



Avaya Solution & Interoperability Test Lab

Application Notes for TelAthena neOn SoftDialer with Avaya Aura® Application Enablement Services 7.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for TelAthena neOn SoftDialer to interoperate with Avaya Aura® Application Enablement Services 7.1 and Avaya Aura® Communication Manager 7.1. TelAthena neOn SoftDialer is a call center outbound solution that supports preview, predictive, inbound, and blended campaigns.

In the compliance testing, TelAthena neOn SoftDialer used the Telephony Services Application Programming Interface from Avaya Aura® Application Enablement Services to monitor VDNs and agent stations on Communication Manager, to provide agent work modes, screen pop, and call control from agent desktops.

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 TelAthena neOn SoftDialer (SoftDialer) to interoperate with Avaya Aura® Application Enablement Services 7.1 and Avaya Aura® Communication Manager 7.1. SoftDialer is a call center outbound solution that supports preview, predictive, inbound, and blended campaigns.

In the compliance testing, SoftDialer used the Telephony Services Application Programming Interface (TSAPI) from Application Enablement Services to monitor VDNs and agent stations on Communication Manager, to provide agent work modes, screen pop, and call control from agent desktops.

The SoftDialer solution consists of the neOn Server, neOn SoftDialer Gateway, supervisor running the TelAthena Supervisor application, and agents with browser connections with the neOn Server. The TSAPI connection with Application Enablement Services is via the neOn SoftDialer Gateway.

The compliance testing utilized custom scripts provided by TelAthena for testing of supported call actions for each campaign. The customization of such campaign scripts is outside the scope of this compliance test.

2. General Test Approach and Test Results

The feature test cases were performed manually. Various campaigns were manually started using the TelAthena Supervisor application. Necessary agent actions such as hold and reconnect were performed from the agent desktops.

The serviceability test cases were performed manually by busy out and release of the pertinent CTI link.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

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

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

For the testing associated with these Application Notes, the interface between Application Enablement Services and SoftDialer did not include use of any specific encryption features as requested by TelAthena.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing.

The feature testing focused on verifying the following on SoftDialer:

- Use of TSAPI query service to query device information and agent states.
- Use of TSAPI event report service to monitor VDNs, agent stations, and active predictive calls.
- Use of TSAPI set feature service to set agent states.
- Use of TSAPI call control service to launch outbound calls with use of UUI data in the make call and make predictive call requests, and support of call control actions from agent desktops
- Proper handling of call scenarios involving screen pop, inbound, outbound, agent drop, customer drop, hold/reconnect, transfer, conference, long duration, multiple agents, inbound campaign, preview campaign, predictive campaign, blended campaign, and manual call within preview campaign.

The serviceability test cases were performed manually by busy out and release of the pertinent CTI link.

2.2. Test Results

All test cases were executed and verified. The following were observations on SoftDialer.

- By design, a separate TSAPI session is created for each VDN monitor upon campaign activation, and for each agent station upon agent login.
- By design, SoftDialer requires agents to use desktops for all call related actions.
- By design, SoftDialer supports multiple active campaigns, as long as there is no common agent across the active campaigns.
- By design, all transfer and conference destinations are controlled and provided as part of customized scripts, with the destinations required to be non-agent. Therefore, screen pop at the transfer-to and conference-to destination is not applicable.
- When an agent is the last party to drop from a conference, the desktop displayed a system error message. The agent can dismiss the message without adverse impact on the next call.
- In the event that the dialed number associated with a manual or preview call is invalid, the agent will hear the reorder tone along with a system error message displayed on the desktop. The agent can dismiss the message without adverse impact on the next call.
- For a blended campaign, the supervisor is expected to monitor the queue and to instruct agents to manually switch between inbound and outbound modes on an as-needed basis.
- After a busy out and release of the CTI link on Communication Manager, the agent screens ceased to screen pop information on subsequent calls. The workaround is for agents to restart the browser to exit and log back into SoftDialer.
- After a disconnect and reconnect of the Ethernet connection to the neOn SoftDialer Gateway, the agent screens ceased to screen pop information on subsequent calls, and an “ATMS system died! Failed to receive Heartbeat from Server!” message appeared on the Campaign Controller console a few minutes later. By design, the neOn Server and neOn SoftDialer Gateway are tightly coupled and cannot be changed, with disruption to one component without the other considered catastrophic and required manual restart of TelAthena CTC Server service, Campaign Controller console, and agents’ browser. For additional help, reach out to TelAthena Support.

2.3. Support

Technical support on SoftDialer can be obtained through the following:

- **Phone:** (888) 777-7565
- **Web:** <http://www.telathena.com/aboutus.html>

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, and of call center devices are not the focus of these Application Notes and will not be described.

In the compliance testing, the Media Server and the TN2312BP IP Server Interface circuit pack in the G650 Media Gateway were used for answering machine detections.

The agent station extensions used in the compliance testing were “65001” and “65002”, and the supervisor station extension was “65000”.

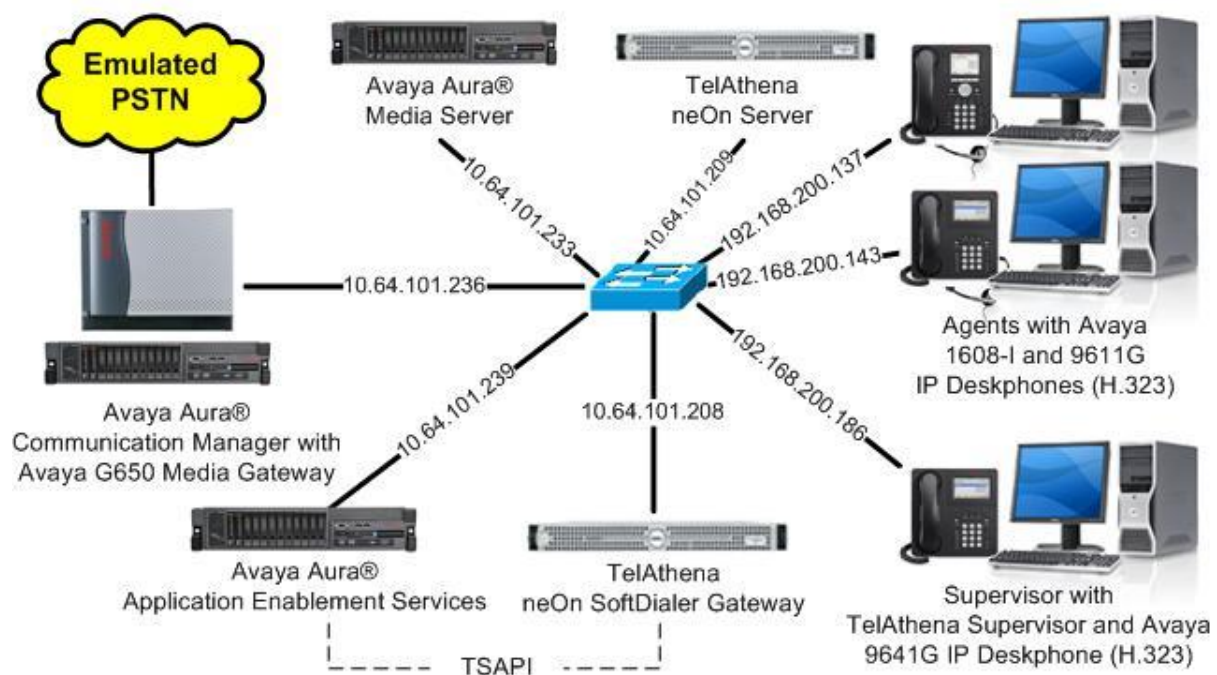


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	7.1.1 (7.1.1.0.0.532.23985)
Avaya G650 Media Gateway <ul style="list-style-type: none">TN2312BP IP Server Interface	HW28 FW058
Avaya Aura® Media Server in Virtual Environment	7.8.0.333
Avaya Aura® Application Enablement Services in Virtual Environment	7.1.1 (7.1.1.0.0.5-0)
Avaya 1608-I IP Deskphone (H.323)	1.3110
Avaya 9611G & 9641G IP Deskphones (H.323)	6.6506
TelAthena neOn Server on RedHat Enterprise	5.17 7.0
TelAthena neOn SoftDialer Gateway on Microsoft Windows Server 2012 <ul style="list-style-type: none">Avaya TSAPI Windows Client (csta32.dll)	5.4.8 R2 Standard 7.0.0.131
TelAthena Supervisor on Microsoft Windows 10	6.4.0 Pro

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 system parameters features
- Administer SIT treatment
- Administer hunt groups, vector, and VDNs
- Administer agent login IDs

5.1. Verify License

Log in to 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 **ASAI Link Core Capabilities**, **ASAI Link Plus Capabilities**, and **Computer Telephony Adjunct Links** customer option are set to “y” on **Page 4**. If these options are not set to “y”, then contact the Avaya sales team or business partner for a proper license file.

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

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

Navigate to **Page 7**, and verify that the **ACD**, **Expert Agent Selection (EAS)**, and **Vectoring (Basic)** customer options are set to “y”.

display system-parameters customer-options		Page 7 of 12
CALL CENTER OPTIONAL FEATURES		
Call Center Release: 7.0		
ACD? y		Reason Codes? y
BCMS (Basic)? y		Service Level Maximizer? n
BCMS/VuStats Service Level? y		Service Observing (Basic)? y
BSR Local Treatment for IP & ISDN? y	Service Observing (Remote/By FAC)? y	
Business Advocate? n	Service Observing (VDNs)? y	
Call Work Codes? y	Timed ACW? y	
DTMF Feedback Signals For VRU? y	Vectoring (Basic)? y	
Dynamic Advocate? n	Vectoring (Prompting)? y	
Expert Agent Selection (EAS)? y	Vectoring (G3V4 Enhanced)? y	
EAS-PHD? Y	Vectoring (3.0 Enhanced)? y	

5.2. Administer CTI Link

Add a CTI link using the “add cti-link n” command, where “n” is an available CTI link number.

Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter “ADJ-IP” in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

add cti-link 1	Page 1 of 3
CTI LINK	
CTI Link: 1	
Extension: 60111	
Type: ADJ-IP	
	COR: 1
Name: AES CTI Link	

5.3. Administer System Parameters Features

Use the “change system-parameters features” command to make certain **Expert Agent Selection (EAS) Enabled** is set to “y”, which is located on **Page 11**.

Set **Minimum Agent-LoginID Password Length** to blank, which is required by SoftDialer for logging agents into Communication Manager without use of passwords.

```
change system-parameters features                                     Page 11 of 19
                                FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
EAS
    Expert Agent Selection (EAS) Enabled? y
    Minimum Agent-LoginID Password Length:
        Direct Agent Announcement Extension:                      Delay:
    Message Waiting Lamp Indicates Status For: station
                                Work Mode On Login: aux
VECTORING
    Converse First Data Delay: 0          Second Data Delay: 2
    Converse Signaling Tone (msec): 100    Pause (msec): 70
    Prompting Timeout (secs): 10
    Interflow-qpos EWT Threshold: 2
    Reverse Star/Pound Digit For Collect Step? n
    Available Agent Adjustments for BSR? n
                                BSR Tie Strategy: 1st-found
```

Navigate to **Page 13**, and enable **Call Classification After Answer Supervision**. This setting instructs Communication Manager to rely on the network to provide answer/busy/drop classification, and to add a call classifier after the call has been answered.

```
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? y
                                Send UCID to ASAI? n
    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 SIT Treatment

Enter the “change sit-treatment” command. Set **Pause Duration (seconds)** and **Talk Duration (seconds)** to the values shown below, as recommended by SoftDialer. The **AMD Treatment** parameter was left at the default value, with specific treatment for answering machine detection configured on the SoftDialer.

For customers requiring SIT tone classification with use of an applicable resource such as the TN2312BP IP Server Interface or the TN744 Call Classifier circuit pack, set the SIT parameters as desired. In the compliance testing, SIT tone classification was not tested with all related parameters left at the default values shown below.

```
change sit-treatment                                     Page 1 of 1
SIT TREATMENT FOR CALL CLASSIFICATION

SIT Ineffective Other: dropped
SIT Intercept: answered
SIT No Circuit: dropped
SIT Reorder: dropped
SIT Vacant Code: dropped
SIT Unknown: dropped

AMD Treatment: dropped
Pause Duration (seconds): 1.0
Talk Duration (seconds): 1.5
```

5.5. Administer Hunt Groups, Vectors, and VDNs

Administer hunt groups, vectors, and VDNs for use by the call campaigns. The hunt groups, vectors, and VDNs that were configured and used in the compliance testing are shown below.

VDN	Vector	Skill	Campaigns
67701	701	701	inbound & blended
67702	702	702	predictive
NA	NA	703	preview & blended

5.5.1. Inbound

Administer a set of hunt group, vector, and VDN for routing of inbound calls used by the inbound and blended campaigns.

Add a hunt group using the “add hunt-group n” command, where “n” is an available hunt group number. This hunt group will be used for routing of inbound calls to agents for both the inbound and blended campaigns. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Number:** The available group number.
- **Group Name:** A descriptive name.
- **Group Extension:** An available extension number.
- **ACD:** “y”
- **Queue:** “y”
- **Vector:** “y”

add hunt-group 701		Page 1 of 62
HUNT GROUP		
Group Number: 701	ACD? y	
Group Name: TelAthena Inbound	Queue? y	
Group Extension: 68701	Vector? y	
Group Type: ucd-mia		
TN: 1		
COR: 1		
MM Early Answer? n		
Security Code:		
Local Agent Preference? n		

Navigate to **Page 2**, and set **Skill** to “y” as shown below.

add hunt-group 701		Page 2 of 62
HUNT GROUP		
Skill? y	Expected Call Handling Time <sec>: 180	
AAS? n		
Measured: none		
Supervisor Extension:		

Modify a vector using the “change vector n” command, where “n” is an available vector number. This vector will provide routing of inbound calls for both the inbound and blended campaigns.

Configure treatment steps for the inbound call as desired, which can vary based on customer requirements. Administer a **queue-to** step with the hunt group number from above along with desired priority.

The vector used in the compliance testing for routing of inbound calls is shown below.

change vector 701				Page 1 of 6			
CALL VECTOR							
Number: 701				Name: TelAthena Inbound Vector			
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 701 pri m						
03							
04							

Add a VDN using the “add vdn n” command, where “n” is an available extension. This VDN will provide routing of inbound calls for both the inbound and blended campaigns.

- **Name:** A descriptive name.
- **Destination:** “Vector Number”
- **Vector Number:** The vector number from above for handling of inbound calls.

add vdn 67701			Page 1 of 3		
VECTOR DIRECTORY NUMBER					
Extension: 67701					
Name*: TelAthena Inbound VDN					
Destination: Vector Number				701	

5.5.2. Predictive

Administer a set of hunt group, vector, and VDN for routing of outbound calls used by the predictive campaign.

Add a hunt group using the “add hunt-group n” command, where “n” is an available hunt group number. This hunt group will be used for routing of answered outbound calls to agents for the predictive campaign. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Number:** The available group number.
- **Group Name:** A descriptive name.
- **Group Extension:** An available extension number.
- **ACD:** “y”
- **Queue:** “n”
- **Vector:** “y”

Note that **Queue** is required to be disabled on this hunt group.

add hunt-group 702		Page 1 of 62
HUNT GROUP		
Group Number: 702	ACD? y	
Group Name: TelAthena Predictive	Queue? n	
Group Extension: 68702	Vector? y	
Group Type: ucd-mia		
TN: 1		
COR: 1	MM Early Answer? n	
Security Code:	Local Agent Preference? n	
ISDN/SIP Caller Display:		

Navigate to **Page 2**, and set **Skill** to “y” as shown below.

add hunt-group 701		Page 2 of 62
HUNT GROUP		
Skill? y	Expected Call Handling Time <sec>: 180	
AAS? n		
Measured: none		
Supervisor Extension:		

Modify a vector using the “change vector n” command, where “n” is an available vector number. This vector will provide routing of answered outbound calls to agents for the predictive campaign.

Administer a **queue-to** step with the hunt group number from above along with desired priority.

The vector used in the compliance testing is shown below.

change vector 702				CALL VECTOR				Page	1 of	6
Number: 702				Name: TelAthena Predictive Vector						
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	queue-to	skill 702	pri m							
02										
03										
04										

Add a VDN using the “add vdn n” command, where “n” is an available extension. This VDN will provide routing of outbound calls for the predictive campaign.

- **Name:** A descriptive name.
- **Destination:** “Vector Number”
- **Vector Number:** The vector number from above for handling of outbound calls.

add vdn 67702		VECTOR DIRECTORY NUMBER		Page	1 of	3
		Extension: 67702				
		Name*: TelAthena Predictive VDN				
		Destination: Vector Number 702				

5.5.3. Preview

SoftDialer can support either ACD or non-ACD method of routing for outbound calls used by the preview campaign. This section is only necessary for the ACD method, which was the method used in the compliance testing.

Add a hunt group using the “add hunt-group n” command, where “n” is an available hunt group number. This hunt group will be used for routing of outbound calls for the preview campaign. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Number:** The available group number.
- **Group Name:** A descriptive name.
- **Group Extension:** An available extension number.
- **ACD:** “y”
- **Queue:** “n”
- **Vector:** “y”

Note that **Queue** is required to be disabled on this hunt group.

add hunt-group 703		Page 1 of 62
HUNT GROUP		
Group Number: 703	ACD? y	
Group Name: TelAthena Inbound	Queue? n	
Group Extension: 68703	Vector? y	
Group Type: ucd-mia		
TN: 1		
COR: 1		
MM Early Answer? n		
Security Code: Local Agent Preference? n		
ISDN/SIP Caller Display:		

Navigate to **Page 2**, and set **Skill** to “y” as shown below.

add hunt-group 703		Page 2 of 62
HUNT GROUP		
Skill? y	Expected Call Handling Time <sec>: 180	
AAS? n		
Measured: none		
Supervisor Extension:		

5.6. Administer Agent Login IDs

Use the “add agent-loginID n” command, where “n” is an available extension number. Enter a descriptive **Name**. Leave the two password fields blank, and set **Auto Answer** to “acd”, which are required by SoftDialer.

```

add agent-loginID 67991                                     Page 1 of 3

                                AGENT LOGINID

Login ID: 67991                                           AAS? n
Name: TelAthena Agent 1                                   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
Attribute:                                               AUDIX Name for Messaging:

                                LoginID for ISDN/SIP Display? n
                                Password:
                                Password (enter again):
                                Auto Answer: acd

AUX Agent Remains in LOA Queue: system                   MIA Across Skills: system
  
```

Navigate to **Page 2**. For **SN**, administer an entry for each hunt group number from **Section 5.5**, and set the corresponding **SL** to the desired skill level, as shown below.

```

add agent-loginID 67991                                     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: 701  1      16:      31:      46:
2: 702  1      17:      32:      47:
3: 703  1      18:      33:      48:
4:      19:      34:      49:
  
```

Repeat this section to add an agent ID for each agent from **Section 3**. In the compliance testing, two agent IDs were added, as shown below.

```

list agent-loginID 67991 count 2

                                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
67991    TelAthena Agentunstaffed  1  lv1
          701/01  702/01  703/01  /      /      /      /      /
67992    TelAthena Agentunstaffed  1  lv1
          701/01  702/01  703/01  /      /      /      /      /
  
```


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
- Restart service
- Obtain Tlink name
- Administer TelAthena user
- Administer security database

6.1. Launch OAM Interface

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

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



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

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". On the right, a "Welcome" message displays user information: "Welcome: User", "Last login: Wed Feb 6 09:39:48 2018 from 192.168.200.20", "Number of prior failed login attempts: 0", "HostName/IP: aes7/10.64.101.239", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 7.1.1.0.0.5-0", "Server Date and Time: Wed Feb 07 09:44:48 EST 2018", and "HA Status: Not Configured". Below the header is a red navigation bar with "Home", "Help", and "Logout" links. The left sidebar contains a menu with options: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The main content area displays the "Welcome to OAM" message, stating: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:" followed by a bulleted list of domains and their functions. At the bottom, it notes: "Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain."

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Wed Feb 6 09:39:48 2018 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Wed Feb 07 09:44:48 EST 2018
HA Status: Not Configured

Home | Help | Logout

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

Welcome to OAM

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

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

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

6.2. Verify License

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

The screenshot shows the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the left sidebar. The top header and "Welcome" message are identical to the previous screenshot. The red navigation bar now shows "Licensing" as the active page. The left sidebar menu highlights "Licensing" and includes sub-items: "WebLM Server Address", "WebLM Server Access", and "Reserved Licenses". The main content area displays the "Licensing" title and provides instructions for setting up, importing, and maintaining licenses, with a bulleted list of required actions: "WebLM Server Address", "WebLM Server Access", and "Reserved Licenses".

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Wed Feb 6 09:39:48 2018 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Wed Feb 07 09:44:48 EST 2018
HA Status: Not Configured

Licensing | Home | Help | Logout

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

Licensing

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

- WebLM Server Address

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

- WebLM Server Access

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

- Reserved Licenses

Select **Licensed products** → **APPL_ENAB** → **Application Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

Verify that there is sufficient license 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: 7 - SID: 10503000

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

License installed on: September 13, 2017 1:10:08 PM +00:00

License File Host IDs: V7-2E-92-63-88-4C-01

Licensed Features

10 Items Show All

Feature (License Keyword)	Expiration date	Licensed capacity
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	3
DLG VALUE_AES_DLG	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	3

6.3. Administer TSAPI Link

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area displays the "TSAPI Links" screen, which includes a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

The **Add TSAPI Links** screen is displayed next.

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection “cm7” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Set **Security** to “Unencrypted”, and “7” was the **ASAI Link Version** used in the compliance testing.

The screenshot shows the Avaya Application Enablement Services Management Console, specifically the "Add TSAPI Links" screen. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area displays the "Add TSAPI Links" form, which includes fields for Link, Switch Connection, Switch CTI Link Number, ASAI Link Version, and Security. The Security field is set to "Unencrypted". Below the form are buttons for "Apply Changes" and "Cancel Changes".

6.4. Restart Service

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**.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Wed Feb 6 09:39:48 2018 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Wed Feb 07 09:44:48 EST 2018
HA Status: Not Configured

Maintenance | Service Controller

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

Service Controller

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

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

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

6.5. 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 SoftDialer.

In this case, the associated Tlink name is “AVAYA#CM7#CSTA#AES7”.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the text "Application Enablement Services Management Console". On the right side of the header, there is a welcome message for the user, including the last login time (Wed Feb 6 09:39:48 2018), the number of failed login attempts (0), the host name/IP (aes7/10.64.101.239), the server offer type (VIRTUAL_APPLIANCE_ON_VMWARE), the software version (7.1.1.0.0.5-0), the server date and time (Wed Feb 07 09:44:48 EST 2018), and the HA status (Not Configured). Below the header, there is a red navigation bar with the text "Security | Security Database | Tlinks" and links for "Home | Help | Logout". The left sidebar contains a tree view of the application's structure, with "Security" expanded to show "Security Database" and "Tlinks" selected. The main content area shows the "Tlinks" page with a "Tlink Name" field containing "AVAYA#CM7#CSTA#AES7" and a "Delete Tlink" button.

6.6. Administer TelAthena User

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

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

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Wed Feb 6 09:39:48 2018 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Wed Feb 07 09:44:48 EST 2018
HA Status: Not Configured

User Management | User Admin | Add User

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

■ Add User

■ Change User Password

■ List All Users

■ Modify Default Users

■ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Idtelathena

* Common Nametelathena

* Surnametelathena

* User Password.....

* Confirm Password.....

Admin Note

Avaya RoleNone ▼

Business Category

Car License

CM Home

Css Home

CT UserYes ▼

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

6.7. 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. Make certain that **Enable SDB for TSAPI Service, JTAPI and Telephony Web Services** is unchecked, as shown below.

In the event that the security database is used by the customer with the parameter enabled, then follow reference [2] to configure access privileges for the TelAthena user from **Section 6.6**.

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

Welcome: User
Last login: Wed Feb 6 09:39:48 2018 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Wed Feb 07 09:44:48 EST 2018
HA Status: Not Configured

Security | Security Database | Control Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control

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

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

Apply Changes

7. Configure TelAthena Systems neOn SoftDialer

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

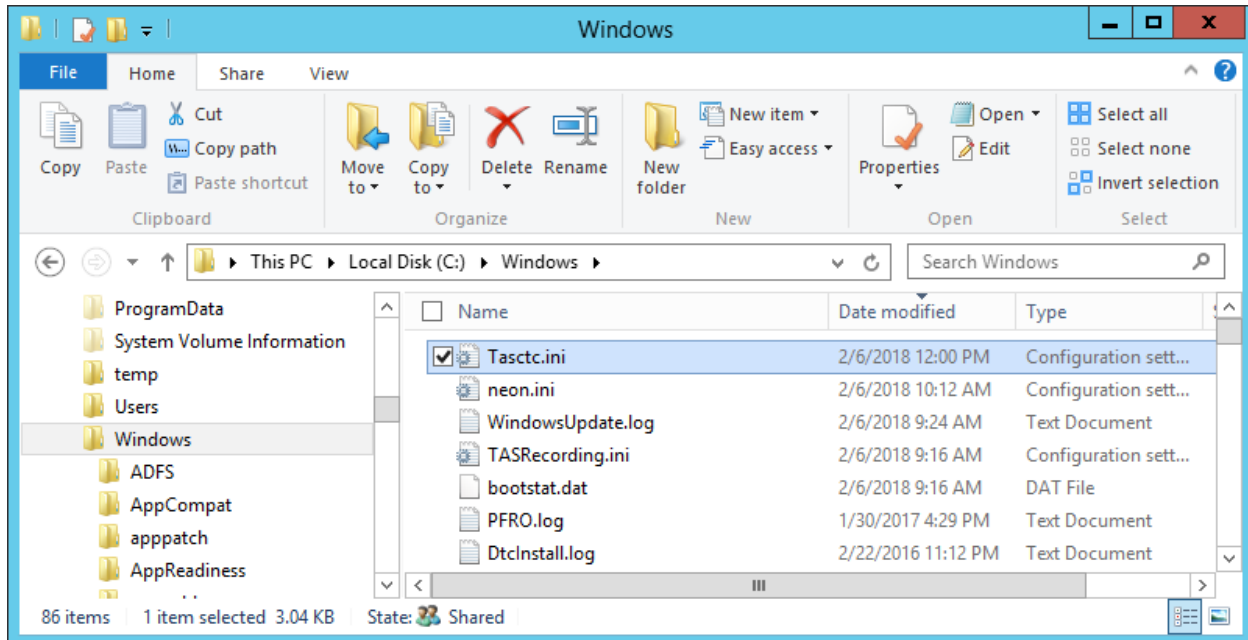
- Administer Tasctc.ini
- Administer TSLIB.INI
- Launch TelAthena Supervisor
- Administer user ID maintenance
- Administer operations
- Administer Campaign Controller maintenance

The configuration of SoftDialer is performed by TelAthena Support engineers. The procedural steps are presented in these Application Notes for informational purposes.

In addition to the shown procedural steps, the application requires the location, branch, Campaign Controller, user status, and job assignments to be configured by following reference [3].

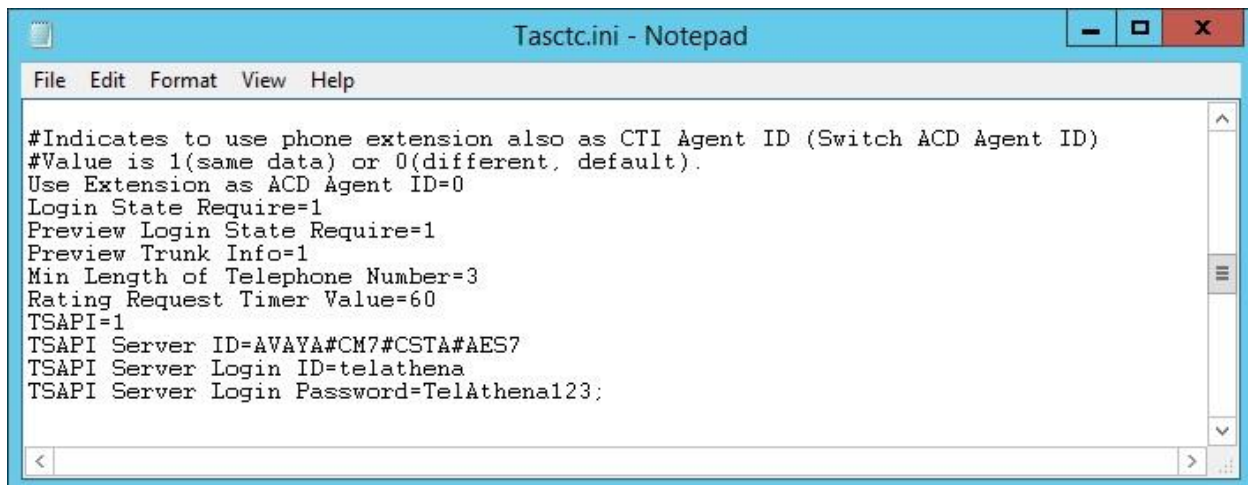
7.1. Administer Tasctc.ini

From the neOn SoftDialer Gateway, navigate to the **C:\Windows** directory to edit the **Tasctc.ini** file shown below.



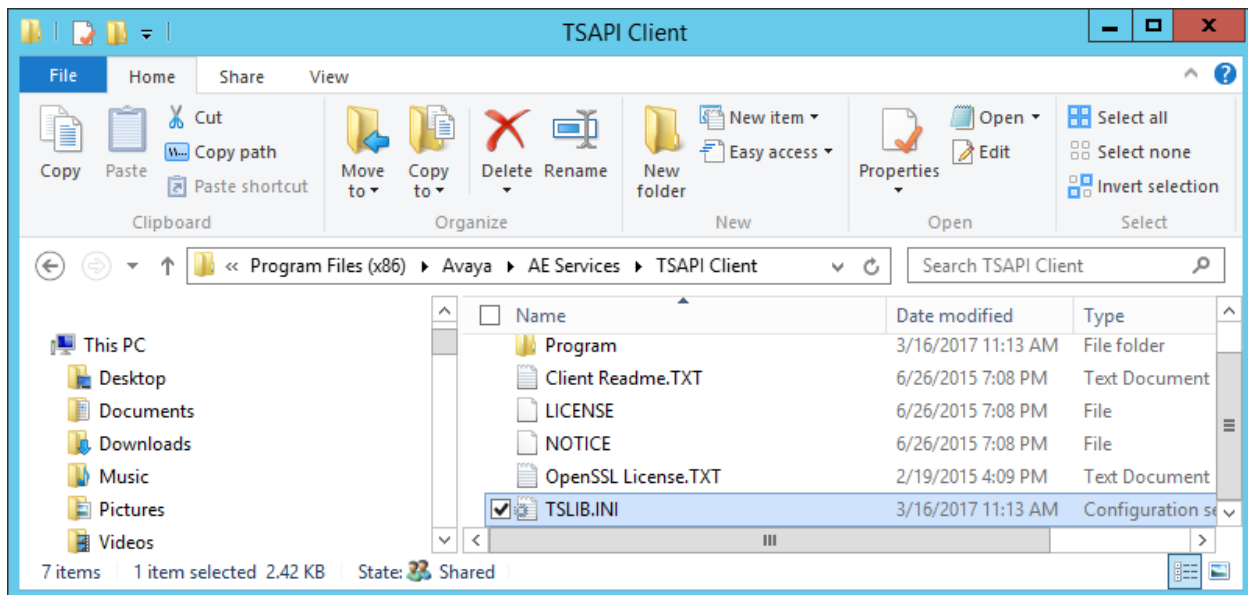
Scroll down to the **CTI Agent ID** sub-section. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **TSAPI Server ID:** The Tlink name from **Section 6.5**.
- **TSAPI Server Login ID:** The TelAthena user credentials from **Section 6.6**.
- **TSAPI Server Login Password:** The TelAthena user credentials from **Section 6.6**.

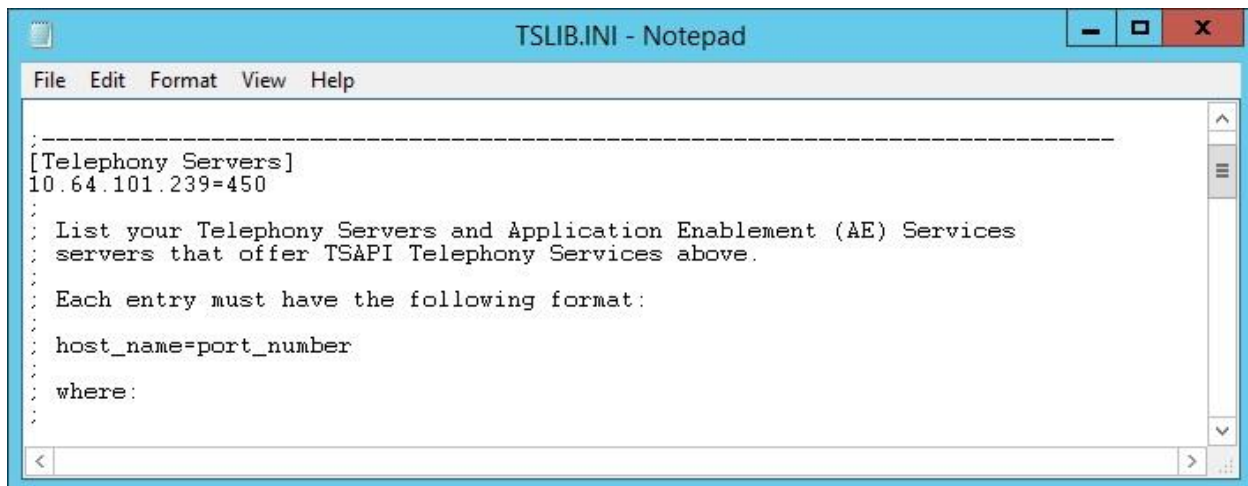


7.2. Administer TSLIB.INI

Navigate to the **C:\Program Files (x86)\Avaya\AE Service\TSAPI Client** directory to edit the **TSLIB.INI** file shown below.



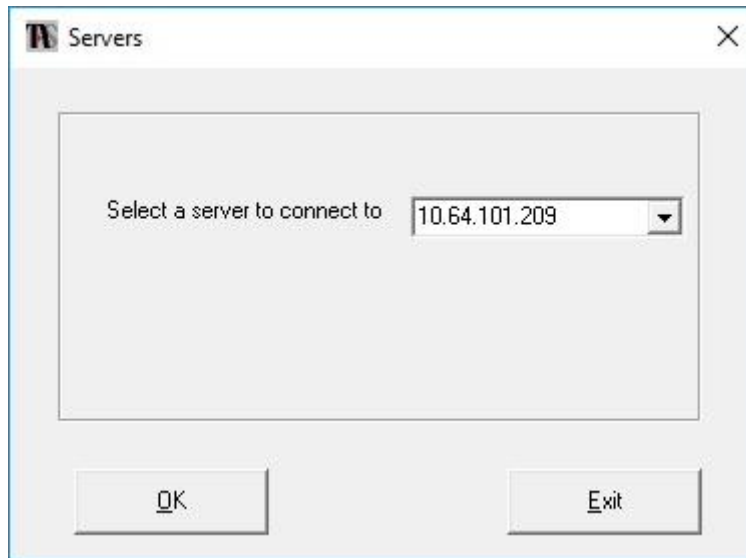
In the **Telephony Servers** sub-section, enter an entry shown below, where “10.64.101.239” is the IP address of Application Enablement Services.



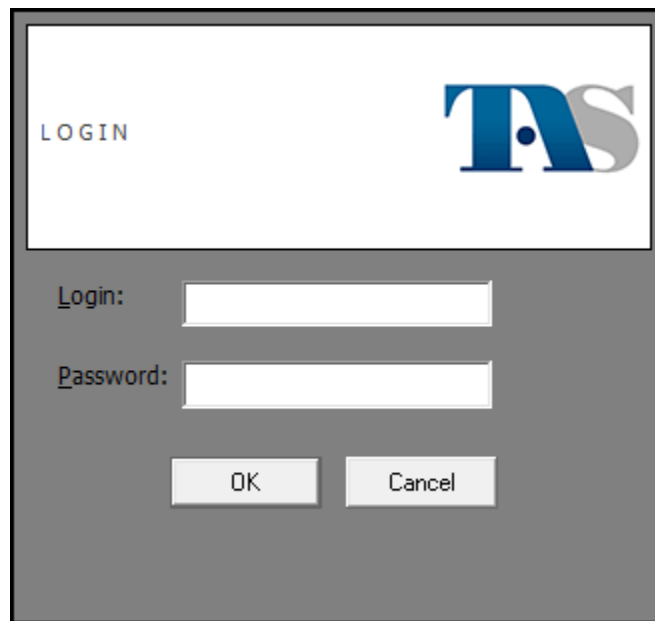
7.3. Launch TelAthena Supervisor

From the supervisor PC running the TelAthena Supervisor application, select **Windows** → **TELEATHENA SYSTEMS** → **TelAthena Supervisor 6.4.0** to launch the application.

The **Servers** screen is displayed. Select the pertinent server, in this case “10.64.101.209”, which is the IP address of the neOn Server.



The **LOGIN** screen is displayed next. Log in using the appropriate credentials.

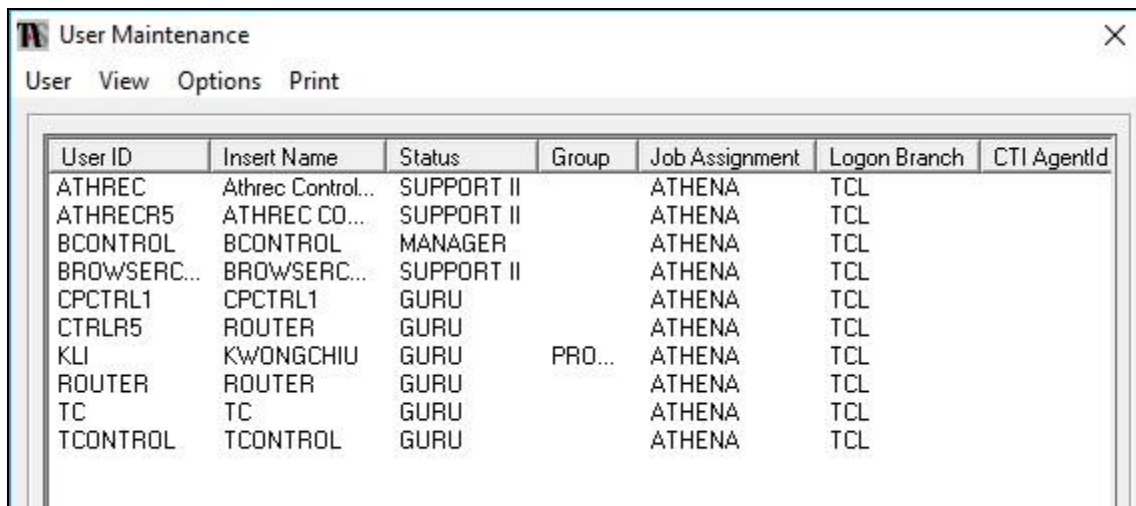


7.4. Administer User ID Maintenance

The **Control Panel** screen is displayed. Double click on **User ID Maintenance**.



The **User Maintenance** screen is displayed next. Select **User** → **New** to add a new user.

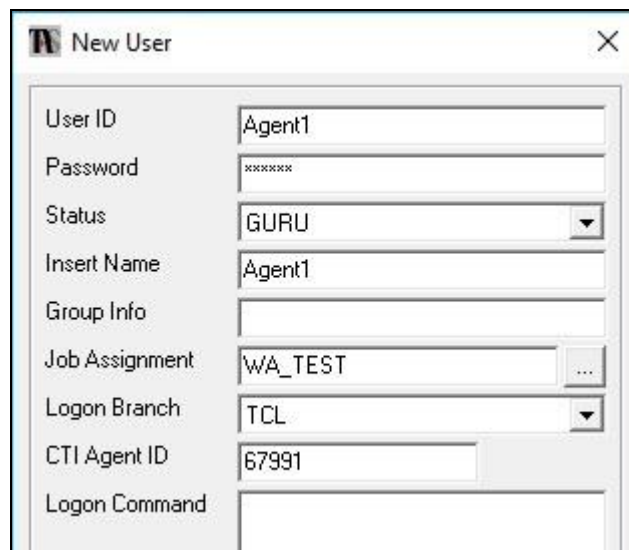


The screenshot shows a 'User Maintenance' window with a menu bar containing 'User', 'View', 'Options', and 'Print'. Below the menu bar is a table with the following data:

User ID	Insert Name	Status	Group	Job Assignment	Logon Branch	CTI AgentId
ATHREC	Athrec Control...	SUPPORT II		ATHENA	TCL	
ATHRECR5	ATHREC CO...	SUPPORT II		ATHENA	TCL	
BCONTROL	BCONTROL	MANAGER		ATHENA	TCL	
BROWSERC...	BROWSERC...	SUPPORT II		ATHENA	TCL	
CPCTRL1	CPCTRL1	GURU		ATHENA	TCL	
CTRLR5	ROUTER	GURU		ATHENA	TCL	
KLI	KWONGCHIU	GURU	PRO...	ATHENA	TCL	
ROUTER	ROUTER	GURU		ATHENA	TCL	
TC	TC	GURU		ATHENA	TCL	
TCONTROL	TCONTROL	GURU		ATHENA	TCL	

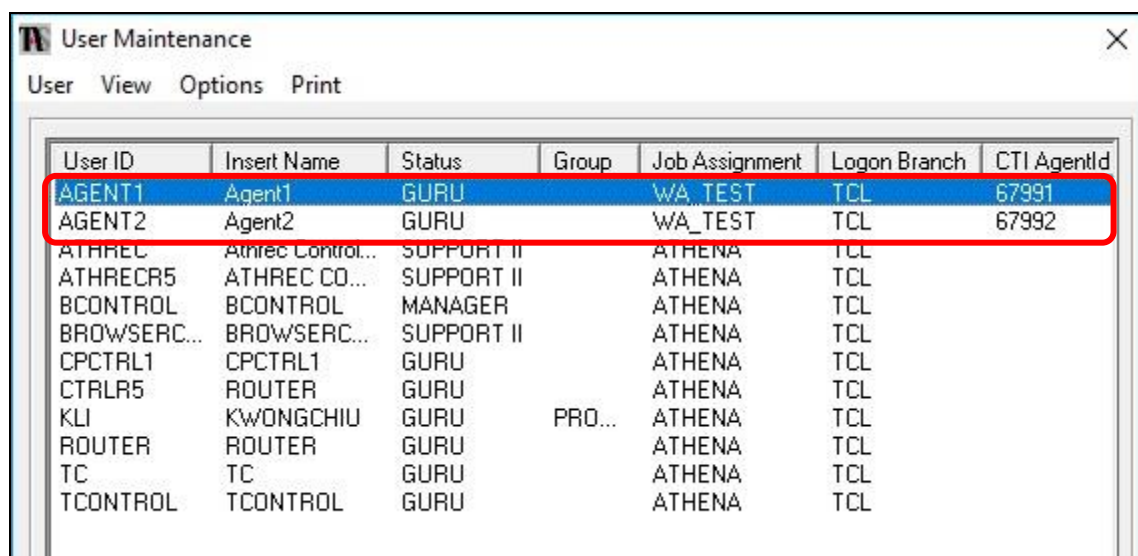
The **New User** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **User ID:** A desired login name for the first agent user from **Section 3**.
- **Password:** A desired password for authentication with SoftDialer.
- **Status:** Select an applicable and pre-existing status.
- **Insert Name:** A desired display name for the first agent user from **Section 3**.
- **Job Assignment:** Select an applicable and pre-existing job assignment.
- **Logon Branch:** Select an applicable and pre-existing branch.
- **CTI Agent ID:** The corresponding agent login ID from **Section 5.6**.



User ID	Agent1
Password	xxxxxx
Status	GURU
Insert Name	Agent1
Group Info	
Job Assignment	WA_TEST
Logon Branch	TCL
CTI Agent ID	67991
Logon Command	

Repeat this section to create a user for each agent from **Section 3**. In the compliance testing, two users were configured, as shown below.



User ID	Insert Name	Status	Group	Job Assignment	Logon Branch	CTI AgentId
AGENT1	Agent1	GURU		WA_TEST	TCL	67991
AGENT2	Agent2	GURU		WA_TEST	TCL	67992
ATHREC	Athrec Control...	SUPPORT II		ATHENA	TCL	
ATHRECR5	ATHREC CO...	SUPPORT II		ATHENA	TCL	
BCONTROL	BCONTROL	MANAGER		ATHENA	TCL	
BROWSERC...	BROWSERC...	SUPPORT II		ATHENA	TCL	
CPCTRL1	CPCTRL1	GURU		ATHENA	TCL	
CTRLR5	ROUTER	GURU		ATHENA	TCL	
KLI	KWONGCHIU	GURU	PRO...	ATHENA	TCL	
ROUTER	ROUTER	GURU		ATHENA	TCL	
TC	TC	GURU		ATHENA	TCL	
TCONTROL	TCONTROL	GURU		ATHENA	TCL	

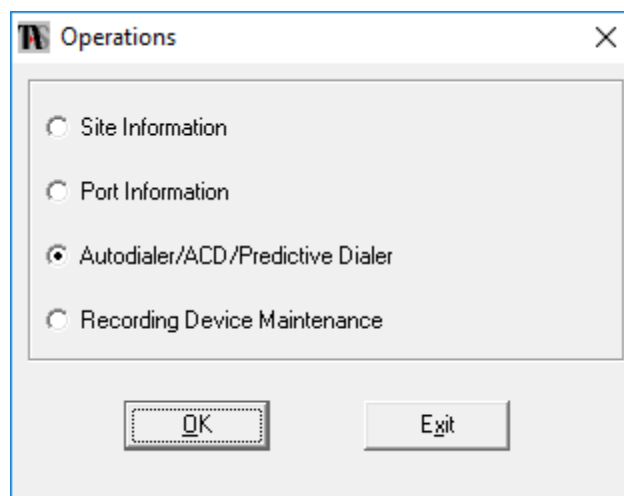
7.5. Administer Operations

The **Control Panel** screen is displayed again. Double click on **Operations**.



7.5.1. Autodialer/ACD/Predictive Dialer

The **Operations** screen is displayed next. Select **Autodialer/ACD/Predictive Dialer**.



The **Autodialer/ACD/Predictive Dialer** screen is displayed. For **Select Campaign Controller**, select the pertinent and pre-existing controller. For **Constant Dialing Prefix**, enter the required prefix for outbound calls for the network to the PSTN, in this case “91”. Retain the default value in the remaining fields.

Select **Translation Table** from the top menu.

Autodialer/ACD/Predictive Dialer

ACD INFORMATION

Select Campaign Controller

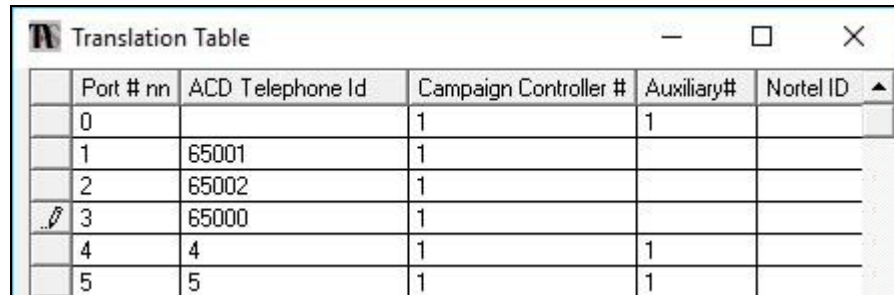
CtcCamController-NY

Type of ACD	CTC	Constant Hangup Prefix	
Wakeup Command		Hangup Completion Information	
Hangup Command		ACD Reply to Hangup?	<input type="checkbox"/>
Dialing Command		Hangup Command Required?	<input checked="" type="checkbox"/>
Transmission Termination Command		ACD Reply to Dial?	<input type="checkbox"/>
Constant Dialing Prefix	91	ACD acknowledge reception?	<input checked="" type="checkbox"/>
Dial Local Area Code ?	<input type="checkbox"/>	Seconds before aborting	15
Local Area Code Prefix		Mask for Telephone Number Info	
Non-Local Area Code Prefix		Mask all Commands?	<input type="checkbox"/>
Suffix After Telno		Constant Prefix, All Commands	
		Constant Suffix, All Commands	
		Number Dialer Cprs	
		Number Bill Code Digits	
		IP Address and Port(s)	10.64.101.208,6003

Save Exit

The **Translation Table** screen is displayed. Starting with the **Port # nn** of “1” row, fill out a row for each agent and supervisor station from **Section 3**, as shown below.

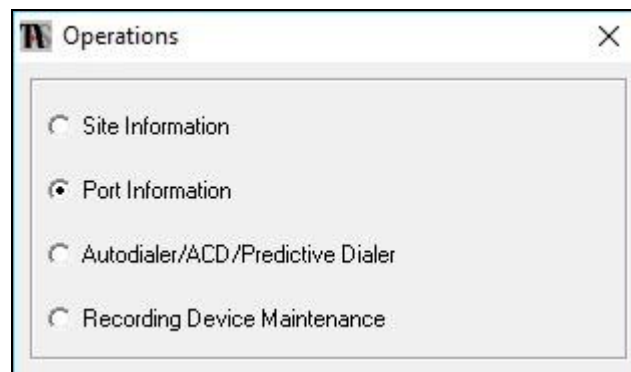
- **ACD Telephone Id:** The pertinent station extension from **Section 3**.
- **Campaign Controller #:** The pertinent and pre-existing Campaign Controller number.
- **Auxiliary#:** Blank out the default value.



Port # nn	ACD Telephone Id	Campaign Controller #	Auxiliary#	Nortel ID
0		1	1	
1	65001	1		
2	65002	1		
3	65000	1		
4	4	1	1	
5	5	1	1	

7.5.2. Port Information

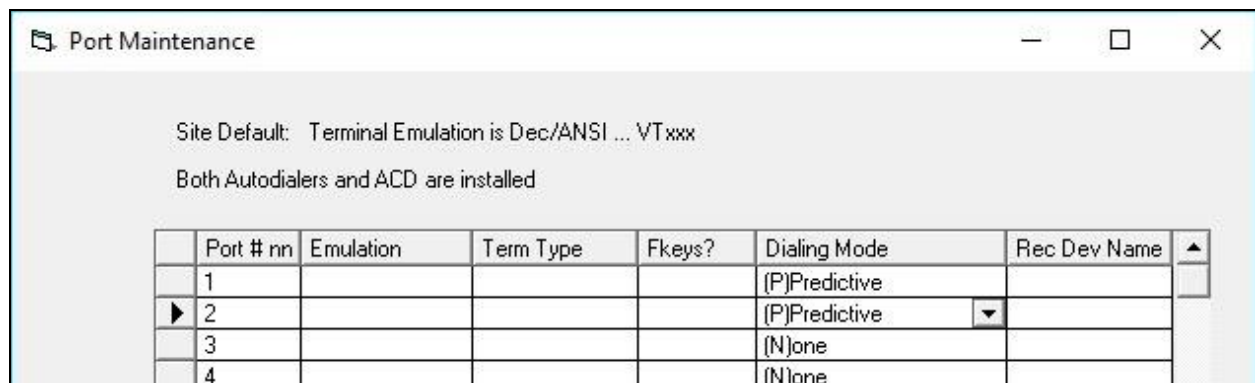
The **Operations** screen is displayed again. Select **Port Information**.



Operations

☐ Site Information
☒ Port Information
☐ Autodialer/ACD/Predictive Dialer
☐ Recording Device Maintenance

The **Port Maintenance** screen is displayed. For each translation table entry from **Section 7.5.1** that is associated with an agent station, configure the corresponding **Port # nn** row. For **Dialing Mode**, select **(P)Predictive**, as shown below.



Port Maintenance

Site Default: Terminal Emulation is Dec/ANSI ... VTxxx

Both Autodialers and ACD are installed

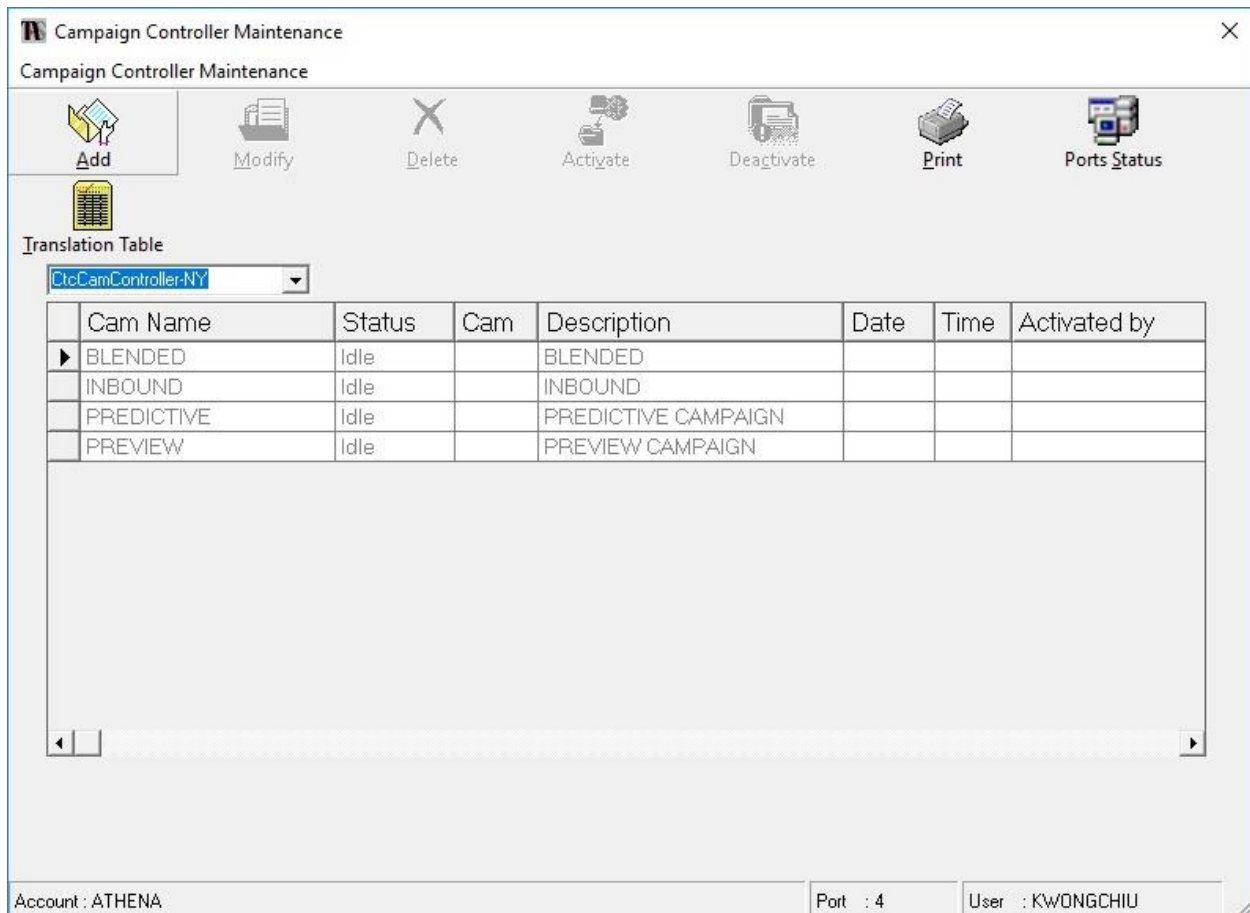
Port # nn	Emulation	Term Type	Fkeys?	Dialing Mode	Rec Dev Name
1				(P)Predictive	
2				(P)Predictive	
3				(N)one	
4				(N)one	

7.6. Administer Campaign Controller Maintenance

The **Control Panel** screen is displayed again. Double click on **Campaign Controller Maintenance**.



The **Campaign Controller Maintenance** screen is displayed. Select **Add** from the top menu, and follow reference [3] to create needed campaigns. In the compliance testing, four campaigns were created, as shown below.



7.6.1. Blended Campaign

For the blended campaign, enter the following values for the specified fields, and configure the remaining parameters by following reference [3].

- **Default DNIS:** The full PSTN number for the inbound VDN from **Section 5.5.1**.
- **Default RouteDest:** The inbound hunt group extension from **Section 5.5.1**.
- **Default RouteLoc:** The inbound VDN extension from **Section 5.5.1**.

Campaign BLENDED Status: Idle Last Use: 06 Feb 2018 02:32PM by GURU KLI

Activate **Translation Table** **Print**

Comment: BLENDED

Account: WA_TEST

Modifier: Blended

Drop Percent: 50

Telno File:

Telno Attribute:

NA Timeout: 30

Bill Code:

Ans Machine? ☒

AutoLogoff? ☐

Logical Link Id: 1

CamStopForce: ☐

UserPace: 100

DNIS-RouterDest: ☒

MaxCallOverride:

Ivr User Info:

Remote DB Name:

Table Name:

AnsMachineExtn:

698 Queued within 9 Queues

Queues	Status	Count
DEMO	R	204
KLI	R	257
LP	R	6
PD.ANSMACH	R	13
PD.BUSY	R	106
PD.NOANSWER	R	14
PD.NUISANCE	R	3
PD.UNKNOWN	R	82
PRED_UAT	R	13

Ports **Cam** **User**

1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		

Cam Ports

1-2

Default DNIS: 3035367701

Default RouteDest: 68701

Default RouteLoc: 67701

7.6.2. Inbound Campaign

For the inbound campaign, enter the following values for the specified fields, and configure the remaining parameters by following reference [3].

- **Default DNIS:** The full PSTN number for the inbound VDN from **Section 5.5.1**.
- **Default RouteDest:** The inbound hunt group extension from **Section 5.5.1**.
- **Default RouteLoc:** The inbound VDN extension from **Section 5.5.1**.

Campaign INBOUND Status: Idle Last Use: 07 Feb 2018 01:12PM by GURU KLI

Activate Translation Table Print

Comment: INBOUND

Account: WA_TEST

Modifier: Inbound

Drop Percent: 50

Telno File:

Telno Attribute:

NA Timeout: 30

Bill Code:

Ans Machine? ☒

AutoLogoff? ☐

Logical Link Id: 1

CamStopForce: ☐

UserPace: 100

DNIS-RouterDest: ☒

MaxCallOverride:

Ivr User Info:

Remote DB Name:

Table Name:

AnsMachineExtn:

Default DNIS: 3035367701

Default RouteDest: 68701

Default RouteLoc: 67701

698 Queued within 9 Queues

Queues	Status	Count
DEMO	R	204
KLI	R	257
LP	R	6
PD.ANSMACH	R	13
PD.BUSY	R	106
PD.NOANSWER	R	14
PD.NUISANCE	R	3
PD.UNKNOWN	R	82
PRED_UAT	R	13

Ports	Cam	User	Cam Ports
1			1-2
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			

7.6.3. Predictive Campaign

For the predictive campaign, enter the following values for the specified fields, and configure the remaining parameters by following reference [3].

- **Default RouteDest:** The predictive hunt group extension from **Section 5.5.2.**
- **Default RouteLoc:** The predictive VDN extension from **Section 5.5.2.**

Campaign PREDICTIVE Status: Idle Last Use: 09 Feb 2018 11:10AM by GURU KLI

Activate **Translation Table** **Print**

Comment: PREDICTIVE CAM
Account: WA_TEST
Modifier: Predictive
Drop Percent: 50
Telno File: CLIENT
Telno Attribute: 7
NA Timeout: 30
Bill Code:
Ans Machine? ☐
AutoLogoff? ☐
Logical Link Id: 1
CamStopForce ☐
UserPace: 100
DNIS-RouterDest ☒
MaxCallOverride:
Ivr User Info:
Remote DB Name:
Table Name:
AnsMachineExtn:
SmartConnect ☐

698 Queued within 9 Queues

Queues	Status	Count
DEMO	R	204
KLI	R	257
LP	R	6
PD.ANSMACH	R	13
PD.BUSY	R	106
PD.NOANSWER	R	14
PD.NUISANCE	R	3
PD.UNKNOWN	R	82
PRED_UAT	R	13

Ports **Cam** **User** **Cam Ports**

1			1-2
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			

Default RouteDest: 68702
Default RouteLoc: 67702

7.6.4. Preview Campaign

For the Preview campaign, enter the following values for the specified fields, and configure the remaining parameters by following reference [3].

- **Default RouteDest:** The preview hunt group extension from **Section 5.5.3**, if applicable.
- **Default RouteLoc:** The preview hunt group extension from **Section 5.5.3**, if applicable.

Campaign PREVIEW Status: Idle Last Use: 06 Feb 2018 02:28PM by GURU KLI

Activate **Translation Table** **Print**

Comment: PREVIEW CAMPA
Account: WA_TEST
Modifier: Preview
Drop Percent: 50
Telno File:
Telno Attribute:
NA Timeout: 30
Bill Code:
Ans Machine?: ☒
AutoLogoff?: ☐
Logical Link Id: 1
CamStopForce: ☐
UserPace: 100
DNIS-RouterDest: ☒
MaxCallOverride:
Ivr User Info: 8887777565
Remote DB Name:
Table Name:
AnsMachineExtn:

Default RouteDest: 68703
Default RouteLoc: 68703

698 Queued within 9 Queues

Queues	Status	Count
DEMO	R	204
KLI	R	257
LP	R	6
PD.ANSMACH	R	13
PD.BUSY	R	106
PD.NOANSWER	R	14
PD.NUISANCE	R	3
PD.UNKNOWN	R	82
PRED_UAT	R	13

Ports **Cam** **User** **Cam Ports**

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17

1-2

8. Verification Steps

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

8.1. Verify Avaya Aura® Communication Manager

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


```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	7	no	aes7	established	72	63

8.2. Verify Avaya Aura® Application Enablement Services

From Application Enablement Services, verify status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** (not shown) 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 total number of active campaigns, logged in agents, and active predictive calls. In the case below, there was one active campaign with two logged in agents, and therefore “3”.

**Application Enablement Services**
Management Console

Welcome: User
Last login: Wed Feb 7 09:40:44 2018 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Wed Feb 07 10:00:16 EST 2018
HA Status: Not Configured

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

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Log Manager

▶ Logs

▼ Status and Control

TSAPI Link Details

☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	cm7	1	Talking	Wed Feb 7 09:06:25 2018	Online	17	3	22	26	30

Online Offline

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

8.3. Verify TelAthena neOn SoftDialer

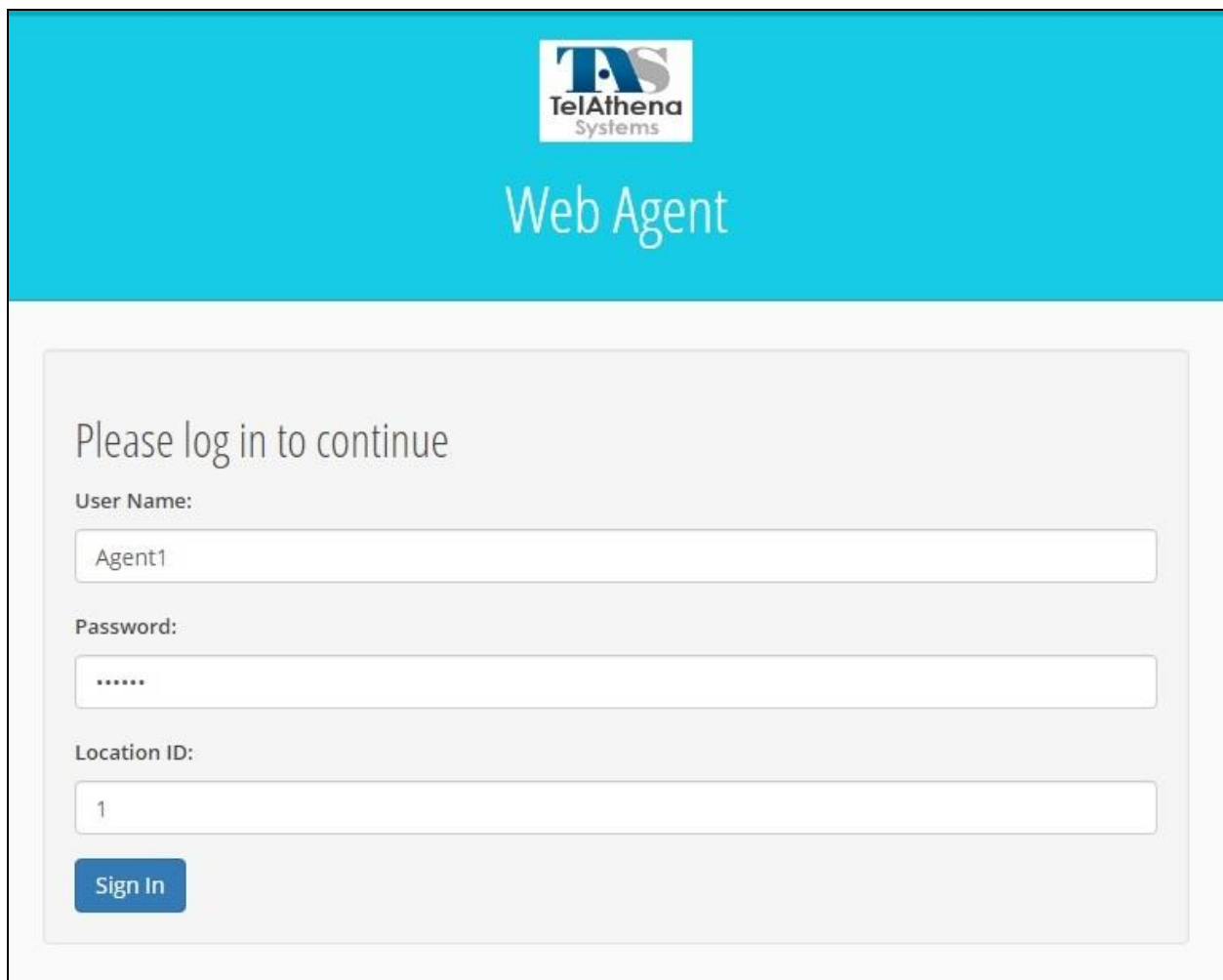
This section provides the tests that can be performed to verify inbound, outbound preview, and outbound predictive calls.

8.3.1. Verify Inbound

Follow reference [3] to start a blended campaign via the TelAthena Supervisor application. Note that the blended campaign covers both inbound and outbound preview calls.

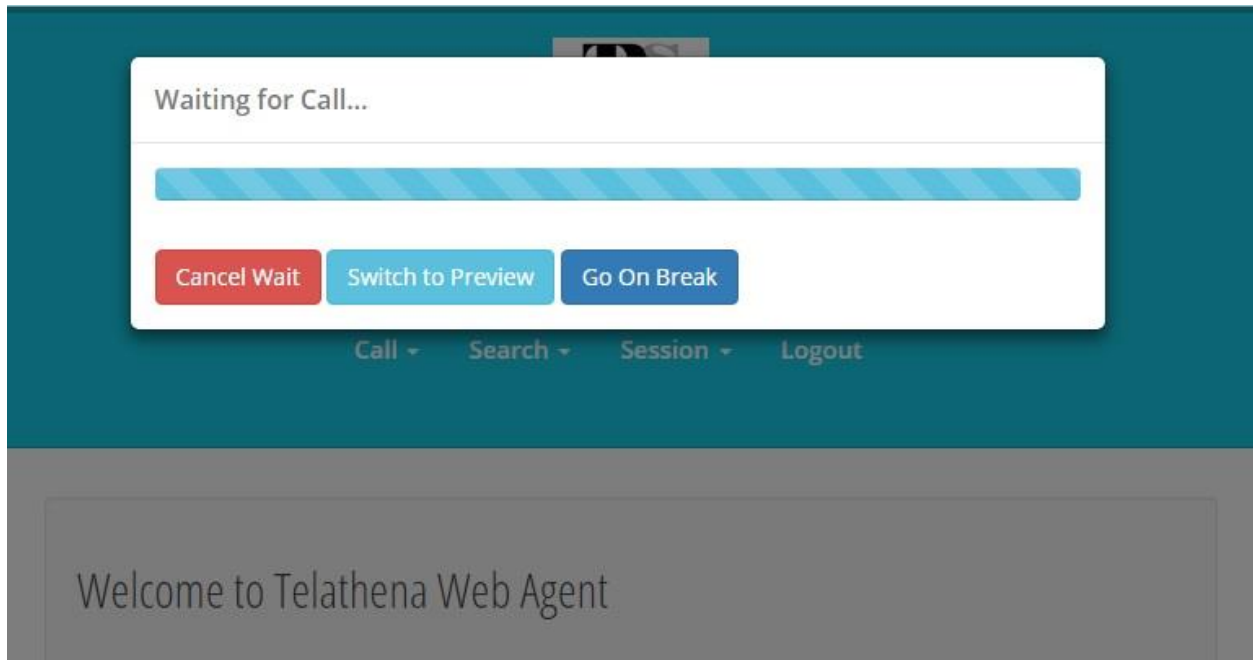
From an agent desktop, access the web-based interface by using the URL “https://ip-address:8080/webagent3/login.htm” in an Internet browser window, where “ip-address” is the IP address of the neOn Server.

The **Web Agent** screen below is displayed. Log in using an appropriate credential from **Section 7.4**, and enter an applicable and pre-existing location ID.

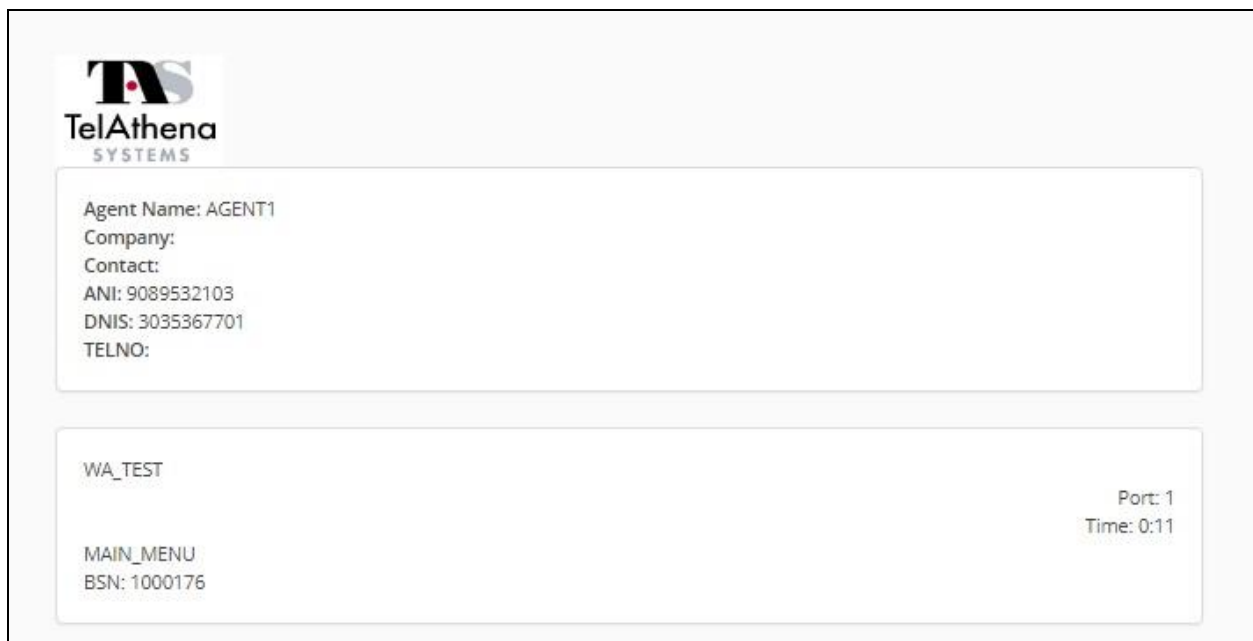


The screenshot shows the TelAthena Web Agent login interface. At the top, there is a blue header bar containing the TelAthena Systems logo and the text "Web Agent". Below the header, the main content area is light gray and contains a login form. The form starts with the text "Please log in to continue". It then has three input fields: "User Name:" with the value "Agent1", "Password:" with the value "*****", and "Location ID:" with the value "1". At the bottom left of the form is a blue "Sign In" button.

The **Waiting for Call** screen is displayed next, showing the agent being available for inbound calls.



Place an inbound call from the PSTN to the full number associated with the inbound VDN from **Section 5.5.1**. Verify that the available agent is automatically connected to the PSTN caller with two-way talk path, and that the agent screen is updated with proper values in the **ANI** and **DNIS** fields shown below.



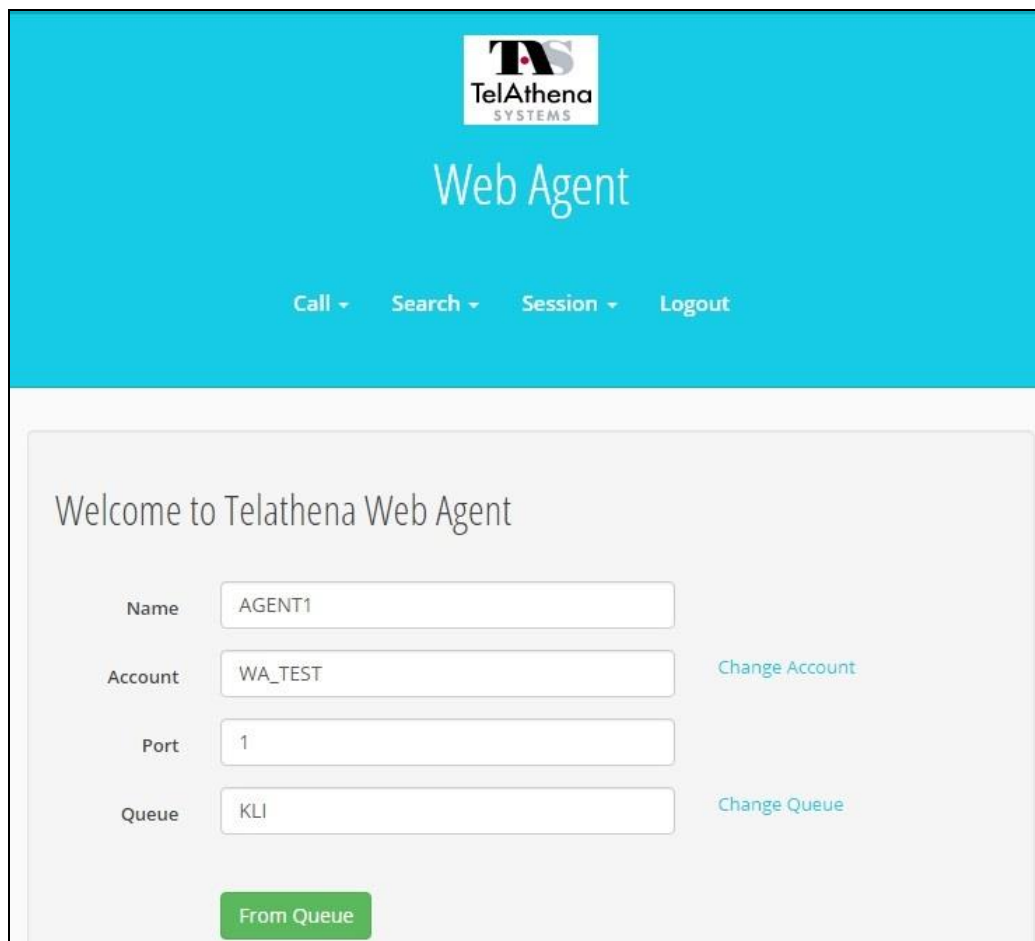
8.3.2. Verify Preview

Follow reference [3] to complete the inbound call from **Section 8.3.1**. The **Waiting for Call** screen is displayed again.

Select **Switch to Preview**.



Verify the screen below is displayed next. Select **From Queue**.

A screenshot of the TelAthena Web Agent 'Welcome' screen. The top section has a blue header with the TelAthena logo and the text 'Web Agent'. Below the header are four links: 'Call', 'Search', 'Session', and 'Logout'. The main content area is light gray and contains the text 'Welcome to Telathena Web Agent'. Below this text are four input fields: 'Name' (AGENT1), 'Account' (WA_TEST), 'Port' (1), and 'Queue' (KLI). To the right of the 'Account' and 'Queue' fields are links 'Change Account' and 'Change Queue' respectively. At the bottom of the form is a green button labeled 'From Queue'.

Verify the screen below is displayed, which contained customer record information for the agent to preview.

Scroll down the agent screen as necessary and select **Dial** (not shown) to launch the outbound preview call. Verify that an outbound call is launched on behalf of agent to the PSTN destination shown below, and that the agent can hear the call progress tones.

Answer the outbound call at the PSTN destination, and verify that the agent is connected with the PSTN party with two-way talk path.

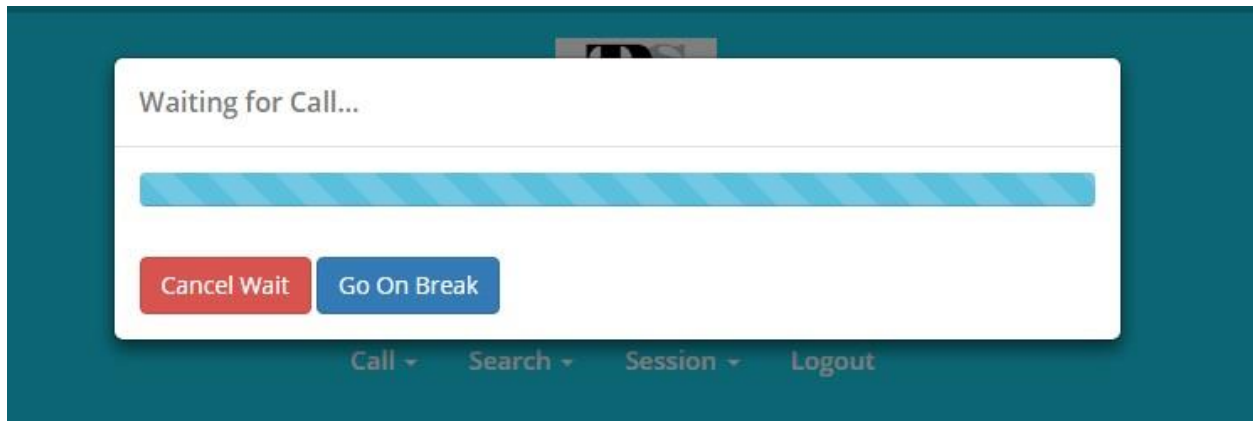


The screenshot displays the TelAthena SYSTEMS agent interface. At the top left is the TelAthena logo. Below it, a white box contains the following text: Agent Name: AGENT1, Company: Smith Industries, Contact: Rybolt, ANI:, DNIS:, and TELNO:2027448584. Below this box, another white box contains the text: WA_TEST, KLI, MAIN_MENU, and BSN: 53. In the bottom right corner of the interface, the text 'Port: 1' and 'Time: 0:05' is displayed.

8.3.3. Verify Predictive

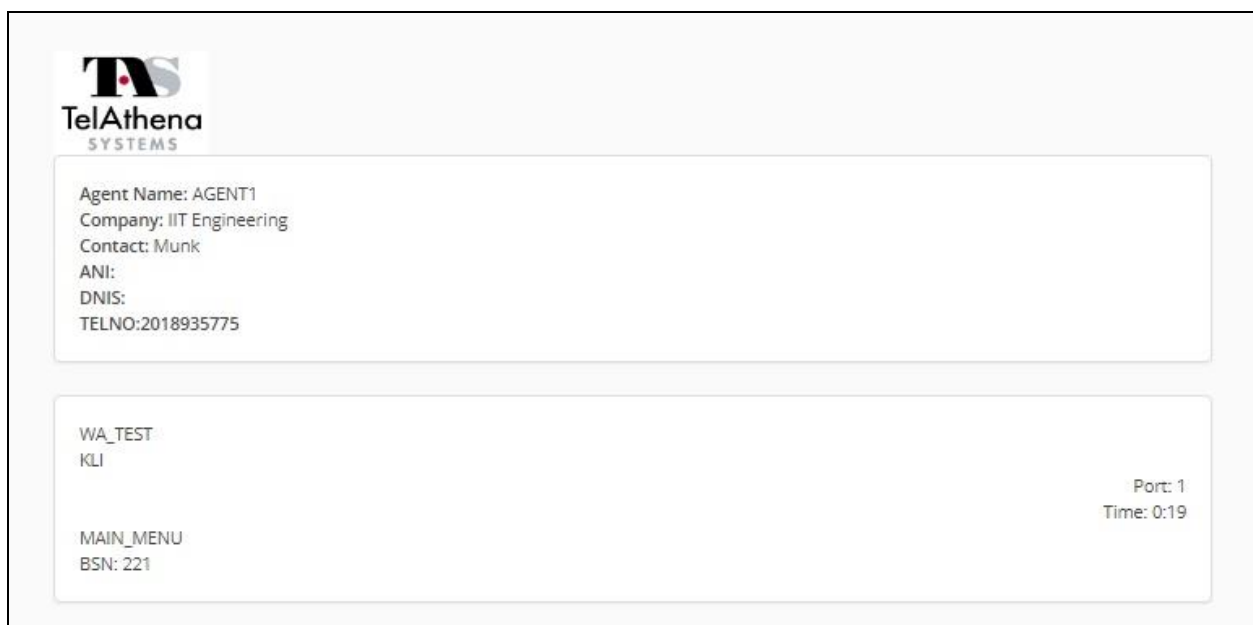
Follow reference [3] to start a predictive campaign via the TelAthena Supervisor application, and follow the procedures in **Section 8.3.1** to log an agent into SoftDialer.

The **Waiting for Call** screen below is displayed on the agent desktop.



Verify that a predictive call is automatically launched by SoftDialer to a PSTN destination associated with the predictive campaign calling list, and with call progress tones classified by Communication Manager.

Answer the call at the PSTN destination. Verify that the available agent is automatically connected to the PSTN party with two-way talk path, and that the agent screen is updated with the pertinent customer record information, as shown below.



9. Conclusion

These Application Notes describe the configuration steps required for TelAthena neOn SoftDialer to successfully interoperate with Avaya Aura® Application Enablement Services 7.1.1 and Avaya Aura® Communication Manager 7.1.1. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 7.1.1, Issue 2, August 2017, available at <http://support.avaya.com>.
2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.1.1, Issue 3, September 2017, available at <http://support.avaya.com>.
3. *TelAthena Systems Administrator Guide*, Rev 1.1, available upon request to TelAthena Support.

©2018 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.