



Avaya Solution & Interoperability Test Lab

Application Notes for Pegasystems Pega Call 8.7 with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1– Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Pegasystems Pega Call 8.7 to interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1. Pegasystems Pega Call provides telephony integration for Pegasystems' customer relationship and process management frameworks.

In the compliance testing, Pegasystems Pega Call used the Java Telephony Application Programming Interface from Avaya Aura® Application Enablement Services to route incoming calls to Avaya Aura® Communication Manager and provide screen pop and call control via a web-based agent interface.

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 Pegasystems Pega Call 8.7 to interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1. Pegasystems Pega Call provides telephony integration for Pegasystems' customer relationship and process management frameworks.

In the compliance testing, Pegasystems Pega Call used the Java Telephony Application Programming Interface (JTAPI) from Avaya Aura® Application Enablement Services to provide screen pop and call control via a web-based agent interface. The testing also included the optional Enhanced Routing feature on Pegasystems Pega Call, which used JTAPI adjunct routing capabilities to route incoming calls on Avaya Aura® Communication Manager.

JTAPI is a client-side interface to the Telephony Services Application Programmer Interface (TSAPI) on Avaya Aura® Application Enablement Services. As such, these Application Notes will describe the required configurations for creation and connectivity to the TSAPI service.

The compliance test covered the default out-of-the-box Phone Toolbar used by the agents and a sample routing rule. Any customized agent and routing applications developed using Pegasystems Pega Call is outside the scope of these Application Notes.

2. General Test Approach and Test Results

The feature test cases were performed manually. Incoming calls were placed to the routing VDNs with available agents running the web based Pega Call Phone Toolbar application on their desktops. Manual call controls were exercised from Pega Call to verify proper call actions such as answer and transfer.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connections to the Pega Call server and to the agent desktop.

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 Pegasystem Pega Call utilized enabled capabilities of secure JTAPI.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing focused on verifying the following on Pega Call:

- Handling of JTAPI/TSAPI messages in the areas of event notifications, value queries, and set agent states.
- Use of JTAPI/TSAPI routing services to properly route incoming calls.
- Use of JTAPI/TSAPI call control services to support call control actions such as answer and transfer from the agent desktops.
- Proper handling of call scenarios involving inbound, outbound, ACD, non-ACD, transfer, conference, multiple agents, multiple calls, and long duration.

The serviceability testing focused on verifying the ability of Pega Call to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connections to the Pega Call server and to the agent desktop.

2.2. Test Results

All test cases were executed and verified successfully. The following were observations on Pega Call from the compliance testing.

- By design, Pega Call uses a separate JTAPI session for support of the Enhanced Routing feature.

2.3. Support

Technical support on Pega Call can be obtained through the following:

- **Phone:** +1 (800) 414-8064, +1 (617) 866-6700
- **Email:** support@pega.com
- **Web:** <http://pdn.pega.com>

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The detailed administration of basic connectivity between Communication Manager and Application Enablement Services is not the focus of these Application Notes and will not be described. In the compliance testing, Pega Call monitored the agent station extensions shown in the table below.

Device Type	Extension
Routing VDN	88000, 88001
Skill Group	87000, 87001
Agent Station	70009, 70010
Supervisor Station	80000
Agent ID	80001, 80002

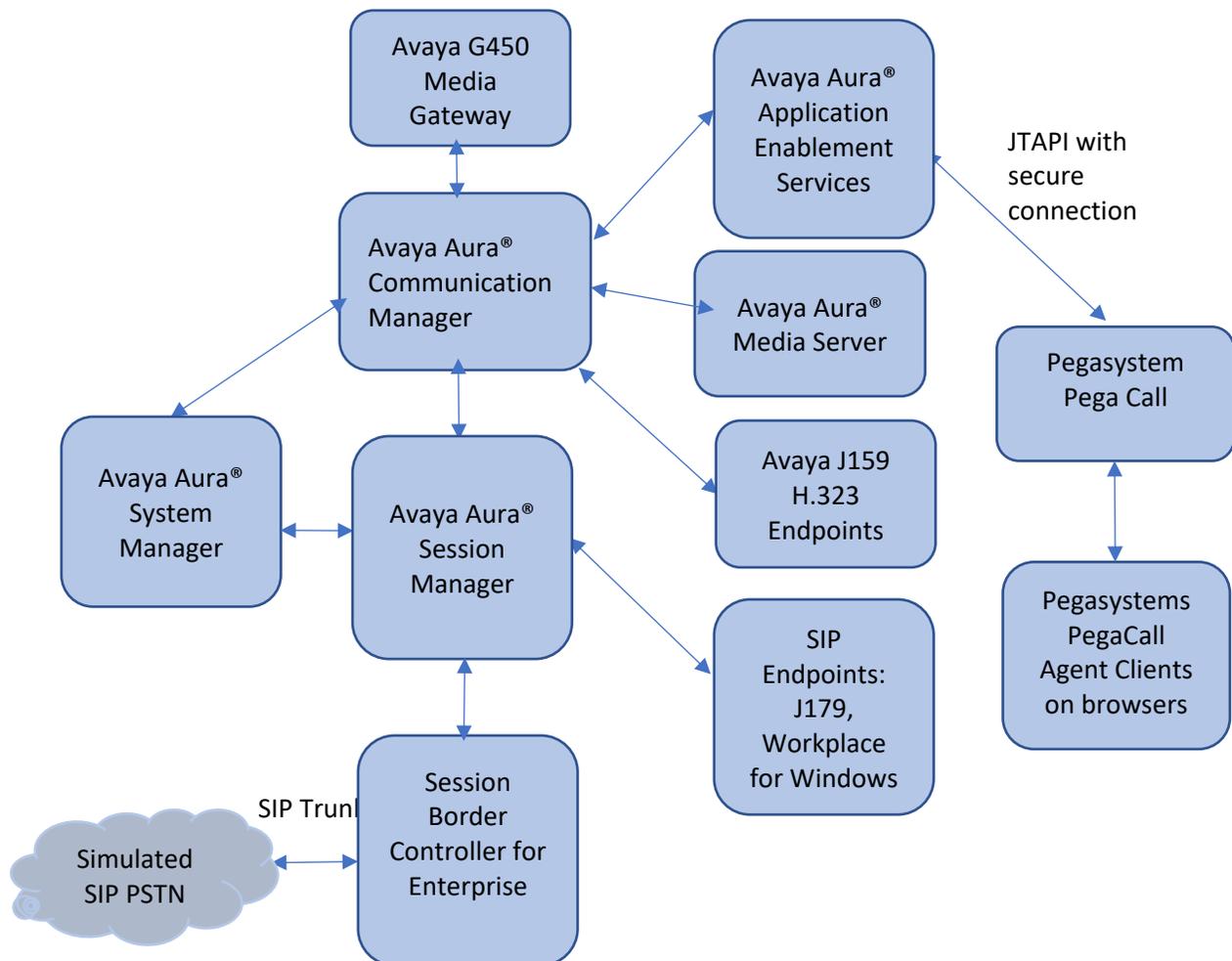


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager in Virtual Environment	10.1.0.0.537353
Avaya Aura® Session Manager in Virtual Environment	10.1.0.1.1010105
Avaya Aura® Communication Manager in Virtual Environment	10.1.0.1 SP1 Build 01.0.974.0-27372
Avaya G450 Media Gateway	41.34.1
Avaya Aura® Media Server in Virtual Environment	10.1.0.77
Avaya Aura® Application Enablement Services in Virtual Environment	10.1.0.1.0.7
Avaya Session Border Controller for Enterprise	10.1
Avaya Workplace Client for Windows	3.25.0.73
Avaya J179 IP Phone (SIP)	4.0.12.1
Avaya J159 IP Deskphone (H.323)	6.8.5
Pegasystems PegaCall - Avaya JTAPI Client	8.7 8.1.3

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
- Obtain UCID setting
- Administer reason codes
- Administer hunt group and agent
- Administer vectors and VDNs

5.1. Verify License

Log into the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the **display system-parameters customer-options** command to verify that the **Computer Telephony Adjunct Links** customer option is set to **y** on **Page 4**. If this option is not set to **y**, then contact the Avaya sales team or business partner for a proper license file.

```
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? y                                     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.)
```

Navigate to **Page 7**, and verify that **Vectoring (Basic)** is set to **y**.

```
display system-parameters customer-options                               Page 7 of 12
CALL CENTER OPTIONAL FEATURES

Call Center Release: 10.1

ACD? y                                                                Reason Codes? y
BCMS (Basic)? y                                                       Service Level Maximizer? n
BCMS/VuStats Service Level? y                                         Service Observing (Basic)? y
BSR Local Treatment for IP & ISDN? y   Service Observing (Remote/By FAC)? y
Business Advocate? n                                                  Service Observing (VDNs)? y
Call Work Codes? y                                                    Timed ACW? y
DTMF Feedback Signals For VRU? y                                       Vectoring (Basic)? y
Dynamic Advocate? n                                                   Vectoring (Prompting)? y
Expert Agent Selection (EAS)? y                                         Vectoring (G3V4 Enhanced)? y
EAS-PHD? y                                                            Vectoring (3.0 Enhanced)? y
Forced ACD Calls? n                                                   Vectoring (ANI/II-Digits Routing)? y
Least Occupied Agent? y                                               Vectoring (G3V4 Advanced Routing)? y
Lookahead Interflow (LAI)? y                                         Vectoring (CINFO)? y
Multiple Call Handling (On Request)? y   Vectoring (Best Service Routing)? y
Multiple Call Handling (Forced)? y                                       Vectoring (Holidays)? y
PASTE (Display PBX Data on Phone)? y   Vectoring (Variables)? y
(NOTE: You must logoff & login to effect the permission changes.)
```

5.2. Administer CTI Link

Add a CTI link using the **add cti-link n** command, where **n** is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

```
add cti-link 1                                                         Page 1 of 3
CTI LINK
CTI Link: 1
Extension: 79999
Type: ADJ-IP
COR: 1
Name: aes95
Unicode Name? n
```

5.3. Obtain UCID Setting

Use the **display system-parameters features** command and navigate to **Page 5**. Make a note of the **Create Universal Call ID (UCID)** setting, which will be used later to configure Pega Call.

```
change system-parameters features                               Page 5 of 19
                                FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:                               Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                                Switch Name:
      Emergency Extension Forwarding (min): 10
      Enable Inter-Gateway Alternate Routing? n
Enable Dial Plan Transparency in Survivable Mode? n
                                COR to Use for DPT: station
                                EC500 Routing in Survivable Mode: dpt-then-ec500
MALICIOUS CALL TRACE PARAMETERS
      Apply MCT Warning Tone? n   MCT Voice Recorder Trunk Group:
      Delay Sending Release (seconds): 0
SEND ALL CALLS OPTIONS
      Send All Calls Applies to: station   Auto Inspect on Send All Calls? n
      Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
      Create Universal Call ID (UCID)? y   UCID Network Node ID:1
      Copy UCID for Station Conference/Transfer? n
```

Navigate to **Page 13**, and make a note of the **Send UCID to ASAI** setting, which will be used later to configure Pega Call.

```
change system-parameters features                               Page 13 of 19
                                FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER MISCELLANEOUS
      Callr-info Display Timer (sec): 10
                                Clear Callr-info: next-call
      Allow Ringer-off with Auto-Answer? n

      Reporting for PC Non-Predictive Calls? n

      Agent/Caller Disconnect Tones? n
Interruptible Aux Notification Timer (sec): 3
      Zip Tone Burst for Callmaster Endpoints: double

ASAI
      Copy ASAI UII During Conference/Transfer? n
      Call Classification After Answer Supervision? n
                                Send UCID to ASAI? y
      For ASAI Send DTMF Tone to Call Originator? y
      Send Connect Event to ASAI For Announcement Answer? n
      Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```

5.4. Administer Reason Codes

For contact centers that use reason codes, enter the **change reason-code-names** command. Configure the **Aux Work** and **Logout** reason codes as desired. The compliance testing used the default values used by Pega Call, which are shown below.

```
change reason-code-names                                     Page 1 of 1

                                REASON CODE NAMES

                                Aux Work/                Logout
                                Interruptible?

Reason Code 1: In a Meeting    /n Break
Reason Code 2: Out of Office /n Lunch
Reason Code 3: Lunch          /n
Reason Code 4:                  /n
Reason Code 5:                  /n
Reason Code 6:                  /n
Reason Code 7:                  /n Other
Reason Code 8:                  /n
Reason Code 9:                  /n

Default Reason Code:
```

5.5. Administer Hunt Group and Agent

This section shows the steps required to add a new service or skill on Communication Manager. Services are accessed by calling a Vector Directory Number (VDN), which points to a vector. The vector then points to a hunt group associated with an agent. The following sections give step by step instructions on how to add the following.

- Hunt Group
- Agent

5.5.1. Add Hunt Group

To add a new skillset or hunt group type, **add hunt-group x**, where **x** is the new hunt group number. For example, hunt group **1** is added for the **Voice Service** queue. Ensure that **ACD**, **Queue** and **Vector** are all set to **y**. Also, that **Group Type** is set to **ucd-mia**.

```
add hunt-group 1                                     Page 1 of 4
                                                    HUNT GROUP
      Group Number: 1                                ACD? y
      Group Name: Voice Service                      Queue? y
      Group Extension: 87000                          Vector? y
      Group Type: ucd-mia
      TN: 1
      COR: 1
      Security Code:                                MM Early Answer? n
      ISDN/SIP Caller Display:                      Local Agent Preference? n
      Queue Limit: unlimited
      Calls Warning Threshold:      Port:
      Time Warning Threshold:      Port:
```

On **Page 2** ensure that **Skill** is set to **y** as shown below.

```
add hunt-group 1                                     Page 2 of 4
                                                    HUNT GROUP
      Expected Call Handling Time (sec):
      Skill? y                                       180
      AAS? n
      Measured: none
      Supervisor Extension:
      Controlling Adjunct:
      Multiple Call Handling: none
      Timed ACW Interval
      (sec):                                         After Xfer or Held Call Drops? n
```

5.5.2. Add Agent

In the compliance testing, the agents 80000 and 80001 were created.

To add a new agent, type **add agent-loginID x**, where x is the login id for the new agent.

```

add agent-login 80000                                     Page 1 of 3
                                                    AGENT LOGINID
    Login ID: 80000                                     AAS? n
    Name: Voice Agent                                  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
                                                    AUDIX Name for Messaging:

                                                    LoginID for ISDN/SIP Display? n
                                                    Password:****
                                                    Password (enter again):****
    MWI Served User Type: sip-adjunct                 Auto Answer: station
    AUX Agent Remains in LOA Queue: system            MIA Across Skills: system
    AUX Agent Considered Idle (MIA): system ACW Agent Considered Idle: system
    Work Mode on Login: 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**, add the required skills. Note that the skill **1** is added to this agent so when a call for **Voice Service** is initiated, the call can be routed to this agent.

```

add agent-loginID 80000                                     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:
  
```

Repeat this section to add another agent 80001.

5.6. Administer Vectors and VDNs

Add a vector using the **change vector n** command, where **n** is a vector number. Note that the vector steps may vary, and below is a sample vector used in the compliance testing. The **adjunct routing link** number must match the number configured in the cti-link form in **Section 5.2**.

```
change vector 1                                     Page 1 of 6
                                     CALL VECTOR
Number: 1                                           Name: VoiceService
Multimedia? n      Attendant Vectoring? n      Meet-me Conf? n      Lock? n
Basic? y      EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing? y
Prompting? y      LAI? y      G3V4 Adv Route? y      CINFO? y      BSR? y      Holidays? y
Variables? y      3.0 Enhanced? y
01 adjunct      routing link 1
02 wait-time      5      secs hearing silence
03 route-to      number 88000      cov n if unconditionally
04 stop
05
06
07
08
09
10
11
12

Press 'Esc f 6' for Vector Editing
```

Add a VDN using the **add vdn n** command, where **n** is an available extension number. Enter a descriptive **Name** and the vector number from above for **Destination**. Retain the default values for all remaining fields.

```

add vdn 88000                                     Page 1 of 3
          VECTOR DIRECTORY NUMBER
          Extension: 88000                          Unicode Name? n
          Name*: Voice VDN
          Destination: Vector Number                1
Attendant Vectoring? n
Meet-me Conferencing? n
Allow VDN Override? n
          COR: 1
          TN*: 1
          Measured: none      Report Adjunct Calls as ACD*? n

VDN of Origin Annc. Extension*:
          1st Skill*:
          2nd Skill*:
          3rd Skill*:

SIP URI:

* Follows VDN Override Rules
  
```

Repeat this section to administer the desired number of vectors and VDNs. In the compliance testing, two sets of vectors and VDNs were created, as shown below.

```

list vdn
          VECTOR DIRECTORY NUMBERS
Name (22 characters)  Ext/Skills  VDN      Vec      Orig      Evtnt
Ovr COR  TN PRT Num  Meas Annc  Noti
Adj
Voice VDN             88000      n 1      1  V  1      none      1
Voice VDN             88001      n 1      1  V  2      none      1
  
```

6. Configure Avaya Aura® Application Enablement Services

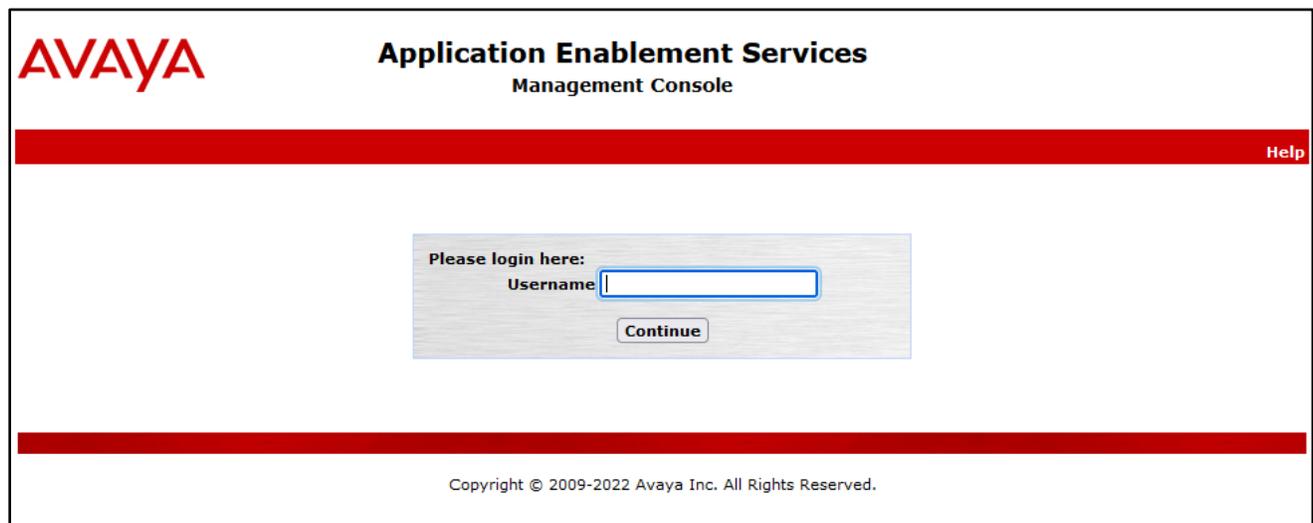
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer TCP Settings
- Administer Pega user
- Administer security database
- Restart services
- Obtain Tlink name

6.1. Launch OAM Interface

Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where **ip-address** is the IP address of the Application Enablement Services server.

The **Please login here** screen is displayed. Log in using the appropriate credentials.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. The title "Application Enablement Services Management Console" is centered at the top. A red horizontal bar spans the width of the page, with the word "Help" in white text on the right side. In the center, there is a light gray login box containing the text "Please login here:" followed by "Username" and a text input field. Below the input field is a "Continue" button. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2022 Avaya Inc. All Rights Reserved." is displayed.

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

The screenshot shows the Avaya Application Enablement Services Management Console. At the top left is the Avaya logo. The main title is "Application Enablement Services Management Console". On the top right, there is a system information block with the following text: "welcome: User cust", "Last login: Mon Jun 27 16:37:37 2022 from 172.16.8.16", "Number of prior failed login attempts: 0", "HostName/IP: aes95/10.30.5.95", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 10.1.0.1.0.7-0", "Server Date and Time: Tue Jul 05 06:22:34 EDT 2022", and "HA Status: Not Configured". Below the title bar is a red navigation bar with "Home" on the left and "Home | Help | Logout" on the right. A left-hand navigation menu contains the following items: "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 the following text: "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: "• 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". Below the list, it 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." At the bottom of the page, there is a copyright notice: "Copyright © 2009-2022 Avaya Inc. All Rights Reserved."

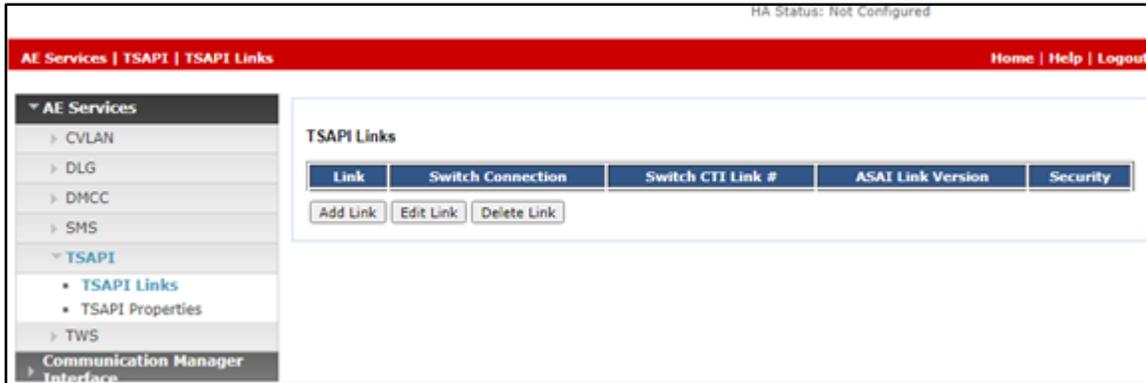
6.2. Verify License

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).

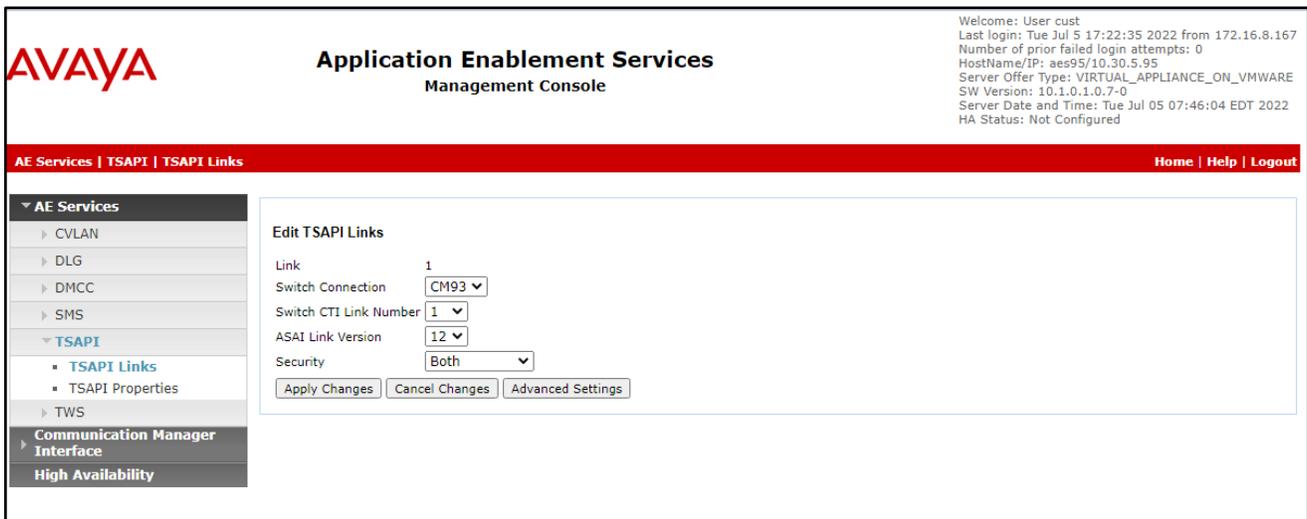
The screenshot displays the Avaya Application Enablement Services Management Console. At the top left is the Avaya logo and the title "Application Enablement Services Management Console". On the top right, there is a welcome message for user "cust" and system information including last login time, failed login attempts, host name, server offer type, SW version, server date and time, and HA status. A red navigation bar contains "Licensing" and "Home | Help | Logout". A left-hand navigation pane lists various services, with "Licensing" expanded to show "WebLM Server Address", "WebLM Server Access", and "Reserved Licenses". The main content area, titled "Licensing", provides instructions on how to set up, import, and maintain licenses, listing "WebLM Server Address", "WebLM Server Access", and "Reserved Licenses" as required items. A red note at the bottom of the main content area states: "NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page". The footer contains the copyright notice: "Copyright © 2009-2022 Avaya Inc. All Rights Reserved."

6.3. Administer TSAPI Link

Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.



The **Add TSAPI Links** screen is displayed next. The **Link** field is only local to the Application Enablement Services server and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection **CM93** is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.



6.4. Administer TCP Settings

Select **Networking** → **TCP/TLS Settings** from the left pane, to display the **TCP / TLS Settings** screen in the right pane. For **TCP Retransmission Count**, select **TSAPI Routing Application Configuration (6)**, as shown below.

The screenshot displays the Avaya Application Enablement Services Management Console. The top left features the Avaya logo. The main header reads "Application Enablement Services Management Console". In the top right corner, a user status block shows: "Welcome: User cust", "Last login: Tue Jul 5 17:22:35 2022 from 172.16.8.167", "Number of prior failed login attempts: 0", "HostName/IP: aes95/10.30.5.95", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 10.1.0.1.0.7-0", "Server Date and Time: Tue Jul 05 07:49:24 EDT 2022", and "HA Status: Not Configured".

A red navigation bar contains "Networking | TCP / TLS Settings" on the left and "Home | Help | Logout" on the right. The left sidebar menu includes: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking" (expanded), "AE Service IP (Local IP)", "Network Configure", "Ports", "TCP/TLS Settings" (highlighted), "Security", "Status", "User Management", "Utilities", and "Help".

The main content area is titled "TCP / TLS Settings". It contains two sections:

- TLSv1 Protocol Configuration:** Three checked checkboxes for "Support TLSv1.0 Protocol", "Support TLSv1.1 Protocol", and "Support TLSv1.2 Protocol".
- TCP Retransmission Count:** Two radio button options: "Standard Configuration (15)" (unselected) and "TSAPI Routing Application Configuration (6)" (selected).

Below these settings are three buttons: "Apply Changes", "Restore Defaults", and "Cancel Changes".

A note states: "Note: A smaller TCP Retransmission Count reduces the amount of time that the AE Services server waits for a TCP acknowledgement before closing the socket. Select the Standard Configuration setting unless this AE Services server is used by TSAPI routing applications." A warning follows: "Warning: This setting applies to all TCP and TLS sockets on the AE Services Server and so it should be used with caution."

6.5. Administer Pega User

Select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane.

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select **Yes** from the drop-down list. Retain the default value in the remaining fields.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and system information such as "Welcome: User cust", "Last login: Tue Jul 5 17:22:35 2022 from 172.16.8.167", "Number of prior failed login attempts: 0", "HostName/IP: aes95/10.30.5.95", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 10.1.0.1.0.7-0", "Server Date and Time: Tue Jul 05 07:52:07 EDT 2022", and "HA Status: Not Configured".

The navigation bar shows "User Management | User Admin | Add User" and "Home | Help | Logout". The left sidebar contains a tree view with categories like "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", and "Help".

The main content area is titled "Add User" and includes a note: "Fields marked with * can not be empty." The form fields are as follows:

* User Id	<input type="text" value="pega"/>
* Common Name	<input type="text" value="pega"/>
* Surname	<input type="text" value="pega"/>
* 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"/>

6.6. 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. Uncheck both fields below.

In the event that the security database is used by the customer with parameters already enabled, then follow reference [4] to configure access privileges for the Pega user from **Section 6.4**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top left features the Avaya logo. The main header reads "Application Enablement Services Management Console". In the top right corner, system information is provided: "Welcome: User cust", "Last login: Tue Jul 5 17:22:35 2022 from 172.16.8.167", "Number of prior failed login attempts: 0", "HostName/IP: aes95/10.30.5.95", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 10.1.0.1.0.7-0", "Server Date and Time: Tue Jul 05 07:53:47 EDT 2022", and "HA Status: Not Configured". A red navigation bar contains "Security | Security Database | Control" on the left and "Home | Help | Logout" on the right. The left sidebar lists various service categories, with "Security Database" expanded to show "Control" selected. The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services", along with an "Apply Changes" button.

6.7. 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**.

The screenshot shows the Avaya Application Enablement Services Management Console. The top left features the Avaya logo. The main title is "Application Enablement Services Management Console". In the top right corner, there is a welcome message and system information: "Welcome: user cust", "Last login: Tue Jul 5 17:22:35 2022 from 172.16.8.167", "Number of prior failed login attempts: 0", "HostName/IP: aes95/10.30.5.95", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 10.1.0.1.0.7-0", "Server Date and Time: Tue Jul 05 07:56:33 EDT 2022", and "HA Status: Not Configured".

The left navigation pane includes the following items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance (expanded), Date Time/NTP Server, Security Database, Service Controller (selected), Server Data, Networking, Security, Status, User Management, Utilities, and Help.

The main content area is titled "Service Controller" and contains a table with the following data:

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

Below the table, there is a note: "For status on actual services, please use [Status and Control](#)". At the bottom of the main content area, there are several buttons: Start, Stop, Restart Service, Restart AE Server, Restart Linux, and Restart Web Server.

6.8. Obtain Tlink Name

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 Pega Call.

In this case, the associated Tlink name is **AVAYA#CM93#CSTA-S#AES95**. Note the use of the switch connection **CM93** from **Section 6.3** as part of the Tlink name.

The screenshot displays the Avaya Application Enablement Services Management Console. The top left features the Avaya logo. The main title is "Application Enablement Services Management Console". In the top right corner, system information is provided: "Welcome: User cust", "Last login: Tue Jul 5 18:18:32 2022 from 172.16.8.167", "Number of prior failed login attempts: 0", "HostName/IP: aes95/10.30.5.95", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 10.1.0.1.0.7-0", "Server Date and Time: Tue Jul 05 07:58:38 EDT 2022", and "HA Status: Not Configured".

A red navigation bar contains "Security | Security Database | Tlinks" on the left and "Home | Help | Logout" on the right. The left sidebar menu includes: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security (expanded), Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database (expanded), Control, CTI Users, Devices, Device Groups, and Tlinks (selected).

The main content area is titled "Tlinks" and shows a "Tlink Name" section with two radio button options: "AVAYA#CM93#CSTA#AES95" (unselected) and "AVAYA#CM93#CSTA-S#AES95" (selected). A "Delete Tlink" button is located below the options.

7. Configure Pegasystems Pega Call

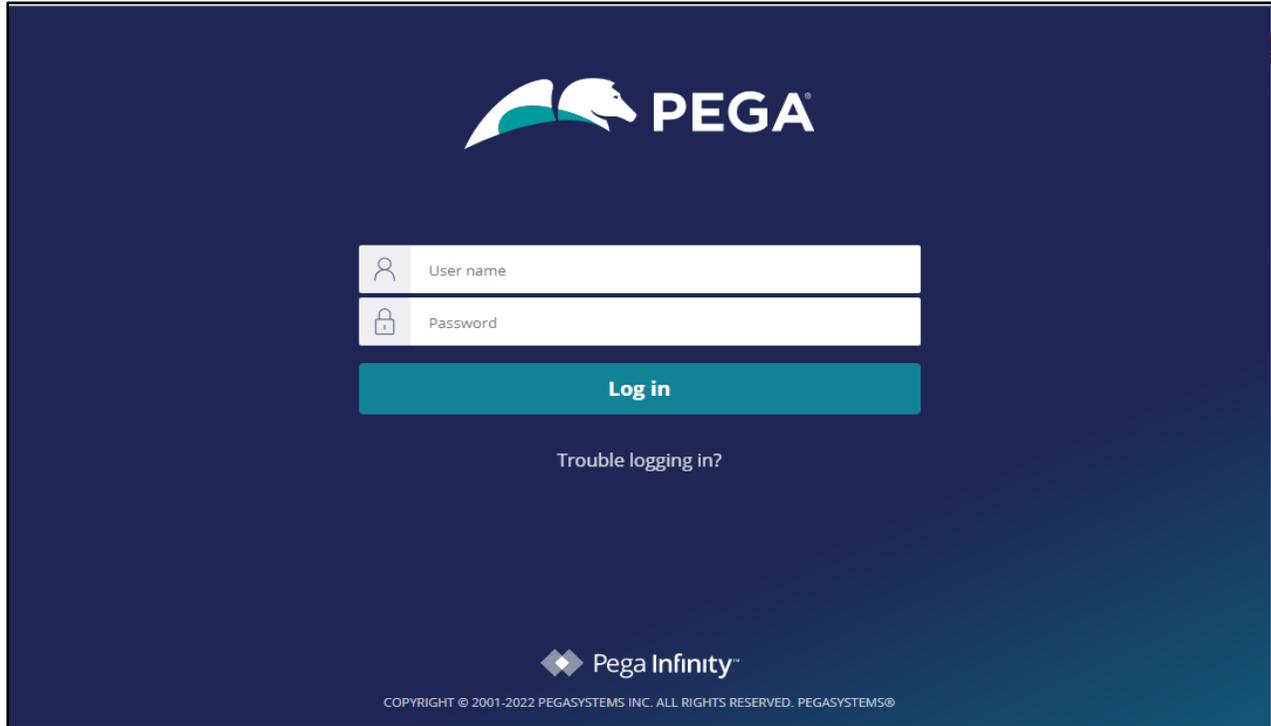
This section provides the procedures for configuring Pega Call. The procedures include the following areas:

- Launch web interface
- Administer CTI link
- Administer route points
- Administer decision tree

The configuration of Pega Call is performed by Pegasystems service personnel. The procedural steps are presented in these Application Notes for informational purposes. Pega Call can be configured on a single server or with components distributed across multiple servers. The solution provides a customizable platform that uses the J2EE framework with either Tomcat, WebSphere, WebLogic or JBoss as the application server, and either Oracle, SQL, DB2 or PostgreSQL as the database component. For ease of compliance testing, the configuration used a single server hosting all components including Tomcat and PostgreSQL.

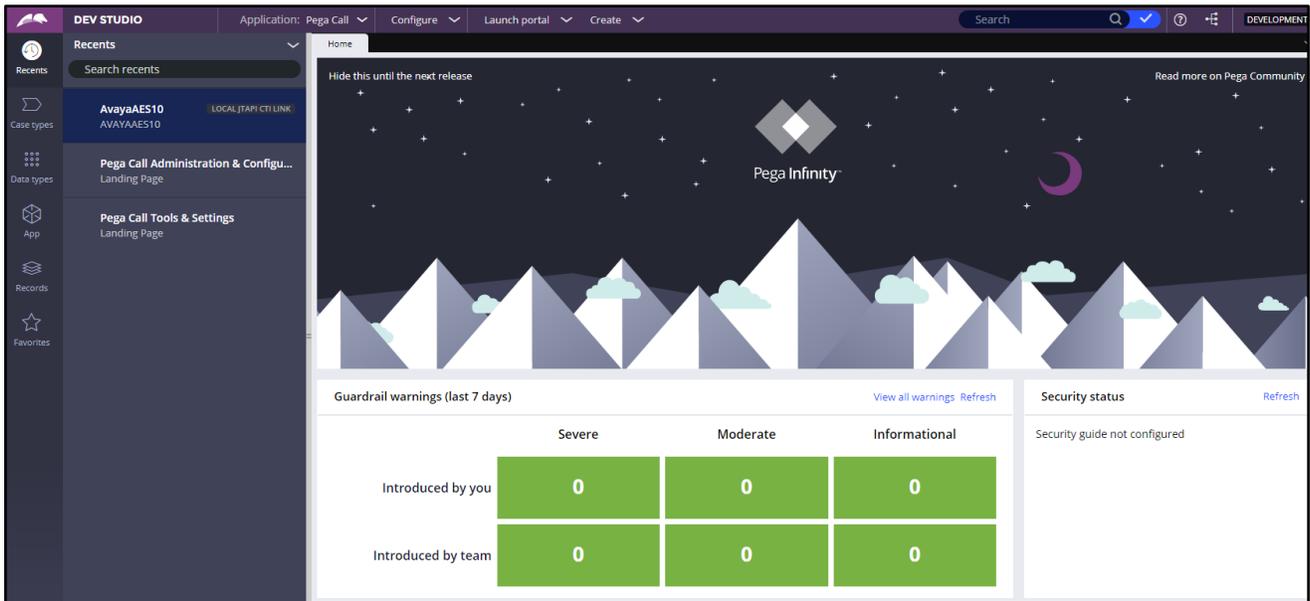
7.1. Launch Web Interface

Access the web-based interface by using the URL “http://ip-address:port/prweb/PRServlet” in an Internet browser window, where “ip-address” is the IP address of the Pega Call server, and “port” is the pertinent port number from Pegasystems. The screen below is displayed. Log in using the administrator credentials.



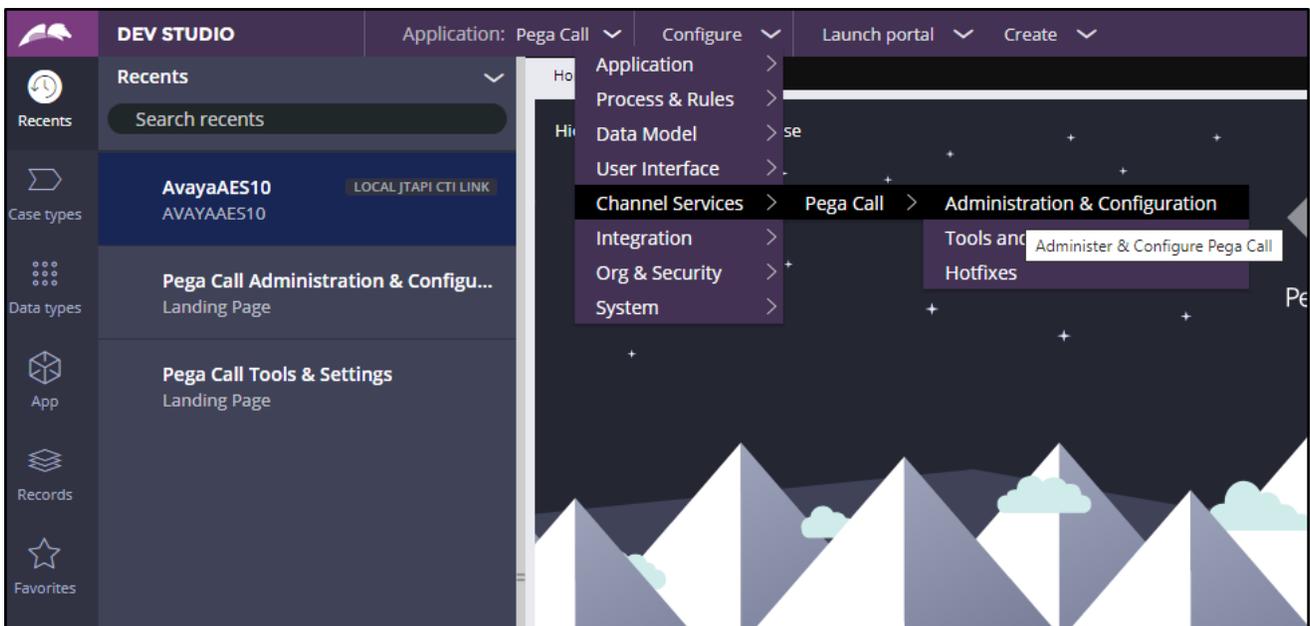
The screenshot shows the Pega Call web interface login screen. At the top center is the Pega logo, which consists of a stylized white horse head and the word "PEGA" in white capital letters. Below the logo are two white input fields: the first is labeled "User name" and the second is labeled "Password". Below the password field is a teal button with the text "Log in" in white. Below the button is a link that says "Trouble logging in?". At the bottom of the screen, there is a "Pega Infinity" logo and the text "COPYRIGHT © 2001-2022 PEGASYSTEMS INC. ALL RIGHTS RESERVED. PEGASYSTEMS®".

After login successfully the screen below is displayed.

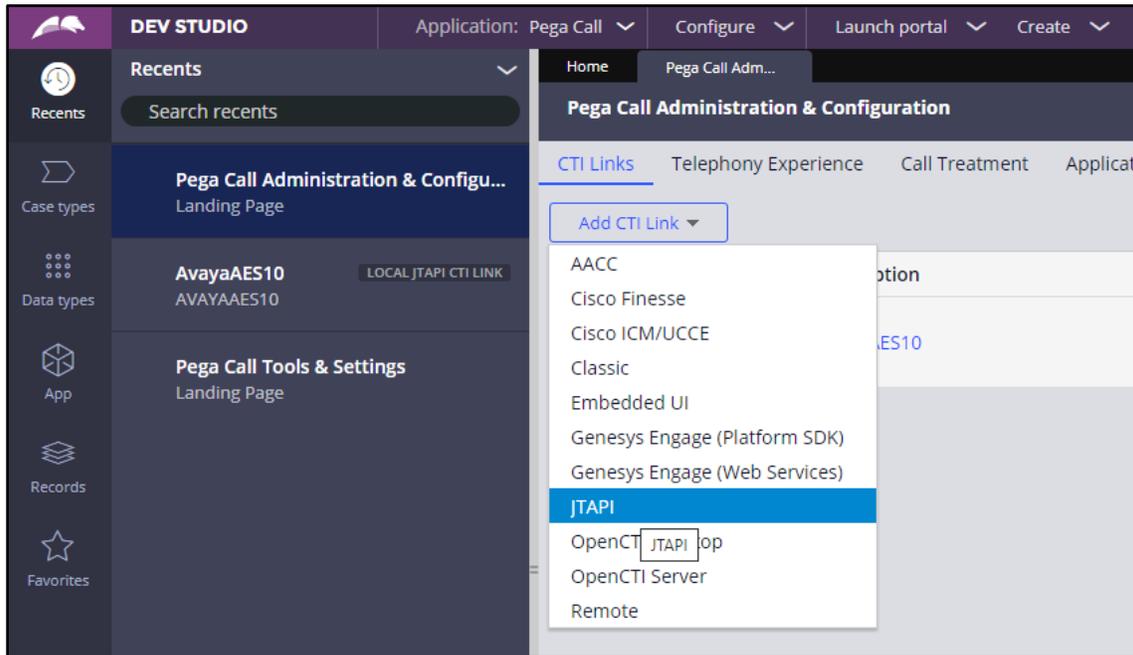


7.2. Administer CTI Link

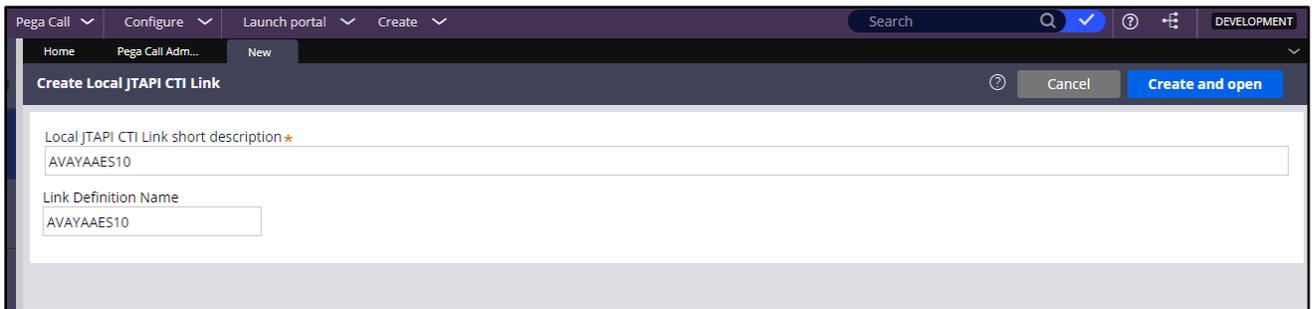
The screen below is displayed next. Select **Configure** → **Channel Services** → **Pega Call** → **Administration & Configuration** from the top menu.



The **Pega Call Administration & Configuration** screen is displayed. Select **CTI Links** → **Add CTI Link** → **JTAPI**, as shown below.

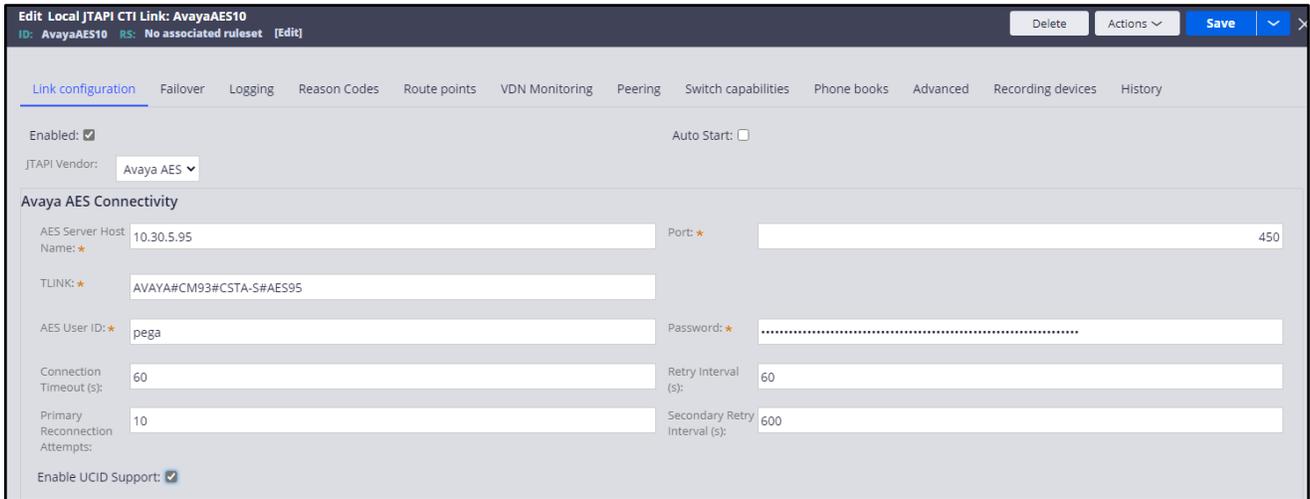


The **Create Local JTAPI CTI Link** screen is displayed. Enter desired values for **Local JTAPI CTI Link short description** and **Link Definition Name**. Click **Create and open**.



The **Edit Local JTAPI CTI Link** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Auto Start:** Check this field.
- **AES Server Host Name:** IP address of Application Enablement Services.
- **TLINK:** The Tlink name from **Section 6.7**.
- **AES User ID:** The Pega Call user credentials from **Section 6.4**.
- **Password:** The Pega Call user credentials from **Section 6.4**.
- **Enable UCID Support:** Check when both UCID settings in **Section 5.3** are enabled.

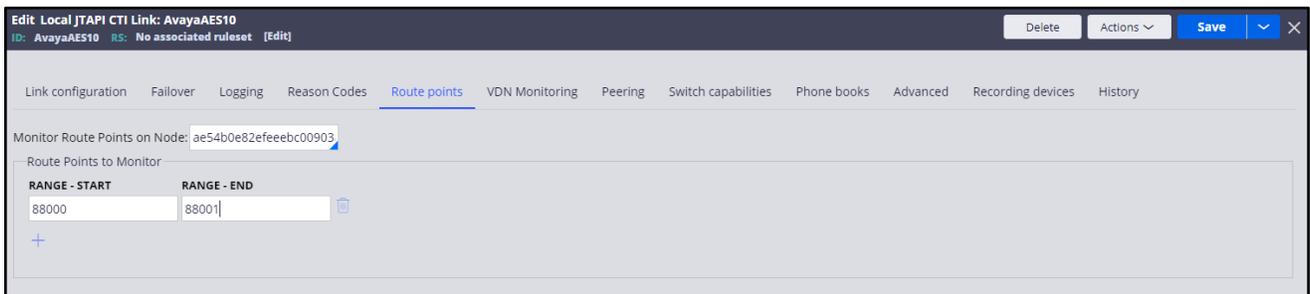


7.3. Administer Route Points

This section is only applicable to systems that use the Enhanced Routing feature.

Select the **Route points** tab. For **Monitor Route Points on Node**, select the applicable node. In the **Route Points to Monitor** sub-section, add the routing VDN extensions from **Section 5.6**.

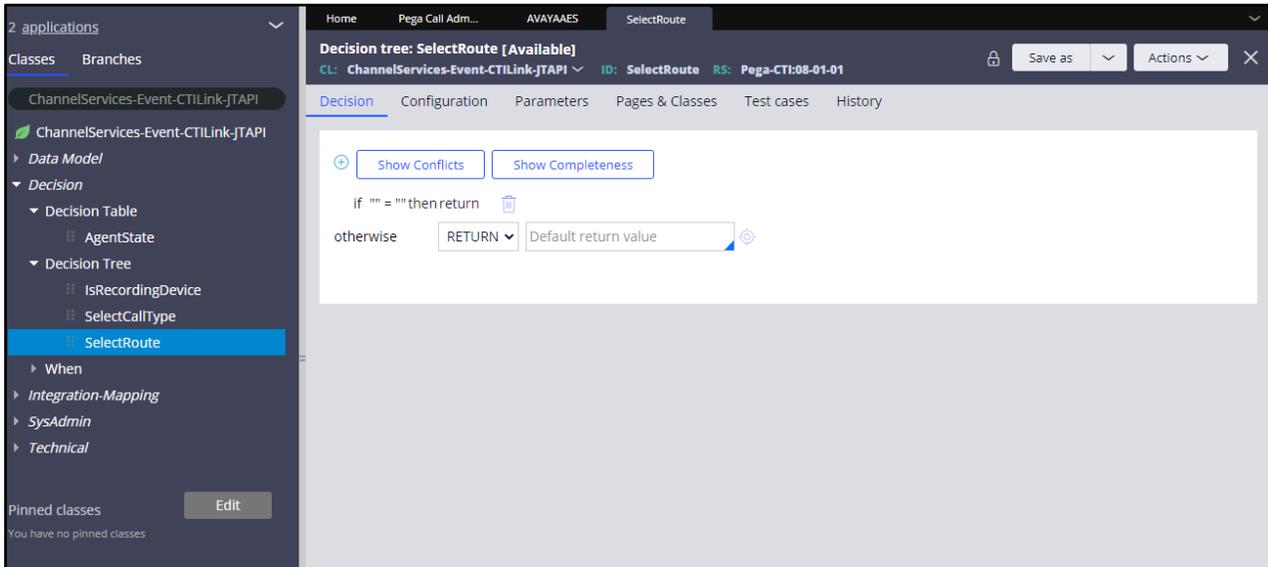
For systems that use the Enhanced Routing feature, click on the menu selection drop-down list from the upper left corner of the screen shown below.



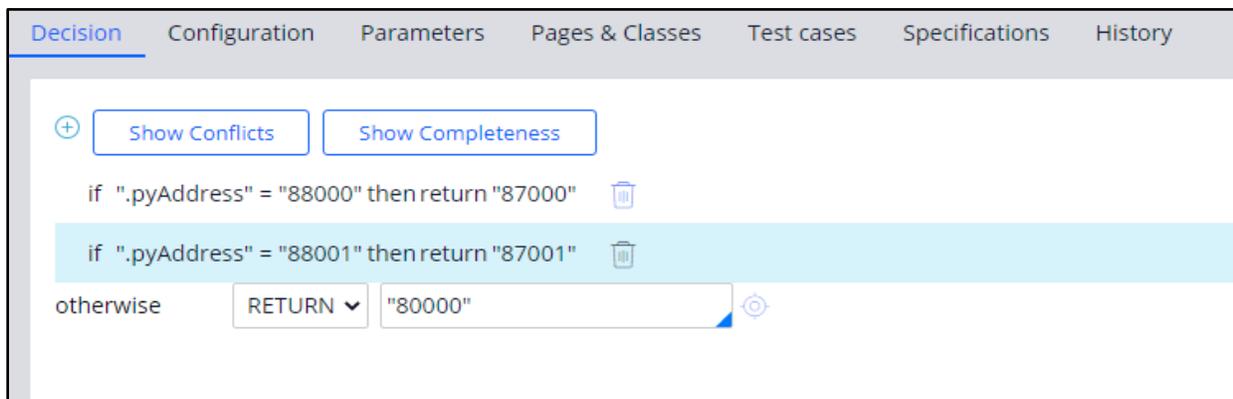
7.4. Administer Decision Tree

This section is only applicable to systems that use the Enhanced Routing feature.

Prior to administering decision tree, follow reference [6] to create a RuleSet, which is a set of rules that define an application or a major portion of an application. In the compliance testing, the default out-of-box RuleSet named **Pega-CTI** with ID of **SelectRoute** was used. The screen below is displayed next. Select **App** from the far-left pane (not shown) and enter “**ChannelServices-Event-CTILink-JTAPI**” in the search area. Scroll down the left pane and select **Decision** → **Decision Tree** → **SelectRoute**.



The **Decision Tree: SelectRoute** screen is displayed. Follow reference [6] to configure the desired routing logic. The screenshot below shows the routing logic used in the compliance testing. The **.pyAddress** parameter was used as the matching criteria to the routing VDN extensions in **Section 5.6**. As shown in **Section 3**, extensions **87000** and **87001** are existing skill groups on Communication Manager, and extension **80000** is the supervisor.



8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, and Pega Call.

8.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify status of the administered CTI link by using the “status aevcs cti-link” command. Verify that the **Service State** is “established” for the CTI link number administered in **Section 5.2. as shown below.**

```
status aevcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	12	no	aes95	established	1780	1780

Enter the command **list agent-loginID** verify that agents **80000** and **80001** shown in **Section 5.4** is logged-in to extension **70010** and **70009**.

```
list agent-loginID
```

AGENT LOGINID									
Login ID	Name	Extension	Dir	Agt	AAS/AUD	COR	Ag	Pr	SO
	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv
80000	Voice Agent 1/01	70009 /	/	/	/	/	1	lv1	
80001	Voice Agent1 1/01	70010 /	/	/	/	/	1	lv1	

8.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the TSAPI link by selecting **Status** → **Status and Control** → **TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify the **Status** is “Talking” for the TSAPI link administered in **Section 6.3** and that the **Associations** column reflects the number of agents that are logged in.



Application Enablement Services

Management Console

Welcome: User cust
 Last login: Tue Jul 5 18:56:10 2022 from 172.16.8.167
 Number of prior failed login attempts: 0
 HostName/IP: aes95/10.30.5.95
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 10.1.0.1.0.7-0
 Server Date and Time: Tue Jul 05 19:36:41 ICT 2022
 HA Status: Not Configured

Status | Status and Control | TSAPI Service Summary Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▼ Status
 - Alarm Viewer
 - ▶ Logs
 - ▶ Log Manager
 - ▼ Status and Control
 - CVLAN Service Summary
 - DLG Services Summary
 - DMCC Service Summary
 - Switch Conn Summary
 - **TSAPI Service Summary**
 - ▶ User Management
 - ▶ Utilities
 - ▶ Help

TSAPI Link Details

Enable page refresh every seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	CM93	1	Talking	Thu Jun 16 14:40:40 2022	Online	20	1	1807	1807	30

For service-wide information, choose one of the following:

NAQ; Reviewed
SPOC 11/16/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

30 of 38
PGCall87-AES10

Verify the CTI user status by selecting **Status** → **Status and Control** → **TSAPI Service Summary** → **CTI User Status**. The **Open Streams** section of this page displays open stream created by the **pega** user with the **Tlink**.



Application Enablement Services

Management Console

Welcome: User cust
 Last login: Tue Jul 5 18:56:10 2022 from 172.16.8.167
 Number of prior failed login attempts: 0
 HostName/IP: aes95/10.30.5.95
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 10.1.0.1.0.7-0
 Server Date and Time: Tue Jul 05 19:39:03 ICT 2022
 HA Status: Not Configured

Status | Status and Control | TSAPI Service Summary
Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▼ Status
 - Alarm Viewer
 - ▶ Logs
 - ▶ Log Manager
 - ▼ Status and Control
 - CVLAN Service Summary
 - DLG Services Summary
 - DMCC Service Summary
 - Switch Conn Summary
 - TSAPI Service Summary
 - ▶ User Management
 - ▶ Utilities
 - ▶ Help

CTI User Status

Enable page refresh every 60 seconds

CTI Users All Users Submit

Open Streams 4
Closed Streams 50

Open Streams

Name	Time Opened	Time Closed	Tlink Name
engelbart	Mon 27 Jun 2022 05:27:47 PM +07		AVAYA#CM93#CSTA#AES95
pega	Tue 05 Jul 2022 07:30:47 PM +07		AVAYA#CM93#CSTA-S#AES95
pega	Tue 05 Jul 2022 09:37:31 AM +07		AVAYA#CM93#CSTA-S#AES95
DMCCLCUserDoNotModify	Tue 28 Jun 2022 03:41:29 PM +07		AVAYA#CM93#CSTA#AES95

Show Closed Streams
Close All Opened Streams
Back

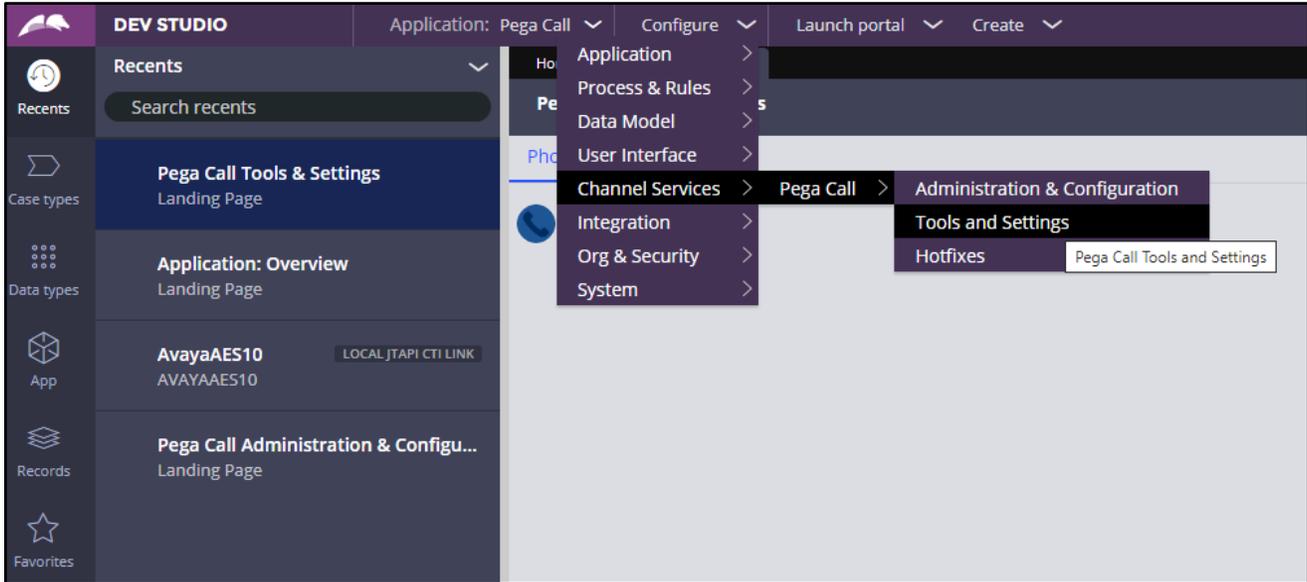
NAQ; Reviewed
SPOC 11/16/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

31 of 38
PGCall87-AES10

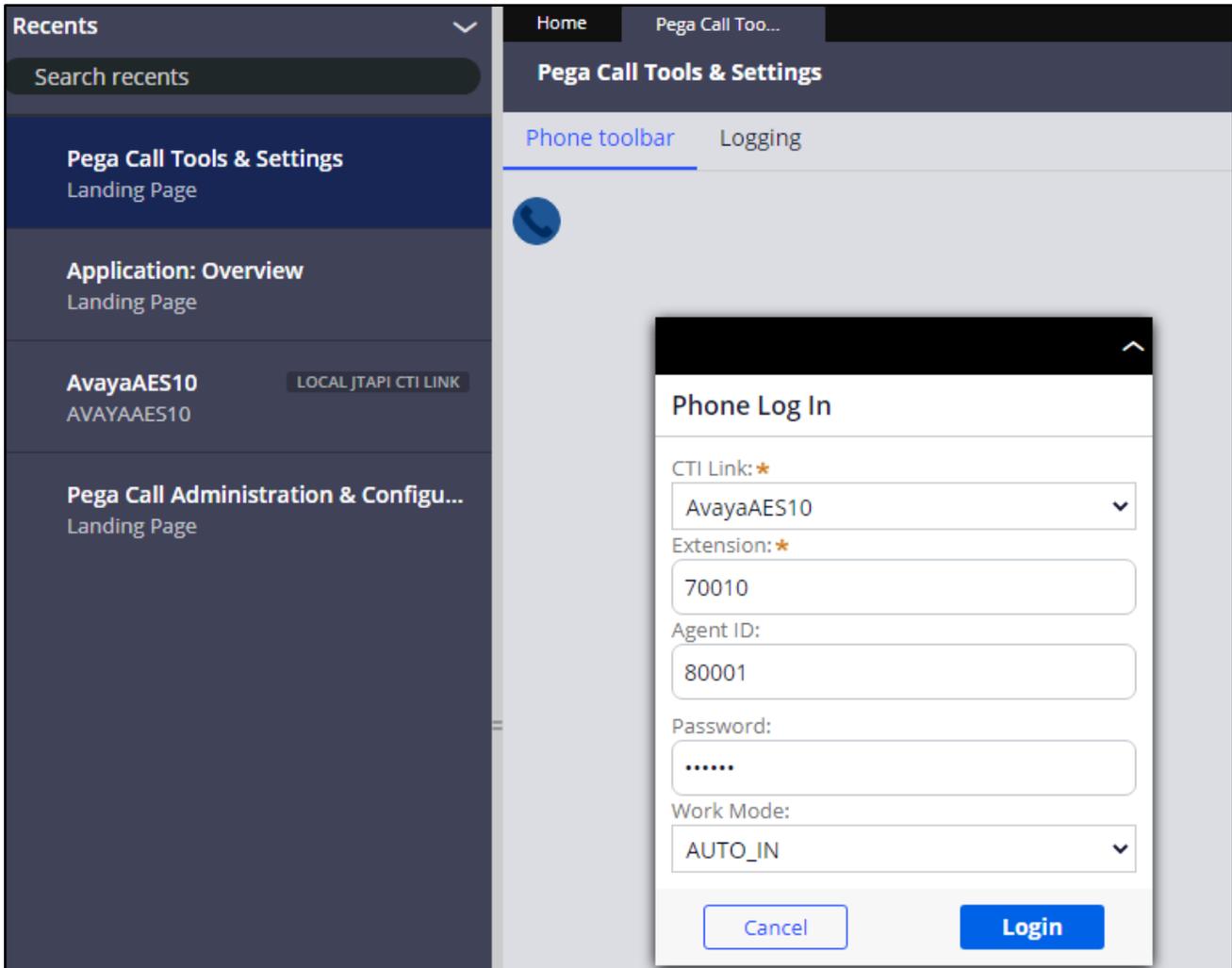
8.3. Verify Pegasystems Pega Call

From the agent PC, follow the procedures in **Section 7.1** to launch the web-based interface, and log in using the appropriate user credentials. Select **DEV STUDIO** → **Channel Services** → **Pega Call** → **Tools and Settings** from the top menu.

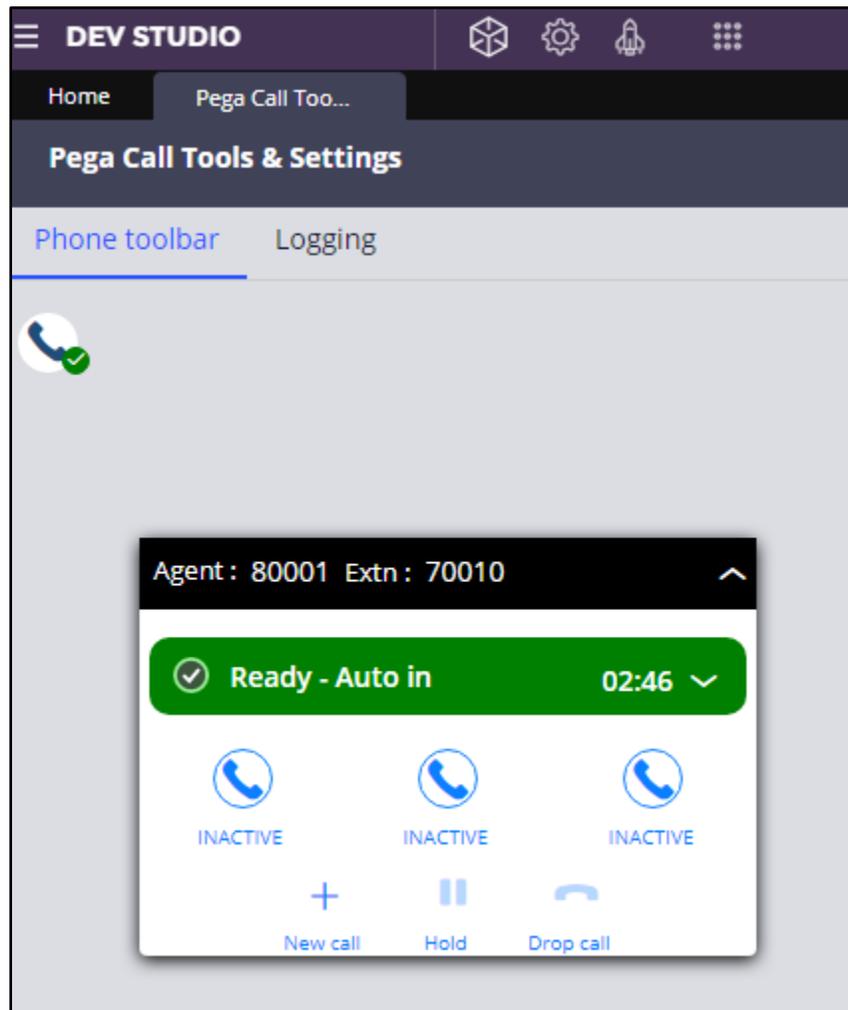


The **Phone Login** pop-up box is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields. Click **Login**.

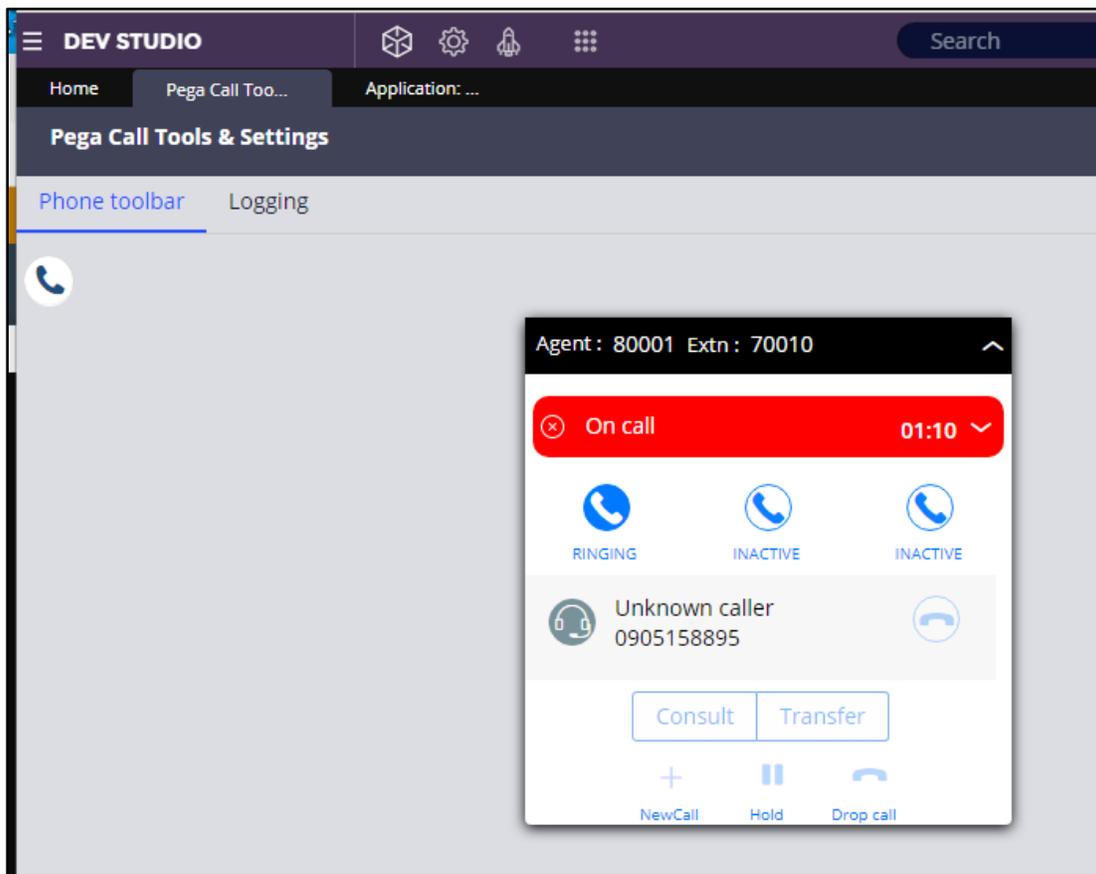
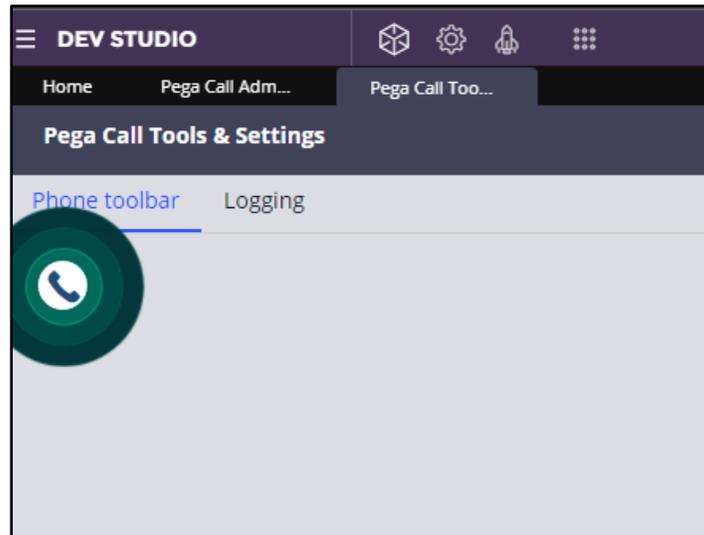
- **CTI Link:** Select the CTI link from **Section 7.2**.
- **Extension:** The relevant agent station extension from **Section 3**.
- **Agent ID:** The relevant agent ID from **Section 3**.
- **Password:** The relevant agent password from **Section 3**.
- **Work Mode:** Select the desired work mode, in this case “AUTO_IN”.



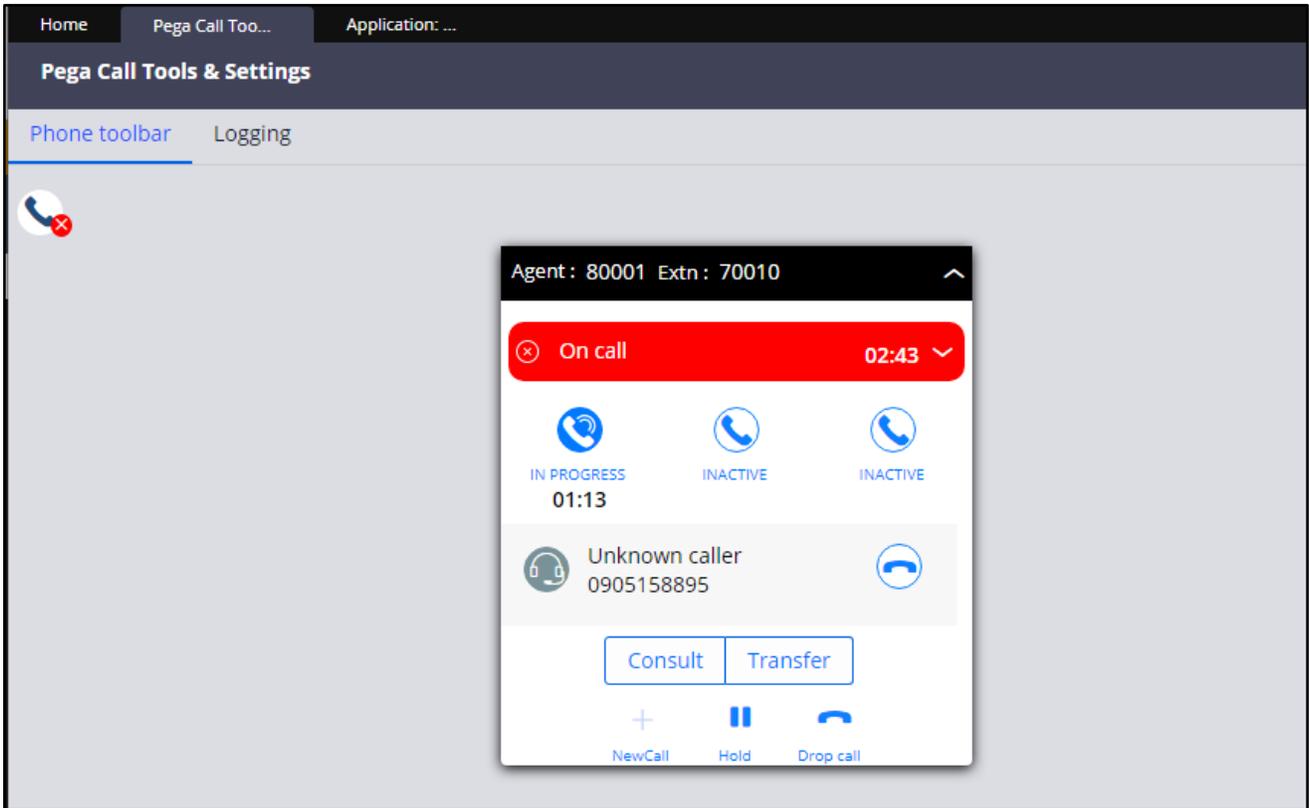
Verify that the screen is updated as shown below with a green handset icon and Agent status show as **Ready - Auto in** indicating the agent is logged in and available for ACD calls.



Make an incoming call from the PSTN to one of the routing VDNs. Verify that the call is ringing at the available agent's telephone. Also verify that a pop-up box is displayed on the agent desktop with proper call information, as shown below.



Press **RINGING** (not shown) line to connect the call. Verify that the agent is connected to the PSTN with two-way talk path, and that the agent screen is updated with **IN PROGRESS** line as shown below.



9. Conclusion

These Application Notes describe the configuration steps required for the Pegasystems Pega Call 8.7 to successfully interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

This section references the Avaya and Pega product documentation that are relevant to these Application Notes.

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

1. *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 1, Dec 2021
2. *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 3, April 2022
3. *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 6, June 2022
4. *Administering Avaya Aura® Application Enablement Services*, Release 10.1.x, Issue 4, April 2022
5. *Pega Call Configuration and Operations Guide for CTI Link Engine with Avaya AES CTI*, Software Version 7.21, May 2016, available at <https://pdn.pega.com>.
6. *Pega 8.7 platform Help for application developers*, available as part of the Pegasystems web interface and at <https://pdn.pega.com>.

©2022 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.