



Avaya Solution & Interoperability Test Lab

Application Notes for Interactive Northwest, Inc INI SureConnect™ with Avaya Aura® Application Enablement Service and Avaya Aura® Experience Portal – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Interactive Northwest, Inc INI SureConnect™ with Avaya Aura® Application Enablement Service and Avaya Aura® Experience Portal.

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 to integrate Interactive Northwest, Inc INI SureConnect™ (SureConnect) with Avaya Aura® Application Enablement Service (AES) and Avaya Aura® Experience Portal (Experience Portal). SureConnect offers contact center callers the ability to request a callback instead of waiting in queue. Once the callback has been requested, SureConnect offers call centers two different types of options:

- **AgentFirst:** SureConnect (via Experience Portal) calls the agent first and once agent confirms callers' information, customer is connected to the call.
- **CallerFirst:** SureConnect (via Experience Portal) calls the customer first and once the customer agrees, an available agent is connected to the call.

SureConnect integrates with Experience Portal via VoiceXML and CCXML applications to offer callback requests to callers and generate callbacks. SureConnect uses the application web interface provided by Experience Portal to place calls to those callers/agents for outbound callbacks. SureConnect integrates with AES via TSAPI interface. SureConnect monitors the skill configured on Communication Manager via AES to monitor calls to agent skills.

The incoming contact center caller call flow follows:

- Customer calls the contact center and gets routed to Experience Portal via vector programming.
- Once the call is answered by the SureConnect application configured on Experience Portal (via H.323 channels), caller is offered a call back.
- If callback is accepted, SureConnect confirms the caller's phone number.
- If customer decides to decline the callback option, call is routed back to queue on Communication Manager.
- SureConnect places the call back request to the caller via Experience Portal (via SIP).
- If CallerFirst option is used, the caller answers, call is transferred to agent queue (with high priority) on Communication Manager.
- If AgentFirst option is used, the agent answers, confirms customers information, and launches callback to the customer, who is then connected to the call.

2. General Test Approach and Test Results

This section describes the interoperability compliance testing used to verify the SureConnect with AES and Experience Portal.

The interoperability compliance test included feature and serviceability testing. The feature testing focused on routing calls to Experience Portal and running the SureConnect application to allow the caller the option to request a call back. All of the call back request options available in the SureConnect Inbound application were tested. In addition, the SureConnect Outbound application was also verified. The Outbound module initiated the call back to the agent and caller and established a two-way talk path. Conditions where the call back could not be established were also verified. In these cases, the call was either rescheduled or marked as failed, if the number of retries were exceeded. Finally, the registered call back requests and call back status were verified in SureConnect reports.

The serviceability testing focused on verifying the ability of SureConnect server, and AES and Experience Portal to recover from adverse conditions, such as power failures and disconnecting network.

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.

2.1. Interoperability Compliance Testing

Interoperability compliance testing included feature and serviceability testing. The feature testing focused on the following functionality:

- Routing incoming calls to Experience Portal via H.323 channels.
- Experience Portal successfully running SureConnect application.
- The ability of the caller to continue waiting in queue for an agent.
- The ability of the caller to make a call back request. Various offered call back options were tested.
- Routing outbound calls from Experience Portal via SIP trunk.
- SureConnect servicing call back requests (agent first and customer first) via Experience Portal.
- The ability to reschedule a call back if the call to the agent or caller is not completed within a specified timeout value.

The serviceability testing focused on verifying the ability of SureConnect to recover from adverse conditions, such as power and network failures.

2.2. Test Results

All executed test cases passed.

2.3. Support

For technical support on the SureConnect, contact Interactive Northwest, Inc via phone, email, or internet.

- **Phone:** 800-808-8090
- **Email:** support@interactivenw.com
- **Web:** <https://www.interactivenw.com/>

3. Reference Configuration

Figure 1 below depicts the lab configuration used for testing. In this configuration, Experience Portal interfaces with Communication Manager via H.323 channels for inbound calls and with Session Manager via SIP trunk for outbound calls. The SureConnect server hosted the SureConnect application. The SureConnect server also connected to AES via TSAPI.

Note that connectivity between Communication Manager, Session Manager and Experience Portal is standard in nature and as such, it is not included in this document. Please refer to documentation in **Section 11**.

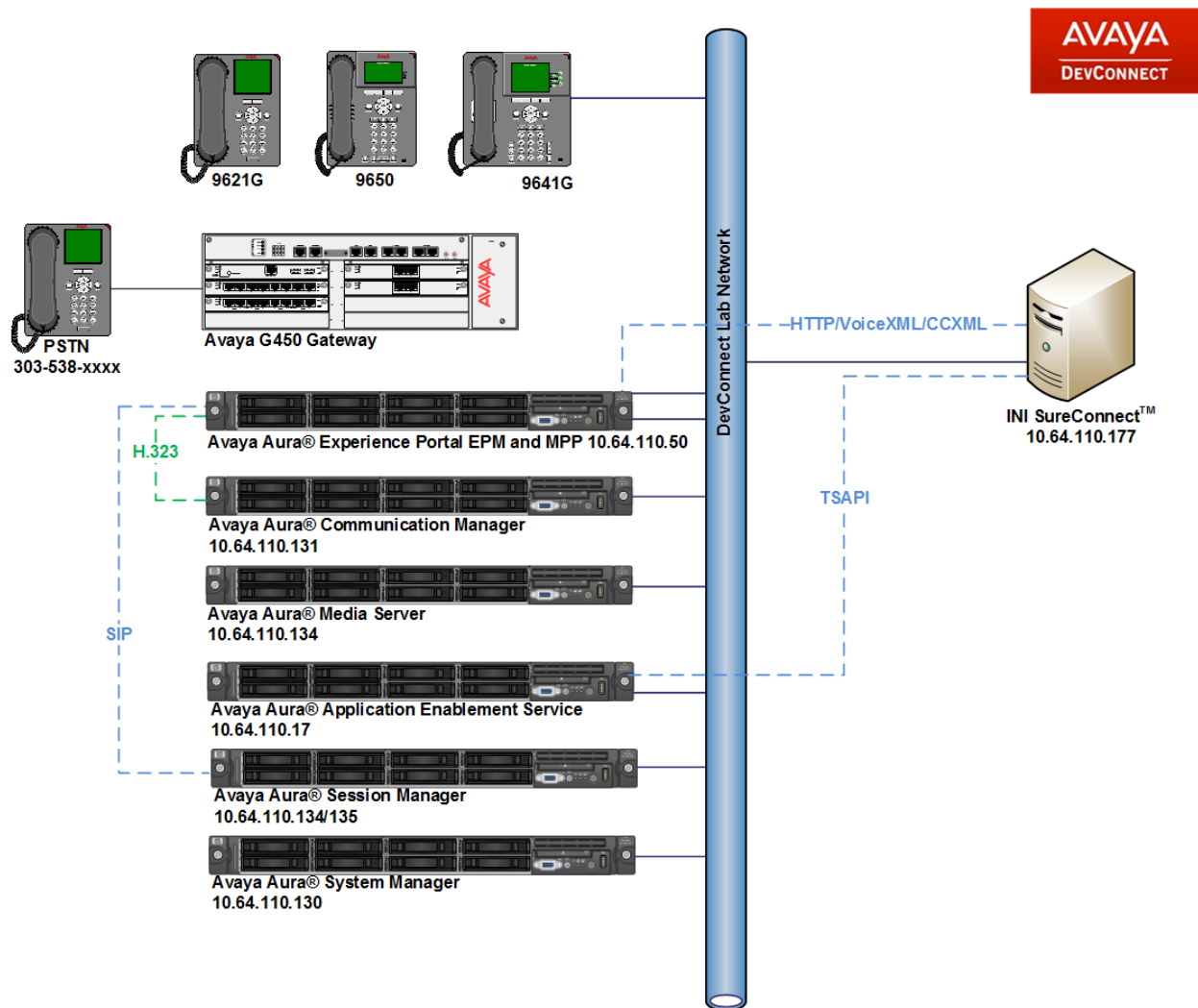


Figure 1: Test Configuration Diagram

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	8.0.0.1.2 Service Pack 1 Patch 2
Avaya Aura® Session Manager	8.0.0.0.800035
Avaya Aura® System Manager	8.0.0.0.931077
Avaya Aura® Application Enablement Services	8.0.0.0.6-0
Avaya Aura® Media Server	8.0.0.150
Avaya Aura® Experience Portal	7.2.1.0.0605
Avaya G450 Media Gateway	40.10.1
Avaya 9641GS H323 IP Deskphone	6.6.6
Avaya 9621G SIP IP Deskphone	7.1.29
INI SureConnect™	6.3.24
Avaya TSAPI Client and SDK	7.1.3.20

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager via the System Access Terminal (SAT). The procedures include the following areas:

- Administer System Parameters Features.
- Administer Hunt Groups for Agents.
- Administer Agent IDs for Agents.
- Administer Call Vectoring.
- Administer AES Connectivity.
- Administer SIP Trunks
- Administer AAR Table
- Administer AES Connectivity

5.1. Administer System Parameters Features

Configure **System Parameter Features** that were configured during compliance test. On Page 5, enable **Create Universal Call ID** and provide a unique **UCID Network Node**.

change system-parameters features	Page 5 of 19
19	
FEATURE-RELATED SYSTEM PARAMETERS	
SYSTEM PRINTER PARAMETERS	
Endpoint:	Lines Per Page: 60
SYSTEM-WIDE PARAMETERS	
Switch Name:	
Emergency Extension Forwarding (min): 10	
Enable Inter-Gateway Alternate Routing? n	
Enable Dial Plan Transparency in Survivable Mode? n	
COR to Use for DPT: station	
EC500 Routing in Survivable Mode: dpt-then-ec500	
MALICIOUS CALL TRACE PARAMETERS	
Apply MCT Warning Tone? n MCT Voice Recorder Trunk Group:	
Delay Sending RElease (seconds): 0	
SEND ALL CALLS OPTIONS	
Send All Calls Applies to: station Auto Inspect on Send All Calls? n	
Preserve previous AUX Work button states after deactivation? n	
UNIVERSAL CALL ID	
Create Universal Call ID (UCID)? y UCID Network Node ID: 1	

On Page 13, enable **Copy ASAI UII During Conference/Transfer** and **Send UCID to ASAI**.

change system-parameters features	Page 13 of 19
FEATURE-RELATED SYSTEM PARAMETERS	
CALL CENTER MISCELLANEOUS	
Callr-info Display Timer (sec): 10	
Clear Callr-info: next-call	
Allow Ringer-off with Auto-Answer? n	
Reporting for PC Non-Predictive Calls? n	
Agent/Caller Disconnect Tones? n	
Interruptible Aux Notification Timer (sec): 3	
Zip Tone Burst for Callmaster Endpoints: double	
ASAI	
Copy ASAI UII During Conference/Transfer? y	
Call Classification After Answer Supervision? n	
Send UCID to ASAI? y	
For ASAI Send DTMF Tone to Call Originator? y	
Send Connect Event to ASAI For Announcement Answer? n	
Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n	

5.2. Administer Hunt Groups

This section provides the Hunt Group configuration for the call center agents. Agents will log into Hunt Group 1 configured below. Provide a descriptive name and set the **Group Extension** field to a valid extension. Enable the **ACD**, **Queue**, and **Vector** options. This hunt group will be specified in the **Agent LoginIDs** configured in **Section 5.3**.

add hunt-group 1	Page 1 of 4
HUNT GROUP	
Group Number: 1	ACD? y
Group Name: Skill 1	Queue? y
Group Extension: 59001	Vector? y
Group Type: ucd-mia	
TN: 1	
COR: 1	MM Early Answer? n
Security Code:	Local Agent Preference? n
ISDN/SIP Caller Display:	
Queue Limit: unlimited	
Calls Warning Threshold:	Port:
Time Warning Threshold:	Port:
SIP URI:	

On Page 2 of the Hunt Group form, enable the **Skill** option.

add hunt-group 1	Page 2 of 4
HUNT GROUP	
Skill? y	Expected Call Handling Time (sec): 10
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): 20	After Xfer or Held Call Drops? n

5.3. Administer Agent IDs

This section provides the Agent Login IDs for the agents. Add an **Agent Login ID** for each agent in the call center as shown below. In this configuration, agent login IDs 55001, 55002 and 55003 were created for three call center agents.

add agent-loginID 55001		Page 1 of 2
AGENT LOGINID		
Login ID: 55001		AAS? n
Name: CC 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: station		
AUX Agent Remains in LOA Queue: system		MIA Across Skills: system
AUX Agent Considered Idle (MIA): system		ACW Agent Considered Idle: system
Work Mode on Login: system		Aux Work Reason Code Type: system
		Logout Reason Code Type: system
Maximum time agent in ACW before logout (sec): system		
Forced Agent Logout Time: :		
WARNING: Agent must log in again before changes take effect		

On Page 2 of the **Agent LoginID** form, set the skill number (**SN**) to hunt group 1, which is the hunt group (skill) that the agents will log into.

add agent-loginID 55001		Page 2 of 2
AGENT LOGINID		
Direct Agent Skill:		Service Objective? n
Call Handling Preference: skill-level		Local Call Preference? n
SN	RL SL	SN RL SL
1: 1	1	16:
2:		17:
3:		18:
4:		19:
5:		20:
6:		
7:		
8:		
9:		
10:		
11:		
12:		
13:		
14:		
15:		

5.4. Administer Call Vectoring

This section describes the procedures for configuring call vectoring for calls queued to agents and inbound calls to SureConnect. There were three VDNs created during the compliance test:

- 22211: Inbound calls and routing to Experience Portal and offered call backs for caller first
- 22212: Inbound calls and routing to Experience Portal and offered call backs for agent first
- 22213: Outbound calls for caller first
- 22214: Outbound calls for agent first

These four VDNs were configured with vectors 111, 112, 113 and 114, respectively.

Screen captures below show the VDN configuration:

add vdn 22211	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 22211	
Name*: SC CF Test Inbound	
Destination: Vector Number 111	
Attendant Vectoring? n	
Meet-me Conferencing? n	
Allow VDN Override? n	
COR: 1	
TN*: 1	
Measured: none Report Adjunct Calls as	
ACD*? n	
VDN of Origin Annc. Extension*:	
1st Skill*:	
2nd Skill*:	
3rd Skill*:	
SIP URI:	
* Follows VDN Override Rules	

```
add vdn 22212                                     Page 1 of 3
                                         VECTOR DIRECTORY NUMBER

      Extension: 22212
      Name*: SC AF Test Inbound
      Destination: Vector Number 112
      Attendant Vectoring? n
      Meet-me Conferencing? n
      Allow VDN Override? n
      COR: 1
      TN*: 1
      Measured: none      Report Adjunct Calls as
ACD*? n

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

SIP URI:

* Follows VDN Override Rules
```

```
add vdn 22213                                     Page 1 of 3
                                         VECTOR DIRECTORY NUMBER

      Extension: 22213
      Name*: SC CF Test Outbound
      Destination: Vector Number 113
      Attendant Vectoring? n
      Meet-me Conferencing? n
      Allow VDN Override? n
      COR: 1
      TN*: 1
      Measured: none      Report Adjunct Calls as
ACD*? n

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

SIP URI:

* Follows VDN Override Rules
```

```

add vdn 22214
                                                    Page 1 of 3
                                VECTOR DIRECTORY NUMBER

                                Extension: 22214
                                Name*: SC AF Test Outbound
                                Destination: Vector Number 114
                                Attendant Vectoring? n
                                Meet-me Conferencing? n
                                Allow VDN Override? n
                                COR: 1
                                TN*: 1
                                Measured: none      Report Adjunct Calls as
ACD*? n

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

SIP URI:

* Follows VDN Override Rules

```

Screen captures below show the Vector configuration:

```

change vector 111
                                                    Page 1 of 6
                                CALL VECTOR

                                Number: 111      Name: SC CF Test Inbound
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 goto step      6      if expected-wait      for call      > 60
04 wait-time      60      secs hearing ringback
05 goto step      4      if unconditionally
06 converse-on      skill 99      pri m passing 333      and wait
07 collect      1      digits after announcement none      for none
08 goto step      11      if digits      =      1
09 goto step      12      if digits      =      2
10 goto step      4      if unconditionally
11 disconnect      after announcement 57771
12 disconnect      after announcement 57772
13 stop
14

```

change vector 112	CALL VECTOR					Page 1 of 6
Number: 112	Name: SC AF Test Inbound					
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 goto step	6	if expected-wait			for call	> 60
04 wait-time	60	secs hearing ringback				
05 goto step	4	if unconditionally				
06 converse-on	skill 99	pri m	passing 333	and wait		
07 collect	1	digits after announcement		none	for none	
08 goto step	11	if digits		=	1	
09 goto step	12	if digits		=	2	
10 goto step	4	if unconditionally				
11 disconnect	after announcement 57771					
12 disconnect	after announcement 57772					

change vector 113				Page 1 of 6	
CALL VECTOR					
Number: 113		Name: SC CF Test Outbound			
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 h			
03 wait-time	30	secs hearing ringback			
04 goto step	3	if unconditionally			
05 stop					

change vector 114					Page 1 of 6				
CALL VECTOR									
Number: 114		Name: SC AF Test Outbound							
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 1		pri h						
02 stop									

5.5. Administer H.323 Channels to Experience Portal

During the compliance test, calls from Communication Manager to Experience Portal were routed via H.323 Channels. These H.323 channels are combinations of hunt group / stations / agents configured on Communication Manager.

5.5.1. Administer Hunt Group

This section provides the Hunt Group configuration for the H.323 channels needed for Communication Manager to communicate with Experience Portal. Virtual Agents will auto log into Hunt Group 75 configured below. Provide a descriptive name and set the **Group Extension** field to a valid extension. Enable the **ACD**, **Queue** and **Vector** options. This hunt group will be specified in the **Agent LoginIDs** configured in **Section 5.5.2**. Calls are routed to Experience Portal, by the use of this hunt group, as per the vector configuration in **Section 5.4**.

add hunt-group 99		Page 1 of 4
HUNT GROUP		
Group Number: 99	ACD? y	
Group Name: AAEP Hunt Group	Queue? y	
Group Extension: 29999	Vector? y	
Group Type: ucd-mia		
TN: 1		
COR: 1	MM Early Answer? n	
Security Code:	Local Agent Preference? n	
ISDN/SIP Caller Display:		
Queue Limit: unlimited		
Calls Warning Threshold:	Port:	
Time Warning Threshold:	Port:	

One Page 2, enable **Skill** and **AAS**.

add hunt-group 99		Page 2 of 4
HUNT GROUP		
Skill? y	Expected Call Handling Time (sec): 180	
AAS? y		
Measured: none		
Supervisor Extension:		
Controlling Adjunct: none		
Multiple Call Handling: none		
Timed ACW Interval (sec):	After Xfer or Held Call Drops? n	

5.5.2. Administer Stations

This section provides the Stations that will be configured in Experience Portal as H.323 channels. Add a **Station** extension for each H.323 channel that will be configured on Experience Portal. During the compliance test, 5 stations, 54441 – 54445, were configured. Set the **Type** to **7434ND**, set a **Security Code** and enable **IP SoftPhone**. Note that the Security Code must be exactly same for all the stations configured for Experience Portal connectivity.

add station 54441		Page 1 of 6
STATION		
Extension: 54441	Lock Messages? n	BCC: 0
Type: 7434ND	Security Code: *	TN: 1
Port: S00008	Coverage Path 1:	COR: 1
Name: AAEP Station 1	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
	Time of Day Lock Table:	
Loss Group: 2	Personalized Ringing Pattern: 1	
Data Module? n	Message Lamp Ext: 54441	
Display Module? y		
Display Language: english	Coverage Module? n	
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	Remote Office Phone? n	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	

5.5.3. Administer Agent IDs

This section provides the Agent Login IDs for each configured Station above. Add an **Agent Login ID** for each agent used by Experience Portal stations. In this configuration, agent login IDs 54451 – 54452 were created. Enable **AAS**, set **Auto Answer** to **none**, and set the **Port Extension** to each corresponding station extensions configured above (54441 – 54445).

add agent-loginID 54451		Page 1 of 2
AGENT LOGINID		
Login ID: 54451		AAS? y
Name: AAEP 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:	
Port Extension: 54441	LoginID for ISDN/SIP Display? n	
Auto Answer: station		
AUX Agent Remains in LOA Queue: system		MIA Across Skills: system
AUX Agent Considered Idle (MIA): system		ACW Agent Considered Idle: system
Work Mode on Login: system		Aux Work Reason Code Type: system
		Logout Reason Code Type: system
Maximum time agent in ACW before logout (sec): system		
		Forced Agent Logout Time: :
WARNING: Agent must log in again before changes take effect		

One Page 2, configure the **SN** to the skill configured in **Section 5.5.1**.

add agent-loginID 54451		Page 2 of 2
AGENT LOGINID		
Direct Agent Skill:		Service Objective? n
Call Handling Preference: skill-level		Local Call Preference? n
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:

5.6. Administer SIP Trunks

Outbound calls from Experience Portal to customer routed via Session Manager and Communication Manager to customers and agents using SIP trunks.

For the SIP trunk between Communication Manager and Session Manager, on Page 3, set **UI Treatment** to **Shared** and **Send UCID** to **y**.

change trunk-group 2	Page 3 of 22
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Suppress # Outpulsing? n Numbering Format: private	
	UI Treatment: shared
	Maximum Size of UI Contents: 128
	Replace Restricted Numbers? n
	Replace Unavailable Numbers? n
	Hold/Unhold Notifications? y
	Modify Tandem Calling Number: no
Send UCID? y	
Show ANSWERED BY on Display? y	

5.7. Administer AES Connectivity

Configuration for AES and CTI link used during compliance test is standard in nature and is outside of scope for this document. For more information, please refer to documentation in **Section 11**.

6. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring AES. Switch connection and TSAPI configuration for connectivity to Communication Manager was preconfigured and standard in nature; thus, not mentioned in this document.

SureConnect server connected to AES via TSAPI to monitor hunt group configured on Communication Manager. This includes:

- Administer User
- Obtain Tlink

Access the AES OAM web interface by using the URL “https://ip-address” in a web browser, where “ip-address” is the IP address of AES. Log on using appropriate credentials.



Application Enablement Services Management Console

[Help](#)

Please login here:

Username

Copyright © 2009-2016 Avaya Inc. All Rights Reserved.

6.1. Administer User

Once logged on, navigate to **User Management → User Admin → Add User**. Screen capture below depicts the user configured during the compliance test. Note that **CT User** is set to **Yes**.

The screenshot shows the 'Add User' form within the 'User Management' section. The left sidebar lists various system components, with 'User Management' expanded to show 'User Admin' and 'Add User'. The form fields are as follows:

- * User Id: sureconnect
- * Common Name: sureconnect
- * Surname: sureconnect
- * User Password: [masked]
- * Confirm Password: [masked]
- Admin Note: [empty]
- Avaya Role: None (dropdown)
- Business Category: [empty]
- Car License: [empty]
- CM Home: [empty]
- Css Home: [empty]
- CT User: Yes (dropdown)
- Department Number: [empty]

Fields marked with * are required.

Navigate to **Security → Security Database → CTI Users → List All Users**, and edit the user added above; check box for **Unrestricted Access**.

The screenshot shows the 'Edit CTI User' form within the 'Security Database' section. The left sidebar lists various system components, with 'Security' expanded to show 'Security Database'. The form displays the user profile and various control settings:

Edit CTI User		
User Profile:		
User ID	sureconnect	
Common Name	sureconnect	
Worktop Name	NONE (dropdown)	
Unrestricted Access	<input checked="" type="checkbox"/>	
Call and Device Control:		
Call Origination/Termination and Device Status	None (dropdown)	
Call and Device Monitoring:		
Device Monitoring	None (dropdown)	
Calls On A Device Monitoring	None (dropdown)	
Call Monitoring	<input type="checkbox"/>	
Routing Control:		
Allow Routing on Listed Devices	None (dropdown)	
<input type="button" value="Apply Changes"/> <input type="button" value="Cancel Changes"/>		

6.2. Obtain Tlink

Obtain the Tlink that will be used by iAssist Admin server to connect to AES. Navigate to **Security → Security Database → Tlinks** and note the Tlink to be used by SureConnect.

The screenshot shows the iAssist Admin web interface. At the top, a red navigation bar contains the text "Security | Security Database | Tlinks" on the left and "Home | Help | Logout" on the right. On the left side, there is a dark grey sidebar menu with the following items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", and "Networking". The "Security" item is partially visible at the bottom. The main content area is titled "Tlinks" and contains a "Tlink Name" section with two radio button options: "AVAYA#CM8#CSTA#AES8" (which is selected) and "AVAYA#CM8#CSTA-S#AES8". Below these options is a "Delete Tlink" button.

7. Configure Avaya Aura® Experience Portal

Experience Portal is configured via the Experience Portal Manager (EPM) web interface, to access the web interface, enter http:// “ip-address”/ as the URL in a web browser, where “ip-address” is the IP address of Experience Portal. Log in using the appropriate credentials.



Note: Some of the screens in this section are shown after the Experience Portal had been configured. Don't forget to save the screen parameters as you configure Experience Portal.

7.1. Configure SureConnect Applications

Three applications were configured on Experience Portal:

- Inbound application to schedule callback for both agent first and customer first options
- Outbound application to call customer for customer first option
- Outbound application to call agent for agent first option

In the **Applications** page, add SureConnect applications as shown in the sections below.

7.1.1. Inbound Application

- **Type:** Configure as **VoiceXML**
- **VoiceXML URL:** Configure the URL provided by SureConnect
- **Application Launch:** Configure as **Inbound** and add the inbound VDNs configured in Communication Manager as per **Section 5.4**.

The screenshot shows the configuration page for an application named 'CollectCallbackRequest' in the Avaya Aura Experience Portal 7.2.1. The page is divided into a left sidebar with navigation links and a main configuration area. The main area is titled 'Use this page to change the configuration of an application.' and contains several sections: 'Name' (CollectCallbackRequest), 'Enable' (Yes), 'Type' (VoiceXML), 'Reserved SIP Calls' (None), 'Requested' (empty), 'URI' (Single), 'VoiceXML URL' (https://10.64.110.158:8844/CollectCallbackRequest/Start), 'Mutual Certificate Authentication' (No), 'Basic Authentication' (No), 'Speech Servers' (ASR: No ASR, TTS: No TTS), 'Application Launch' (Inbound), 'Called Number' (22212, 22211), and 'Advanced Parameters' (Support Remote DTMF Processing: No, DTMF Type Ahead Enabled: Yes, Converse-On: Yes, Network Media Service: No). Red boxes highlight the 'VoiceXML URL', 'Inbound' option, 'Called Number' list, and 'Converse-On' option.

Avaya Aura® Experience Portal 7.2.1 (ExperiencePortal)

Expand All | Collapse All

Use this page to change the configuration of an application.

Name: CollectCallbackRequest

Enable: ☒ Yes ☐ No

Type: VoiceXML

Reserved SIP Calls: ☒ None ☐ Minimum ☐ Maximum

Requested:

URI

☒ Single ☐ Fail Over ☐ Load Balance

VoiceXML URL: https://10.64.110.158:8844/CollectCallbackRequest/Start **Verify**

Mutual Certificate Authentication: ☐ Yes ☒ No

Basic Authentication: ☐ Yes ☒ No

Speech Servers

ASR: No ASR

TTS: No TTS

Application Launch

☒ Inbound ☐ Inbound Default ☐ Outbound

☒ Number ☐ Number Range ☐ URI

Called Number: **Add**

22212
22211 **Remove**

Advanced Parameters

Support Remote DTMF Processing: ☐ Yes ☒ No

DTMF Type Ahead Enabled: ☒ Yes ☐ No

Converse-On: ☒ Yes ☐ No

Network Media Service: ☐ Yes ☒ No

7.1.2. Outbound Application for Caller First Option

- **Type:** Configure as **VoiceXML**
- **VoiceXML URL:** Configure the URL provided by SureConnect
- **Application Launch:** Configure as **Outbound**

Avaya Aura® Experience Portal 7.2.1 (ExperiencePortal) [Home](#) [Help](#) [Logoff](#)

Expand All | Collapse All

- ▼ **User Management**
 - Roles
 - Users
 - Login Options
- ▼ **Real-time Monitoring**
 - System Monitor
 - Active Calls
 - Port Distribution
- ▼ **System Maintenance**
 - Audit Log Viewer
 - Trace Viewer
 - Log Viewer
 - Alarm Manager
- ▼ **System Management**
 - EPM Manager
 - MPP Manager
 - Software Upgrade
 - System Backup
- ▼ **System Configuration**
 - Applications
 - EPM Servers
 - MPP Servers
 - SNMP
 - Speech Servers
 - VoIP Connections
 - Zones
- ▼ **Security**
 - Certificates
 - Licensing
- ▼ **Reports**
 - Standard
 - Custom
 - Scheduled
- ▼ **Multi-Media Configuration**
 - Email
 - HTML
 - SMS

You are here: [Home](#) > [System Configuration](#) > [Applications](#) > [Change Application](#)

Change Application

Use this page to change the configuration of an application.

Name: CallerFirst

Enable: ☒ Yes ☐ No

Type:

Reserved SIP Calls: ☒ None ☐ Minimum ☐ Maximum

Requested:

URI

☒ Single ☐ Fail Over ☐ Load Balance

VoiceXML URL: [Verify](#)

Mutual Certificate Authentication: ☐ Yes ☒ No

Basic Authentication: ☐ Yes ☒ No

Speech Servers

ASR:

TTS:

Application Launch

☐ Inbound ☐ Inbound Default ☒ Outbound

7.1.3. Outbound Application for Agent First Option

- **Type:** Configure as **CCXML**
- **CCXML URL:** Configure the URL provided by SureConnect
- **Application Launch:** Configure as **Outbound**

Avaya Aura® Experience Portal 7.2.1 (ExperiencePortal) Home ? Help Logoff

Expand All Collapse All

You are here: [Home](#) > [System Configuration](#) > [Applications](#) > Change Application

Change Application

Use this page to change the configuration of an application.

Name: AgentFirstDialer

Enable: ☒ Yes ☐ No

Type:

Reserved SIP Calls: ☒ None ☐ Minimum ☐ Maximum

Requested:

URI

☒ Single ☐ Fail Over ☐ Load Balance

CCXML URL:

Mutual Certificate Authentication: ☐ Yes ☒ No

Basic Authentication: ☐ Yes ☒ No

Speech Servers

ASR:

TTS:

Application Launch

☐ Inbound ☐ Inbound Default ☒ Outbound

7.2. Configure VoIP Connections

Inbound calls to Experience Portal from Communication Manager used H.323 connection. To add a new H.323 connection, select **VoIP** on the left pane and select the **H.323** tab. Select **Add** to add a new H.323 connection. Screen capture below shows the H.323 connection created during the compliance test. Note the configured station in **Section 5.5.2** were added **Inbound Only** stations.

Avaya Aura® Experience Portal 7.2.1 (ExperiencePortal)

Expand All | Collapse All

Home Help Logout

You are here: Home > System Configuration > VoIP Connections > Change H.323 Connection

Change H.323 Connection

Use this page to change the configuration of an H.323 connection.

Name: ACM8

Enable: ☒ Yes ☐ No

Gatekeeper Address: 10.64.110.131

Alternative Gatekeeper Address:

Gatekeeper Port: 1719

Media Encryption: ☐ Yes ☒ No

New Stations

Station	From	To	Password	Station Type
	54441	54445	*****	<input checked="" type="radio"/> Same Password <input type="radio"/> Use sequential passwords

Station Type: Inbound and Outbound
Inbound Only
Maintenance

Add

Configured Stations (M for Maintenance, I for Inbound Only)

54441 - 54445 I

Remove

Similarly, select **SIP** tab and select **Add** too add a SIP connection for outbound calls to Session Manager. Note that only Outbound calls were allowed for this SIP connection.

Avaya Aura® Experience Portal 7.2.1 (ExperiencePortal) Home Help Logoff

Expand All Collapse All

User Management
Roles
Users
Login Options

Real-time Monitoring
System Monitor
Active Calls
Port Distribution

System Maintenance
Audit Log Viewer
Trace Viewer
Log Viewer
Alarm Manager

System Management
EPM Manager
MPP Manager
Software Upgrade
System Backup

System Configuration
Applications
EPM Servers
MPP Servers
SNMP
Speech Servers
VoIP Connections
Zones

Security
Certificates
Licensing

Reports
Standard
Custom
Scheduled

Multi-Media Configuration
Email
HTML
SMS

You are here: [Home](#) > [System Configuration](#) > [VoIP Connections](#) > [Change SIP Connection](#)

Change SIP Connection

Use this page to change the configuration of a SIP connection.

Name: ASM8

Enable: ☒ Yes ☐ No

Proxy Transport: TCP

☒ Proxy Servers ☐ DNS SRV Domain

Address	Port	Priority	Weight	
10.64.110.135	5060	0	0	Remove

Additional Proxy Server

Listener Port: 5060

SIP Domain: avaya.com

P-Asserted-Identity:

Maximum Redirection Attempts: 0

Consultative Transfer: ☒ INVITE with REPLACES ☐ REFER

SIP Reject Response Code: ☒ ASM (503) ☐ SES (480) ☐ Custom 503

SIP Timers

T1: 250 milliseconds

T2: 2000 milliseconds

B and F: 4000 milliseconds

Call Capacity

Maximum Simultaneous Calls: 25

☐ All Calls can be either inbound or outbound

☒ Configure number of inbound and outbound calls allowed

Inbound Calls Allowed: 0

Outbound Calls Allowed: 25

7.3. Configure SureConnect User

On the left pane select **User** and select **Add** to add a new user for SureConnect. Following user was created with **Web Services** access.

Avaya Aura® Experience Portal 7.2.1 (ExperiencePortal) Home Help Logoff

Expand All Collapse All

User Management
Roles
Users
Login Options

Real-time Monitoring
System Monitor
Active Calls
Port Distribution

System Maintenance
Audit Log Viewer
Trace Viewer
Log Viewer
Alarm Manager

System Management
EPM Manager
MPP Manager
Software Upgrade
System Backup

System Configuration
Applications
EPM Servers
MPP Servers
SNMP
Speech Servers
VoIP Connections

You are here: [Home](#) > [User Management](#) > [Users](#) > [Change User](#)

Change User

Use this page to modify a EPM user account. You can change the user role and password.

Name: sureconnect

Enable: ☒ Yes ☐ No

☐ Administration ☐ Auditor ☐ Maintenance

☐ Operations ☐ Privacy Manager ☐ Reporting

☐ User Manager ☒ Web Services

Created: 10/3/18 1:03 PM

Password:

Verify Password:

Enforce Password Longevity: ☐

7.4. Import Application Server Certificate

For SureConnect applications to securely connect to Experience Portal via HTTPS, the root certificate of certificate authority needs to be added to the application server. During the compliance test, System Manager was used as the certificate authority. As such, the root certificate of System Manager was obtained and installed on the application server.

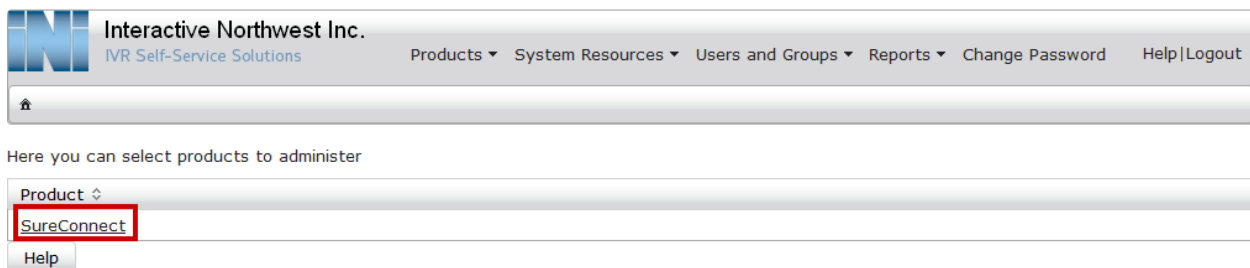
8. Configure INI SureConnect™

Configuration for SureConnect is performed via SureConnect web portal. Log onto the SureConnect web portal using appropriate credentials.



The screenshot shows the login page for Interactive Northwest Inc. (INI) SureConnect. The page has a grey background. In the top left corner, there is the INI logo and the text "Interactive Northwest Inc. IVR Self-Service Solutions". In the center, there is a white box with a light blue border containing the login form. The form has the title "Enter your Username and Password". It includes two input fields: "Username:" and "Password:". Below the password field, there is a checkbox labeled "Warn me before logging me into other sites." and a "LOGIN" button next to a "clear" link. At the bottom of the page, there is a copyright notice: "Copyright © 2012-2016 Interactive Northwest, Inc. All rights reserved."

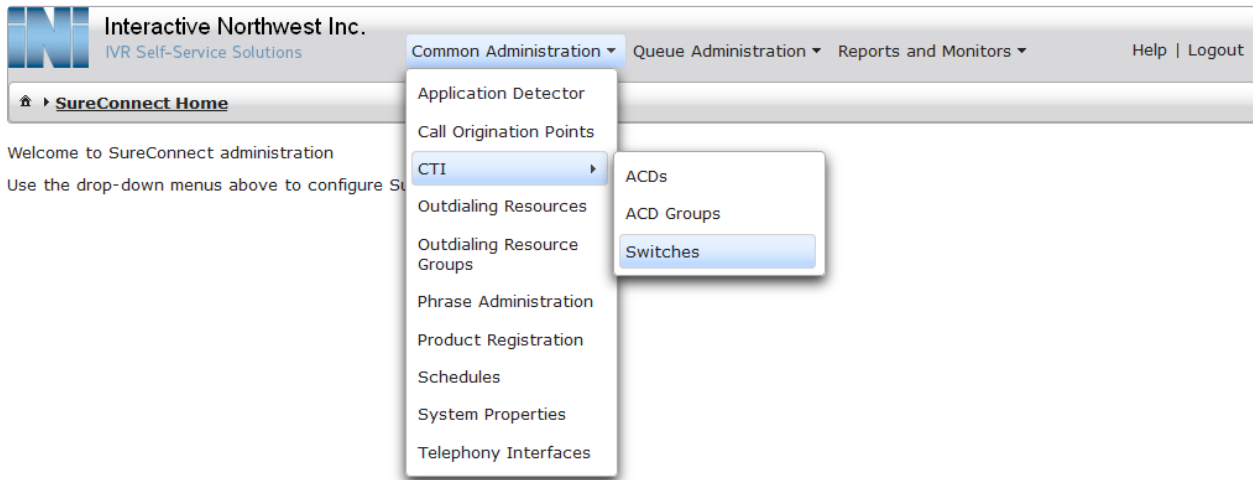
Once logged in select **SureConnect** to start the configuration.



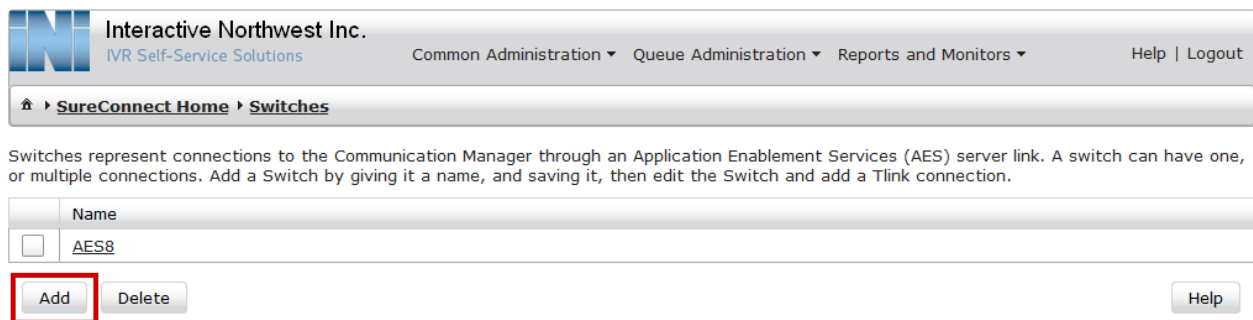
The screenshot shows the dashboard of the INI SureConnect web portal. At the top, there is a header bar with the INI logo and the text "Interactive Northwest Inc. IVR Self-Service Solutions". To the right of the header, there are several navigation links: "Products", "System Resources", "Users and Groups", "Reports", "Change Password", and "Help | Logout". Below the header, there is a section titled "Here you can select products to administer". This section contains a dropdown menu labeled "Product" with a small upward and downward arrow. The dropdown menu is open, showing a list of products. The product "SureConnect" is highlighted with a red rectangular box. Below the dropdown menu, there is a "Help" button.

8.1. Configure Switches

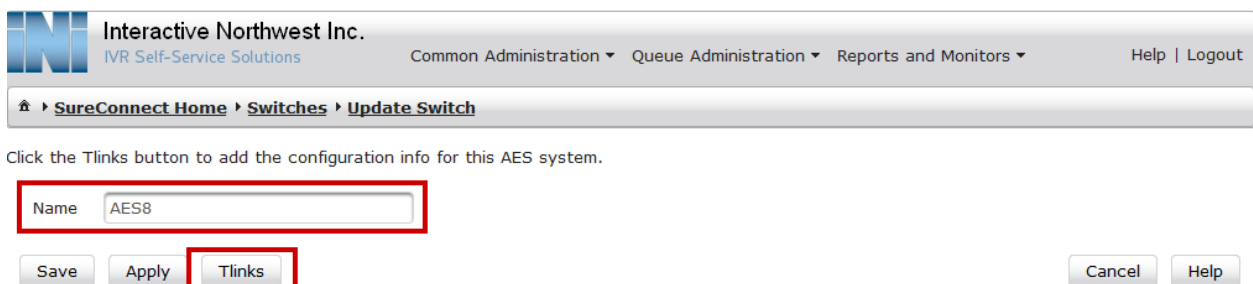
To configure AES connectivity, navigate to **Common Administration** → **CTI** → **Switches**.



Select **Add** to create a new connection.



Type in a name for the connection and select **Tlinks**.



Select **Add** to add a Tlink (not shown). Configure the details as per **Section 6**. Once done, select **Save**.

The screenshot shows the 'Update Tlink Configuration' page in the Interactive Northwest Inc. SureConnect application. The breadcrumb trail is: SureConnect Home > Switches > Update Switch (AES8) > Tlink Configurations > Update Tlink Configuration. The page instructs the user to 'Use this page to change the Tlink configuration.' A red box highlights the input fields: Name (CM8), Service (AVAYA#CM8#CSTA#AES8), Username (sureconnect), Password (masked with dots), and Peer (empty). Below the fields, the 'Save' button is highlighted with a red box, along with 'Apply', 'Cancel', and 'Help' buttons.

8.2. Administer ACD

The hunt group configured in **Section 5.2** will be used by SureConnect to monitor agent related activities via TSAPI. Navigate to **Common Administration → CTI → ACDs** and select **Add** to add a new ACD (not shown). Configure the hunt group from **Section 5.2** in **Number** field and select the **Switch** configured in previous section. Select **Save** once done.

The screenshot shows the 'Update ACD' page in the Interactive Northwest Inc. SureConnect application. The breadcrumb trail is: SureConnect Home > ACDs > Update ACD. The page instructs the user to 'Use this page to change the ACD configuration.' A red box highlights the input fields: Name (Test Skill 1), Number (59001), and Switch (AES8). Below the fields, the 'Save' button is highlighted with a red box, along with 'Apply', 'Cancel', and 'Help' buttons.

8.3. Administer ACD Group

To create a new ACD group for the ACD created in previous section, navigate to **Common Administration → CTI → ACD Groups** and select **Add** (not shown). Select the **Switch** from **Section 8.1**. Select the **ACD** configured in previous section and select the right arrow to add it to the group. Select **Save** once done.

Interactive Northwest Inc.
IVR Self-Service Solutions

Common Administration ▾ Queue Administration ▾ Reports and Monitors ▾ Help | Logout

🏠 ▶ [SureConnect Home](#) ▶ [ACD Groups](#) ▶ [Update ACD Group](#)

Use this page to change the ACD group configuration.

Name

Switch

Available ACDs:

Test Skill 1 (59001)

Assigned ACDs:

ACDs

→

→+

←

←+

8.4. Administer Call Origination Points

VDNs configured for inbound calls in Communication Manager need to be added as origination points. Two originating points for inbound VDNs from **Section 5.4** need to be added. To a new originating point, navigate to **Common Administration → Call Originating Points** and select **Add** (not shown). Type in VDN as **DNIS** and select **Add**. Select **Save** once done.

Interactive Northwest Inc.
IVR Self-Service Solutions

Common Administration ▾ Queue Administration ▾ Reports and Monitors ▾ Help | Logout

🏠 ▶ [SureConnect Home](#) ▶ [Call Origination Points](#) ▶ [Add Call Origination Point](#)

Use this page to add a new Call Origination Point.

Name

Originating Numbers

No records found.

During compliance test, 2 originating points were added.

Interactive Northwest Inc.
IVR Self-Service Solutions

Common Administration ▾ Queue Administration ▾ Reports and Monitors ▾ Help | Logout

🏠 ▶ [SureConnect Home](#) ▶ [Call Origination Points](#)

A Call Origination Point (COP) is a grouping of one or more VDNs, and is used to route calls from those VDNs into a specific callback queue. Each COP is used by only one callback queue. You must create a COP before you create its corresponding callback queue.

	Name	Originating Numbers
<input type="checkbox"/>	AF Test	22212
<input type="checkbox"/>	CF Test	22211

8.5. Administer Outdialing Resources

For outbound calls backs, SureConnect user the Application Web Interface provided by Experience Portal. To configure, navigate to **Common Administration → Outdialing Resources** and select **Add** (not shown). Configure the **Username** and **Password** as per **Section 7.3**. Type in the Web Services URL for Experience Portal in **Endpoint**. Select **Save** once done.

Interactive Northwest Inc.
IVR Self-Service Solutions

Common Administration ▾ Queue Administration ▾ Reports and Monitors ▾ [Help](#) | [Logout](#)

🏠 ▸ [SureConnect Home](#) ▸ [Outdialing Resources](#) ▸ [Update Outdialing Resource](#)

Use this page to change the outdialing resource configuration.

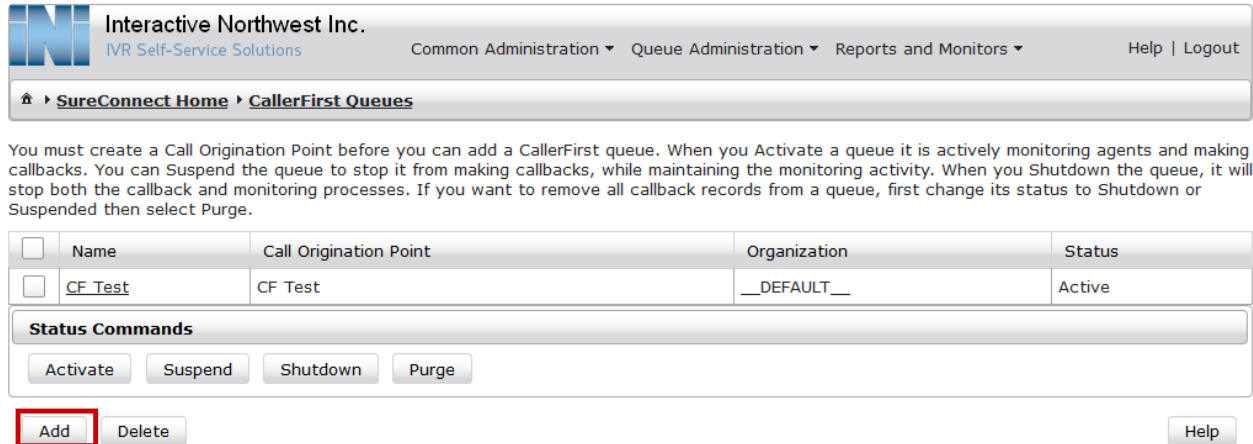
Name	<input type="text" value="EP72"/>
Username	<input type="text" value="sureconnect"/>
Password	<input type="password" value="••••••••"/>
Endpoint	<input type="text" value="https://10.64.110.50/axis2/services/VPAppIntfService"/>
Failover Endpoint	<input type="text" value="https://10.64.110.50/axis2/services/VPAppIntfService"/>

Administer Outdialing Resource Group

For the Outdialing Resource added in previous section, a group needs to be added. Depending on customer requirements parameters can vary. This section displays the configuration performed during the compliance test. Navigate to **Common Administration → Outdialing Resource Group** and select **Add** (not shown). Select the resource group added above and select the right arrow. Select **Save** once done.

8.6. Administer CallerFirst Queues

To configure the parameters for caller first option, navigate to **Queue Administration** → **CallerFirst Queues** and select **Add**.



Interactive Northwest Inc.
IVR Self-Service Solutions

Common Administration ▾ Queue Administration ▾ Reports and Monitors ▾ Help | Logout

🏠 ▶ [SureConnect Home](#) ▶ [CallerFirst Queues](#)

You must create a Call Origination Point before you can add a CallerFirst queue. When you Activate a queue it is actively monitoring agents and making callbacks. You can Suspend the queue to stop it from making callbacks, while maintaining the monitoring activity. When you Shutdown the queue, it will stop both the callback and monitoring processes. If you want to remove all callback records from a queue, first change its status to Shutdown or Suspended then select Purge.

<input type="checkbox"/>	Name	Call Origination Point	Organization	Status
<input type="checkbox"/>	CF Test	CF Test	__DEFAULT__	Active

Status Commands

Select the **Call Originating Point** created for caller first option in **Section 8.4**.

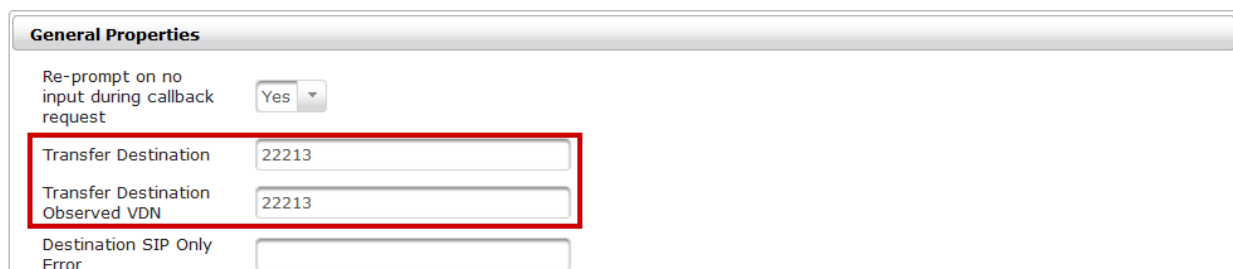
Use this page to change the CallerFirst Queue configuration.

Organization:

Name

Call Origination Point

Continuing from above, under the **General Properties** section, type in the outbound VDN configured for caller first option in **Section 5.4** for call first in **Transfer Destination** and **Transfer Destination Observed VDN**.



General Properties

Re-prompt on no input during callback request

Transfer Destination

Transfer Destination Observed VDN

Destination SIP Only Error

Continuing from above, under the **Data Collection** section, set **Offer ANI for Callback** to **Yes**.

Data Collection	
Collect DTMF Field 1?	No
Collect DTMF Field 2?	No
Offer ANI for Callback?	Yes

Continuing from above, under the **Telephone Properties** section:

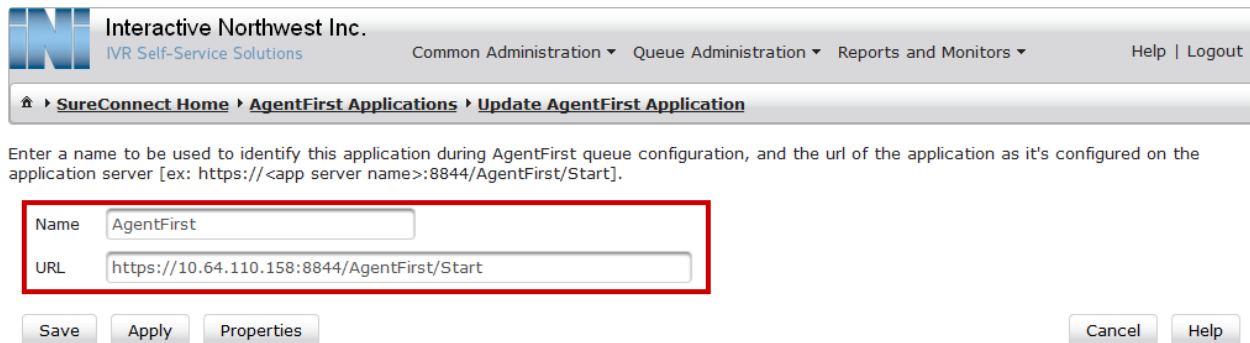
- Configure **ACD Group** as per the **Section 8.3**
- Set **Answering Machine Treatment** to **Reschedule**
- Type in an **ANI** that will be displayed the call is presented to the customer.
- Configure **Outdialing Resource Group** as per the **Section 8.6**

Select **Save** once done.

Telephony Properties	
ACD Group	Test Skill 1
Answering Machine Treatment	Reschedule
Call Classification Recorded Msg Timeout	1500
Call Classification Timeout	2000
CDR FAC	*70
Maximum Ring Time	59s
Detect Greeting End?	Yes
Enable Call Classification?	No
Outbound ANI	3035551212
Outdialing Resource Group	AAEP1
Retry Interval	70s
Telephony ID	TID1
Use CTI Transfer?	No

8.7. Administer AgentFirst Application

To configure AgentFirst Application, navigate to **Queue Administration → AgentFirst → AgentFirst Applications** and select **Add** (not shown). Type in the URL that will be used by Experience Portal for outbound callback requests.



Interactive Northwest Inc.
IVR Self-Service Solutions

Common Administration ▾ Queue Administration ▾ Reports and Monitors ▾ Help | Logout

🏠 ▶ SureConnect Home ▶ AgentFirst Applications ▶ Update AgentFirst Application

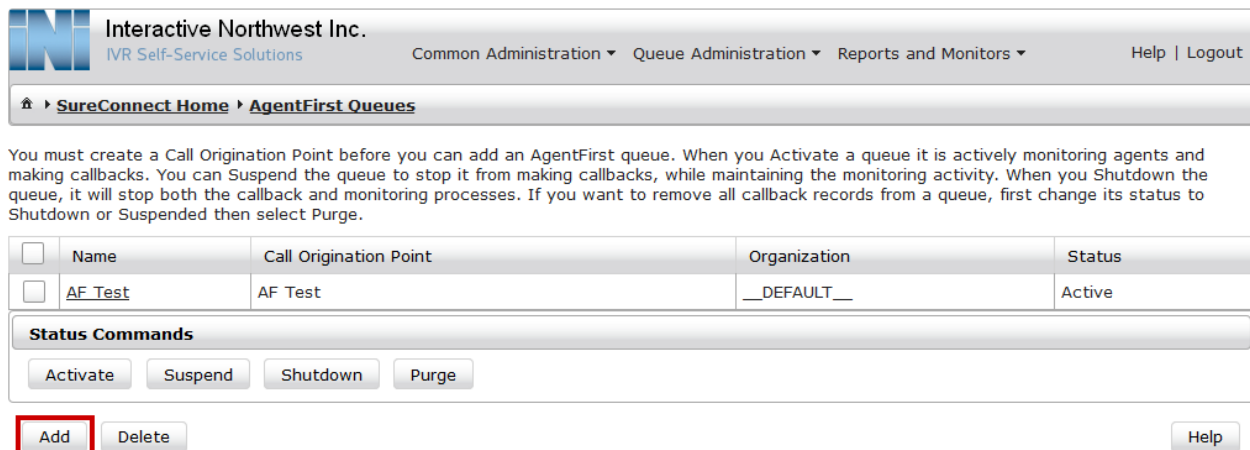
Enter a name to be used to identify this application during AgentFirst queue configuration, and the url of the application as it's configured on the application server [ex: https://<app server name>:8844/AgentFirst/Start].

Name

URL

8.8. Administer AgentFirst Queues

To configure the parameters for caller first option, navigate to **Queue Administration → Agent First → AgentFirst Queues** and select **Add**.



Interactive Northwest Inc.
IVR Self-Service Solutions

Common Administration ▾ Queue Administration ▾ Reports and Monitors ▾ Help | Logout

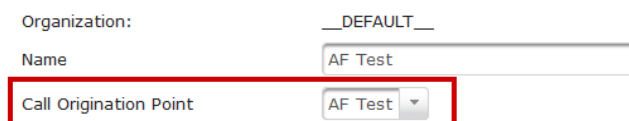
🏠 ▶ SureConnect Home ▶ AgentFirst Queues

You must create a Call Origination Point before you can add an AgentFirst queue. When you Activate a queue it is actively monitoring agents and making callbacks. You can Suspend the queue to stop it from making callbacks, while maintaining the monitoring activity. When you Shutdown the queue, it will stop both the callback and monitoring processes. If you want to remove all callback records from a queue, first change its status to Shutdown or Suspended then select Purge.

<input type="checkbox"/>	Name	Call Origination Point	Organization	Status
<input type="checkbox"/>	AF Test	AF Test	__DEFAULT__	Active

Status Commands

Select the **Call Originating Point** created for agent first option in **Section 8.4**.



Organization:

Name

Call Origination Point

Continuing from above, under the **General Properties** section, type in the outbound VDN configured for agent first option in **Section 5.4** for call first in **Transfer Destination** and **Transfer Destination Observed VDN**.

General Properties

Re-prompt on no input during callback request: Yes

Transfer Destination: 22214

Transfer Destination Observed VDN: 22214

Continuing from above, under the **Data Collection** section, set **Offer ANI for Callback** to **Yes**.

Data Collection

Agent ID Required?: No

Capture UUI via CTI: No

Collect DTMF Field 1?: No

Collect DTMF Field 2?: No

Offer ANI for Callback?: Yes

Voice Recording?: No

Continuing from above, under the **Application and Prompts** section, select the **AgentFirst Application** configured in previous section.

Applications and Prompts

Collect Callback Request Language: English - Female

Voice Enabled: No

AgentFirst Language: English - Female

AgentFirst Application: AgentFirst

Outbound Application: AgentFirstDialer

Continuing from above, under the **Telephone Properties** section:

- Configure **ACD Group** as per the **Section 8.3**
- Type in an **ANI** that will be displayed the call is presented to the customer.
- Configure **Outdialing Resource Group** as per the **Section 8.6**

Select **Save** once done.

Telephony Properties

ACD Group	Test Skill 1 ▼
CDR FAC	*70
Maximum Ring Time	3600s
Outbound ANI	3035551212
Outdialing Resource Group	AAEP1 ▼
Retry Interval	70s
Telephony ID	TID1 ▼

Save Apply Cancel Help

9. Verification Steps

This section provides the verification steps that may be performed to verify that Experience Portal can run iAssist SureConnect applications.

1. From the EPM web interface, verify that the EPM/MPP server is online and running in the **System Monitor** page shown below.

The screenshot shows the 'System Monitor' page in the Avaya Aura Experience Portal 7.2.1. The page title is 'System Monitor (Sep 28, 2018 8:41:51 AM PDT)'. It displays the current state of the local Experience Portal system and any remote systems configured. The page includes a navigation menu on the left with categories like User Management, Real-time Monitoring, System Maintenance, System Management, System Configuration, and Security. The main content area shows a 'Summary' tab selected, displaying a table of system status. The table has columns for Server Name, Type, Mode, State, Config, Call Capacity (Current, Licensed, Maximum), Active Calls (In, Out), Calls Today, and Alarms. The data row shows 'EPM / localMPP' in 'Online Running' state with 'OK' config, 5 current calls, 5 licensed calls, 10 maximum calls, 0 active calls in/out, 0 calls today, and 0 alarms. A 'Help' button is visible below the table.


Server Name	Type	Mode	State	Config	Call Capacity			Active Calls		Calls Today	Alarms
					Current	Licensed	Maximum	In	Out		
EPM / localMPP	EPM/MPP	Online	Running	OK	5	5	10	0	0	0	✓
Summary					5	5	10			0	✓

2. From the EPM web interface, verify that the ports on the MPP server are in-service in the **Port Distribution** page shown below.

The screenshot shows the 'Port Distribution Report' page in the Avaya Aura Experience Portal 7.2.1. The page title is 'Port Distribution Report (Oct 11, 2018 4:13:46 PM PDT)'. It displays information about how telephony resources have been distributed to the MPPs. The page includes a navigation menu on the left with categories like User Management, Real-time Monitoring, System Maintenance, System Management, System Configuration, and Security. The main content area shows a 'Port Distribution' tab selected, displaying a table of port distribution. The table has columns for Port, Mode, State, Port Group, Protocol, Current Allocation, and Base Allocation. The data row shows '10 Online' in 'In service ASM' state with 'SIP_Trunk' protocol and 'localMPP' current allocation. A 'Help' button is visible below the table.

Port	Mode	State	Port Group	Protocol	Current Allocation	Base Allocation
10	Online	In service ASM		SIP_Trunk	localMPP	

3. Via the SureConnect web portal, pending callback requests and completed callback request can be displayed by select **Reports and Monitor**. Screen capture below displays the completed callback request for call first application.



Interactive Northwest Inc.

IVR Self-Service Solutions

Common Administration ▾
Queue Administration ▾
Reports and Monitors ▾

[Help](#) | [Logout](#)

[SureConnect Home](#) ▸
[CallerFirst Activity Detail](#)

Time Period: 10/02/18 - 12/07/18

Queue Name	DNIS	Callback Number	Time Caller Left Request	Type of Callback	Call Status	Requested Callback Date/Time	Actual Callback Date/Time	Originating Channel	CB Request ID	Dial Request ID	Media Platform Session ID
CF Test 54441	8312369822	10/19/18 10:48 AM	Immediate	Complete	10/19/18 10:48 AM	10/19/18 12:16 PM	Voice	e425b831-6a0f-4907-98c3-9a70094e807c	6fd9d9d-cf90-43ec-9f97-1dec286c18fd	taaep-2018292181319-7	
CF Test 54442	8312369822	10/19/18 5:23 PM	Immediate	Complete	10/19/18 5:23 PM	10/19/18 5:23 PM	Voice	201dc26c-3de4-4e20-9ad8-c9d48a91a099	22436d5e-d542-4c76-b8f8-9e25579733da	taaep-2018292232039-10	
CF Test 54442	8312369822	10/24/18 2:50 PM	Immediate	Complete	10/24/18 2:50 PM	10/24/18 2:50 PM	Voice	b12cb01e-7be0-4427-a2e3-fa74fef1485e	4bec0c29-b859-4ed5-89d7-010268e7294a	taaep-2018297204725-15	
CF Test 54441	8312369822	10/24/18 3:12 PM	Immediate	Complete	10/24/18 3:12 PM	10/24/18 3:13 PM	Voice	a615dfa0-61fe-4a8d-b1c9-4aab6bfe3101	ef044035-ebc7-4ce8-ad30-e71d996c885e	taaep-2018297210932-18	
CF Test 22211	8312369822	10/29/18 3:00 PM	Immediate	Complete	10/29/18 3:00 PM	10/29/18 3:00 PM	Voice	6eafffe8-b861-444c-9dc4-fa3303a6d6d4	aa0b5533-4fb2-45ac-aede-48c496236ece	taaep-2018302210014-17	

10. Conclusion

These Application Notes describe the configuration steps required to integrate the INI SureConnect by Interactive Northwest, Inc with Avaya Aura® Application Enablement Services and Avaya Aura® Experience Portal. All feature and serviceability test cases were completed successfully refer to **Section 2.2** for details.

11. Additional References

This section references the Avaya documentation relevant to these Application Notes. The following Avaya product documentation is available at <http://support.avaya.com>.

- [1] Administering Avaya Aura® Communication Manager, Release 8.0, Issue 7, August 2018
- [2] Administering and Maintaining Avaya Aura® Application Enablement Services, Release 8.0, Issue 1, August 2018
- [3] Administering Avaya Aura® Experience Portal, Release 7.2.1, Issue 1, March 2018

Product Documentation for INI SureConnect can be obtained directly from Interactive Northwest, Inc.

©2019 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.