Avaya Solution & Interoperability Test Lab

Application Notes for Pegasystems Pega Call 8.5.5 with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1– Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Pegasystems Pega Call 8.5.5 to interoperate with Avaya Aura® Communication Manager 8.1.3.3 and Avaya Aura® Application Enablement Services 8.1.3.3 Pegasystems Pega Call provides telephony integration for Pegasystems' customer relationship and process management frameworks.

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

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required for Pegasystems Pega Call 8.5.5 to interoperate with Avaya Aura® Communication Manager 8.1.3.3 and Avaya Aura® Application Enablement Services 8.1.3.3 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.

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

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

For the testing associated with this Application Notes, the interface between Avaya systems and Pegasystem Pega Call utilized enabled capabilities of secure JTAPI.

2.1. Interoperability Compliance Testing

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

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

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

2.2. Test Results

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

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

2.3. Support

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

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

3. Reference Configuration

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

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

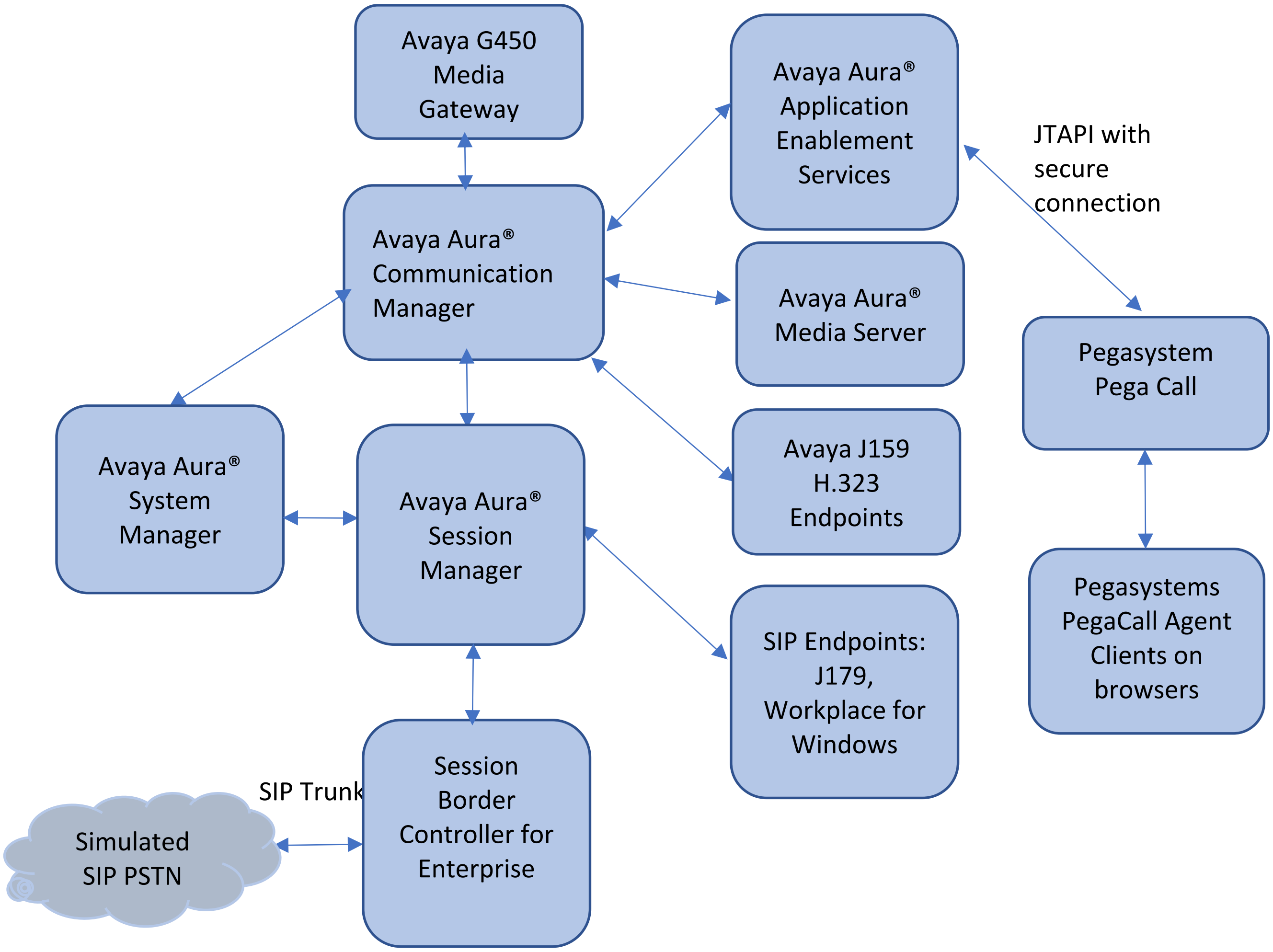

Avaya G450 Media Gateway
Avaya Aura® Application Enablement Services
JTAPI with secure connection
Avaya Aura® Communication Manager
Avaya Aura® Media Server
Pegasystem Pega Call
Avaya Aura® System Manager
Avaya Aura® Session Manager
Avaya J159 H.323 Endpoints
Pegasystems PegaCall Agent Clients on browsers
SIP Endpoints: J179, Workplace for Windows
SIP Trunk
Simulated SIP PSTN
Session Border Controller for Enterprise

Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager in Virtual Environment	8.1.3.3 - 8.1.3.3.1013878
Avaya Aura® Session Manager in Virtual Environment	8.1.3.3 - 8.1.3.3.813310
Avaya Aura® Communication Manager in Virtual Environment	8.1.3.3 - 01.0.890.0-27168
Avaya G450 Media Gateway	41.34.1
Avaya Aura® Media Server in Virtual Environment	8.0 SP2
Avaya Aura® Application Enablement Services in Virtual Environment	8.1.3.3
Avaya Session Border Controller for Enterprise	8.1.3
Avaya Workplace Client for Windows	3.22.0
Avaya J179 IP Phone (SIP)	4.0.9
Avaya J159 IP Deskphone (H.323)	6.8.5
Pegasystems PegaCall - Avaya JTAPI Client	8.5.5 8.1.3

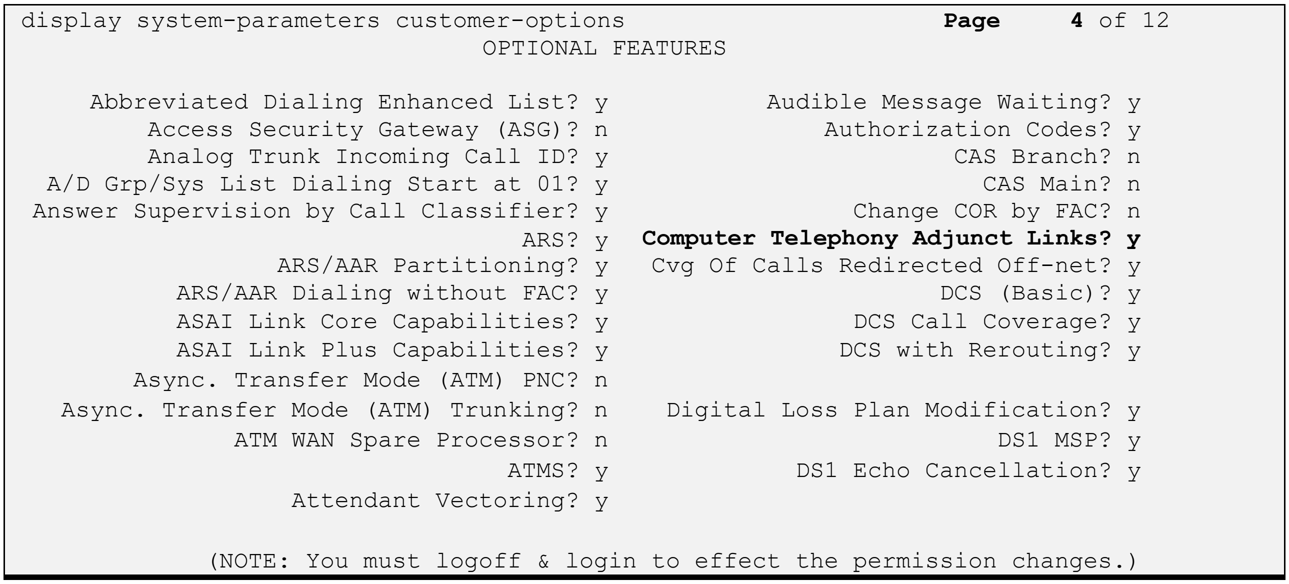
5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Obtain UCID setting
- Administer reason codes
- Administer hunt group and agent
- Administer vectors and VDNs

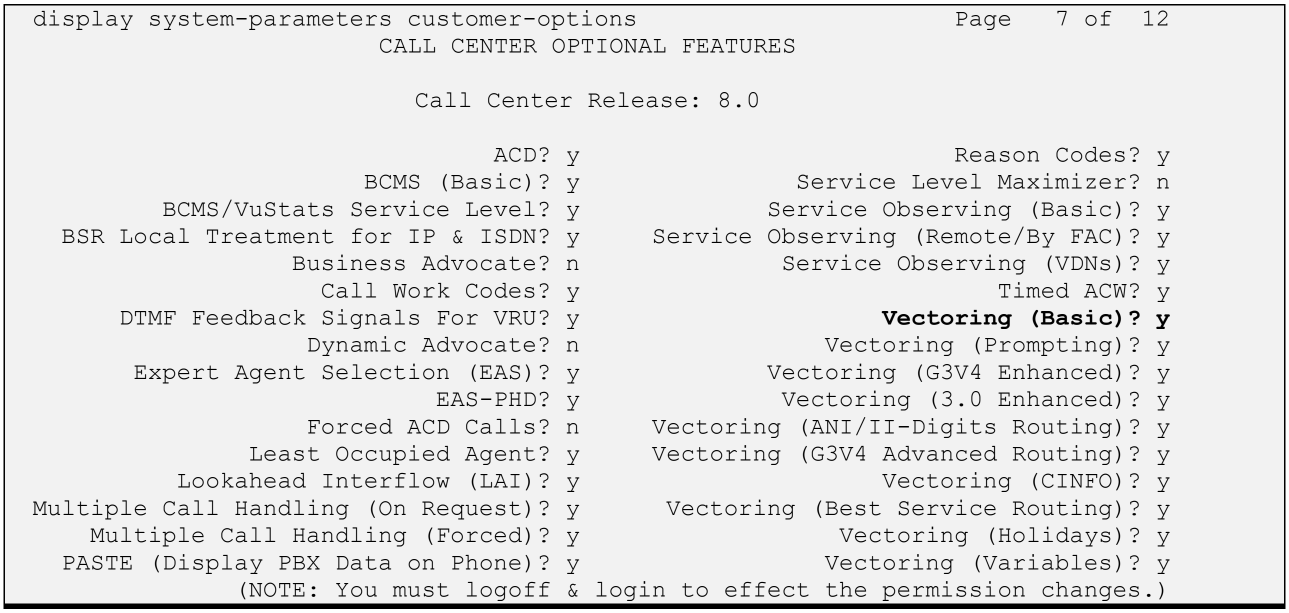
5.1. Verify License

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



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

     Abbreviated Dialing Enhanced List? y           Audible Message Waiting? y
         Access Security Gateway (ASG)? n               Authorization Codes? y
         Analog Trunk Incoming Call ID? y                        CAS Branch? n
  A/D Grp/Sys List Dialing Start at 01? y                          CAS Main? n
 Answer Supervision by Call Classifier? y                 Change COR by FAC? n
                                   ARS? y  Computer Telephony Adjunct Links? y
                  ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
           ARS/AAR Dialing without FAC? y                      DCS (Basic)? y
           ASAI Link Core Capabilities? y                 DCS Call Coverage? y
           ASAI Link Plus Capabilities? y                DCS with Rerouting? y
        Async. Transfer Mode (ATM) PNC? n
   Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
               ATM WAN Spare Processor? n                           DS1 MSP? y
                                  ATMS? y             DS1 Echo Cancellation? y
                   Attendant Vectoring? y


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

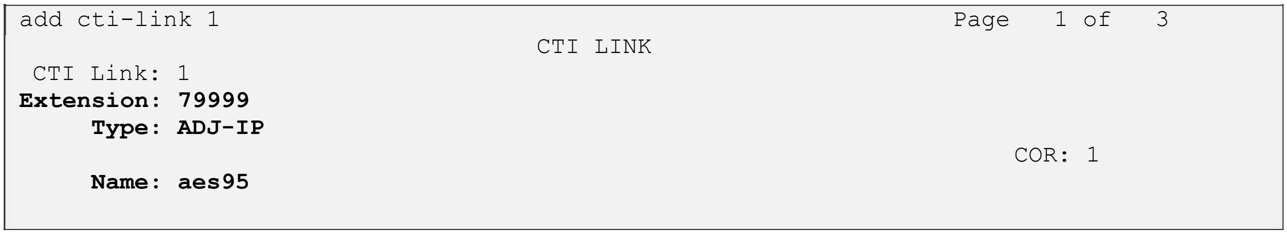
Navigate to **Page 7**, and verify that **Vectoring (Basic)** is set to **y**.



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

                          Call Center Release: 8.0

                               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
                 Forced ACD Calls? n     Vectoring (ANI/II-Digits Routing)? y
             Least Occupied Agent? y     Vectoring (G3V4 Advanced Routing)? y
         Lookahead Interflow (LAI)? y                       Vectoring (CINFO)? y
Multiple Call Handling (On Request)? y      Vectoring (Best Service Routing)? y
    Multiple Call Handling (Forced)? y                   Vectoring (Holidays)? y
  PASTE (Display PBX Data on Phone)? y                  Vectoring (Variables)? y
           (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. Administer CTI Link

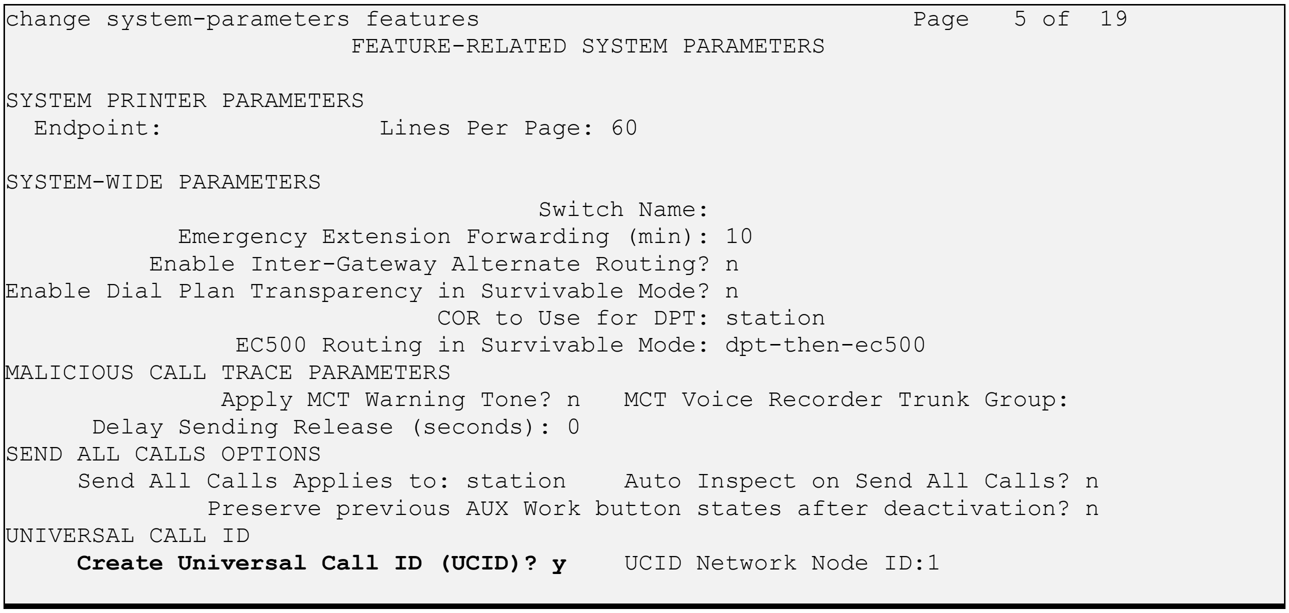
Add a CTI link using the **add cti-link n** command, where **n** is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name**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



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

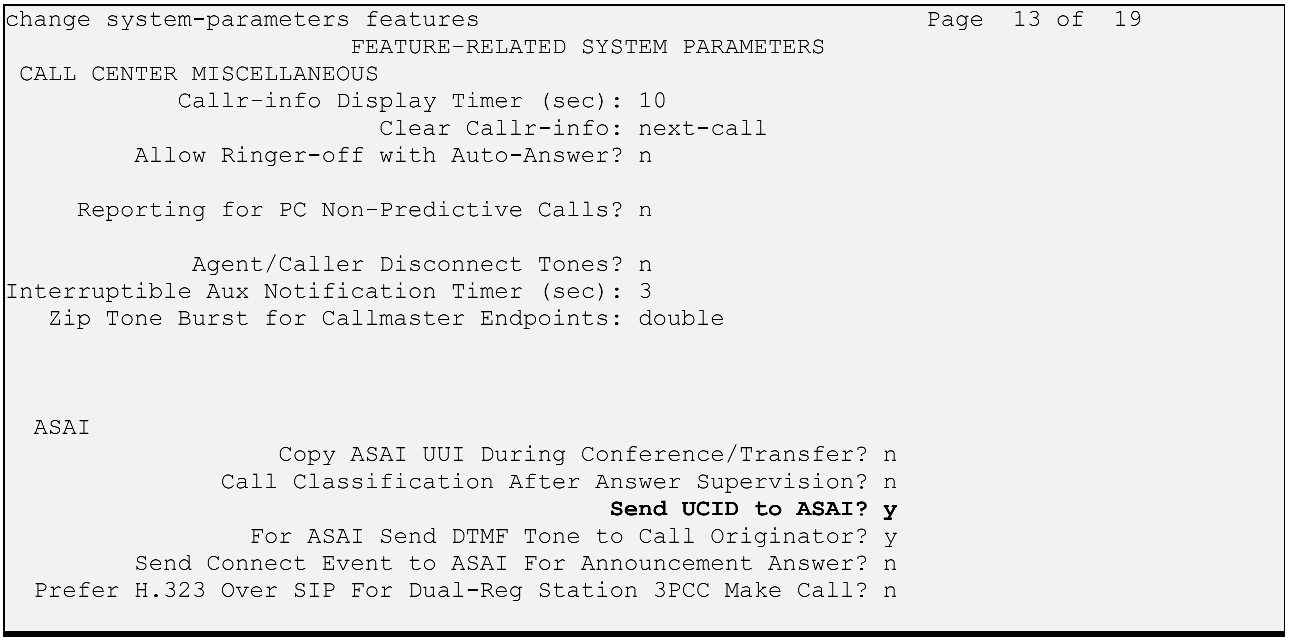
5.3. Obtain UCID Setting

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



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

SYSTEM PRINTER PARAMETERS
  Endpoint:               Lines Per Page: 60

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

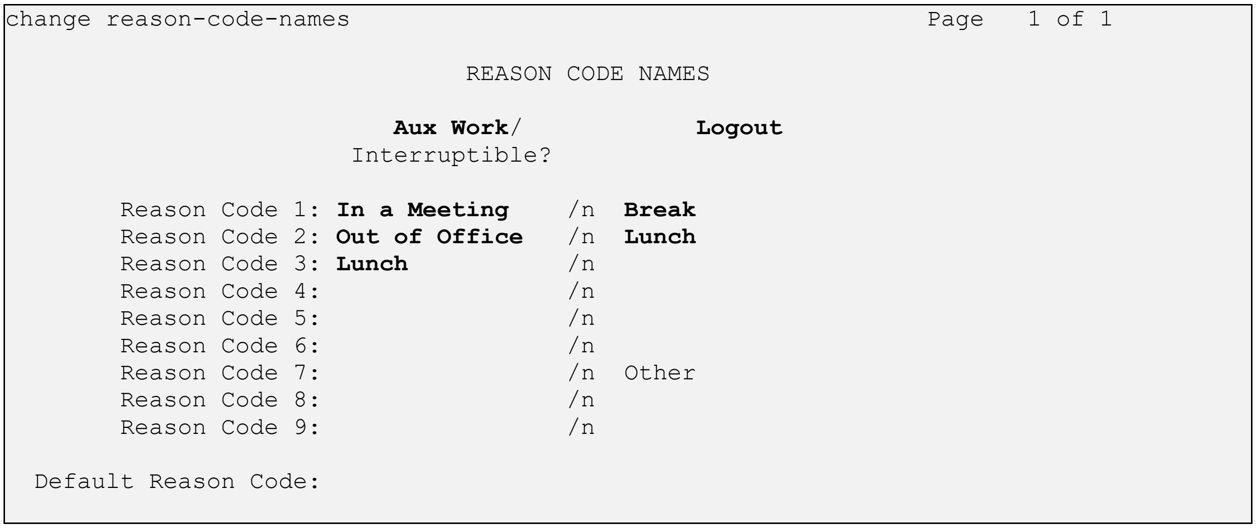
Navigate to **Page 13**, and make a note of the **Send UCID to ASAI** setting, which will be used later to configure Pega Call.



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

5.4. Administer Reason Codes

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



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

                                REASON CODE NAMES

                           Aux Work/                   Logout
                        Interruptible?

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

  Default Reason Code:
```

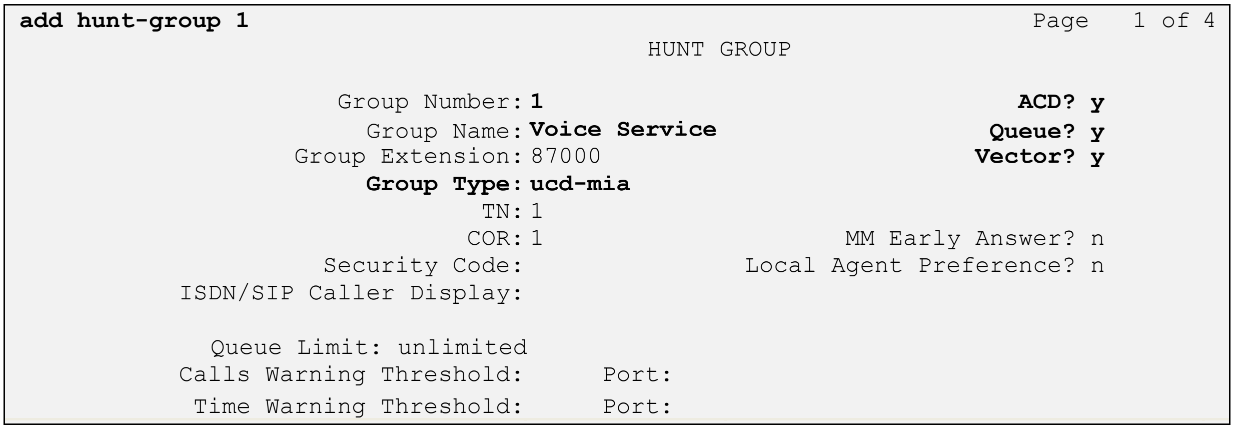
5.5. Administer Hunt Group and Agent

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

- Hunt Group
- Agent

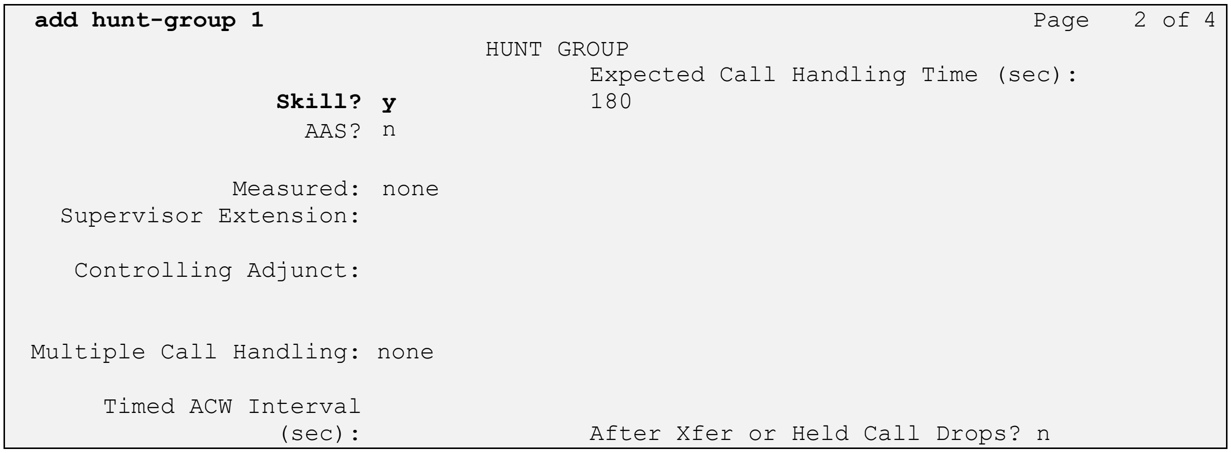
5.5.1. Add Hunt Group

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



```
add hunt-group 1                                                Page   1 of 4
                                  HUNT GROUP

                      Group Number: 1                                ACD? y
                        Group Name: Voice Service                  Queue? y
                   Group Extension: 87000                         Vector? y
                        Group Type: ucd-mia
                                TN: 1
                               COR: 1                   MM Early Answer? n
                     Security Code:              Local Agent Preference? n
           ISDN/SIP Caller Display:

             Queue Limit: unlimited
           Calls Warning Threshold:     Port:
            Time Warning Threshold:     Port:
```

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

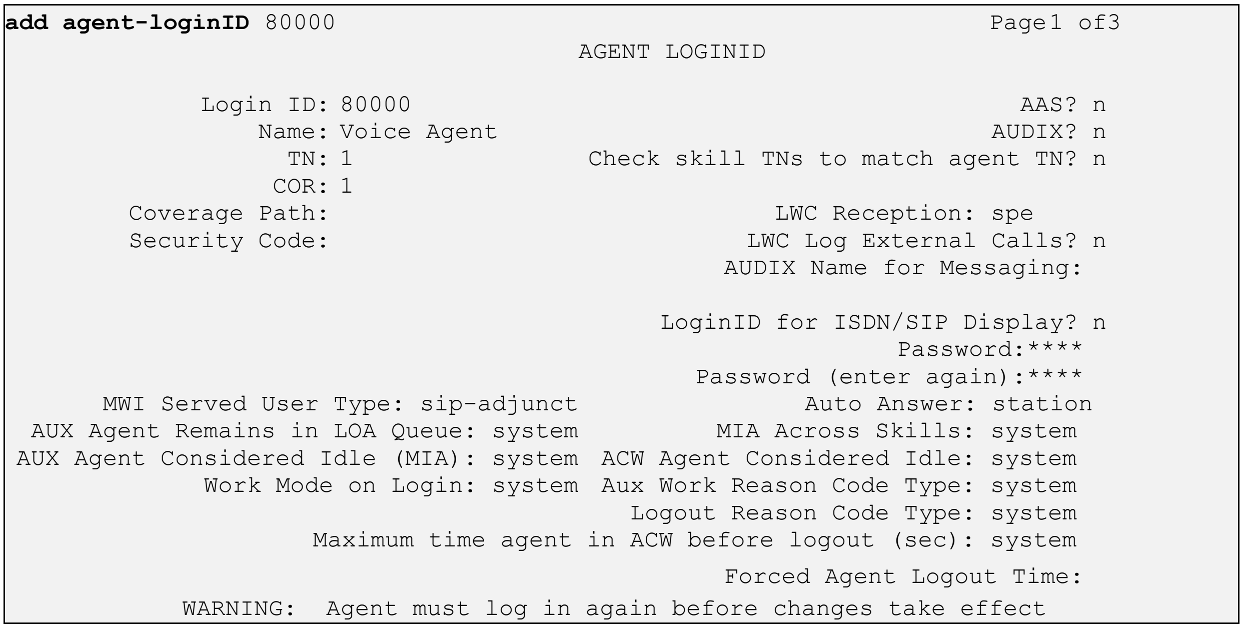


```
 add hunt-group 1                                               Page   2 of 4
                            HUNT GROUP
                                   Expected Call Handling Time (sec):
                 Skill? y          180
                   AAS? n

              Measured: none
  Supervisor Extension:

   Controlling Adjunct:


Multiple Call Handling: none

     Timed ACW Interval
                 (sec):            After Xfer or Held Call Drops? n
```

5.5.2. Add Agent

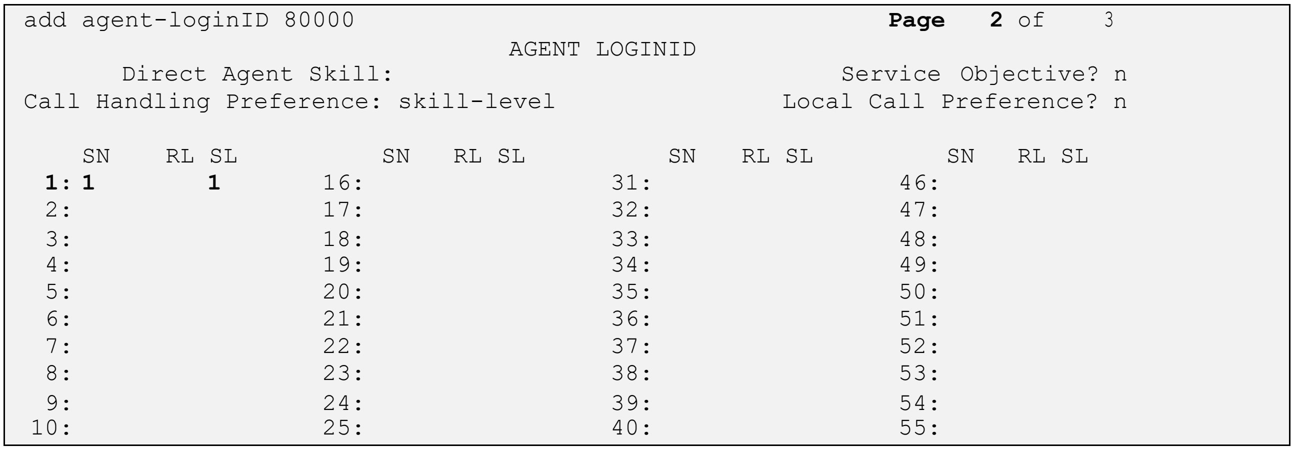
In the compliance testing, the agents 80000 and 80001 were created.

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



```
add agent-loginID 80000                                          Page1 of3
                                AGENT LOGINID

           Login ID: 80000                                          AAS? n
               Name: Voice Agent                                  AUDIX? n
                 TN: 1                Check skill TNs to match agent TN? n
                COR: 1
      Coverage Path:                                 LWC Reception: spe
      Security Code:                             LWC Log External Calls? n
                                              AUDIX Name for Messaging:

                                          LoginID for ISDN/SIP Display? n
                                                              Password:****
                                            Password (enter again):****
     MWI Served User Type: sip-adjunct                Auto Answer: station
 AUX Agent Remains in LOA Queue: system          MIA Across Skills: system
AUX Agent Considered Idle (MIA): system  ACW Agent Considered Idle: system
             Work Mode on Login: system  Aux Work Reason Code Type: system
                                           Logout Reason Code Type: system
                   Maximum time agent in ACW before logout (sec): system
                                              Forced Agent Logout Time:
            WARNING:  Agent must log in again before changes take effect
```

On **Page 2,** add the required skills. Note that the skill **1** is added to this agent so when a call for **Voice Service** is initiated, the call can be routed to this agent.

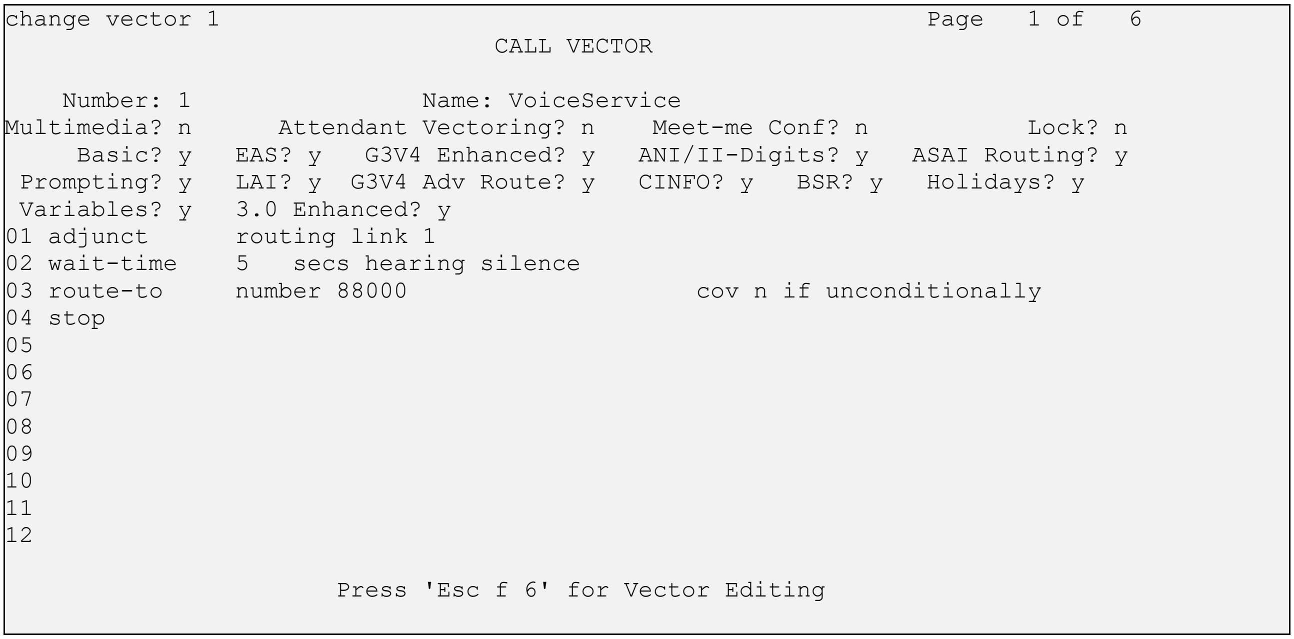


```
add agent-loginID 80000                                   Page   2 of    3
                                AGENT LOGINID
       Direct Agent Skill:                               Service Objective? n
Call Handling Preference: skill-level                 Local Call Preference? n

    SN    RL SL          SN    RL SL          SN    RL SL          SN    RL SL
 1: 1        1       16:                 31:                 46:
 2:                  17:                 32:                 47:
 3:                  18:                 33:                 48:
 4:                  19:                 34:                 49:
 5:                  20:                 35:                 50:
 6:                  21:                 36:                 51:
 7:                  22:                 37:                 52:
 8:                  23:                 38:                 53:
 9:                  24:                 39:                 54:
10:                  25:                 40:                 55:
```

Repeat this section to add another agent 80001.

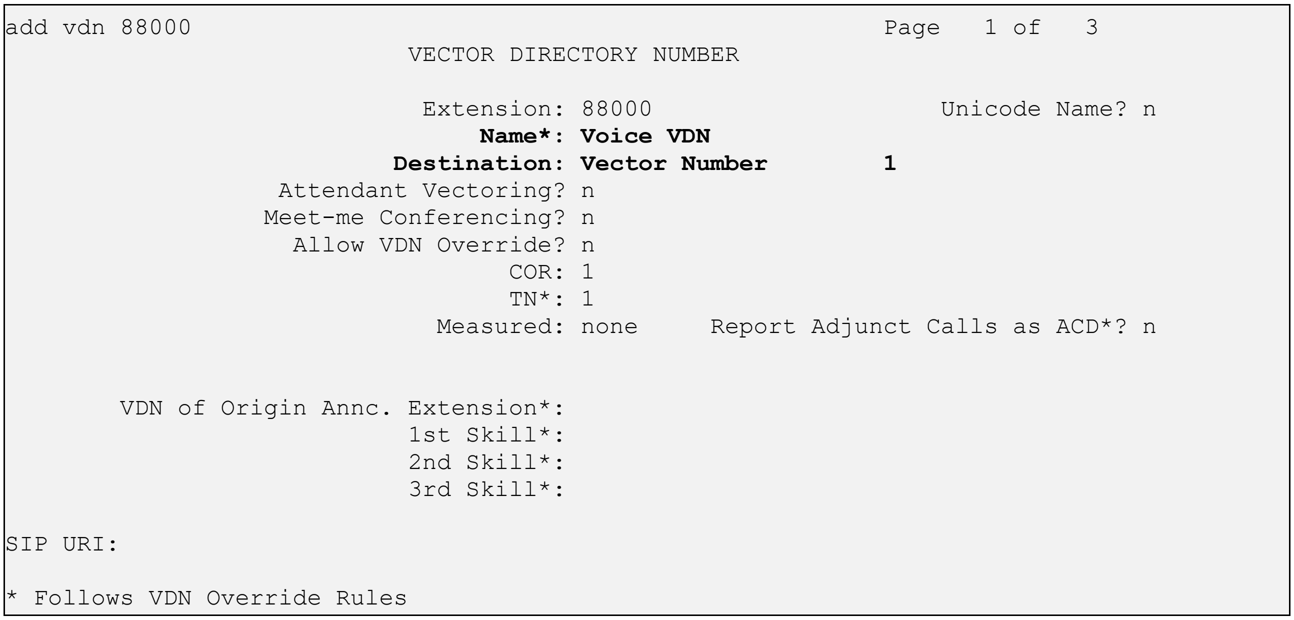
5.6. Administer Vectors and VDNs

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



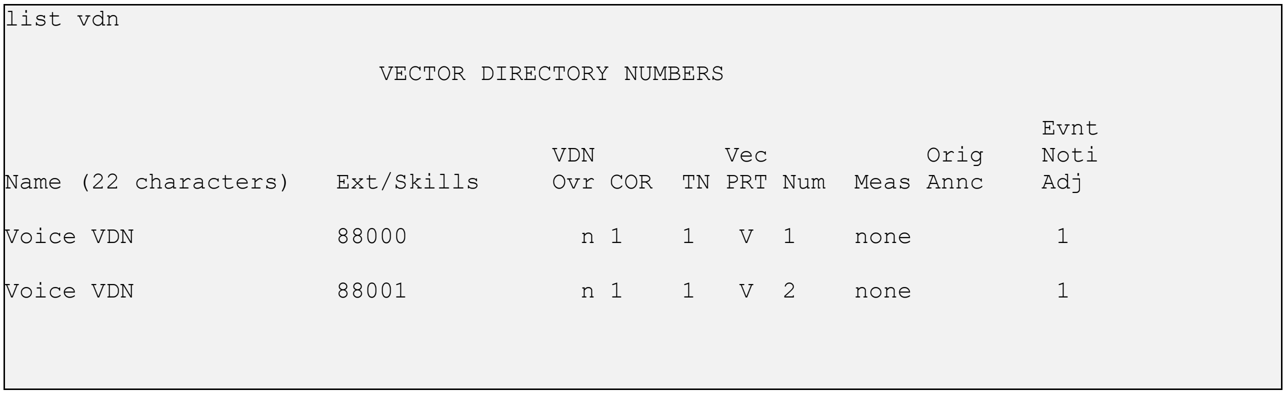
```
change vector 1                                                 Page   1 of   6
                                  CALL VECTOR

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

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

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



```
add vdn 88000                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 88000                    Unicode Name? n
                                 Name*: Voice VDN
                           Destination: Vector Number        1
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none     Report Adjunct Calls as ACD*? n


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

SIP URI:

* Follows VDN Override Rules
```

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



```
list vdn

                          VECTOR DIRECTORY NUMBERS

                                                                        Evnt
                                      VDN         Vec           Orig    Noti
Name (22 characters)   Ext/Skills     Ovr COR  TN PRT Num  Meas Annc    Adj

Voice VDN              88000            n 1    1   V  1    none          1

Voice VDN              88001            n 1    1   V  2    none          1
```

6. Configure Avaya Aura® Application Enablement Services

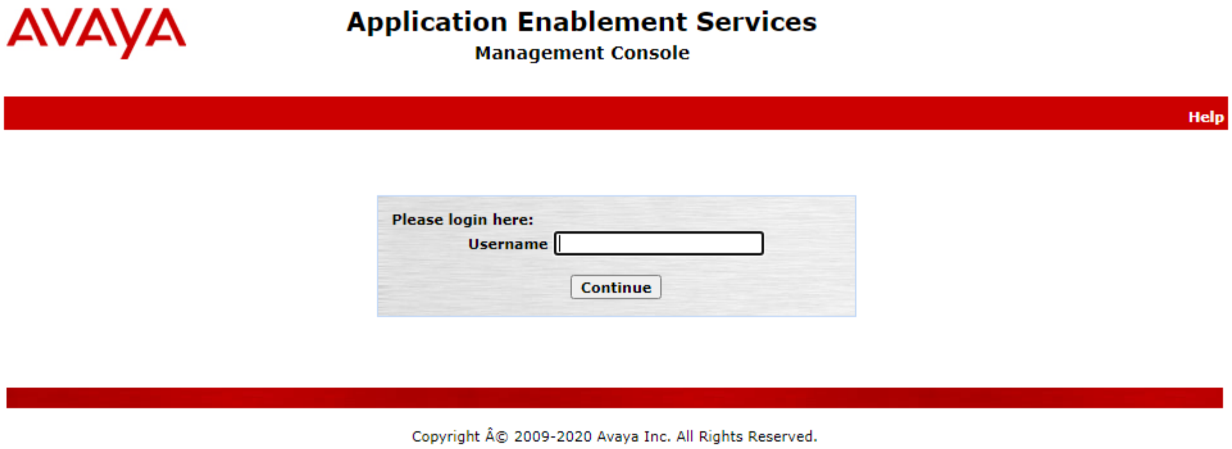
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

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

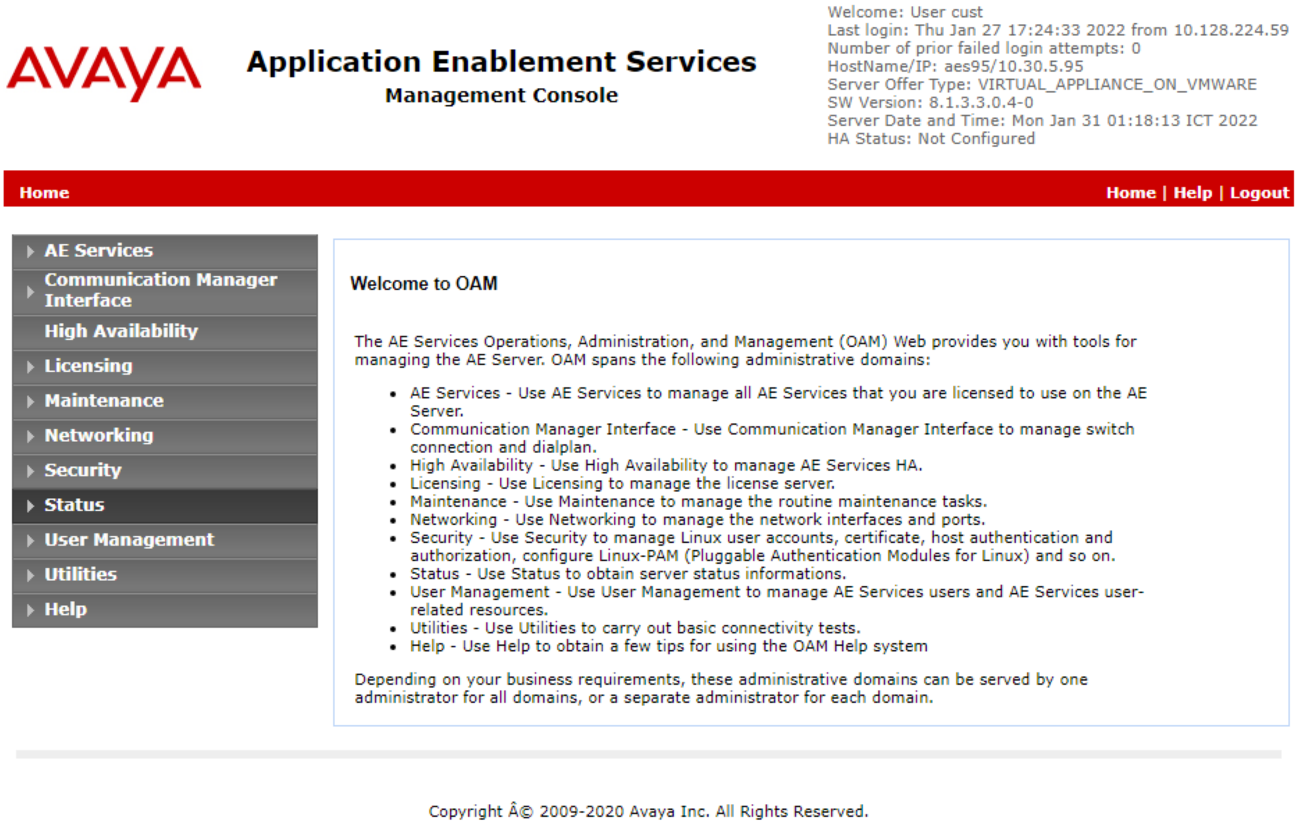
6.1. Launch OAM Interface

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

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


AVAYA
Application Enablement Services
Management Console
Help
Please login here:
Username
Continue
Copyright Â© 2009-2020 Avaya Inc. All Rights Reserved.

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



Welcome: User cust
Last login: Thu Jan 27 17:24:33 2022 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.3.0.4-0
Server Date and Time: Mon Jan 31 01:18:13 ICT 2022
HA Status: Not Configured

Welcome to OAM

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

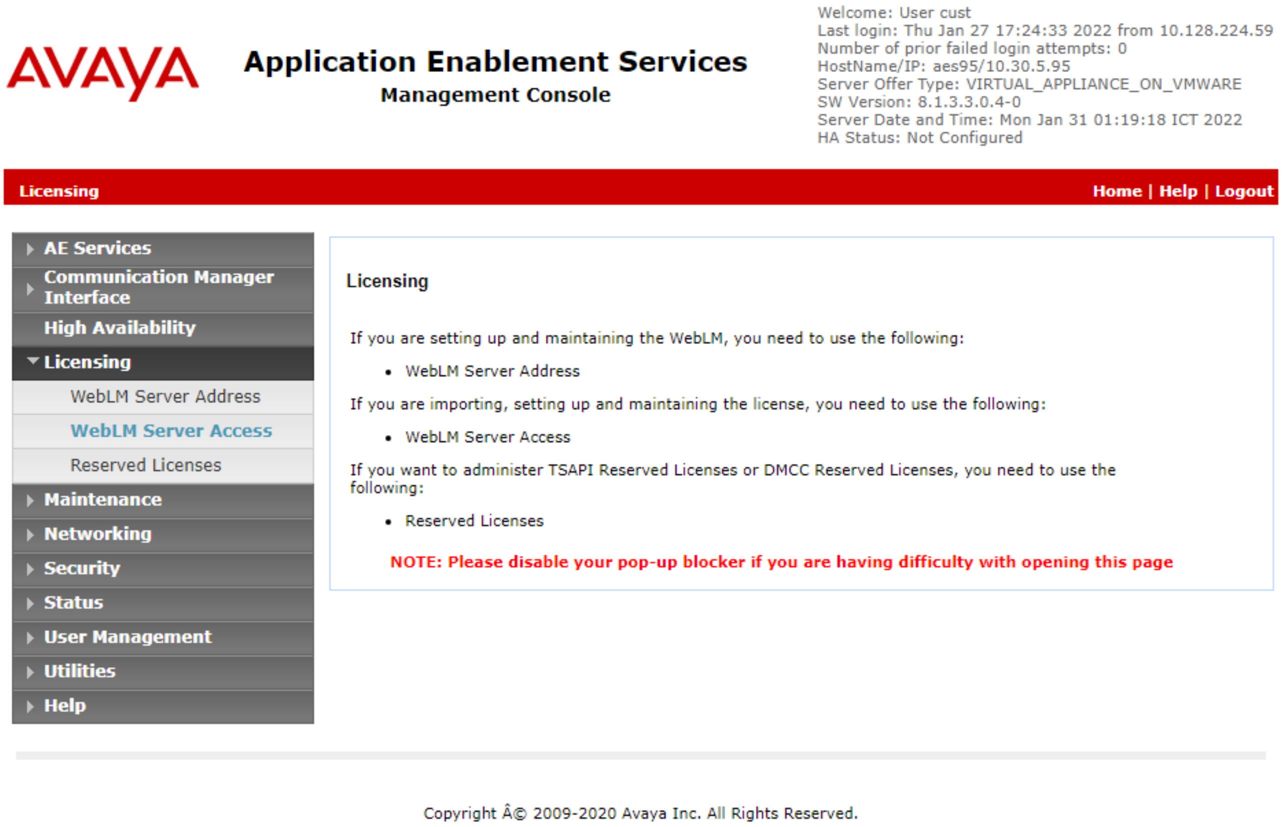
- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing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

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

Copyright Â© 2009-2020 Avaya Inc. All Rights Reserved.

6.2. Verify License

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



Welcome: User cust
Last login: Thu Jan 27 17:24:33 2022 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.3.0.4-0
Server Date and Time: Mon Jan 31 01:19:18 ICT 2022
HA Status: Not Configured

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:

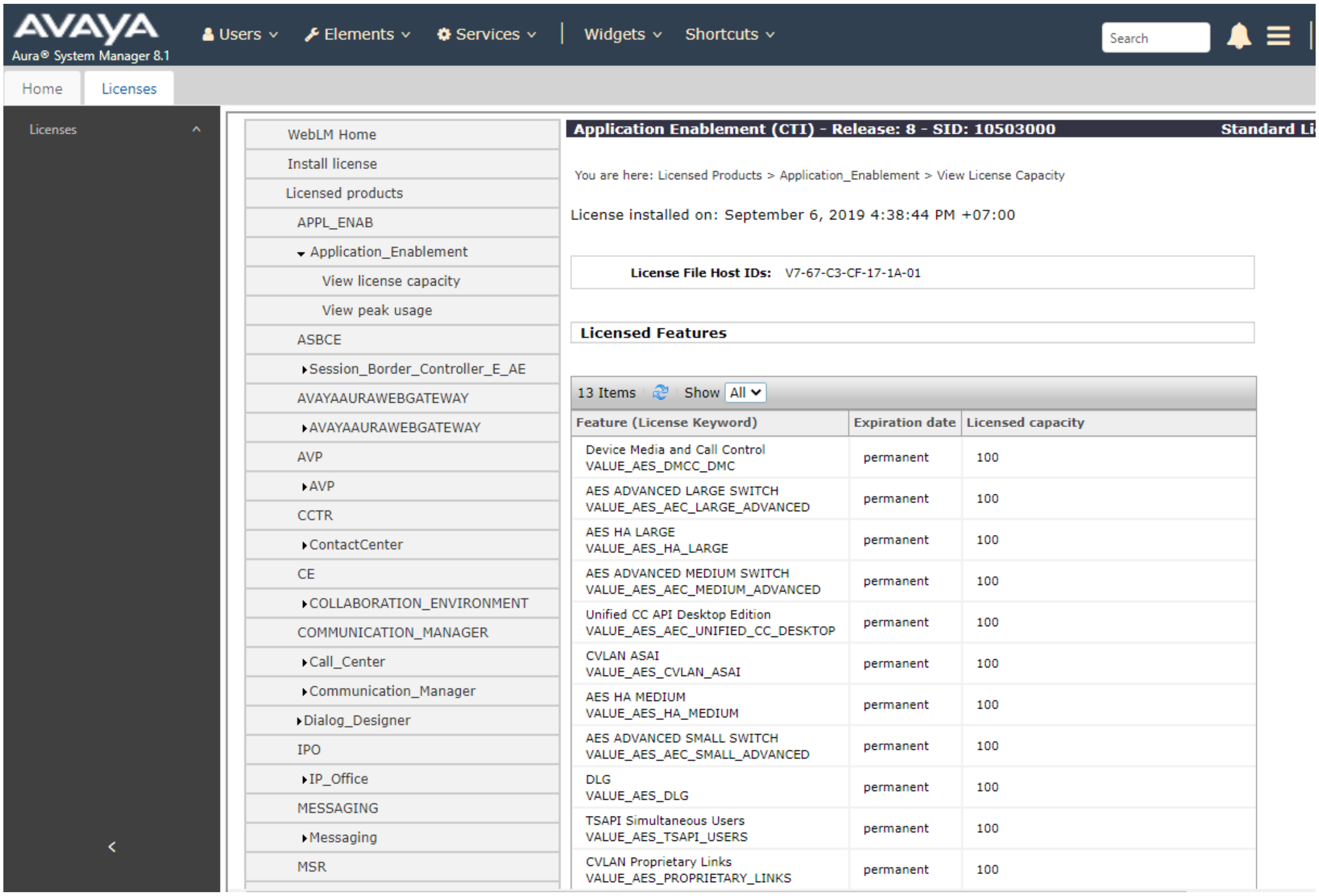
- Reserved Licenses

NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page

Copyright Â© 2009-2020 Avaya Inc. All Rights Reserved.

Select **Licensed products → APPL_ENAB → Application_Enablement** in the left pane, to display the **Licensed Features** screen in the right pane.

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



Application Enablement (CTI) - Release: 8 - SID: 10503000 Standard Li

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

License installed on: September 6, 2019 4:38:44 PM +07:00

License File Host IDs: V7-67-C3-CF-17-1A-01

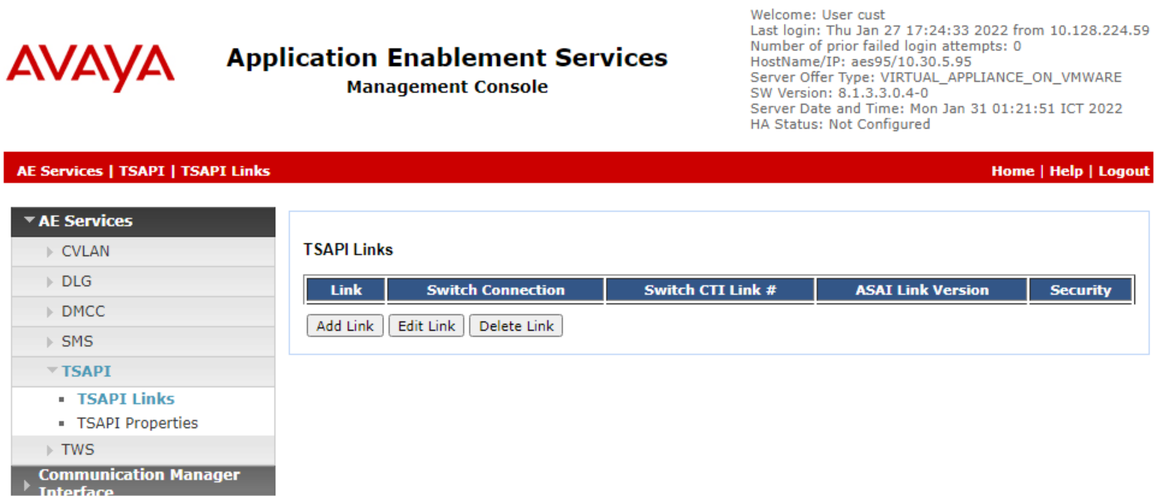
Licensed Features

13 Items Show All

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	100
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	100
AES HA LARGE VALUE_AES_HA_LARGE	permanent	100
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	100
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	100
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	100
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	100
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	100
DLG VALUE_AES_DLG	permanent	100
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	100
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	100

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**.

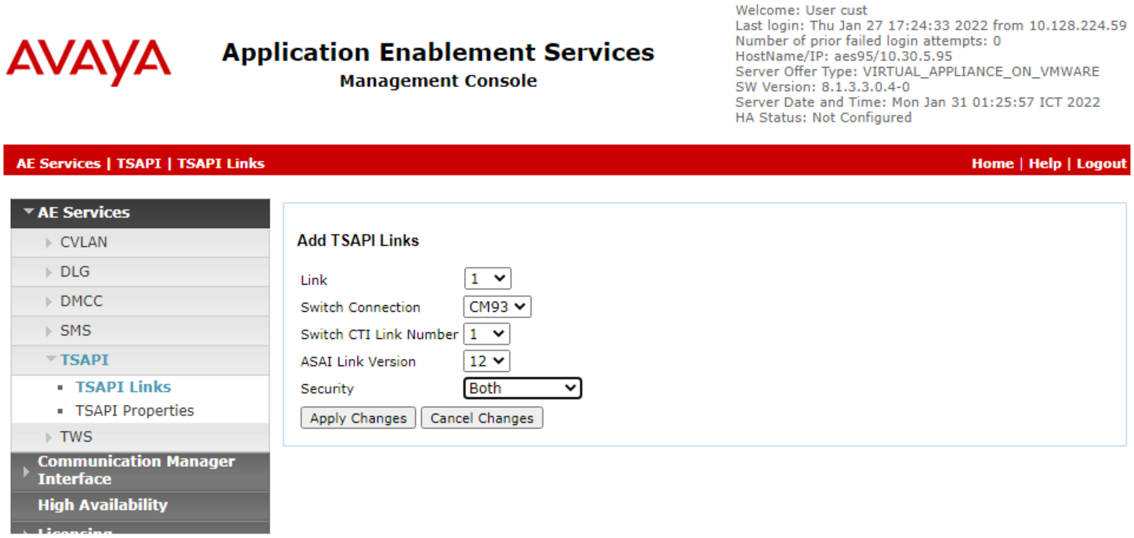


Welcome: User cust
Last login: Thu Jan 27 17:24:33 2022 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.3.0.4-0
Server Date and Time: Mon Jan 31 01:21:51 ICT 2022
HA Status: Not Configured

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security

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



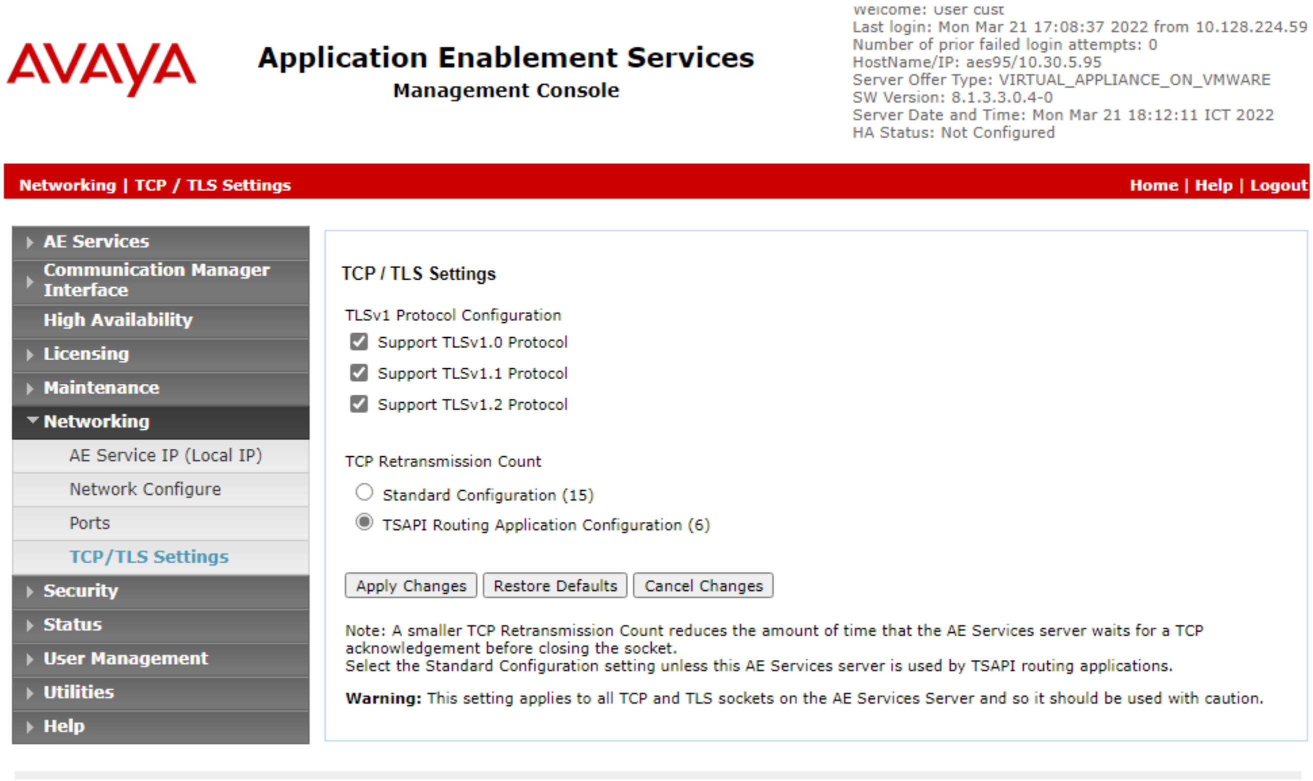
Welcome: User cust
Last login: Thu Jan 27 17:24:33 2022 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.3.0.4-0
Server Date and Time: Mon Jan 31 01:25:57 ICT 2022
HA Status: Not Configured

Add TSAPI Links

Link	1
Switch Connection	CM93
Switch CTI Link Number	1
ASAI Link Version	12
Security	Both

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.



Welcome: User cust
Last login: Mon Mar 21 17:08:37 2022 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.3.0.4-0
Server Date and Time: Mon Mar 21 18:12:11 ICT 2022
HA Status: Not Configured

TCP / TLS Settings

TLSv1 Protocol Configuration

☑ Support TLSv1.0 Protocol

☑ Support TLSv1.1 Protocol

☑ Support TLSv1.2 Protocol

TCP Retransmission Count

○ Standard Configuration (15)

● TSAPI Routing Application Configuration (6)

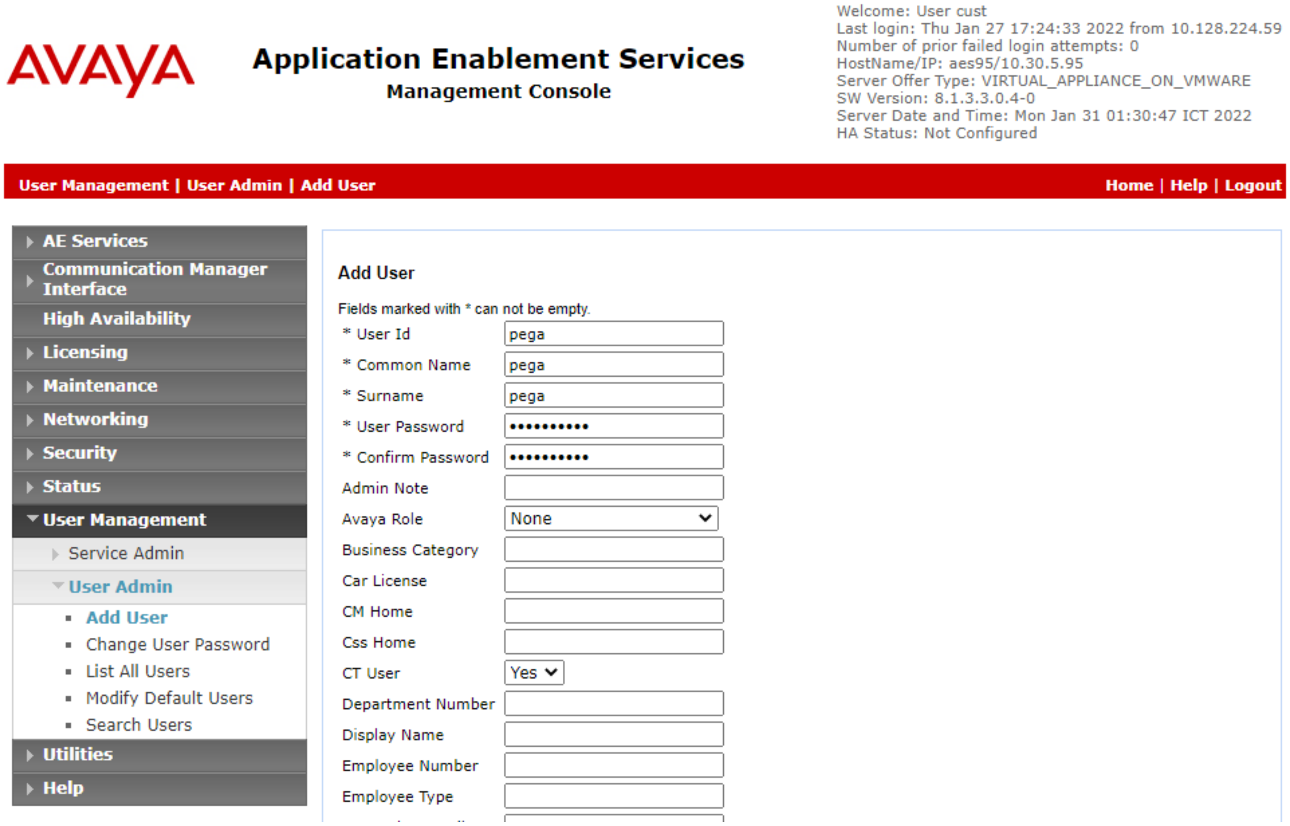
Note: A smaller TCP Retransmission Count reduces the amount of time that the AE Services server waits for a TCP acknowledgement before closing the socket.
Select the Standard Configuration setting unless this AE Services server is used by TSAPI routing applications.

Warning: This setting applies to all TCP and TLS sockets on the AE Services Server and so it should be used with caution.

6.5. Administer Pega User

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

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



Welcome: User cust
Last login: Thu Jan 27 17:24:33 2022 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.3.0.4-0
Server Date and Time: Mon Jan 31 01:30:47 ICT 2022
HA Status: Not Configured

Add User

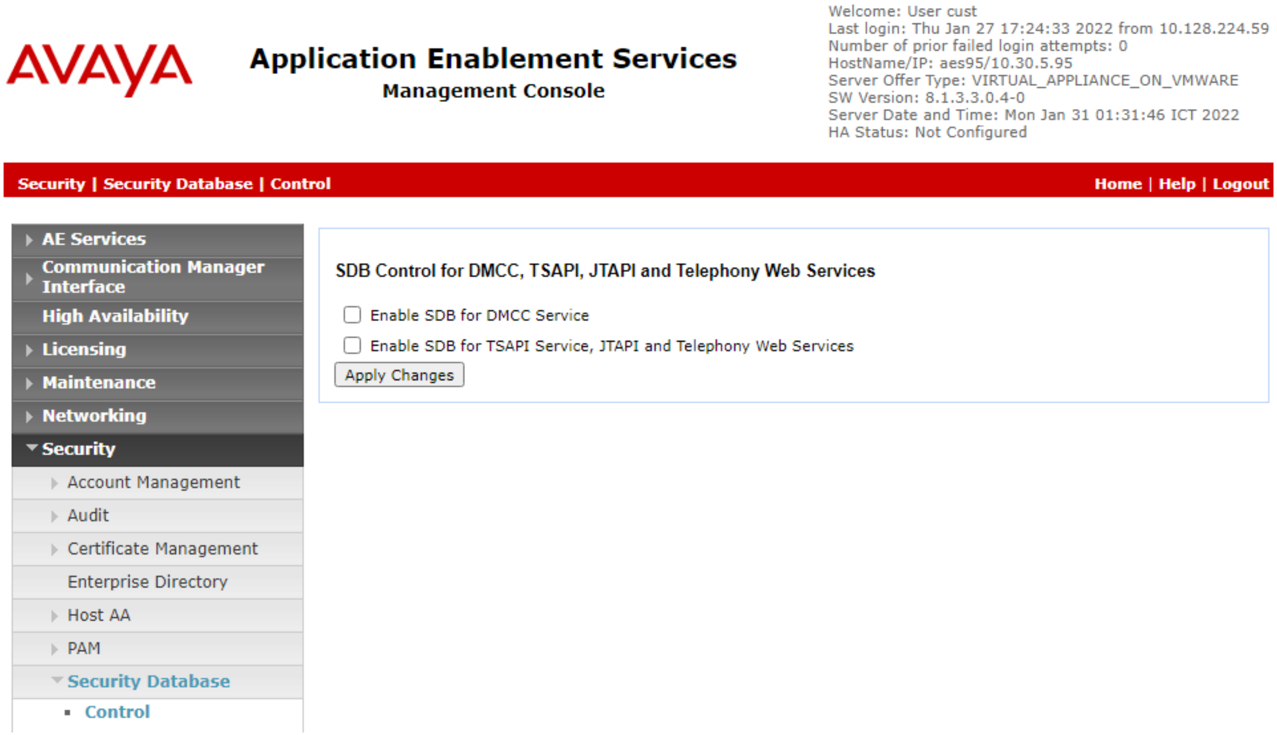
Fields marked with * can not be empty.

* User Id	pega
* Common Name	pega
* Surname	pega
* User Password	••••••••••
* Confirm Password	••••••••••
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	

6.6. Administer Security Database

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

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



Welcome: User cust
Last login: Thu Jan 27 17:24:33 2022 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.3.0.4-0
Server Date and Time: Mon Jan 31 01:31:46 ICT 2022
HA Status: Not Configured

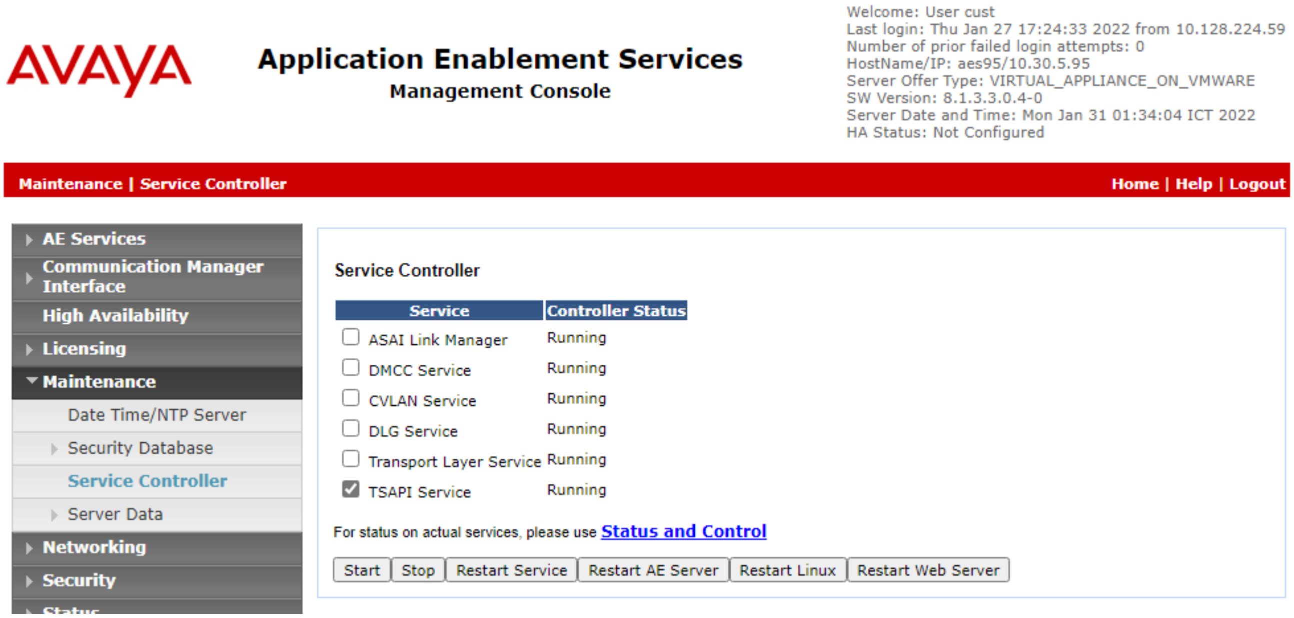
SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

☐ Enable SDB for DMCC Service

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

6.7. Restart Services

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



Welcome: User cust
Last login: Thu Jan 27 17:24:33 2022 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.3.0.4-0
Server Date and Time: Mon Jan 31 01:34:04 ICT 2022
HA Status: Not Configured

Service Controller

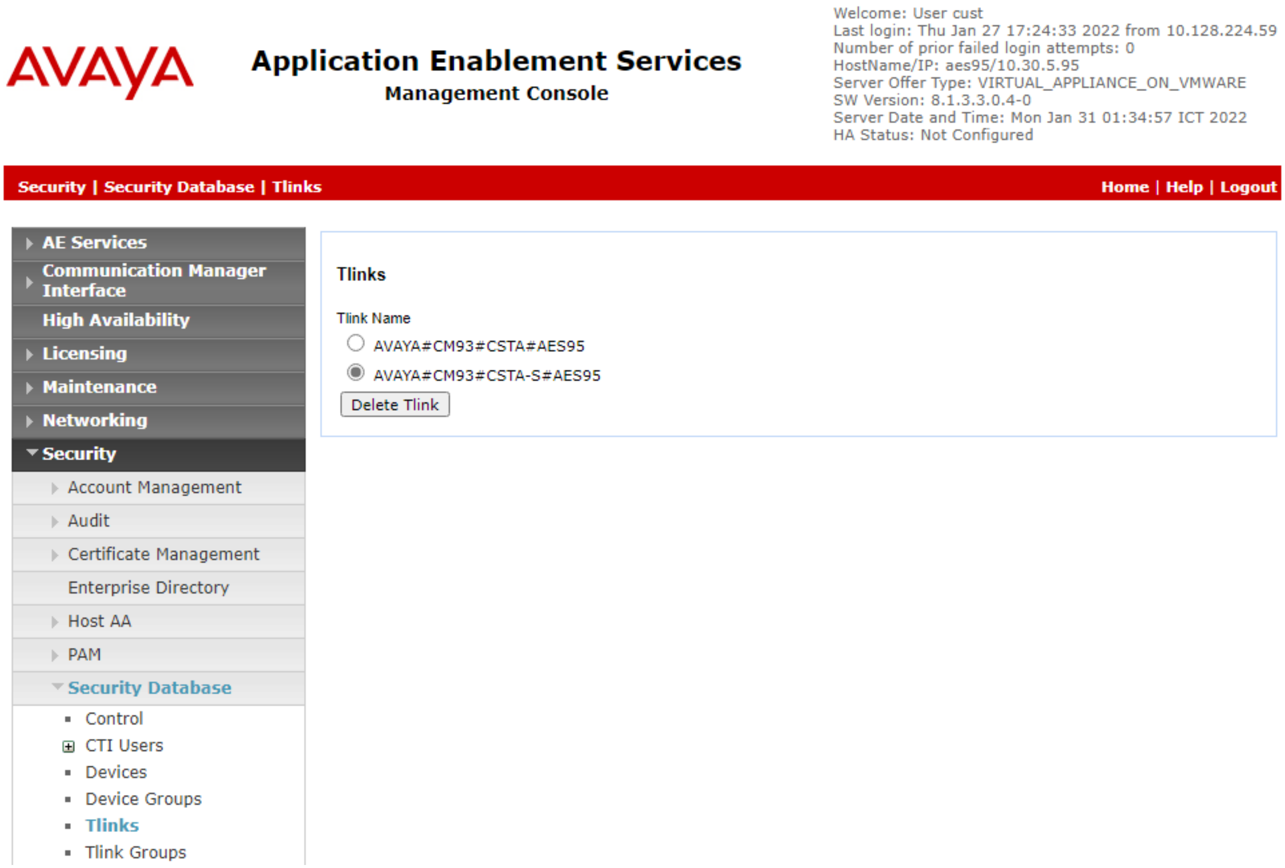
Service	Controller Status
□ ASAI Link Manager	Running
□ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
☑ TSAPI Service	Running

For status on actual services, please use Status and Control

6.8. Obtain Tlink Name

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

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



Welcome: User cust
Last login: Thu Jan 27 17:24:33 2022 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.3.0.4-0
Server Date and Time: Mon Jan 31 01:34:57 ICT 2022
HA Status: Not Configured

Tlinks

Tlink Name

○ AVAYA#CM93#CSTA#AES95
● AVAYA#CM93#CSTA-S#AES95

7. Configure Pegasystems Pega Call

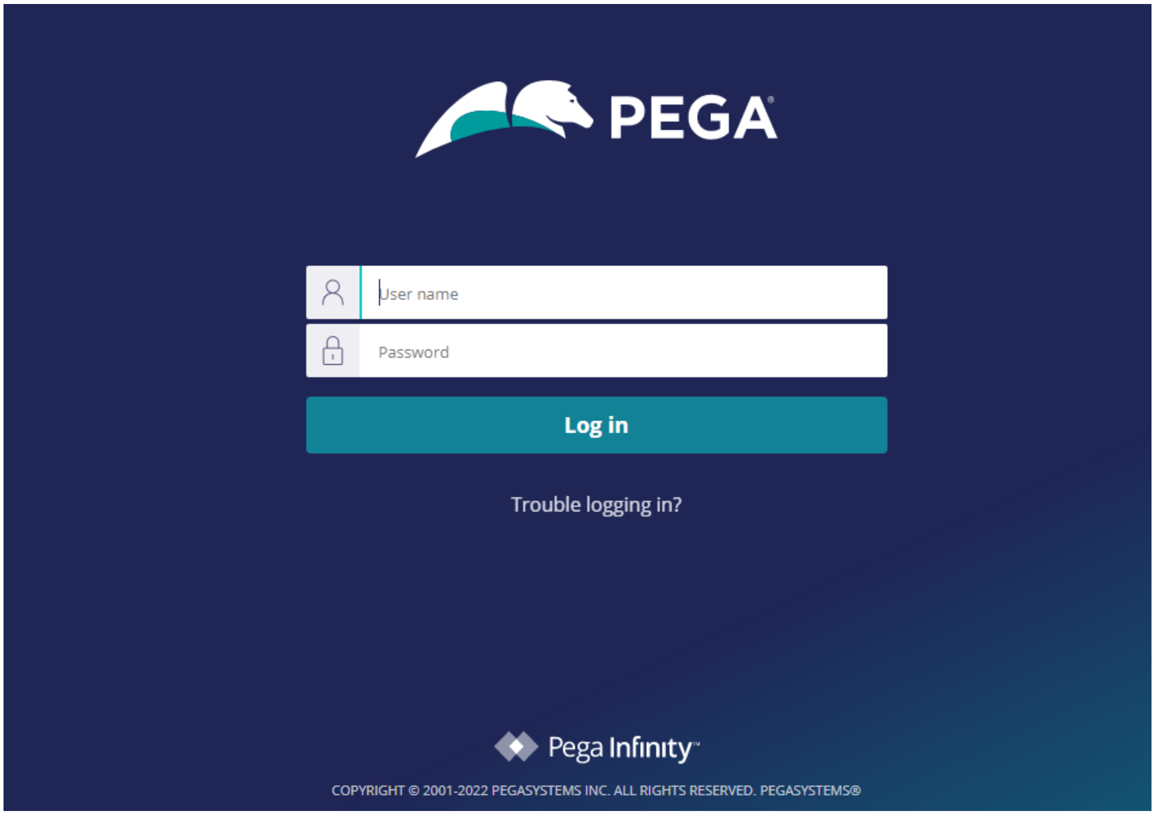
This section provides the procedures for configuring Pega Call. The procedures include the following areas:

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

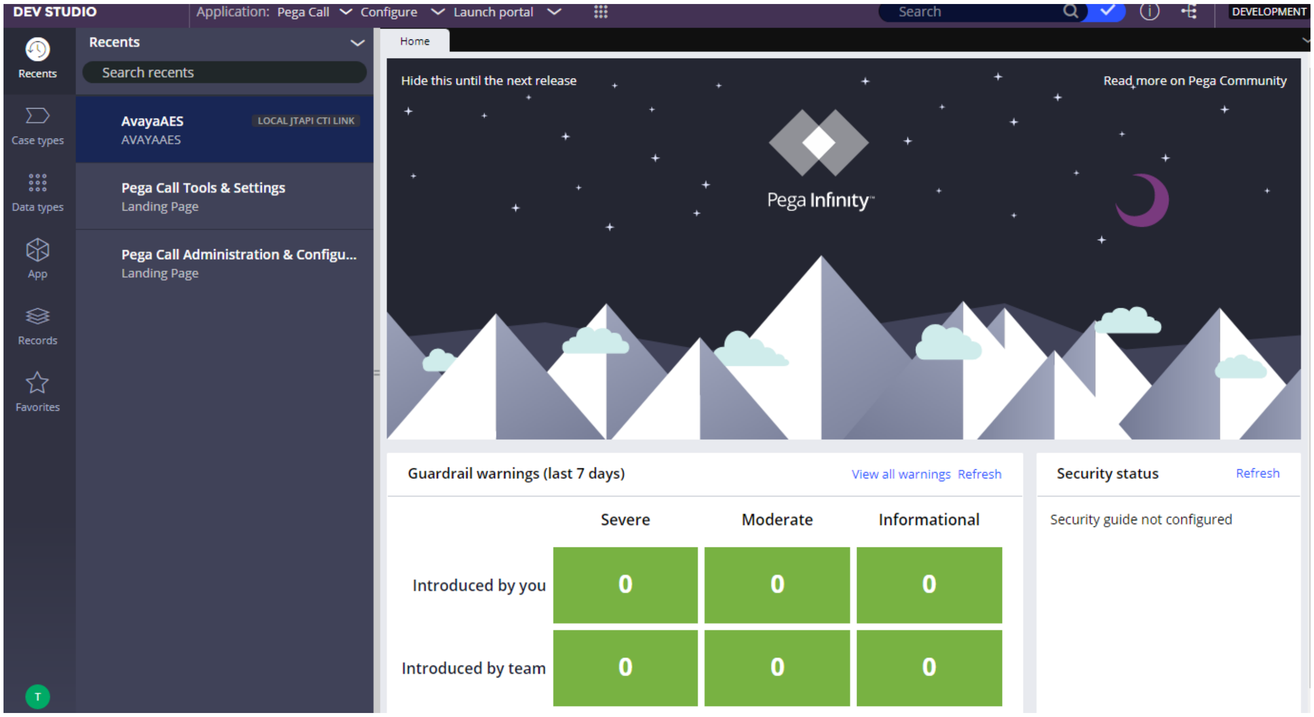
The configuration of Pega Call is performed by Pegasystems service personnel. The procedural steps are presented in these Application Notes for informational purposes. Pega Call can be configured on a single server or with components distributed across multiple servers. The solution provides a customizable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

7.1. Launch Web Interface

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


PEGA
User name
Password
Log in
Trouble logging in?
Pega Infinity
COPYRIGHT © 2001-2022 PEGASYSTEMS INC. ALL RIGHTS RESERVED. PEGASYSTEMS®

After login successfully the screen below is displayed:



Guardrail warnings (last 7 days)

View all warnings Refresh

	Severe	Moderate	Informational
Introduced by you	0	0	0
Introduced by team	0	0	0

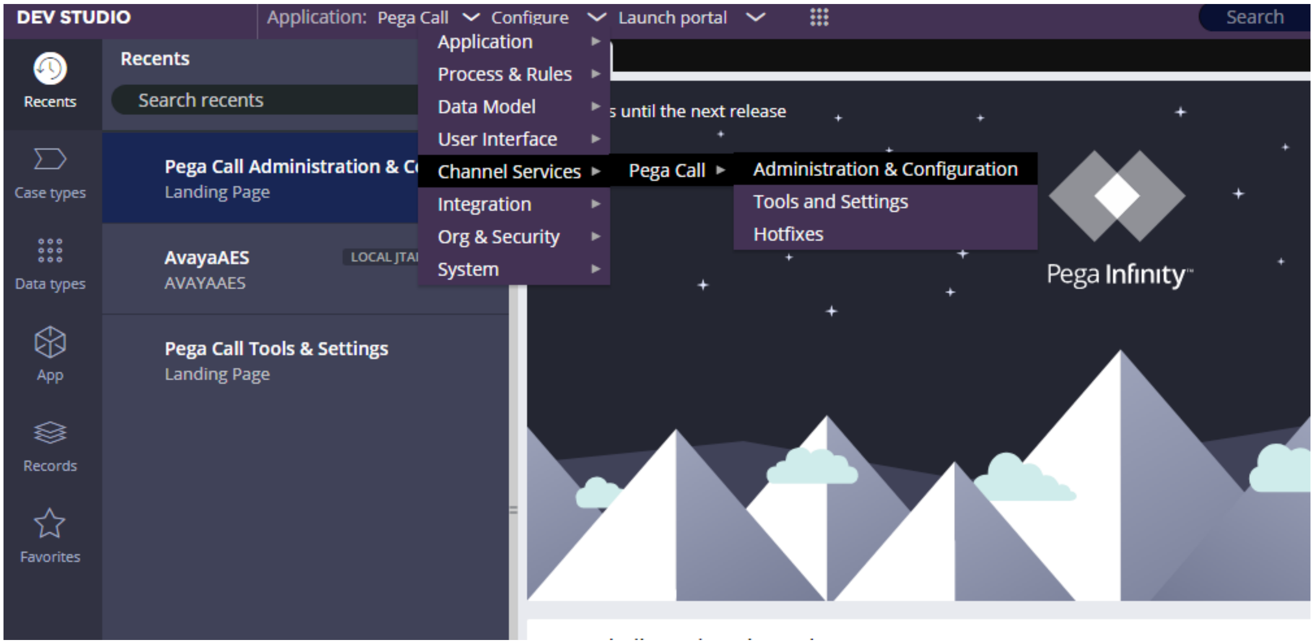
Security status

Refresh

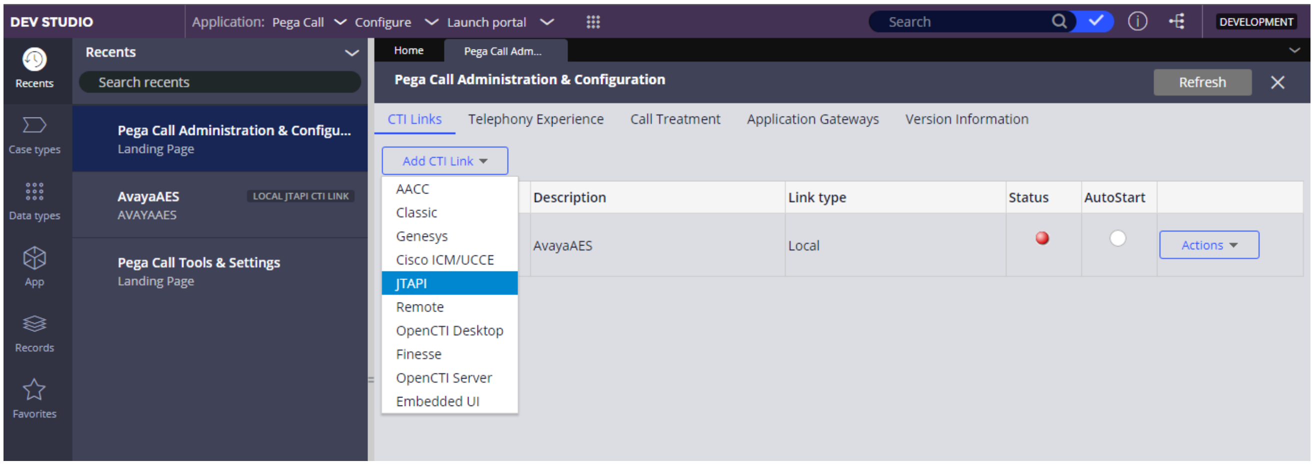
Security guide not configured

7.2. Administer CTI Link

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

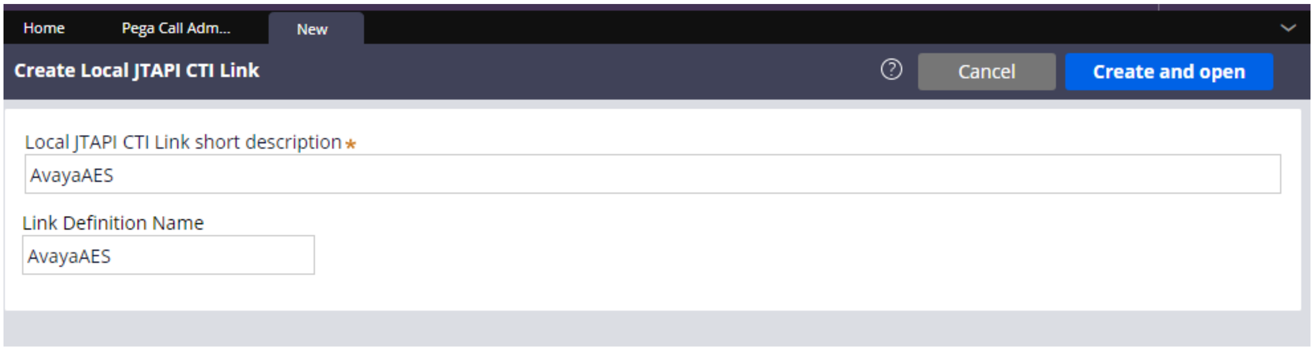


The **Pega Call Administration & Configuration** screen is displayed. Select **CTI Links → Add CTI Link → JTAPI**, as shown below.



Description	Link type	Status	AutoStart	
AvayaAES	Local	●	○	Actions

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

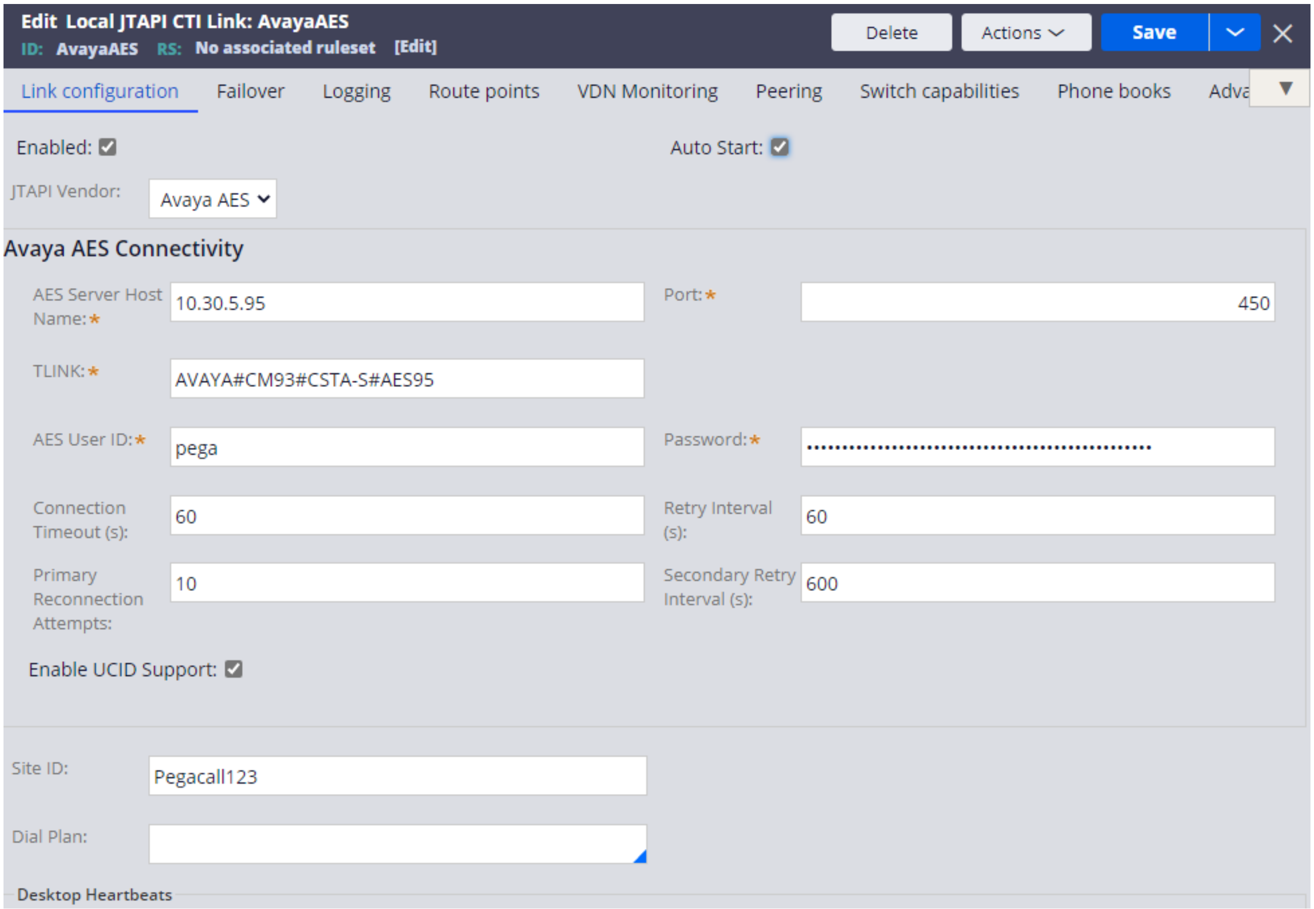


Local JTAPI CTI Link short description* AvayaAES

Link Definition Name AvayaAES

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

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


Edit Local JTAPI CTI Link: AvayaAES
ID: AvayaAES RS: No associated ruleset [Edit]

Enabled: ☑
Auto Start: ☑
JTAPI Vendor: Avaya AES

Avaya AES Connectivity

AES Server Host Name:*	10.30.5.95	Port:*	450
TLINK:*	AVAYA#CM93#CSTA-S#AES95		
AES User ID:*	pega	Password:*	••
Connection Timeout (s):	60	Retry Interval (s):	60
Primary Reconnection Attempts:	10	Secondary Retry Interval (s):	600

Enable UCID Support: ☑

Site ID: Pegacall123

Dial Plan:

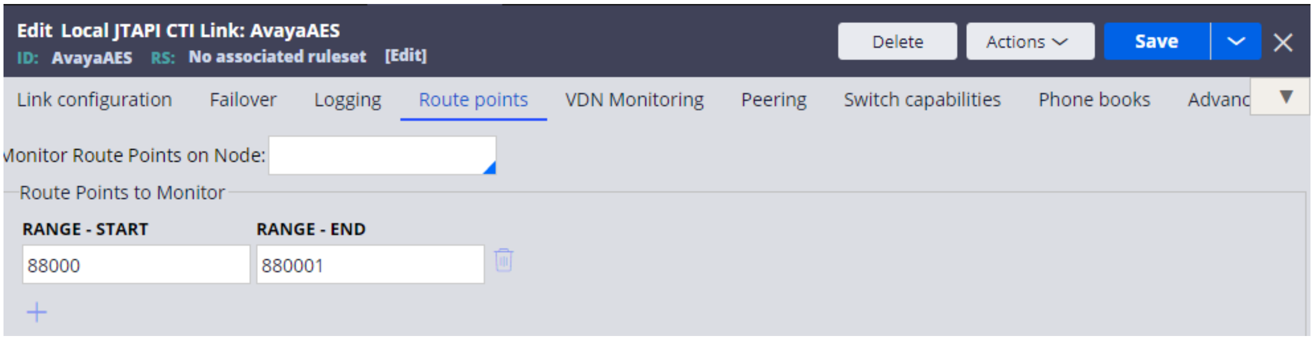
Desktop Heartbeats

7.3. Administer Route Points

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

Select the **Route points** tab. For **Monitor Route Points on Node**, select the applicable node (not shown). In the **Route Points to Monitor** sub-section, add the routing VDN extensions from **Section 5.6**.

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



Edit Local JTAPI CTI Link: AvayaAES

ID: AvayaAES RS: No associated ruleset [Edit]

Monitor Route Points on Node:

Route Points to Monitor

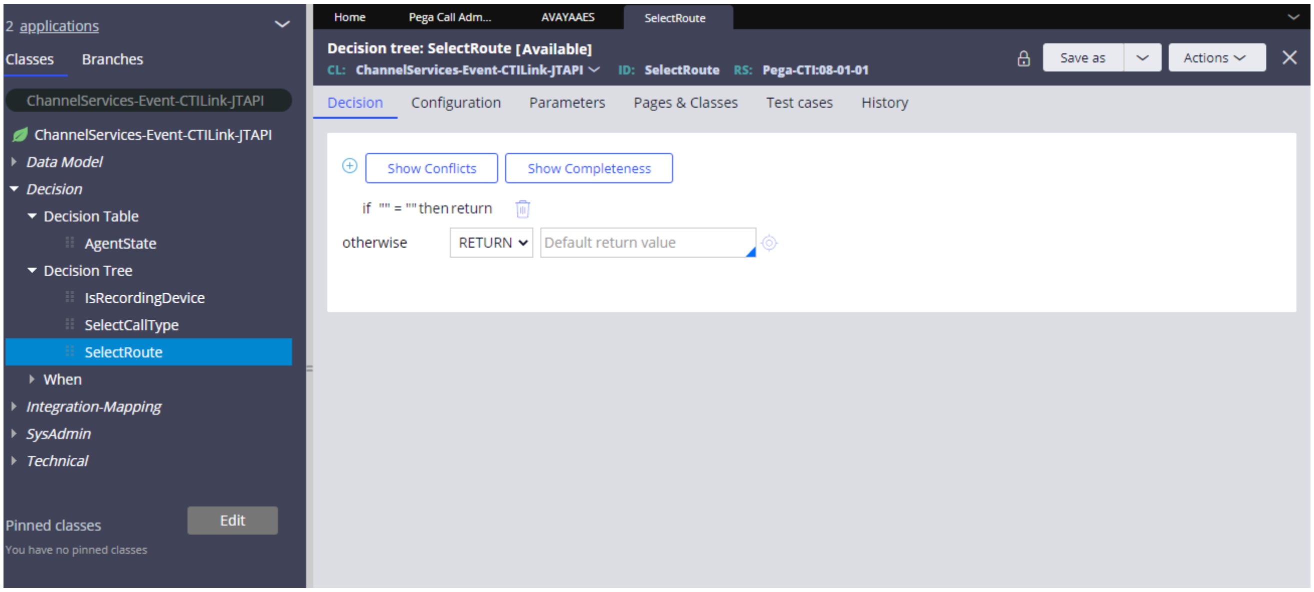
RANGE - START	RANGE - END
88000	880001

7.4. Administer Decision Tree

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

Prior to administering decision tree, follow reference **[6]** to create a RuleSet, which is a set of 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 (not shown) and enter "**ChannelServices-Event-CTILink-JTAPI**" in the search area.

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



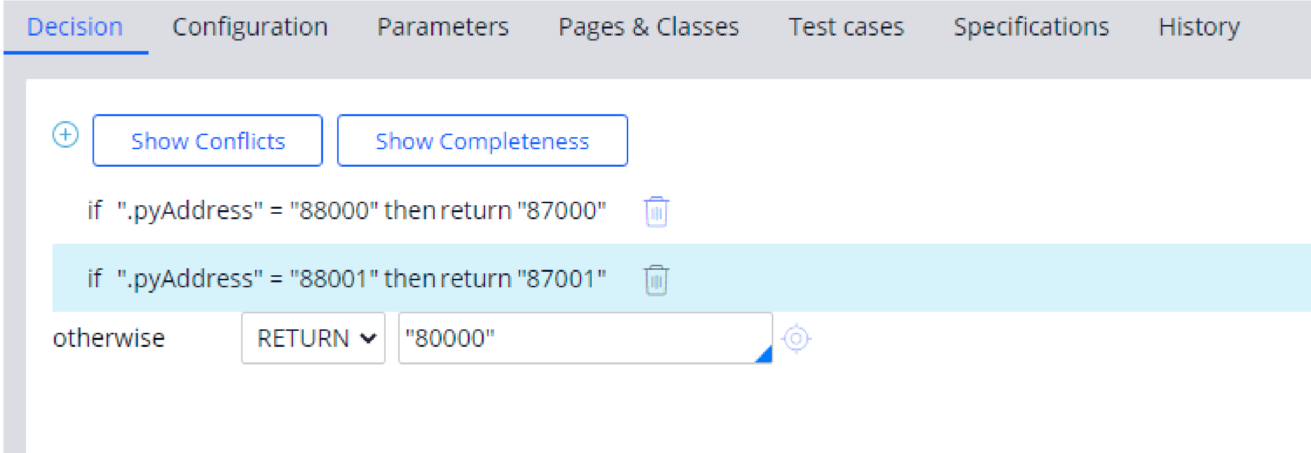
Decision tree: SelectRoute [Available]
CL: ChannelServices-Event-CTILink-JTAPI ID: SelectRoute RS: Pega-CTI:08-01-01

if "" = "" then return
otherwise RETURN Default return value

The **Decision Tree: SelectRoute** screen is displayed. Follow reference **[6]** to configure the desired routing logic.

The screenshot below shows the routing logic used in the compliance testing. The **.pyAddress** parameter was used as the matching criteria to the routing VDN extensions in **Section 5.6**.

As shown in **Section 3**, extensions **87000** and **87001** are existing skill groups on Communication Manager, and extension **80000** is the supervisor.



if ".pyAddress" = "88000" then return "87000"

if ".pyAddress" = "88001" then return "87001"

otherwise RETURN "80000"

8. Verification Steps

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

8.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify status of the administered CTI link by using the “status 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   Version  Mnt   AE Services      Service       Msgs     Msgs
Link           Busy  Server           State         Sent     Rcvd

1     12       no    aes95            established   14       14
```

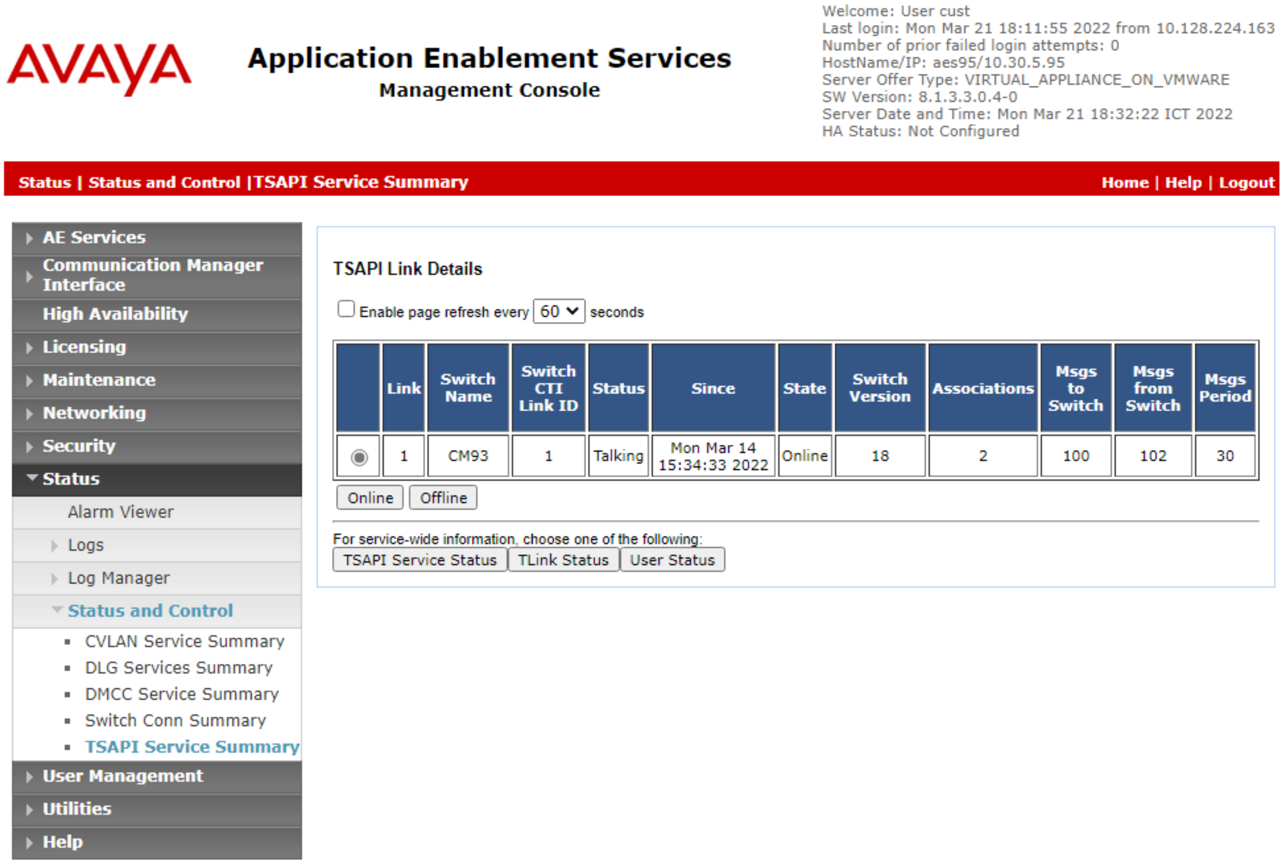
Enter the command **list agent-loginID** verify that agent **80000** and **80001** shown in **Section 5.4** is logged-in to extension **70010** and **70009**.

```
list agent-loginID
                               AGENT LOGINID
Login ID     Name           Extension     Dir Agt  AAS/AUD        COR Ag Pr SO
               Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv

80000         Voice Agent    70010                             1   lvl
                 1/01     /       /       /       /       /

80001         Voice Agent1   70009                             1   lvl
                 1/01     /       /       /       /       /
```

8.2. Verify Avaya Aura® Application Enablement Services

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

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



Welcome: User cust
Last login: Mon Mar 21 18:11:55 2022 from 10.128.224.163
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.3.0.4-0
Server Date and Time: Mon Mar 21 18:32:22 ICT 2022
HA Status: Not Configured

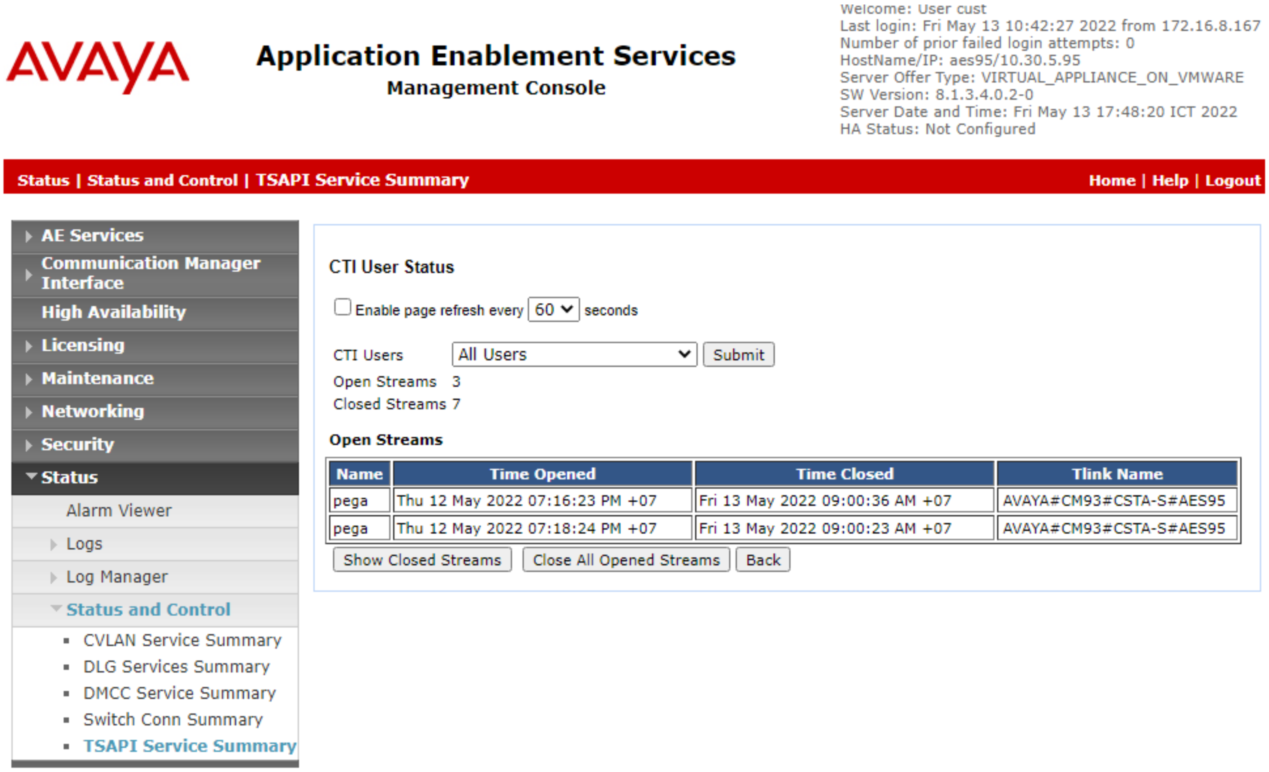
TSAPI Link Details

☐ 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
●	1	CM93	1	Talking	Mon Mar 14 15:34:33 2022	Online	18	2	100	102	30

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

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



Welcome: User cust
Last login: Fri May 13 10:42:27 2022 from 172.16.8.167
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.4.0.2-0
Server Date and Time: Fri May 13 17:48:20 ICT 2022
HA Status: Not Configured

CTI User Status

☐ Enable page refresh every 60 seconds

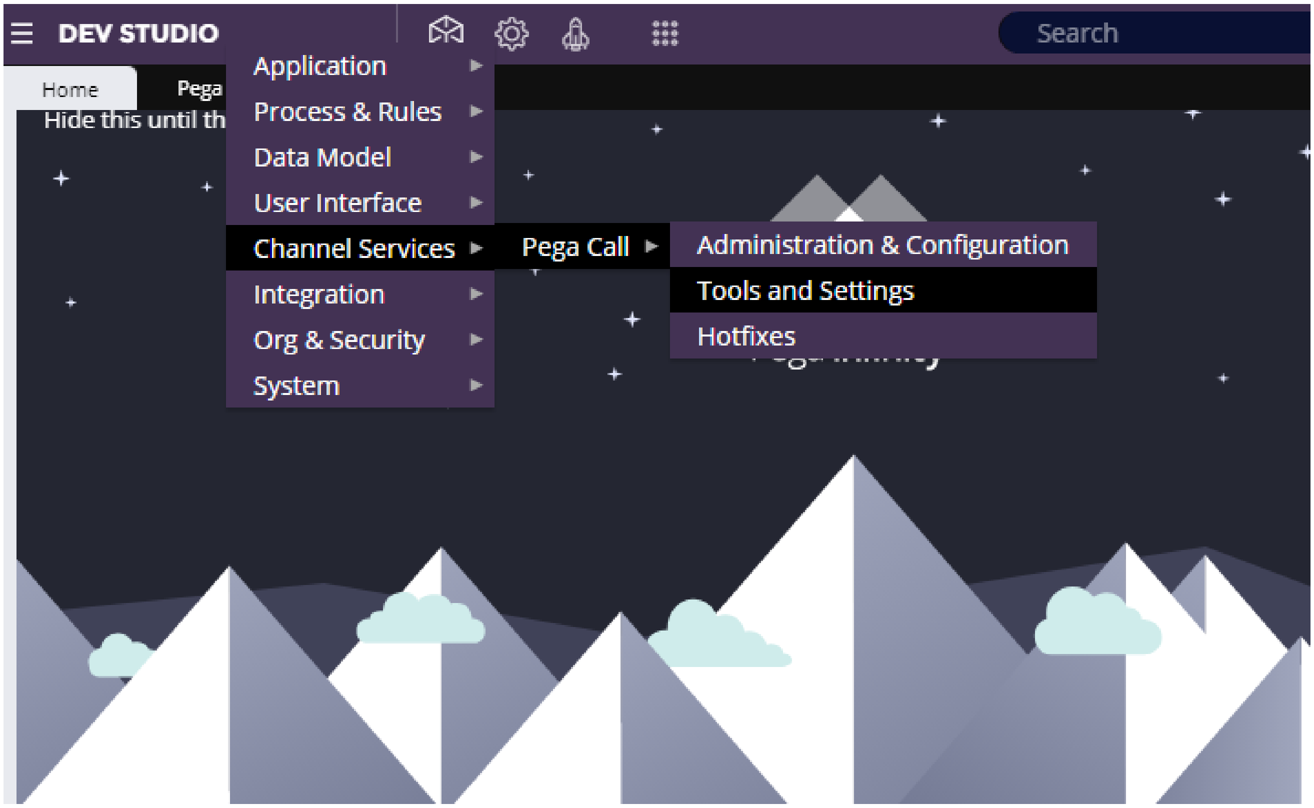
CTI Users: All Users
Open Streams 3
Closed Streams 7

Open Streams

Name	Time Opened	Time Closed	Tlink Name
pega	Thu 12 May 2022 07:16:23 PM +07	Fri 13 May 2022 09:00:36 AM +07	AVAYA#CM93#CSTA-S#AES95
pega	Thu 12 May 2022 07:18:24 PM +07	Fri 13 May 2022 09:00:23 AM +07	AVAYA#CM93#CSTA-S#AES95

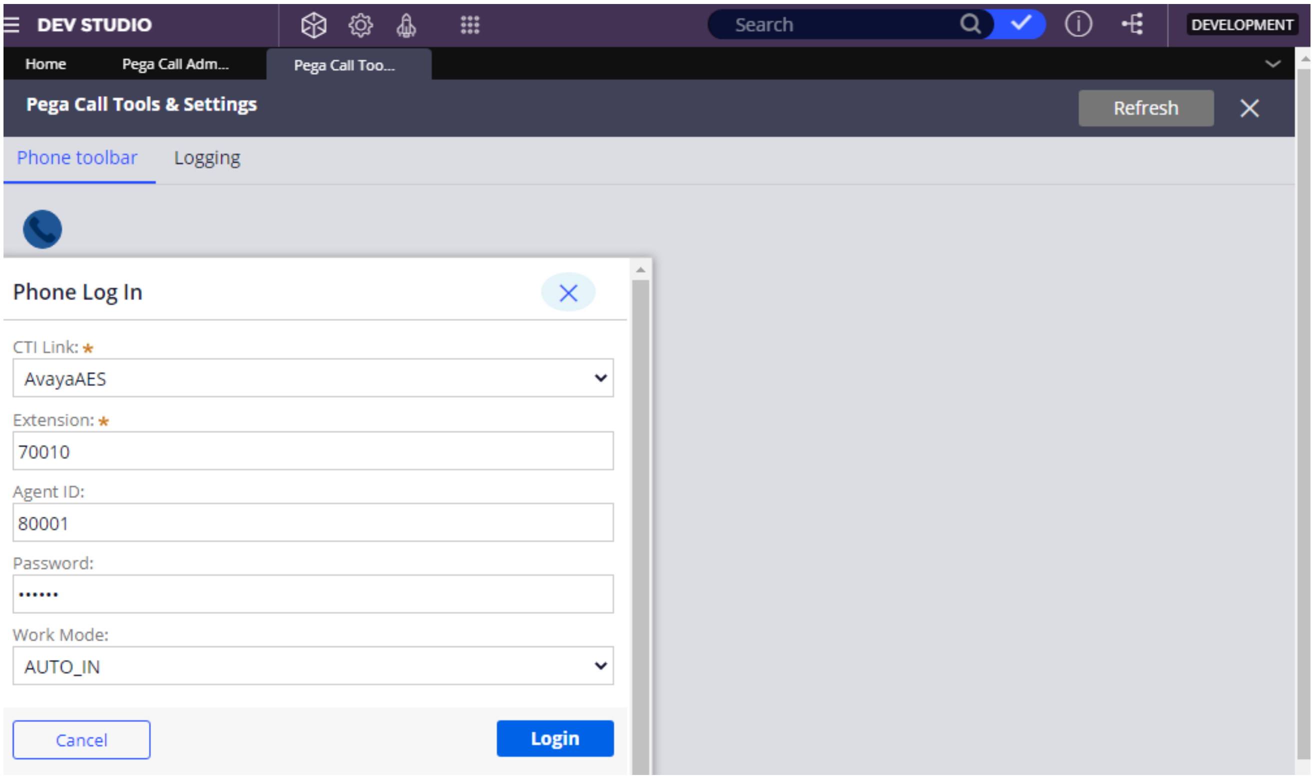
8.3. Verify Pegasystems Pega Call

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



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

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



CTI Link: * AvayaAES

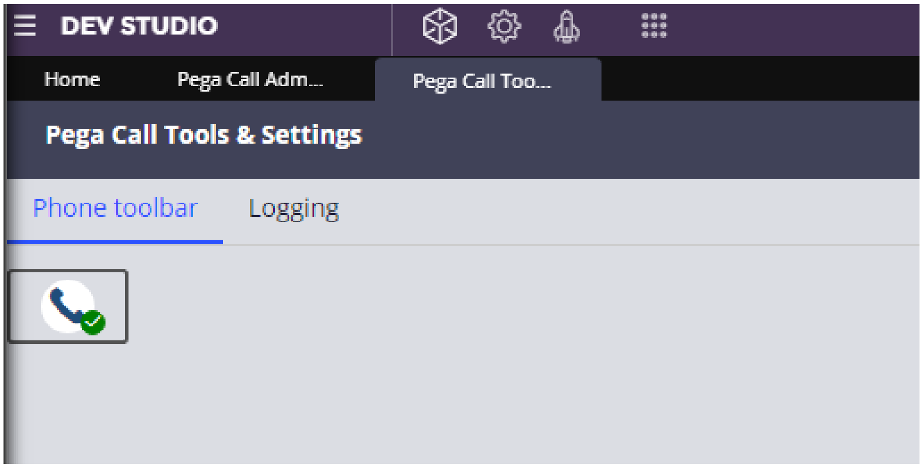
Extension: * 70010

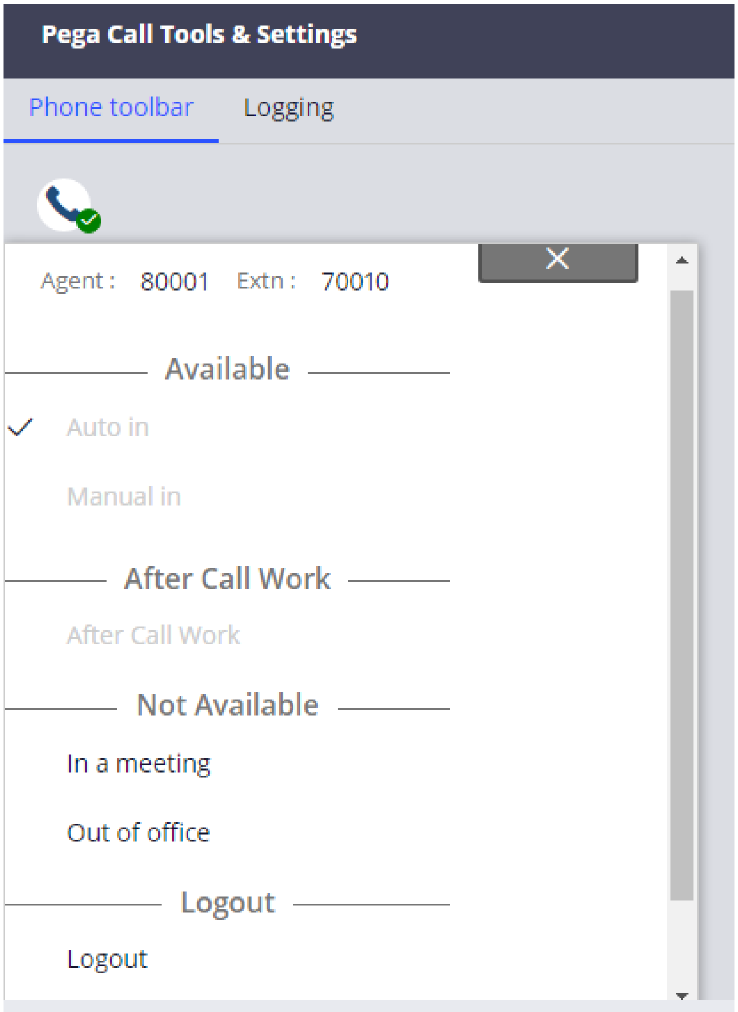
Agent ID: 80001

Password: ••••••

Work Mode: AUTO_IN

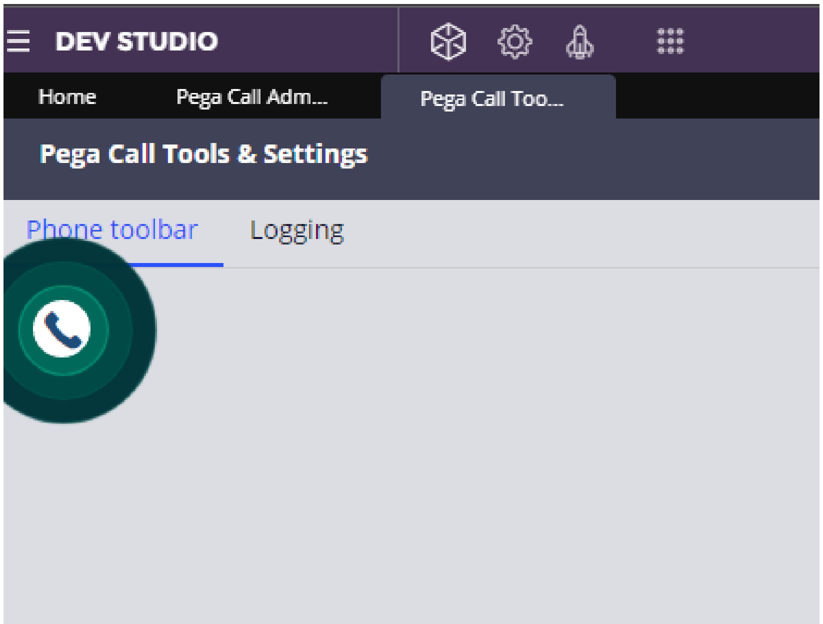
Verify that the screen is updated as shown below with a green handset icon, indicating the agent is logged in and available for ACD calls.

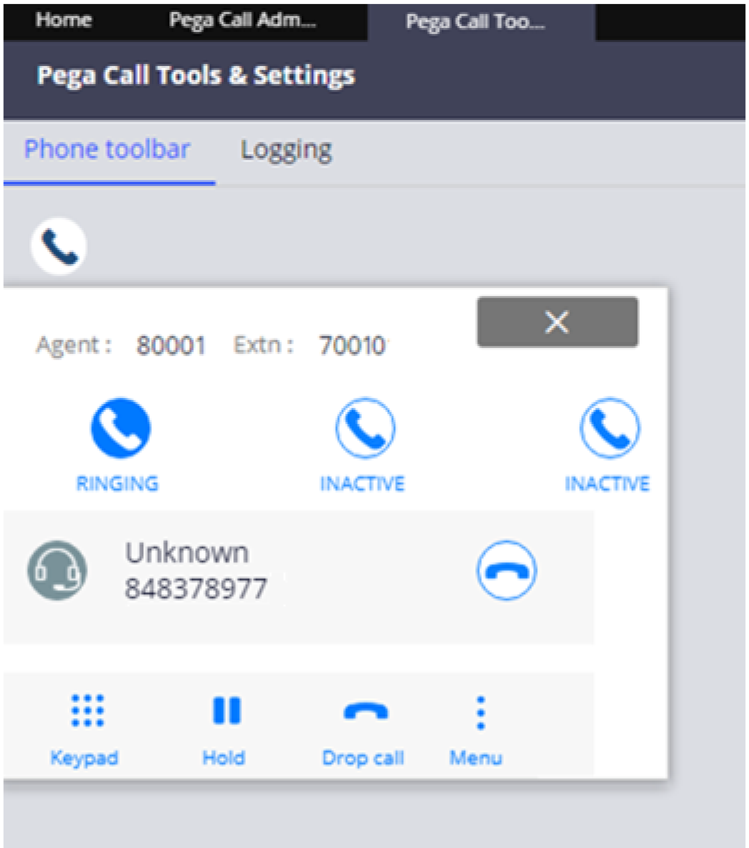




Agent : 80001 Extn : 70010

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.

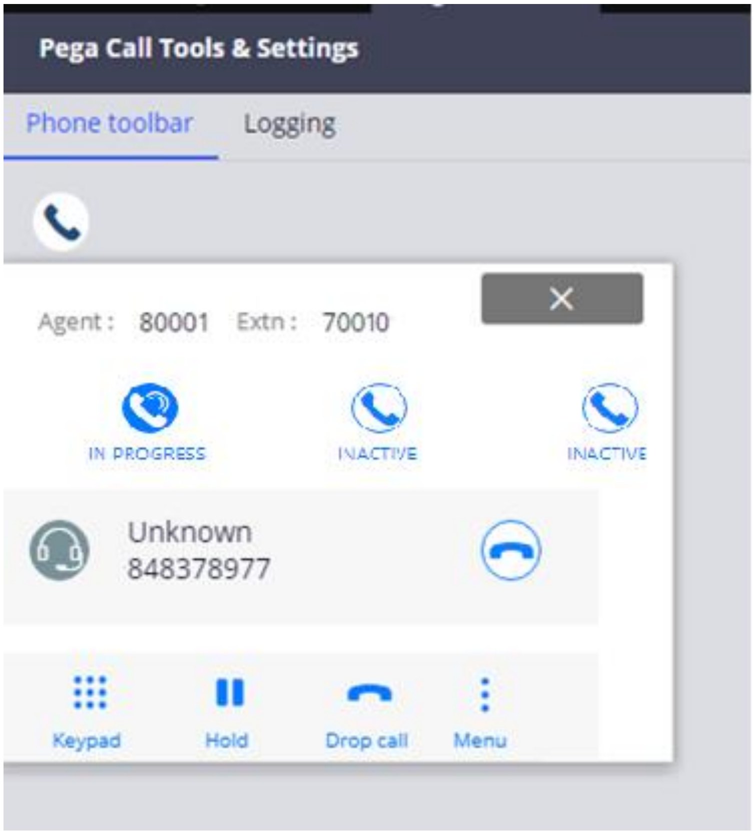




Agent : 80001 Extn : 70010

Unknown
848378977

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



9. Conclusion

These Application Notes describe the configuration steps required for the Pegasystems Pega Call 8.5.5 to successfully interoperate with Avaya Aura® Communication Manager 8.1.3.3 and Avaya Aura® Application Enablement Services 8.1.3.3. All feature and serviceability test cases were completed with observations noted in **Section 2.2.**

10. Additional References

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

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

1. *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 12, July 2021
2. *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 10, Sept 2021
3. *Administering Avaya Aura® System Manager*, Release 8.1.x, Issue 17, Nov 2021
4. *Administering Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 12, Oct 2021
5. *Pega Call Configuration and Operations Guide for CTI Link Engine with Avaya AES CTI*, Software Version 7.21, May 2016, available at https://pdn.pega.com.
6. *Pega 8.5.5 platform Help for application developers*, available as part of the Pegasystems web interface and at https://pdn.pega.com.

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.