Avaya Solution & Interoperability Test Lab

Application Notes for VIS Global RADIUS 3.2.8 with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for VIS Global RADIUS 3.2.8 to interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1. RADIUS is an omni-channel contact center solution which integrates with Avaya contact center CC Elite base solution. On the premise, the Cloud Connector Server (RADIUS XT Connect) uses the Java Telephony Application Programming Interface (JTAPI) from Avaya Aura® Application Enablement Services to provide screen pop and call control via 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 VIS Global RADIUS 3.2.8 to interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1.

RADIUS is built and deployed in Amazon Cloud and can be deployed on premises. The solution supports both inbound and outbound voice calls through integration with Avaya Contact Center Elite via campaigns. In this compliance testing, which was setup as an on-premise solution, a cloud connector server, the RADIUS XT Connect is needed to provide integration to the RADIUS Cloud. The user application components include the following:

- INTELLO – Web base application for Agents
- ATOMOS – Web base applications tools for Supervisors/Administrators
- AXIS – Historical Reporting Tool
- Ctrl+R – Windows base for configuring RADIUS in on-premise deployment

The Agent desktop uses INTELLO for login and perform call center operations whereas the Supervisor desktop uses ATOMOS and AXIS for configuration and obtaining historical reports. However, AXIS will not be utilized in this compliance testing for the historical reporting as it is not the purpose of this compliance testing. Also, this is an off-premise deployment environment, hence the component Ctrl+R will not be utilized here.

RADIUS XT Connect uses 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. VDN and agent stations are monitored to provide this function. 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.

2. General Test Approach and Test Results

The feature test cases were performed manually. Two campaigns are created manually i.e., for inbound and outbound voice calls by the Administrators and/or Supervisors using ATOMOS via browser. RADIUS agent logs in from the PC via INTELO via browser. Incoming calls were placed to a general routing VDNs with available agents running the web based applications on their desktops with Avaya softphones. Manual call controls were exercised from RADIUS to verify proper call actions such as answering and transferring of calls. Outbound calls were also initiated from agents and exercising manual call controls such as hold/resume and transferring of calls.

The serviceability test cases were performed manually by restarting the RADIUS connector to Application Enablement Services (AES) and AES CTI link on Communication Manager.

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 Enablement Services and RADIUS did not include use of any specific encryption features.

This test was conducted in a lab environment simulating a basic customer enterprise network environment. The testing focused on the standards-based interface between the Avaya solution and the third party solution. The results of testing are therefore considered to be applicable to either a premise-based deployment or to a hosted or cloud deployment where some elements of the third party solution may reside beyond the boundaries of the enterprise network, or at a different physical location from the Avaya components.

Readers should be aware that network behaviors (e.g. jitter, packet loss, delay, speed, etc.) can vary significantly from one location to another, and may affect the reliability or performance of the overall solution. Different network elements (e.g. session border controllers, soft switches, firewalls, NAT appliances, etc.) can also affect how the solution performs.

If a customer is considering implementation of this solution in a cloud environment, the customer should evaluate and discuss the network characteristics with their cloud service provider and network organizations, and evaluate if the solution is viable to be deployed in the cloud.

The network characteristics required to support this solution are outside the scope of these Application Notes. Readers should consult the appropriate Avaya and third party documentation for the product network requirements. Avaya makes no guarantee that this solution will work in all potential deployment configurations.

2.1. Interoperability Compliance Testing

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

- 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 and outbound ACD calls, call transfer, consult, conference, multiple agents and multiple calls.

The serviceability testing focused on verifying the ability of RADIUS to recover from adverse conditions, such as restart of RADIUS XT Connect server connection to AES and restart of Avaya AES CTI link.

2.2. Test Results

All test cases were executed and verified successfully.

2.3. Support

Technical support on RADIUS can be obtained from VIS Global through the following:

- Email: salesenquiry@visnet.in
- Phone: +91 80 45453300

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1** on the next page. 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, the following in the table are the summary of the agent and routing setup for Avaya contact center.

Device Type	Extension
Inbound VDN	14001
Skill Group	13001
Agent Station	10002, 10003
Agent ID	11002, 11003

Agents log into the INTELLO web based application via browser on their Desktop. Agents uses softphone such as Avaya one-X® Communicator or Avaya Agent for Desktop for voice communication with customer. Supervisor/Administrator log into ATOMOS web based application via browser for configuration and setup but do not handle the voice calls.

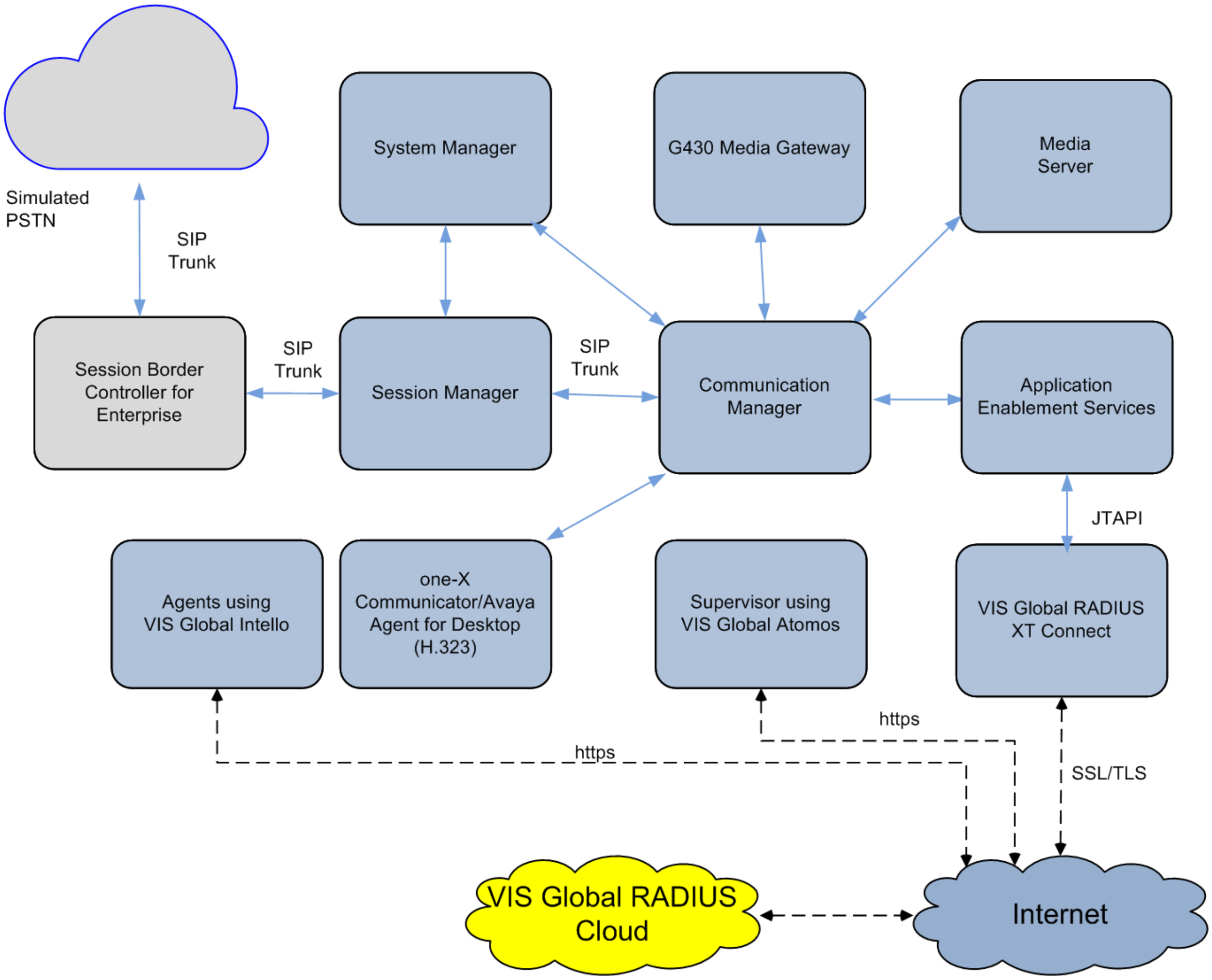

Simulated PSTN
SIP Trunk
System Manager
G430 Media Gateway
Media Server
Session Border Controller for Enterprise
SIP Trunk
Session Manager
SIP Trunk
Communication Manager
Application Enablement Services
JTAPI
Agents using VIS Global Intello
one-X Communicator/Avaya Agent for Desktop (H.323)
Supervisor using VIS Global Atomos
VIS Global RADIUS XT Connect
https
https
SSL/TLS
VIS Global RADIUS Cloud
Internet

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	R10.1 SP2 (10.1.0.2.0.974.27607)
Avaya G430 Media Gateway	42.4.0
Avaya Aura® Media Server	10.1.0.101
Avaya Aura® Session Manager	R10.1 SP2 (10.1.0.2.1010215)
Avaya Aura® System Manager	R10.1 SP2 Build 10.1.0.0.537353 Hot Fix 1010215160
Avaya Application Enablement Services	R10.1 SP2 (10.1.0.2.0.12)
Avaya Session Border Controller for Enterprise	10.1.0.0-32-21432
Avaya one-X® Communicator (H.323)	6.2.14.4-SP14p5
Avaya Agent for Desktop (H.323)	2.0.6.24.3002
VIS Global RADIUS XT Connect (Cloud Connector) running on Virtual Machine • CentOS Stream • Avaya JTAPI Client SDK	3.2.8 8 10.1.0.2 HF50
VIS Global RADIUS Cloud • INTELLO • ATOMOS	 3.2.8 3.2.8

Note: *All Avaya servers and RADIUS server are running on Virtual Machines.*

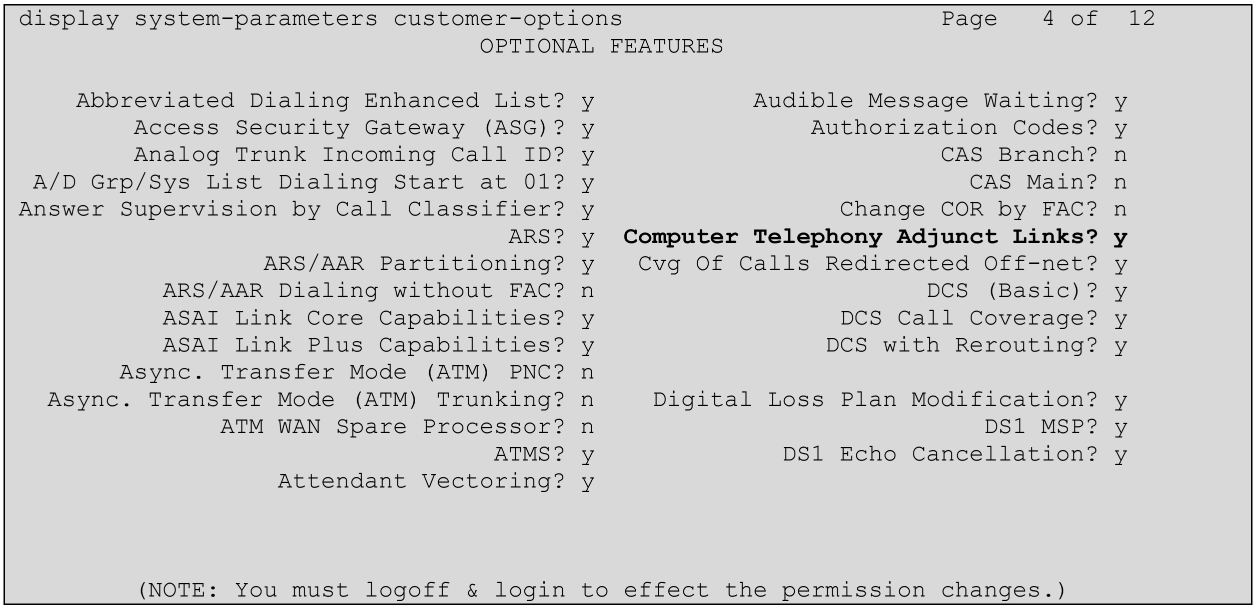
5. Configure Avaya Aura® Communication Manager

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

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



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

5.2. 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 3                                                  Page   1 of   3
                                    CTI LINK
 CTI Link: 3
Extension: 10093
     Type: ADJ-IP
                                                                       COR: 1
     Name: TSAPI Service - AES 10x
Unicode Name? n
```

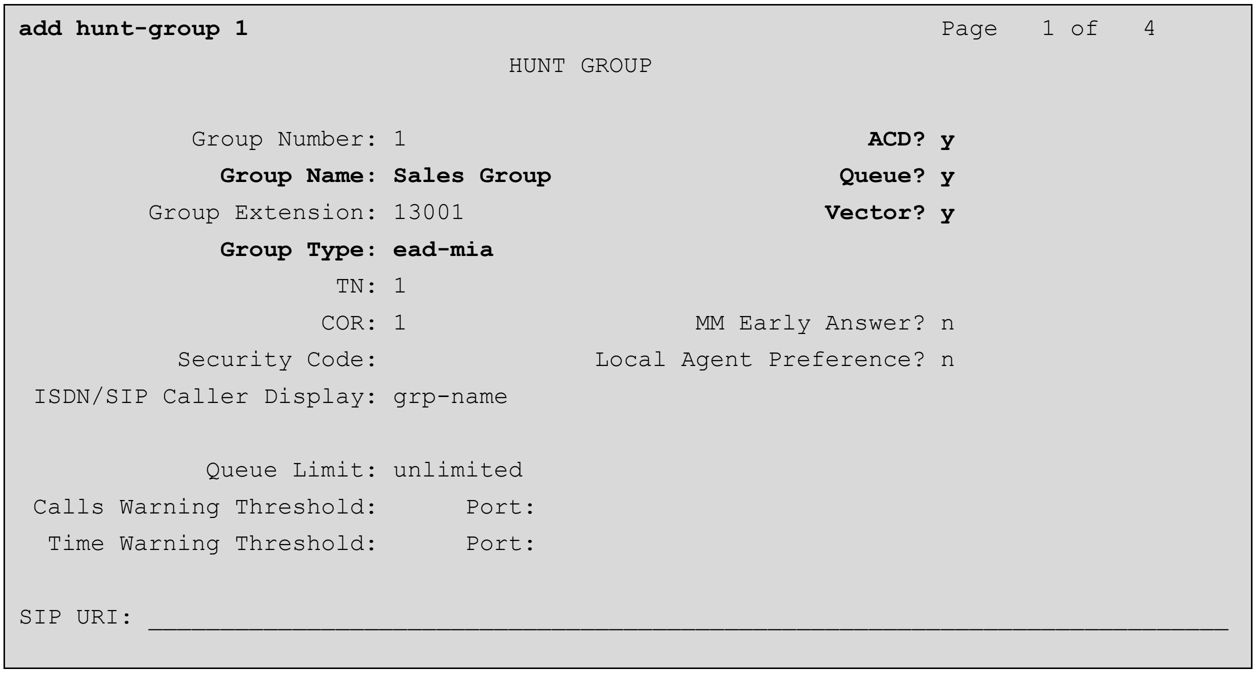
5.3. Administer Hunt Group and Agent

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

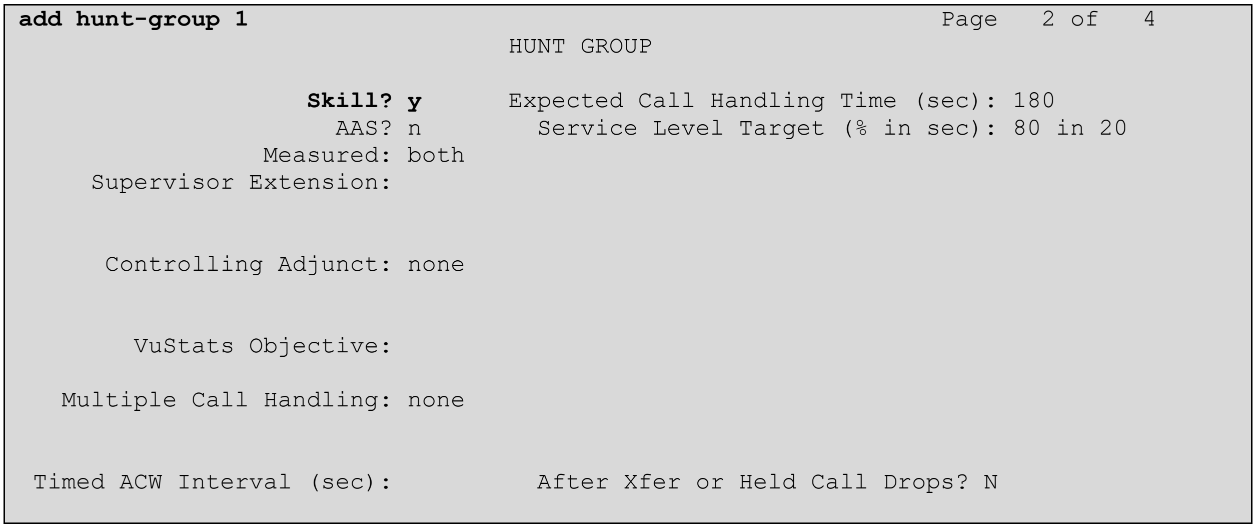
5.3.1. Add Hunt Group

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 **Sales Group** queue. Ensure that **ACD**, **Queue** and **Vector** are all set to **y**. Also, set the **Group Type** to **ead-mia**.



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

            Group Number: 1                                ACD? y
              Group Name: Sales Group                    Queue? y
         Group Extension: 13001                         Vector? y
              Group Type: ead-mia
                      TN: 1
                     COR: 1                    MM Early Answer? n
           Security Code:               Local Agent Preference? n
 ISDN/SIP Caller Display: grp-name

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

SIP URI: ___________________________________________________________________________
```

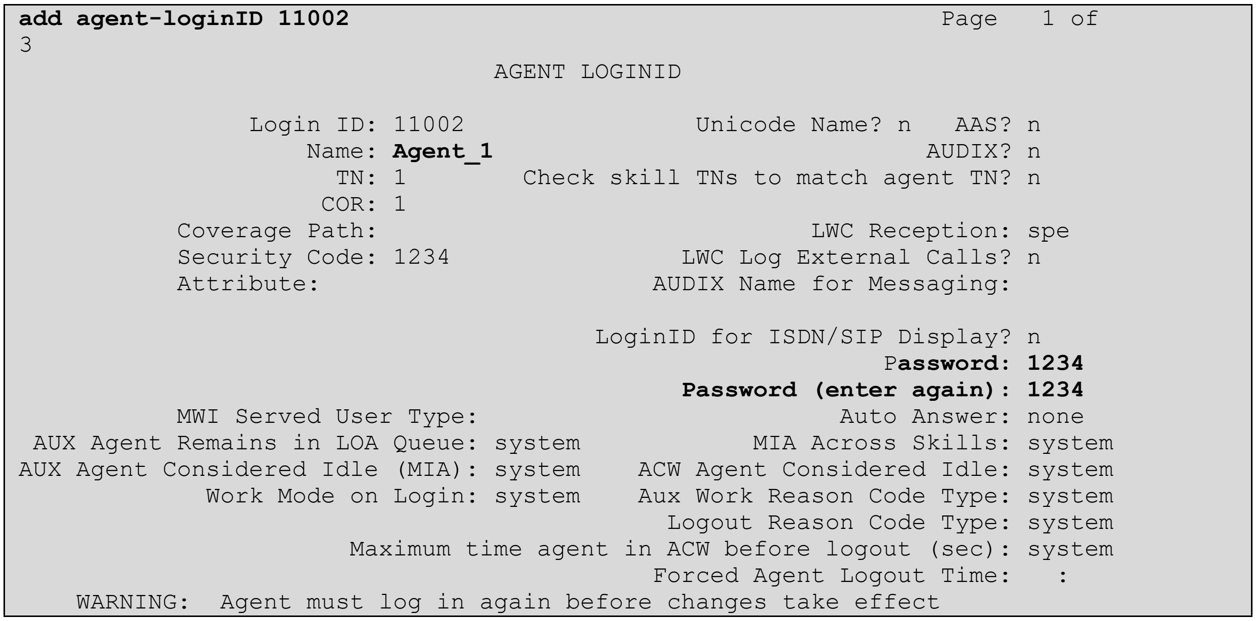
On **Page 2** ensure that **Skill** is set to **y** as shown below.



```
add hunt-group 1                                              Page   2 of   4
                                  HUNT GROUP

                    Skill? y      Expected Call Handling Time (sec): 180
                      AAS? n        Service Level Target (% in sec): 80 in 20
                 Measured: both
     Supervisor Extension:


      Controlling Adjunct: none


        VuStats Objective:

   Multiple Call Handling: none


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

5.3.2. Add Agent

In the compliance testing, the agents 11002 and 11003 were created. To add a new agent, type **add agent-loginID x**, where x is the login id for the new agent. Enter a descriptive **Name** and the agent login **Password**.



```
add agent-loginID 11002                                       Page   1 of
3
                                 AGENT LOGINID

                 Login ID: 11002               Unicode Name? n   AAS? n
                     Name: Agent_1                              AUDIX? n
                       TN: 1       Check skill TNs to match agent TN? n
                      COR: 1
           Coverage Path:                               LWC Reception: spe
           Security Code: 1234                 LWC Log External Calls? n
           Attribute:                        AUDIX Name for Messaging:

                                        LoginID for ISDN/SIP Display? n
                                                            Password: 1234
                                              Password (enter again): 1234
           MWI Served User Type:                           Auto Answer: none
 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 **Sales Group** is initiated, the call can be routed to this agent.

```
add agent-loginID 11001                                           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:
11:                 26:                 41:                 56:
12:                 27:                 42:                 57:
13:                 28:                 43:                 58:
14:                 29:                 44:                 59:
15:                 30:                 45:                 60:
```

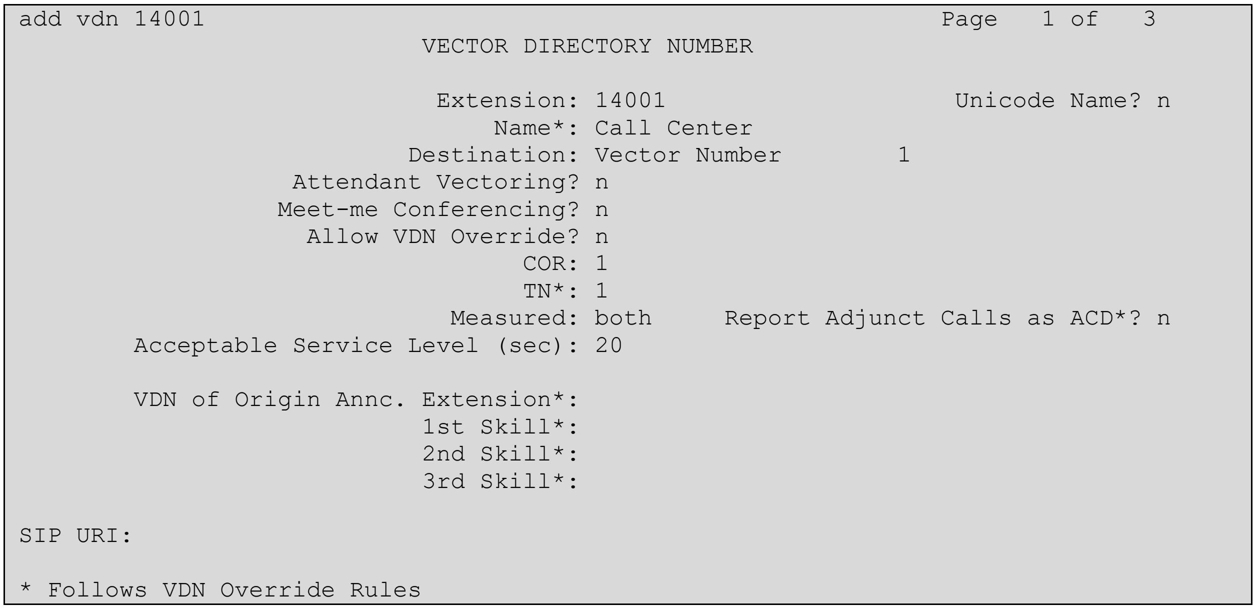
Repeat this section to add another agent login ID 11003.

5.4. 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.

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

    Number: 1                Name: Sales
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n            Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    2   secs hearing ringback
02 queue-to     skill 1    pri m
03 wait-time    900 secs hearing music
04 disconnect   after announcement none
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 14001                                                   Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 14001                    Unicode Name? n
                                 Name*: Call Center
                           Destination: Vector Number        1
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: both     Report Adjunct Calls as ACD*? n
        Acceptable Service Level (sec): 20

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

SIP URI:

* Follows VDN Override Rules
```

6. Configure Avaya Aura® Application Enablement Services

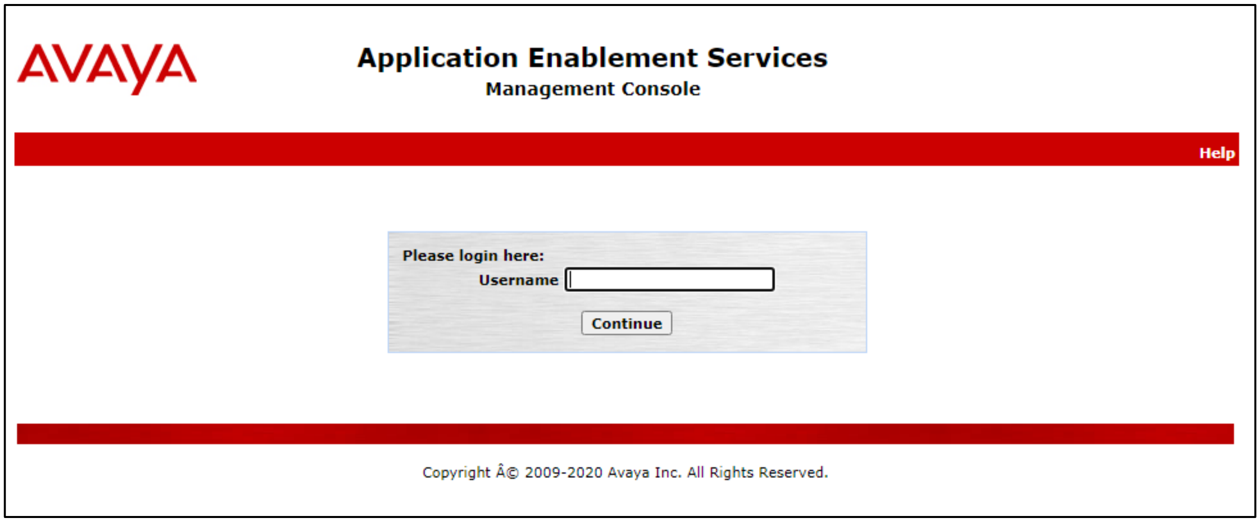
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

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

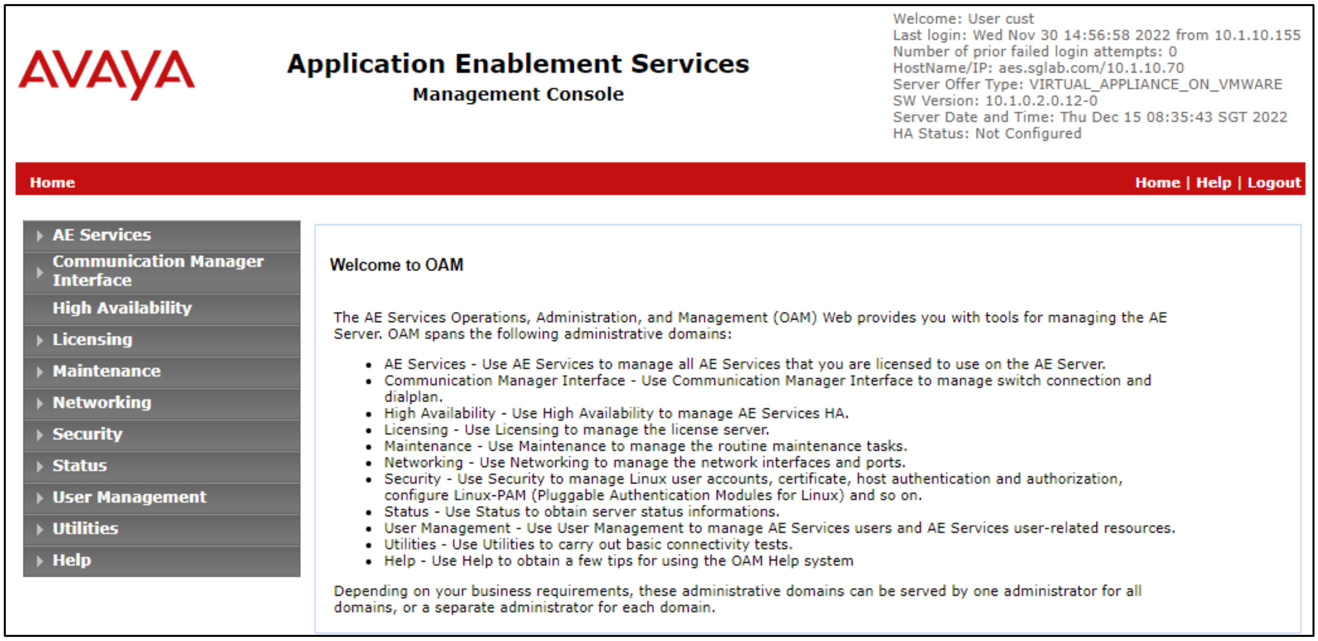
6.1. Launch OAM Interface

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: Wed Nov 30 14:56:58 2022 from 10.1.10.155
Number of prior failed login attempts: 0
HostName/IP: aes.sglab.com/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.2.0.12-0
Server Date and Time: Thu Dec 15 08:35:43 SGT 2022
HA Status: Not Configured

Welcome to OAM

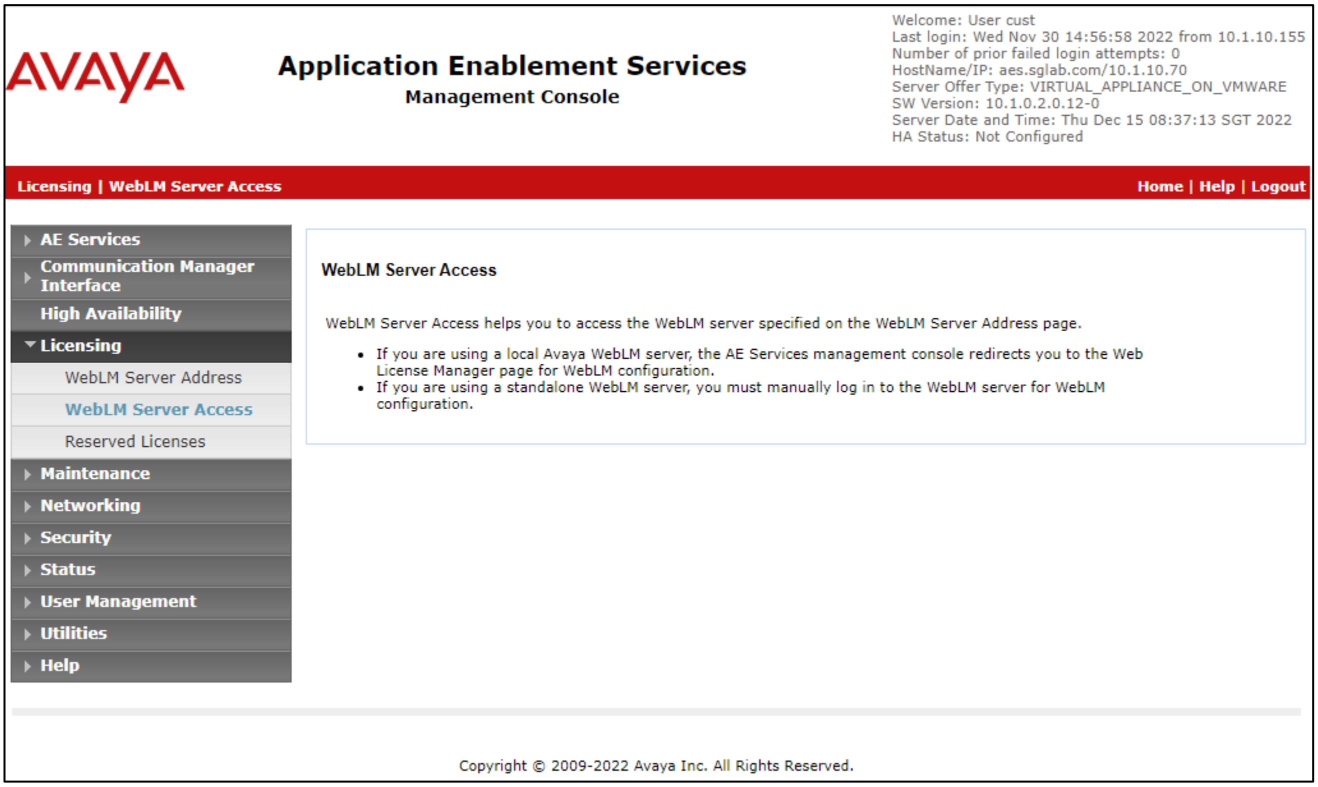
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- 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.

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: Wed Nov 30 14:56:58 2022 from 10.1.10.155
Number of prior failed login attempts: 0
HostName/IP: aes.sglab.com/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.2.0.12-0
Server Date and Time: Thu Dec 15 08:37:13 SGT 2022
HA Status: Not Configured

WebLM Server Access

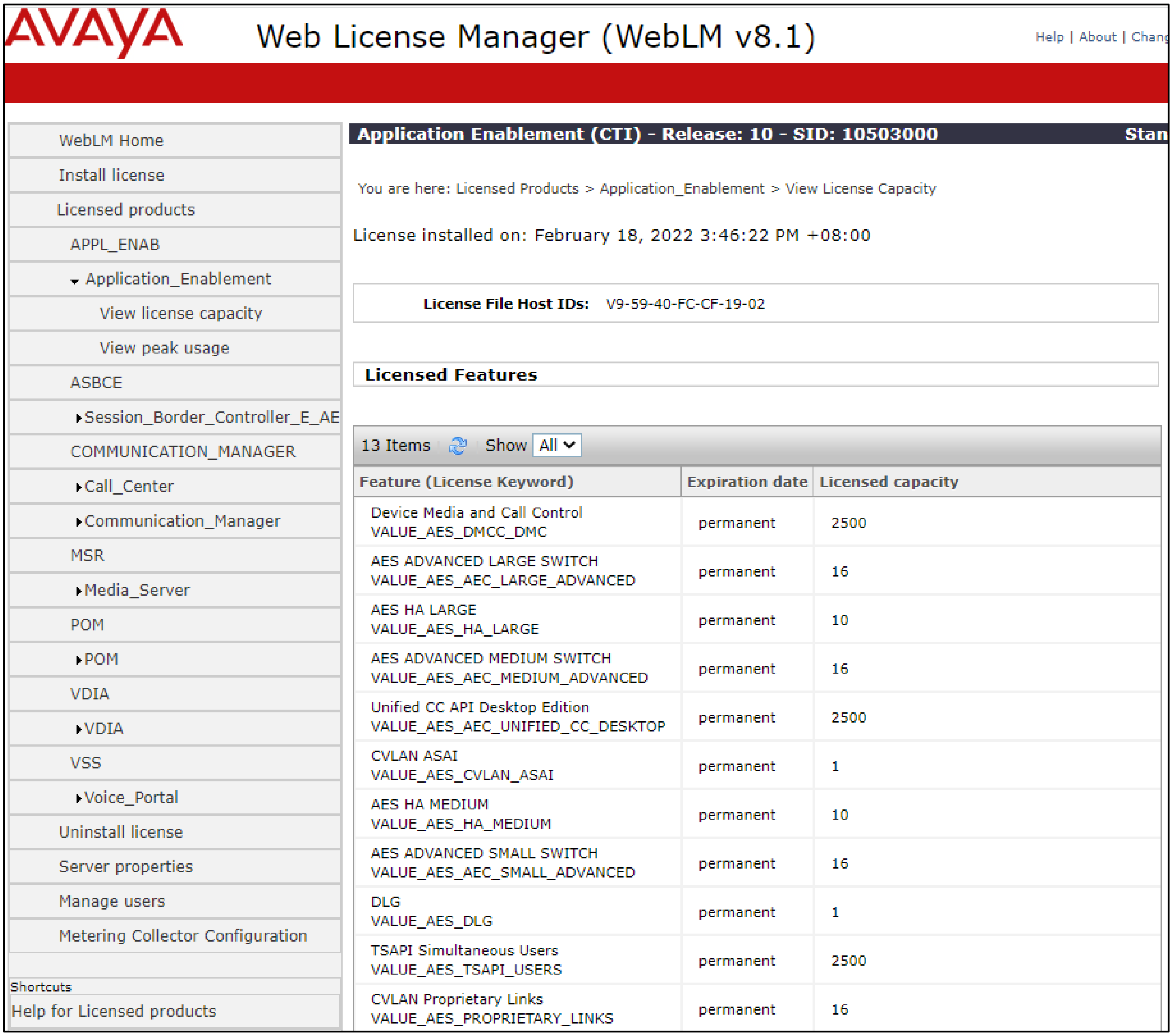
WebLM Server Access helps you to access the WebLM server specified on the WebLM Server Address page.

- If you are using a local Avaya WebLM server, the AE Services management console redirects you to the Web License Manager page for WebLM configuration.
- If you are using a standalone WebLM server, you must manually log in to the WebLM server for WebLM configuration.

Copyright © 2009-2022 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.



Application Enablement (CTI) - Release: 10 - SID: 10503000 Stan

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

License installed on: February 18, 2022 3:46:22 PM +08:00

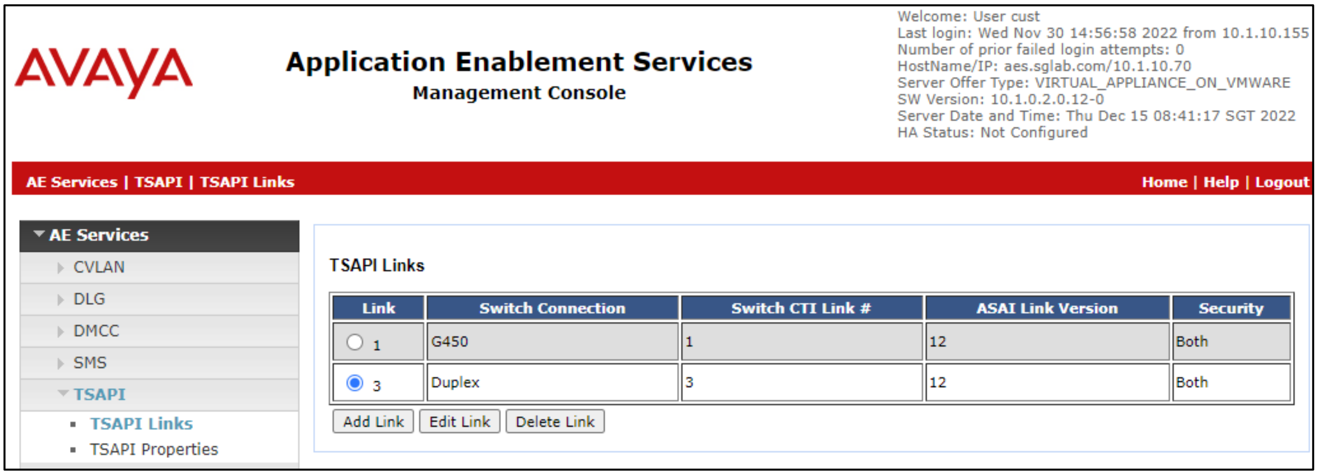
License File Host IDs: V9-59-40-FC-CF-19-02

Licensed Features

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	2500
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
AES HA LARGE VALUE_AES_HA_LARGE	permanent	10
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	2500
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	1
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	10
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
DLG VALUE_AES_DLG	permanent	1
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	2500
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16

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** from the appropriate switch connection, in this case **Duplex**.

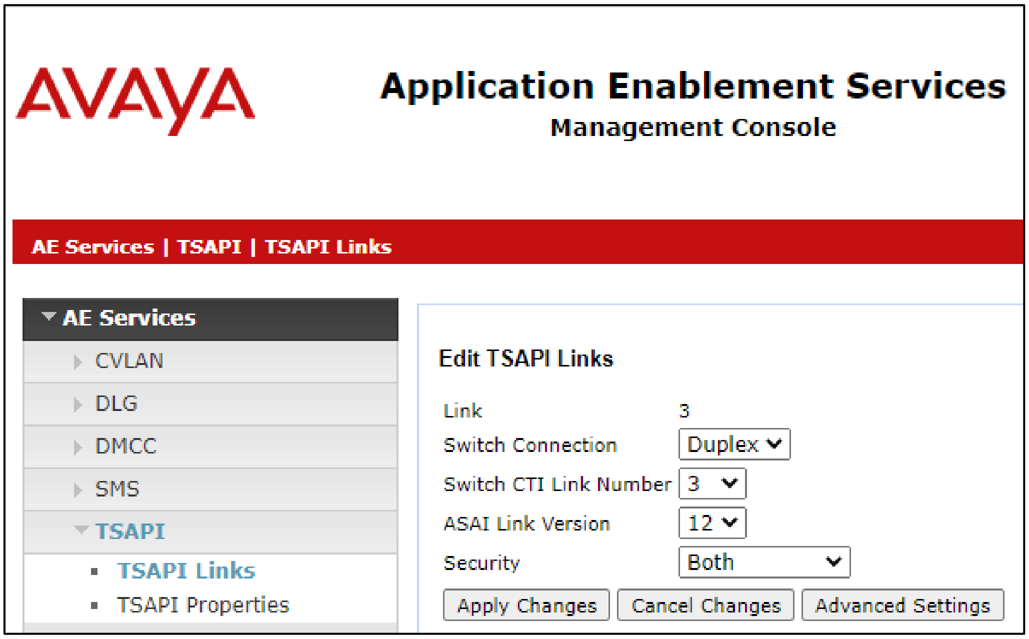


Welcome: User cust
Last login: Wed Nov 30 14:56:58 2022 from 10.1.10.155
Number of prior failed login attempts: 0
HostName/IP: aes.sglab.com/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.2.0.12-0
Server Date and Time: Thu Dec 15 08:41:17 SGT 2022
HA Status: Not Configured

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
○ 1	G450	1	12	Both
● 3	Duplex	3	12	Both

The **Add TSAPI Links** screen is displayed next (not shown). 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 **Duplex** is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields. Below shows the configured settings.



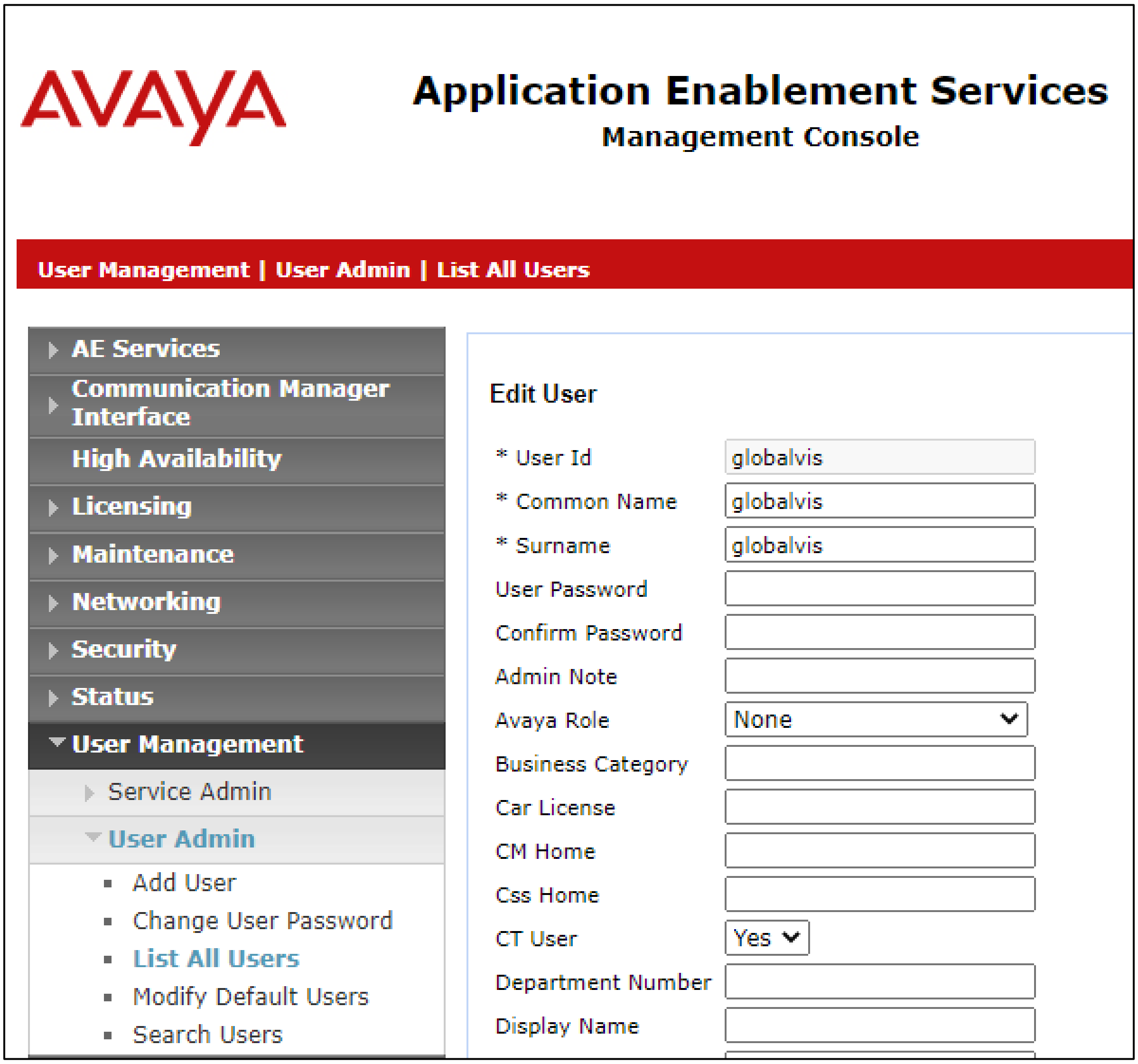
Edit TSAPI Links

Link	3
Switch Connection	Duplex
Switch CTI Link Number	3
ASAI Link Version	12
Security	Both

6.4. Administer User

Select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane (not shown).

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. Below show the configured user **globalvis**.



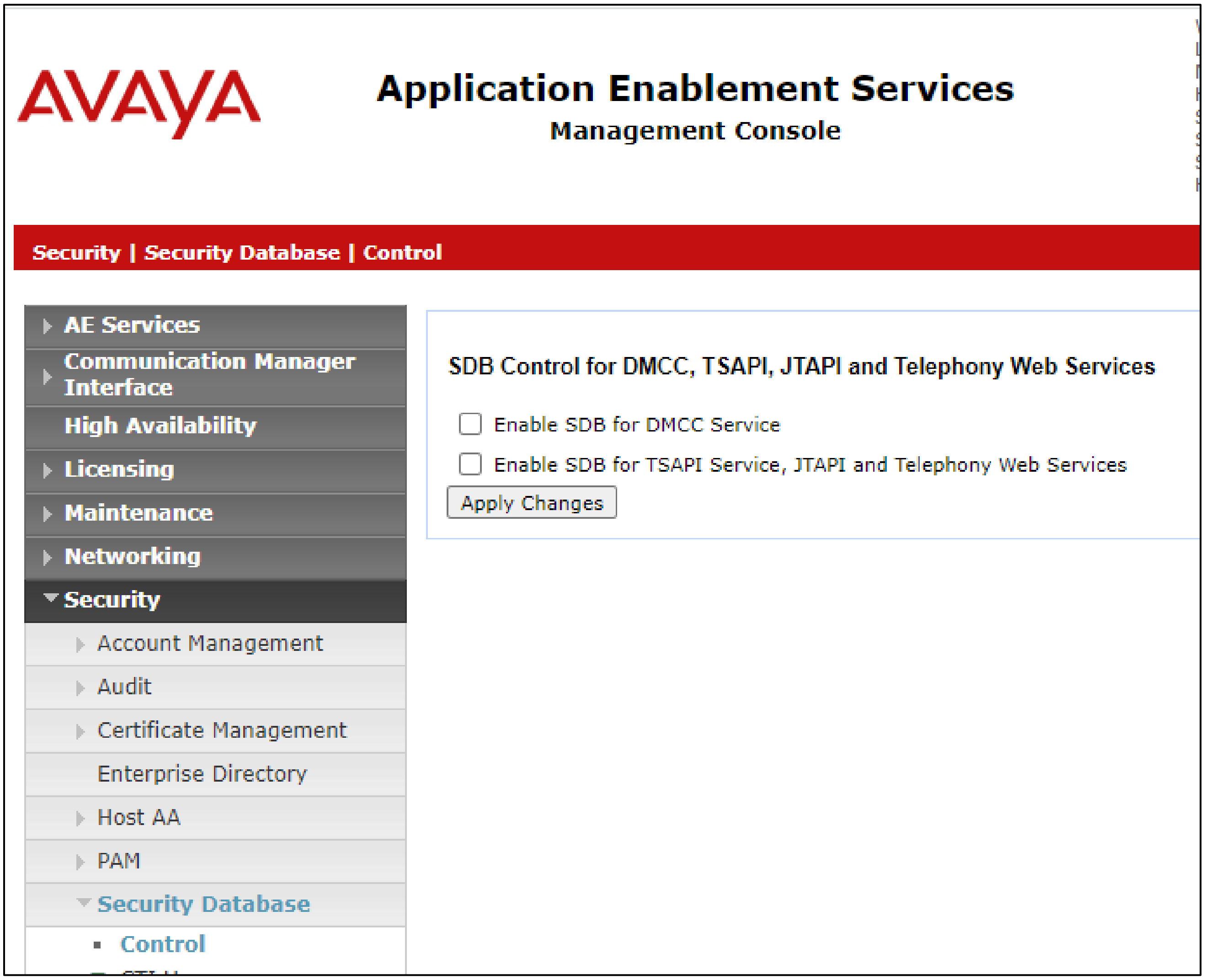
Edit User

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

6.5. 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 user from **Section 6.4.**



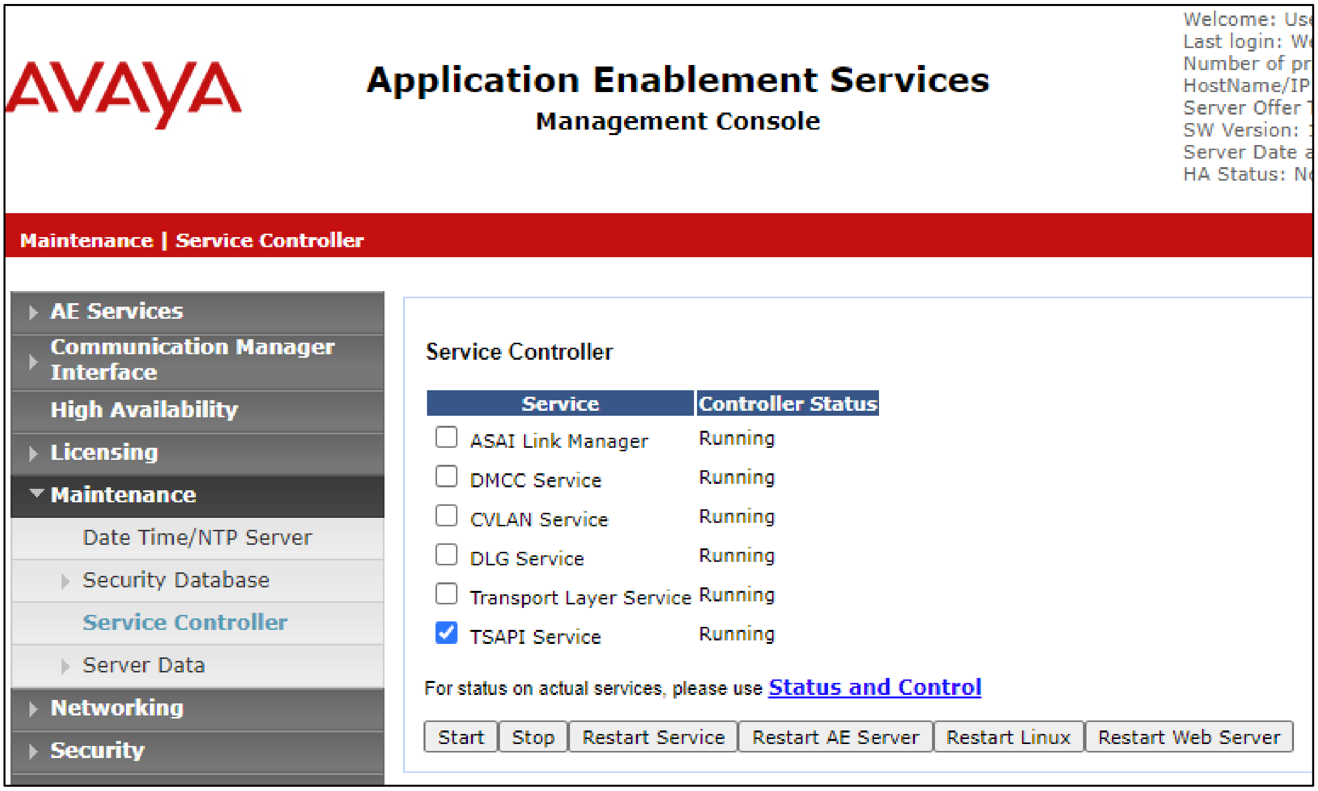
SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

☐ Enable SDB for DMCC Service

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

6.6. Restart Services

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



Service Controller

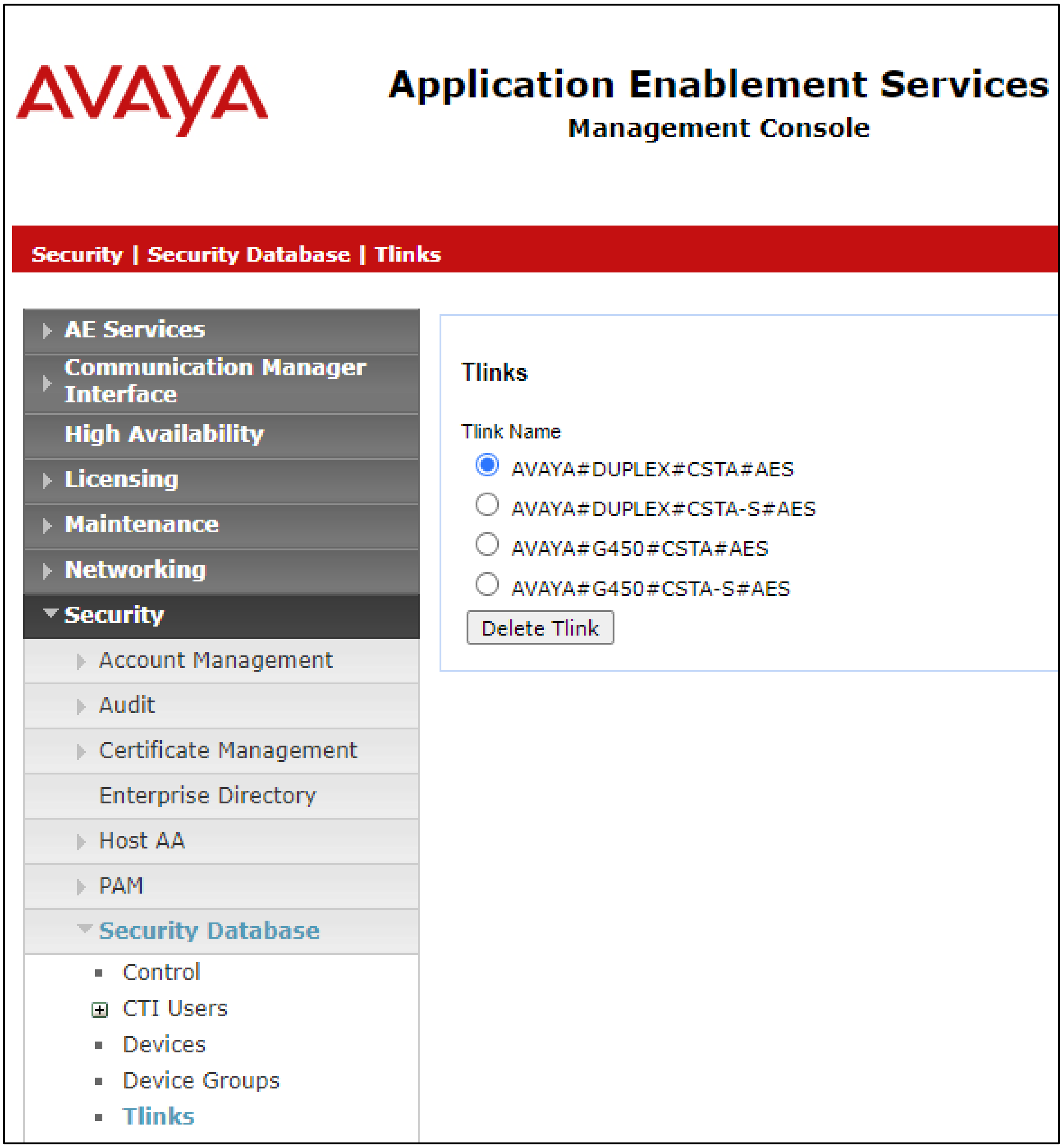
Service	Controller Status
□ ASAI Link Manager	Running
□ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
☑ TSAPI Service	Running

For status on actual services, please use Status and Control

6.7. 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 RADIUS.

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



Tlinks

Tlink Name

● AVAYA#DUPLEX#CSTA#AES
○ AVAYA#DUPLEX#CSTA-S#AES
○ AVAYA#G450#CSTA#AES
○ AVAYA#G450#CSTA-S#AES

7. Configure VIS Global RADIUS

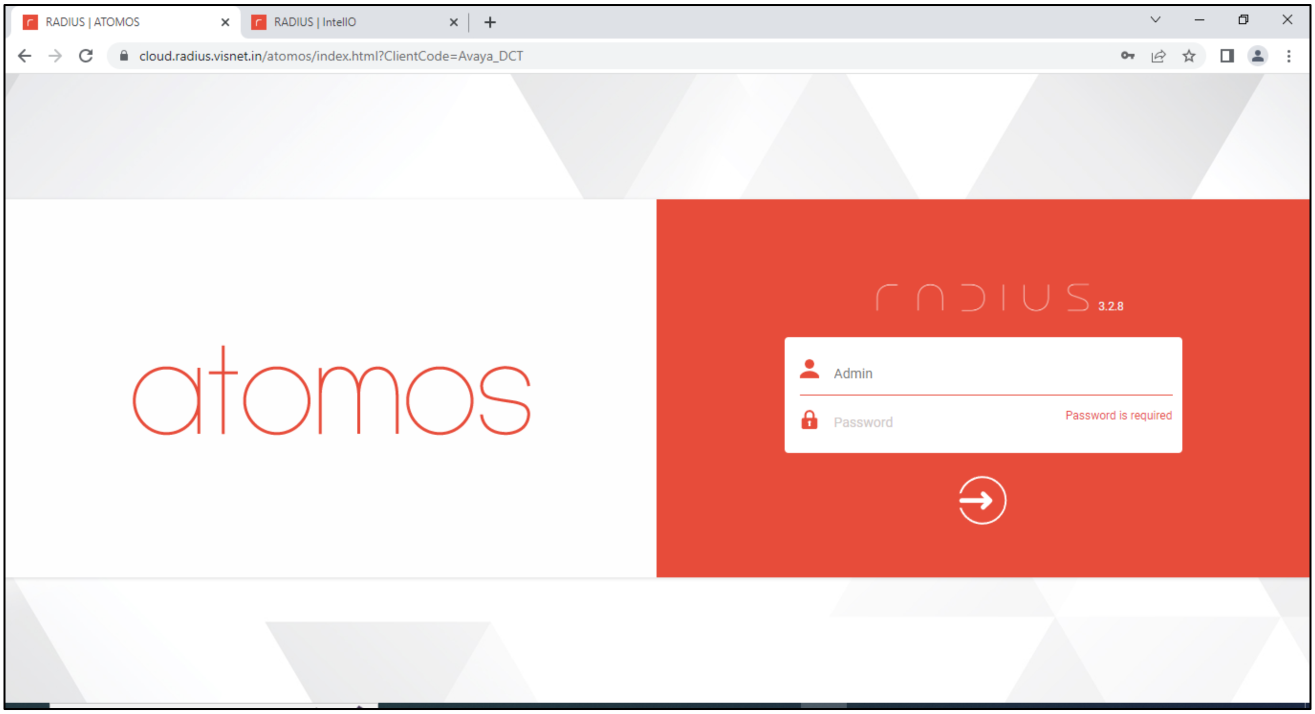
All installation and configuration related to RADIUS is performed by VIS Global engineers including terminals, agents, campaigns and media server, and thus, is not documented. The following are for information purposes only to illustrate steps they configured Media Server using Tlink name, VDN, Split, and Terminals.

- Supervisor/Administrator ATOMOS login
- Media Server setup
- Terminals, VDN and ACD setup
- Campaigns list

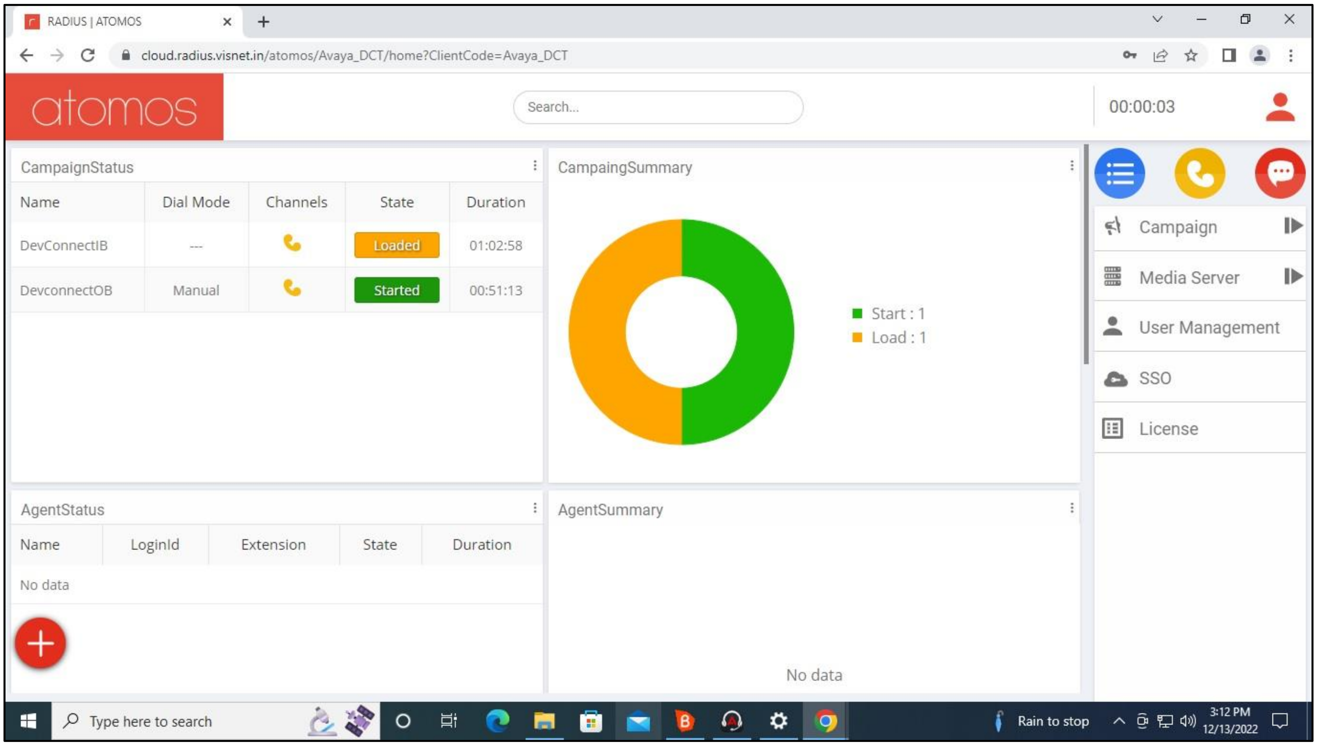
The campaigns that are pre-configured are also listed.

7.1. Supervisor/Administrator ATOMOS login

Access the ATOMOS web-based interface by using the URL provided by VIS Global in an Internet browser window. Log in using the appropriate credentials.



The screenshot below shows the home page after logging in.



CampaignStatus

Name	Dial Mode	Channels	State	Duration
DevConnectIB	---	☎	Loaded	01:02:58
DevconnectOB	Manual	☎	Started	00:51:13

CampaingSummary

🟩 Start : 1
🟧 Load : 1

AgentStatus

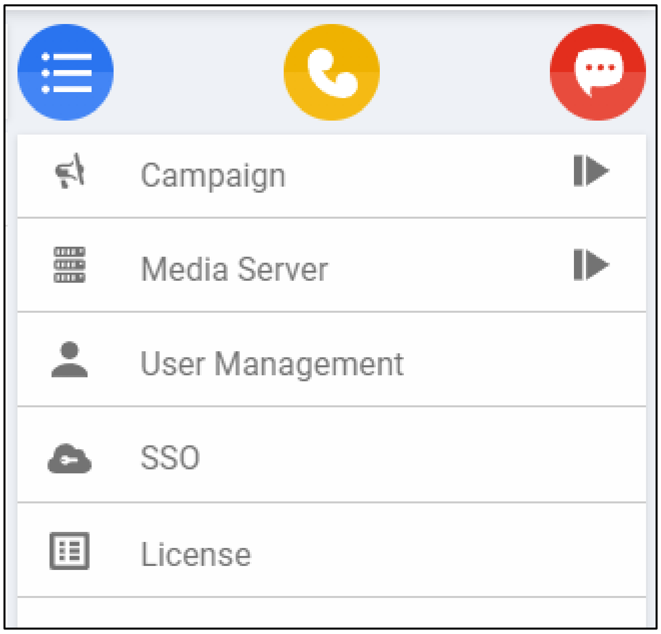
Name	LoginId	Extension	State	Duration
No data				

AgentSummary

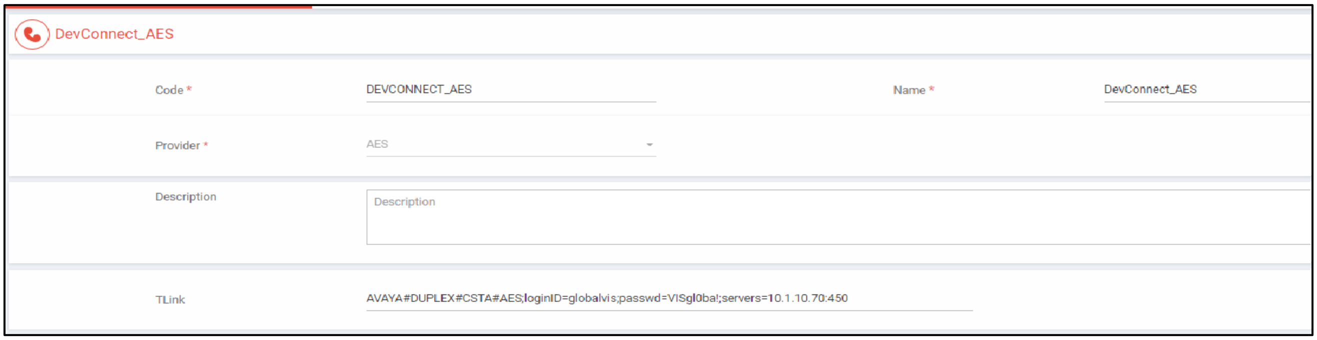
No data

7.2. Media Server Setup

From the menu on the top right pane shown below, click **Media Server → Telephone** and click the + icon (not shown).



Check an appropriate **Code** desired (this is an internal code). Check that an appropriate **Name** is given for the AES connection and take note. Check the "STRING" for the **TLINK** name is entered includes the Tlink name from **Section 6.7**, the CTI User login and password created in **Section 6.4,** AES **ip address**, and TSAPI **port** (default).

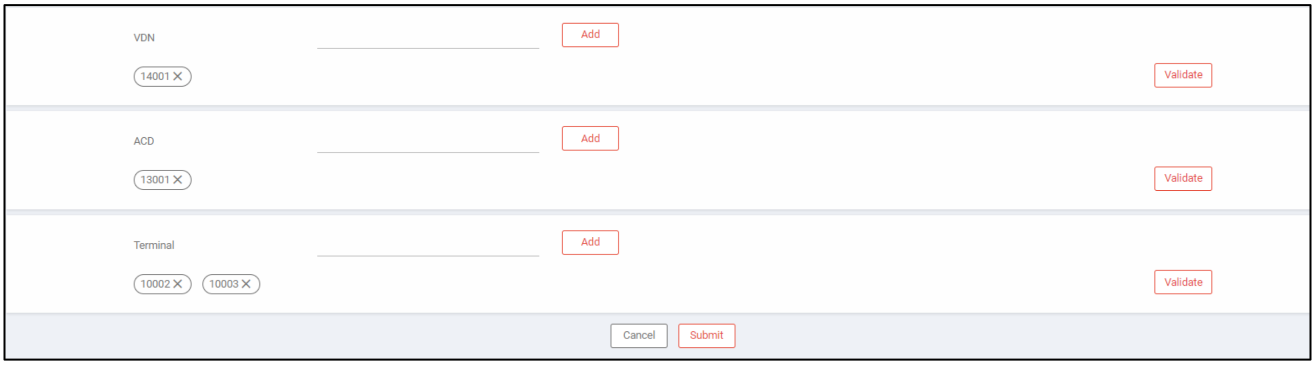


DevConnect_AES

Code *	DEVCONNECT_AES	Name *	DevConnect_AES
Provider *	AES		
Description	Description		
TLink	AVAYA#DUPLEX#CSTA#AES;loginID=globalvis;passwd=VISgl0ba!;servers=10.1.10.70:450		

7.3. Terminals, VDN and ACD Setup

Scroll down to the bottom and check that the **VDN** configured in **Section 5.4** and **ACD** Hunt Group configured in **Section 5.3** of Communication Manager are added below. The station (**Terminal**) used for testing are also added (see **Section 3**).



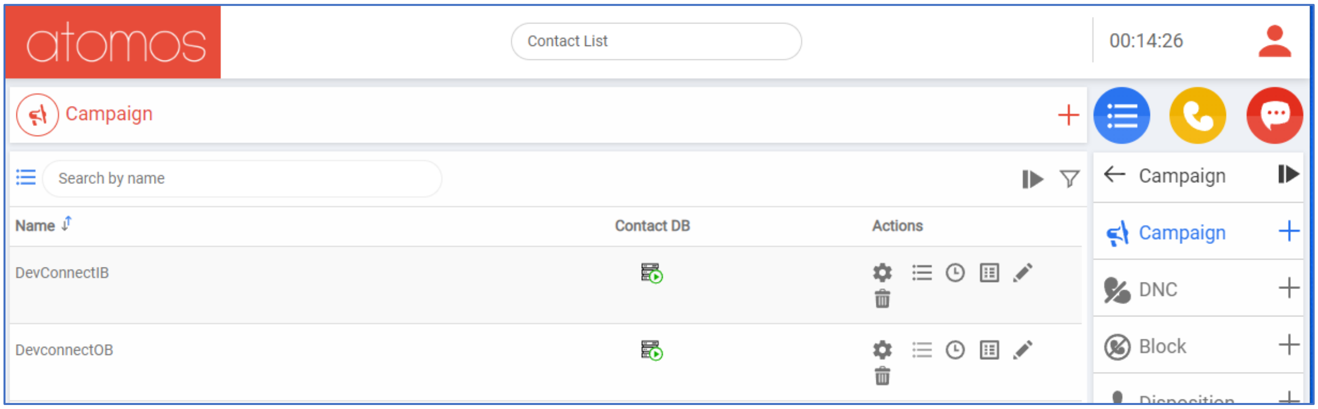
VDN: 14001 ✕

ACD: 13001 ✕

Terminal: 10002 ✕ 10003 ✕

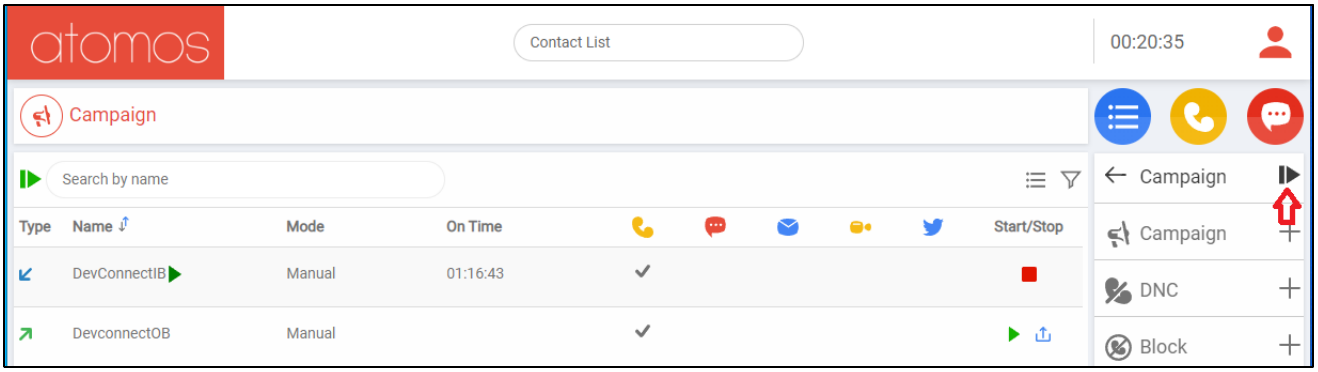
7.4. Campaigns Setup

From the main menu in **Section 7.2**, click **Campaign**. The screenshot below shows two campaigns created for inbound and outbound calls.



Name	Contact DB	Actions
DevConnectIB		
DevconnectOB		

Click on the “black play button” on the right of the word “Campaign” shown below to show the Campaign status on the left pane. The screenshots show the campaigns for inbound “DevConnectIB” calls which is running and outbound “DevconnectOB” calls which is stopped. To stop the campaign, click the “red stop button” under **Start/Stop**. To start the campaign, in the outbound campaign, click the “green play button” under **Start/Stop**.



Type	Name	Mode	On Time	☎	💬	✉		🐦	Start/Stop
↙	DevConnectIB ▶	Manual	01:16:43	✓					■
↗	DevconnectOB	Manual		✓					▶

8. Verification Steps

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

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

3     12       no    aes              established   22       23
4     12       no    aes              established   15       15
```

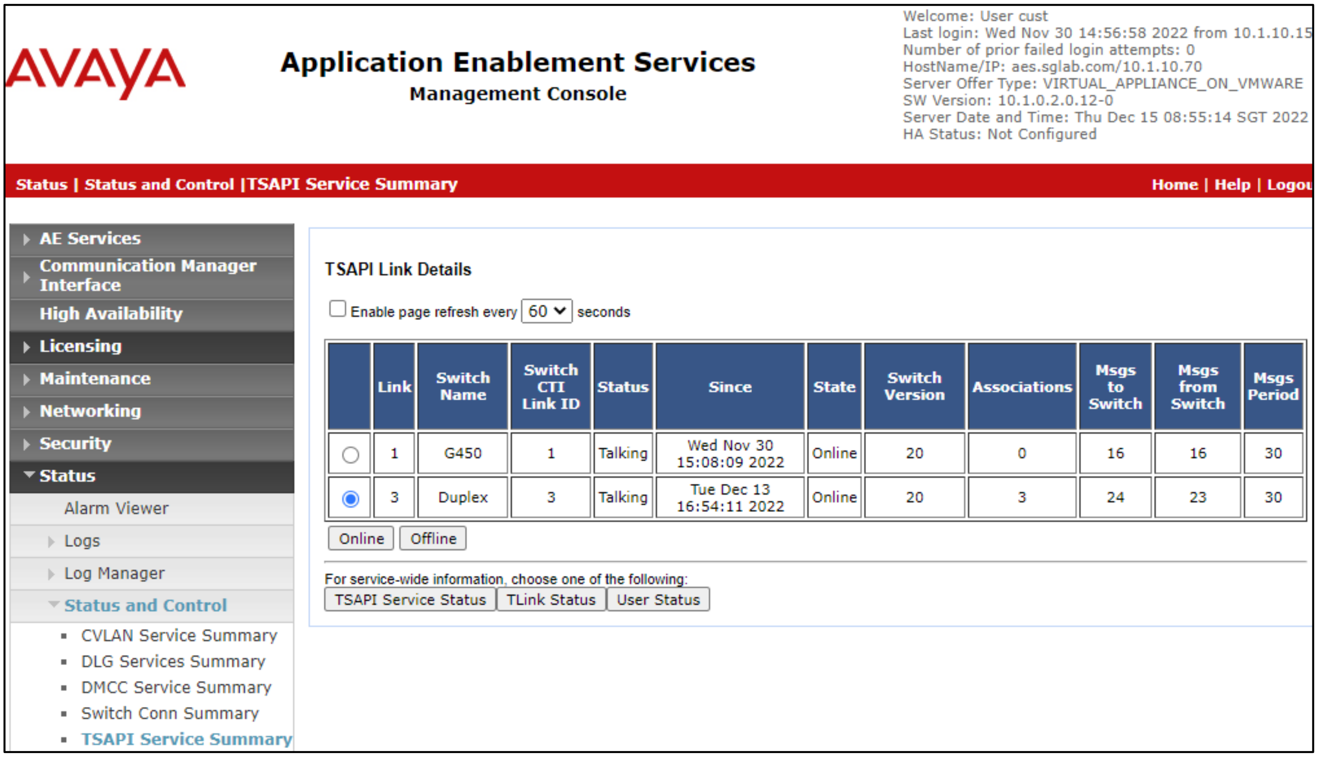
Enter the command **list agent-loginID.** Verify that agent **11002** and **11003** shown in **Section 5.4** is logged-in to extension **10002** and **10003** respectively.

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

11001            Agent_1         unstaffed                           1    lvl
                  1/01     /       /       /       /       /       /       /
11002            Agent_2         10002                               1    lvl
                  1/01     /       /       /       /       /       /       /
11003            Agent_3         10003                               1    lvl
                  1/01     /       /       /       /       /       /       /
11004            Agent 4         unstaffed                           1    lvl
                  1/01    2/02     /       /       /       /       /       /
11005            Agent #5        unstaffed                           1    lvl
                  1/01     /       /       /       /       /       /       /
11006            Agent #6        unstaffed                           1    lvl
                  1/01     /       /       /       /       /       /       /
11007            Agent #7        unstaffed                           1    lvl
                  1/01     /       /       /       /       /       /       /
11008            Agent #8        unstaffed                           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 total number of sessions reflects the number of VDN and agent stations monitored.



Welcome: User cust
Last login: Wed Nov 30 14:56:58 2022 from 10.1.10.15
Number of prior failed login attempts: 0
HostName/IP: aes.sglab.com/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.2.0.12-0
Server Date and Time: Thu Dec 15 08:55:14 SGT 2022
HA Status: Not Configured

TSAPI Link Details

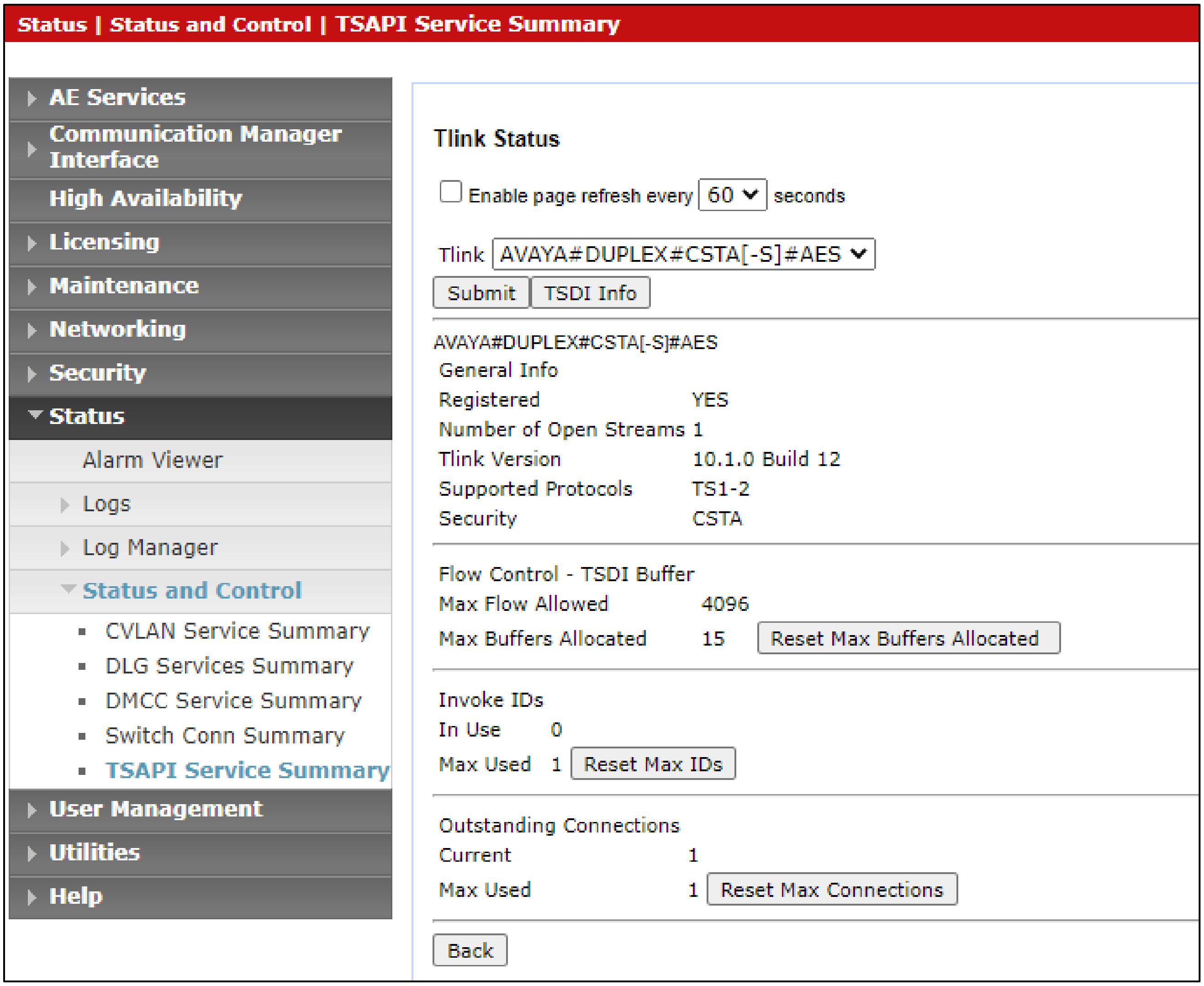
□ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
○	1	G450	1	Talking	Wed Nov 30 15:08:09 2022	Online	20	0	16	16	30
●	3	Duplex	3	Talking	Tue Dec 13 16:54:11 2022	Online	20	3	24	23	30

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

Click on the **Tlink Status** to verify user is connected as shown on the next page.

Select the **Tlink** as indicated in **Section 7.2** and click **Submit** below. Verify the **Outstanding Connections** for **Current** is “1” as shown with no other connections connected initially for the switch.



Tlink Status

☐ Enable page refresh every 60 seconds

Tlink AVAYA#DUPLEX#CSTA[-S]#AES

AVAYA#DUPLEX#CSTA[-S]#AES

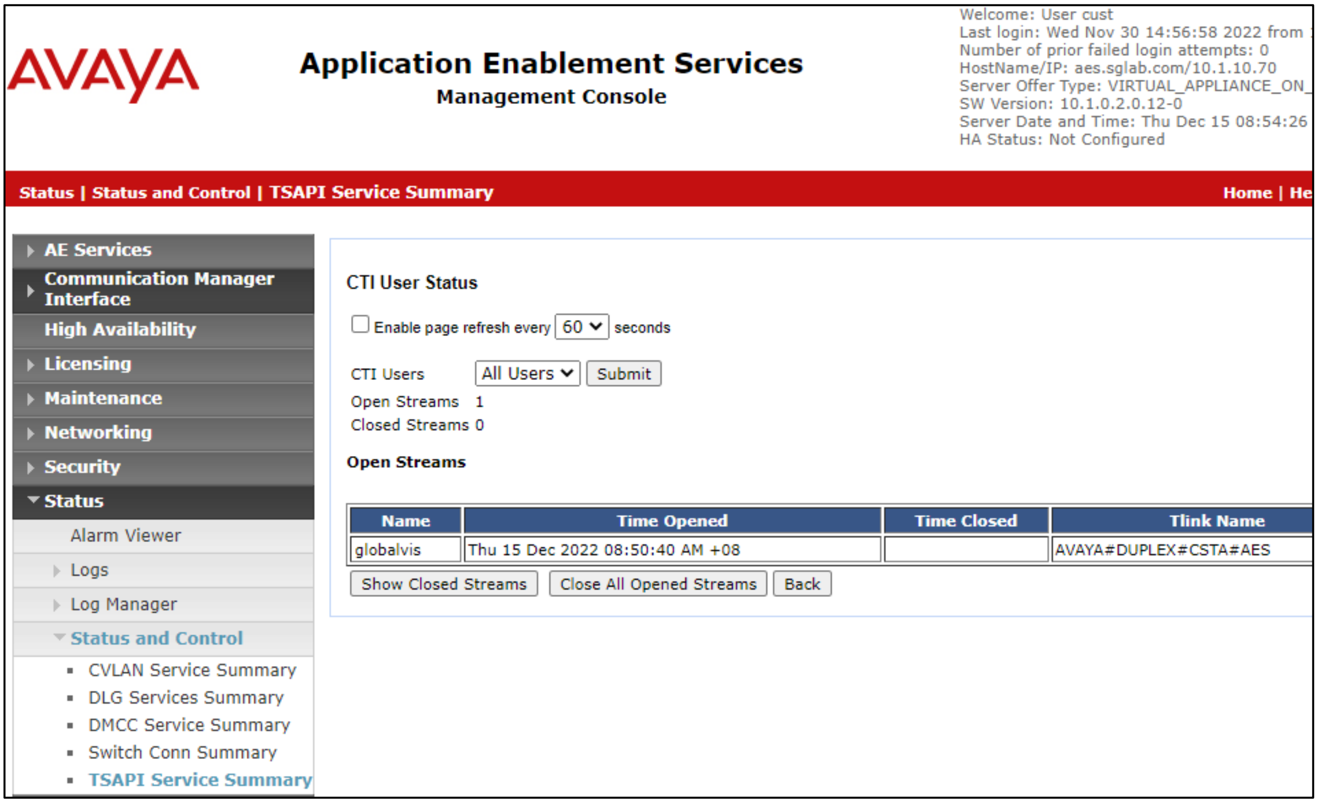
General Info	
Registered	YES
Number of Open Streams	1
Tlink Version	10.1.0 Build 12
Supported Protocols	TS1-2
Security	CSTA

Flow Control - TSDI Buffer	
Max Flow Allowed	4096
Max Buffers Allocated	15

Invoke IDs	
In Use	0
Max Used	1

Outstanding Connections	
Current	1
Max Used	1

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



Welcome: User cust
Last login: Wed Nov 30 14:56:58 2022 from
Number of prior failed login attempts: 0
HostName/IP: aes.sglab.com/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_
SW Version: 10.1.0.2.0.12-0
Server Date and Time: Thu Dec 15 08:54:26
HA Status: Not Configured

CTI User Status

□ Enable page refresh every 60 seconds

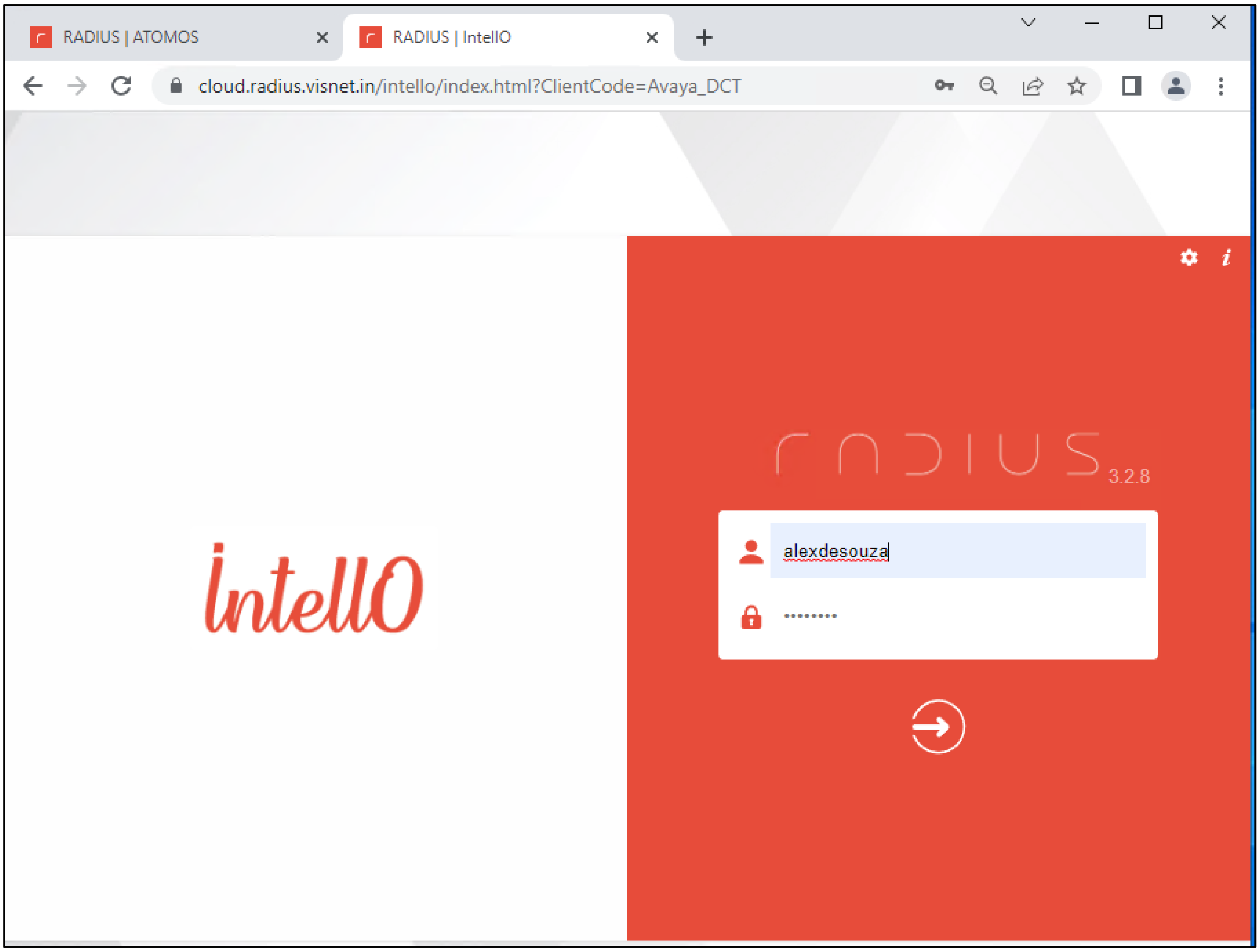
CTI Users All Users Submit
Open Streams 1
Closed Streams 0

Open Streams

Name	Time Opened	Time Closed	Tlink Name
globalvis	Thu 15 Dec 2022 08:50:40 AM +08		AVAYA#DUPLEX#CSTA#AES

8.3. Verify RADIUS Agent

From the agent PC, launch INTELLO web-based interface using URL provided by VIS Global. Enter the appropriate agent login and password.



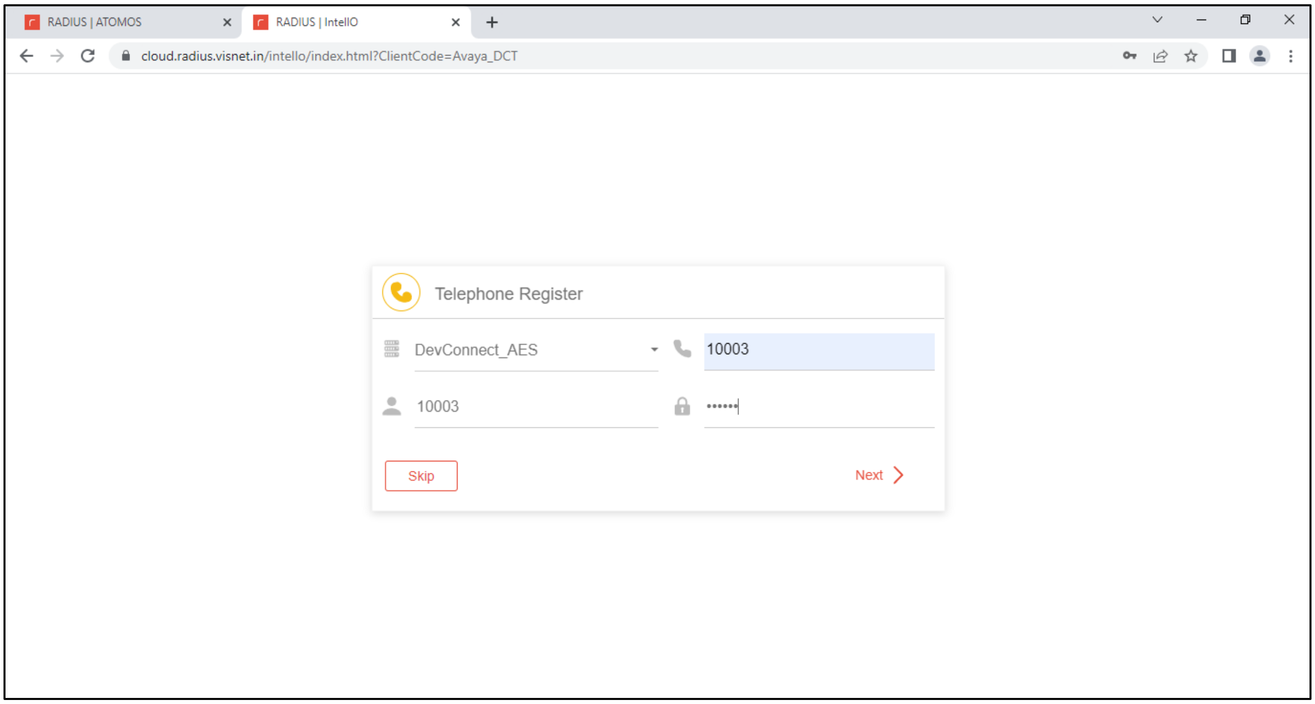
cloud.radius.visnet.in/intello/index.html?ClientCode=Avaya_DCT

alexdesouza

••••••••

The **Telephone Register** is displayed if successful. Enter the following values and click **Next**.

- **Media Server**: Select the AES configured in **Section 7.2**.
- **Telephone**: Enter the station.
- **User**: Enter the station user login.
- **Password (Lock)**: Enter the station user password.


RADIUS | ATOMOS
RADIUS | IntelIO
cloud.radius.visnet.in/intello/index.html?ClientCode=Avaya_DCT

Telephone Register

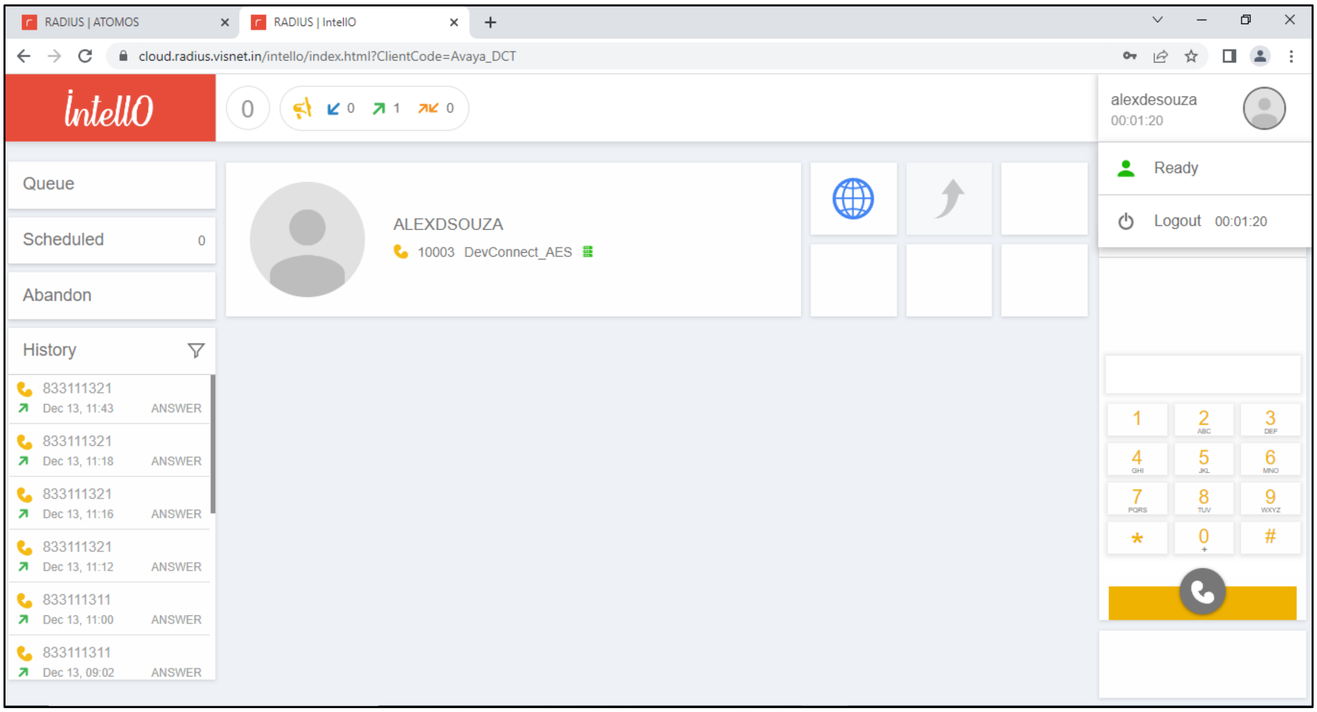
DevConnect_AES

10003

10003

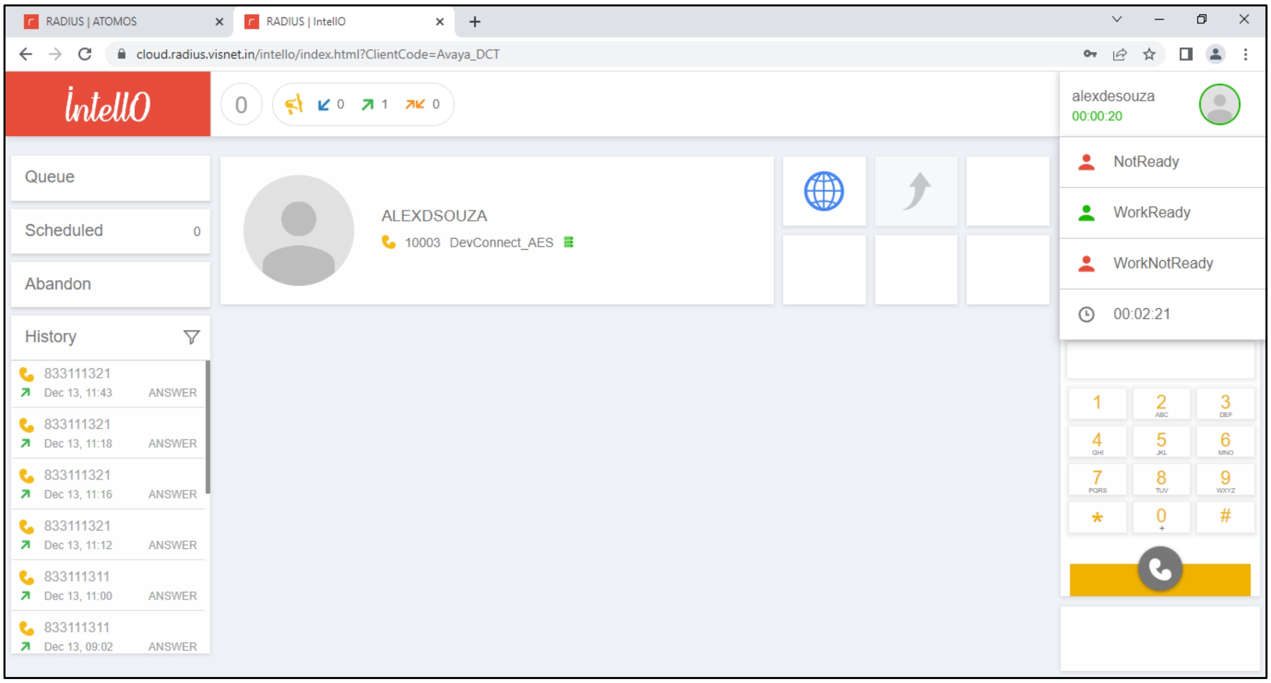
••••••

After login successfully, screenshot below shows the agent login screen. Select the agent picture icon (grey) on the top right pane as shown below and click **Ready** (in green).



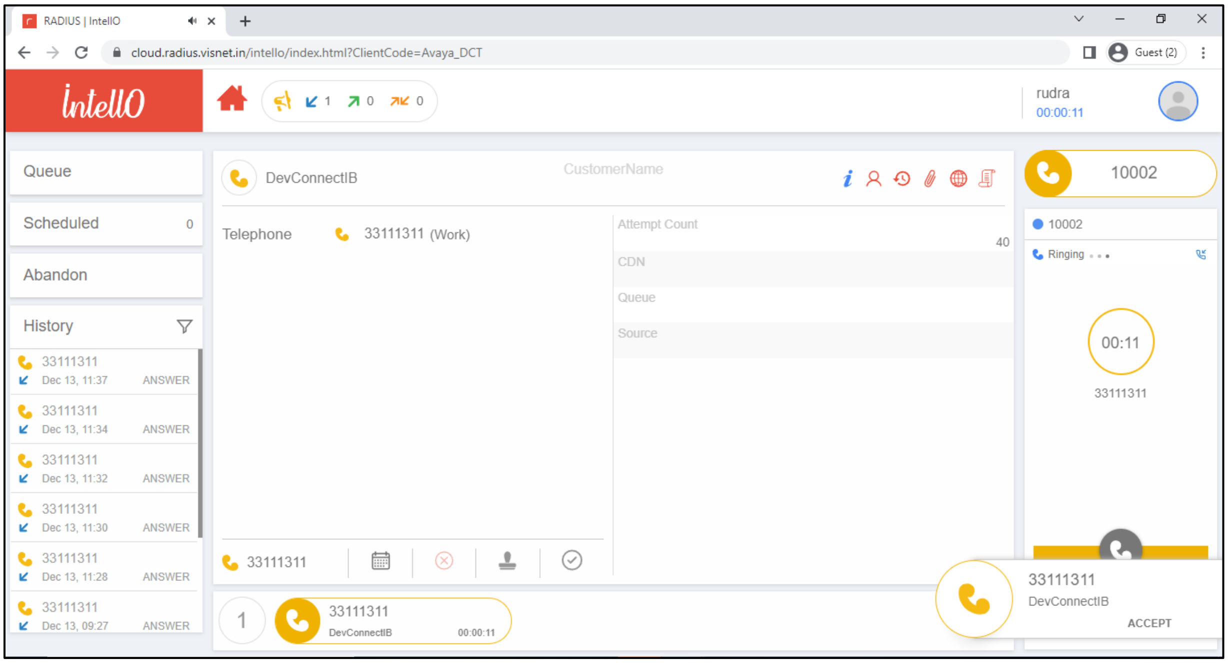
833111321 Dec 13, 11:43	ANSWER
833111321 Dec 13, 11:18	ANSWER
833111321 Dec 13, 11:16	ANSWER
833111321 Dec 13, 11:12	ANSWER
833111311 Dec 13, 11:00	ANSWER
833111311 Dec 13, 09:02	ANSWER

Verify that agent change to ready (agent picture icon ring turns green) as shown below. Select Ready or **WorkReady** below it for agent to be available for call.



833111321 Dec 13, 11:43 ANSWER
833111321 Dec 13, 11:18 ANSWER
833111321 Dec 13, 11:16 ANSWER
833111321 Dec 13, 11:12 ANSWER
833111311 Dec 13, 11:00 ANSWER
833111311 Dec 13, 09:02 ANSWER

Make an incoming call from the PSTN to the VDN. 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. DevConnectIB is the inbound campaign that was mapped to the incoming VDN with the Calling Party Number shown.



Scheduled 0

Telephone 33111311 (Work)

Attempt Count 40

CDN

Queue

Source

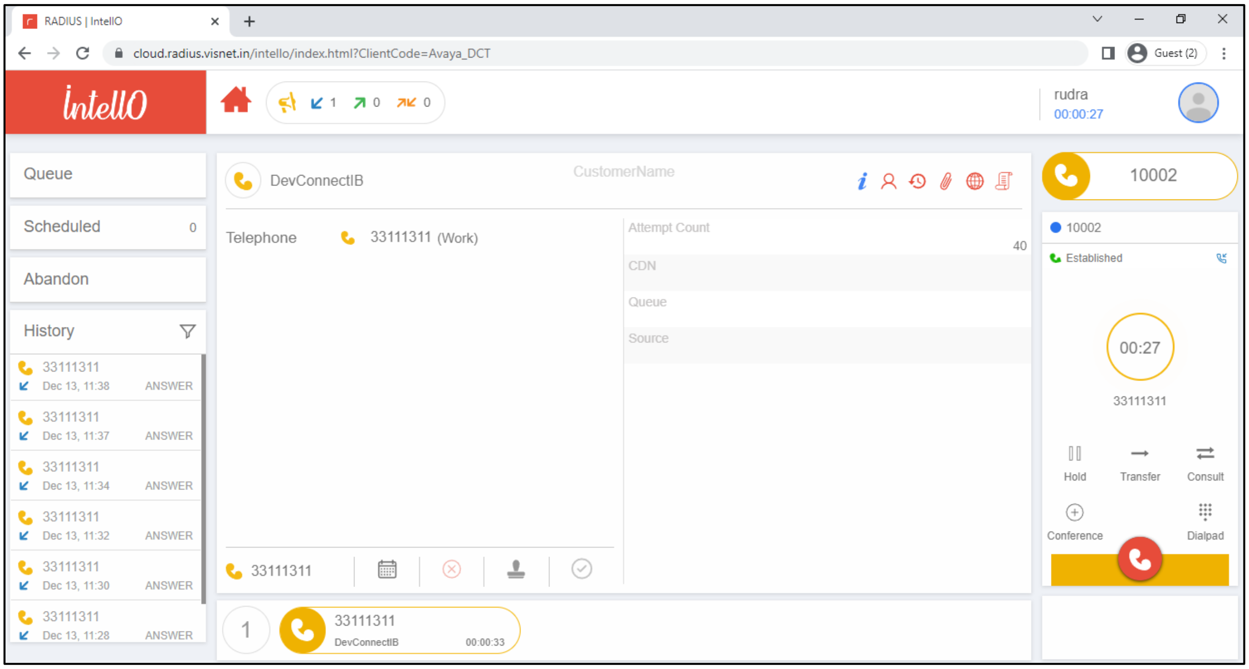
33111311	Dec 13, 11:37	ANSWER
33111311	Dec 13, 11:34	ANSWER
33111311	Dec 13, 11:32	ANSWER
33111311	Dec 13, 11:30	ANSWER
33111311	Dec 13, 11:28	ANSWER
33111311	Dec 13, 09:27	ANSWER

10002 Ringing 33111311

1 33111311 DevConnectIB 00:00:11

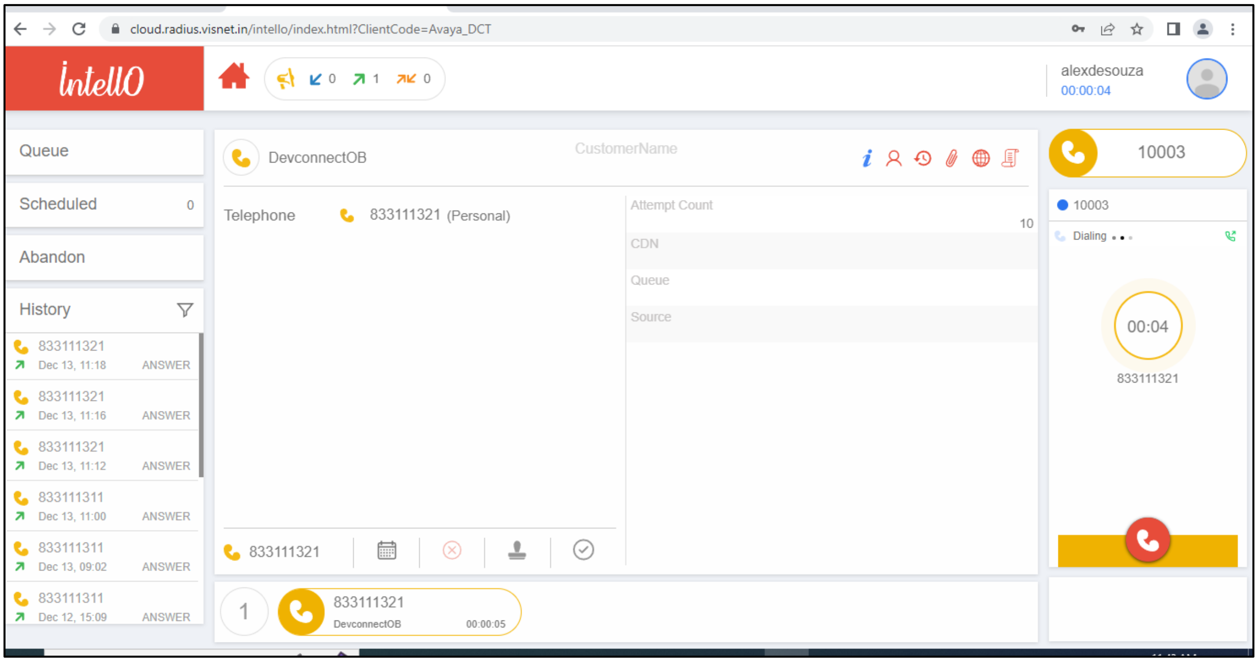
33111311 DevConnectIB ACCEPT

Press **Accept** 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 **Established** state as shown below.



33111311	Dec 13, 11:38	ANSWER
33111311	Dec 13, 11:37	ANSWER
33111311	Dec 13, 11:34	ANSWER
33111311	Dec 13, 11:32	ANSWER
33111311	Dec 13, 11:30	ANSWER
33111311	Dec 13, 11:28	ANSWER

For outbound call, click the **Dialpad** and dial the customer number manually, and verified the call show the **Established** status similar to the inbound call. Note that Outbound campaign is not relevant to this integration test.



833111321	Dec 13, 11:18	ANSWER
833111321	Dec 13, 11:16	ANSWER
833111321	Dec 13, 11:12	ANSWER
833111311	Dec 13, 11:00	ANSWER
833111311	Dec 13, 09:02	ANSWER
833111311	Dec 12, 15:09	ANSWER

9. Conclusion

These Application Notes describe the configuration steps required for the VIS Global RADIUS 3.2.8 to interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1. All feature and serviceability test cases were completed**.**

10. Additional References

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

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

1. *Administering Avaya Aura® Communication Manager,* Release 10.1, September 2022
2. *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 3, April 2022
3. *Administering Avaya Aura® System Manager*, Release 10.1, Issue 3, February 2022
4. *Administering Avaya Aura® Application Enablement Services,* Release 10.1, September 2022

Product documentation for RADIUS can be obtained from VIS Global from the contacts in **Section 2.3** .

5. *Omni-Channel Contact Center Solution*, Version 1.1, October 2022

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.