



Application Notes for Pegasystems PegaCALL 7.1 with Avaya Aura® Application Enablement Services 6.3 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Pegasystems PegaCALL 7.1 to interoperate with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Application Enablement Services 6.3. Pegasystems PegaCALL provides telephony integration for Pegasystems' customer relationship and process management frameworks.

In the compliance testing, Pegasystems PegaCALL used the Java Telephony Application Programming Interface from Avaya Aura® Application Enablement Services to route incoming calls to Avaya Aura® Communication Manager, and provide call control via a thin client 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 PegaCALL 7.1 to interoperate with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Application Enablement Services 6.3. Pegasystems PegaCALL provides telephony integration for Pegasystems' customer relationship and process management frameworks.

In the compliance testing, Pegasystems PegaCALL used the Java Telephony Application Programming Interface (JTAPI) from Avaya Aura® Application Enablement Services to provide call control via a thin client web-based agent interface. The testing also included the optional Enhanced Routing feature on Pegasystems PegaCALL, which used JTAPI adjunct routing capabilities to route incoming calls to 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 and a sample routing rule. Any customized agent and routing applications developed using Pegasystems PegaCALL 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 that running the web-based PegaCALL. Manual call controls were exercised from PegaCALL 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 PegaCALL server and to the agent PC.

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 PegaCALL:

- 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 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 PegaCALL to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connections to the PegaCALL server and to the agents.

2.2. Test Results

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

- Setting the work mode to values other than the default AUTO_IN as part of initial login process did not take effect with agent placed in AUTO_IN. The workaround is to manually change the work mode to the desired state after logging in.
- The current implementation for population of DNIS requires the original dialed number to differ from the most recent, such as having a separate IVR application to vary the dialed number. The compliance testing environment did not include such application, and therefore DNIS was not populated in the testing.
- After dialing an invalid destination, the agent hears the reorder tone but cannot drop the active call from the application. The workaround is to manually drop the unsuccessful call via the phone.
- After blind transfer of an outbound call, the transfer-from agent browser page was not updated and continued to show an active call. The workaround is to manually refresh the page to reflect agent in idle state.

2.3. Support

Technical support on PegaCALL 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

PegaCALL 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, PegaCALL monitored the agent station extensions shown in the table below.

Device Type	Extension
Routing VDN	60001, 60002
Skill Group	65081, 65082
Agent Station	65001, 65002
Supervisor Station	65000
Agent ID and Password	65881, 65882

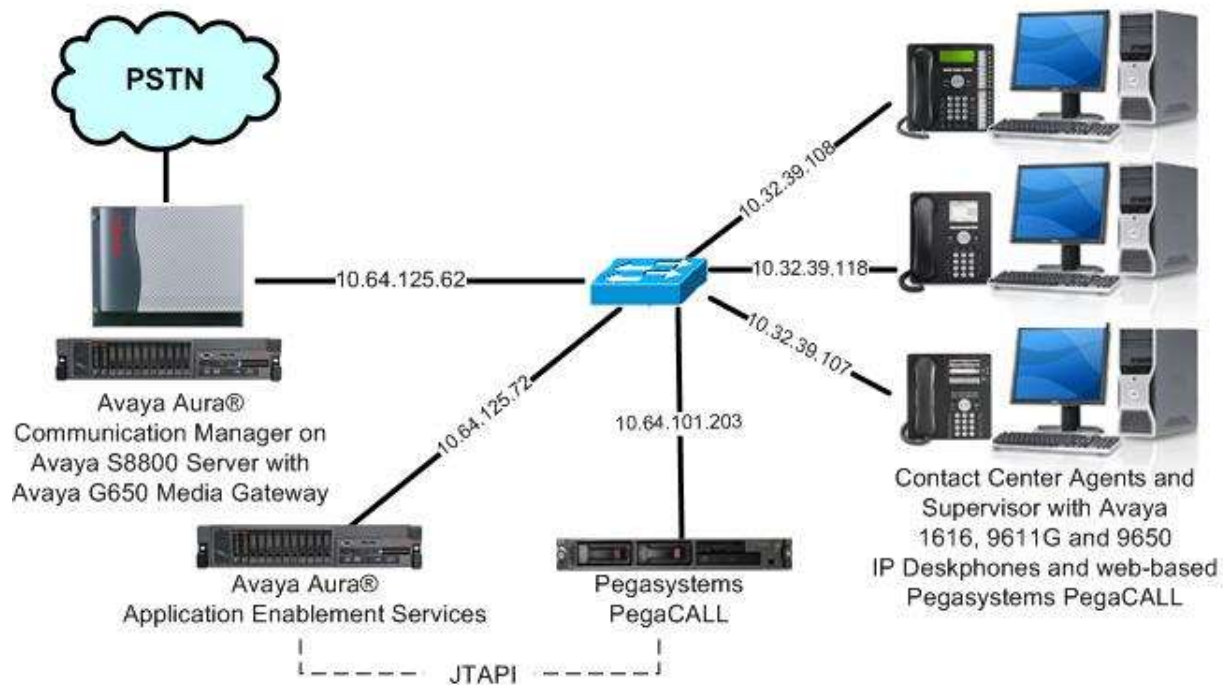


Figure 1: Compliance Testing Configuration

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 on Avaya S8800 Server with Avaya G650 Media Gateway	6.3.11 (R016x.03.0.124.0-22361)
Avaya Aura® Application Enablement Services	6.3.3 SP4 (6.3.3.4.10-0)
Avaya 1616 IP Deskphone (H.323)	1.350B
Avaya 9611G IP Deskphone (H.323)	6.4.0.14
Avaya 9650 IP Deskphone (H.323)	3.230A
Pegasystems PegaCALL on CentOS <ul style="list-style-type: none">• Avaya JTAPI Client (ecsjtapia.jar)• Apache Tomcat• PostgreSQL	7.1.3.1 6.5 6.3.3.26 7.0.53 9.2.9

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 3**. 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 3 of 11
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? n	DCS Call Coverage? y	
ASAI Link Plus Capabilities? n	DCS with Rerouting? y	
Async. Transfer Mode (ATM) PNC? n		

Navigate to **Page 6**, and verify that **Vectoring (Basic)** is set to “y”.

display system-parameters customer-options		Page 6 of 11
CALL CENTER OPTIONAL FEATURES		
Call Center Release: 6.0		
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 2                                     Page 1 of 3
                                         CTI LINK
CTI Link: 2
Extension: 60100
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 PegaCALL.

```
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
```


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 PegaCALL, which are shown below.

change reason-code-names	Page 1 of 1
REASON CODE NAMES	
Aux Work/ Interruptible?	Logout
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 PegaCALL.

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: PegaCALL
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 2
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*: PegaCALL Sales
                                Destination: Vector Number      1
                                Attendant Vectoring? n
                                Meet-me Conferencing? n
                                Allow VDN Override? n
                                COR: 1
                                TN*: 1
                                Measured: none
```

Repeat this section to administer the desired number of vectors and VDNs. In the compliance testing, the same vector was used to route incoming calls to two VDNs, 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
PegaCALL Sales	60001	n	1	1	V 1	none		
PegaCALL Support	60002	n	1	1	V 1	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 PegaCALL 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" and "Management Console" is displayed. A red horizontal bar spans the width of the page, with a "Help" link on the right. In the center, there is a login box with the text "Please login here:" followed by a "Username" label 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 © 2009-2014 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. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left sidebar contains a navigation menu with options like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area displays the "Welcome to OAM" message, explaining that the OAM Web provides tools for managing the AE Server and listing the administrative domains it covers: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. It also notes that these domains can be served by one administrator for all domains or a separate administrator for each domain.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Jul 7 07:18:03 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.4.10-0
Server Date and Time: Tue Jul 07 07:40:44 MDT 2015
HA Status: Not Configured

Home | Help | Logout

Home

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 shows the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the left sidebar. The main content area displays the "Licensing" page, which provides instructions on how to set up and maintain the WebLM, import licenses, and administer reserved licenses. It lists the required steps for each task: setting up the WebLM (WebLM Server Address), importing licenses (WebLM Server Access), and administering reserved licenses (Reserved Licenses).

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Jul 7 07:18:03 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.4.10-0
Server Date and Time: Tue Jul 07 07:45:51 MDT 2015
HA Status: Not Configured

Home | Help | Logout

Licensing

AE Services
Communication Manager Interface
High Availability
Licensing
WebLM Server Address
WebLM Server Access
Reserved Licenses
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

The **Web License Manager** screen is displayed. Select **Licensed products** → **APPL_ENAB** → **Application_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

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** for the Avaya S8800 Server.

Web License Manager (WebLM v6.3)
Help About Change Password

WebLM Home
Install license
Licensed products
APPL_ENAB
▼ Application_Enablement
View license capacity
View peak usage
Uninstall license
Server properties
Manage users
Shortcuts
Help for Installed Product

Application Enablement (CTI) - Release: 6 - SID: 10503000
Standard License file

You are here: Licensed Products > Application_Enablement > View License Capacity
License installed on: May 11, 2012 7:07:47 PM -04:00

License File Host IDs:
00-16-3E-48-E0-82

Licensed Features

10 Items
Show ALL

Feature (License Keyword)	Expiration date	Licensed capacity
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	10000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;leaptop;CtiS MediumServerTypes: ibmx306;ibmx306m;del1950;xen;hs20;hs20_ LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;ur TrustedApplications: IPS_001, BasicUnrestricted DMCUnrestricted: IXP_001, BasicUnrestricted DMCUnrestricted: IXN_001, BasicUnrestricted DMCUnrestricted: PC_001, BasicUnrestricted DMCUnrestricted: CJE_001, BasicUnrestricted DMCUnrestricted: OSFC_001, BasicUnrestricted DMCUnrestricted: VP_001, BasicUnrestricted DMCUnrestricted: SAMETIME_001 VALUE_AEC_UNIFIED_CC_DESKTOP_n; CCE_ AdvancedUnrestricted, DMCUnrestricted: CSI AdvancedUnrestricted, DMCUnrestricted: CSI AdvancedUnrestricted, DMCUnrestricted: AVA BasicUnrestricted, AdvancedUnrestricted, DMC CCT_ELITE_CALL_CTRL_001, BasicUnrestricted DMCUnrestricted, AgentEvents;
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	10000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16

TLT; Reviewed:
SPOC 8/18/2015

Solution & Interoperability Test Lab Application Notes
©2015 Avaya Inc. All Rights Reserved.

13 of 30
PegaCALL-AES63

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".

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 "S8800" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields. In the compliance testing, **ASAI Link Version** was set to "6", as shown below.

The screenshot shows the AVAYA Application Enablement Services Management Console with the "Add TSAPI Links" screen displayed. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. 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: S8800, Switch CTI Link Number: 2, ASAI Link Version: 6, and Security: Unencrypted. Below the form are buttons for "Apply Changes" and "Cancel Changes".

6.4. Administer TCP Settings

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

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 left navigation pane shows a tree structure with "Networking" expanded, highlighting "TCP Settings". The main content area is titled "TCP Settings" and contains the "TCP Retransmission Count" section. Two radio buttons are present: "Standard Configuration (15)" and "TSAPI Routing Application Configuration (6)", with the latter being selected. Below the radio buttons are "Apply Changes" and "Cancel Changes" buttons. A note explains that a smaller retransmission count reduces server wait time for TCP acknowledgments. A warning states that the setting applies to all TCP and TLS sockets.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Jul 7 07:40:33 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.4.10-0
Server Date and Time: Tue Jul 07 08:13:18 MDT 2015
HA Status: Not Configured

Networking | TCP Settings Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
▼ Networking
AE Service IP (Local IP)
Network Configure
Ports
TCP Settings
Security

TCP Settings

TCP Retransmission Count

☐ Standard Configuration (15)
☒ TSAPI Routing Application Configuration (6)


Apply Changes Cancel Changes

Note: A smaller TCP Retransmission Count reduces the amount of time that the 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.

Warning: This setting applies to all TCP and TLS sockets on the AE 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**.

**Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Jul 7 07:40:33 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.4.10-0
Server Date and Time: Tue Jul 07 08:18:23 MDT 2015
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

▶ User Management

Service Controller

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

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

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart Web Server

6.6. 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 PegaCALL.

In this case, the associated Tlink name is “AVAYA#S8800#CSTA#AES_125_72”. Note the use of the switch connection “S8800” 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 list of Tlink names. Two Tlink names are listed: "AVAYA#S8300D#CSTA#AES_125_72" and "AVAYA#S8800#CSTA#AES_125_72". The second Tlink name is selected, and a "Delete Tlink" button is visible below it.

Welcome: User
Last login: Tue Jul 7 07:18:03 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.4.10-0
Server Date and Time: Tue Jul 07 07:40:44 MDT 2015
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#S8300D#CSTA#AES_125_72

☒ AVAYA#S8800#CSTA#AES_125_72

Delete Tlink

6.7. Administer PegaCALL 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 Jul 7 07:40:33 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.4.10-0
Server Date and Time: Tue Jul 07 08:27:28 MDT 2015
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

Given Name

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** retained the default value of 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 PegaCALL user from **Section 6.7**.

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 "Control". The right pane shows the "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" configuration page, which includes two unchecked checkboxes for enabling SDB for specific services and an "Apply Changes" button.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Jul 7 07:18:03 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.4.10-0
Server Date and Time: Tue Jul 07 07:40:44 MDT 2015
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

Apply Changes

7. Configure Pegasystems PegaCALL

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

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

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

PegaCALL 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

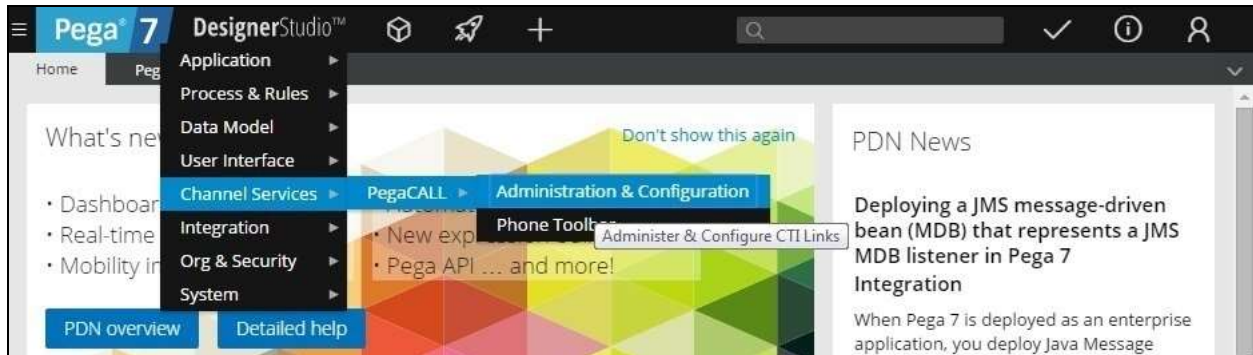
Access the web-based interface by using the URL “http://ip-address:9080/ prweb/PRServlet” in an Internet browser window, where “ip-address” is the IP address of the PegaCALL server.

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

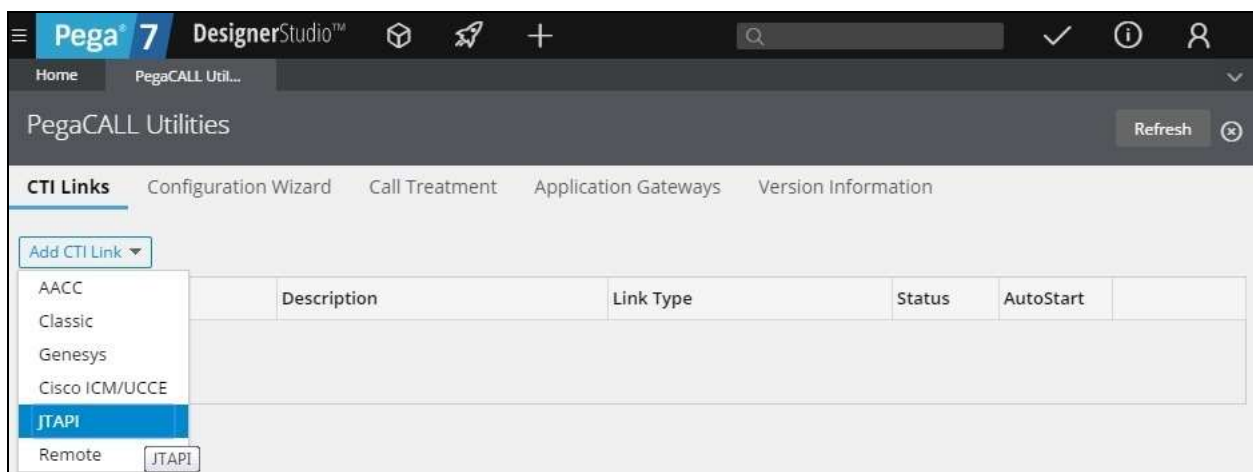
The image shows the Pega 7 login interface. At the top center is the Pega 7 logo, which consists of the word "Pega" in white on a blue background, followed by a large white number "7" on a blue background. Below the logo are two white input fields: the first is labeled "User Name" and the second is labeled "Password". Below these fields is a blue button with the text "Log In" in white. At the bottom of the screen, there is small text that reads: "Pega 7.1.8", "a356683200fd5dc897f4337e088b5c18", "coreAssemblyCached_718_675", "Copyright © 2001-2015 Pegasystems Inc. All rights reserved.", and "Pegasystems ®".

7.2. Administer CTI Link

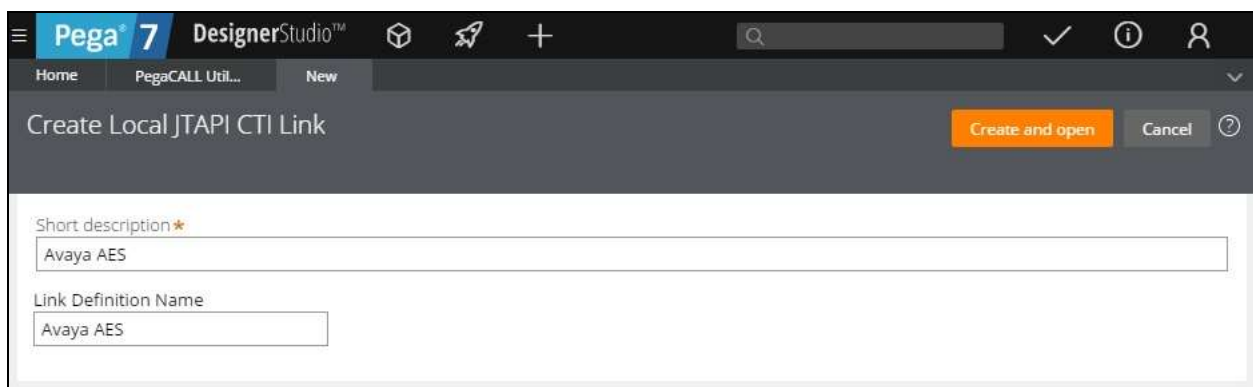
The screen below is displayed next. Select **DesignerStudio** → **Channel Services** → **PegaCALL** → **Administration & Configuration** from the top menu.



The **PegaCALL Utilities** 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 PegaCALL user credentials from **Section 6.7**.
- **Password:** The PegaCALL user credentials from **Section 6.7**.
- **Enable UCID Support:** Configure to match the UCID setting in **Section 5.3**.

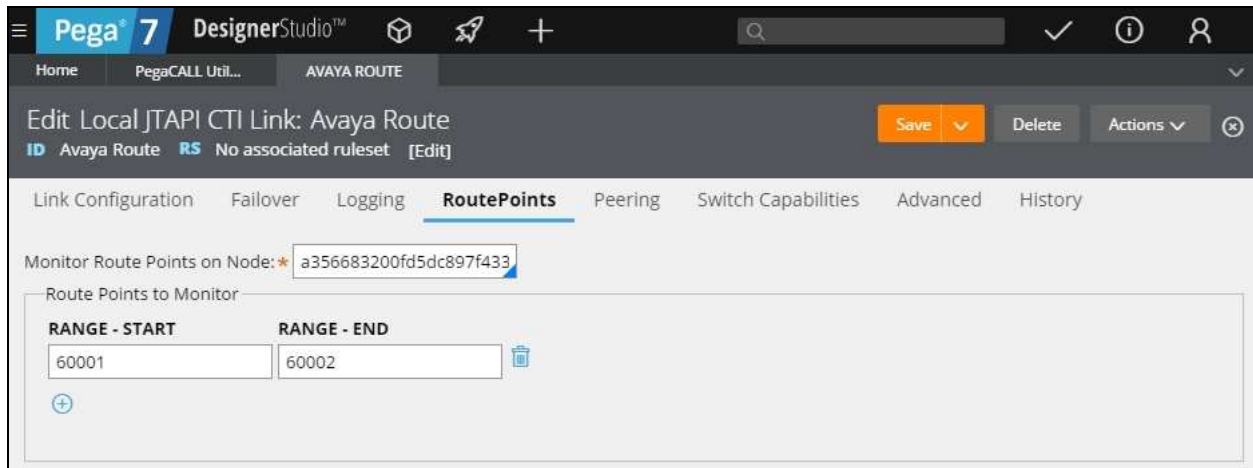
The screenshot shows the Pega 7 DesignerStudio interface for editing a Local JTAPI CTI Link. The title bar indicates 'Pega 7 DesignerStudio™'. The main header shows 'Edit Local JTAPI CTI Link: Avaya AES' with a 'Save' button and an 'Actions' dropdown. Below the header, there are tabs for 'Link Configuration',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

- Enabled:** ☒
- Auto Start:** ☒
- JTAPI Vendor:** Avaya AES (dropdown)
- Avaya AES Connectivity:**
 - AES Server Host Name:** 10.64.125.72
 - Port:** 450
 - TLINK:** AVAYA#S8800#CSTA#AES_125_72
 - 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)

7.3. 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**.

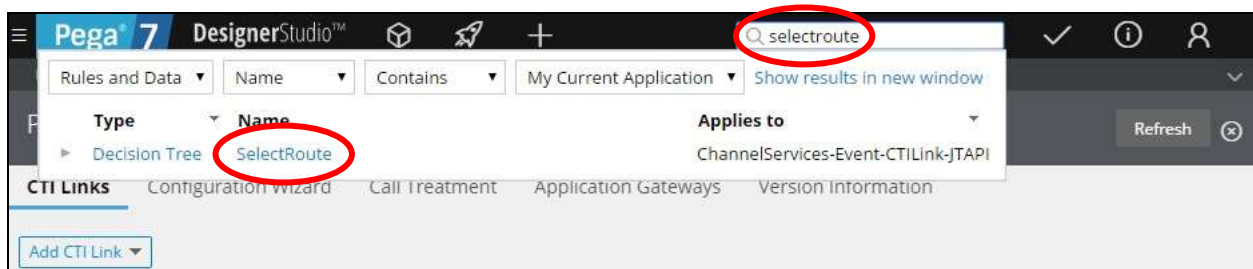


7.4. Administer Decision Tree

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

Prior to administering decision tree, follow reference [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, a RuleSet named **Pega-CTI** was pre-configured.

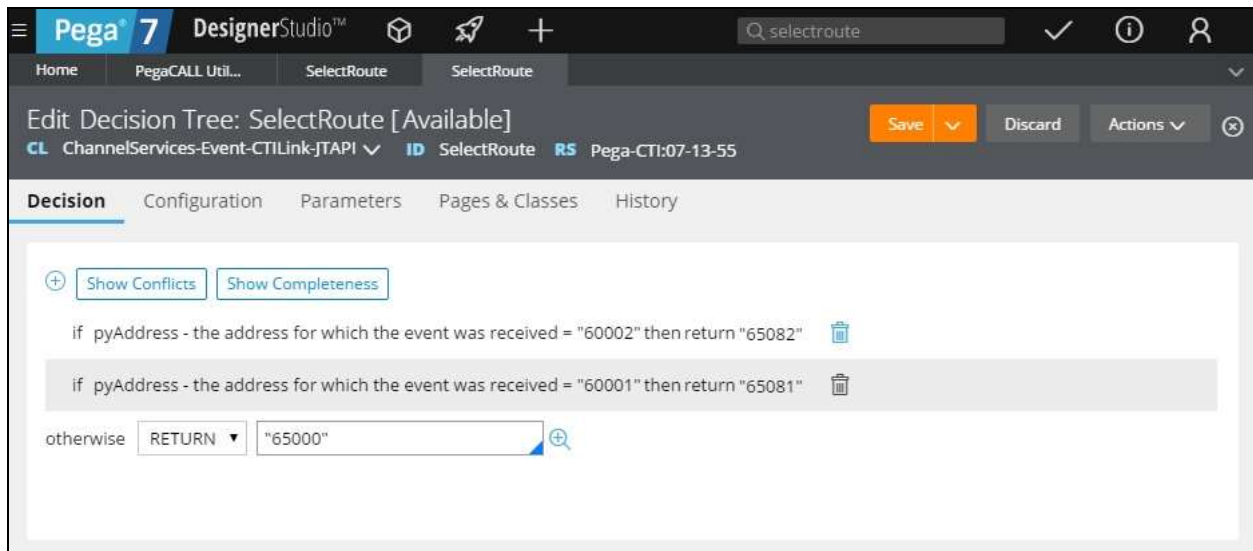
Enter “selectroute” in the top menu search area, and click **SelectRoute** from the result of the search, as shown below.



The **Edit Decision Tree** 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 **65081** and **65082** are existing skill groups on Communication Manager, and extension **65000** 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 PegaCALL.

8.1. 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
2	6	no	aes_125_72	established	40	38

8.2. Verify Avaya Aura® Application Enablement Services

Log in at least one agent using PegaCALL 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: Tue Jul 7 12:09:36 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.4.10-0
Server Date and Time: Tue Jul 07 13:09:43 MDT 2015
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

Log Manager

▶ Logs

▼ Status and Control

CVLAN Service Summary

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	S8800	2	Talking	Wed Jul 1 12:38:21 2015	Online	16	2	38	40	30
<input type="radio"/>	2	S8300D	1	Switch Down	Wed Jul 1 12:38:21 2015	Online	16	0	0	0	30

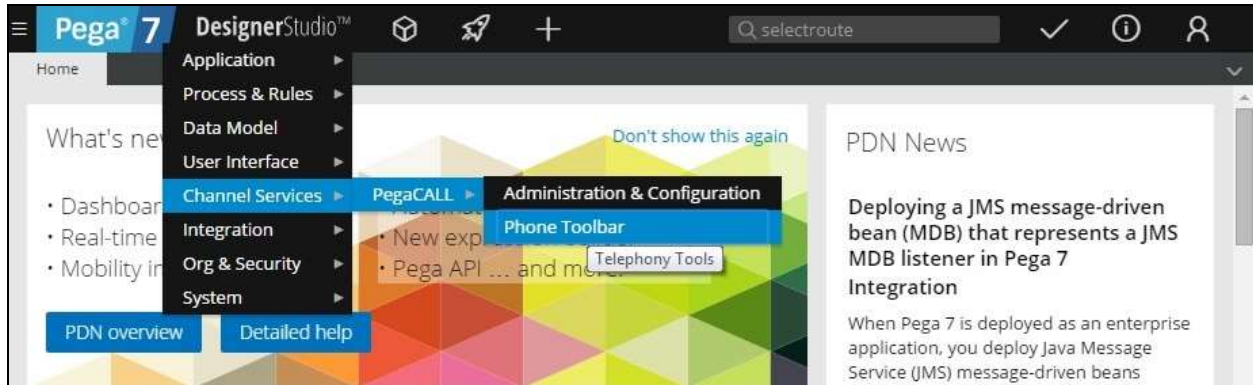
Online Offline

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

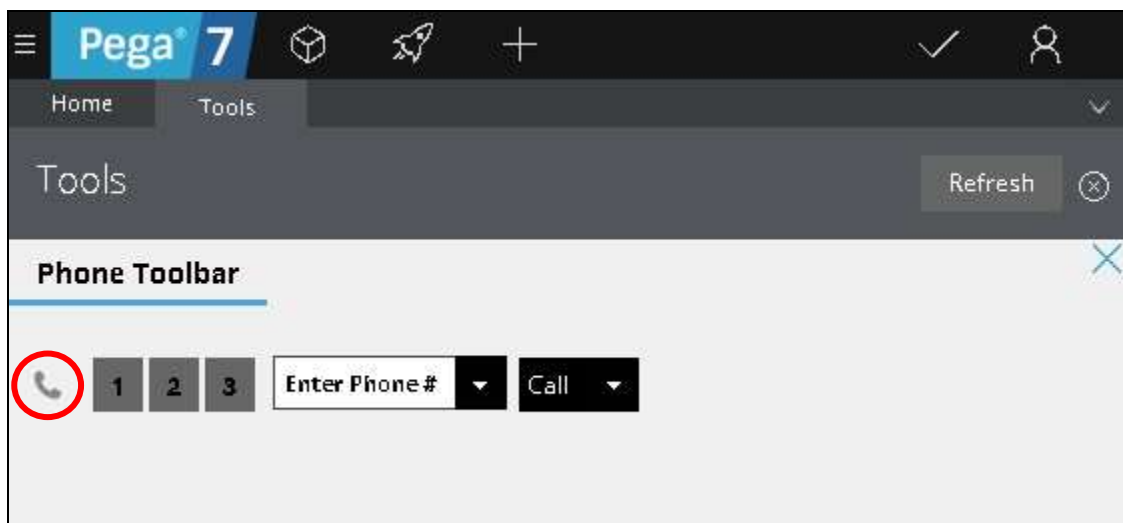
TSAPI Service Status TLink Status User Status

8.3. Verify Pegasystems PegaCALL

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 **DesignerStudio** → **Channel Services** → **PegaCALL** → **Phone Toolbar** from the top menu.

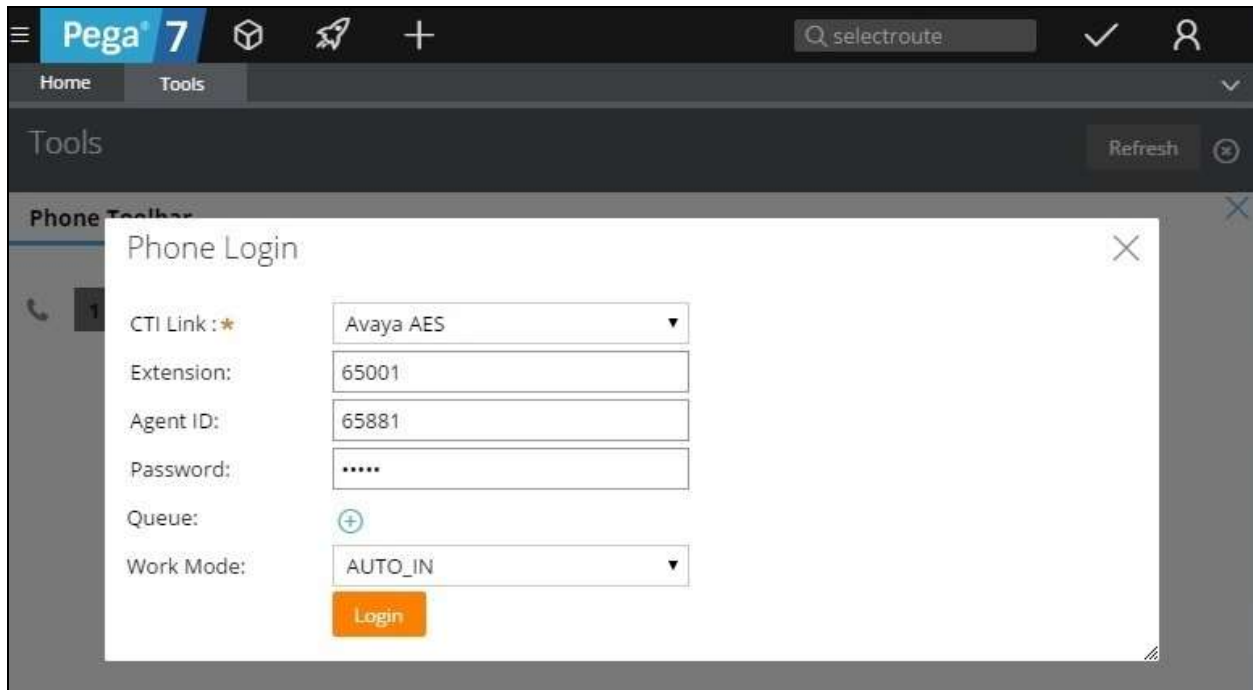


The screen is updated with a **Tools** tab, as shown below. Click on the handset icon.



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 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”.

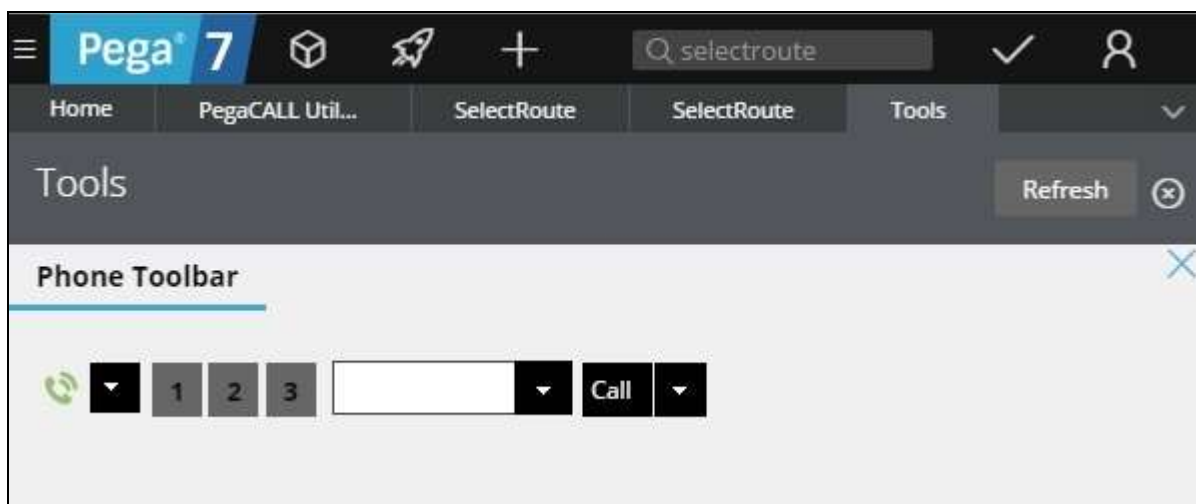


The screenshot shows the Pega 7 user interface. At the top, there is a navigation bar with 'Home' and 'Tools' tabs. Below this, a 'Tools' section is visible. A 'Phone Login' pop-up box is displayed in the foreground. The pop-up contains the following fields and values:

Field	Value
CTI Link :*	Avaya AES
Extension:	65001
Agent ID:	65881
Password:	*****
Queue:	(+)
Work Mode:	AUTO_IN

At the bottom of the pop-up is an orange 'Login' button.

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

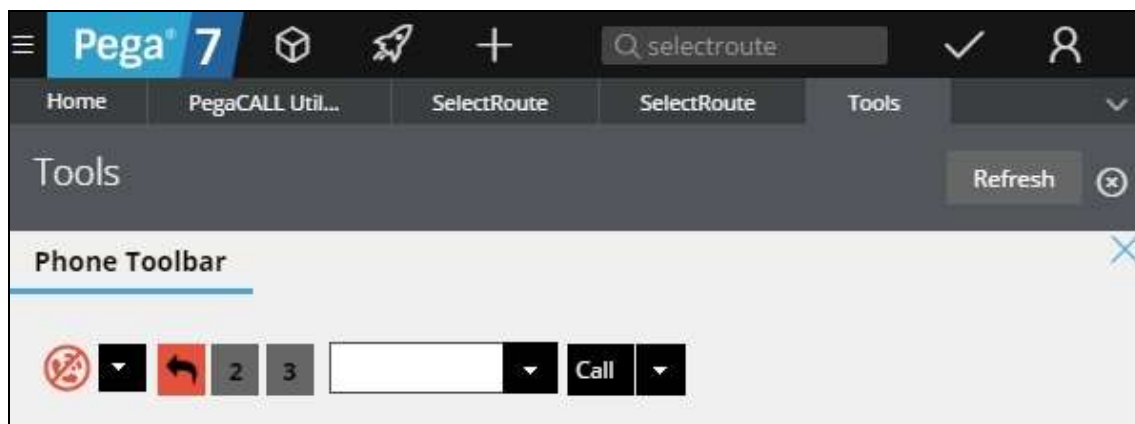


The screenshot shows the Pega 7 user interface after the login process. The 'Tools' section is now updated to show a 'Phone Toolbar'. The toolbar includes a green phone icon, a dropdown menu, and three buttons labeled '1', '2', and '3'. To the right of these buttons is a text input field, followed by a dropdown menu and a 'Call' button. The background of the interface remains the same, with the 'Tools' tab selected.

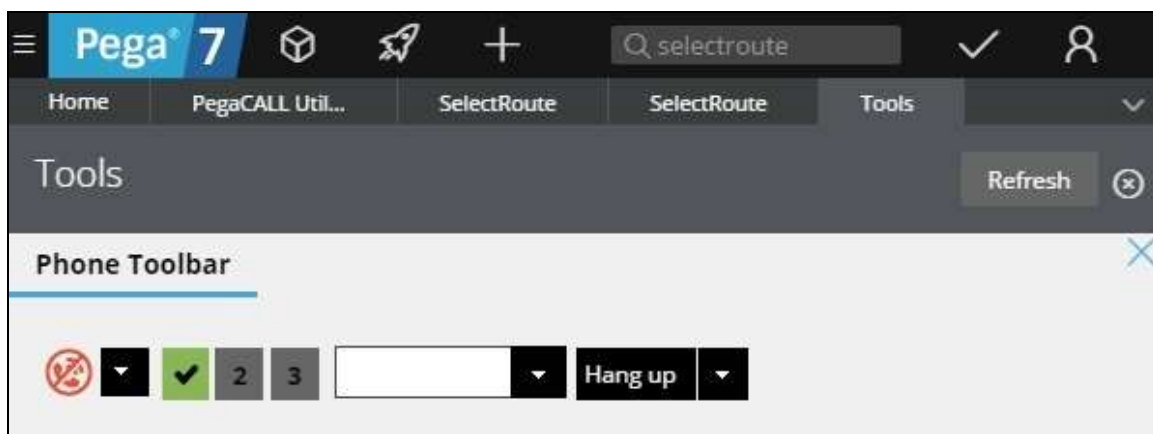
Make an incoming call from the PSTN to one of the routing VDNs. Verify that the call is ringing at the agent's telephone. Also verify that a pop-up dialog box is displayed with the proper calling party number, as shown below.

Incoming Call	
Call From	919088485601
ANI	919088485601
DNIS	
Call Type	INBOUND
<div>Decline Accept</div>	

In addition, verify that the 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 screen is updated with solid green on the applicable call appearance icon, as shown below.



9. Conclusion

These Application Notes describe the configuration steps required for Pegasystems PegaCALL 7.1 to successfully interoperate with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Application Enablement Services 6.3. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 10, Release 6.3, June 2014, available at <http://support.avaya.com>.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3, 02-300357, June 2014, available at <http://support.avaya.com>.
3. *PegaCALL Configuration and Operations Guide for CTI Link Engine with Avaya AES CTI*, Software Version 7.1.3.1, June, 2015, 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>.

©2015 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.