



Avaya Solution & Interoperability Test Lab

Application Notes for Acqueon iAssist Call Back Manager Version 2.1 with Avaya Aura® Experience Portal R6.0 and Avaya Aura® Contact Center R6.3 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate the Acqueon iAssist Call Back Manager with Avaya Aura® Experience Portal and Avaya Aura® Contact Center. 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.

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 with Avaya Aura® Contact Center R6.3 and Avaya Aura® Experience Portal R6.0. 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.

The iAssist Call Back Manager (CBM) consists of two modules: the Inbound Module and the Outbound Module. 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 call back, and then dials the agent queue. If the agent is available, 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.
- If the wait time in queue is more than the threshold set (Expected Wait Time), calls are routed to the inbound CBM application on Avaya Aura® Experience Portal.
- Once the call is answered by the CBM inbound channel on Avaya Aura® 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.
 - Call back on a different date/time.
 - Call back after a specified time interval.
- 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.

The CBM outbound module running on the iAssist Admin server continuously polls the database on a regular interval to retrieve pending call back requests. The outbound module then calls the appropriate agent group number to get an agent to process the call back. 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.

2. General Test Approach and Test Results

This section describes the interoperability compliance testing used to verify the iAssist CBM applications with Contact Center 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 iAssist CBM applications to allow the caller the option to request a call back. All of the call back request options available in the Inbound CBM application were tested. In addition, the Outbound CBM application was also verified. The iAssist Outbound CBM Module initiated the call back to the agent and caller and established a two-way speech 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 Experience Portal to recover from adverse conditions, such as power failures and disconnecting cables to the IP 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.

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 when the expected wait time for an agent exceeds a configured threshold.
- Experience Portal successfully running the iAssist Inbound CBM application and all of the call back options tested.
- The ability of the caller to continue waiting in queue for an agent.
- The ability of the caller to make a call back request. Call back options described above were tested.
- iAssist CBM servicing pending call back requests and running the iAssist Outbound CBM application.
- Failure conditions, such as the call back failing due to network problems, and verifying that the call back was rescheduled.
- 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 failures and disconnecting cables to the IP network.

2.2. Test Results

All test cases passed. Experience Portal and Contact Center were successful in running the iAssist Call Back Manager applications.

2.3. Support

For technical support on the iAssist Call Back Manager, contact Acqueon via phone, email, or internet.

- **Phone:** +9198403 57893 (or) +1 888 946 6878
- **Email:** support@acqueon.com
- **Web:** <http://acqueon.issuetrak.com>

3. Reference Configuration

Figure 1 illustrates the configuration used for testing. In this configuration, Avaya Experience Portal interfaces with Contact Center via SIP for inbound calls and interfaces with Session Manager via SIP for outbound calls. The application server hosts the iAssist CBM application. The Acqueon iAssist Admin server contains the Microsoft SQL database and is used to configure the iAssist CBM application.

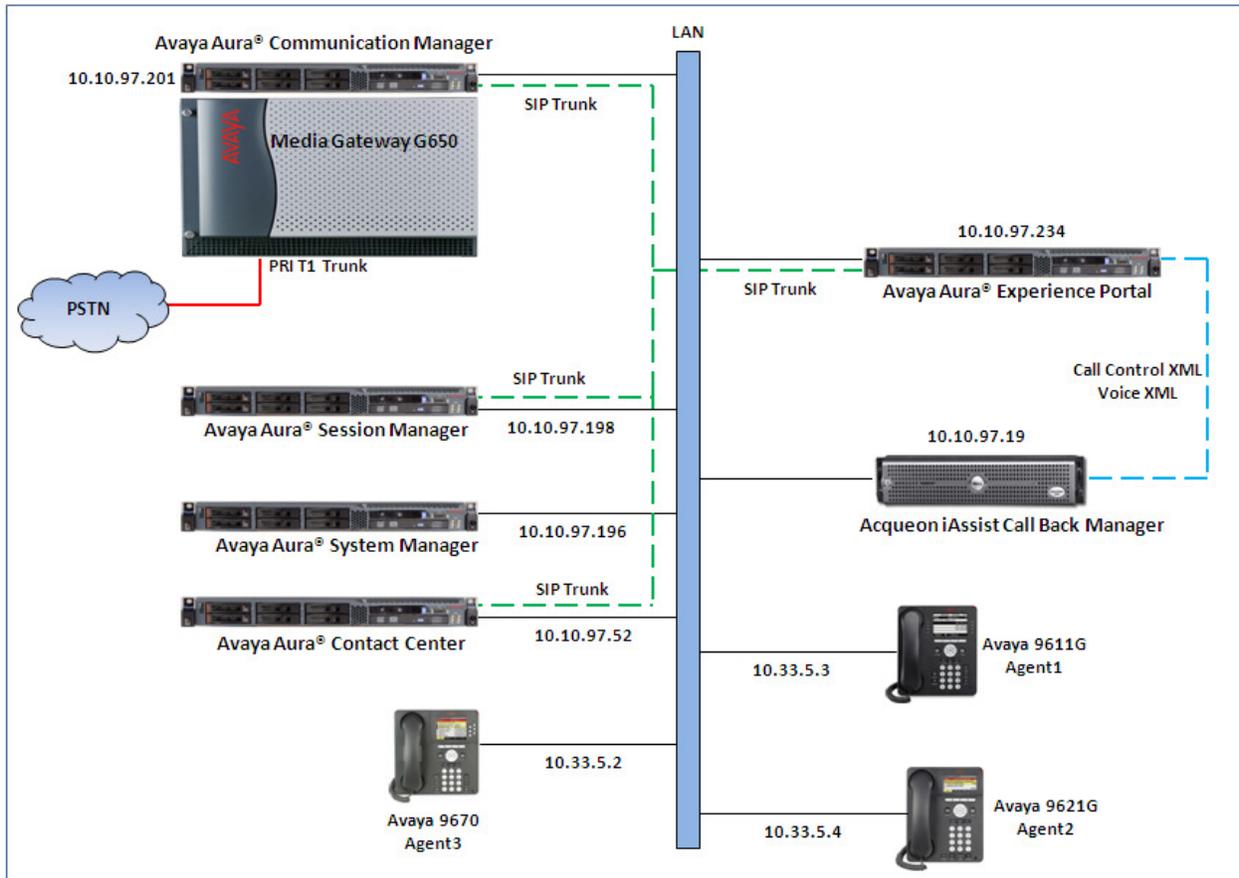


Figure 1: Test Configuration Diagram

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 on an Avaya S8800 Server	R6.3 - FP2 Build R016x.03.0.124.0 Patch 20553
Avaya Aura® System Manager running on an Avaya S8800 Server	R.6.3 – FP2 Build 6.3.0.8.5682
Avaya Aura® Session Manager running on an Avaya S8800 Server	6.3-FP2 Build 6.3.2.632001
Avaya Aura® Experience Portal running on an Avaya S8800 server	6.0
Avaya Aura® Contact Center running on an Avaya S8800 Server	6.3 SP10
Avaya Media Gateway G650 <ul style="list-style-type: none">• IP Server interface TN2312BP• IP Media Processor TN2302AP	HW06 - FW043 HW20 - FW117
Avaya IP 9611	6.23.13
Avaya IP 9621	6.23.13
Avaya IP 9670	6.23.13
Acqueon iAssist Call Back Manager	2.1

5. Configure Avaya Aura® Session Manager

This document assumes that Session Manager is already installed and administered. This section describes the necessary configurations for the Session Manager to work with Contact Center and Experience Portal systems. For more information on how to administer Session Manager, refer to **Section 11**. The following areas are configured on the Session Manager.

- Administer SIP Domain.
- Administer Locations.
- Administer SIP Entities.
- Administer Entity Links.
- Administer Time Ranges.
- Administer Routing Policy.
- Administer Dial Patterns.

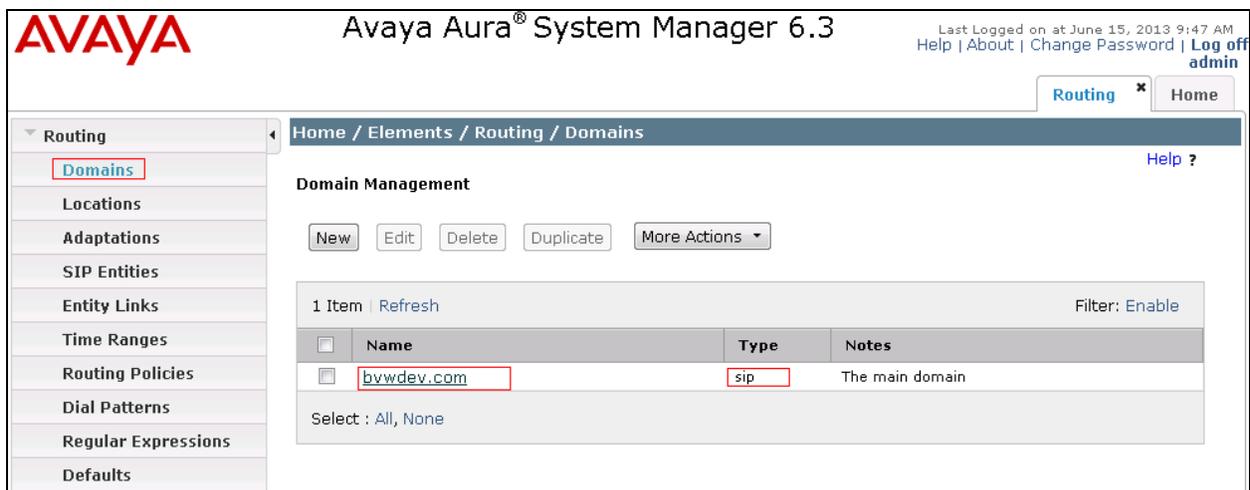
5.1. Administer SIP Domain

Launch a web browser, enter **https://<IP address of System Manager>** or **http://<FQDN of System Manager>** in the URL, and log in with the appropriate credentials (not shown).

Navigate to **Elements→Routing→Domains** and click on the **New** button to create a new SIP Domain (screen not shown). Enter the following values and use defaults for the remaining fields:

- **Name** –Enter the Authoritative Domain name specified in **Section Error! Reference source not found.**, which is **bvwddev.com**.
- **Type** – Select **SIP**.

Click **Commit** to save. The following screen shows the Domains page used during the compliance test.



The screenshot displays the Avaya Aura System Manager 6.3 interface. The top navigation bar includes the Avaya logo, the product name 'Avaya Aura® System Manager 6.3', and user information: 'Last Logged on at June 15, 2013 9:47 AM', 'Help | About | Change Password | Log off admin'. The breadcrumb trail is 'Home / Elements / Routing / Domains'. A left-hand navigation menu is visible with 'Domains' selected. The main content area is titled 'Domain Management' and contains buttons for 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. Below this is a table with one item:

<input type="checkbox"/>	Name	Type	Notes
<input type="checkbox"/>	bvwddev.com	sip	The main domain

Below the table, it shows '1 Item Refresh' and 'Filter: Enable'. At the bottom of the table area, it says 'Select : All, None'.

5.2. Administer Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. This is used for bandwidth management or location-based routing.

Navigate to **Routing**→**Locations** (not shown), and click on the **New** button to create a new SIP Entity location (screen not shown).

General section

Enter the following values and use default values for the remaining fields.

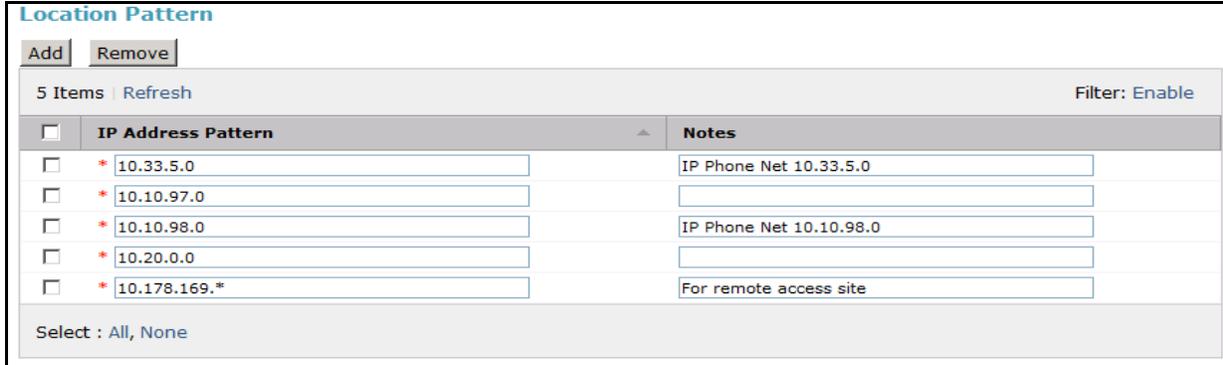
- Enter a descriptive Location in the **Name** field (e.g. **Belleville**).
- Enter a description in the **Notes** field if desired.

Location Pattern section

Click **Add** and enter the following values:

- The IP address information for the **IP Address Pattern** (e.g. **10.10.97.0**).
- A description in the **Notes** field if desired.

Repeat these steps in the Location Pattern section if the Location has multiple IP segments. Modify the remaining values on the form, if necessary; otherwise, use all the default values. Click on the **Commit** button. The screen below shows the IP Address Pattern for the Location Pattern section.



The screenshot shows a web interface titled "Location Pattern". At the top, there are "Add" and "Remove" buttons. Below them, it says "5 Items" and "Refresh", with a "Filter: Enable" option on the right. The main part of the interface is a table with two columns: "IP Address Pattern" and "Notes". Each row has a checkbox on the left. The table contains five entries:

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.33.5.0	IP Phone Net 10.33.5.0
<input type="checkbox"/>	* 10.10.97.0	
<input type="checkbox"/>	* 10.10.98.0	IP Phone Net 10.10.98.0
<input type="checkbox"/>	* 10.20.0.0	
<input type="checkbox"/>	* 10.178.169.*	For remote access site

At the bottom left of the table area, there is a "Select : All, None" option.

The following screen shows the Location page used during the compliance test.



5.3. Administer SIP Entities

A SIP Entity must be added for Session Manager and for each network component that has a SIP trunk. During the compliance test the following SIP Entities were configured:

- Session Manager.
- Contact Center.
- Experience Portal.

Navigate to **Routing → SIP Entities** (not shown) and click on the **New** button to create a new SIP entity (screen not shown). Provide the following information:

General section

Enter the following and use default values for the remaining fields:

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the IP address **10.10.97.198** of the Session Manager signaling.
- Select **Session Manager** from the Type drop down menu.
- Enter a description in the **Notes** field if desired.
- Select the location **Belleville** as configured in **Section 5.2**.
- Select the appropriate time zone.
- Port (only available for the Session Manager SIP Entity): Add port **5060** for **TCP** and **UDP**, and **5061** for **TLS** protocols, and select the sip domain “**bvwdev.com**” in the Default Domain column for each added port.
- Accept the other default values.

Click on the **Commit** button to save each SIP entity. Repeat all the steps for each new SIP entity. The screen below shows the Session Manger **SIP Entity Details**.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The breadcrumb navigation is Home / Elements / Routing / SIP Entities. The left sidebar shows a menu with 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and has a 'General' section. A red box highlights the following fields:

- * Name: DevSM
- * FQDN or IP Address: 10.10.97.198
- Type: Session Manager (dropdown)
- Notes: SIP Entity for Session Manager

 Other visible fields include:

- Location: Belleville (dropdown)
- Outbound Proxy: (empty dropdown)
- Time Zone: America/Toronto (dropdown)
- Credential name: (empty text field)

 Buttons for 'Commit' and 'Cancel' are visible at the top right of the form area. The top right of the page shows 'Last Logged on at May 13, 2013 4:11 PM' and 'Log of admin'.

General section: For the Contact Center SIP Entity, enter the following and use default values for the remaining fields:

- **Name**: Enter a descriptive name.
- **FQDN or IP Address**: Enter the TLAN IP address **10.10.97.52** of the Contact Center interface.
- Select **Other** in the **Type** drop down menu.
- Enter a description in the **Notes** field if desired.
- Select the **Location Belleville** as configured in **Section 5.2**.
- Select the appropriate **Time Zone**.

The screen below shows the Contact Center **SIP Entity Details**.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The breadcrumb navigation is Home / Elements / Routing / SIP Entities. The left sidebar shows a menu with 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and has a 'General' section. A red box highlights the following fields:

- * Name: AACC-HA1
- * FQDN or IP Address: 10.10.97.52
- Type: Other (dropdown)
- Notes: SIP Entity for SIP AACC63

 Other visible fields include:

- Adaptation: (empty dropdown)
- Location: Belleville (dropdown)
- Time Zone: America/Toronto (dropdown)

 Buttons for 'Commit' and 'Cancel' are visible at the top right of the form area. The top right of the page shows 'Routing' and 'Home' tabs.

General section: For the Experience Portal SIP Entity, enter the following and use default values for the remaining fields:

- **Name**: Enter a descriptive name.
- **FQDN or IP Address**: Enter the IP address **10.10.97.234** of the Experience Portal interface.
- Select **Voice Portal** in the **Type** drop down menu.
- Enter a description in the **Notes** field if desired.
- Select the **Location Belleville** as configured in **Section 5.2**.
- Select the appropriate **Time Zone**.

The screen below shows the **Experience Portal SIP Entity Details**.

The screenshot displays the 'SIP Entity Details' configuration page. The left sidebar shows a navigation menu with 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and 'General'. The fields are as follows:

- Name**: Experience-Portal
- FQDN or IP Address**: 10.10.97.234
- Type**: Voice Portal
- Notes**: SIP Entity for Avaya Experience Po
- Adaptation**: (empty)
- Location**: Belleville
- Time Zone**: America/Toronto

Buttons for 'Commit' and 'Cancel' are visible in the top right corner.

5.4. Administer Entity Links

Entity Links define the connections between SIP Entities, in this case, Contact Center, Experience Portal and Session Manager. In the compliance test, the following entity links are defined from Session Manager.

- Session Manager ↔ Contact Center.
- Session Manager ↔ Experience Portal.

Navigate to **Routing** → **Entity Links** (not shown) and click on the **New** button to create a new entity link (screen not shown). Provide the following information:

- **Name**: Enter a descriptive name.
- In the **SIP Entity 1** drop down menu, select the Session Manager SIP Entity created in **Section Error! Reference source not found.** (e.g. **DevASM**).
- In the **Protocol** drop down menu, select the **TCP** protocol.
- In the **Port** field, enter the port to be used (e.g. **5060**).
- In the **SIP Entity 2** drop down menu, select **AACC-HA1** for the entity link between Session Manager and Contact Center and select **Experience-Portal** for the entity link between Session Manager and Experience Portal.
- In the **Port** field, enter the port to be used (e.g. **5060**).
- Check the **Trusted** box.
- Enter a description in the **Notes** field if desired.

Click on the **Commit** button to save each Entity Link definition. Repeat all the steps for each new SIP Entity Link.

The newly created entity link between Session Manager and Contact Center system is shown in the screen shot below.

The screenshot shows the 'Entity Links' configuration page. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Entity Links'. On the right side, there is a 'Help ?' link and two buttons: 'Commit' and 'Cancel'. Below this, the page title 'Entity Links' is displayed. A table with one item is shown, with columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, and Connection Policy. The table contains one row with the following values: Name: '* DevSM_AACC-HA1_5', SIP Entity 1: '* DevSM', Protocol: 'TCP', Port: '* 5060', SIP Entity 2: '* AACC-HA1', Port: '* 5060', and Connection Policy: 'trusted'. Below the table, there is a 'Select : All, None' option.

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	* DevSM_AACC-HA1_5	* DevSM	TCP	* 5060	* AACC-HA1	* 5060	trusted

The newly created entity link between Session Manager and Experience Portal system is shown in the screen shot below.

The screenshot shows the 'Entity Links' configuration page. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Entity Links'. On the right side, there is a 'Help ?' link and two buttons: 'Commit' and 'Cancel'. Below this, the page title 'Entity Links' is displayed. A table with one item is shown, with columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, and Connection Policy. The table contains one row with the following values: Name: '* DevSM_Experience-Portal', SIP Entity 1: '* DevSM', Protocol: 'TCP', Port: '* 5060', SIP Entity 2: '* Experience-Portal', Port: '* 5060', and Connection Policy: 'trusted'. Below the table, there is a 'Select : All, None' option.

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	* DevSM_Experience-Portal	* DevSM	TCP	* 5060	* Experience-Portal	* 5060	trusted

5.5. Administer Time Ranges

Time Ranges define admission control criteria to be specified for Routing Policies (**Section Error! Reference source not found.**). In the reference configuration, no restrictions were used.

To add a Time Range, navigate to **Routing**→**Time Ranges** (not shown), and click on the **New** button (screen not shown). Provide the following information:

- Enter a descriptive name in the **Name** field (e.g. **24/7**).
- Check each day of the week.
- In the **Start Time** field, enter **00:00**.
- In the **End Time** field, enter **23:59**.
- Enter a description in the **Notes** field if desired.

Click the **Commit** button. The following screen shows the Time Ranges page used during the compliance test.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The top navigation bar includes the Avaya logo, the product name, and user information (Last Logged on at May 13, 2013 4:11 PM, Help | About | Change Password | Log off admin). The main content area is titled 'Time Ranges' and features a sidebar with a navigation menu. The 'Time Ranges' menu item is highlighted. The main area contains a table with the following data:

	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
<input type="checkbox"/>	24/7	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7						

Below the table, there is a 'Select : All, None' option.

5.6. Administer Routing Policy

Routing Policies associate destination SIP Entities (**Section 5.3**) with Time of Day admission control parameters (**Section 5.5**) and Dial Patterns (**Section 5.7**). In the reference configuration, Routing Policies are defined for:

- Inbound calls to Contact Center.
- Inbound calls to Experience Portal.

To add a Routing Policy, navigate to **Routing** → **Routing Policies** (not shown) and click on the **New** button on the right (screen not shown). Provide the following information:

General section

- Enter a descriptive name in the **Name** field (e.g. **“To-AACC-HA1”, To-samwin**).
- Enter a description in the **Notes** field if desired.

SIP Entity as Destination section

- Click the **Select** button.
- Select the SIP Entity that will be the destination for this call.
- Click the **Select** button and return to the **Routing Policy Details** form.

Time of Day section

- Leave at default values.

Click **Commit** to save Routing Policy definition. Repeat the steps for each new Routing Policy.

The following screen shows the Routing Policy used for Contact Center during the compliance test.

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details Commit Cancel

General

* Name:

Disabled:

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
AACC-HA1	10.10.97.52	Other	SIP Entity for SIP AACC63

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Ranking ^	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7						

The following screen shows the Routing Policy used for Experience Portal during the compliance test.

The screenshot shows the 'Routing Policy Details' page for a policy named 'To-Experience-Portal'. The interface includes a left-hand navigation menu with 'Routing Policies' selected. The main content area is divided into sections: 'General', 'SIP Entity as Destination', and 'Time of Day'. In the 'General' section, the 'Name' is 'To-Experience-Portal', 'Disabled' is unchecked, 'Retries' is 0, and the 'Notes' are 'Route to Avaya Experience Portal'. The 'SIP Entity as Destination' section shows a table with one entry: 'Experience-Portal' with FQDN or IP Address '10.10.97.234', Type 'Voice Portal', and Notes 'SIP Entity for Avaya Experience Portal'. The 'Time of Day' section shows a table with one entry: '0' with Name '24/7', Start Time '00:00', End Time '23:59', and Notes 'Time Range 24/7'.

5.7. Administer Dial Patterns

Dial Patterns define digit strings to be matched for inbound and outbound call routing. In the compliance test, the following dial patterns are defined from Session Manager.

- **40xx** – dial pattern used to route calls to Contact Center.
- **44xxx** – dial pattern used to route calls to Experience Portal.

To add a Dial Pattern, select **Routing → Dial Patterns** (not shown) and click on the **New** button (screen not shown) in the right pane. Provide the following information:

General section

- Enter a unique pattern in the **Pattern** field (e.g. **40**).
- In the **Min** field enter the minimum number of digits (e.g. **4** or **5**).
- In the **Max** field enter the maximum number of digits (e.g. **5**).
- In the **SIP Domain** drop down menu select the domain **bwvdev.com** defined in **Section 5.1**.

Originating Locations and Routing Policies section

- Click on the **Add** button and a window will open (screen not shown).
- Click on the box for the appropriate Originating Locations, and Routing Policies (see **Section 5.7**) that pertain to this Dial Pattern.
 - Select the Originating Location to apply the selected routing policies to **All** originating locations.
 - Select appropriate Routing Policy.
 - Click on the **Select** button and return to the **Dial Pattern** page.

Click the **Commit** button to save the new definition. Repeat steps for remaining Dial Patterns.

The following screen shows the dial pattern **40xx** used to route calls to the Contact Center during the compliance test.

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details Commit Cancel

General

* Pattern: 40
 * Min: 4
 * Max: 4

Emergency Call:
 Emergency Priority: 1
 Emergency Type:
 SIP Domain: bvwdev.com
 Notes: Dial Pattern to SIP AACC63 HA1

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name ^	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		To-AACC-HA1		<input type="checkbox"/>	AACC-HA1	Route to SIP AACC63 HA1

The following screen shows the dial pattern **44xxx** used to route calls to the Experience Portal server during the compliance test.

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details Commit Cancel

General

* Pattern: 44
 * Min: 5
 * Max: 5

Emergency Call:
 Emergency Priority: 1
 Emergency Type:
 SIP Domain: bvwdev.com
 Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name ^	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		To-Experience-Portal		<input type="checkbox"/>	Experience-Portal	Route to Avaya Experience Portal

6. Configure Avaya Aura® Experience Portal

This document assumes that the Experience Portal is already installed and configured. This section describes the necessary configurations for the Experience Portal system to work with Session Manager, Communication Manager, Contact Center and iAssist Call Back Manager. For more information on how to configure the Experience Portal system, refer to **Section 11**. The following areas are configured:

- Administer VOIP Connections.
- Administer Applications.

6.1. Administer VoIP Connections

Experience Portal is configured via the Experience Portal Management (EPM) web interface. In order to access the web interface enter `http://<ip-addr>/` as the URL in an internet browser, where `<ip-addr>` is the IP address of the EPM (not shown). Log in using the administrator user role. The screen shown below is displayed.

The screenshot displays the Avaya Aura® Experience Portal 6.0 (ExperiencePortal) web interface. The header includes the Avaya logo, the user name 'Welcome, admin', and the last login time 'Last logged in yesterday at 7:35:44 AM EDT'. The navigation menu on the left lists various system management options such as User Management, Real-Time Monitoring, System Maintenance, System Management, System Configuration, Security, and Reports. The main content area features a breadcrumb trail 'You are here: Home' and a title 'Avaya Aura® Experience Portal Manager'. Below the title, there is a description of the EPM interface and its purpose. The 'Installed Components' section describes the Media Processing Platform (MPP). The 'Legal Notice' section contains copyright information and a disclaimer.

To add SIP connection, navigate to the **System Configuration → VoIP Connections** page and then click on the SIP tab (not shown). The **Add SIP Connection** page is displayed in the right. Enter a descriptive name in the **Name** field, select **Yes** option in the **Enable** field, select **TCP** in the Proxy Transport dropdown menu, select **Proxy Servers** radio option, enter IP address of Session Manager **10.10.97.198** in the **Address** field, **5060** in the **Port** and **Listener** fields, sip domain **bwvdev.com** in the **SIP Domain** field, and keep other fields at default. Click **Save** button to save and complete adding the new SIP connection.

AVAYA Welcome, admin
Last logged in today at 7:15:07 AM EDT

Avaya Aura® Experience Portal 6.0 (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**
 - MPP Manager
 - Software Upgrade
 - System Backup
- ▼ **System Configuration**
 - Alarm Codes
 - Alarm/Log Options
 - Applications
 - EPM Servers
 - MPP Servers
 - Report Data
 - SNMP
 - Speech Servers
 - VoIP Connections**
- ▼ **Security**
 - Certificates
 - Licensing
- ▼ **Reports**
 - Standard
 - Custom
 - Scheduled

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

Add SIP Connection

Use this page to add a new SIP connection.

Name:

Enable: Yes No

Proxy Transport:

Proxy Servers DNS SRV Domain

Address	Port	Priority	Weight	
<input type="text" value="10.10.97.198"/>	<input type="text" value="5060"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Remove

Additional Proxy Server

Listener Port:

SIP Domain:

P-Asserted-Identity:

Maximum Redirection Attempts:

Consultative Transfer: INVITE with REPLACES REFER

SIP Timers

T1: millisecond(s)

T2: millisecond(s)

B and F: millisecond(s)

Call Capacity

Maximum Simultaneous Calls:

All Calls can be either inbound or outbound

Configure number of inbound and outbound calls allowed

6.2. Administer iAssist Call Back Manager Applications

Two iAssist CBM applications are configured in Experience Portal, one to handle inbound calls and the second one to make outbound calls.

To configure inbound CBM application, navigate to **System Configuration** → **Applications**. The **Applications** page is displayed in the right, click on **Add** button to add a new application (not shown). In the **Add Applications** page, configure the application as shown below. Set the Type to **VoiceXML**, select **Single** for URL, and enter a VoiceXML URL provided by Acqueon. Select **Inbound** under **Application Launch** and provide Called Number **44000** as matched with the dial pattern in **Section 5.7**. Click **Save** button to save and complete adding the new inbound CBM application.

The screenshot displays the 'Add Application' configuration page in the Avaya Aura Experience Portal. The page is titled 'Add Application' and includes a breadcrumb trail: 'Home > System Configuration > Applications > Add Application'. The main content area is divided into several sections:

- Name:** iAssist_Inbound_CBM
- Enable:** Yes No
- Type:** VoiceXML
- URI:** Single Fail Over Load Balance
- VoiceXML URL:** http://10.10.97.19:8080/Inbound_CBM/Start (with a **Verify** button)
- 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: 44000 (with an **Add** button)
- A list containing '<No Called Number or Called URI configured>' (with a **Remove** button)
- Speech Parameters**, **Reporting Parameters**, and **Advanced Parameters** (all with expandable arrows)

At the bottom of the page, there are three buttons: **Save**, **Cancel**, and **Help**.

To configure an outbound CBM application, in the **Applications** page, click **Add** button to add another new application (not shown). The outbound CBM application uses the call control XML (CCXML) to make outbound call. Configure the application as the screen shown below. Click **Save** button to save and complete adding the new outbound CBM application.

AVAYA Welcome, admin
Last logged in yesterday at 11:37:17 AM EDT

Avaya Aura® Experience Portal 6.0 (ExperiencePortal) Home Help Logoff

Expand All | Collapse All

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

Add Application

Use this page to deploy and configure a new application on the Experience Portal system.

Name:

Enable: Yes No

Type:

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

Speech Parameters ▶
Reporting Parameters ▶
Advanced Parameters ▶

6.3. Administer Outcall Authentication

Configure the Outcall User Name and Password that will be sent by iAssist CBM. Click on EPM Servers in the left navigation pane. The EPM Servers is displayed in the right (not shown), click on EPM Settings to display the page below. Under the **Outcall** section, configure the **User Name** and **Password** used by iAssist CBM when it makes an outcall request to Experience Portal.

The screenshot shows the Avaya Aura Experience Portal 6.0 administration interface. The top navigation bar includes the Avaya logo, the user name 'admin', and the login time 'Last logged in today at 7:15:07 AM EDT'. The main header displays 'Avaya Aura® Experience Portal 6.0 (ExperiencePortal)' and navigation links for Home, Help, and Logoff. The left sidebar contains a navigation tree with categories like User Management, Real-Time Monitoring, System Maintenance, System Management, System Configuration, Security, and Reports. The 'EPM Servers' item under System Configuration is highlighted with a red box. The main content area shows the 'EPM Settings' page, which includes a breadcrumb trail: 'Home > System Configuration > EPM Servers > EPM Settings'. The page title is 'EPM Settings' and the description is 'Use this page to configure system parameters that affect the Experience Portal system.' The settings include: Experience Portal Name (ExperiencePortal), Number of Application Server Failover Logs (10), and Commands to Retain in Configuration History (50). There is a section for 'Resource Alerting Thresholds (%)' with 'High Water' and 'Low Water' settings (90 and 80 respectively). Below that is the 'Web Service Authentication' section, which includes 'Application Reporting' with fields for User Name (<Default>), Password (masked), and Verify Password. The 'Outcall' section, highlighted with a red box, contains fields for User Name (outcall), Password (masked), and Verify Password. At the bottom, there are buttons for 'Save', 'Apply', 'Cancel', and 'Help'.

7. Configure Avaya Aura® Contact Center

This document assumes that Contact Center system is already installed and configured. This section describes the necessary configurations for Contact Center to work with Session Manager and Experience Portal. For more information on how to configure Contact Center, refer to **Section 11**.

7.1. Administer SIP Connection

To configure a SIP trunk connection between Contact Center and Session Manager, from Contact Center Manager Server (CCMS) server, navigate to menu **Start → All Programs → Avaya → Contact Center → Manager Server → Server Configuration** (not shown). Enter the IP address **10.10.97.198** of Session Manager in the **Voice Proxy Server** field, **5060** in the **Port** field, and select **TCP** in the **Network Transport** field. The configuration is shown in the screen below.

The screenshot shows the 'Server Configuration' window for Avaya Contact Center. The title bar reads 'Server Configuration'. The Avaya logo is prominently displayed in red. Below the logo, the text 'Contact Center Server Configuration' is shown in red. On the left side, there is a 'Main Menu' tree with the following items: Local Settings, Licensing, SIP (expanded), Network Settings (highlighted), Local Subscriber, CCT Server, WS Open Interfaces, and Salesforce. The main area is titled 'SIP Network Settings' and contains several configuration fields:

	IP or FQDN	Port	Network Transport
<input checked="" type="checkbox"/> Voice Proxy Server	10.10.97.198	5060	TCP
Backup Voice Proxy Server			TCP
<input checked="" type="checkbox"/> CTI Proxy Server	10.10.98.17	4723	TLS
IM Proxy Server			TCP
IM Provider	Aura Presence Services		
XMPP Domain			

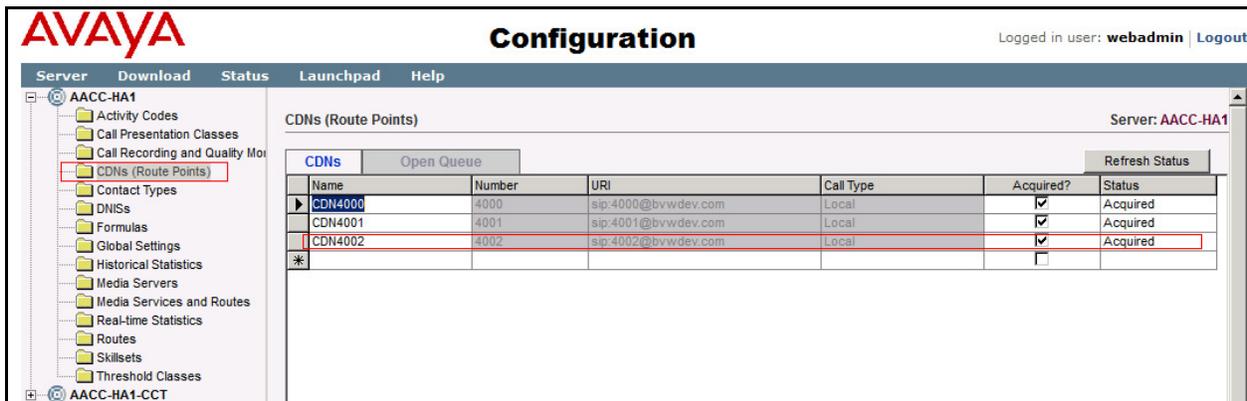
At the bottom right of the window, there are three buttons: 'Exit', 'Apply All', and 'OK'.

7.2. Administer CDN

The Controlled Directory Number (CDN) is used to route calls to Contact Center and it is configured via Contact Center Manager webpage. Log in the Contact Center Manager webpage (not shown), the screen below shows the homepage of Contact Center Manager Administrator.

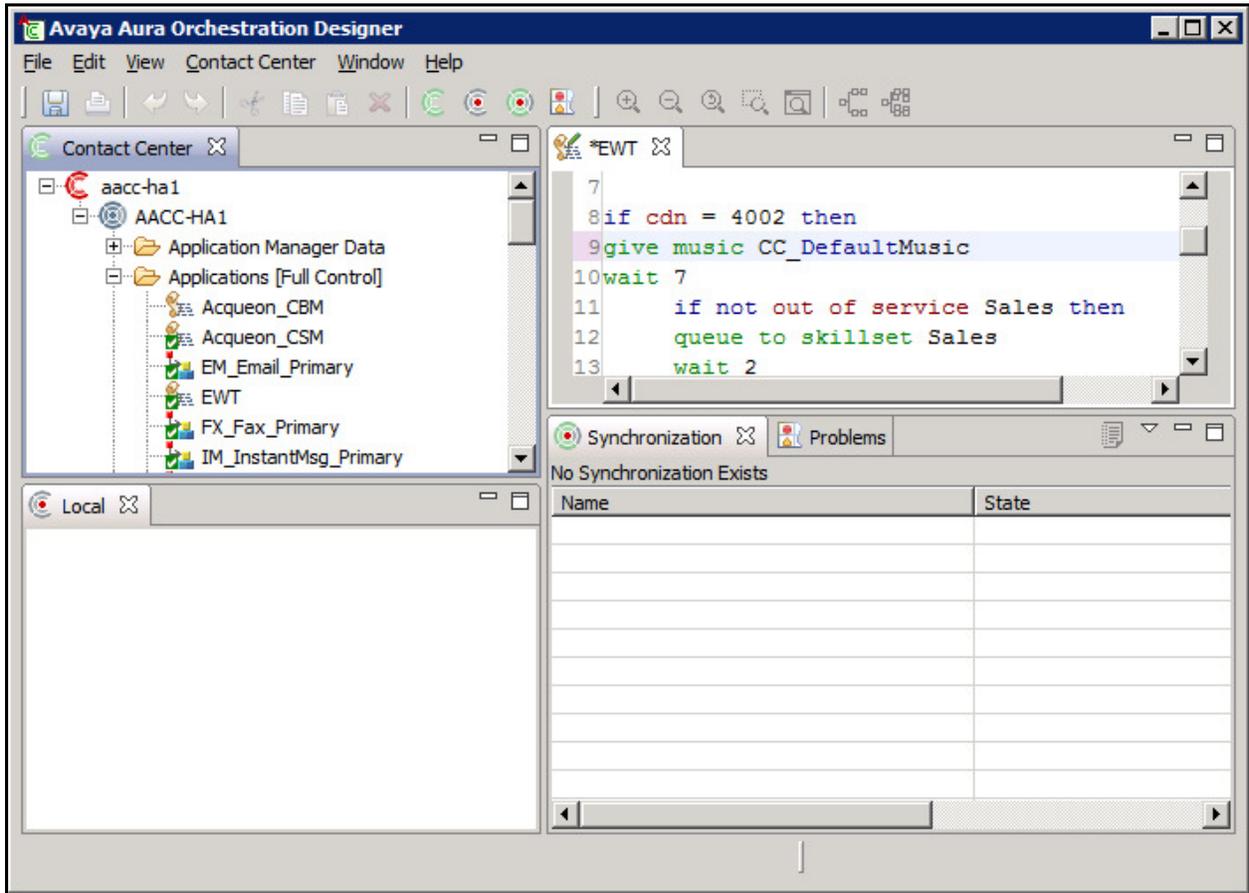


Click on **Configuration** link on the screen above to access to the **Configuration** page. In the left navigation pane, select **CDNs (Route Points)** under the **AACC-HA1** Contact Center. The **CDNs (Route Points)** page is displayed in the right. Create a CDN number **4002** and make sure it is acquired as shown in the screen below.



7.3. Administer Contact Center Scripting

From the homepage of Contact Center Manager, click on **Scripting** link. The scripting page is displayed (not shown), from the Scripting page, navigate to **Orchestration Designer** → **Launch Orchestration Designer**. Avaya Aura® Orchestration Designer application is launched as the screen below.



The following script is used for the compliance test. User dials Contact Center **CDN 4002**, user hears music for **7** seconds, and the call is then queued to **Default_Skillset** skillset if there is no agent available and the contact center calculate the expected wait time greater than **30** seconds it will route the call to Experience Portal with DN **44000** via SIP trunk. When the call comes in the Experience Portal, base on the DN 44000 the proper iAssist inbound CBM application will be launched and the user will interact with options whether the user wants to continue waiting in the queue to talk to agent or wants agent calls back. If the user decides to wait in the queue, the application will transfer the call back to Contact Center CDN 4002 and the user will continue to wait in the queue otherwise the CBM application collects the user's information and schedule a call back between agent and the user.

```
/* Acqueon_Inbound_CBM */
if cdn = 4002 then
give music CC_DefaultMusic
wait 7
    if not out of service Default_Skillset then
queue to skillset Default_Skillset
wait 2
    else disconnect
    end if
wait 2
Assign EXPECTED WAIT TIME Sales TO c_estimated_wait_time_cv
if (c_estimated_wait_time_cv > 30 ) then
route call 44000
else
    if not out of service Default_Skillset then
queue to skillset Default_Skillset
wait 3
    else disconnect
    end if
end if
end if
```

Please note that the process of assigning **CDN 4002** to the Application **Acqueon_Inbound_CBM** is not shown here but is described in the document *Avaya Aura® Contact Center Server Administration* outlined in **Section 11**.

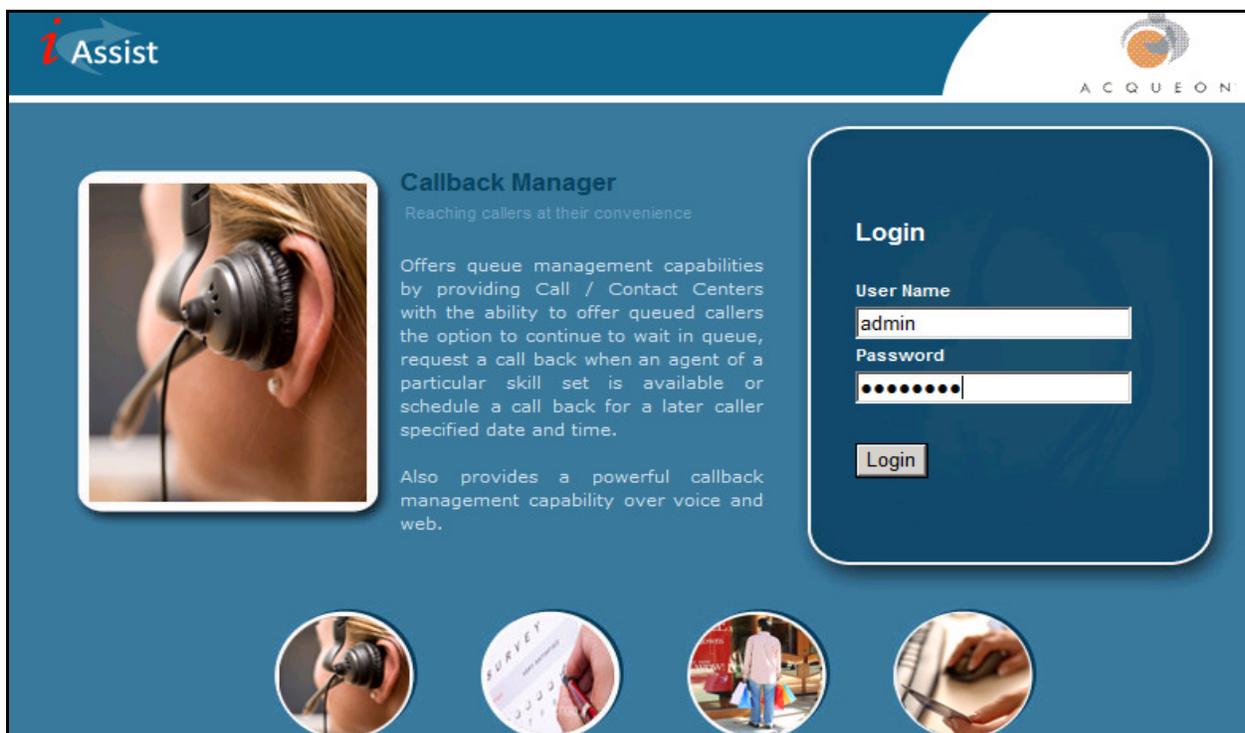
8. Configure Acqueon iAssist Call Back Manager

This section assumes that the iAssist server is already installed and configured by an Acqueon engineer. This guide provides necessary configuration on how to use the iAssist Admin application to administer the Call Back Manager (CBM) to work with Experience Portal and Contact Center systems. For more information on how to configure iAssist CBM application, refer to **Section 11**. The following areas are covered for iAssist CBM application.

- Administer Site.
- Administer Business Group.
- Administer Business Group Collection.
- Administer Call Flow Generator.
- Administer Application Configuration.
- Administer CBM Business Group Configuration.

8.1. Administer Site

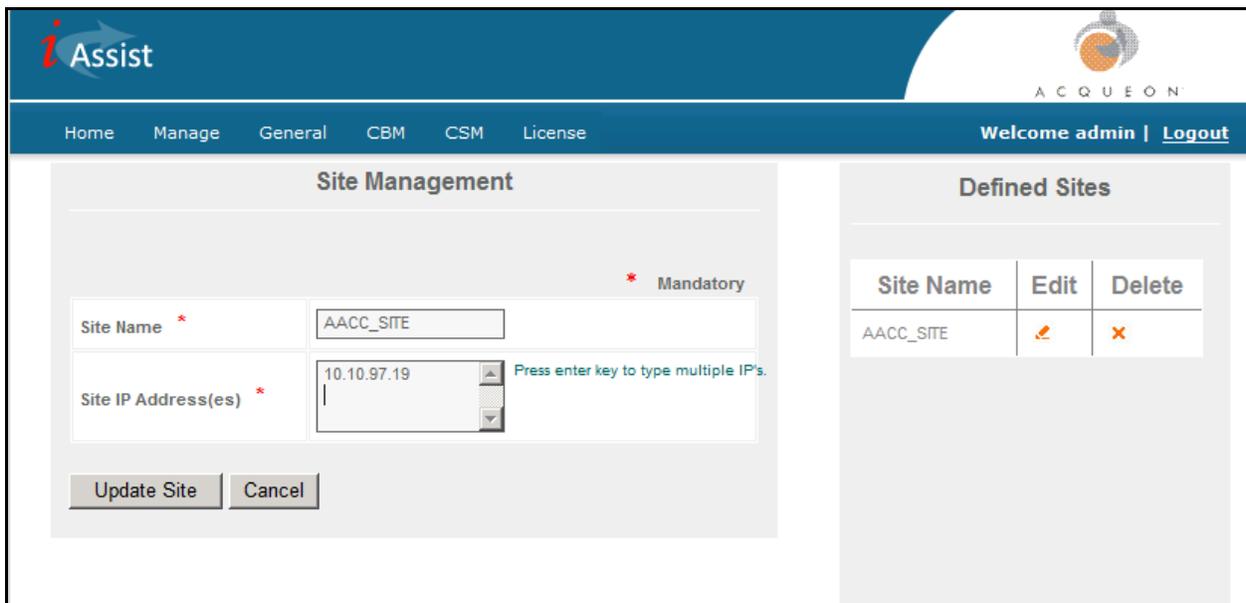
The iAssist application is web-based application. To configure the iAssist application, launch Microsoft Internet browser and enter IP address of the iAssist application into the address bar. The screen below shows the iAssist login page.



Enter the proper credentials to log in the iAssist application. The screen below shows the homepage of the iAssist application.



To administer a site on the iAssist application, navigate to **General** → **Site**. The **Site Management** page is displayed, and click on **Create Site** (not shown) button to create a new site. The screen below shows configuration for the new site, the **Site Name** is **AACC_SITE** and the **Site IP Address(es)** is **10.10.97.19** this is IP address of iAssist server.



8.2. Administer Business Group

To administer a business group, from the homepage of the iAssist application, navigate to **Generate** → **Business Group** (not shown). The **Business Group Management** page is displayed and click on **Create Business Group** button (not shown) to create a new business group. The screen below show the configurations for the new business group, enter name as **AACC_IN_CBM_44000**, the incoming number as **44000** matched with the dial pattern 44xxx which is defined for Experience Portal in **Section 5.7** and select the site **AACC_SITE** which is created in **Section 8.1**.

The screenshot displays the 'BusinessGroup Management' interface. The top navigation bar includes 'Home', 'Manage', 'General', 'CBM', 'CSM', and 'License'. The user is logged in as 'admin' and can click 'Logout'. The main content area is divided into two sections:

BusinessGroup Management

* Mandatory

Business Group Name *	<input type="text" value="AACC_IN_CBM_44000"/>
Incoming Number *	<input type="text" value="44000"/>
Site	<input type="text" value="AACC_SITE"/>
Language	<input type="text" value="US English"/>
IVR Configuration Template	<input type="text" value="DEFAULT_CBM_CONFIG"/>

Buttons: Close, Clear

Defined Business Group(s)

Business Group	Edit	Delete
AACC_IN_CBM_44000		
AACC_IN_CSM_44001		
BG_FOR_0Question		

8.3. Administer Business Group Collections

To administer a business group, from the homepage of the iAssist application, navigate to **Generate** → **Business Group Collections**. The **Business Group Collections** page is displayed and click on **Create** button (not shown) to create a new business group collection. The screen below shows configurations for the new business group collections. Select the **AACC_SITE** defined in **Section 8.1** in the **Site** field, enter a descriptive name e.g. **Test_CBM_BGC** in the **Business Group Collection**, select **CallBack Manager** in the **Application** field and select the **AACC_IN_CBM_44000** business group defined in **Section 8.2** in the **Business Group** field.

The screenshot displays the 'Business Group Collections' configuration page in the iAssist application. The page header includes the iAssist logo and navigation tabs: Home, Manage, General, CBM, CSM, License. The user is logged in as 'admin'.

The main configuration area is titled 'Business Group Collections' and includes a 'Mandatory' indicator. The fields are as follows:

- Site ***: AACC_SITE (dropdown menu)
- Business Group Collection ***: Test_CBM_BGC (text input)
- Application ***: Callback Manager (dropdown menu)
- BusinessGroups ***: AACC_IN_CBM_44000 (checkbox and dropdown menu)

At the bottom of the form are 'Update' and 'Cancel' buttons.

On the right side, there is a section titled 'Defined Business Group Collections' containing a table:

Name	Edit	Delete
Test_CBM_BGC		
Test_CSM_BGC		

8.4. Administer Call Flow Generator

To administer a call flow generator, from the homepage of the iAssist application, navigate to **Generate → Call Flow Generator**. The **Call Flow Generator** page is displayed and click on **Generate CallFlow** button (not shown) to create a new call flow. There are two call flows created for the Call Back Manager: one for inbound calls and one for outbound calls.

The screen below shows the configuration for the new inbound call flow.

The screenshot shows the iAssist application interface. The top navigation bar includes 'Home', 'Manage', 'General', 'CBM', 'CSM', and 'License'. The user is logged in as 'admin'. The main content area is titled 'Call Flow Generator' and contains a form with the following fields:

- CallFlow Name ***: AACC_IN_CBM_DEMO
- Site ***: AACC_SITE
- Application**: CBM - Inbound
- FilterType ***: By BusinessGroupID (selected)
- Business Group ***: A list of business groups with 'AACC_IN_CBM_44000' selected.

A red box highlights the 'CallFlow Name', 'Site', and 'Application' fields. A 'Mandatory' label is present next to the 'CallFlow Name' field. To the right, a 'Defined CallFlow(s)' table lists existing call flows:

CallFlow	Edit	Delete
AACC_IN_CBM_DEMO		
AACC_OUT_CBM		
AACC_IN_CSM		
AACC_OUT_CSM		

The screen below shows the configurations for the new outbound call flow.

The screenshot shows the iAssist application interface. The top navigation bar includes 'Home', 'Manage', 'General', 'CBM', 'CSM', and 'License'. The user is logged in as 'admin'. The main content area is titled 'Call Flow Generator' and contains a form with the following fields:

- CallFlow Name ***: AACC_OUT_CBM
- Site ***: AACC_SITE
- Application**: CBM - Outbound
- FilterType ***: By BusinessGroupID (selected)
- Business Group ***: A list of business groups with 'AACC_IN_CBM_44000' selected.

A red box highlights the 'CallFlow Name', 'Site', and 'Application' fields. A 'Mandatory' label is present next to the 'CallFlow Name' field. To the right, a 'Defined CallFlow(s)' table lists existing call flows:

CallFlow	Edit	Delete
AACC_IN_CBM_DEMO		
AACC_OUT_CBM		
AACC_IN_CSM		
AACC_OUT_CSM		

8.5. Administer Application Configurations

To administer the application configurations, from the homepage of the iAssist application, navigate to **Generate** → **Application Configurations** (not shown). The **Application Configuration** page is displayed and click on **DEFAULT_CBM_CONFIG** to update the configuration for the CBM application. The screen below shows the application configurations for the CBM. Enter the **outcall** username and its password as defined in **Section 6.3** in the **Avaya VPMS User name for outcall** and **Avaya VPMS Password for outcall**.

Application Configurations

Defined Configuration(s)

Config Group	Edit	Delete
DEFAULT_CBM_CONFIG		
DEFAULT_CSM_CONFIG		

Application Configuration Details:

Config Group: DEFAULT_CBM_CONFIG (Mandatory)

Description:

Key:

Value:

Update Config | Cancel

Indicates whether the call is CTI Call or not	Y	
Denotes the CBM module type; values: CCXML, CTI	CCXML	
Avaya VPMS User name for outcall	outcall	
Avaya VPMS Password for outcall	outcall123	
Avaya VPMS timeout	60000	
Avaya VPMS Outbound Application name to	IASSIST_CBM_OUTBOUND	

Save | Save As | ConfigName: | Cancel

Scroll down to the **Possible values are: H323 OR SIP**, and set it to **SIP** and enter the Session Manager IP address **10.10.97.198** in the **SES IP to be used for SIP Calls**.

Possible values are : H323 OR SIP	<input type="text" value="SIP"/>	
SES IP to be used for SIP Calls	<input type="text" value="10.10.97.198"/>	

8.6. Administer CBM Business Group Configuration

The business group **AACC_IN_CBM_44000** is already defined in **Section 8.2**. This section provides more detail configuration for CBM application. To administer the business group configuration for CBM, from the homepage of the iAssist application, navigate to **CBM → Business Group Configuration** (not shown). The Business Group Configuration page is displayed. The business group **AACC_IN_CBM_44000** consists of 8 sections to be configured however in this section just shows 2 important sections to the compliance test.

The Screen below shows the CBM – Business Group Configurations. Enter the IP address of Experience Portal server **10.10.97.234** in the **IVR IP address**, the Contact Center CDN **4002** in the **Outgoing Number** and **Error VDN** fields, and keep other fields at default.

The screenshot displays the iAssist application interface for configuring a Business Group. The main configuration area is titled "CBM - Business Group Configuration [AACC_IN_CBM_44000]". It contains several fields, with three highlighted by red boxes: "Outgoing Number" (4002), "IVR IP Address" (10.10.97.234), and "Error VDN" (4002). Other fields include "Business Group Name" (AACC_IN_CBM_44000), "High Priority Queue" (checkbox), "High Priority Queue VDN", "Time Zone" (UTC-05:00 Eastern Time (US & Canada)), "Priority" (HIGH), "UI Data processing" (checkbox), and "RealTime Queue". Below the main configuration area are several expandable sections: "Business Hour and Break Hour", "Holiday", "Timezones", "Time Slots", "SLA Config", and "Config Options". At the bottom are "Update Business Group" and "Cancel" buttons. On the right, a "Defined Business Group(s)" table lists the group AACC_IN_CBM_44000 with an "Edit" button.

Business Group	Edit
AACC_IN_CBM_44000	

Expand the **Config Options** tab, in the **Callback Options** sub-tab check options that are shown in the screen below.

The screenshot displays the iAssist web application interface. At the top, the 'iAssist' logo is on the left, and the 'ACQUEON' logo is on the right. Below the logo is a navigation bar with links for 'Home', 'Manage', 'General', 'CBM', 'CSM', and 'License'. On the right side of the navigation bar, it says 'Welcome admin | Logout'.

The main content area is divided into two columns. The left column contains a list of configuration tabs: 'CBM - Business Group Configuration [AACC_IN_CBM_44000]', 'RealTime Queue', 'Business Hour and Break Hour', 'Holiday', 'Timezones', 'Time Slots', 'SLA Config', and 'Config Options'. The 'Config Options' tab is expanded, showing sub-tabs: 'Callback Options', 'Duplicate Filter', 'Outbound Configuration', and 'Failure Outcomes'. The 'Callback Options' sub-tab is active, displaying a 'Hidden' section with a list of options and checkboxes:

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"/>

A red box highlights the first five options. Below this list are 'Update Business Group' and 'Cancel' buttons.

The right column is titled 'Defined Business Group(s)' and contains a table with the following data:

Business Group	Edit
AACC_IN_CBM_44000	

9. Verification Steps

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

- From the left navigation pane of EPM web interface, navigate to **Real-Time Monitoring** → **System Monitor** and verify that the MPP server is online and running in the System Monitor page shown below.

System Monitor (Jul 29, 2013 11:41:13 AM EDT) Refresh

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: Jul 29, 2013 11:41:08 AM EDT

Server Name	Type	Mode	State	Config	Call Capacity			Active Calls		Calls Today	Alarms
					Current	Licensed	Maximum	In	Out		
EPM / MPP	EPM/MPP	Online	Running	OK	20	20	50	0	0	2	
Summary					20	20	50	0	0	2	

[Help](#)

- From the left navigation pane of EPM web interface, navigate to **Real-Time Monitoring** → **Port Distribution** and verify that the ports on the MPP server are in-service in the **Port Distribution** page shown below. Note that the CBM application only uses SIP trunk for inbound and outbound calls, the H.323 trunk in the screen below is not applied for this document.

Port Distribution (Jul 29, 2013 11:43:35 AM EDT) Refresh

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: 20 Last Poll: Jul 29, 2013 11:43:30 AM EDT

Port	Mode	State	Port Group	Protocol	Current Allocation	Base Allocation
53060	Online	In service	H323_Trunk	H323	MPP	
53061	Online	In service	H323_Trunk	H323	MPP	
53062	Online	In service	H323_Trunk	H323	MPP	
53063	Online	In service	H323_Trunk	H323	MPP	
53064	Online	In service	H323_Trunk	H323	MPP	
1	Online	In service	DevSM	SIP_Trunk	MPP	
2	Online	In service	DevSM	SIP_Trunk	MPP	
3	Online	In service	DevSM	SIP_Trunk	MPP	
4	Online	In service	DevSM	SIP_Trunk	MPP	
5	Online	In service	DevSM	SIP_Trunk	MPP	
6	Online	In service	DevSM	SIP_Trunk	MPP	
7	Online	In service	DevSM	SIP_Trunk	MPP	
8	Online	In service	DevSM	SIP_Trunk	MPP	
9	Online	In service	DevSM	SIP_Trunk	MPP	
10	Online	In service	DevSM	SIP_Trunk	MPP	
11	Online	In service	DevSM	SIP_Trunk	MPP	
12	Online	In service	DevSM	SIP_Trunk	MPP	
13	Online	In service	DevSM	SIP_Trunk	MPP	
14	Online	In service	DevSM	SIP_Trunk	MPP	
15	Online	In service	DevSM	SIP_Trunk	MPP	

- Place inbound call to Contact Center CDN 4002, the call is then routed to Experience Portal with DN 44000 based on the Expected wait time in the agent queue. While the call is connected to Experience Portal and launch the iAssist inbound CBM application, **navigate to Real-Time Monitoring → Active Calls** and check **Active Calls** in the Experience Portal, there should be one call presented.

Active Calls (Jul 30, 2013 12:10:44 PM EDT) Refresh										
This page displays the status of all the active calls being handled by the Experience Portal system.										
Total Active Calls: 1 Last Poll: Jul 30, 2013 12:10:42 PM EDT										
Port	Port Group	Protocol	Call Type	MPP Server	Start Time	Calling Number/URI	Called Number/URI	Application	ASR Server	TTS Server
1	DevSM	SIP_Trunk	Inbound	MPP	Jul 30, 2013 12:10:41 PM EDT	sip:16139675288@bvwddev.com	sip:44000@bvwddev.com	iAssist_Inbound_CBM		

- To run a report for the call back request, navigate to **CBM → Report**. The detailed call back request report shows as the screen below.

Main Report										
DETAILED CALLBACK REQUEST REPORT										
From: 07/30/2013			To: 07/30/2013				Site: AACC_SITE			
Record Number	Callback Number	Customer ID	Request Type	Status	Request Received Time	Callback Requested Time	Time of Last Attempt Made	Agent Attempts	Customer Attempts	
Business Group AACC_IN_CBM_44000					Outgoing Number :4002					
1	16139675288	11111	As soon as agent available	Pending	07/30/2013 04:15:50 PM	07/30/2013 04:15:50 PM		0	0	

10. Conclusion

These Application Notes describe the configuration steps required to integrate the Acqueon iAssist Call Back Manager application with Avaya Aura® Experience Portal and Avaya Aura® Contact Center. All feature and serviceability test cases were completed successfully.

11. Additional References

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

- [1] Administering Avaya Aura® Experience Portal, April 2012.
- [2] Administering Avaya Aura® Communication Manager, Release 6.3, Document 03-300509, Issue 7.0, June 2013.
- [3] Administering Avaya Aura® Session Manager, Release 6.3, Issue 2, Jun 2013.
- [4] Avaya Aura® Contact Center Server Administration, Release 6.3, Issue 04.02, Document NN44400-610, May 2013.
- [5] iAssist CBM 2.0 Admin Guide.

©2013 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.