



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Acqueon iAssist Call Back Manager 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 the Acqueon iAssist Call Back Manager with Avaya Aura® Application Enablement Service and Avaya Aura® Experience Portal. The iAssist Call Back Manager offers callers queued to a call center the option to continue to wait in queue for an agent or request a call back when either an agent becomes available or schedule a call back for a specified date and time.

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 the Acqueon iAssist Call Back Manager (CBM) with Avaya Aura® Application Enablement Service (AES) and Avaya Aura® Experience Portal (Experience Portal). CBM offers callers queued to a call center the option to continue to wait in queue for an agent or request a call back when either an agent becomes available or schedule a call back for a specified date and time.

CBM integrates with Experience Portal via VoiceXML and CCXML applications to offer call backs requests to callers and place calls to those callers who requested callbacks. iAssist (RapCTI module) integrates with AES via TSAPI interface to monitor the H.323 ports configured for Experience Portal.

CBM consists of two modules: an Inbound module and an Outbound module; both of these modules are installed on iAssist Admin server. The Inbound module is designed to take a call back request from a caller waiting to be serviced by an agent. The Outbound module retrieves the call back request based on priority and time of the callback and then dials the agent queue. If an agent becomes available, the Outbound module places a call to the agent, the call details are voiced to the agent and then an outbound call to the telephone number specified by the caller is made. The incoming call flow is described below.

- Customer calls the contact center and gets routed to an agent queue.
- Call is routed to CBM via Communication Manager (H.323 channels).
- Once the call is answered by the CBM Inbound module (application) configured on Experience Portal, CBM offers various options to leave a call back request. The following are the call back options:
  - Call back as soon as an agent is available
  - Call back on same day at a later time
  - Call back on a future day and time
- CBM then prompts the customer to enter the call back contact number, account information, and appropriate date/time of call back. A request is then registered into the CBM database.
- If a customer decides to decline the callback option, call is routed back in queue on Communication Manager.

The CBM Outbound module running on the iAssist Admin server continuously polls the database on a regular interval to retrieve pending callback requests. The Outbound module then calls the appropriate agent group number to get an agent to process the callback. Once the agent answers the call, CBM plays the customer's information to the agent. CBM then dials the customer's number and conferences the call with the agent. If the customer call cannot be completed, CBM reschedules the call based on a pre-defined schedule interval. CBM reschedules the call for a specified number of times. Once the maximum attempts have been made unsuccessfully, the call is marked as failed.

Another Acqueon related solution is described in Application Notes for Acqueon iAssist Call Survey Manager with Avaya Aura® Experience Portal.

## **2. General Test Approach and Test Results**

This section describes the interoperability compliance testing used to verify the CBM applications 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 CBM applications to allow the caller the option to request a call back. All of the call back request options available in the CBM Inbound application were tested. In addition, the CBM 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 iAssist reports.

The serviceability testing focused on verifying the ability of iAssist Admin 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 on Communication Manager.
- Experience Portal successfully running both CBM applications.
- 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.
- CBM servicing pending call back requests.
- The ability to reschedule a call back if the call to the agent or caller is not completed within a specified timeout value.
- iAssist reports showing the registered call back requests and the call back status.

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

## 2.2. Test Results

All executed test cases passed.

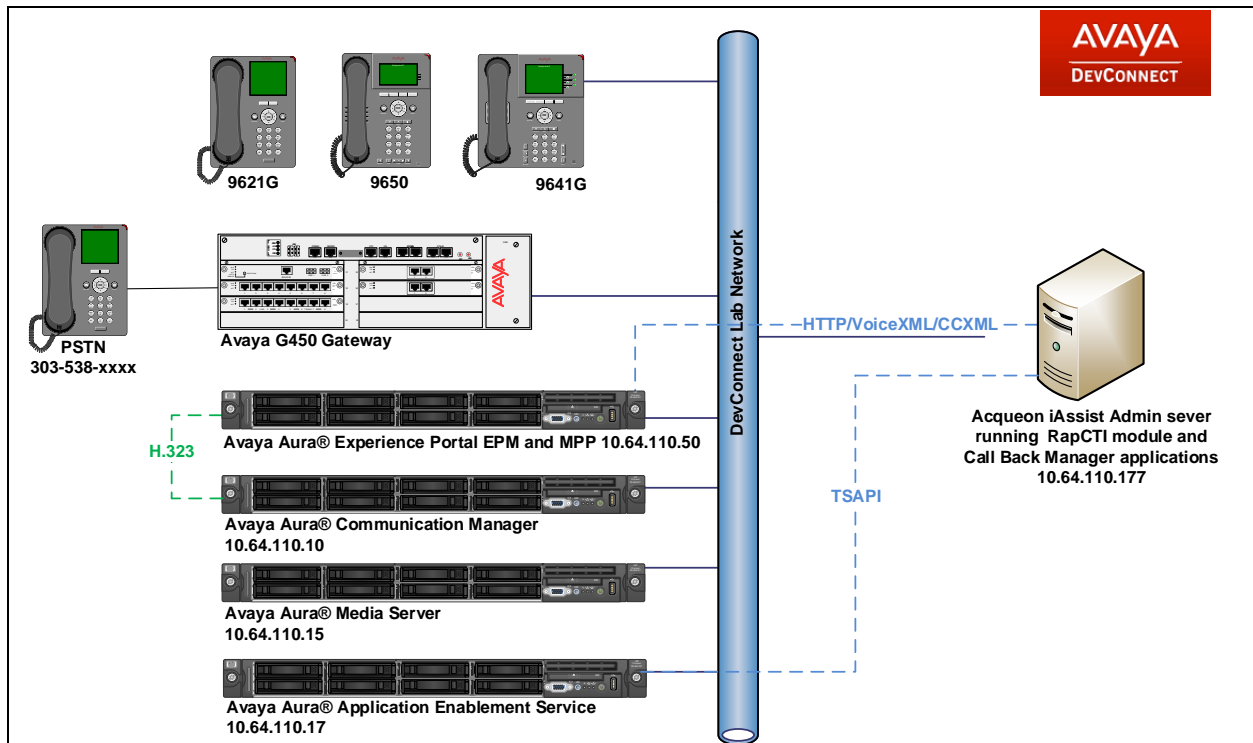
## 2.3. Support

For technical support on the iAssist Call Back Manager, contact Acqueon via phone, email, or internet. You can also raise the ticket in our Acqueon portal by using your Issue Trak Login ID. You can reach our Product Support desk by reaching below Contact number.

- **Phone:** +91 44 3089 4888/+91 44 6108 4888(APAC and MEA)  
+1 888 946 6878(USA and Europe)
- **Email:** support@acqueon.com
- **Web:** <http://acqueon.issuetrak.com>

### 3. Reference Configuration

Error! Reference source not found. **Figure 1** below depicts the lab configuration used for testing. In this configuration, Experience Portal interfaces with Communication Manager via H.323. The iAssist Admin server hosted the CBM applications supporting the CBM Inbound and Outbound modules. The iAssist Admin server also connected to AES via TSAPI. The iAssist Admin server used the Microsoft SQL Server database.



**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 running on Virtualized Environment	7.1.3 R017x.01.0.532.0 Build 24515
Avaya Aura® Application Enablement Services running on Virtualized Environment	7.1.3.0.1.7-0
Avaya Aura® Media Server running on Virtualized Environment	7.8
Avaya Aura® Experience Portal running on Virtualized Environment	7.2.1.0.0605
Avaya G450 Media Gateway	38.19.0
Avaya 9641GS H323 IP Deskphone	6.6.6
Avaya 9621G SIP IP Deskphone	7.1.29
Acqueon iAssist Admin server running on a Virtualized Environment hosting: RapCTI module Call Back Manager applications Avaya Aura® Orchestration Designer (aesconnector and runtimeconfig)	Microsoft Windows Server 2012 R2 Microsoft SQL Server 2012 2.2.1.17 AT8 C115  7.2 Feature Pack 1

**Note:** aesconnector.jar was running on Acqueon iAssist Admin Server, is owned by Avaya. This aesconnect.jar file comes bundled with Avaya Aura® Orchestration Designer package.

## 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 H.323 Channels for Experience Portal.
  - Administer Hunt Group
  - Administer Stations
  - Administer Agent IDs
- 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	
<b>Create Universal Call ID (UCID)? y UCID Network Node ID: 1</b>	

On Page 6, enable **7434ND**. This is used by H.323 channels configured for Communication Manager to communicate with Experience Portal.

change system-parameters features	Page 6 of 19
FEATURE-RELATED SYSTEM PARAMETERS	
Public Network Trunks on Conference Call: 5	Auto Start? n
Conference Parties with Public Network Trunks: 6	Auto Hold? n
Conference Parties without Public Network Trunks: 6	Attendant Tone? y
Night Service Disconnect Timer (seconds): 180	Bridging Tone? n
Short Interdigit Timer (seconds): 3	Conference Tone? n
Unanswered DID Call Timer (seconds):	Intrusion Tone? n
Line Intercept Tone Timer (seconds): 30	Mode Code Interface? n
Long Hold Recall Timer (seconds): 0	
Reset Shift Timer (seconds): 0	
Station Call Transfer Recall Timer (seconds): 0	Recall from VDN? n
Trunk Alerting Tone Interval (seconds): 15	
DID Busy Treatment: tone	
Allow AAR/ARS Access from DID/DIOD? n	
Allow ANI Restriction on AAR/ARS? n	
Use Trunk COR for Outgoing Trunk Disconnect/Alert? n	
7405ND Numeric Terminal Display? n	<b>7434ND? y</b>
DTMF Tone Feedback Signal to VRU - Connection: Disconnection:	



Note that there were other System Parameters Features were also enabled, but such parameters are standard in nature for a call center configuration and are out of scope for this document.

## 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		<b>ACD?</b>	<b>y</b>
Group Name: Skill 1		<b>Queue?</b>	<b>y</b>
Group Extension: 23001		<b>Vector?</b>	<b>y</b>
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			
<b>Skill?</b>	<b>y</b>	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 6001 and 6002 were created for two call center agents.

add agent-loginID 6001		Page 1 of 2
AGENT LOGINID		
Login ID: 6001	AAS? n	
Name: Agent 1	AUDIX? n	
TN: 1	Check skill TNs to match agent TN? n	
COR: 1		
Coverage Path:	LWC Reception: spe	
Security Code:	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 6001		Page 2 of 2
AGENT LOGINID		
Direct Agent Skill: 1		Service Objective? n
Call Handling Preference: skill-level		Local Call Preference? n
<b>SN</b>	<b>RL SL</b>	<b>SN RL SL</b>
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:

## 5.4. Administer Call Vectoring

This section describes the procedures for configuring call vectoring for calls queued to agents and inbound calls to CBM.

Configure the **Vector Directory Number** (VDN) that will handle incoming customer calls. The VDN invokes a vector that will queue the call to an agent split and also route the call to the iAssist CBM application on Experience Portal (via H.323 Channels configured later in this section) if the call is queued and the expected wait time exceeds a configured threshold in the associated vector. In this example, VDN 22001 and vector 1 were used for inbound calls that route to Experience Portal. VDN 22002 was configured with vector 2 as well for outbound call backs.

add vdn 22001	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 22001	
Name*: VDN 1	
Destination: Vector Number 1	
Attendant Vectoring? n	
Meet-me Conferencing? n	
Allow VDN Override? y	
COR: 1	
TN*: 1	
Measured: both Report Adjunct Calls as	
ACD*? n	
Acceptable Service Level (sec): 20	
VDN of Origin Annc. Extension*:	
1st Skill*:	
2nd Skill*:	
3rd Skill*:	
SIP URI:	

Vector 1 queues the call to the agent split (skill 1), checks available call center agents on split (skill 1), and depending on the agent availability, the call is either queued to skill 1 or routed to Experience Portal via H.323 channels. Configuration for H.323 channels to Experience Portal is described later in this section.

change vector 1						Page	1 of
6							
CALL VECTOR							
Number: 1		Name: Acqueon Vector 1					
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 goto step	3 if available-agents in skill 1						< 1
03 queue-to	skill 75 pri m						
04 wait-time	30 secs hearing ringback						
05 stop							

Vector 2 was configured to queue outbound call back calls to skill 1 with priority set to high.

change vector 2						Page	1 of
6							
CALL VECTOR							
Number: 2		Name: Acqueon Vector 2					
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 silence						
02 queue-to	skill 1 pri h						
03 wait-time	30 secs hearing ringback						
04 goto step	1 if unconditionally						

## 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 5.3**. Calls are routed to Experience Portal, by the use of this hunt group, as per the configuration in **Section 5.4**.

add hunt-group 75		Page 1 of 4
HUNT GROUP		
Group Number: 75	<b>ACD? y</b>	
Group Name: Voice Portal	<b>Queue? y</b>	
Group Extension: 51112	<b>Vector? y</b>	
Group Type: ucd-mia		
TN: 1		
COR: 1	MM Early Answer? n	
Security Code:	Local Agent Preference? n	
ISDN/SIP Caller Display: grp-name		
Queue Limit: unlimited		
Calls Warning Threshold:	Port:	
Time Warning Threshold:	Port:	

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

add hunt-group 75		Page 2 of 4
HUNT GROUP		
<b>Skill? y</b>	Expected Call Handling Time (sec): 180	
<b>AAS? y</b>		
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, 65001 – 65005, 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 65001		Page 1 of 6
STATION		
Extension: 65001	Lock Messages? n	BCC: 0
<b>Type: 7434ND</b>	<b>Security Code: *</b>	TN: 1
Port: S00079	Coverage Path 1:	COR: 1
Name: H.323 VP 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: 65001	
Display Module? y		
Display Language: english	Coverage Module? n	
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	<b>IP SoftPhone? y</b>	
	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 6501 - 6502 were created. Enable **AAS**, set **Auto Answer** to **none**, and set the **Port Extension** to each corresponding station extensions configured above (65001 – 65005).

add agent-loginID 6501		Page 1 of 2
AGENT LOGINID		
Login ID: 6501		<b>AAS? y</b>
Name: VP Agent 1		AUDIX? n
TN: 1	Check skill TNs to match agent TN? n	
COR: 1		
Coverage Path:	LWC Reception: none	
Security Code:	LWC Log External Calls? n	
Attribute:	AUDIX Name for Messaging:	
<b>Port Extension: 65001</b>	LoginID for ISDN/SIP Display? n	
		<b>Auto Answer: none</b>
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 6501		Page 2 of 2
AGENT LOGINID		
Direct Agent Skill:		Service Objective? n
Call Handling Preference: skill-level		Local Call Preference? n
<b>SN</b>	RL SL	SN RL SL
1: <b>75</b>	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 AES Connectivity**

Configuration for AES and CTI link used during compliance test is standard in nature and is outside of scope for this document.



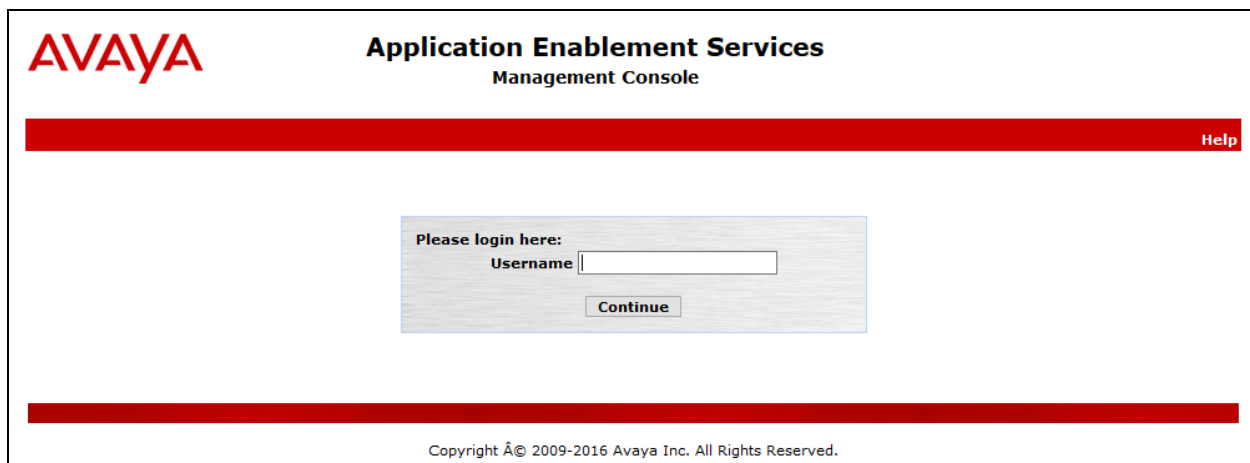
## 6. Configure Avaya Aura® Application Enablement Services

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.

iAssist Admin server connected to AES via TSAPI to monitor stations 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.



The screenshot displays the Avaya Application Enablement Services (AES) Management Console login interface. At the top left is the Avaya logo, and to its right is the title "Application Enablement Services Management Console". A red horizontal bar spans the width of the page, with a "Help" link on the right. In the center, a light gray box contains the text "Please login here:" followed by a "Username" label and a text input field. Below the input field is a "Continue" button. At the bottom of the page, another red horizontal bar is present, with the copyright notice "Copyright © 2009-2016 Avaya Inc. All Rights Reserved." centered below it.

## 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 Avaya Application Enablement Services Management Console. The top right corner displays system information: Welcome: User cust, Last login: Thu Sep 27 12:37:59 2018 from 10.64.10.202, Number of prior failed login attempts: 0, HostName/IP: aes/10.64.110.17, Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE, SW Version: 7.1.3.0.1.7-0, Server Date and Time: Thu Sep 27 12:46:09 MDT 2018, HA Status: Not Configured. The breadcrumb navigation is **User Management | User Admin | List All Users**. The left sidebar shows a tree view with **User Management** expanded, and **User Admin** selected. The main content area is titled **Edit User** and contains the following fields:

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

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 Avaya Application Enablement Services Management Console. The breadcrumb navigation is **Security | Security Database | CTI Users | List All Users**. The left sidebar shows a tree view with **Security** expanded, and **Security Database** selected. The main content area is titled **Edit CTI User** and contains the following fields:

User Profile:	User ID	acqueon
	Common Name	acqueon
	Worktop Name	NONE
	Unrestricted Access	<input checked="" type="checkbox"/>
Call and Device Control:	Call Origination/Termination and Device Status	None
Call and Device Monitoring:	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	<input type="checkbox"/>
Routing Control:	Allow Routing on Listed Devices	None
<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.

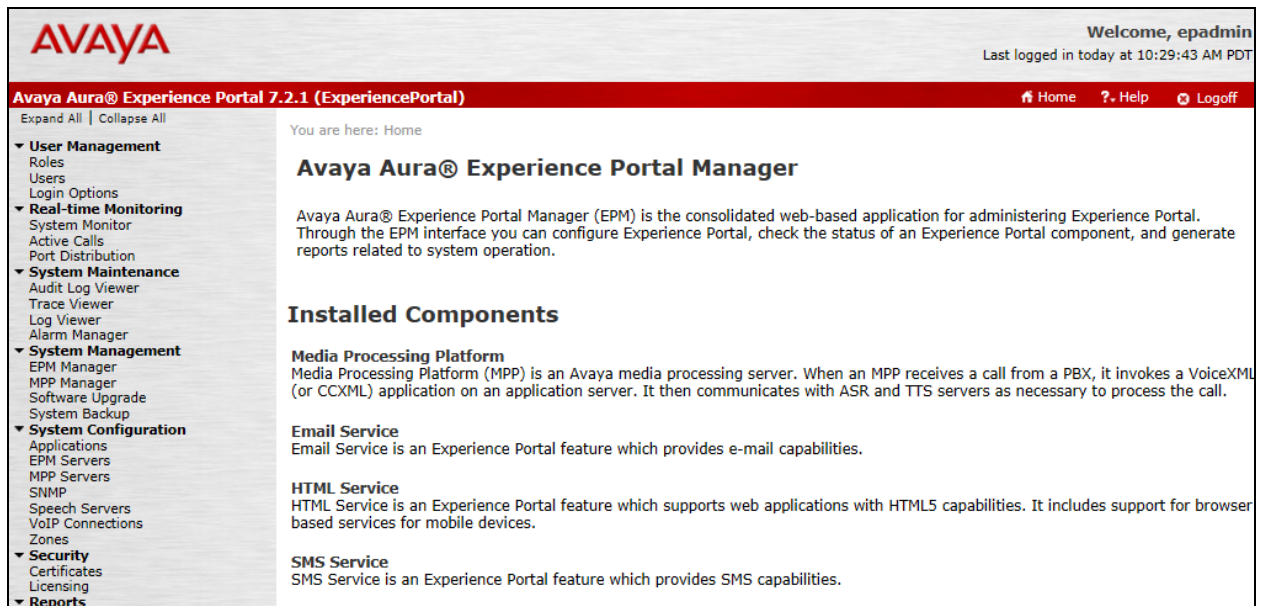
The screenshot shows a web interface for the iAssist Admin Security Database. The top navigation bar is red and contains the text "Security | Security Database | Tlinks" on the left and "Home | Help | Logout" on the right. On the left side, there is a vertical menu with the following items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", and "Security" (which is expanded). The main content area is titled "Tlinks" and contains a section labeled "Tlink Name" with three radio button options: "AVAYA#CM15014#CSTA#AES15019" (selected), "AVAYA#CM15014#CSTA-S#AES15019", and "AVAYA#CM15088#CSTA#AES15019". Below these options is a button labeled "Delete Tlink".

## 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. Administer VoIP Connection

On the left pane, click on the **VoIP Connections** under **System Configuration** (not shown). To add an **H.323 Connection**, click on **H.323** tab on **VoIP Connections** page (not shown). Fill in **Name**, in the **Gatekeeper Address** and **Gatekeeper Port**, type in the IP Address of Communication Manager and default port of **1719**, respectively. Under **New Stations** section, type in the range of stations, as configured in **Section 5.5.2**, in **From** and **To** fields; type in the **Password** as configured in **Section 5.5.2**. Select **Inbound and Outbound** for **Station Type**, and select **Add**. Click **Save** to save changes.

The screenshot displays the Avaya Aura Experience Portal 7.2.1 (ExperiencePortal) interface. The top navigation bar includes the Avaya logo, a welcome message for 'epadmin', and the last login time '10:29:43 AM PDT'. The main navigation menu on the left lists various system configuration options, with 'VoIP Connections' highlighted under 'System Configuration'. The main content area is titled 'Change H.323 Connection' and provides instructions for changing the configuration of an H.323 connection. The configuration fields include: Name (ACM), Enable (Yes/No), Gatekeeper Address (10.64.110.10), Alternative Gatekeeper Address, Gatekeeper Port (1719), and Media Encryption (Yes/No). The 'New Stations' section allows for adding stations by specifying a range (From/To), password, and station type (Inbound and Outbound, Inbound Only, or Maintenance). The 'Configured Stations' section shows a list of configured stations (65001 - 65005) with a 'Remove' button. The bottom of the page features 'Save', 'Apply', 'Cancel', and 'Help' buttons.

**AVAYA** Welcome, epadmin  
Last logged in today at 10:29:43 AM PDT

**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 H.323 Connection](#)

### Change H.323 Connection

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

Name: ACM

Enable: ☒ Yes ☐ No

Gatekeeper Address:

Alternative Gatekeeper Address:

Gatekeeper Port:

Media Encryption: ☐ Yes ☒ No

#### New Stations

From	To
Station: <input type="text"/>	<input type="text"/>
Password: <input type="text"/>	
<input checked="" type="radio"/> Same Password	
<input type="radio"/> Use sequential passwords	
Station Type: <input type="text" value="Inbound and Outbound"/>	<input type="button" value="Add"/>
<input type="text" value="Inbound Only"/>	
<input type="text" value="Maintenance"/>	

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

65001 - 65005	<input type="button" value="Remove"/>
---------------	---------------------------------------

## 7.2. Configure iAssist CBM Applications

Two applications are configured in Experience Portal, one to handle inbound calls that are queued to the agent split and the second one to handle the call back request (i.e., outbound calls to agent and caller).

### 7.2.1. Configure the Inbound CBM Application

In the **Applications** page, add an Experience Portal application to handle incoming. This application will provide the caller the option to either continue waiting in the agent queue or to request a call back. Configure the application as shown below.

Note that the **Called Number** configured is the inbound VDN Extension as configured in **Section 5.4**.

The screenshot displays the Avaya Aura Experience Portal 7.2.1 (ExperiencePortal) interface. The top navigation bar includes the Avaya logo, a welcome message for 'epadm', and a timestamp 'Last logged in today at 10:29:43 AM P'. The main navigation menu on the left lists various system management and configuration options. The central content area is titled 'Change Application' and provides a form to configure an application. The application name is 'iAssist\_Inbound\_CBM'. The 'Enable' checkbox is checked. The 'Type' is set to 'VoiceXML'. The 'Reserved SIP Calls' are set to 'None'. The 'Requested' field is empty. The 'URI' section has 'Single' selected. The 'VoiceXML URL' is 'http://10.64.110.177:8080/Inbound\_CBM/Start'. The 'Mutual Certificate Authentication' and 'Basic Authentication' are both set to 'No'. The 'Speech Servers' section has 'ASR' set to 'No ASR' and 'TTS' set to 'No TTS'. The 'Application Launch' section has 'Inbound' selected, and the 'Called Number' is '22001'. There are 'Add' and 'Remove' buttons for the called number list.

**AVAYA** Welcome, epadm  
Last logged in today at 10:29:43 AM P

**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: iAssist\_Inbound\_CBM

Enable: ☒ Yes ☐ No

Type: VoiceXML

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

☒ Number ☐ Number Range ☐ URI

Called Number:  **Add**

**Remove**

## 7.2.2. Configure the Outbound CBM Application

In the **Applications** page, add another Experience Portal application to handle the outbound calls to the agent and caller. Configure the application as shown below.

The screenshot shows the Avaya Aura Experience Portal 7.2.1 (ExperiencePortal) interface. The top header includes the Avaya logo, the user 'epadmin', and the login time 'Last logged in today at 10:29:43 AM PDT'. The main navigation bar shows 'Home', 'Help', and 'Logoff'. The left sidebar contains a tree view with categories: User Management, Real-time Monitoring, System Maintenance, System Management, System Configuration, Security, Reports, and Multi-Media Configuration. The 'System Configuration' category is expanded, showing 'Applications' as the selected item. The main content area is titled 'Change Application' and shows the configuration for the 'iAssist\_Outbound\_CBM' application. The configuration includes fields for Name, Enable (Yes/No), Type (CCXML), Reserved SIP Calls (None/Minimum/Maximum), Requested (text input), URI (Single/Fail Over/Load Balance), CCXML URL (http://10.64.110.177:8080/iAssistOutboundCBM\_H323\_CCXML/ccxml/start.jsp), Mutual Certificate Authentication (Yes/No), Basic Authentication (Yes/No), Speech Servers (ASR: No ASR, TTS: No TTS), and Application Launch (Inbound, Inbound Default, Outbound).

**AVAYA**

Welcome, epadmin  
Last logged in today at 10:29:43 AM PDT

**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: iAssist\_Outbound\_CBM

Enable: ☒ Yes ☐ No

Type: CCXML

Reserved SIP Calls: ☒ None ☐ Minimum ☐ Maximum

Requested:

**URI**

☒ Single ☐ Fail Over ☐ Load Balance

CCXML URL:  **Verify**

Mutual Certificate Authentication: ☐ Yes ☒ No

Basic Authentication: ☐ Yes ☒ No

**Speech Servers**

ASR: No ASR

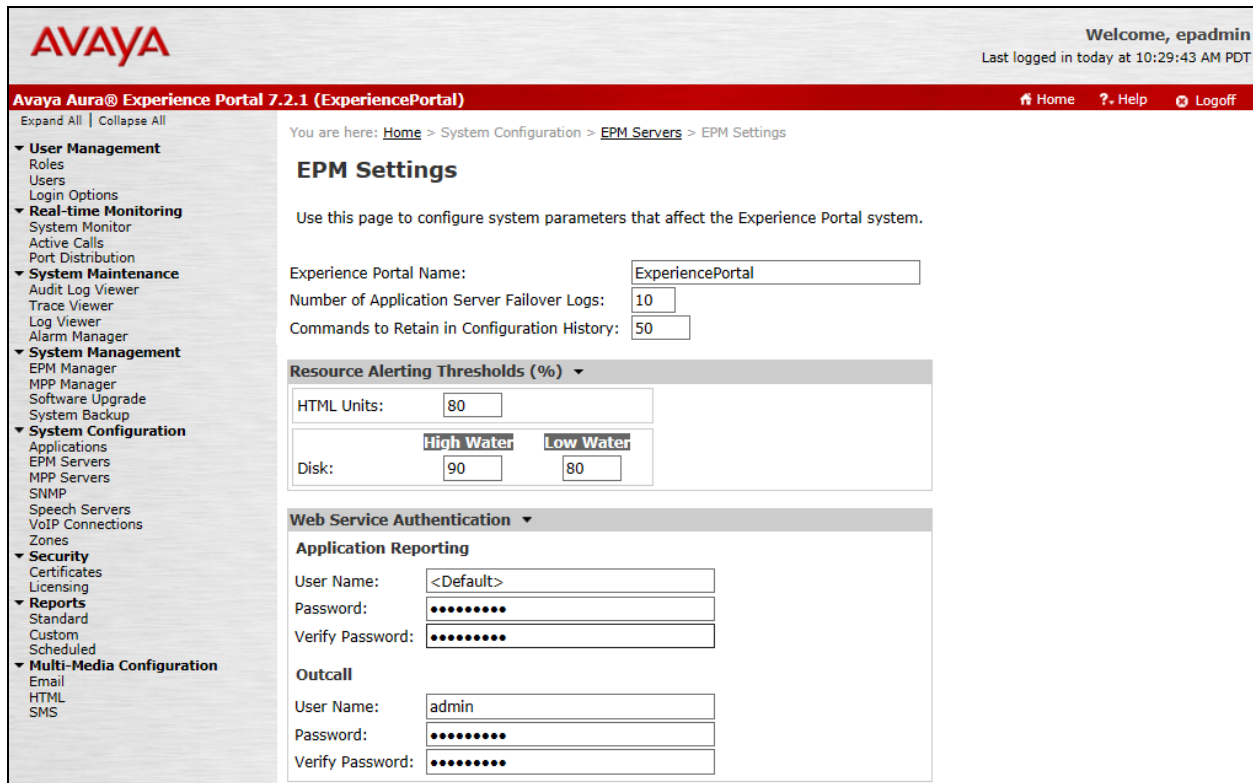
TTS: No TTS

**Application Launch**

☐ Inbound ☐ Inbound Default ☒ Outbound

### 7.3. Configure the Outcall Authentication

Configure the Outcall User Name and Password that will be sent by CBM Outbound module to initiate a call back. Click on **EPM Servers** in the left pane, in the resulting page, click on **EPM Settings** to display the page below. Under the **Outcall** section, configure the **User Name** and **Password** used by CBM when it makes an outcall request to Experience Portal.



**AVAYA** Welcome, eadmin  
Last logged in today at 10:29:43 AM PDT

**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 > [EPM Servers](#) > EPM Settings

### EPM Settings

Use this page to configure system parameters that affect the Experience Portal system.

Experience Portal Name:

Number of Application Server Failover Logs:

Commands to Retain in Configuration History:

**Resource Alerting Thresholds (%) ▼**

HTML Units:

Disk:  **High Water**  **Low Water**

**Web Service Authentication ▼**

**Application Reporting**

User Name:

Password:

Verify Password:

**Outcall**

User Name:

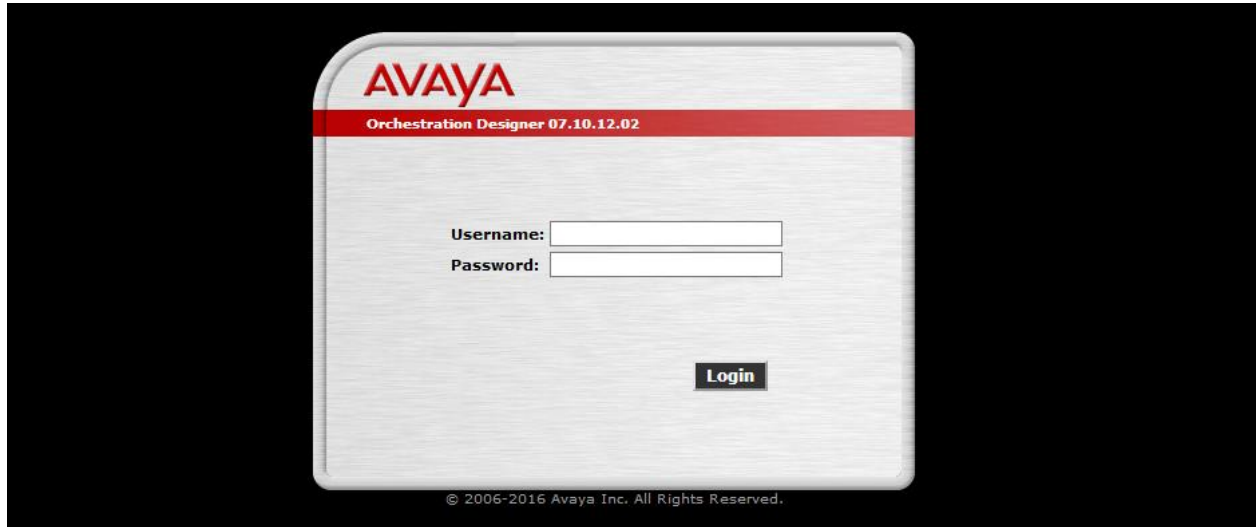
Password:

Verify Password:

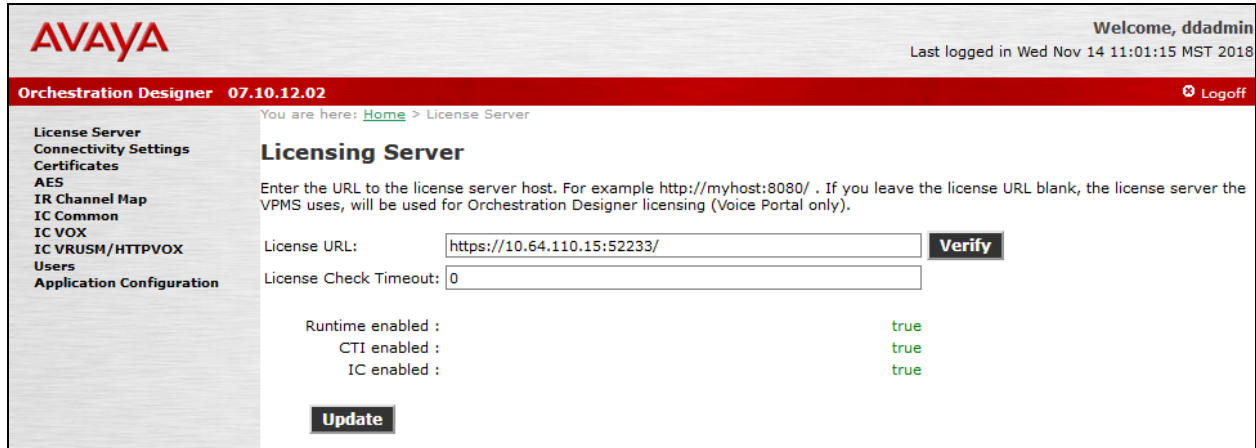


## 7.4. Configure Avaya Aura® Orchestration Designer

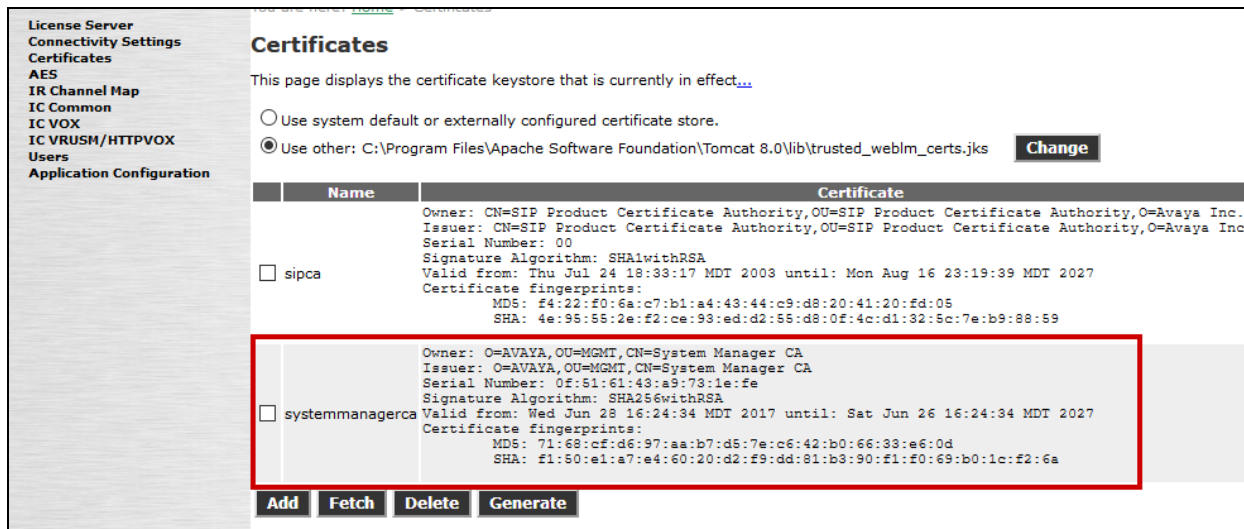
iAssist Admin server hosted the runtimeconfig and aesconnector connectors. Access the runtimeconfig via a web browser and log on using appropriate credentials.



On the left pane, select **License Server** and configured the URL for WebLM server that is hosting the licenses. Select **Verify** to ensure that licenses are retrieved.



On the left pane, select **Certificates** and update the root certificate of the certificate authority that is used for signing certificates, for secure connectivity, in the lab environment. During compliance test, Avaya Aura® System Manager was used as the Certificate Authority. System Manager root certificate was added as shown below.



On the left pane, select **AES** to configure AES connectivity. Configure the AES parameters as per **Section 6**. Select **Add Tserver/AES** once done.

Name:  A unique name to identify this entry. The tserver and failover names cannot contain '\*'.  
Service Name:  Identifies the service provider in the format: vendor#switch#type#server.  
User Name:  Username to connect to this tserver/AES.  
Password:  Unencrypted password to connect to this tserver/AES.  
Confirm Password:  Confirm password must match password.

**Add TServer/AES**

**Note:** You will need to restart the AES Connector for changes to take affect  
You will also need to modify tsapi.pro that is included with your runtimesupport files before connecting to a TServer/AES. Please read Orchestration Designer documentation for correct location to place this file.

Once AES Connector has been added, select **map** under **Ext map**.

**AES Connector**

Timeout:

Time in ms to wait for TServer/AES to obtain the call.  
Do not end the input with 'ms'.

Trace Verbosity:

Amount of debug output: 0-off - 3 full.

**Update**

<input type="checkbox"/>	Type	Name	Service Name	User Name	Ext Map	Add Failover
<input type="checkbox"/>	tserver/AES	<a href="#">iAssist</a>	AVAYA#CM15014#CSTA#AES15019	acqueon	<b>map</b>	<a href="#">add failover</a>

**Delete**

Add the H.323 Channels (Extensions) that were added in **Section 5.5.2**.

**Tserver Extension Map**

Extension Map for Tserver : [iAssist](#)

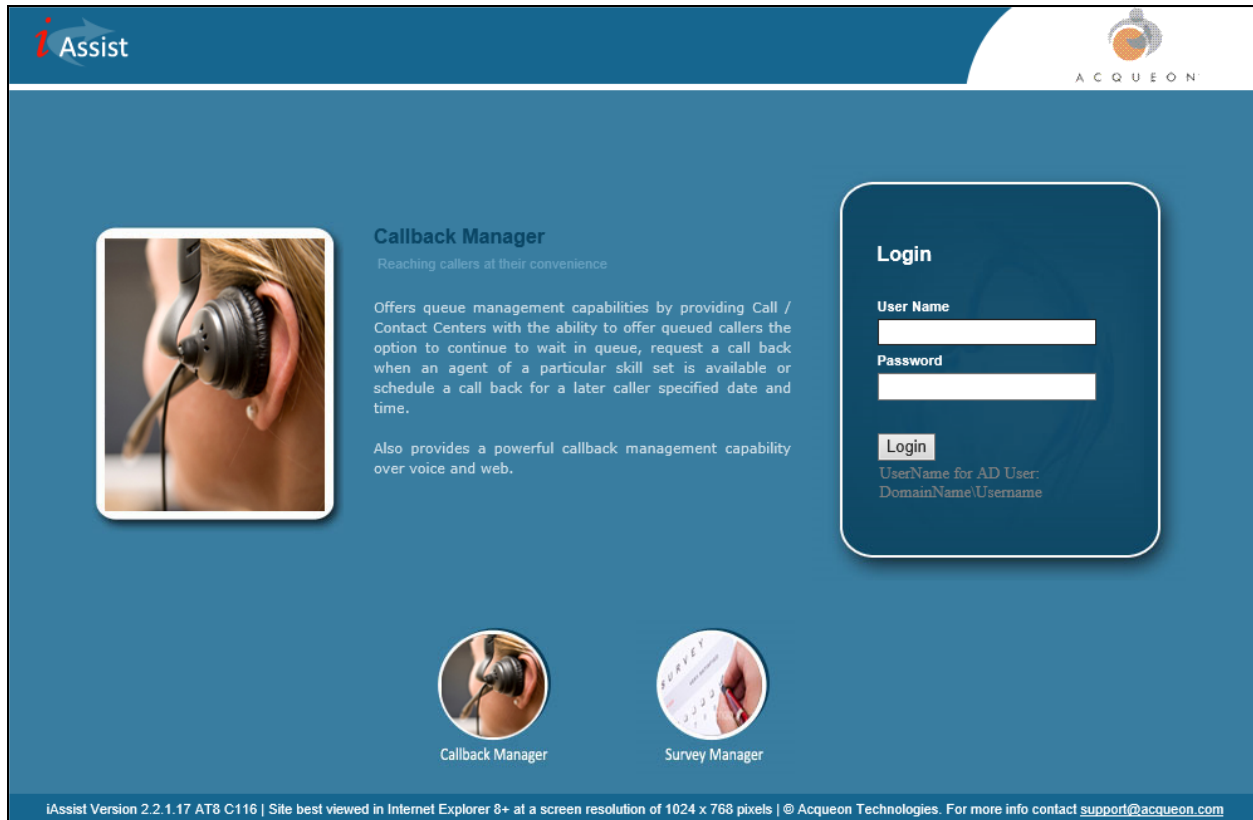
<input type="checkbox"/>	Channel	Mapped Extension	Observe On Startup
<input type="checkbox"/>	65001	65001	true
<input type="checkbox"/>	65002	65002	true
<input type="checkbox"/>	65003	65003	true
<input type="checkbox"/>	65004	65004	true
<input type="checkbox"/>	65005	65005	true

**Delete**

## 8. Configure Acqueon iAssist CallBack Manager

This section provides the procedures for configuring CBM via the iAssist Admin web console. Access the iAssist Admin web console by using the URL “https://ip-address” in a web browser, where “ip-address” is the IP address of iAssist server. Log on using appropriate credentials.

**Note:** The current version of Acqueon iAssist Callback Manager only supports Microsoft Internet Explorer.



## 8.1. Add a Business group

Business Group refers to the type of business the application caters. Each business group will have a language and a unique number where the call will be routed to so that the application can identify the caller.

Business Group Management enables configuration and management of a business group. Use the **Business Group** option under the **General** tab to add, modify or delete a business group.

- Enter a valid **Business Group Name**.
- Set the **Incoming Number** to the inbound VDN extension number configured in **Section 5.4**.
- Select a pre-configured **Site** to from the dropdown menu to associate the business group to a site.
- Select an appropriate **Language**.
- Select a pre-configured **IVR Configuration Template**.

The screenshot displays the iAssist Business Group Management interface. The top navigation bar includes the iAssist logo, the Acqueon logo, and a user welcome message: "Welcome admin | Logout". The main content area is divided into two sections: "Business Group Management" and "Defined Business Group(s)".

**Business Group Management**

This section contains a form for adding a new business group. The form has the following fields:

- Business Group Name \***: A text input field with the value "CBM Business Group". A red asterisk indicates it is mandatory.
- Incoming Number \***: A text input field with the value "22001". A red asterisk indicates it is mandatory.
- Site**: A dropdown menu with the value "DevConnect Site".
- Language**: A dropdown menu with the value "US English".
- IVR Configuration Template**: A dropdown menu with the value "DEFAULT\_CBM\_CONFIG".

At the bottom of the form are two buttons: "Update Business Group" and "Cancel".

**Defined Business Group(s)**

This section contains a table listing the defined business groups:

Business Group	Edit	Delete
CBM Business Group		
CSM Business Group		

## 8.2. Configure Business Group

Access the **Business Group Configuration** option from the **CBM** tab. Click the **Edit** icon of the Business Group configured above under the **Defined Business Group(s)** displayed in the right pane. The Business Group Name will be populated automatically.

- Enter an **Outgoing Number** (VDN number configured to reach the available agent who is configured/ logged into a particular skill, as per the outbound VDN configured in **Section 5.4**).
- Select the **High Priority Queue** check box.
- Provide the **High Priority Queue VDN Number**, same as the **Outgoing Number**.
- Enter **IVR IP Address**, which is the IP Address of Experience Portal EPM.
- **Time Zone** (Time zone of system in which iAssist application is deployed).
- Select **High** from the **Priority** drop down menu.

**iAssist** ACQUEON

Home Manage General **CBM** CSM License Welcome admin | Logout

### CBM - Business Group Configuration [CBM Business Group]

**\* Mandatory**

Business Group Name	CBM Business Group
Outgoing Number *	22002
High Priority Queue	<input checked="" type="checkbox"/>
High Priority Queue VDN	22002
IVR IP Address *	10.64.110.50
Time Zone	(UTC-08:00) Pacific Time (US & Canada) ▼
Priority	HIGH ▼

**Defined Business Group(s)**

Business Group	Edit
CBM Business Group	

## 8.3. RealTime Queue

Continuing from above, select the **RealTime Queue** option. Check box for **RealTime Queue Enabled** to enable the RealTime Queue. This ensures that the callback requester remains in a virtual queue.

### RealTime Queue

RealTime Queue Enabled	<input checked="" type="checkbox"/>
Allow Calls to be Rescheduled for next day	<input checked="" type="checkbox"/>
High priority threshold	2
IRC Buffer Call Duration (min)	10
IRC CallTimer (min)	0

**Defined Business Group(s)**

Business Group	Edit
CBM Business Group	

## 8.4. Business Hours and Break Hours

Continuing from above, select the **Business Hour and Break Hour** option. It should be entered in the 24-hour format, the break hour is an interval within the business hours, for example, lunch break. Call back request options will be offered to the callers based on the business hours and will not be allowed outside of this schedule. Business hours and break hours should be configured for each day of the week separately as shown. Following was configured during the compliance test.

**CBM - Business Group Configuration [CBM Business Group]**

**RealTime Queue**

**Business Hour and Break Hour**

	Business Hour [24 Hrs Format]			Break Hour [24 Hrs Format]	
	StartTime	Inbound-EndTime	Outbound-End Time(Dialing)	Start Time	End Time
Monday	00:00	18:00	18:15	00:00	00:00
Tuesday	00:00	18:00	18:15	00:00	00:00
Wednesday	00:00	18:00	18:15	00:00	00:00
Thursday	00:00	18:00	18:15	00:00	00:00
Friday	00:00	18:00	18:15	00:00	00:00
Saturday	00:00	18:00	18:15	00:00	00:00
Sunday	00:00	18:00	18:15	00:00	00:00

**Defined Business Group(s)**

Business Group	Edit
CBM Business Group	

## 8.5. Time Slots

Continuing from above, select the **Time Slot** option. Time Slot is a defined interval, or slot of time that is offered to callers to choose the call back time. If this is configured, the Inbound CBM will offer the caller the list of configured time slots and the caller can choose one. If this is not configured, the caller will be prompted to enter a time to receive the call back. Timeslots will be played to the caller for the callback options (S- same date and later time and F- Future date and time), if configured.

**Time Slots**

Start Time & End Time: 09:00 18:00

Max Threshold:

Time Slot	MaxThreshold	Delete
09:30 - 10:00	1	

## 8.6. Config Options

Continuing from above, select the **Config Options** option. In Config Options, the **Callback Options** tab allows setting of the various options to be offered to the caller to log a callback request and receive a callback. These options will be dynamically offered based on the settings like Business Hours and Holidays, which are configured. Following were configured as shown in the screen capture below.

The screenshot shows the 'Config Options' section with the 'Callback Options' tab selected. The tab contains a list of options with checkboxes:

Option	Checked
As soon as agent available	<input checked="" type="checkbox"/>
Immediate Callback	<input type="checkbox"/>
Same date later time	<input checked="" type="checkbox"/>
Future date and time	<input checked="" type="checkbox"/>
After 1 hour	<input checked="" type="checkbox"/>
Route back to Agent Queue	<input checked="" type="checkbox"/>

## 8.7. Call Flow Generator

Select the **CallFlow Generator** option under the **General** tab. Under this section, call flows are generated for a business group or business group collection. During the compliance test, two call flows were configured; one for inbound calls and another for outbound calls.

The screenshot shows the 'Call Flow Generator' interface. The left pane contains a form for creating a new call flow, and the right pane shows a table of 'Defined CallFlow(s)'.

**Call Flow Generator Form:**

- CallFlow Name \***: CBM\_Inbound
- Site \***: DevConnect Site
- Appplication**: CBM - Inbound
- Filter Type \***: ☐ By Business Group Collection, ☒ By BusinessGroupID
- Business Group \***: ☒ CBM Business Group
- Select All**: ☐

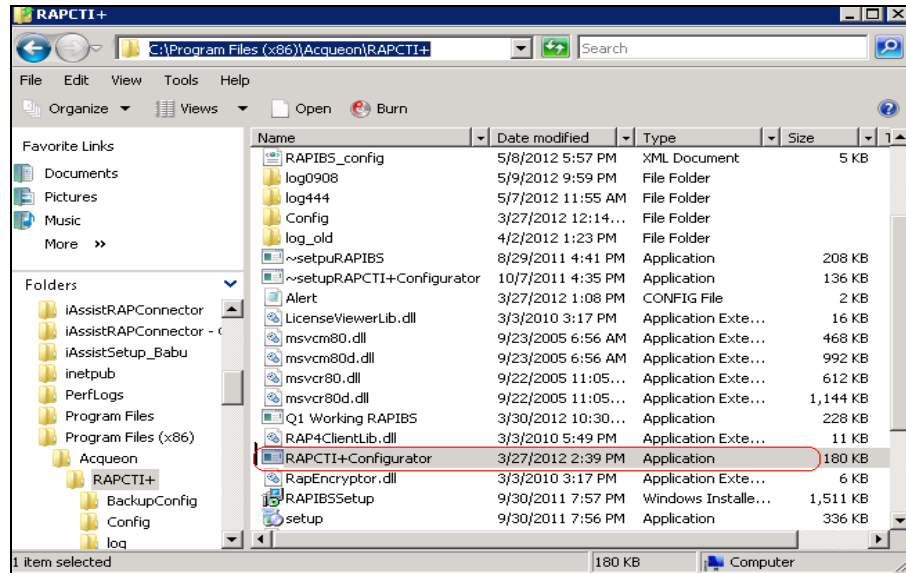
**Defined CallFlow(s) Table:**

CallFlow	Edit	Delete
CBM_Inbound		
CBM_Outbound		
CSM_Inbound		

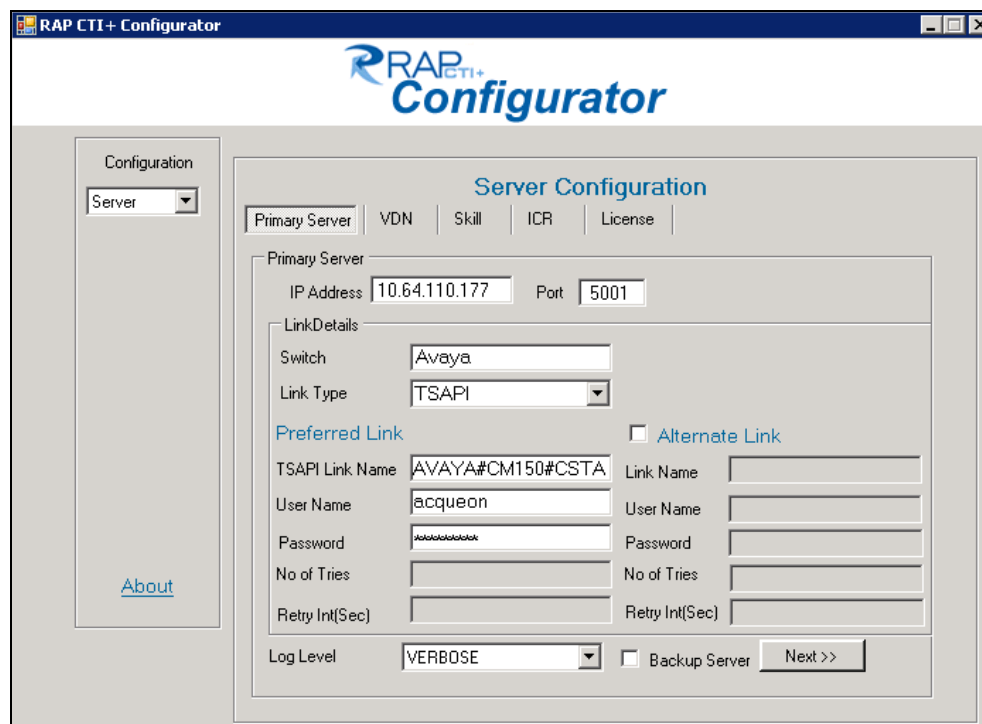


## 8.8. Configure RapCTI

On the iAssist Admin server, open RAPCTI+Configurator from the path (C:\Program Files (x86)\Acqeon\RAPCTI+) to configure the VDN that will be used for monitoring.



Double click on RAPCTI+Configurator to open the screen below. Under the **Primary Server** tab, configure AES connectivity as per **Section 6**.



Select the **VDN** tab:

- Configure the VDN that was configured in **Section 5.4** for incoming calls (22001).
- Select **Originating VDN** from the **VDN Type** drop down list
- Select **Add**.

The screenshot shows the 'RAP CTI+ Configurator' application window. On the left is a 'Configuration' sidebar with a 'Server' dropdown and an 'About' link. The main area is titled 'Server Configuration' and has tabs for 'VDN', 'Skill', 'ICR', and 'License'. The 'VDN' tab is active, showing 'VDN Details'. A red box highlights the 'VDN Number' field (containing '22001') and the 'VDN Type' dropdown (set to 'Originating VDN'). Below these is an 'Add' button. Further down are fields for 'Originating VDN' (containing '22001') and 'Route VDN', each with a red 'X' icon to its right. At the bottom, there is a 'Failed VDN retry Timer' set to '1 (in Minutes)' and navigation buttons '<< Previous' and 'Next >>'.

Select the **VDN** tab:

- Configure the VDN that was configured in **Section 5.4** for callback requests (22002).
- Select **Route VDN** from the **VDN Type** drop down list
- Select **Add**.

The screenshot shows the 'RAP CTI+ Configurator' application window. The 'Server Configuration' tab is active, and the 'VDN' sub-tab is selected. In the 'VDN Details' section, the 'VDN Number' is set to '22002' and the 'VDN Type' is set to 'Route VDN'. A red rectangle highlights these two fields. Below them is an 'Add' button. The 'Originating VDN' field contains '22001' and the 'Route VDN' field contains '22002', both with red 'X' icons to their right. The 'Send VDN as DNIS' checkbox is unchecked. At the bottom, the 'Failed VDN retry Timer' is set to '1' (in Minutes). Navigation buttons '<< Previous' and 'Next >>' are located at the bottom right. A sidebar on the left contains a 'Configuration' dropdown set to 'Server' and an 'About' link.

Select **Next** >> 3 times.

The screenshot shows the 'RAP CTI+ Configurator' application window. The 'Server Configuration' tab is active, with sub-tabs for 'VDN', 'Skill', 'ICR', and 'License'. The 'VDN Details' section includes a 'VDN Number' field with '22002', a 'VDN Type' dropdown set to 'Route VDN', and an unchecked 'Send VDN as DNIS' checkbox. Below these are lists for 'Originating VDN' (containing '22001') and 'Route VDN' (containing '22002'), each with a red 'X' icon. At the bottom, the 'Failed VDN retry Timer' is set to '1 (in Minutes)'. The 'Next >>' button is highlighted with a red rectangle.

Select **Save** and **Yes** to complete save the configuration.

This screenshot shows the same 'RAP CTI+ Configurator' window, but with a 'Confirm Save' dialog box open in the center. The dialog box contains the text 'Are You Sure to Save RAP Configuration?' and two buttons: 'Yes' and 'No'. The 'Yes' button is highlighted with a red rectangle. In the background, the 'Save' button on the main configuration screen is also highlighted with a red rectangle. The background window shows a list of hexadecimal strings.

## 9. Verification Steps

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

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

Avaya Aura® Experience Portal 7.2.1 (ExperiencePortal)

Expand All | Collapse All

Home ? Help Logoff

You are here: Home > Real-Time Monitoring > System Monitor

### System Monitor (Sep 28, 2018 8:41:51 AM PDT)

This page displays the current state of the local Experience Portal system plus any remote Experience Portal systems that you have configured. For information about the colored alarm symbols, click Help.

Summary ExperiencePortal Details

Last Poll: Sep 28, 2018 8:41:37 AM PDT

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	✓

Help

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

Avaya Aura® Experience Portal 7.2.1 (ExperiencePortal)

Expand All | Collapse All

Home ? Help Logoff

You are here: Home > Real-Time Monitoring > Port Distribution > Port Distribution Report

### Port Distribution Report (Sep 28, 2018 8:42:50 AM PDT)

This page displays information about how the telephony resources have been distributed to the MPPs. You configure the telephony resources on the VoIP Connections page.



Total Ports: 5 Last Poll: Sep 28, 2018 8:42:44 AM PDT

Port	Mode	State	Port Group	Protocol	Current Allocation	Base Allocation
65001	Online	In service	ACM	H323	localMPP	
65002	Online	In service	ACM	H323	localMPP	
65003	Online	In service	ACM	H323	localMPP	
65004	Online	In service	ACM	H323	localMPP	
65005	Online	In service	ACM	H323	localMPP	

Help

3. Place a call to the inbound VDN configured in **Section 5.4** and verify call back options are played by the CBM Inbound module.
4. Continuing from above, select a call back option so the CBM Outbound module adds a call back request in the database.

- To check the status of callback, select **General → Status Management**, in the Call Status field (not shown) select a status to display, e.g. “Pending”, “Completed”, or “Failed”. The screenshot below shows the “Completed” call back.

[Home](#)
[Manage](#)
[General](#)
[CBM](#)
[CSM](#)
[License](#)
Welcome admin | [Logout](#)

### Status Management

Site  
From Date  
Call Status

Business Group  
End Date  
Total no of Records

SI No	Call ID	BusinessGroup	Request Time	Customer Number	<input type="checkbox"/> Select
1	2018081514244665002	CBM Business Group	8/15/2018 3:26:11 PM	7209772872	<input type="checkbox"/>
2	2018081514234665004	CBM Business Group	8/15/2018 3:24:23 PM	7204548441	<input type="checkbox"/>
3	2018081514225165003	CBM Business Group	8/15/2018 3:23:34 PM	3035380121	<input type="checkbox"/>
4	2018081514172965001	CBM Business Group	8/15/2018 3:18:11 PM	7204548441	<input type="checkbox"/>
5	2018081513150665002	CBM Business Group	8/15/2018 2:15:17 PM	3035380121	<input type="checkbox"/>
6	2018081512533165005	CBM Business Group	8/15/2018 1:53:59 PM	3035380121	<input type="checkbox"/>
7	2018081512040165003	CBM Business Group	8/15/2018 1:05:00 PM	3035380121	<input type="checkbox"/>
8	2018081511563265002	CBM Business Group	8/15/2018 12:56:49 PM	3035380121	<input type="checkbox"/>
9	2018081511455465001	CBM Business Group	8/15/2018 12:46:17 PM	3035380121	<input type="checkbox"/>

## 10. Conclusion

These Application Notes describe the configuration steps required to integrate the Acqueon iAssist Call Back Manager application 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 7.1.3, Issue 7, May 2018
- [2] Administering and Maintaining Avaya Aura® Application Enablement Services, Release 7.1.3, Issue 5, May 2018
- [3] Administering Avaya Aura® Experience Portal, Release 7.2.1, Issue 1, March 2018

Product Documentation for Acqueon iAssist Callback Manager can be obtained directly from Acqueon.

- [4] Acqueon iAssist Configuration Guide – AVP, Version 2.2, January 2014

---

**©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](mailto:devconnect@avaya.com).