



## **Application Notes for OpenMethods Harmony 4.0 with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1 using Oracle Service Cloud – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for OpenMethods Harmony 4.0 to interoperate with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1 using Oracle Service Cloud. OpenMethods Harmony is a CRM CTI connector that bridges the customer telephony system with the Oracle Service Cloud product suite.

In the compliance testing, OpenMethods Harmony used the Java Telephony Application Programming Interface and the Device, Media, and Call Control interface from Avaya Aura® Application Enablement Services to monitor contact center agents on Avaya Aura® Communication Manager, to provide screen pop and channel work item control features from the agent desktops connected to Oracle Service Cloud.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

These Application Notes describe the configuration steps required for OpenMethods Harmony 4.0 to interoperate with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1 using Oracle Service Cloud. Harmony is a CRM CTI connector that bridges the customer telephony system with the Oracle Service Cloud product suite.

In the compliance testing, Harmony used the Java Telephony Application Programming Interface (JTAPI) and the Device, Media, and Call Control (DMCC) .Net interface from Application Enablement Services to monitor contact center agents on Communication Manager, to provide screen pop and channel work item control features from agent desktops connected to Oracle Service Cloud via the Oracle Service Cloud CX Desktop application.

JTAPI is a client-side interface to the Telephony Services Application Programmer Interface (TSAPI) on Application Enablement Services. As such, these Application Notes will describe the required configurations for creation and connectivity to the TSAPI service.

The Harmony solution consisted of the Integration Server, Queue Adapter, MediaBar, and PopFlow components. The MediaBar and PopFlow components resided on the Oracle Service Cloud, and interfaced with Oracle Service Cloud CX Desktop running on the agent desktops to facilitate screen pop and control of channel work items. The Integration Server and Queue Adapter components resided on the same Harmony server in the compliance testing.

The Integration Server component used JTAPI to integrate with Application Enablement Services, to monitor agent station extensions, support of screen pop, and control of voice, email, and chat work items from the agent desktops.

The Queue Adapter component used DMCC to integrate with Application Enablement Services, along with use of the Administration Without Hardware (AWOH) feature on Communication Manager for initiation of phantom calls for email and chat work items. Phantom calls were initiated from the applicable hunt group of email or chat AWOH stations as calling party and the applicable skill group for email or chat as destination.

The compliance testing used the basic default PopFlow, which supports one active work item at the agent at any time. In addition, the basic default PopFlow does not support population of DNIS at the answering agent desktop, nor population of original ANI, original DNIS, and original customer contact record at the transfer-to/conference-to agent desktops. The full PopFlow product was outside the scope of this compliance test.

## 2. General Test Approach and Test Results

The feature test cases were performed manually. Upon an agent logging into Harmony, the application used JTAPI/TSAPI to query agent state, logged the agent into the ACD on Communication Manager if needed, and requested device monitoring.

For manual part of the testing, incoming ACD calls were placed from the PSTN with available agents that have desktops running the Oracle Service Cloud CX Desktop application. All necessary call actions were initiated from the agent desktops and/or telephones. The email and chat work items were initiated from the Internet, via the URLs provided by OpenMethods.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the Harmony server.

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

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

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

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

## 2.1. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing.

The feature testing focused on verifying the following on Harmony:

- Use of DMCC device and call control services to support initiation and clearing of phantom calls and support of UUI data for email and chat work items.
- Handling of JTAPI/TSAPI messages in the areas of event notifications, value queries, and set agent states.
- Use of JTAPI/TSAPI call control services to support call control actions such as answer and transfer from agent desktops.
- Proper handling of call scenarios involving inbound, outbound, internal, external, ACD, non-ACD, screen pop, drop, hold/resume, multiple calls, multiple agents, conference, transfer, long duration, send DTMF, pending aux work, and reason codes.
- Proper handling of email and chat scenarios involving screen pop, accept, and close.

The serviceability testing focused on verifying the ability of Harmony to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to Harmony.

## 2.2. Test Results

All test cases were executed and verified. The following were observations on Harmony from the compliance testing.

- After an agent accepted the phantom call associated with an email or chat work item, Harmony automatically held the phantom call by design. This design did not appear to have any adverse impact other than flickering of the associated call appearance light at the agent telephone, and possible long hold reminder calls when configured on Communication Manager.
- Upon ending the call associated with a voice work item, the agent desktop showed **HandlingInteraction** despite agent considered to be available by Communication Manager. While in this state, subsequent calls can still be delivered and answered by agent. Per Harmony design, the agent needs to select the **Complete the current interaction** icon post handling of voice work item, in order for **Available** to be reflected.
- Upon selecting an aux work reason code such as **Lunch** from the agent desktop, the desktop reflected **Unavailable** per Harmony design.

## 2.3. Support

Technical support on Harmony can be obtained through the following:

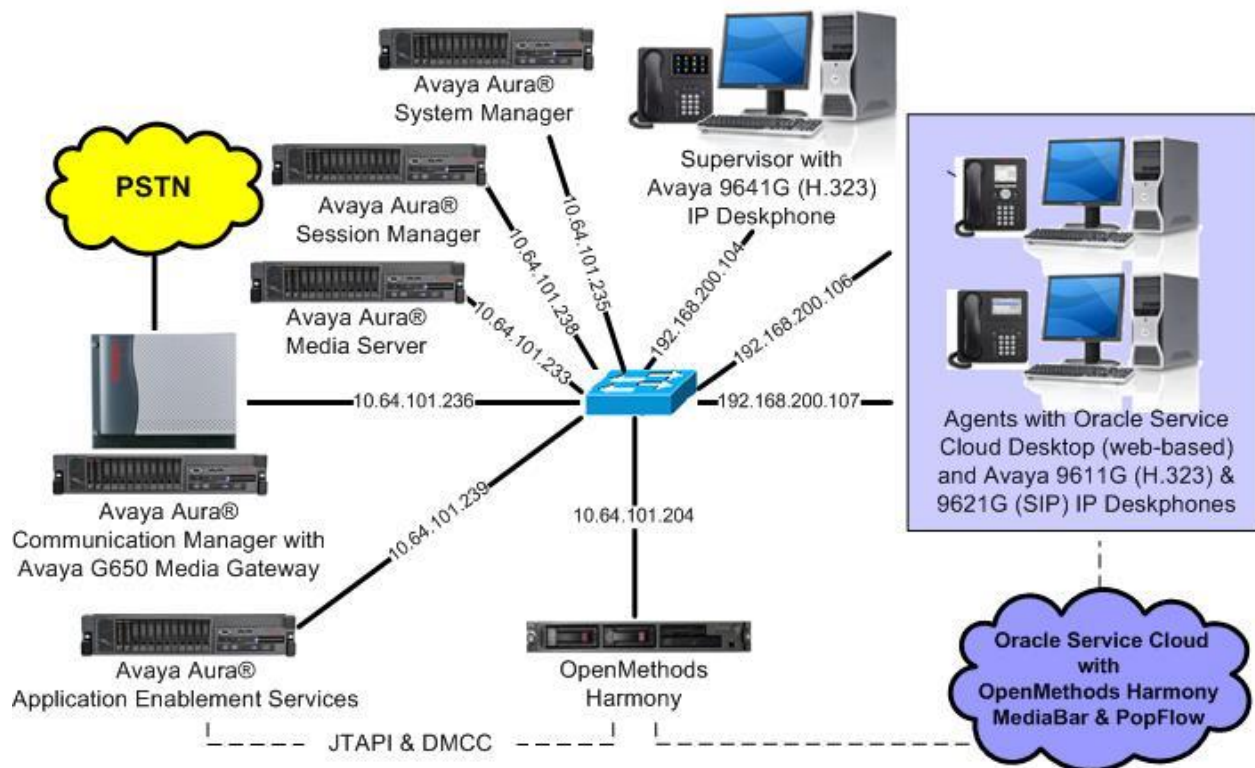
- **Phone:** (816) 283-8965, extension 1
- **Email:** [care@openmethods.com](mailto:care@openmethods.com)
- **Web:** [www.openmethods.com](http://www.openmethods.com)

### 3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of contact center devices are not the focus of these Application Notes and will not be described.

In the compliance testing, Harmony monitored the agent stations shown in the table below.

Device Type	Number
Supervisor Station	65000
Agent Stations	65001, 66002
Agent IDs	65881, 65882
Agent Passwords	65881, 65882



**Figure 1: Compliance Testing Configuration**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	7.1.1 (7.1.1.0.0.532.23985)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	7.8.0.333
Avaya Aura® Application Enablement Services in Virtual Environment	7.1.1 (7.1.1.0.0.5-0)
Avaya Aura® Session Manager in Virtual Environment	7.1.1 (7.1.1.0.711008)
Avaya Aura® System Manager in Virtual Environment	7.1 .1 (7.1.1.0.046931)
Avaya 9611G and 9641G IP Deskphones (H.323)	6.6506
Avaya 9621G IP Deskphone (SIP)	7.1.0.1.1
OpenMethods Harmony on Microsoft Windows Server 2012 <ul style="list-style-type: none"> <li>Integration Server</li> <li>QueueAdapter</li> <li>Avaya JTAPI SDK</li> <li>DMCC .Net (ServiceProvider.dll)</li> </ul>	4.0.164.0 R2 Standard 4.0.164.01.20171031729 Hot Fix 1 4.0.164.0 6.3.3.26 6.3.3.14
Oracle Service Cloud CX Desktop on Microsoft Windows 10 Pro	16.11.0.272
OpenMethods Harmony MediaBar and OpenMethods Harmony PopFlow on Oracle Service Cloud	4.0.164.0 4.0.164.0 16.11.0.272

## 5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Obtain reason codes
- Administer system parameters features
- Administer AWOH stations
- Administer AWOH hunt groups
- Administer email and chat skills
- Administer agent IDs

### 5.1. Verify License

Log into the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command. On **Page 1**, verify that there is sufficient capacity for AWOH stations by comparing the **Maximum Stations** field value with the corresponding value in the **USED** column.

display system-parameters customer-options		Page 1 of 12
OPTIONAL FEATURES		
G3 Version: V17	Software Package: Enterprise	
Location: 2	System ID (SID): 1	
Platform: 28	Module ID (MID): 1	
USED		
Platform Maximum Ports:		65000 197
Maximum Stations:		41000 22
Maximum XMOBILE Stations:		41000 0

Navigate to **Page 4**, and verify that the **Computer Telephony Adjunct Links** customer option is set to “y”. If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.

display system-parameters customer-options		Page 4 of 12
OPTIONAL FEATURES		
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? y	
Access Security Gateway (ASG)? n	Authorization Codes? y	
Analog Trunk Incoming Call ID? y	CAS Branch? n	
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n	
Answer Supervision by Call Classifier? y	Change COR by FAC? n	
ARS? y	<b>Computer Telephony Adjunct Links? y</b>	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? n	DCS (Basic)? y	
ASAI Link Core Capabilities? y	DCS Call Coverage? y	
ASAI Link Plus Capabilities? y	DCS with Rerouting? y	



## 5.2. Administer CTI Link

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

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

## 5.3. Obtain Reason Codes

For contact centers that use reason codes, enter the “change reason-code-names” command to display the configured reason codes. Make a note of the **Aux Work** reason codes, which will be used later to configure Harmony.

```
change reason-code-names                           Page 1 of 1
REASON CODE NAMES
Aux Work/ Logout
Interruptible?
Reason Code 1: Lunch /n Finished Shift
Reason Code 2: Coffee /n
Reason Code 3: /n
Reason Code 4: /n
Reason Code 5: /n
Reason Code 6: /n
Reason Code 7: /n Other
Reason Code 8: /n
Reason Code 9: /n
Default Reason Code:
```

## 5.4. Administer System Parameters Features

Use the “change system-parameters features” command to enable **Create Universal Call ID (UCID)**, which is located on **Page 5**. For **UCID Network Node ID**, enter an available node ID.

```
change system-parameters features                                     Page 5 of 19
                                FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:                      Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                                Switch Name:
  Emergency Extension Forwarding (min): 10
  Enable Inter-Gateway Alternate Routing? n
  Enable Dial Plan Transparency in Survivable Mode? n
                                COR to Use for DPT: station
                                EC500 Routing in Survivable Mode: dpt-then-ec500
MALICIOUS CALL TRACE PARAMETERS
  Apply MCT Warning Tone? n      MCT Voice Recorder Trunk Group:
  Delay Sending RElease (seconds): 0
SEND ALL CALLS OPTIONS
  Send All Calls Applies to: station  Auto Inspect on Send All Calls? n
  Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
  Create Universal Call ID (UCID)? y    UCID Network Node ID: 27
```

Navigate to **Page 13**, and enable **Send UCID to ASAI**. This parameter allows for the universal call ID to be sent to Harmony.

```
change system-parameters features                                     Page 13 of 19
                                FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER MISCELLANEOUS
  Callr-info Display Timer (sec): 10
                                Clear Callr-info: next-call
  Allow Ringer-off with Auto-Answer? n

  Reporting for PC Non-Predictive Calls? n

  Agent/Caller Disconnect Tones? n
  Interruptible Aux Notification Timer (sec): 3
  Zip Tone Burst for Callmaster Endpoints: double

ASAI
  Copy ASAI UII During Conference/Transfer? n
  Call Classification After Answer Supervision? y
                                Send UCID to ASAI? y
  For ASAI Send DTMF Tone to Call Originator? y
  Send Connect Event to ASAI For Announcement Answer? n
  Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```

## 5.5. Administer AWOH Stations

Add an AWOH station using the “add station n” command, where “n” is an available extension number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Extension:** The available extension number.
- **Port:** “X”
- **Name:** A descriptive name.

```
add station 63991
```

Page 1 of 5

STATION		
<b>Extension: 63991</b>	Lock Messages? n	BCC: 0
Type: 6408D+	Security Code:	TN: 1
<b>Port: x</b>	Coverage Path 1:	COR: 1
<b>Name: Email AWOH 1</b>	Coverage Path 2:	COS: 1
	Hunt-to Station:	

STATION OPTIONS

Loss Group: 2	Time of Day Lock Table:
Data Module? n	Personalized Ringing Pattern: 1
Speakerphone: 2-way	Message Lamp Ext: 63991
Display Language: english	Mute Button Enabled? y
Survivable COR: internal	Media Complex Ext:
Survivable Trunk Dest? y	IP SoftPhone? n
	Remote Office Phone? n
	IP Video? n

Repeat this section to administer the desired number of AWOH stations, to be used as originators of phantom calls for email and chat work items. The number of AWOH stations configured should correspond to the desired number of simultaneous email and chat work items.

In the compliance testing, two AWOH stations with extensions 63991-63992 were configured as originators of phantom calls for email, two AWOH stations with extensions 64991-64992 were configured as originators of phantom calls for chat, as shown below.

```
list station 63991 count 4
```

STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ TN Jack		
63991	X	Email AWOH 1				1			
	6408D+		no			1			
63992	X	Email AWOH 2				1			
	6408D+		no			1			
64991	X	Chat AWOH 1				1			
	6408D+		no			1			
64992	X	Chat AWOH 2				1			
	6408D+		no			1			

## 5.6. Administer AWOH Hunt Groups

Administer a hunt group to be used for origination of phantom calls for email work items. Use the “add hunt-group n” command, where “n” is an available hunt group number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Number:** The available group number.
- **Group Name:** A descriptive name.
- **Group Extension:** An available extension number.

add hunt-group 33		Page 1 of 60	
HUNT GROUP			
Group Number: 33		ACD? n	
Group Name: Email AWOH		Queue? n	
Group Extension: 63333		Vector? n	
Group Type: ucd-mia		Coverage Path:	
TN: 1		Night Service Destination:	
COR: 1		MM Early Answer? n	
Security Code:		Local Agent Preference? n	
ISDN/SIP Caller Display:			

Navigate to **Page 3**, and enter the extensions of all AWOH station extensions for email from **Section 5.5** as members. Harmony will use this group as originator of phantom calls for email work items.

add hunt-group 33		Page 3 of 60	
HUNT GROUP			
Group Number: 33		Group Extension: 63333	
Group Type: ucd-mia			
Member Range Allowed: 1 - 1500		Administered Members (min/max): 0 /0	
Total Administered Members: 0			
GROUP MEMBER ASSIGNMENTS			
Ext	Name(19 characters)	Ext	Name(19 characters)
1: 63991		14:	
2: 63992		15:	
3:		16:	

Repeat this section to administer another hunt group for origination of phantom calls for chat work items, with AWOH station extensions for chat from **Section 5.5** as members, as shown below.

add hunt-group 44		Page 3 of 60	
HUNT GROUP			
Group Number: 44		Group Extension: 64444	
Group Type: ucd-mia			
Member Range Allowed: 1 - 1500		Administered Members (min/max): 0 /0	
Total Administered Members: 0			
GROUP MEMBER ASSIGNMENTS			
Ext	Name(19 characters)	Ext	Name(19 characters)
1: 64991		14:	
2: 64992		15:	
3:		16:	

## 5.7. Administer Email and Chat Skills

Administer a skill group to be used for routing of phantom calls for email work items to agents. Use the “add hunt-group n” command, where “n” is an available hunt group number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

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

```
add hunt-group 3
```

Page 1 of 4

HUNT GROUP

<b>Group Number:</b> 3	<b>ACD?</b> y
<b>Group Name:</b> Email Skill	<b>Queue?</b> y
<b>Group Extension:</b> 63101	<b>Vector?</b> y
Group Type: ucd-mia	
TN: 1	
COR: 1	MM Early Answer? n
Security Code:	Local Agent Preference? n
ISDN/SIP Caller Display:	

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

```
add hunt-group 3
```

Page 2 of 4

HUNT GROUP

<b>Skill?</b> y	Expected Call Handling Time <sec>: 180
AAS? n	
Measured: none	
Supervisor Extension:	
Controlling Adjunct: none	

Repeat this section to administer another skill group for routing of phantom calls for chat work items to agents. In the compliance testing, two skill groups were created as shown below.

```
list hunt-group 3 count 2
```

HUNT GROUPS											
Grp No.	Grp Name/Ext	Grp Type	ACD/MEAS	Vec	MCH	Que	No. Mem	Cov Path	Notif/ Ctg Adj	Dom Ctrl	Message Center
3	Email Skill 63101	ucd-mia	y/I	SK	none	y	0		n		n
4	Chat Skill 64101	ucd-mia	y/I	SK	none	y	0		n		n

## 5.8. Administer Agent IDs

The newly created email and chat skills need to be added to the applicable agents. Use the “change agent-loginID n” command, where “n” is the first agent ID from **Section 3**. Navigate to **Page 2**, and add the desired email and/or chat skill group numbers from **Section 5.7** for the agent under **SN**, and set the desired skill level under **SL**, as shown below. Note that skills 1 and 2 were pre-existing skills for voice.

change agent-loginID 65881											
AGENT LOGINID											
Direct Agent Skill:						Service Objective? n					
Call Handling Preference: skill-level						Local Call Preference? n					
<b>SN</b>	<b>RL</b>	<b>SL</b>	<b>SN</b>	<b>RL</b>	<b>SL</b>	<b>SN</b>	<b>RL</b>	<b>SL</b>	<b>SN</b>	<b>RL</b>	<b>SL</b>
1: 1		1	16:			31:			46:		
2: 2		1	17:			32:			47:		
3: <b>3</b>		<b>1</b>	18:			33:			48:		
4: <b>4</b>		<b>1</b>	19:			34:			49:		
5:			20:			35:			50:		

Repeat this section to add email and/or chat skills to all desired agents. In the compliance testing, email and chat skills were added to both agents from **Section 3**, as shown below.

list agent-loginID 65881 count 2											
AGENT LOGINID											
Login ID	Name	Extension		Dir	Agt	AAS/AUD		COR Ag Pr SO			
		Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	
<b>65881</b>	CM Agent 1	unstaffed						1	lvl		
	1/01	2/01	<b>3/01</b>	<b>4/01</b>	/	/	/	/	/	/	
<b>65882</b>	CM Agent 2	unstaffed						1	lvl		
	1/01	2/01	<b>3/01</b>	<b>4/01</b>	/	/	/	/	/	/	

## 6. Configure Avaya Aura® Application Enablement Services

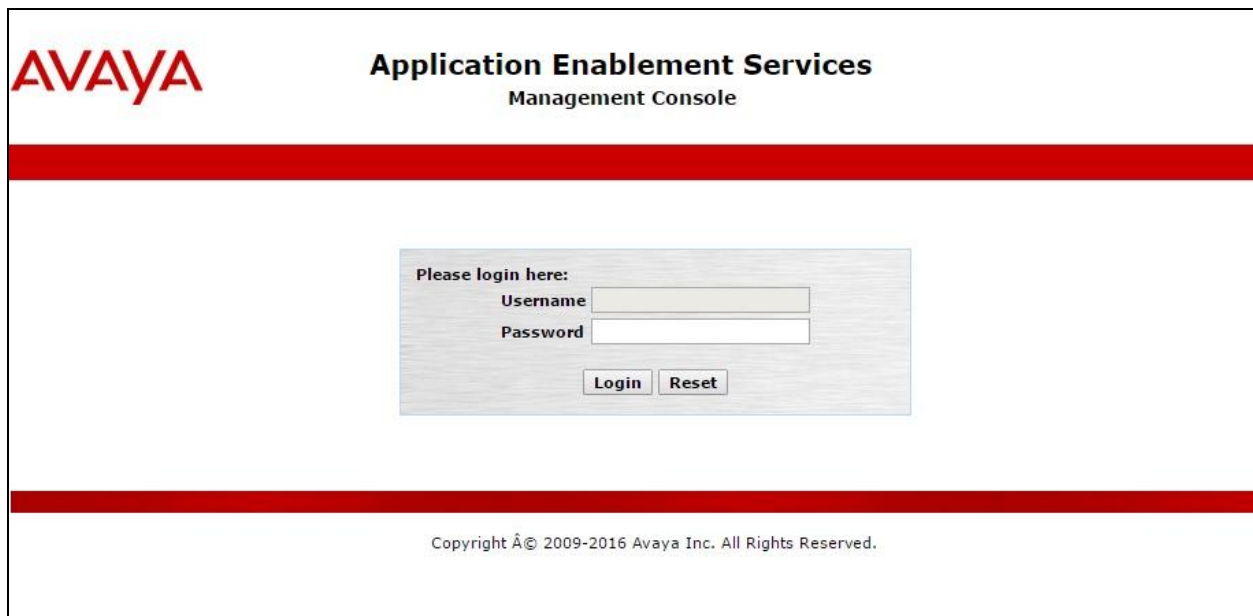
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

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

### 6.1. Launch OAM Interface

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

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



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

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". On the right, a "Welcome" message displays user information: "Welcome: User", "Last login: Tue Oct 3 13:45:16 2017 from 192.168.200.20", "Number of prior failed login attempts: 0", "HostName/IP: aes7/10.64.101.239", "Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE", "SW Version: 7.1.1.0.0.5-0", "Server Date and Time: Tue Oct 03 14:50:22 EDT 2017", and "HA Status: Not Configured". A red navigation bar at the top contains "Home", "Help", and "Logout". The left sidebar lists menu items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The main content area is titled "Welcome to OAM" and contains a paragraph: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:". This is followed by a bulleted list of domains and their functions: "AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.", "Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.", "High Availability - Use High Availability to manage AE Services HA.", "Licensing - Use Licensing to manage the license server.", "Maintenance - Use Maintenance to manage the routine maintenance tasks.", "Networking - Use Networking to manage the network interfaces and ports.", "Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.", "Status - Use Status to obtain server status informations.", "User Management - Use User Management to manage AE Services users and AE Services user-related resources.", "Utilities - Use Utilities to carry out basic connectivity tests.", and "Help - Use Help to obtain a few tips for using the OAM Help system". A final paragraph states: "Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain."

## 6.2. Verify License

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

The screenshot shows the Avaya Application Enablement Services Management Console with the "Licensing" menu item selected in the left sidebar. The top header and "Welcome" message are identical to the previous screenshot. The red navigation bar now includes "Licensing" in addition to "Home", "Help", and "Logout". The left sidebar highlights "Licensing" and shows sub-items: "WebLM Server Address", "WebLM Server Access", and "Reserved Licenses". The main content area is titled "Licensing" and contains three paragraphs of instructions: "If you are setting up and maintaining the WebLM, you need to use the following:" followed by a bullet point "WebLM Server Address"; "If you are importing, setting up and maintaining the license, you need to use the following:" followed by a bullet point "WebLM Server Access"; and "If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:" followed by a bullet point "Reserved Licenses".



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

Verify that there are sufficient licenses for **TSAPI Simultaneous Users**, as shown below. Note that TSAPI licenses are needed for agent monitoring and call control, and for phantom calls via DMCC.

**Application Enablement (CTI) - Release: 7 - SID: 10503000**

You are here: Licensed Products > Application\_Enablement > View License Capacity

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

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

**Licensed Features**

10 Items Show All

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

### 6.3. Administer TSAPI Link

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

The screenshot shows the AVAYA Application Enablement Services Management Console. The top right corner displays user information: Welcome: User, Last login: Tue Oct 3 13:45:16 2017 from 192.168.200.20, Number of prior failed login attempts: 0, HostName/IP: aes7/10.64.101.239, Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE, SW Version: 7.1.1.0.0.5-0, Server Date and Time: Tue Oct 03 14:50:22 EDT 2017, HA Status: Not Configured. The left navigation pane shows 'AE Services' expanded, with 'TSAPI' selected, and 'TSAPI Links' highlighted. The main content area is titled 'TSAPI Links' and contains a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are buttons for 'Add Link', 'Edit Link', and 'Delete Link'.

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

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

The screenshot shows the AVAYA Application Enablement Services Management Console with the 'Add TSAPI Links' screen. The left navigation pane shows 'AE Services' expanded, with 'TSAPI' selected, and 'TSAPI Links' highlighted. The main content area is titled 'Add TSAPI Links' and contains form fields for: Link (dropdown menu with '1' selected), Switch Connection (dropdown menu with 'cm7' selected), Switch CTI Link Number (dropdown menu with '1' selected), ASAI Link Version (dropdown menu with '7' selected), and Security (dropdown menu with 'Unencrypted' selected). Below the fields are buttons for 'Apply Changes' and 'Cancel Changes'.

## 6.4. Administer Harmony User

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

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

**AVAYA** **Application Enablement Services**  
Management Console

Welcome: User  
Last login: Tue Oct 3 13:45:16 2017 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 7.1.1.0.0.5-0  
Server Date and Time: Tue Oct 03 14:50:22 EDT 2017  
HA Status: Not Configured

User Management | User Admin | Add UserHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

■ Add User

■ Change User Password

■ List All Users

■ Modify Default Users

■ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with \* can not be empty.

\* User Idharmony

\* Common Nameharmony

\* Surnameharmony

\* User Password\*\*\*\*\*

\* Confirm Password\*\*\*\*\*

Admin Note

Avaya RoleNone ▼

Business Category

Car License

CM Home

Css Home

CT UserYes ▼

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

## 6.5. Administer Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Make certain that both parameters are unchecked, as shown below.

In the event that the security database is used by the customer with parameters already enabled, then follow reference [2] to configure access privileges for the Harmony user from **Section 6.4**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows a tree structure with "Security" expanded, leading to "Security Database" and then "Control". The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is located below these options.

Welcome: User  
Last login: Tue Oct 3 13:45:16 2017 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 7.1.1.0.0.5-0  
Server Date and Time: Tue Oct 03 14:50:22 EDT 2017  
HA Status: Not Configured

Security | Security Database | Control Home | Help | Logout

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

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

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

## 6.6. Administer Ports

Select **Networking** → **Ports** from the left pane, to display the **Ports** screen in the right pane.

In the **DMCC Server Ports** section, select the radio button for **Unencrypted Port** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.

**AVAYA** **Application Enablement Services**  
Management Console

Welcome: User  
Last login: Tue Oct 3 13:45:16 2017 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 7.1.1.0.0.5-0  
Server Date and Time: Tue Oct 03 14:50:22 EDT 2017  
HA Status: Not Configured

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

▶ AE Service IP (Local IP)

▶ Network Configure

▶ Ports

▶ TCP/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port 9999

Enabled Disabled

Encrypted TCP Port 9998

DLG Port TCP Port 5678

TSAPI Ports

TSAPI Service Port 450

Enabled Disabled

Local TLINK Ports

TCP Port Min 1024

TCP Port Max 1039

Unencrypted TLINK Ports

TCP Port Min 1050

TCP Port Max 1065

Encrypted TLINK Ports

TCP Port Min 1066

TCP Port Max 1081

DMCC Server Ports

Unencrypted Port 4721

Enabled Disabled

Encrypted Port 4722

TR/87 Port 4723

H.323 Ports

## 6.7. Restart Services

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A welcome message for the user is shown in the top right corner, including login details and system information. The main navigation pane on the left lists various sections: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance (selected), Date Time/NTP Server, Security Database, Service Controller (highlighted), Server Data, Networking, Security, and Status. The main content area, titled "Service Controller", contains a table with two columns: "Service" and "Controller Status". The table lists several services, with checkboxes for "DMCC Service" and "TSAPI Service" selected. Below the table, there is a link to "Status and Control" and a row of buttons: "Start", "Stop", "Restart Service", "Restart AE Server", "Restart Linux", and "Restart Web Server".

Welcome: User  
Last login: Tue Oct 3 13:45:16 2017 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 7.1.1.0.0.5-0  
Server Date and Time: Tue Oct 03 14:50:22 EDT 2017  
HA Status: Not Configured

Maintenance | Service Controller Home | Help | Logout

AE Services  
Communication Manager Interface  
High Availability  
Licensing  
Maintenance  
Date Time/NTP Server  
Security Database  
Service Controller  
Server Data  
Networking  
Security  
Status

Service Controller

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

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

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



## 6.8. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring Harmony.

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the text "Application Enablement Services Management Console". On the right side of the header, there is a welcome message for the user, including the last login time (Tue Oct 3 13:45:16 2017), the number of failed login attempts (0), the host name/IP (aes7/10.64.101.239), the server offer type (VIRTUAL\_APPLIANCE\_ON\_VMWARE), the software version (7.1.1.0.0.5-0), the server date and time (Tue Oct 03 14:50:22 EDT 2017), and the HA status (Not Configured).

The main navigation bar is red and contains the text "Security | Security Database | Tlinks" on the left and "Home | Help | Logout" on the right. The left sidebar is a dark gray menu with the following items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security" (expanded), "Account Management", "Audit", "Certificate Management", "Enterprise Directory", "Host AA", "PAM", "Security Database" (expanded), "Control", "CTI Users", "Devices", "Device Groups", and "Tlinks" (selected).

The main content area is titled "Tlinks" and shows a single Tlink name: "AVAYA#CM7#CSTA#AES7". There is a radio button next to the name and a "Delete Tlink" button below it.

## 7. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer users

### 7.1. Launch System Manager

Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.

Recommended access to System Manager is via FQDN.  
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

User ID:

Password:

[Change Password](#)

### 7.2. Administer Users

In the subsequent screen (not shown), select **Users → User Management**. Select **User Management → Manage Users** from the left pane to display the **User Management** screen below. Select the entry associated with the first SIP agent station from **Section 3**, in this case “66002”, and click **Edit**.

AVAYA  
Aura® System Manager 7.1

Last Logged on at:

Home / Users / User Management / Manage Users

Search

**User Management**

**Users**

3 Items  All

<input type="checkbox"/>	Last Name	First Name	Display Name	Login Name	SIP Handle	Last Login
<input checked="" type="checkbox"/>	Avaya	SIP 2	Avaya, SIP 2	66002@dr220.com	66002	



The **User Profile Edit** screen is displayed. Select the **Communication Profile** tab to display the screen below.

Navigate to the **CM Endpoint Profile** sub-section, and click **Endpoint Editor**.

AVAYA  
Aura® System Manager 7.1

Last Logged on at  
Go...

Home / Users / User Management / Manage Users

**User Profile Edit: 66002@dr220.com** [Commit & Continue](#)

**Communication Profile**

Communication Profile Password: ..... [Edit](#)

[New](#) [Delete](#) [Done](#) [Cancel](#)

**Name**

☒ Primary

Select : None

\* Name:

Default : ☒

**Communication Address**

[New](#) [Edit](#) [Delete](#)

Type	Handle	Domain
<input type="checkbox"/> Avaya SIP	66002	dr220.com

Select : All, None

☒ **Session Manager Profile**

☒ **CM Endpoint Profile**

\* System:

\* Profile Type:

Use Existing Endpoints: ☐

\* Extension:  [Display Extension Ranges](#) **Endpoint Editor**

Template:

Set Type:

The **Edit Endpoint** screen is displayed next. For **Type of 3PCC Enabled**, select “Avaya” from the drop-down list as shown below. Retain the default values in the remaining fields.

Repeat this section for all SIP agent users.

**AVAYA**  
Aura® System Manager 7.1

Last Logged on at  
Go...

Home | **User Management**

Home / Users / User Management / Manage Users

### Edit Endpoint

**System** DR220-CM7-ES **Extension** 66002  
**Template** Select **Set Type** 9621SIPCC  
**Port** S00004 **Security Code**  
**Name** Avaya, SIP 2

**General Options (G)** **Feature Options (F)** **Site Data (S)** **Abbreviated Call Dialing (A)**

**Enhanced Call Fwd (E)** **Button Assignment (B)** **Profile Settings (P)** **Group Membership**

\* **Class of Restriction (COR)** 1 \* **Class Of Service (COS)** 1  
\* **Emergency Location Ext** 66002 \* **Message Lamp Ext.** 66002  
\* **Tenant Number** 1  
\* **SIP Trunk** aar **Type of 3PCC Enabled** Avaya  
**Coverage Path 1** 1 **Coverage Path 2**  
**Lock Message** ☐ **Localized Display Name** Avaya, SIP 2  
**Multibyte Language** Not Applicable **Enable Reachability for Station Domain Control** system

\*Required

## 8. Configure OpenMethods Harmony

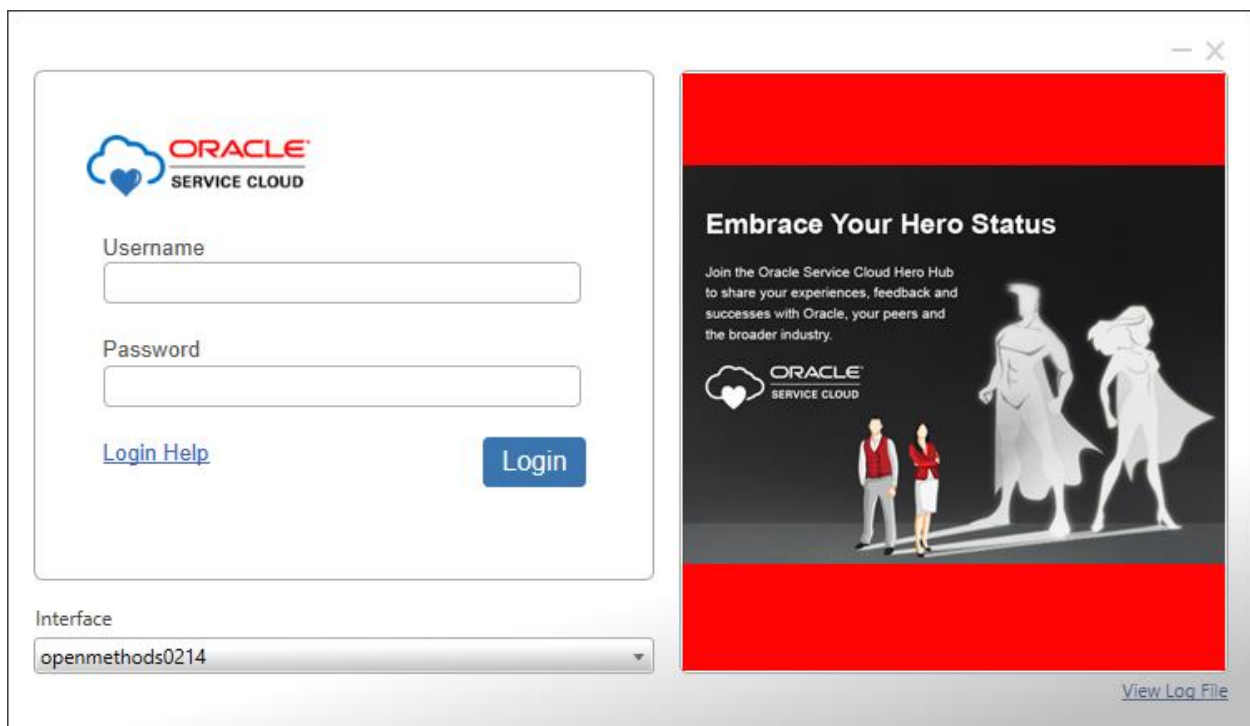
This section provides the procedures for configuring Harmony. The procedures include the following areas:

- Launch Oracle Service Cloud CX Desktop
- Administer add-ins
- Administer agent info
- Administer agent states
- Administer queue adapter
- Administer servers
- Administer omis.json
- Install as service
- Administer registry
- Start services

The configuration of Harmony is performed by the OpenMethods installation engineers. The procedural steps are presented in these Application Notes for informational purposes.

### 8.1. Launch Oracle Service Cloud CX Desktop

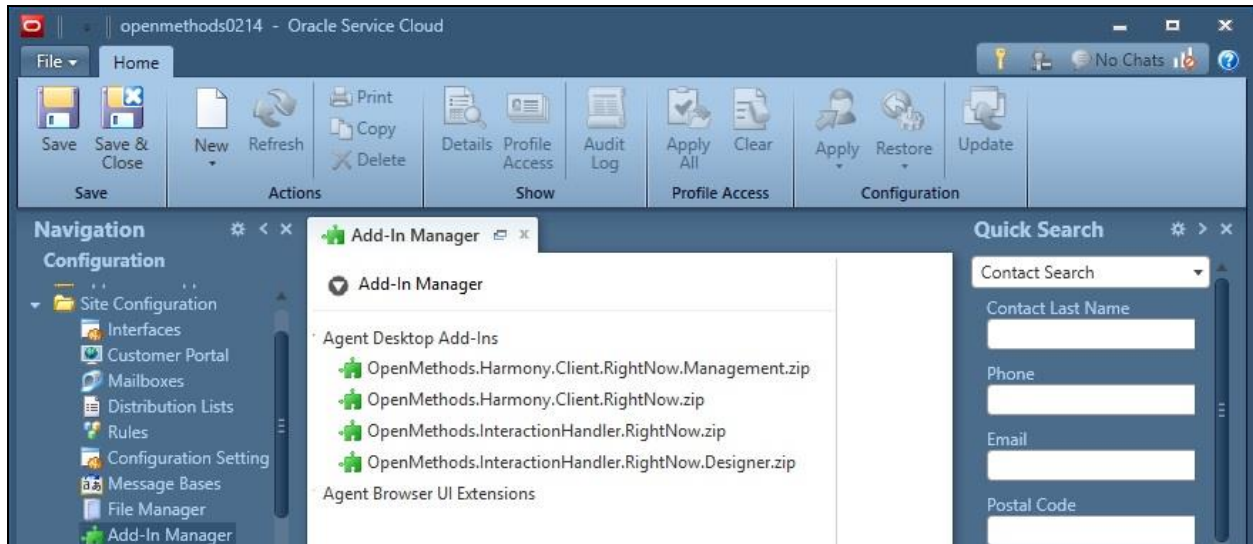
From a PC running the Oracle Service Cloud CX Desktop application, select **All Apps → RightNow → RightNow (openmethods0214)** to launch the application. The screen below is displayed. Log in using the administrator credentials.



The screenshot displays the Oracle Service Cloud CX Desktop login interface. On the left, there is a login form with the Oracle Service Cloud logo at the top. The form includes input fields for 'Username' and 'Password', a 'Login' button, and a 'Login Help' link. Below the login form is a dropdown menu labeled 'Interface' with 'openmethods0214' selected. To the right of the login form is a promotional banner titled 'Embrace Your Hero Status' with the Oracle Service Cloud logo and an illustration of two people in superhero costumes. A 'View Log File' link is at the bottom right.

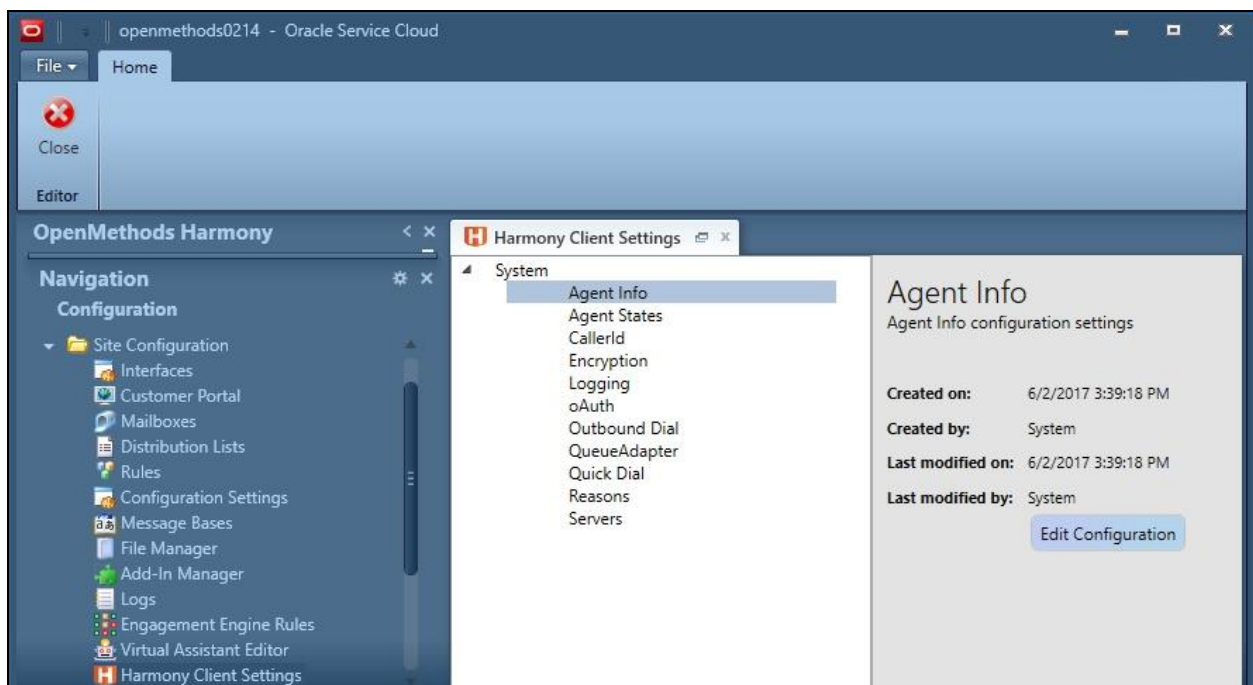
## 8.2. Administer Add-Ins

The **openmethods0214 – Oracle Service Cloud** screen is displayed. In the left **Navigation** pane, expand and double click on **Site Configuration → Add-In Manager** to display the **Add-In Manager** tab in the middle pane. Follow reference [3] to add all four add-ins shown below.



## 8.3. Administer Agent Info

In the left **Navigation** pane, double click on **Site Configuration → Harmony Client Settings** to display the **Harmony Client Settings** tab in the middle pane. Select **Agent Info** in the middle pane, to display **Agent Info** in the right pane. Click **Edit Configuration** in the right pane.



The **Agent Info Configuration** screen is displayed. Select the first pre-created agent from the left pane, in this case “Avaya Cert1”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Username:** The first agent login ID from **Section 3**.
- **Password:** The first agent login password from **Section 3**.
- **Client Defined Channels:** Check this field.

In the **Client Defined Channels** sub-section, follow reference [3] to add the applicable **Telephony, Email, and Chat** channels, with the first agent station extension from **Section 3**.

Repeat this section to update all applicable agents with proper agent login and station information. In the compliance testing, both agents shown in the left pane below were updated. **Save** and **Close** the screen when done.

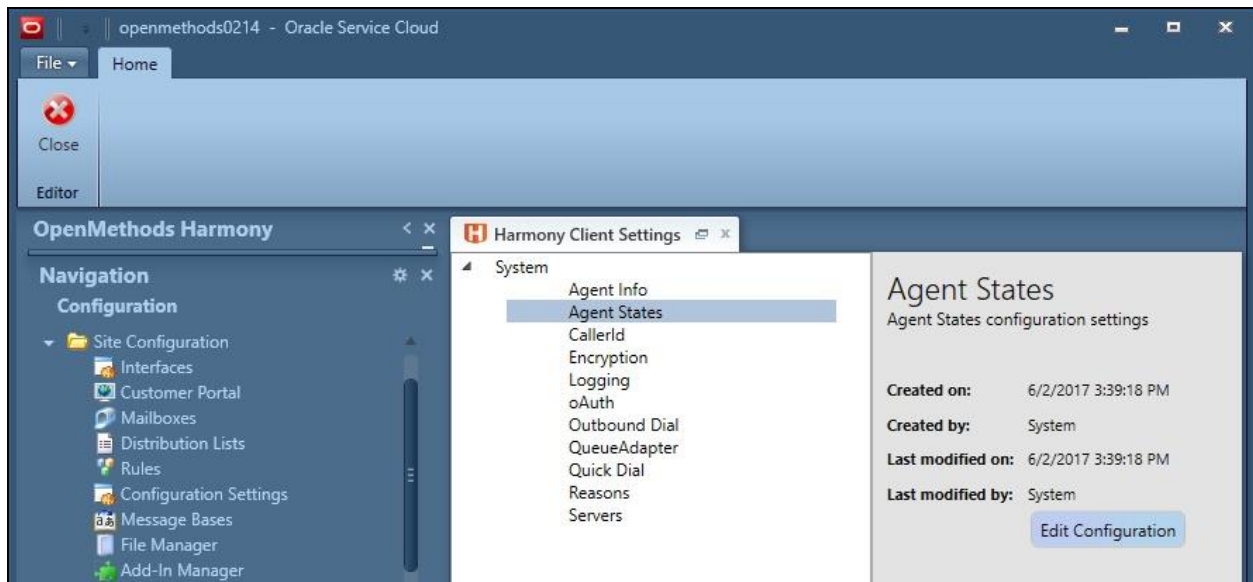
The screenshot shows the 'Agent Info Configuration' window with three main panes: Agents, Agent Details, and Channel Details.

- Agents (123):** A list on the left with 'Avaya Cert1' selected.
- Agent Details:**
  - Display Name: Avaya Cert1
  - Username: 65881
  - Password: [masked]
  - End Completes Interaction: ☐ Auto Answer: ☐
  - Single SignOn Enabled: ☐ Type: Basic
  - Station Type: Workstation
  - WorkStation: [empty]
  - Remote Number: [empty]
  - Developer Mode: [empty] (comma delimited)
  - Screen Pop: ☐ On Ring ☒ On Answer
  - Report Pop: ☒ On Ring ☐ On Answer
  - Use OSC Native Chat: ☐
- Channel Details:**
  - Defaults:**
    - Channel: [empty]
    - Channel Type: Telephony
    - Channel Group: [empty]
    - Queue(s): [empty] (comma delimited)
  - Client Defined Channels:** ☒

Channel	65001	Telephony
	65001	Email
	65001	Chat
  - Channel Name: [empty]
  - Channel Type: Unknown
  - Queue(s): [empty] (comma delimited)
  - Buttons: Add, Clear, Remove
- Agent Import/Export:**
  - Select Platform: [dropdown]
  - Buttons: Export, Import
- Search For:** [input field]
- Buttons:** Save, Close

## 8.4. Administer Agent States

The **openmethods0214 – Oracle Service Cloud** screen is displayed again. For contact centers that use reason codes, select **Agent States** in the middle pane, to display **Agent States** in the right pane. Click **Edit Configuration** in the right pane.



The **Agent States Configuration** screen is displayed. Click **Add Agent State** and add an entry for each reason code from **Section 5.3**. Enter the following values for the specified fields, and retain the default values for the remaining fields. **Save** and **Close** the screen when done.

- **Name:** The reason code name from **Section 5.3**.
- **Description:** A desired description.
- **Code:** The reason code value from **Section 5.3**.
- **IsAgentSelectable:** Check this field.

The screenshot shows the "Agent States Configuration" window. It contains a table with the following data:

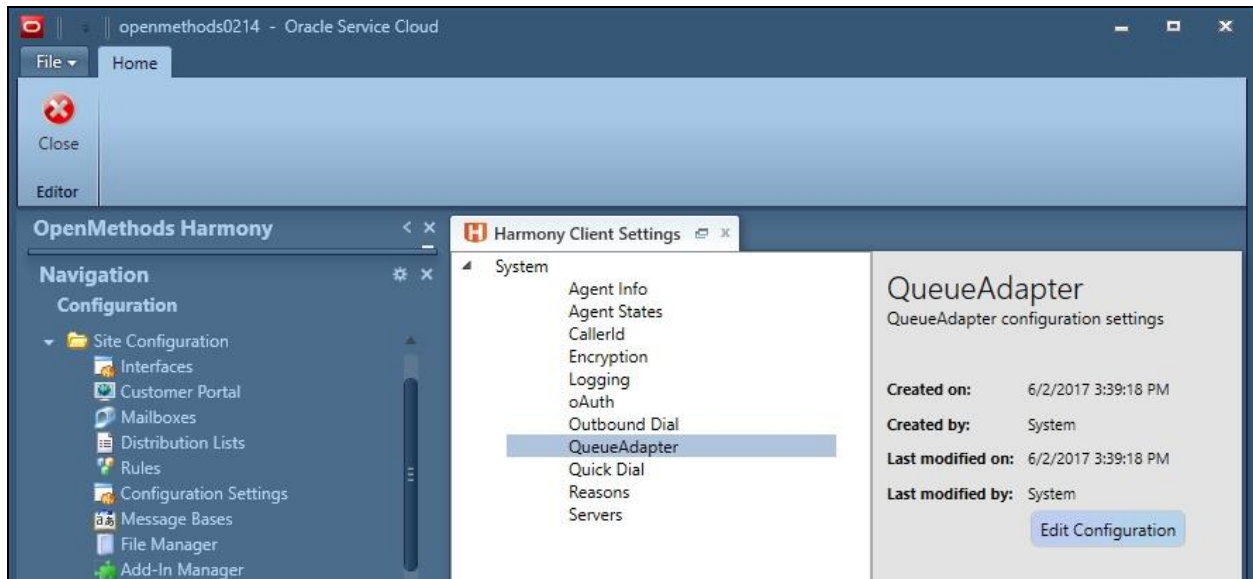
	Id	Order	Name	Description	Code	IsAgentSelectable	Type	ChannelType
	5FECB3C0-25FD-4996-99D8-AE9FC70ACEFF	1	Lunch	Lunch	1	<input checked="" type="checkbox"/>	Unavailable	Any
	5FECB3C0-25FD-4996-99D8-AE9FC70ACEF0	2	Coffee	Coffee	2	<input checked="" type="checkbox"/>	Unavailable	Any

Below the table are four buttons: "Remove Selected Agent State", "Add Agent State", "Save", and "Close".



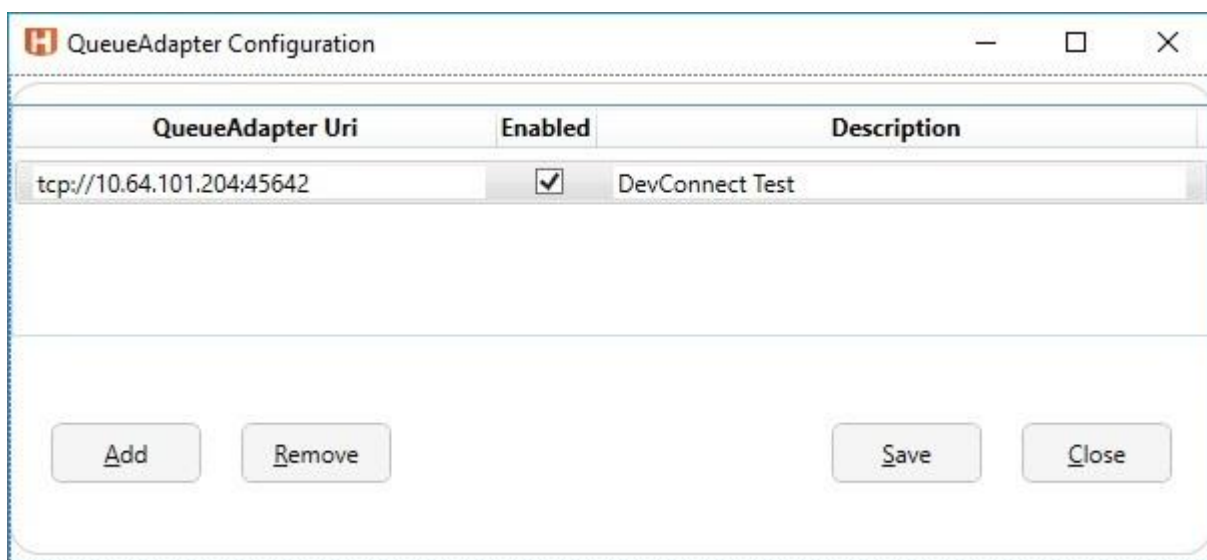
## 8.5. Administer Queue Adapter

The **openmethods0214 – Oracle Service Cloud** screen is displayed again. Select **QueueAdapter** in the middle pane, to display **QueueAdapter** in the right pane. Click **Edit Configuration** in the right pane.



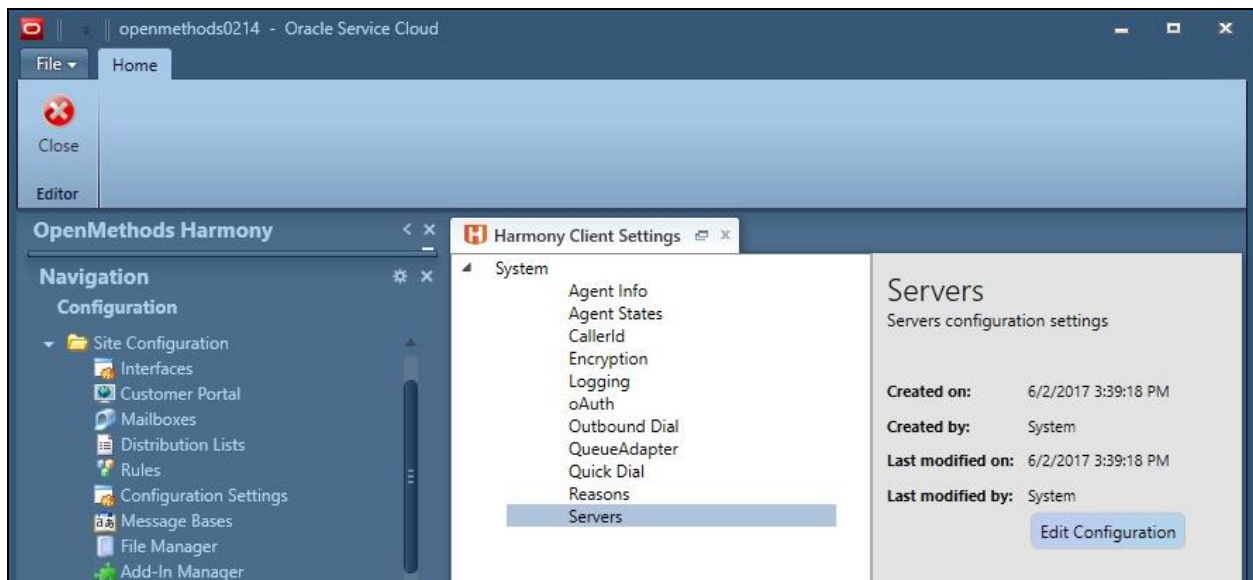
The **QueueAdapter Configuration** screen is displayed. Click **Add**. Enter the following values for the specified fields, and retain the default values for the remaining fields. **Save** and **Close** the screen when done.

- **QueueAdapter Uri:** Replace “0.0.0.0” with IP address of the Harmony server.
- **Enabled:** Check this field.
- **Description:** A desired description.



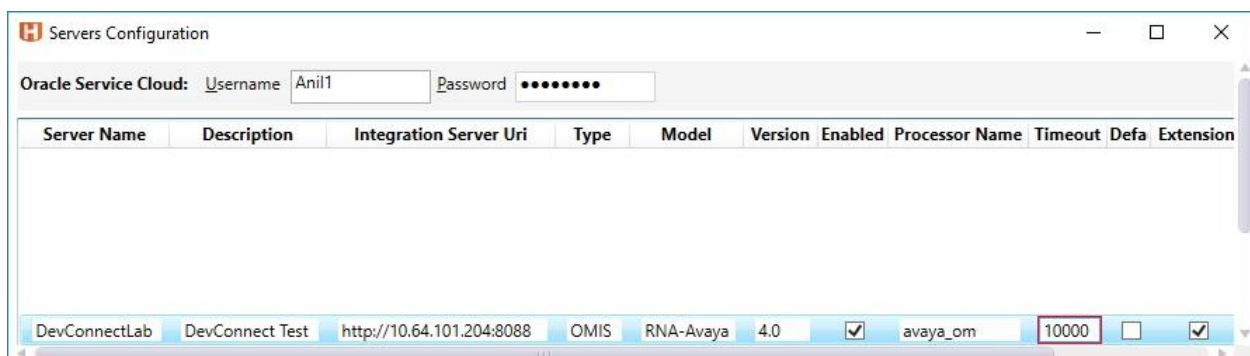
## 8.6. Administer Servers

The **openmethods0214 – Oracle Service Cloud** screen is displayed again. Select **Servers** in the middle pane, to display **Servers** in the right pane. Click **Edit Configuration** in the right pane.



The **Servers Configuration** screen is displayed. Click **Add New** (not shown). Enter the following values for the specified fields, and retain the default values for the remaining fields. **Save** and **Close** the screen when done.

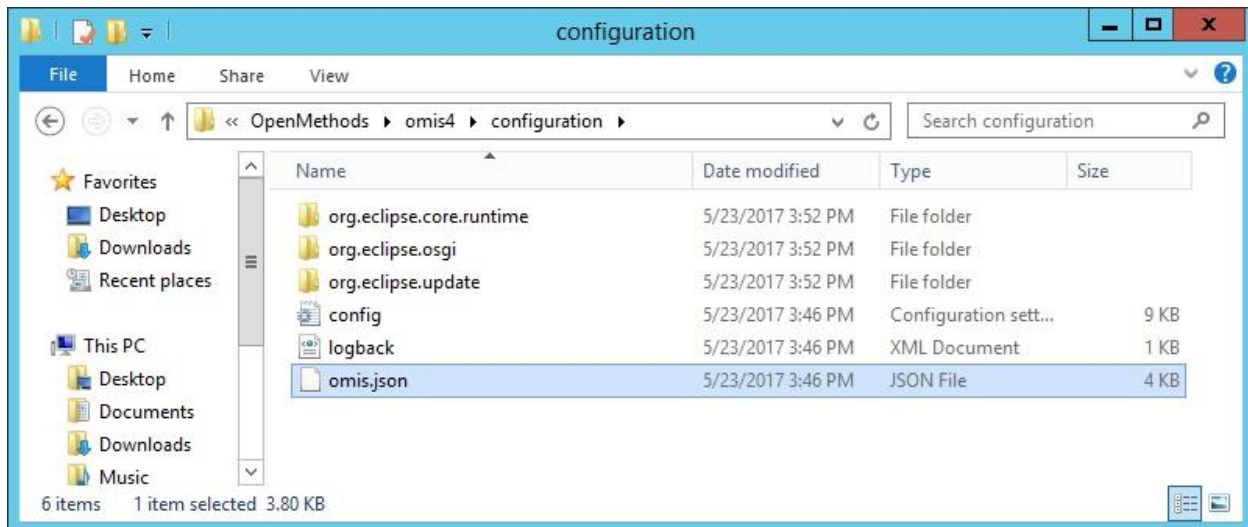
- **Server Name:** A desired server name.
- **Description:** A desired description.
- **Integration Server Uri:** Replace "0.0.0.0" with IP address of the Harmony server.
- **Model:** "RNA-Avaya"
- **Enabled:** Check this field.
- **Processor Name:** "avaya\_om"
- **Timeout:** "10000"
- **Extension:** Check this field.



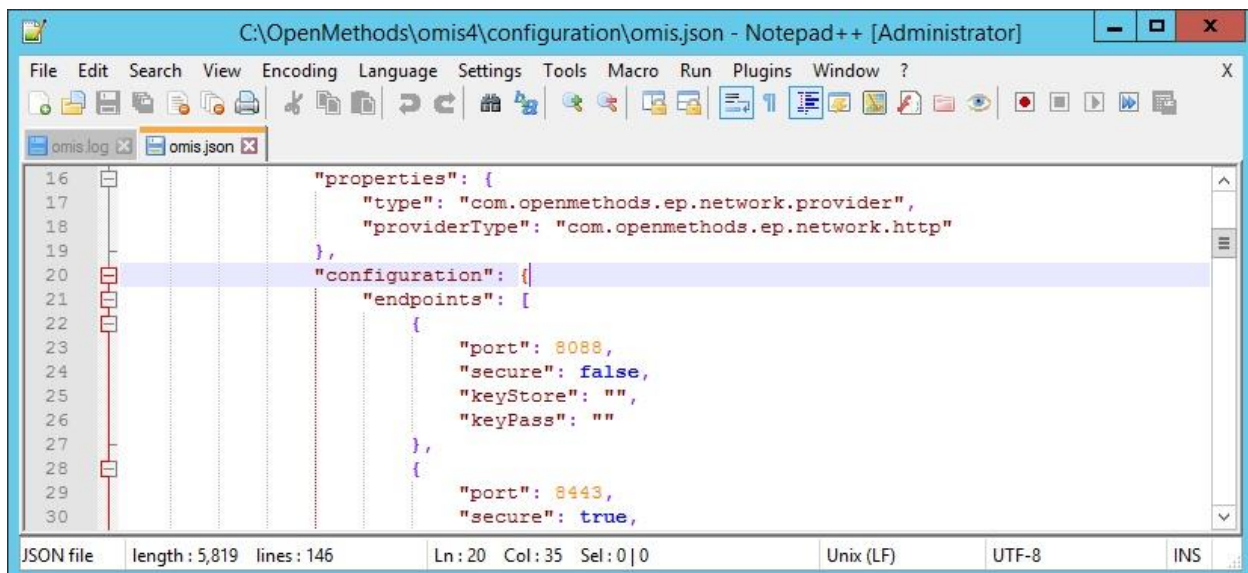


## 8.7. Administer omis.json

From the Harmony server, navigate to **C:\OpenMethods\omis4\configuration** to locate the **omis.json** file shown below. Replace the default **omis.json** file with the Avaya version from OpenMethods, which contained relevant parameters and default values for integration with Avaya.

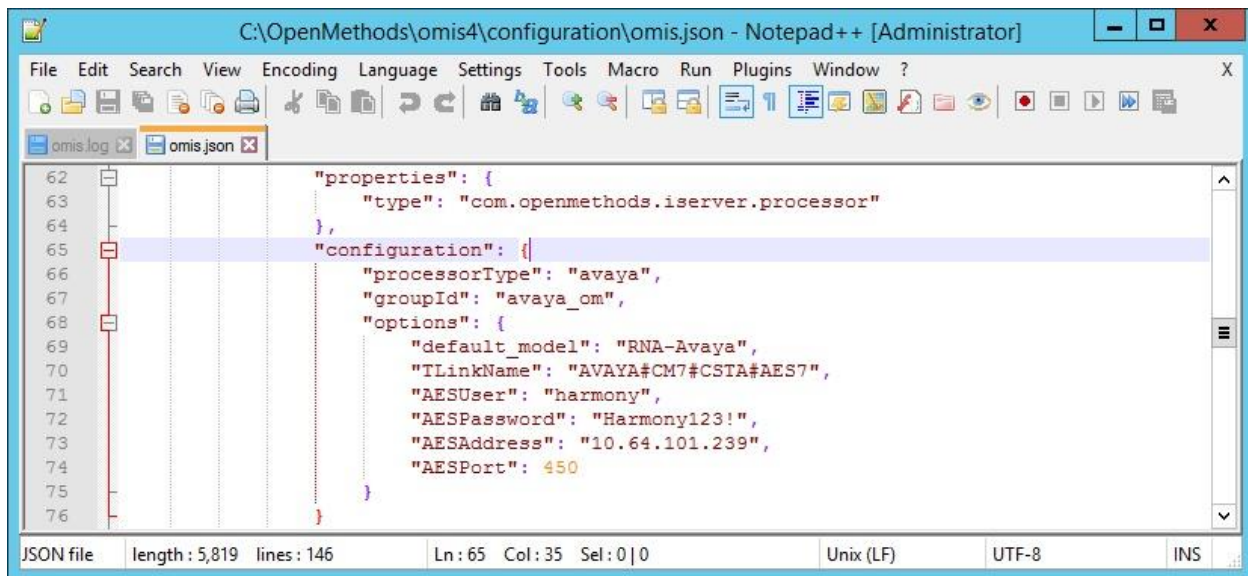


Open the **omis.json** file with an application such as Notepad++, and navigate to the **configuration** sub-section for endpoint network shown below. Update the first **port** value to "8088", which matches to the default port value in the server URI from **Section 8.6**.



Navigate to the **configuration** sub-section for server processor shown below. Enter the following values for the specified fields, and retain the default values in the remaining fields.

- **TLinkName:** The Tlink name from **Section 6.8**.
- **AESUser:** The Harmony user credentials from **Section 6.4**.
- **AESPassword:** The Harmony user credentials from **Section 6.4**.
- **AESAddress:** IP address of Application Enablement Services.

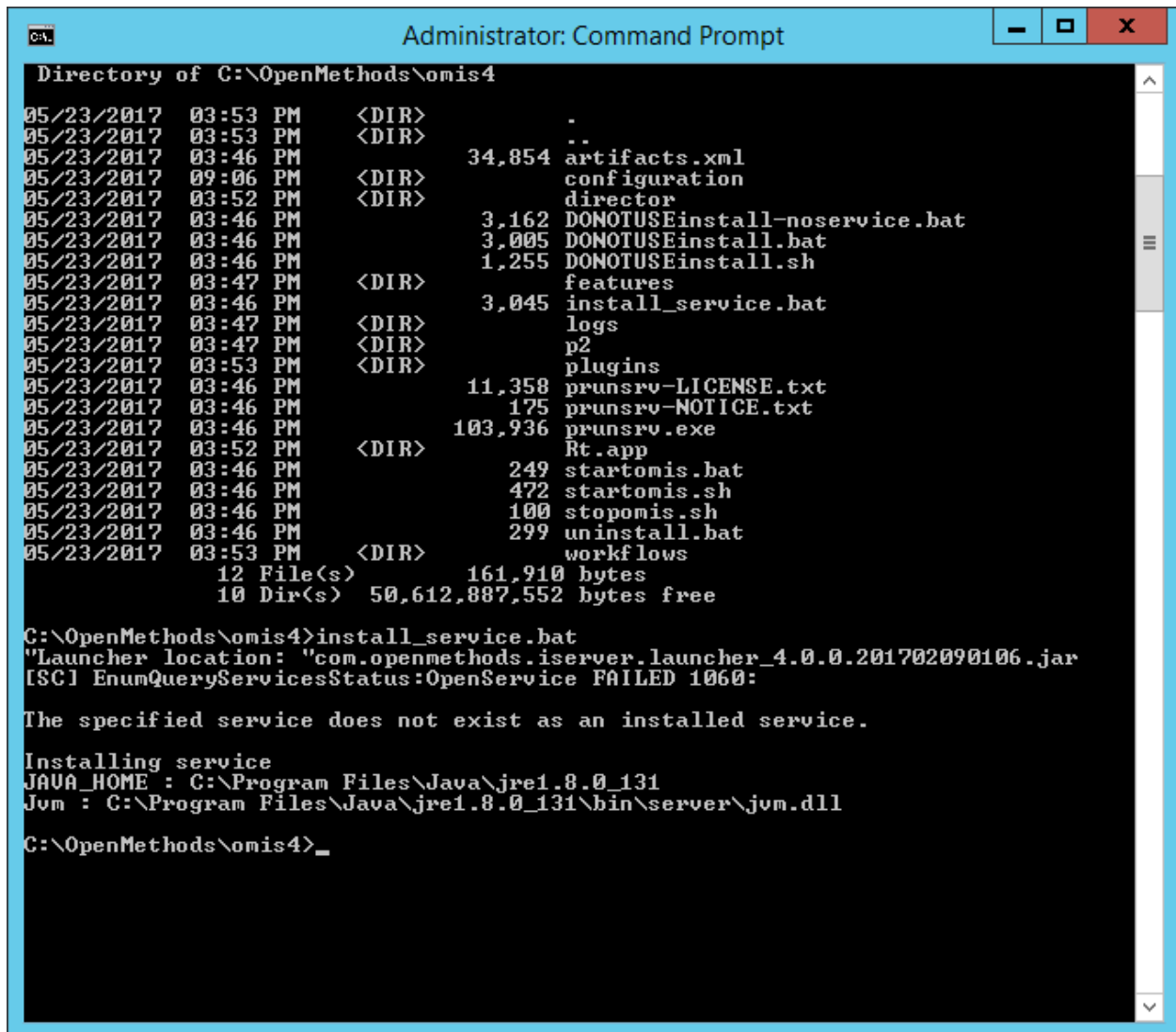


```
C:\OpenMethods\omis4\configuration\omis.json - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
omis.log x omis.json x
62 | "properties": {
63 |     "type": "com.openmethods.iserver.processor"
64 | },
65 | "configuration": {
66 |     "processorType": "avaya",
67 |     "groupId": "avaya_om",
68 |     "options": {
69 |         "default_model": "RNA-Avaya",
70 |         "TLinkName": "AVAYA#CM7#CSTA#AES7",
71 |         "AESUser": "harmony",
72 |         "AESPassword": "Harmony123!",
73 |         "AESAddress": "10.64.101.239",
74 |         "AESPort": 450
75 |     }
76 | }
```

JSON file   length : 5,819   lines : 146   Ln : 65   Col : 35   Sel : 0 | 0   Unix (LF)   UTF-8   INS

## 8.8. Install as Service

From the Harmony server, open a command prompt window, and navigate to the C:\OpenMethods\omis4 directory. Enter “install\_service.bat” to install the application as a service, as shown below.



```
Administrator: Command Prompt

Directory of C:\OpenMethods\omis4
05/23/2017 03:53 PM <DIR> .
05/23/2017 03:53 PM <DIR> ..
05/23/2017 03:46 PM      34,854 artifacts.xml
05/23/2017 09:06 PM <DIR> configuration
05/23/2017 03:52 PM <DIR> director
05/23/2017 03:46 PM      3,162 DONOTUSEinstall-noservice.bat
05/23/2017 03:46 PM      3,005 DONOTUSEinstall.bat
05/23/2017 03:46 PM      1,255 DONOTUSEinstall.sh
05/23/2017 03:47 PM <DIR> features
05/23/2017 03:46 PM      3,045 install_service.bat
05/23/2017 03:47 PM <DIR> logs
05/23/2017 03:47 PM <DIR> p2
05/23/2017 03:53 PM <DIR> plugins
05/23/2017 03:46 PM     11,358 prunsrv-LICENSE.txt
05/23/2017 03:46 PM       175 prunsrv-NOTICE.txt
05/23/2017 03:46 PM    103,936 prunsrv.exe
05/23/2017 03:52 PM <DIR> Rt.app
05/23/2017 03:46 PM       249 startomis.bat
05/23/2017 03:46 PM       472 startomis.sh
05/23/2017 03:46 PM       100 stopomis.sh
05/23/2017 03:46 PM       299 uninstall.bat
05/23/2017 03:53 PM <DIR> workflows
                12 File(s)      161,910 bytes
                10 Dir(s)    50,612,887,552 bytes free

C:\OpenMethods\omis4>install_service.bat
"Launcher location: "com.openmethods.iserver.launcher_4.0.0.201702090106.jar
[SC] EnumQueryServicesStatus:OpenService FAILED 1060:

The specified service does not exist as an installed service.

Installing service
JAVA_HOME : C:\Program Files\Java\jre1.8.0_131
Jvm : C:\Program Files\Java\jre1.8.0_131\bin\server\jvm.dll

C:\OpenMethods\omis4>_
```

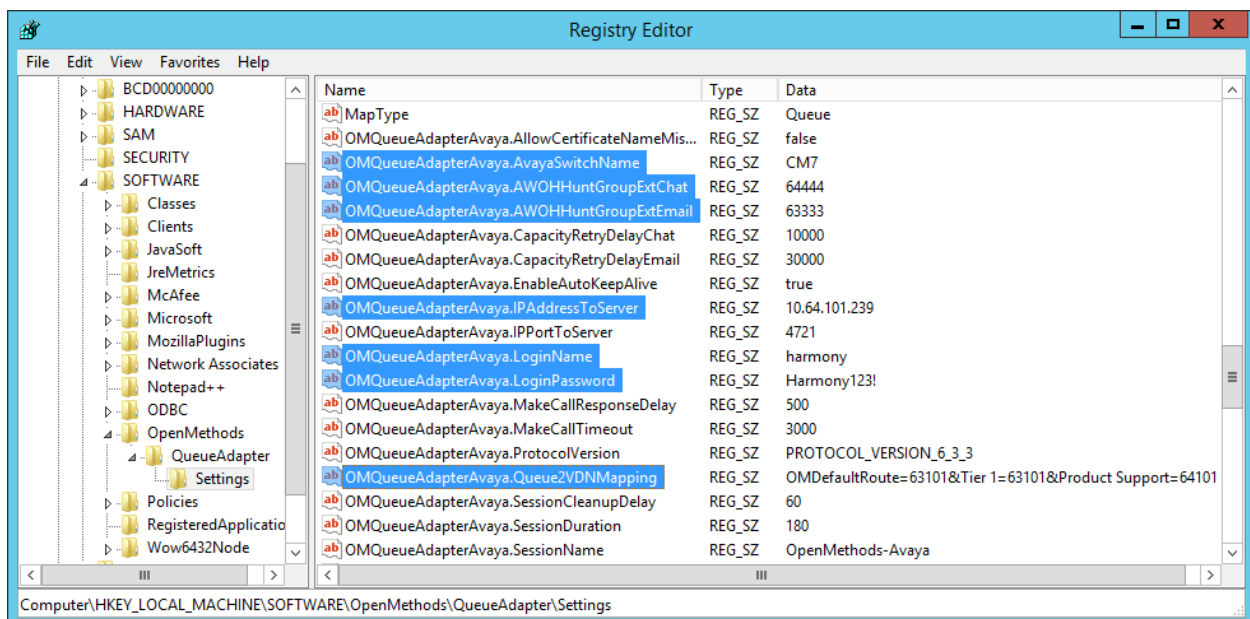
## 8.9. Administer Registry

From the Harmony server, select **Start → Run**, and enter “regedit” to display the **Registry Editor** screen. Navigate to **Computer → HKEY\_LOCAL\_MACHINE → SOFTWARE → OpenMethods → QueueAdapter → Settings**.

Enter the following values for the specified fields, which are referenced below without the common **OMQueueAdapterAvaya** prefix, and retain the default values in the remaining fields.

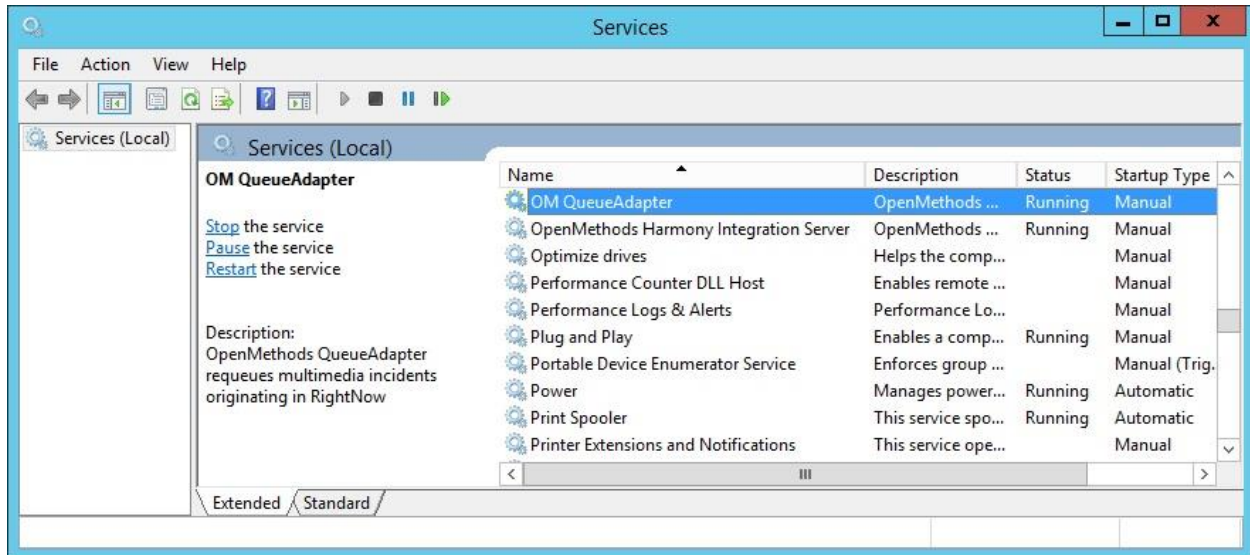
- **AvayaSwitchName:** The switch connection name from **Section 6.3**.
- **AWOHHuntGroupsExtChat:** AWOH hunt group extension for email from **Section 5.6**.
- **AWOHHuntGroupExtEmail:** AWOH hunt group extension for chat from **Section 5.6**.
- **IPAddressToServer:** IP address of Application Enablement Services.
- **LoginName:** The Harmony user credentials from **Section 6.4**.
- **LoginPassword:** The Harmony user credentials from **Section 6.4**.

For **Queue2VDNMapping**, replace the extensions for **OMDefaultRoute** and **Tier 1** with the skill group extension for email from **Section 5.7**, and replace the extension for **Product Support** with the skill group extension for chat from **Section 5.7**, as shown below.



## 8.10. Start Services

From the Harmony server, select **Start → Administrative Tools → Services** to display the **Services** screen. Start the **OM QueueAdapter** and **OpenMethods Harmony Integration Server** services, as shown below.



## 9. Verification Steps

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

### 9.1. Verify Avaya Aura® Communication Manager

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

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	7	no	aes7	established	203	163

### 9.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify status of the TSAPI service by selecting **Status** → **Status and Control** → **TSAPI Service Summary** (not shown) from the left pane. The **TSAPI Link Details** screen is displayed.

Verify that the **Status** is “Talking” for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the number of agents from **Section 3** that are currently logged into Harmony and therefore monitored, in this case “2”.

**AVAYA** **Application Enablement Services**  
Management Console

Welcome: User  
Last login: Tue Oct 3 14:50:02 2017 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 7.1.1.0.0.5-0  
Server Date and Time: Wed Oct 04 16:22:27 EDT 2017  
HA Status: Not Configured

Status | Status and Control | TSAPI Service Summary

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Log Manager

TSAPI Link Details

☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	cm7	1	Talking	Wed Oct 4 15:19:57 2017	Online	17	2	140	167	30



Verify status of the DMCC connection by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

Verify there is an active session with “OpenMethods-Avaya” as **Application**, and with the Harmony user name from **Section 6.4** as **User**, as shown below.

**Application Enablement Services**  
 Management Console

Welcome: User  
 Last login: Wed Oct 4 17:13:09 2017 from 192.168.200.20  
 Number of prior failed login attempts: 0  
 HostName/IP: aes7/10.64.101.239  
 Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
 SW Version: 7.1.1.0.0.5-0  
 Server Date and Time: Thu Oct 05 12:50:06 EDT 2017  
 HA Status: Not Configured

Status | Status and Control | **DMCC Service Summary**
Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▼ **Status**
  - Alarm Viewer
  - ▶ Log Manager
  - ▶ Logs
  - ▼ **Status and Control**
    - CVLAN Service Summary
    - DLG Services Summary
    - **DMCC Service Summary**
    - Switch Conn Summary
    - TSAPI Service Summary

### DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
Generated on Thu Oct 05 12:50:01 EDT 2017

Service Uptime:
0 days, 19 hours 28 minutes

Number of Active Sessions:
1

Number of Sessions Created Since Service Boot:
2

Number of Existing Devices:
0

Number of Devices Created Since Service Boot:
0

■	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
☐	581F0790339C9BD98114D66B7153CC3F-1	harmony	OpenMethods-Avaya	10.64.101.204	XML Unencrypted	0

Terminate Sessions
Show Terminated Sessions

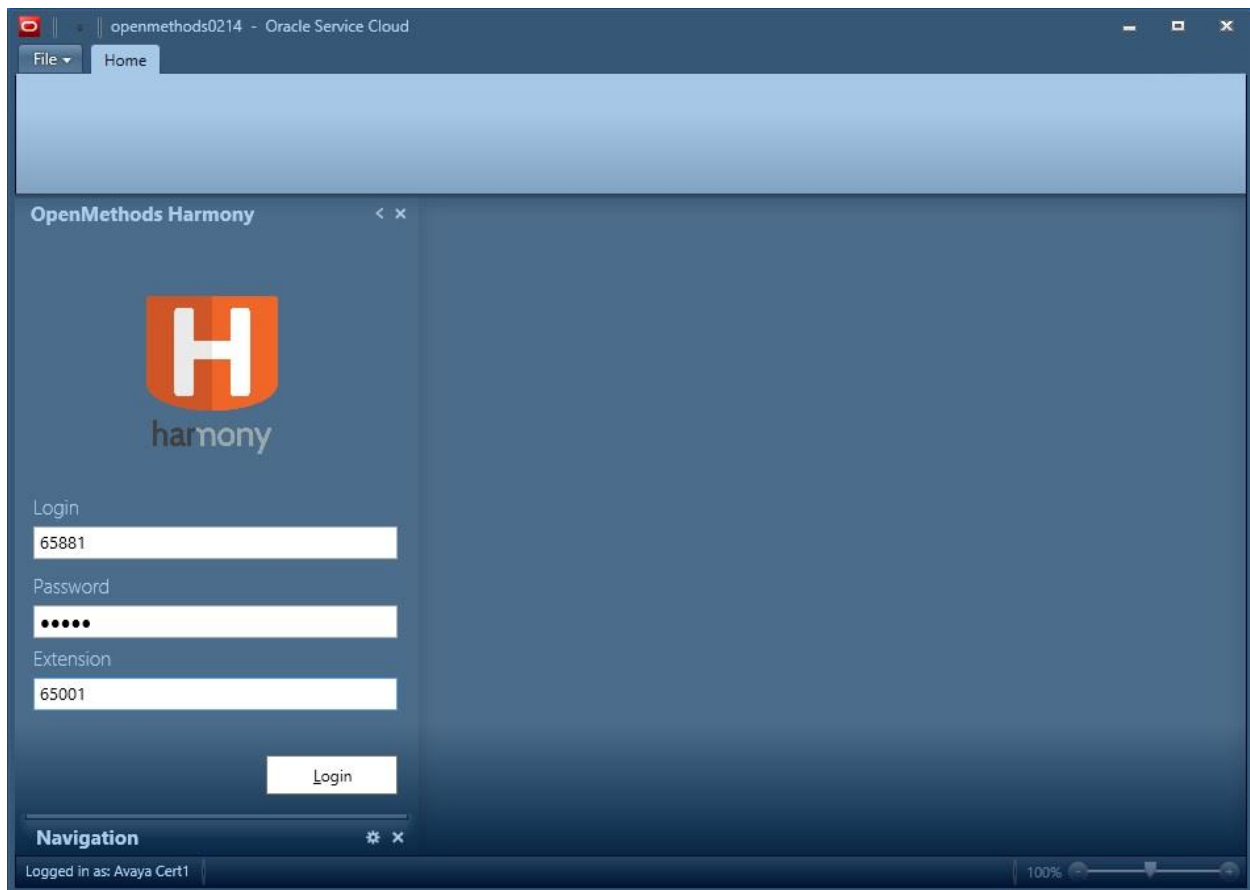
Item 1-1 of 1  
1 Go

### 9.3. Verify OpenMethods Harmony

From an agent PC, follow the procedures in **Section 8.1** to launch the Oracle Service Cloud CX Desktop application, and log in with the relevant user credentials provided by the customer.

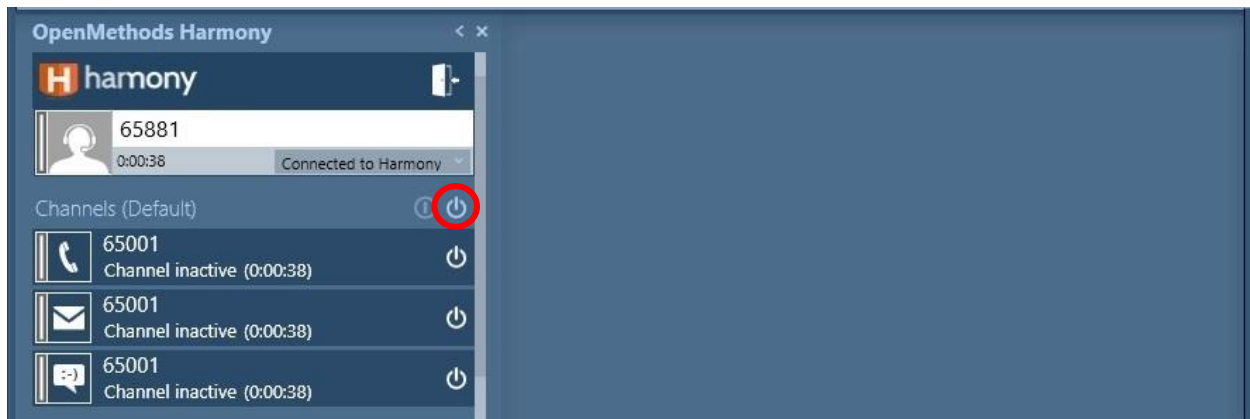
The screen below is displayed. In the **OpenMethods Harmony** sub-section in the left pane, enter the following values for the specified fields.

- **Login:** The relevant agent ID from **Section 3**.
- **Password:** The relevant agent password from **Section 3**.
- **Extension:** The relevant agent station from **Section 3**.

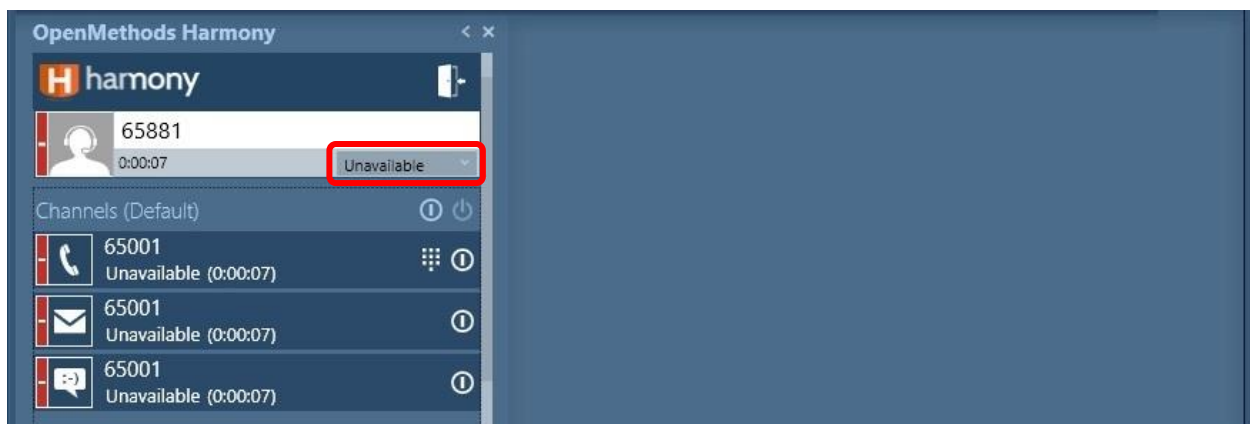




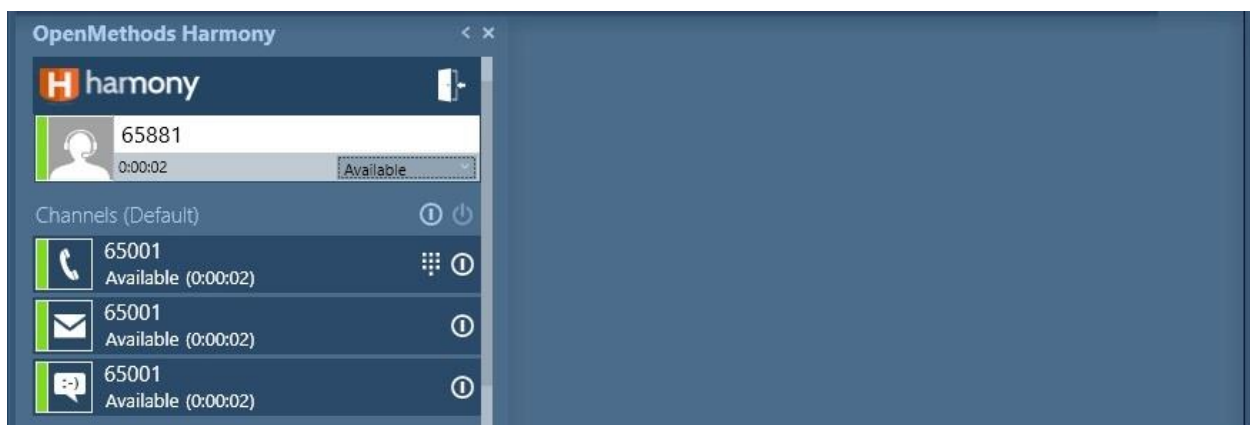
The left pane is updated, with a listing of all configured channels for the agent. Select the **Activate all channels** icon shown below.



Verify that the left pane is updated, showing the agent in the **Unavailable** state. Click on the agent state field shown below and select **Available** from the drop-down list.

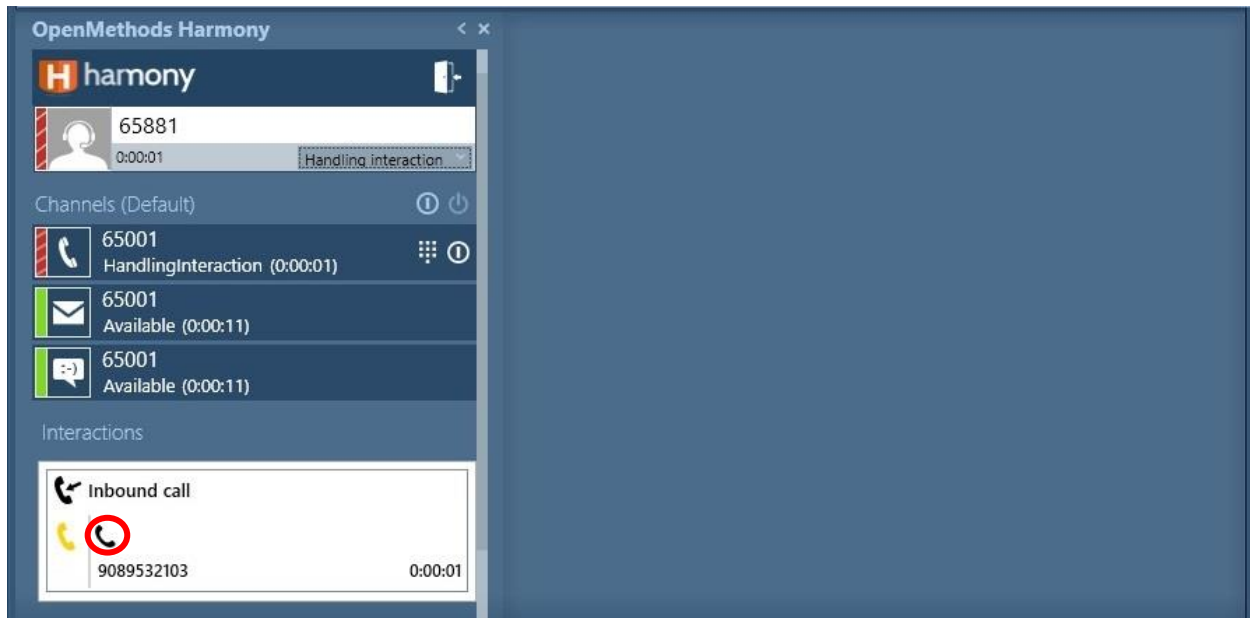


Verify that the left pane is updated to reflect agent in the **Available** state for all channels, as shown below.

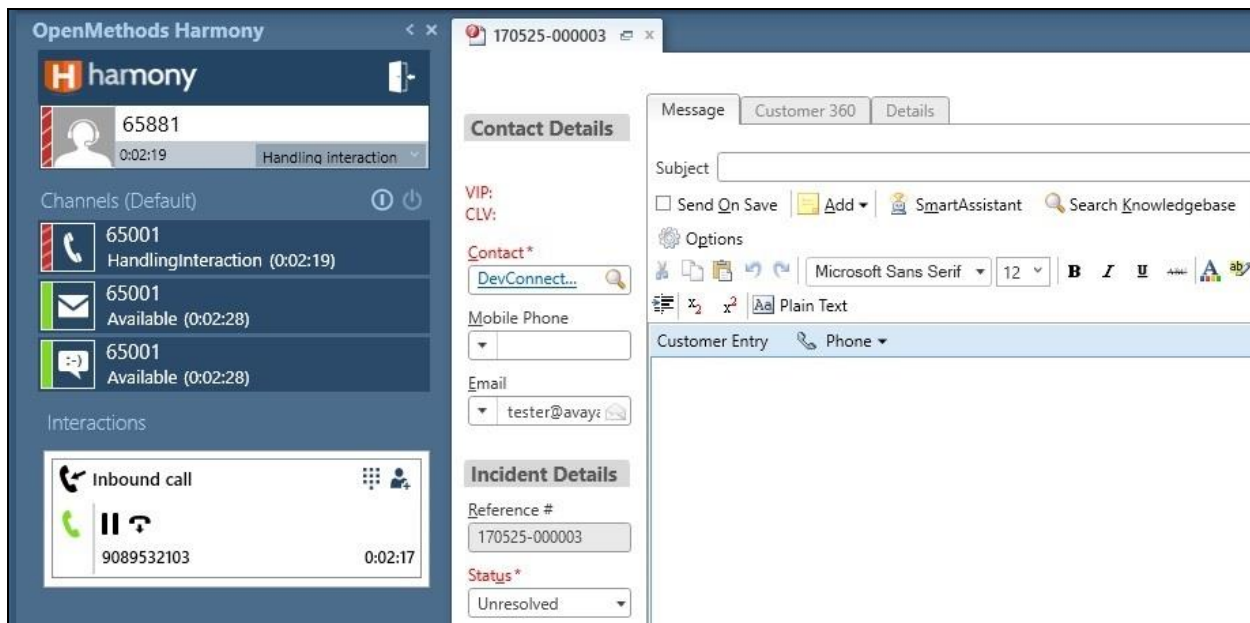


### 9.3.1. Verify Voice

Make an incoming ACD call from the PSTN. Verify that the left pane of the available agent is updated to reflect **HandlingInteraction** for the voice channel. Also verify that the **Interactions** sub-section reflects an “Inbound call” along with the calling party number, in this case “9089532103”. Click on the **Answer incoming call** icon below to answer the call.

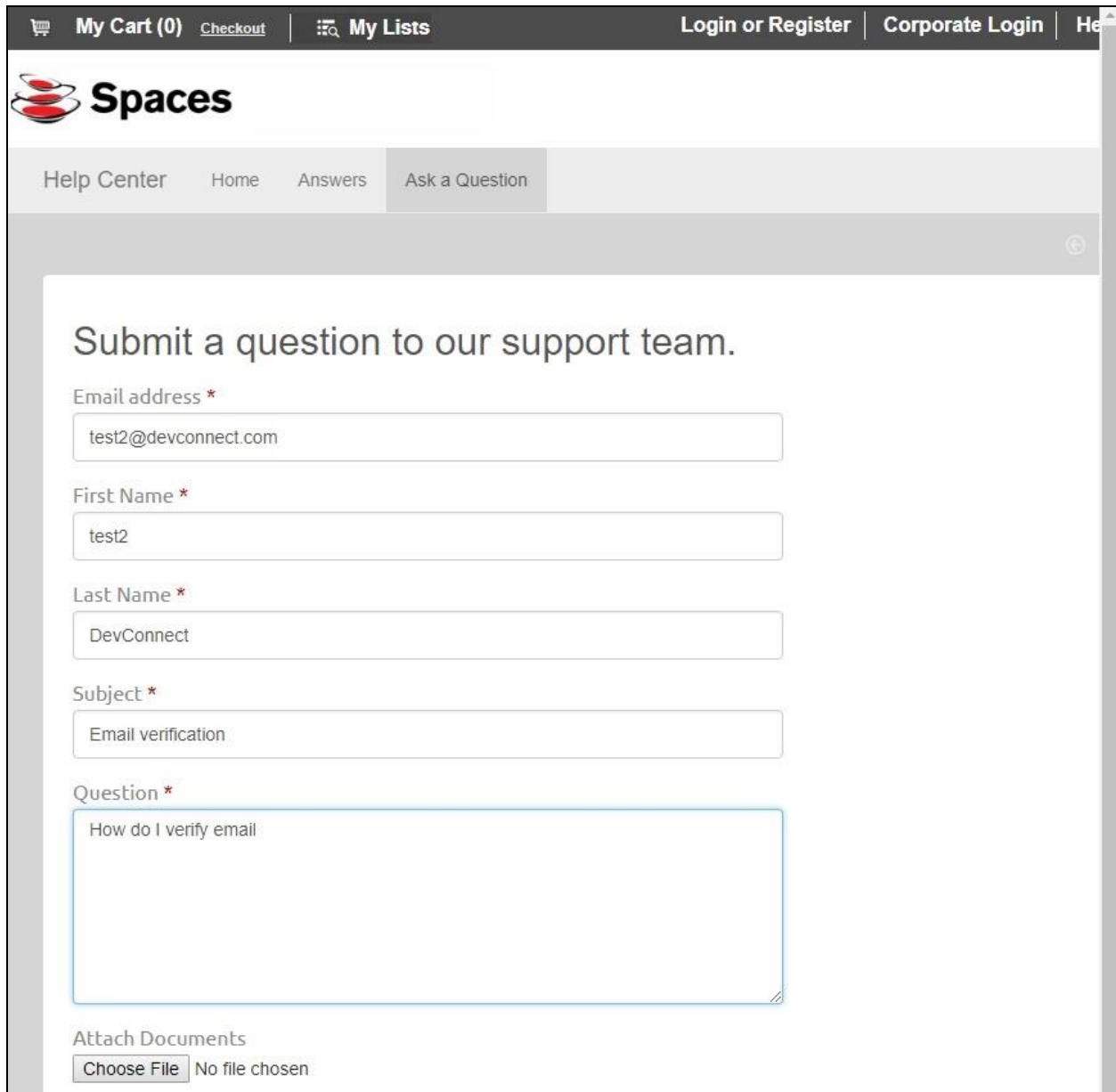


Verify that the agent is connected to the PSTN caller with two-way talk path, and that the left pane is updated to reflect the connected call. Also verify that a tab with a case number is automatically populated in the right pane, along with the matching customer record in the **Contact Details** sub-section.



### 9.3.2. Verify Email

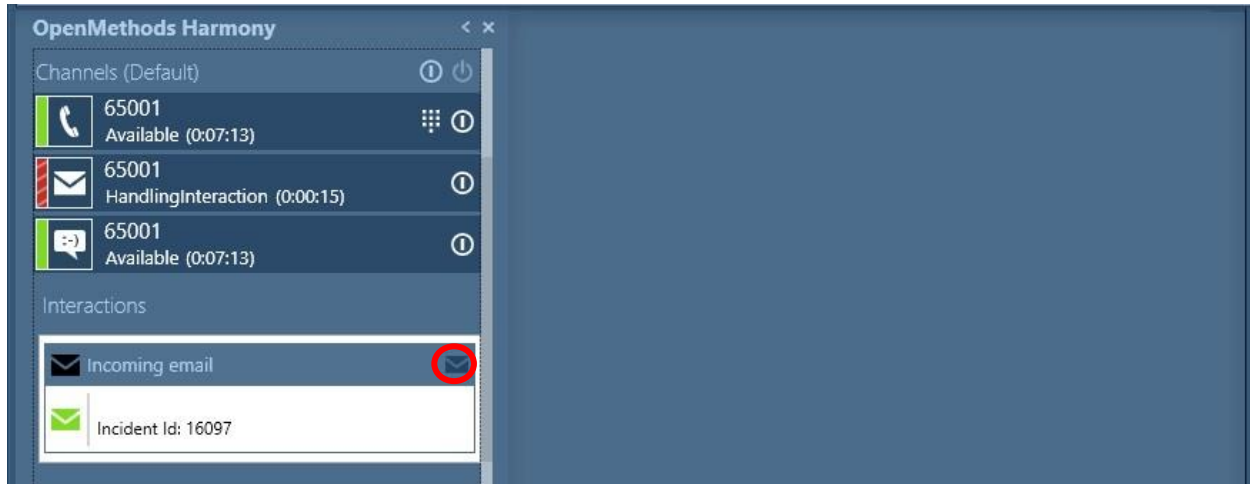
Use the URL provided by the customer to initiate an email from the Internet.



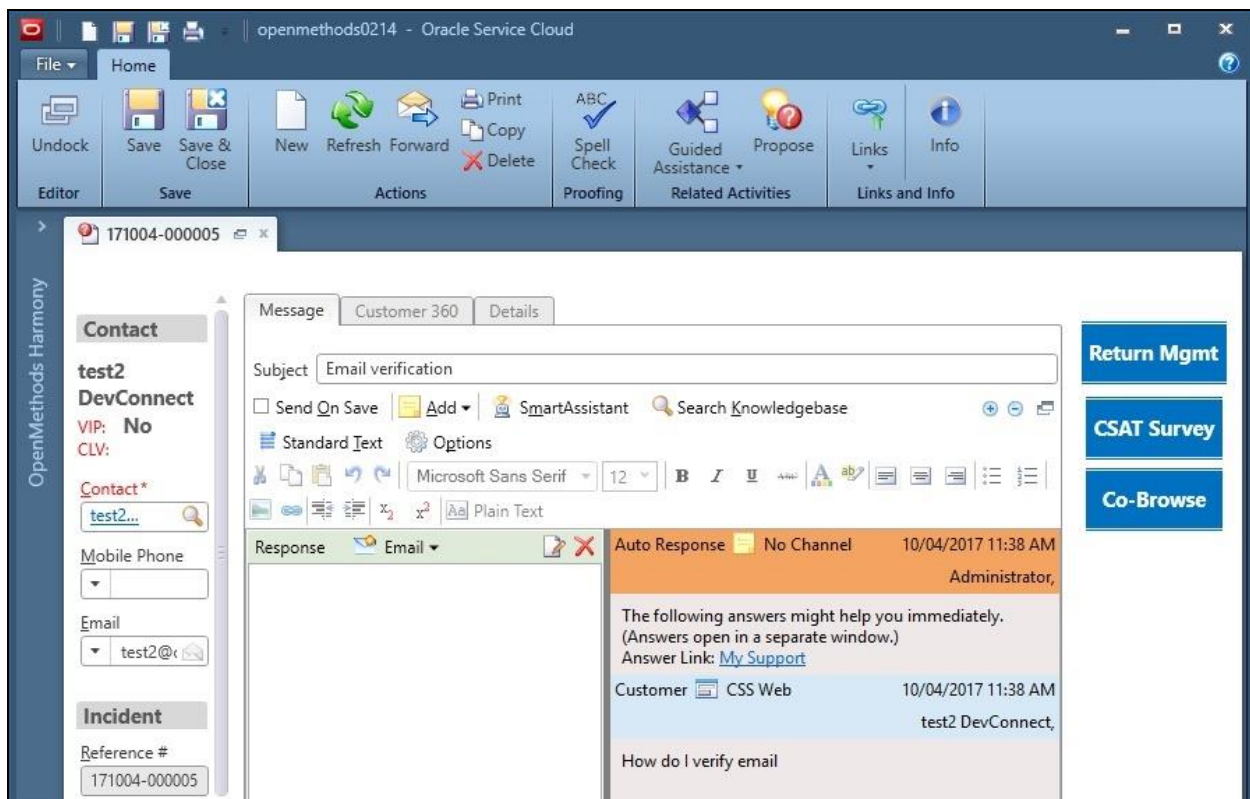
The screenshot shows the 'Ask a Question' page on the Spaces website. The header includes navigation links for 'My Cart (0)', 'Checkout', 'My Lists', 'Login or Register', 'Corporate Login', and 'Help Center'. The main navigation bar contains 'Help Center', 'Home', 'Answers', and 'Ask a Question'. The form is titled 'Submit a question to our support team.' and contains the following fields:

- Email address \***: A text input field containing 'test2@devconnect.com'.
- First Name \***: A text input field containing 'test2'.
- Last Name \***: A text input field containing 'DevConnect'.
- Subject \***: A text input field containing 'Email verification'.
- Question \***: A large text area containing 'How do I verify email'.
- Attach Documents**: A section with a 'Choose File' button and the text 'No file chosen'.

Verify that up to 60 seconds later, the left pane of an available agent is updated to reflect **HandlingInteraction** for the email channel. Also verify that the **Interactions** sub-section reflects “Incoming email” along with an incident ID. Click on the **Accept email** icon below to accept the email.

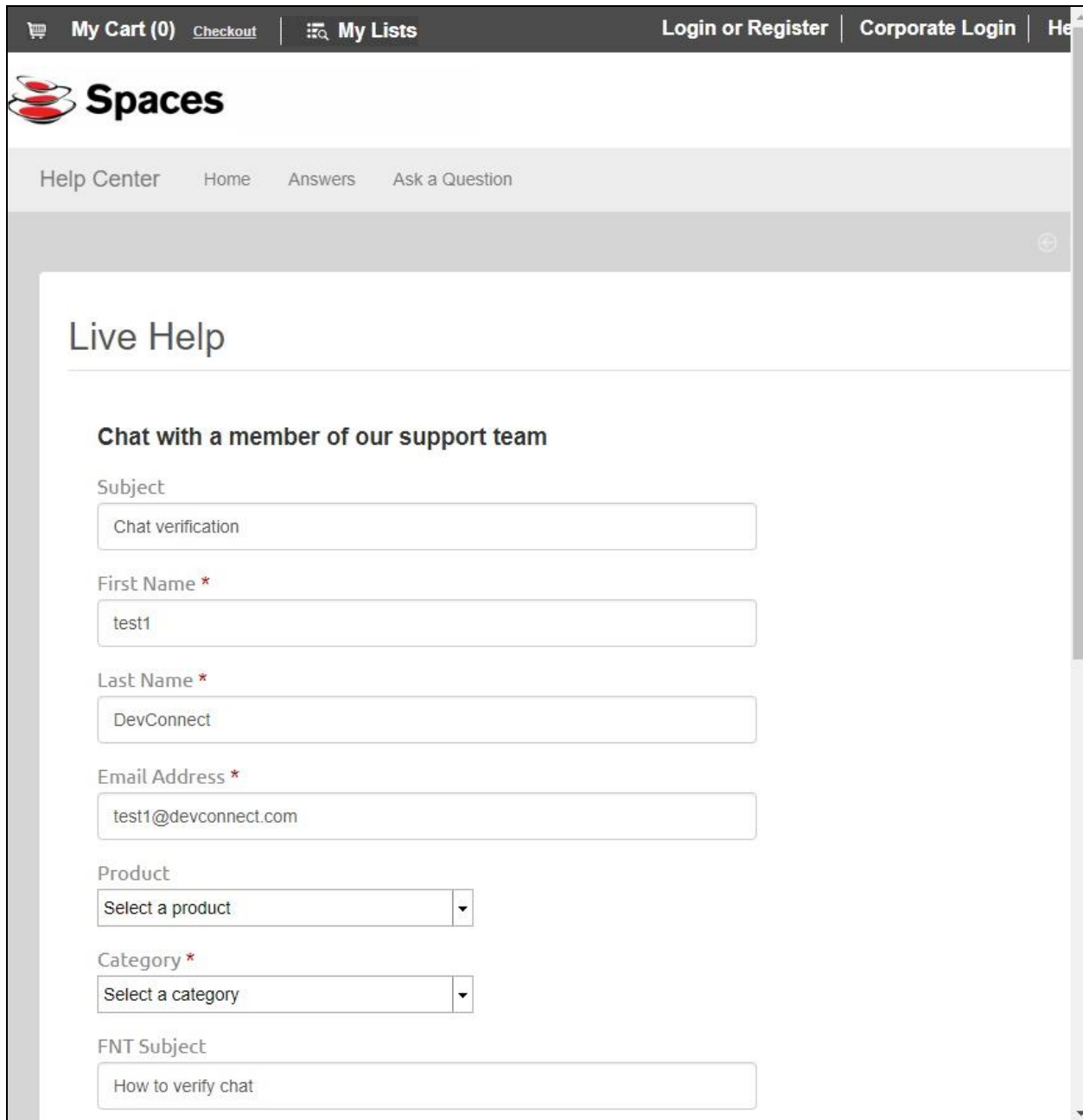


Verify that the agent telephone is connected to the phantom call for the email work item. Also verify that a case tab is automatically populated in the right pane, along with contents of the email, as shown below.




### 9.3.3. Verify Chat

Use the URL provided by the customer to initiate a chat from the Internet.



The screenshot shows the 'Spaces' website's 'Live Help' section. At the top, there is a navigation bar with links for 'My Cart (0)', 'Checkout', 'My Lists', 'Login or Register', 'Corporate Login', and 'Help Center'. Below this is a secondary navigation bar with 'Home', 'Answers', and 'Ask a Question'. The main content area is titled 'Live Help' and contains a section 'Chat with a member of our support team'. This section includes several input fields: 'Subject' (with 'Chat verification'), 'First Name \*' (with 'test1'), 'Last Name \*' (with 'DevConnect'), 'Email Address \*' (with 'test1@devconnect.com'), 'Product' (a dropdown menu with 'Select a product'), 'Category \*' (a dropdown menu with 'Select a category'), and 'FNT Subject' (with 'How to verify chat').

My Cart (0) [Checkout](#) | [My Lists](#) | [Login or Register](#) | [Corporate Login](#) | [Help Center](#)

 **Spaces**

[Help Center](#) | [Home](#) | [Answers](#) | [Ask a Question](#)

## Live Help

**Chat with a member of our support team**

Subject

First Name \*

Last Name \*

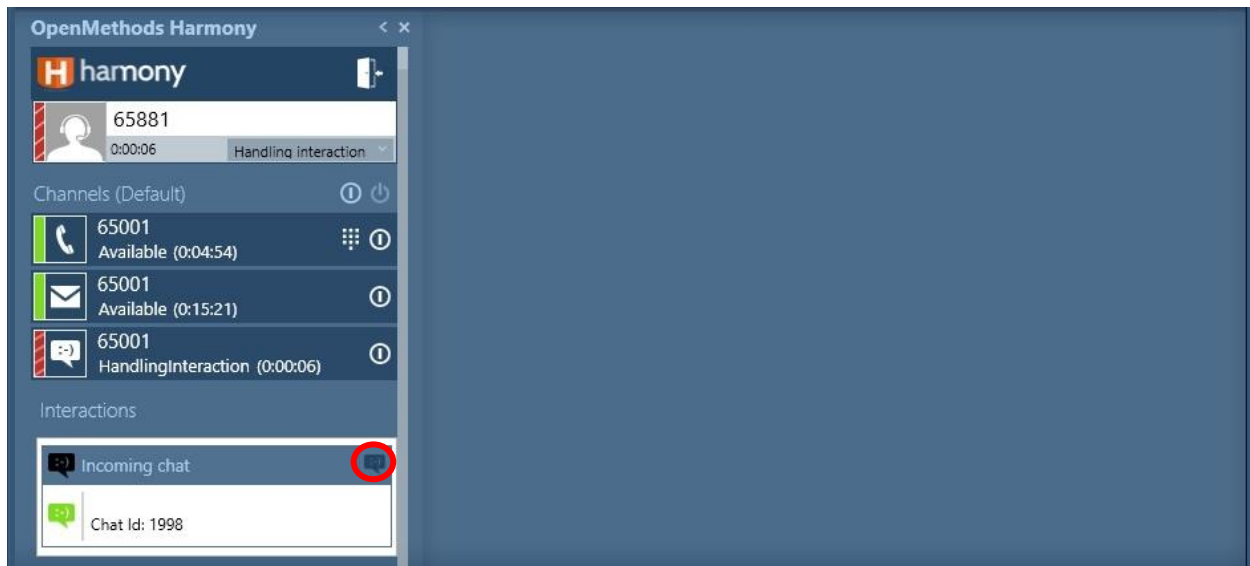
Email Address \*

Product

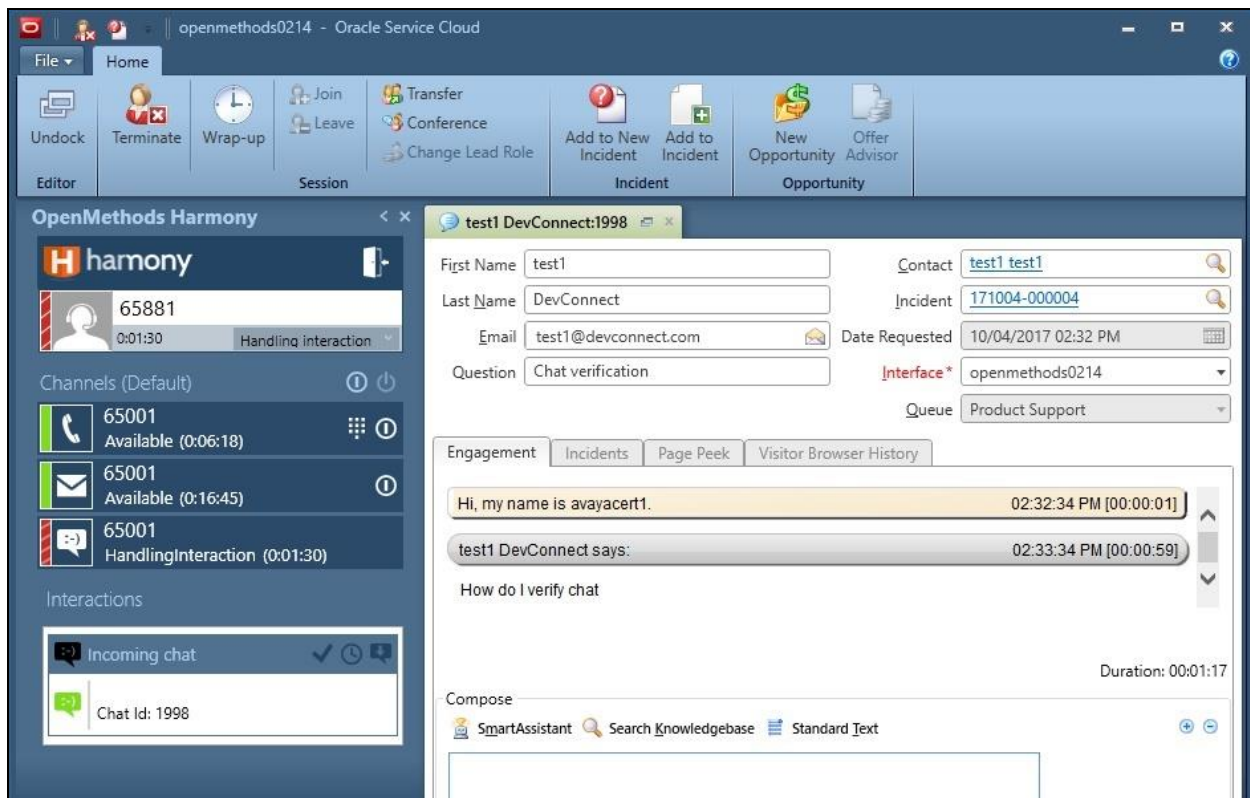
Category \*

FNT Subject

Verify that the left pane of an available agent is updated to reflect **HandlingInteraction** for the chat channel. Also verify that the **Interactions** sub-section reflects “Incoming chat” along with an incident ID. Click on the **Accept chat** icon below to accept the chat.



Verify that the agent telephone is connected to the phantom call for the chat work item. Also verify that a case tab is automatically populated in the right pane, along with content of the chat, as shown below.



## 10. Conclusion

These Application Notes describe the configuration steps required for OpenMethods Harmony 4.0 to successfully interoperate with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1 using Oracle Service Cloud. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

## 11. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 7.1.1, Issue 2, August 2017, available at <http://support.avaya.com>.
2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.1.1, Issue 3, September 2017, available at <http://support.avaya.com>.
3. *OpenMethods Harmony Avaya Administrator Configuration Notes*, V0.0.0, available upon request to OpenMethods support at [care@openmethods.com](mailto:care@openmethods.com).
4. *Harmony Configuration User Guide for Avaya 2016 Q4*, V0.0.0, January 2017, available upon request to OpenMethods support at [care@openmethods.com](mailto:care@openmethods.com).
5. *Harmony User Guide for Avaya 2016 Q4*, V4.0.124, January 2017, available upon request to OpenMethods support at [care@openmethods.com](mailto:care@openmethods.com).



---

**©2017 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).