communication Manager Interface, High Availability, Licensing, WebLM Server Address, WebLM Server Access, Reserved Licenses, Maintenance, Networking, Security, and Status. The main content area is titled "Licensing" and contains three paragraphs of instructions. The first paragraph states: "If you are setting up and maintaining the WebLM, you need to use the following:" followed by a bulleted list: "WebLM Server Address". The second paragraph states: "If you are importing, setting up and maintaining the license, you need to use the following:" followed by a bulleted list: "WebLM Server Access". The third paragraph states: "If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:" followed by a bulleted list: "Reserved Licenses". A red note at the bottom states: "NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page".

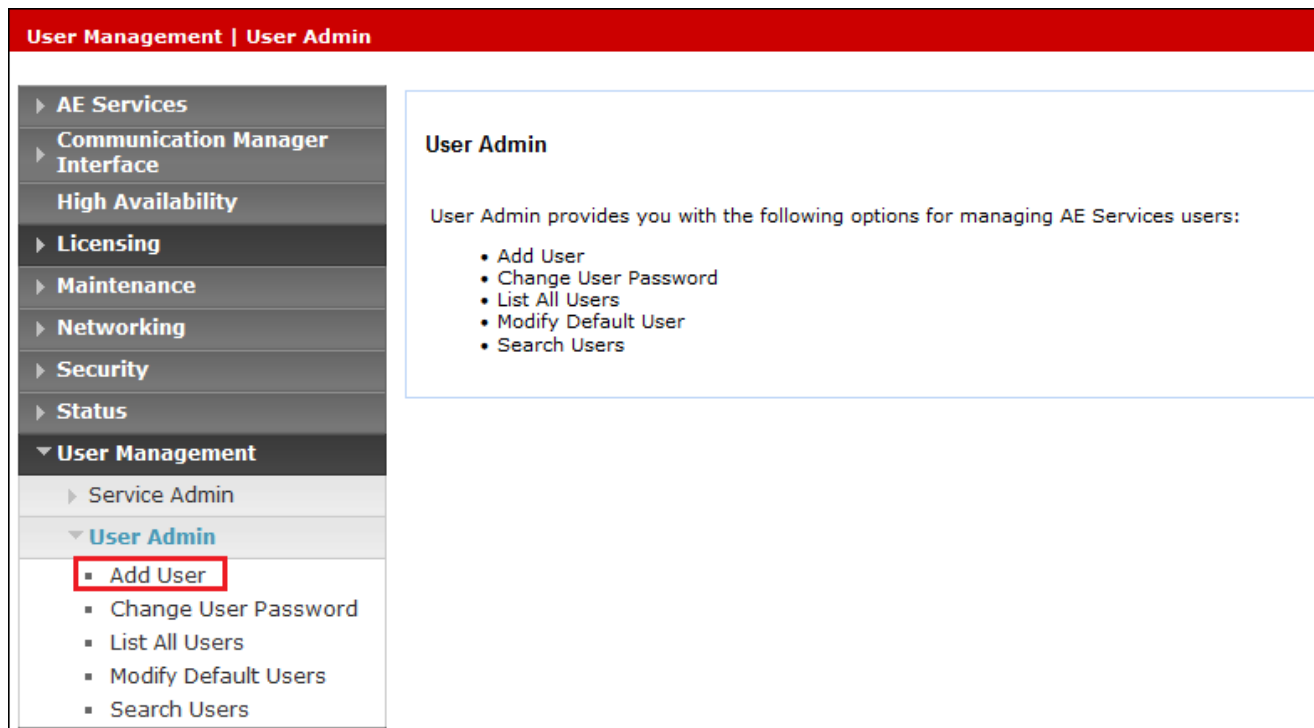
Select **Licensed products** → **APPL\_ENAB** → **Application\_Enablement** in the left pane (not shown), to display the **Licensed Features** screen in the right pane.

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.

| Feature<br>(License Keyword)   | License Capacity   | Currently<br>available |                |
|--|--|------------------------|----------------|
| Unified CC API Desktop Edition<br>(VALUE_AES_AEC_UNIFIED_CC_DESKTOP) | 10   | 10                     |                |
| Device Media and Call Control<br>(VALUE_AES_DMCC_DMC)                | 10   | 10                     |                |
| TSAPI Simultaneous Users<br>(VALUE_AES_TSAPI_USERS)                  | 10   | 8                      |                |
| Product Notes<br>(VALUE_NOTES)                                       | SmallServerTypes:<br>s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer<br>MediumServerTypes:<br>ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer<br>LargeServerTypes:<br>isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer<br>TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted,<br>DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted,<br>DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted,<br>DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted,<br>DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted,<br>DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted,<br>DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted,<br>DMCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP,,<br>CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted;<br>CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted;<br>CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted;<br>AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted,<br>DMCUnrestricted; CCT_ELITE_CALL_CTRL_001, BasicUnrestricted,<br>AdvancedUnrestricted, DMCUnrestricted, AgentEvents; ANAV_001,<br>BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents;<br>UNIFIED_DESKTOP_001, BasicUnrestricted, AdvancedUnrestricted,<br>DMCUnrestricted, AgentEvents; AACC_001, BasicUnrestricted,<br>AdvancedUnrestricted, DMCUnrestricted; CE_AGENT_STATES_001,<br>BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents;<br>TP_CLIENT_001, BasicUnrestricted, , , AgentEvents; EXT_CLIENT_001, , , ,<br>AgentEvents; EXT_CLIENT_002, , , , AgentEvents; EXT_CLIENT_003, , , ,<br>AgentEvents; EXT_CLIENT_004, , , , AgentEvents; EXT_CLIENT_005, , , ,<br>AgentEvents; AAWFO_SELECT_001, BasicUnrestricted,<br>AdvancedUnrestricted, DMCUnrestricted, AgentEvents; OFFICELINX_001,<br>BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted,<br>AgentEvents;ACAL_001, BasicUnrestricted, , DMCUnrestricted,<br>AoentEvents; CRA_001. BasicUnrestricted. AdvancedUnrestricted. |                        | Not<br>counted |

### 6.3. Create CTI User

A User ID and password needs to be configured for the AES Connector on Pronet Dynamic IVR to communicate as a TSAPI client with the Application Enablement Services server. Navigate to the **User Management** → **User Admin** screen then choose the **Add User** option.



In the **Add User** screen shown below, enter the following values and click **Apply** (not shown) at the bottom of the page:

- **User Id** - This will be used by the application AES Connector to connect to AES.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will again be used by the AES Connector.
- **CT User** - Select **Yes** from the drop-down menu.

**User Management | User Admin | Add User**

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

▶ Help

### Add User

Fields marked with \* can not be empty.

|                    |  |
|--------------------|--|
| * User Id          | <input type="text" value="labuser"/>   |
| * Common Name      | <input type="text" value="labuser"/>   |
| * Surname          | <input type="text" value="labuser"/>   |
| * User Password    | <input type="password" value="•••••"/> |
| * Confirm Password | <input type="password" value="•••••"/> |
| Admin Note         | <input type="text"/>                   |
| Avaya Role         | <input type="text" value="None"/>      |
| Business Category  | <input type="text"/>                   |
| Car License        | <input type="text"/>                   |
| CM Home            | <input type="text"/>                   |
| Css Home           | <input type="text"/>                   |
| CT User            | <input type="text" value="Yes"/>       |
| Department Number  | <input type="text"/>                   |
| Display Name       | <input type="text"/>                   |
| Employee Number    | <input type="text"/>                   |
| Employee Type      | <input type="text"/>                   |
| Enterprise Handle  | <input type="text"/>                   |

Navigate to **Security** → **Security Database** → **CTI Users** → **List All Users** (not shown).  
From the list of **CTI Users**, select the **labuser** just created and click **Edit**. Tick on the **User Profile** as **Unrestricted Access**.

AA Status: Not Configured

Security | Security Database | CTI Users | List All Users

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▼ Security
  - ▶ Account Management
  - ▶ Audit
  - ▶ Certificate Management
  - ▶ Enterprise Directory
  - ▶ Host AA
  - ▶ PAM
  - ▼ Security Database
    - Control
    - ▣ CTI Users
      - List All Users
      - Search Users

### Edit CTI User

|               |  |
|---------------|--|
| User Profile: | User ID<br>labuser   |
|               | Common Name<br>labuser                                     |
|               | Worktop Name<br>NONE ▼                                     |
|               | Unrestricted Access<br><input checked="" type="checkbox"/> |

---

|                          |  |
|--------------------------|--|
| Call and Device Control: | Call Origination/Termination and Device Status<br>None ▼ |
|--------------------------|--|

---

|                             |   |
|-----------------------------|---|
| Call and Device Monitoring: | Device Monitoring<br>None ▼                 |
|                             | Calls On A Device Monitoring<br>None ▼      |
|                             | Call Monitoring<br><input type="checkbox"/> |

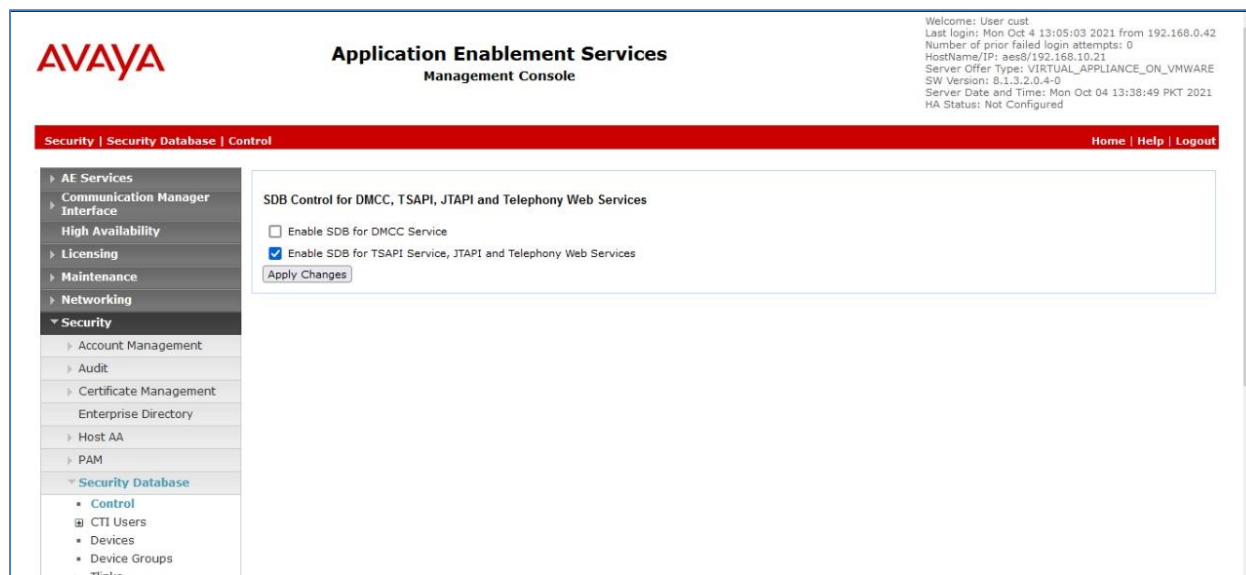
---

|                  |   |
|------------------|---|
| Routing Control: | Allow Routing on Listed Devices<br>None ▼ |
|------------------|---|

Apply ChangesCancel Changes

## 6.4. Administer 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. Check for **Enable SDB for TSAPI Service, JTAPI and Telephony Web Services**.



## 6.5. Add Devices

Select **Security** → **Security Database** → **Devices**. Add the IVR ports as **Devices** as in the list below as created in **Section 5.2** of Communication Manager. These are objects that the Telephony services need for routing and controlling access to the Telephony network.

Security | Security Database | Devices

Home | Help | Logout

▸ AE Services

▸ Communication Manager Interface

▸ High Availability

▸ Licensing

▸ Maintenance

▸ Networking

▼ Security

▸ Account Management

▸ Audit

▸ Certificate Management

▸ Enterprise Directory

▸ Host AA

▸ PAM

▼ Security Database

▸ Control

▸ CTI Users

▸ **Devices**

Devices

Upload devices from file  No file selected.

| <input type="checkbox"/> | Device ID | Tlink Group | Device Type | Location |
|--------------------------|-----------|-------------|-------------|----------|
| <input type="checkbox"/> | 250       | None        | PHONE       |          |
| <input type="checkbox"/> | 251       | None        | PHONE       |          |

0-2 of 2



## 6.6. Restart Services

Select **Maintenance** → **Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check **TSAPI Service** and click **Restart Service**.

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

▶ User Management

▶ Utilities

▶ Help

Service Controller

| Service   | Controller Status |
|---|-------------------|
| <input type="checkbox"/> ASAI Link Manager        | Running           |
| <input type="checkbox"/> DMCC Service             | Running           |
| <input type="checkbox"/> CVLAN Service            | Running           |
| <input type="checkbox"/> DLG Service              | Running           |
| <input type="checkbox"/> Transport Layer Service  | Running           |
| <input checked="" type="checkbox"/> TSAPI Service | Running           |

For status on actual services, please use [Status and Control](#)

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart Web Server

## 6.7. Check TSAPI status and Tlink Name

Select **Status** → **Status and Control** → **TSAPI Service Summary**, the **TSAPI Link Details** are shown below. Note that the **State** is **Online** and **Status** is **Talking**.

The screenshot shows the Avaya Application Enablement Services Management Console. The top navigation bar includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message. The left sidebar contains a tree view with categories like AE Services, Communication Manager, Interface, High Availability, Licensing, Maintenance, Networking, Security, and Status. The main content area displays the "TSAPI Link Details" page. It includes a table with columns: Link, Switch Name, Switch CTI Link ID, Status, Since, State, Switch Version, Associations, Msgs to Switch, Msgs from Switch, and Msgs Period. The table shows one link with ID 1, Switch Name "procr", Switch CTI Link ID 1, Status "Talking", State "Online", Switch Version 18, Associations 4, Msgs to Switch 353, Msgs from Switch 421, and Msgs Period 30. Below the table are buttons for "Online" and "Offline".

| Link | Switch Name | Switch CTI Link ID | Status  | Since                    | State  | Switch Version | Associations | Msgs to Switch | Msgs from Switch | Msgs Period |
|------|-------------|--------------------|---------|--------------------------|--------|----------------|--------------|----------------|------------------|-------------|
| 1    | procr       | 1                  | Talking | Fri Sep 24 09:46:16 2021 | Online | 18             | 4            | 353            | 421              | 30          |

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring Phonet Dynamic IVR.

In this case, the associated Tlink name is "AVAYA#PROC#CSTA#AES8".

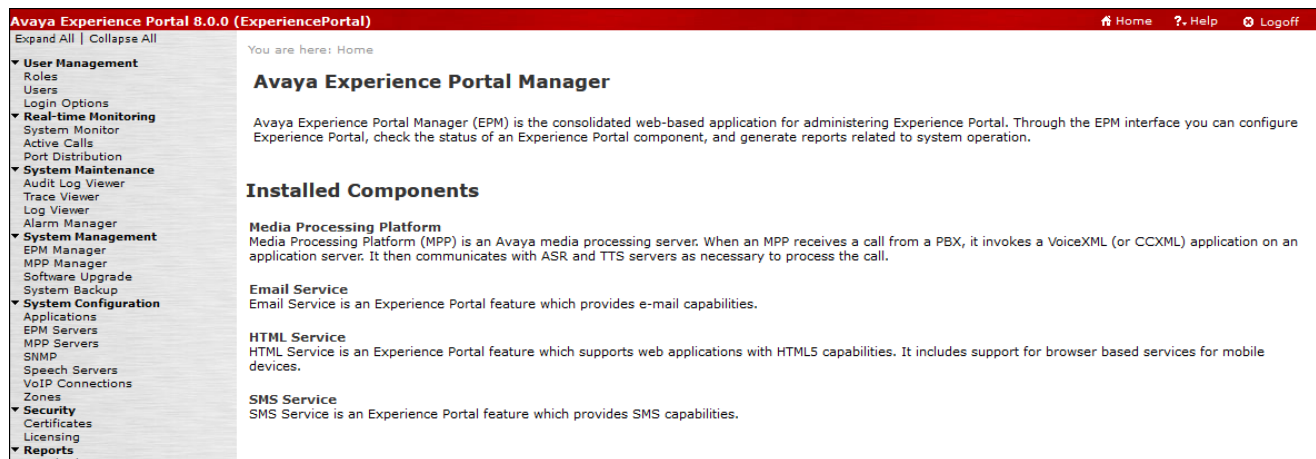
The screenshot shows the Avaya Application Enablement Services Management Console, specifically the "Tlinks" page under the "Security Database" section. The left sidebar shows the "Security" category expanded. The main content area displays a list of Tlink names. The first Tlink name is "AVAYA#PROC#CSTA#AES8", which is selected. Below the list is a "Delete Tlink" button.

| Tlink Name             |
|------------------------|
| AVAYA#PROC#CSTA#AES8   |
| AVAYA#PROC#CSTA-S#AES8 |

## 7. Configure Avaya Experience Portal

The configuration and verification operations illustrated in this section were all performed using browser. The information provided in this section describes the configuration of Experience Portal for this solution. For all other provisioning information such as initial installation, are not the focus of these Application Notes and will not be described.

Login to the Avaya Experience Portal Manager and select **System Configuration** → **Applications** on the left pane.



**Avaya Experience Portal 8.0.0 (ExperiencePortal)** Home Help Logoff

Expand All | Collapse All

**User Management**  
Roles  
Users  
Login Options

**Real-time Monitoring**  
System Monitor  
Active Calls  
Port Distribution

**System Maintenance**  
Audit Log Viewer  
Trace Viewer  
Log Viewer  
Alarm Manager

**System Management**  
EPM Manager  
MPP Manager  
Software Upgrade  
System Backup

**System Configuration**  
Applications  
EPM Servers  
MPP Servers  
SNMP  
Speech Servers  
VoIP Connections  
Zones

**Security**  
Certificates  
Licensing

**Reports**  
Reports

You are here: Home

### Avaya Experience Portal Manager

Avaya Experience Portal Manager (EPM) is the consolidated web-based application for administering Experience Portal. Through the EPM interface you can configure Experience Portal, check the status of an Experience Portal component, and generate reports related to system operation.

#### Installed Components

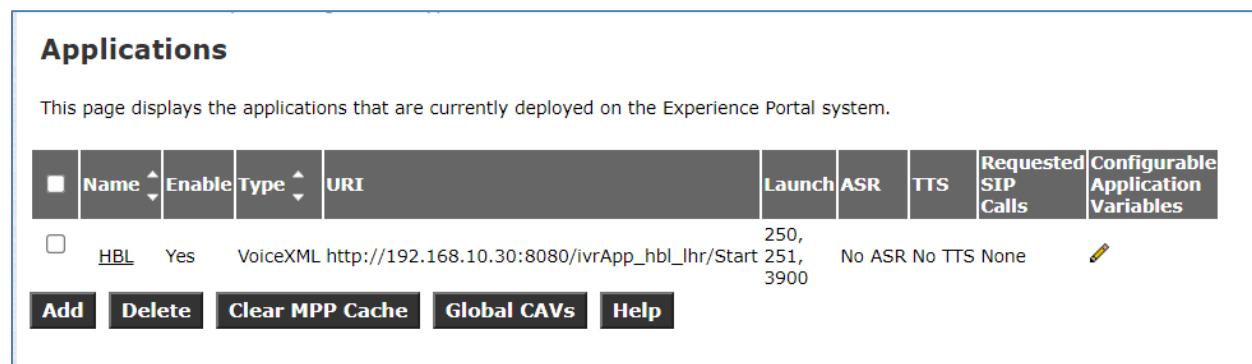
**Media Processing Platform**  
Media Processing Platform (MPP) is an Avaya media processing server. When an MPP receives a call from a PBX, it invokes a VoiceXML (or CCXML) application on an application server. It then communicates with ASR and TTS servers as necessary to process the call.

**Email Service**  
Email Service is an Experience Portal feature which provides e-mail capabilities.

**HTML Service**  
HTML Service is an Experience Portal feature which supports web applications with HTML5 capabilities. It includes support for browser based services for mobile devices.


**SMS Service**  
SMS Service is an Experience Portal feature which provides SMS capabilities.

The following shows the applications listed. Click on the name **HBL** for details on next page.



### Applications

This page displays the applications that are currently deployed on the Experience Portal system.

| <input type="checkbox"/> | Name | Enable | Type     | URI  | Launch         | ASR    | TTS    | Requested SIP Calls | Configurable Application Variables  |
|--------------------------|------|--------|----------|--|----------------|--------|--------|---------------------|---|
| <input type="checkbox"/> | HBL  | Yes    | VoiceXML | http://192.168.10.30:8080/ivrApp_hbl_lhr/Start | 250, 251, 3900 | No ASR | No TTS | None                |  |

**Add** **Delete** **Clear MPP Cache** **Global CAVs** **Help**

The **VoiceXML URL** is administered for pointing to the Pronet's application server running on Tomcat.

“<IP address of application server>:<Port of Tomcat>/<location of application>”

In the section for **Application Launch**, check **Inbound** and add the IVR ports station number as **Called Number**. In our case, 250 and 251 are the ports.

### Change Application

Use this page to change the configuration of an application.

Name: HBL

Enable: ☒ Yes ☐ No

Type: VoiceXML

Reserved SIP Calls: ☒ None ☐ Minimum ☐ Maximum

Requested:

URI

☒ Single ☐ Fail Over ☐ Load Balance

VoiceXML URL: http://192.168.10.30:8080/ivrApp\_hbl\_lhr/Start Verify

Mutual Certificate Authentication: ☐ Yes ☒ No

Basic Authentication: ☐ Yes ☒ No

#### ASR Speech Servers

| Engine Types | Selected Engine Types |
|--------------|-----------------------|
| ASR: <None>  | <None>                |

#### TTS Speech Servers

TTS: No TTS

#### Application Launch

☒ Inbound ☐ Inbound Default ☐ Outbound

☒ Number ☐ Number Range ☐ URI

Called Number: Add

250  
251  
3900

Remove

SIP Header Source: Any

## 8. Configure Pronet Dynamic IVR

The AES Connector used in the application is configured during writing of the applications on Orchestration Designer.

Login to the Orchestration Designer home page, select AES on the left pane and the screen below shows the configured **tserver**. Default values are used for **Timeout** and **Trace Verbosity**. Click on the **aes** for link details.

The screenshot shows the AVAYA Orchestration Designer interface. The left sidebar contains a navigation menu with items: License Server, Connectivity Settings, Certificates, AES, IR Channel Map, IC Common, IC VOX, IC VRUSH/HTTPVOX, Users, and Application Configuration. The main content area is titled 'AES Connector'. It includes a breadcrumb 'You are here: Home > AES'. Below this, there are two input fields: 'Timeout' with a value of 4000 and a description 'Time in ms to wait for TServer/AES to obtain the call. Do not end the input with 'ms'.', and 'Trace Verbosity' with a value of 3 and a description 'Amount of debug output: 0-off - 3 full.'. An 'Update' button is located below these fields. At the bottom, there is a table with columns: Type, Name, Service Name, User Name, Ext Map, and Add Failover. The table contains one row with the following values: Type is 'tserver/AES', Name is 'aes', Service Name is 'AVAYA#PROCR#CSTA#AES8', User Name is 'labuser', Ext Map is 'map', and Add Failover is 'add failover'. A 'Delete' button is located below the table.

| Type                     | Name        | Service Name | User Name             | Ext Map | Add Failover |              |
|--------------------------|-------------|--------------|-----------------------|---------|--------------|--------------|
| <input type="checkbox"/> | tserver/AES | aes          | AVAYA#PROCR#CSTA#AES8 | labuser | map          | add failover |

Note that the **Service Name** is the Tlink name for connecting to AES in **Section 6.7** and the **User Name** configured in **Section 6.3**.

The screenshot shows the AVAYA Orchestration Designer interface. The left sidebar contains a navigation menu with items: License Server, Connectivity Settings, Certificates, AES, IR Channel Map, IC Common, IC VOX, IC VRUSH/HTTPVOX, Users, and Application Configuration. The main content area is titled 'Edit TServer/AES'. It includes a breadcrumb 'You are here: Home > AES > Edit TServer/AES'. Below this, there are four input fields: 'Name' with a value of 'aes', 'Service Name' with a value of 'AVAYA#PROCR#CSTA#AES8', 'User Name' with a value of 'labuser', and 'Change Password' which is unchecked. Below the 'Change Password' field, there are two input fields for 'Password' and 'Confirm Password'. At the bottom, there are 'Save' and 'Cancel' buttons. A note at the bottom states: 'Note: The tserver and failover names cannot contain '\*''. Failover names within a tserver cannot be

Click on the “map” for the mapping of the IVR ports. Note the two IVR ports created earlier in **Section 5.2**.

AVAYA

Orchestration Designer 07.21.05.02

License Server  
Connectivity Settings  
Certificates  
AES  
IR Channel Map  
IC Common  
IC VOX  
IC VRUSH/HTTPVOX  
Users  
Application Configuration

You are here: [Home](#) > [AES](#) > Tserver Extension Map

### Tserver Extension Map

Extension Map for Tserver : [aes](#)

| <input type="checkbox"/> | Channel | Mapped Extension | Observe On Startup |
|--------------------------|---------|------------------|--------------------|
| <input type="checkbox"/> | 0       | 250              | true               |
| <input type="checkbox"/> | 1       | 251              | true               |

Delete

You can map a range of sequential channels to sequential extensions using the format "1-n" in the Channel field.  
You need only to enter the start extension in the Mapped Extension field.

Channel:

Channel call will arrive on for IR. For VP, this value is arbitrary but should be unique to the list.

Mapped Extension:

extension channel maps to for IR. For VP, this is the extension the call will arrive on.

Observe On Startup:

☒

always true.

Add

LYM; Reviewed:  
SPOC 11/4/2021

Solution & Interoperability Test Lab Application Notes  
©2021 Avaya Inc. All Rights Reserved.

22 of 26  
PronetIVR\_AESC

## 9. Verification Steps

This section provides the steps that can be taken to verify correct configuration of the Avaya solution and Pronet Dynamic IVR.

### 9.1. Verify Avaya Aura® Communication Manager CTI Service State

The following steps can validate that the communication between Communication Manager and AES is functioning correctly. Check the AESVCS link status by using the command **status aesvcs cti-link**. Verify the **Service State** of the **CTI link 1** is established.

```
192.168.10.20 - PuTTY
status aesvcs cti-link

      AE SERVICES CTI LINK STATUS

CTI   Version  Mnt   AE Services   Service   Msgs   Msgs
Link                                State      Sent    Rcvd
-----
1     12       no    aes8          established 150     153
2                               down        6        6

Command successfully completed
```

## 9.2. Verify TSAPI Link

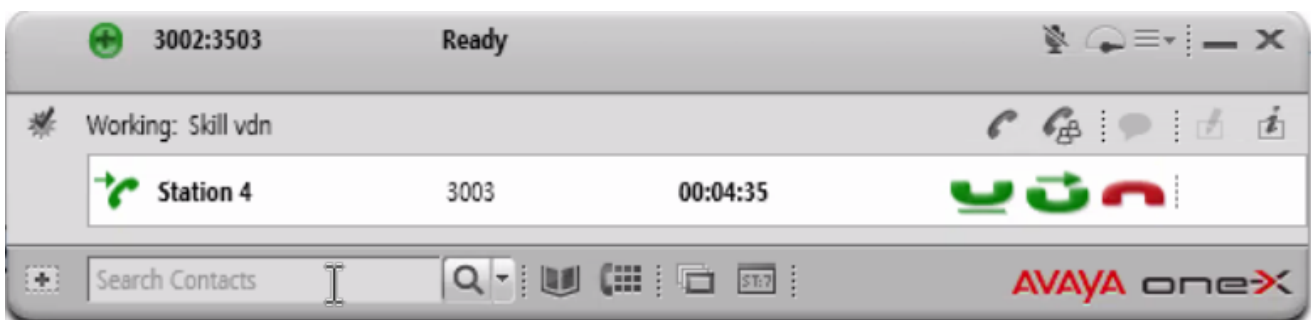
On the AES Management Console verify the status of the TSAPI link by selecting **Status** → **Status and Control** → **TSAPI Service Summary** to display the **TSAPI Link Details** screen. Verify the status of the TSAPI link by checking that the **Status** is **Talking** and the **State** is **Online**.

The screenshot shows the Avaya Application Enablement Services Management Console. The top navigation bar includes 'Status | Status and Control | TSAPI Service Summary'. The left sidebar lists various services, with 'Status and Control' expanded. The main content area displays 'TSAPI Link Details' with a table showing one link in a 'Talking' state and 'Online' state. The table has columns for Link, Switch Name, Switch CTI Link ID, Status, Since, State, Switch Version, Associations, Msgs to Switch, Msgs from Switch, and Msgs Period.

| Link | Switch Name | Switch CTI Link ID | Status  | Since                    | State  | Switch Version | Associations | Msgs to Switch | Msgs from Switch | Msgs Period |
|------|-------------|--------------------|---------|--------------------------|--------|----------------|--------------|----------------|------------------|-------------|
| 1    | procr       | 1                  | Talking | Fri Sep 24 09:46:16 2021 | Online | 18             | 4            | 353            | 421              | 30          |

## 9.3. Pronet Dynamic IVR AES Connector Connection

Make a test call to Communication Manager VDN which routes to the IVR ports and verify announcement is heard from Pronet application. Select the choice for speaking to an agent. Verify the call is successfully transferred by Pronet application as shown below.





## 10. Conclusion

These Application Notes describe the configuration steps required for Pronet Dynamic IVR R1 to interoperate with Avaya Experience Portal R8.0, Avaya Aura® Communication Manager R8.1 and Avaya Aura® Application Enablement Services R8.1. All feature functionality and serviceability test cases were completed successfully with observations noted in **Section 2.2**.

## 11. Additional References

Product documentation for Avaya products may be found at <http://support.avaya.com>

- [1] *Administering Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 11, dated June 2021.
- [2] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 12, dated July 2021.
- [3] *Administering Avaya Experience Portal*, Release 8.1, Issue 1, dated June 2021.
- [4] *Avaya Orchestration Developer's Guide*, Release 8.1, Issue 1, July 2021.

Technical documentation can be obtained for Pronet Dynamic IVR by contacting Pronet with the contact information in **Section 2.3**.

- [5] *IVR Application Development*, Version 2.0.

---

**©2021 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).