



Avaya Solution & Interoperability Test Lab

Application Notes for Pegasystems Pega Call 7.21 with Avaya Aura® Application Enablement Services 7.0 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Pegasystems Pega Call 7.21 to interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0. 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 7.21 to interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0. 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 this compliance test.

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 the 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.

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. 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.
- In the serviceability scenarios where the server or client experienced an Ethernet disruption, the agent may need to press the Refresh button from the Phone Toolbar application to synchronize call status post recovery.

2.3. Support

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

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

3. Reference Configuration

Pega Call can be configured on a single server or with components distributed across multiple servers. The compliance test configuration used a single server configuration.

The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of contact center devices are 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	60001, 60002
Skill Group	61001, 61002
Agent Station	65001, 66002
Supervisor Station	65000
Agent ID and Password	65881, 65882

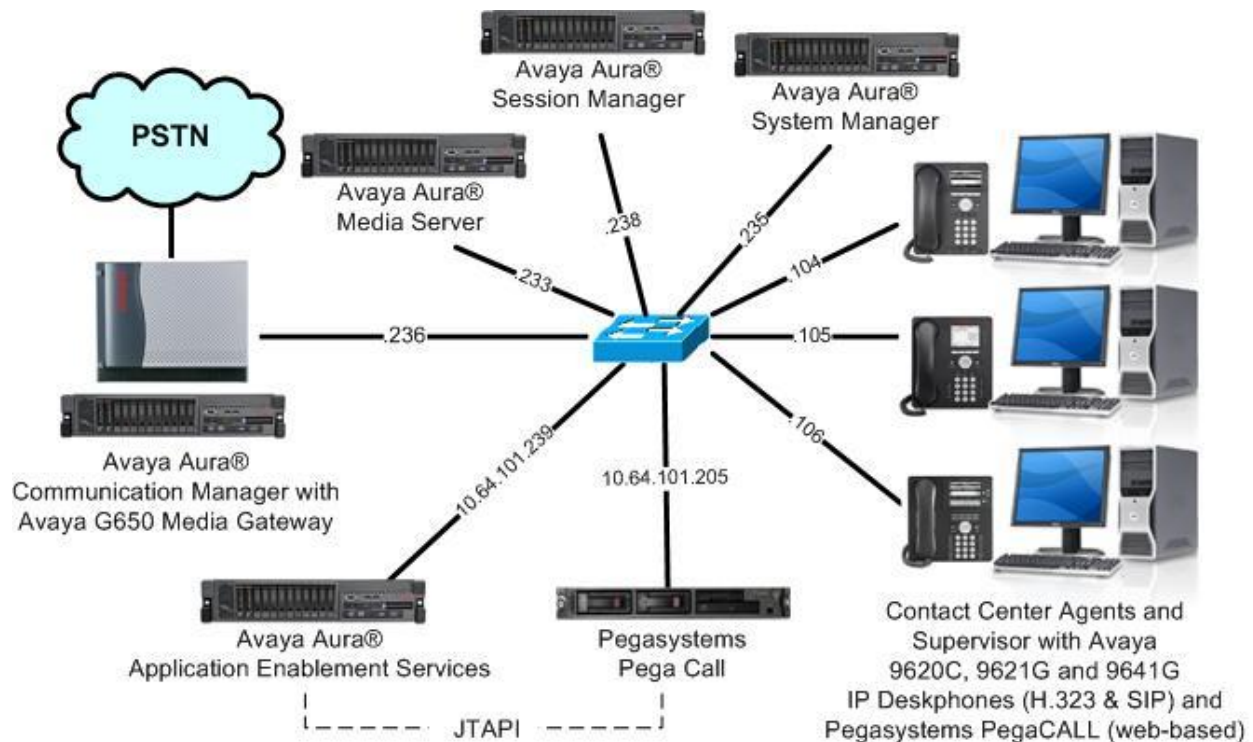


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	7.0.1.1 (7.0.1.1.0.441.23169)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	7.7.0.334
Avaya Aura® Application Enablement Services in Virtual Environment	7.0.1 (7.0.1.0.2.15-0)
Avaya Aura® Session Manager in Virtual Environment	7.0 .1.1 (7.0.1.1.701114)
Avaya Aura® System Manager in Virtual Environment	7.0 .1.1 (7.0.1.1.065378)
Avaya 9620C IP Deskphone (H.323)	3.270B
Avaya 9641G IP Deskphone (H.323)	6.6302
Avaya 9621G IP Deskphone (SIP)	7.0.1.2.9
Pegasystems Pega Call on CentOS <ul style="list-style-type: none">• Avaya JTAPI Client (ecsjtapia.jar)• Apache Tomcat• PostgreSQL	7.21 6.8 7.0.0.64 7.0.72 9.3.14

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 vectors and VDNs

5.1. Verify License

Log into the System Access Terminal (SAT) 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? 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	

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: 7.0	
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

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: 2
Extension: 60111
  Type: ADJ-IP
                                         COR: 1
  Name: AES CTI Link
```

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.

```
display 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: 27
```

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? y
    Call Classification After Answer Supervision? y
        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 Break   /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 Vectors and VDNs

This section is only applicable to contact centers that use the Enhanced Routing feature from Pega Call.

Modify an available vector using the “change vector n” command, where “n” is an existing vector number. The vector will be used to provide routing to the CTI link defined in **Section 5.2**. Note that the vector steps may vary, and below is a sample vector used in the compliance testing.

```
change vector 1                                     Page 1 of 6

                                CALL VECTOR

Number: 1                      Name: Pega Sales
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 ringback
04 route-to         number 65000              with cov n if unconditionally
05
```

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 60001                                     Page 1 of 3

                                VECTOR DIRECTORY NUMBER

Extension: 60001
Name*: Pega Sales
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
```

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 60001 count 2

                                VECTOR DIRECTORY NUMBERS
```

Name (22 characters)	Ext/Skills	VDN Ovr	COR	TN	Vec PRT Num	Meas	Orig Annc	Evt Noti Adj
Pega Sales	60001	n	1	1	V 1	none		
Pega Support	60002	n	1	1	V 2	none		

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
- Restart service
- Obtain Tlink name
- Administer Pega Call user
- Verify security database

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. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A thick red horizontal bar spans the width of the page. Below this bar is a light gray rectangular box containing the login form. The form has the text "Please login here:" followed by two input fields: "Username" and "Password". Below these fields are two buttons: "Login" and "Reset". Another thick red horizontal bar is located below the login box. At the bottom of the page, centered, is the copyright notice: "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A red navigation bar at the top contains "Home", "Help", and "Logout" links. On the left, a sidebar menu lists various services: 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 provides an overview of the OAM Web interface, listing administrative domains and their functions. A list of bullet points details the capabilities of each domain: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. A note at the bottom states that these domains can be managed by a single administrator or separate administrators.

Welcome: User
Last login: Tue Nov 15 09:43:19 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Nov 15 11:53:05 EST 2016
HA Status: Not Configured

Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Welcome to OAM

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

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

6.2. Verify License

Select **Licensing** → **WebLM Server Access** in the left pane, to display the **Web License Manager** pop-up screen (not shown), and log in using the appropriate credentials.

The screenshot displays the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the sidebar. The main content area is titled "Licensing" and provides instructions on how to set up and maintain the WebLM. It includes a list of bullet points for the required information: WebLM Server Address, WebLM Server Access, and Reserved Licenses. A note at the bottom states that these domains can be managed by a single administrator or separate administrators.

Welcome: User
Last login: Tue Nov 15 09:43:19 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Nov 15 11:53:05 EST 2016
HA Status: Not Configured

Licensing | Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking

Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

Verify that there are sufficient licenses for **TSAPI Simultaneous Users**, as shown below. Also verify that there is an applicable advanced switch license, in this case **AES ADVANCED LARGE SWITCH**.

TLT; Reviewed:
SPOC 12/13/2016

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 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 for the user. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area displays the "TSAPI Links" screen, which includes a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
------	-------------------	-------------------	-------------------	----------

Buttons: Add Link, Edit Link, Delete 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 "cm7" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.

The screenshot shows the "Add TSAPI Links" screen in the Avaya Application Enablement Services Management Console. The left navigation pane is the same as the previous screenshot. The main content area displays the "Add TSAPI Links" form, which includes fields for Link, Switch Connection, Switch CTI Link Number, ASAI Link Version, and Security. The values entered are: Link: 1, Switch Connection: cm7, Switch CTI Link Number: 1, ASAI Link Version: 7, and Security: Unencrypted. There are buttons for "Apply Changes" and "Cancel Changes".

Fields and values:

- Link: 1
- Switch Connection: cm7
- Switch CTI Link Number: 1
- ASAI Link Version: 7
- Security: Unencrypted

Buttons: Apply Changes, Cancel Changes

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 header includes the Avaya logo and the title "Application Enablement Services Management Console". A welcome message in the top right corner provides user information: "Welcome: User", "Last login: Tue Nov 15 09:43:19 2016 from 192.168.200.20", "Number of prior failed login attempts: 0", "HostName/IP: aes7/10.64.101.239", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 7.0.1.0.2.15-0", "Server Date and Time: Tue Nov 15 11:53:05 EST 2016", and "HA Status: Not Configured".

The main interface features a left-hand navigation pane with a tree structure. The "Networking" section is expanded, showing sub-items: "AE Service IP (Local IP)", "Network Configure", "Ports", "TCP/TLS Settings" (highlighted in blue), "Security", "Status", "User Management", "Utilities", and "Help".

The right-hand pane displays the "TCP / TLS Settings" configuration page. It includes the following sections:

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

Below the configuration options are three buttons: "Apply Changes", "Restore Defaults", and "Cancel Changes".

A note at the bottom of the page 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. Restart Service

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A welcome message in the top right corner provides user information and system details. The left navigation pane shows a tree structure with "Maintenance" expanded and "Service Controller" selected. The main content area, titled "Service Controller", contains a table of services and their statuses. The "TSAPI Service" is checked. Below the table, there is a link to "Status and Control" and a row of buttons including "Restart Service".

Welcome: User
Last login: Tue Nov 15 09:43:19 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Nov 15 11:53:05 EST 2016
HA Status: Not Configured

Maintenance | Service Controller Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Date Time/NTP Server
Security Database
Service Controller
Server Data
Networking
Security
Status

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](#)

Start Stop Restart Service Restart AE Server Restart Linux Restart Web Server

6.6. 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#CM7#CSTA#AES7”. Note the use of the switch connection “CM7” from **Section 6.3** as part of the Tlink name.

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 a welcome message for the user. The main navigation pane on the left lists various services, with "Security" expanded to show "Security Database" and "Tlinks" selected. The main content area shows the "Tlinks" page with a single Tlink named "AVAYA#CM7#CSTA#AES7" and a "Delete Tlink" button.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Nov 15 09:43:19 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Nov 15 11:53:05 EST 2016
HA Status: Not Configured

Security | Security Database | Tlinks 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
Device Groups
Tlinks

Tlinks

Tlink Name
AVAYA#CM7#CSTA#AES7
Delete Tlink

6.7. Administer Pega Call 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.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Nov 15 09:43:19 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Nov 15 11:51:10 EST 2016
HA Status: Not Configured

User Management | User Admin | Add UserHome | Help | Logout

▶ 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 Idpegacall

* Common Namepegacall

* Surnamepegacall

* User Password.....

* Confirm Password.....

Admin Note

Avaya RoleNone ▼

Business Category

Car License

CM Home

Css Home

CT UserYes ▼

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

6.8. Verify Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane.

Make certain that **Enable SDB for TSAPI Service, JTAPI and Telephony Web Services** is unchecked. In the event that the parameter is enabled with security database used by the customer, then follow reference [2] to configure access privileges for the Pega Call user from **Section 6.7**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A welcome message and system information are shown in the top right corner. The main navigation pane on the left lists various services, with "Security" expanded to show "Security Database" and "Control" selected. The main content area displays the "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" configuration page, which includes two unchecked checkboxes and an "Apply Changes" button.

Welcome: User
Last login: Tue Nov 15 09:43:19 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Nov 15 11:51:10 EST 2016
HA Status: Not Configured

Security | Security Database | Control [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**

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

☐ Enable SDB for DMCC Service

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

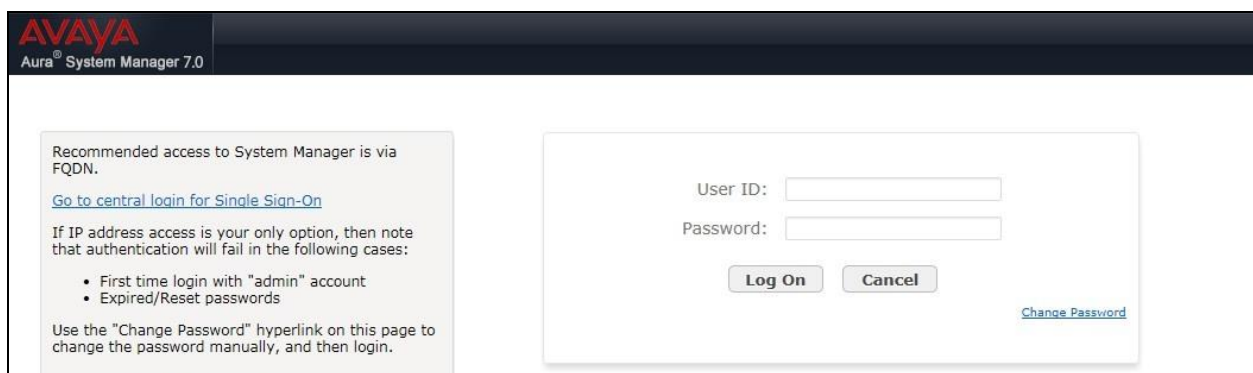
7. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer users

7.1. Launch System Manager

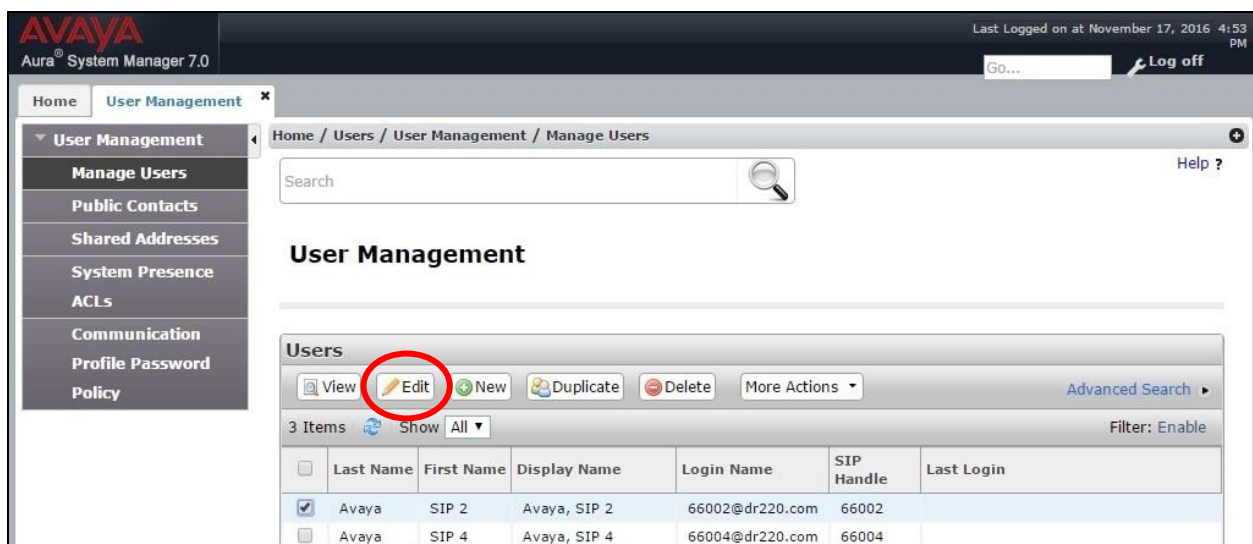
Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.



The screenshot shows the Avaya Aura System Manager 7.0 login page. On the left, there is a text box with instructions: "Recommended access to System Manager is via FQDN. Go to central login for Single Sign-On. If IP address access is your only option, then note that authentication will fail in the following cases: • First time login with 'admin' account • Expired/Reset passwords. Use the 'Change Password' hyperlink on this page to change the password manually, and then login." On the right, there is a login form with fields for "User ID:" and "Password:", a "Log On" button, a "Cancel" button, and a "Change Password" hyperlink.

7.2. Administer Users

In the subsequent screen (not shown), select **Users** → **User Management**. Select **User Management** → **Manage Users** from the left pane to display the **User Management** screen below. Select the entry associated with the first SIP agent station from **Section 3**, in this case “66002”, and click **Edit**.



The screenshot shows the Avaya Aura System Manager 7.0 User Management screen. The left navigation pane has "User Management" selected, with "Manage Users" highlighted. The main content area shows the "User Management" title and a search bar. Below the title, there is a "Users" section with a table of users. The "Edit" button in the "Users" section is circled in red. The table has columns: Last Name, First Name, Display Name, Login Name, SIP Handle, and Last Login. There are 3 items in the table.

	Last Name	First Name	Display Name	Login Name	SIP Handle	Last Login
<input checked="" type="checkbox"/>	Avaya	SIP 2	Avaya, SIP 2	66002@dr220.com	66002	
<input type="checkbox"/>	Avaya	SIP 4	Avaya, SIP 4	66004@dr220.com	66004	

The **User Profile Edit** screen is displayed. Select the **Communication Profile** tab to display the screen below.

Navigate to the **CM Endpoint Profile** sub-section, and click **Endpoint Editor**.

AVAYA
Aura® System Manager 7.0

Last Logged on at November 17, 2016 4:53 PM
Go... Log off

Home User Management x

Home / Users / User Management / Manage Users

Help ?

User Profile Edit: 66002@dr220.com Commit & Conf

Identity * Communication Profile Membership Contacts

Communication Profile

Communication Profile Password: Edit

New Delete Done Cancel

Name

Primary

Select : None

* Name: Primary

Default : ☒

Communication Address

New Edit Delete

Type	Handle	Domain
Avaya SIP	66002	dr220.com

Select : All, None

☒ **Session Manager Profile**

☒ **CM Endpoint Profile**

* System DR220-CM7-ES

* Profile Type Endpoint

Use Existing Endpoints ☐

* Extension 66002 **Endpoint Editor**

Template Select/Reset

Set Type 9621SIPCC

The **Edit Endpoint** screen is displayed next. For **Type of 3PCC Enabled**, select “Avaya” from the drop-down list as shown below. Retain the default values in the remaining fields.

Repeat this section for all SIP agent users.

The screenshot shows the Avaya Aura System Manager 7.0 interface. The top navigation bar includes 'Home', 'User Management', and a breadcrumb trail 'Home / Users / User Management / Manage Users'. The left sidebar lists various management options: 'Manage Users', 'Public Contacts', 'Shared Addresses', 'System Presence', 'ACLs', 'Communication', 'Profile Password', and 'Policy'. The main content area is titled 'Edit Endpoint' and contains several input fields for user configuration. The 'System' field is set to 'DR220-CM7-ES', 'Extension' to '66002', 'Set Type' to '9621SIPCC', 'Port' to 'S00004', and 'Name' to 'Avaya, SIP 2'. Below these fields is a tabbed interface with four tabs: 'General Options (G)', 'Feature Options (F)', 'Site Data (S)', and 'Abbreviated Call Dialing (A)'. The 'General Options (G)' tab is active and contains two columns of settings. The 'Type of 3PCC Enabled' dropdown is highlighted with a red circle. Other settings include 'Class of Restriction (COR)', 'Emergency Location Ext.', 'Tenant Number', 'SIP Trunk', 'Coverage Path 1', 'Lock Message', 'Multibyte Language', 'Class Of Service (COS)', 'Message Lamp Ext.', 'Coverage Path 2', 'Localized Display Name', and 'Enable Reachability for Station Domain Control'. The bottom of the screen has 'Done' and 'Cancel' buttons.

General Options (G) *		Feature Options (F)		Site Data (S)		Abbreviated Call Dialing (A)	
Enhanced Call Fwd (E)		Button Assignment (B)		Profile Settings (P)		Group Membership (M)	
* Class of Restriction (COR)	1	* Class Of Service (COS)	1				
* Emergency Location Ext	66002	* Message Lamp Ext.	66002				
* Tenant Number	1	Type of 3PCC Enabled	Avaya				
* SIP Trunk	Qaar	Coverage Path 2					
Coverage Path 1	1	Localized Display Name	Avaya, SIP 2				
Lock Message	<input type="checkbox"/>	Enable Reachability for Station Domain Control	system				
Multibyte Language	Not Applicable						

8. 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

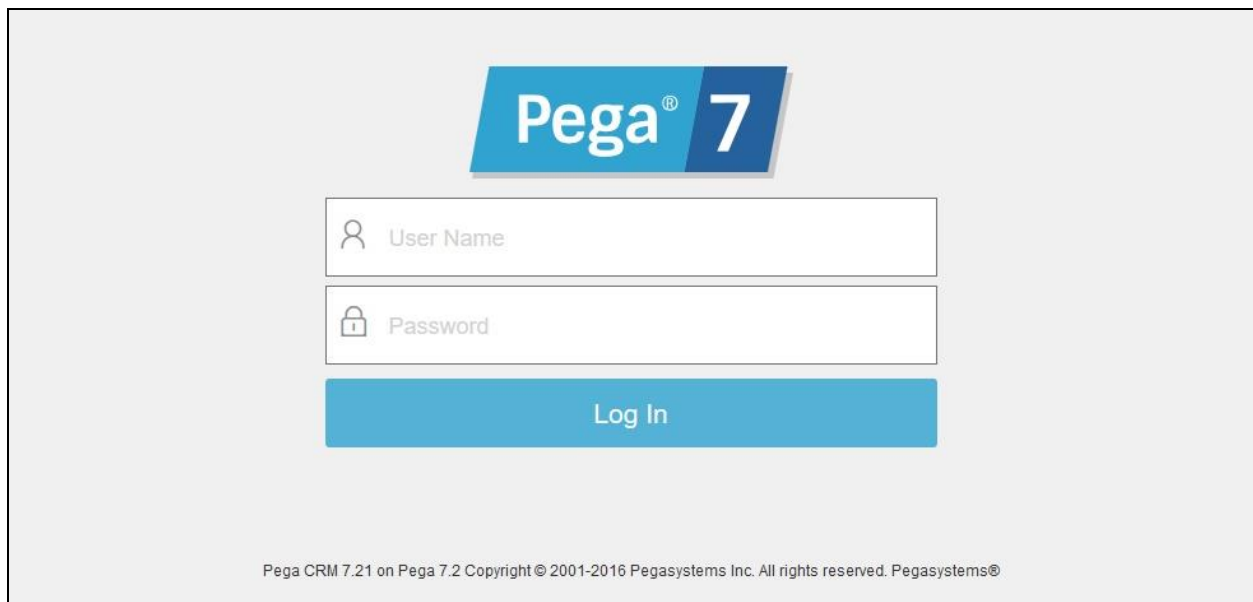
The configuration of Pega Call is performed by Pegasystems service personnel. The procedural steps are presented in these Application Notes for informational purposes.

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.

8.1. 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.

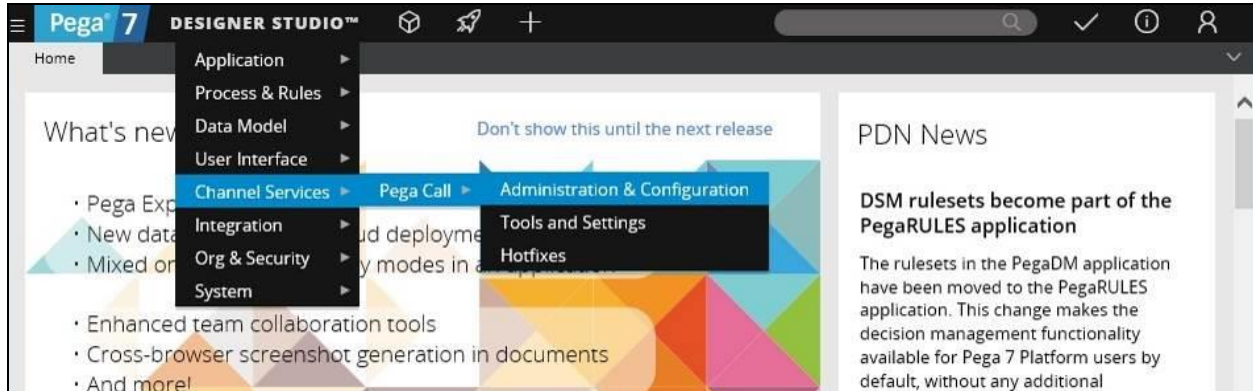
The screen below is displayed. Log in using the administrator credentials.

The image shows a web-based login interface for Pega 7. At the top center is the Pega 7 logo, which consists of the word "Pega" in white on a blue background, followed by a large blue square containing the number "7". Below the logo are two input fields: the first is labeled "User Name" with a person icon, and the second is labeled "Password" with a lock icon. Below these fields is a blue button labeled "Log In". At the bottom of the screen, there is a small line of text: "Pega CRM 7.21 on Pega 7.2 Copyright © 2001-2016 Pegasystems Inc. All rights reserved. Pegasystems®".

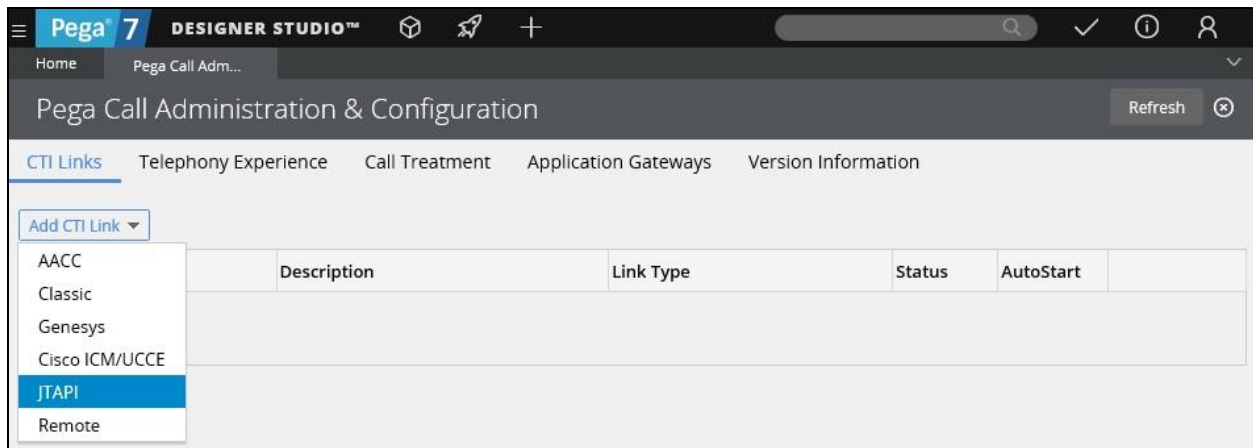
Pega CRM 7.21 on Pega 7.2 Copyright © 2001-2016 Pegasystems Inc. All rights reserved. Pegasystems®

8.2. Administer CTI Link

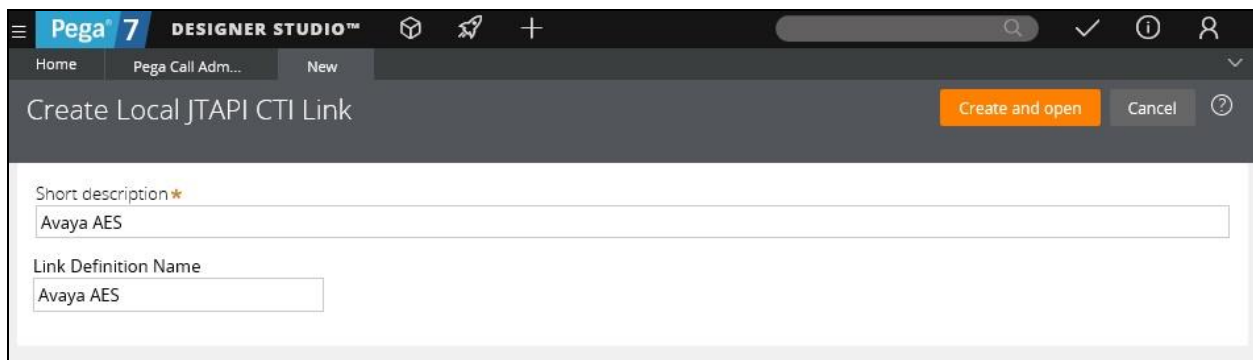
The screen below is displayed next. Select **DESIGNER STUDIO** → **Channel Services** → **Pega Call** → **Administration & Configuration** from the top menu.



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



The **Create Local JTAPI CTI Link** screen is displayed. Enter desired values for **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 6.6**.
- **AES User ID:** The Pega Call user credentials from **Section 6.7**.
- **Password:** The Pega Call user credentials from **Section 6.7**.
- **Enable UCID Support:** Check when both UCID settings in **Section 5.3** are enabled.

The screenshot shows the Pega Designer Studio interface for editing a JTAPI CTI Link. The title bar indicates 'Pega 7 DESIGNER STUDIO™'. The main header shows 'Edit Local JTAPI CTI Link: Avaya AES' with a 'Save' button and an 'Actions' dropdown. Below the header, there are tabs for 'Link Configuration', 'Failover', 'Logging', 'RoutePoints', 'Peering', 'Switch Capabilities', 'Phone Books', 'Advanced', and 'Rec'. The 'Link Configuration' tab is active, showing the following fields:

- Enabled:** ☒
- Auto Start:** ☒
- JTAPI Vendor:** Avaya AES (dropdown)
- Avaya AES Connectivity:**
 - AES Server Host Name:** 10.64.101.239
 - Port:** 450
 - TLINK:** AVAYA#CM7#CSTA#AES7
 - AES User ID:** pegacall
 - Password:** (masked with dots)
 - Connection Timeout (s):** 60
 - Retry Interval (s):** 60
 - Enable UCID Support:** ☒
- Site ID:** (empty field)
- Dial Plan:** (empty field)
- Desktop Heartbeats:**
 - Enabled:** ☒
 - Heartbeat Interval (s):** 60
 - Heartbeat Timeout (s):** 300
 - Behavior upon timeout:** Unmonitor device (stop event subscription) (dropdown)

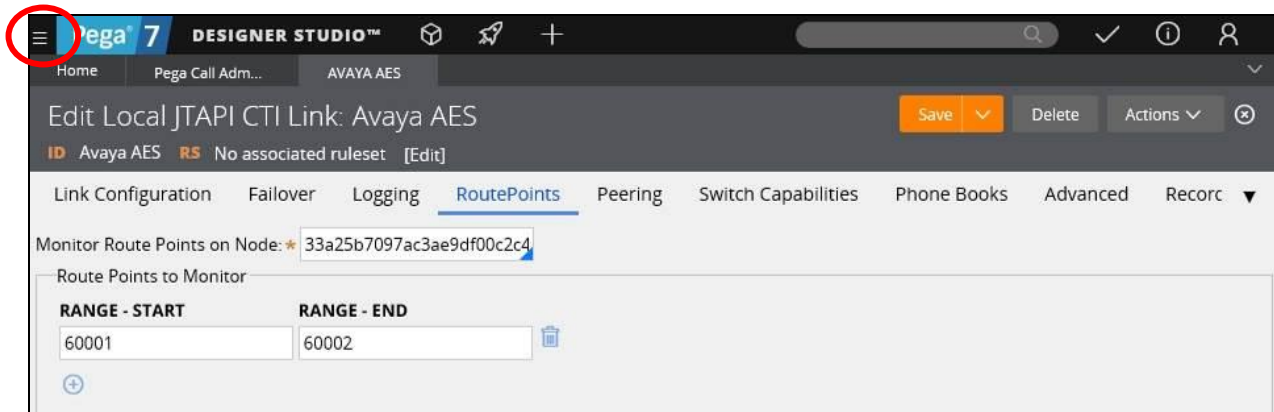
At the bottom, there is a 'Test Connectivity' button and a footer with icons for 'Inspection Prefs', 'PDN', and 'Pega 7.2'.

8.3. Administer Route Points

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

Select the **RoutePoints** 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 5.5**.

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.

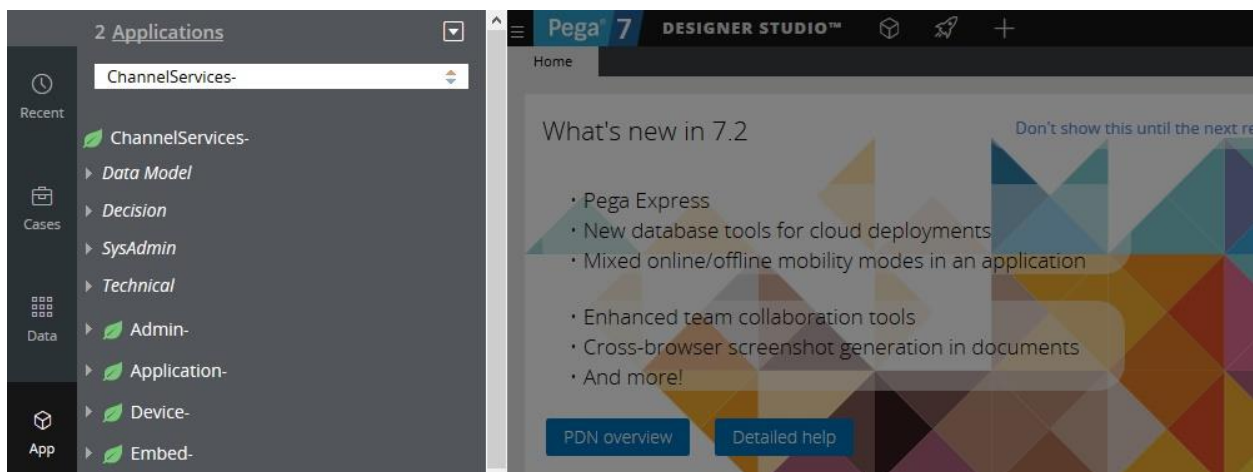


8.4. Administer Decision Tree

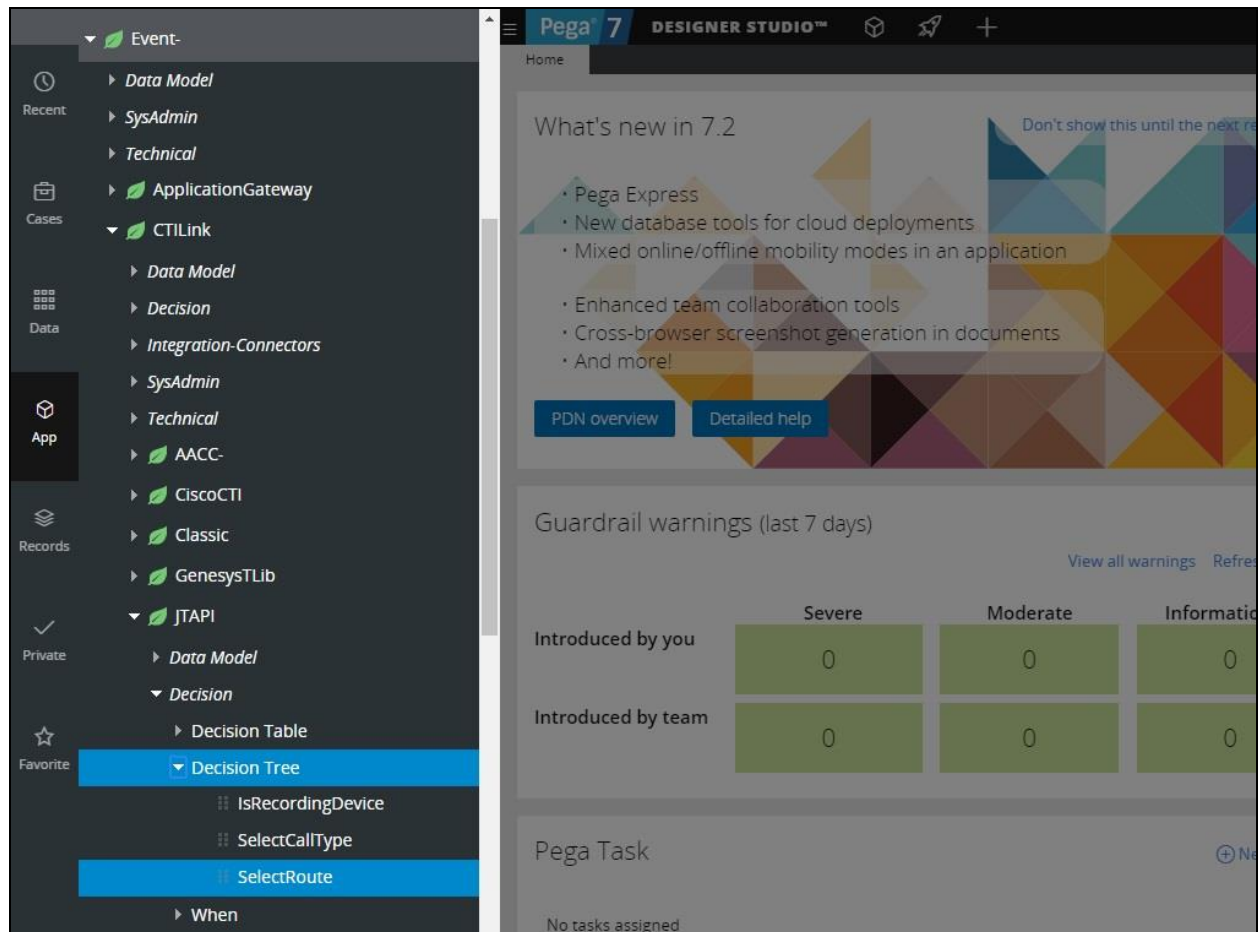
This section is only applicable to systems that use the Enhanced Routing feature.

Prior to administering decision tree, follow reference [4] to create a RuleSet, which is a set of rule 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, and enter “ChannelServices-” in the search area shown below.



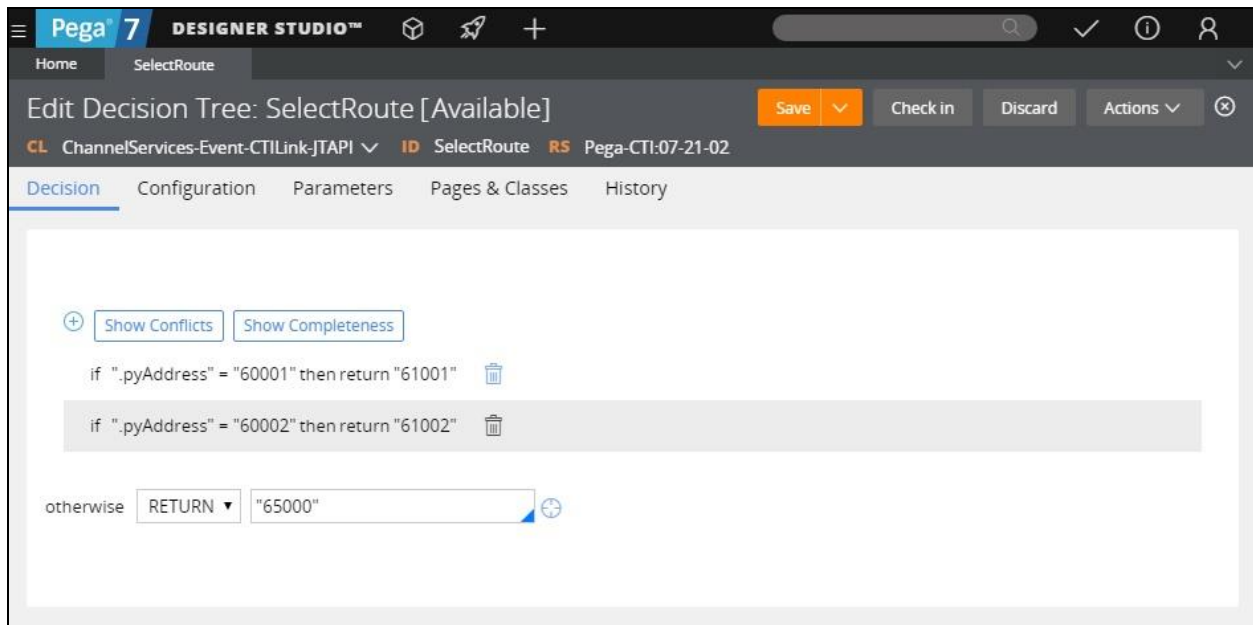
Scroll down the left pane and select **Event** → **CTILink** → **JTAPI** → **Decision** → **Decision Tree** → **SelectRoute**.



The **Decision Tree: SelectRoute** screen is displayed. Follow reference [4] 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 5.5**.

As shown in **Section 3**, extensions **61001** and **61002** are existing skill groups on Communication Manager, and extension **65000** is the supervisor.



9. Verification Steps

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

9.1. Verify Avaya Aura® Communication Manager

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


```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	7	no	aes7	established	61	59

9.2. Verify Avaya Aura® Application Enablement Services

Log in at least one agent using Pega Call as described in **Section 8.3**. On Application Enablement Services, verify status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane (not shown). 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
Last login: Thu Nov 17 09:16:01 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Thu Nov 17 10:07:01 EST 2016
HA Status: Not Configured

Status | Status and Control | TSAPI Service SummaryHome | Help | Logout

▶ AE Services

▶ Communication Manager

▶ Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Log Manager

▶ Logs

▼ Status and Control

TSAPI Link Details

☐ Enable page refresh every 60 seconds

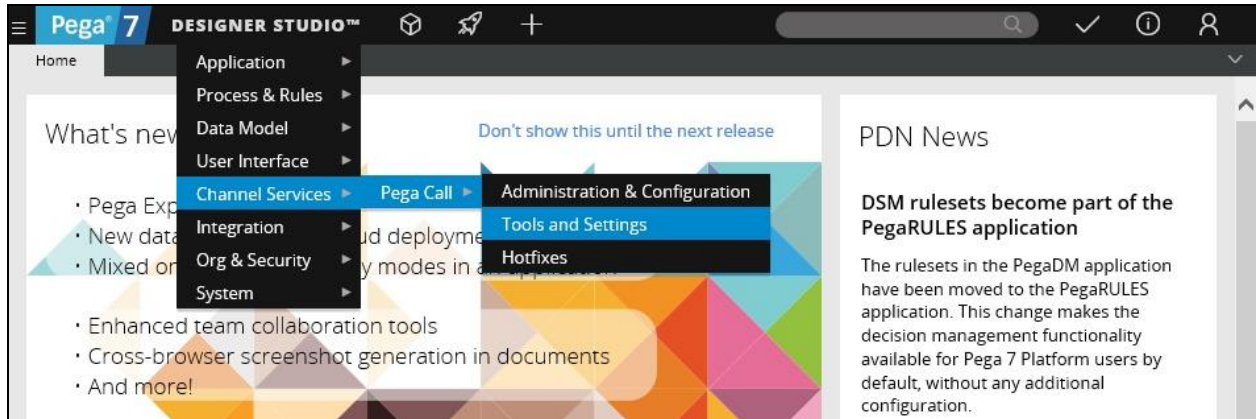
	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	cm7	1	Talking	Tue Nov 15 16:47:55 2016	Online	17	2	59	61	30

Online Offline

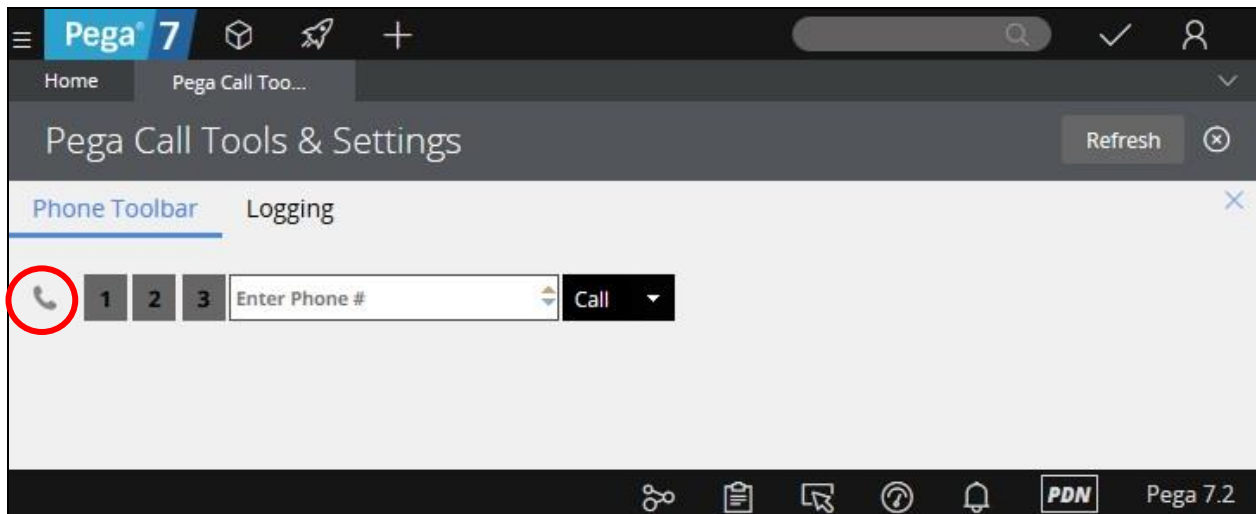
For service-wide information, choose one of the following:
TSAPI Service Status TLink Status User Status

9.3. Verify Pegasystems Pega Call

From the agent PC, follow the procedures in **Section 8.1** to launch the web-based interface, and log in using the appropriate user credentials. Select **DESIGNER STUDIO → Channel Services → Pega Call → Tools and Settings** from the top menu.

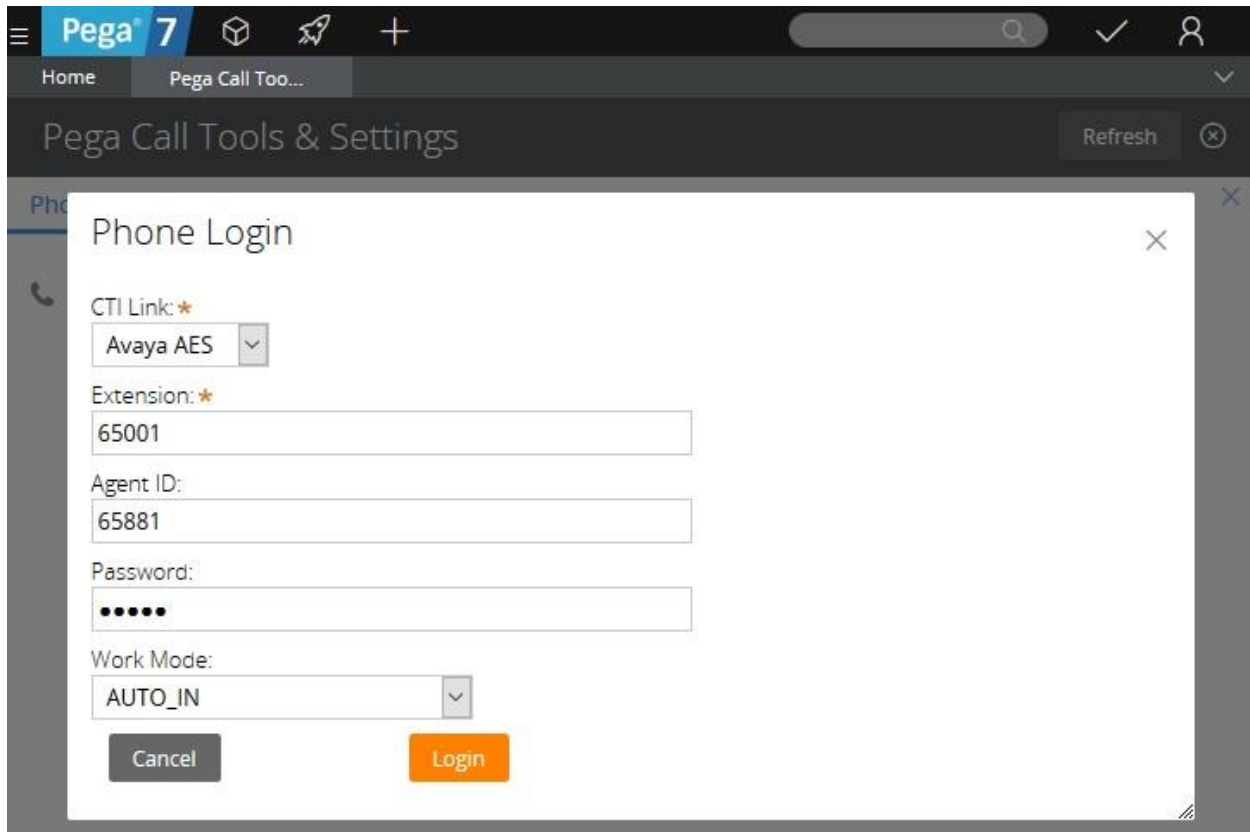


The screen is updated with a **Tools** tab, as shown below. Click on the grey handset icon.



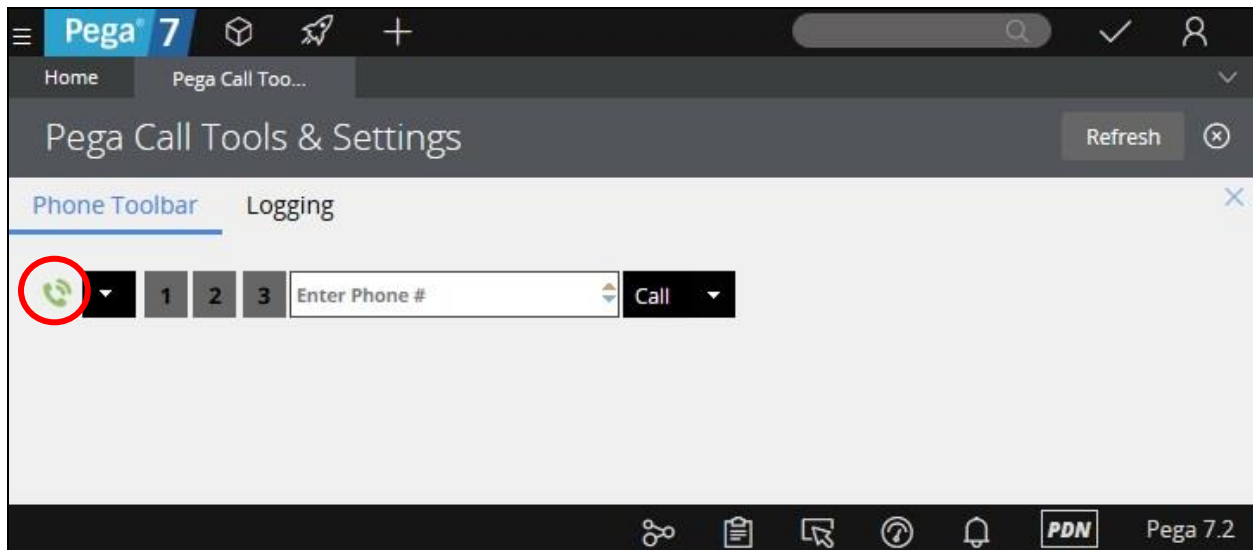
The **Phone Login** pop-up box is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields. Click **Login**.

- **CTI Link:** Select the CTI link from **Section 8.2**.
- **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”.

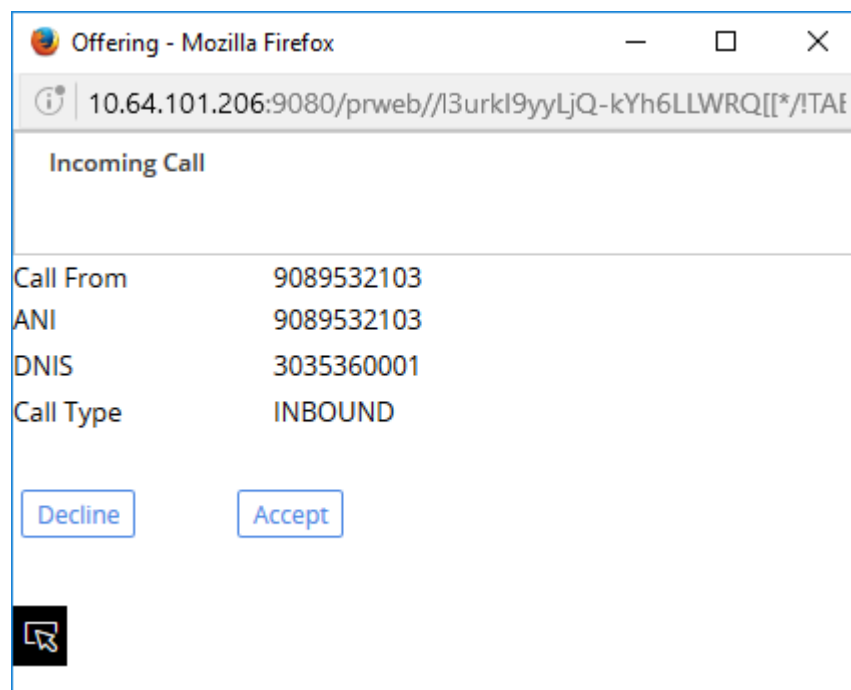


The screenshot shows the Pega 7 user interface. At the top, there is a navigation bar with the Pega logo and version number 7. Below it, a breadcrumb trail shows 'Home' and 'Pega Call Too...'. The main header area is titled 'Pega Call Tools & Settings' and includes a 'Refresh' button. A 'Phone Login' pop-up box is open in the foreground. It contains the following fields: 'CTI Link' with a dropdown menu showing 'Avaya AES'; 'Extension' with a text input field containing '65001'; 'Agent ID' with a text input field containing '65881'; 'Password' with a text input field containing masked characters (dots); and 'Work Mode' with a dropdown menu showing 'AUTO_IN'. At the bottom of the pop-up are two buttons: 'Cancel' and 'Login'.

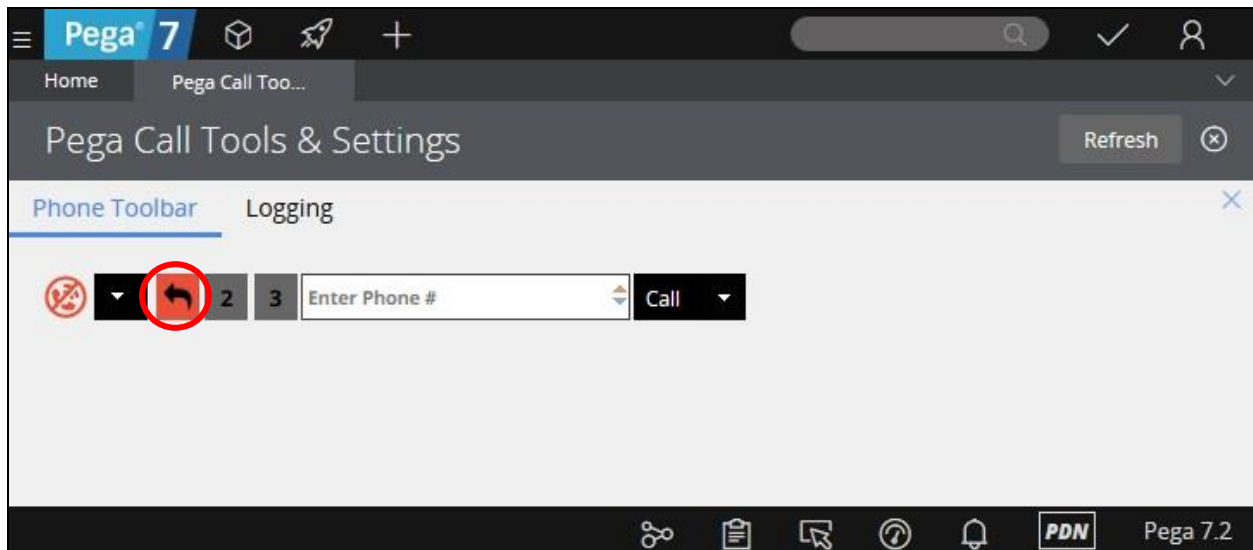
Verify that the screen is updated as shown below with a green handset icon, indicating the agent is logged in and available for ACD calls.



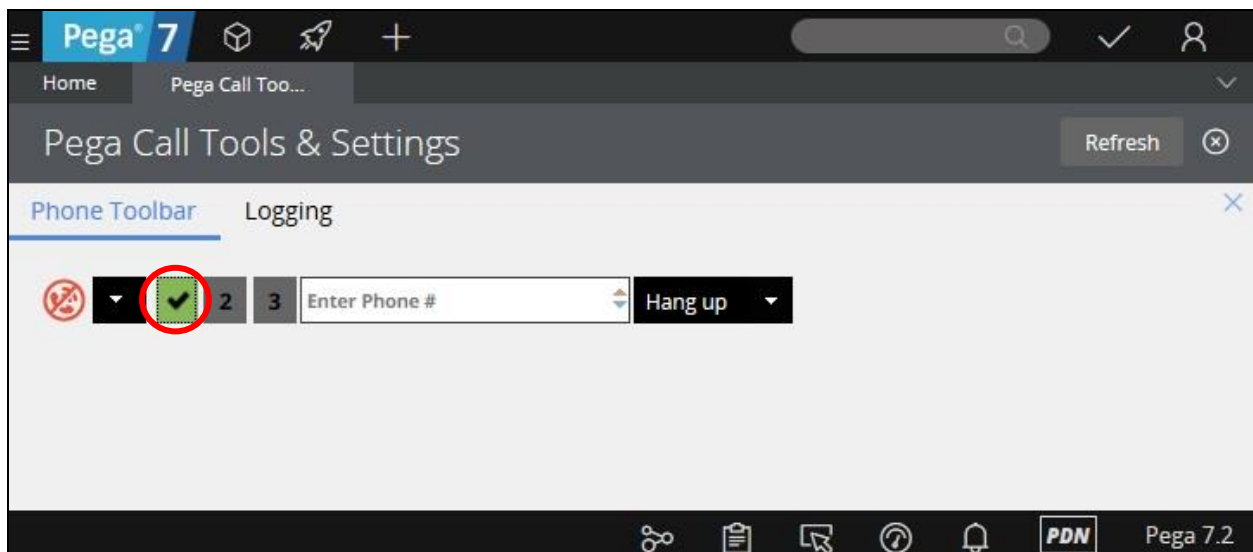
Make an incoming call from the PSTN to one of the routing VDNs. Verify that the call is ringing at the available agent's telephone. Also verify that a pop-up box is displayed on the agent desktop with proper call information, as shown below.



In addition, verify that the agent screen is updated, with flashing red on the applicable call appearance icon. Click on the red call appearance icon.



Verify that the agent is connected to the PSTN with two-way talk path, and that the agent screen is updated with solid green on the applicable call appearance icon, as shown below.



10. Conclusion

These Application Notes describe the configuration steps required for Pegasystems Pega Call 7.21 to successfully interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

11. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya Aura® Communication Manager*, Release 7.0.1, Issue 2.1, August 2016, available at <http://support.avaya.com>.
2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.0.1, Issue 2, August 2016, available at <http://support.avaya.com>.
3. *Pega Call Configuration and Operations Guide for CTI Link Engine with Avaya AES CTI*, Software Version 7.21, May 2016, available at <https://pdn.pegacom>.
4. *Pega 7 platform Help for application developers*, available as part of the Pegasystems web interface and at <https://pdn.pegacom>.

©2016 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.