



Avaya Solution & Interoperability Test Lab

Application Notes for Beta80 IO and emma CAD CTI with Avaya Aura® Communication Manager R7.0 using Avaya one-X Agent 2.5 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Beta80 IO and emma CAD CTI Integration with Avaya Aura® Communication Manager R7.0 using Avaya one-X Agent 2.5. Beta 80 IO and emma CAD CTI platform Provides a Graphical User Interface with Avaya Aura providing Public Safety Answering Points for emergency service calls.

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

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

1. Introduction

These Application Notes describe the configuration steps required to integrate Beta80 IO and emma CAD CTI Integration with Avaya Aura® Communication Manager R7.0 using Avaya one-X Agent 2.5. The Beta 80 IO and emma CAD CTI platform provides a Graphical User Interface providing Public Safety Answering Points (PSAP) for emergency service calls. Beta 80 CAD platform complements Avaya Aura in providing Public Safety Answering Points (PSAP) using a complete, full featured, Computer Aided Dispatch platform; CAD helps PSAP professionals to streamline emergency calls processing by automatically retrieving and displaying the caller's position, suggesting standard operating procedures Agents and dispatchers have to follow given the specific call for service (CFS), monitoring dispatched units and providing necessary information for dispatchers to assure a quick and effective engagement of first responders and resources upon the creation of new incidents.

2. General Test Approach and Test Results

The general test approach was to configure the IO and emma CAD CTI platform to communicate with one-X Agent to allow calls to be identified when routed from a Communication Manager VDN.

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 Avaya systems and the Beta 80 CAD CTI did not include use of any specific encryption features as requested by Beta80.

2.1. Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on interacting with the CAD CTI Platform in different call scenarios. The tests included:

- Make Call
- Call pick up & CLI Import
- Call hang up

2.2. Test Results

All test cases were passed with the following observations.

2.3. Support

E-Mail: sales@beta80group.com

Internet: www.beta80group.com

3. Reference Configuration

The configuration shown in Figure 1 was used during the compliance test of Beta 80 CAD CTI, with Communication Manager using one-X Agent.

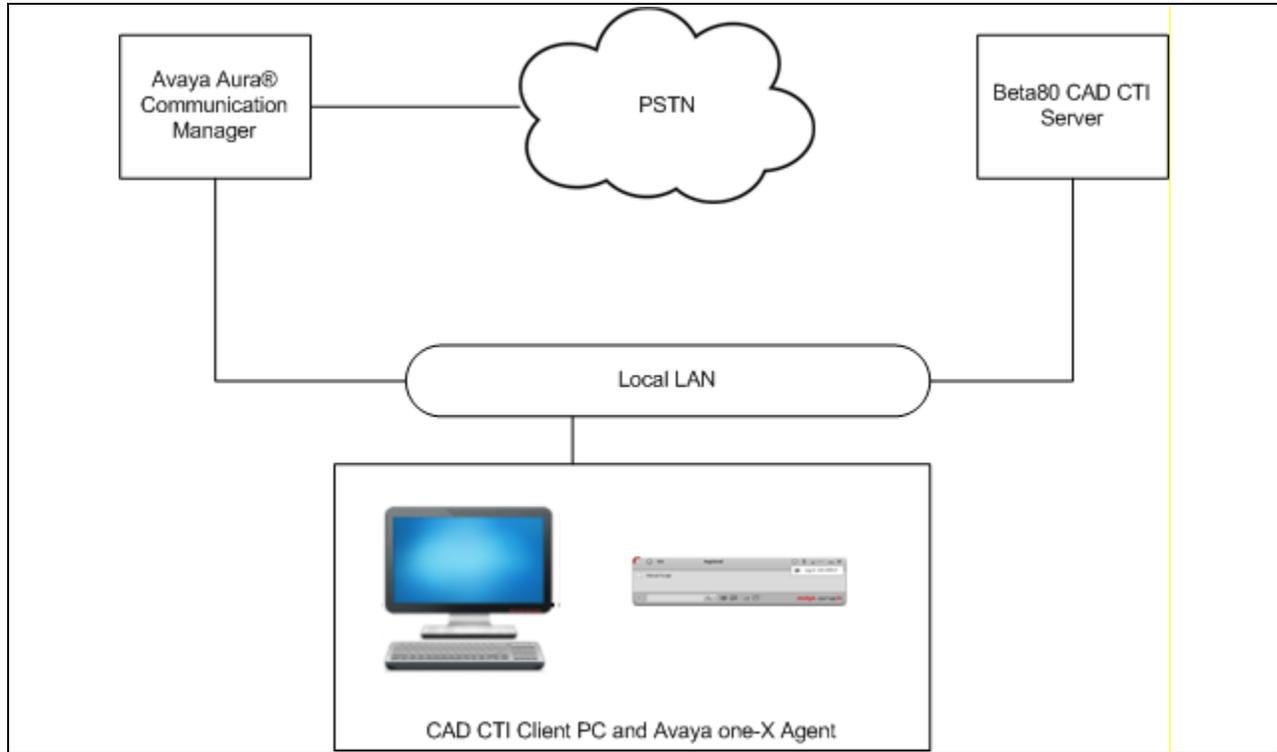


Figure 1: Beta80 CAD CTI with Application Enablement Services

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on a VMware Virtual Machine	7.0.1.2.0-FP1SP2
Avaya one-X Agent H323	2.5.10
Beta 80 EMMA	6.4.0.0

5. Configure Avaya Aura® Communication Manager

The information provided in this section describes the configuration of Communication Manager relevant to this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

The configuration illustrated in this section was performed using Communication Manager System Administration Terminal (SAT).

5.1. Verify System Features

Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 11**, ensure that **IP_Agent** has a sufficient number to allow the required one-X Agent instances.

```
display system-parameters customer-options                               Page 11 of 12
                                MAXIMUM IP REGISTRATIONS BY PRODUCT ID
```

Product ID	Rel. Limit	Used
AgentSC	* : 2400	0
IP_API_A	* : 2400	0
IP_Agent	* : 2400	2
IP_NonAgt	* : 2400	0
IP_Phone	* : 2400	4
IP_ROMax	* : 2400	0
IP_Soft	* : 2400	0
IP_Supv	* : 2400	0
IP_eCons	* : 68	0
oneX_Comm	* : 2400	1

5.2. Add a Softphone extension

Use **add station x** where x is the extension used for one-X agent. Enter a **Security Code** that will be used to log into one-X Agent. Set **IP SoftPhone** to **y**

```
add station 8230004                                     Page 1 of 5
                                                    STATION
Extension: 823-0004                                     Lock Messages? n          BCC: M
Type: 9640                                             Security Code: *         TN: 1
Port: S00003                                          Coverage Path 1:         COR: 1
Name: Station 8230004                                Coverage Path 2:         COS: 1
                                                    Hunt-to Station:         Tests? y

STATION OPTIONS
Loss Group: 19                                         Time of Day Lock Table:
Personalized Ringing Pattern: 1
Message Lamp Ext: 823-0004
Mute Button Enabled? y
Button Modules: 0
Speakerphone: 2-way
Display Language: english
Survivable GK Node Name:
Survivable COR: internal
Survivable Trunk Dest? y
Media Complex Ext:
IP SoftPhone? y
IP Video Softphone? y
Short/Prefixed Registration Allowed: default
Customizable Labels? y
```

5.3. Add an Agent-LoginID

Use **add agent-loginID x** where x is the agent extension used for one-X agent. On **Page 1** enter a **Password** and **Password (enter again)**.

```
add agent-loginID 8231004                             Page 1 of 2
                                                    AGENT LOGINID
Login ID: 823-1004                                     AAS? n
Name: Agent 8231004                                  AUDIX? n
TN: 1                                                 Check skill TNs to match agent TN? n
COR: 1
Coverage Path:                                       LWC Reception: spe
Security Code:                                       LWC Log External Calls? n
Attribute:                                           AUDIX Name for Messaging:

LoginID for ISDN/SIP Display? n
Password:
Password (enter again):
Auto Answer: station
MIA Across Skills: system
AUX Agent Remains in LOA Queue: system
AUX Agent Considered Idle (MIA): system
Work Mode on Login: system
ACW Agent Considered Idle: system
Aux Work Reason Code Type: system
Logout Reason Code Type: system
Maximum time agent in ACW before logout (sec): system
Forced Agent Logout Time:
WARNING: Agent must log in again before changes take effect
```

On **Page 2** enter the skill number (**SN**) and skill level (**SL**) administered in **Section 5.4**.

```
change agent-loginID 8231001                               Page 2 of 2
                                AGENT LOGINID
    Direct Agent Skill: 1                                Service Objective? n
Call Handling Preference: skill-level                    Local Call Preference? n

    SN  RL  SL          SN  RL  SL
1:  1   1           16:
```

5.4. Add a Hunt Group

Use add hunt-group x where x is the number of the hunt group that will be added to the agent.
On **Page 1** set **ACD**, **Queue** and **Vector** to **y**

```
add hunt-group 1                                           Page 1 of 4
                                HUNT GROUP
    Group Number: 1                                ACD? y
    Group Name: ACD Default                        Queue? y
    Group Extension: 823-3001                      Vector? y
    Group Type: ucd-mia
    TN: 1
    COR: 1                                MM Early Answer? n
    Security Code:                                Local Agent Preference? n
ISDN/SIP Caller Display:

    Queue Limit: unlimited
    Calls Warning Threshold: Port:
```

On **Page 2** set **Skill** to **y**.

```
add hunt-group 1                                           Page 2 of 4
                                HUNT GROUP
    Skill? y                                Expected Call Handling Time (sec): 180
    AAS? n
    Measured: none
    Supervisor Extension:

    Controlling Adjunct: none

    Multiple Call Handling: none

    Timed ACW Interval (sec):                    After Xfer or Held Call Drops? n
```

5.5. Add a VDN and edit Vector

Use **add vdn x** where x is the extension number of the VDN used to queue to the hunt group add in **Section 5.4**. Enter a **Name*** and **Destination** as **Vector Number** and in this example **50**. Enter the hunt group number added in **Section 5.4** as **1st Skill***.

```
add vdn 8234050                                     Page 1 of 3
                                                    VECTOR DIRECTORY NUMBER
                                                    Extension: 823-4050
                                                    Name*: Default Agent
                                                    Destination: Vector Number      50
Attendant Vectoring? n
Meet-me Conferencing? n
Allow VDN Override? n
COR: 1
TN*: 1
Measured: none      Report Adjunct Calls as ACD*? n

VDN of Origin Annc. Extension*:
1st Skill*: 1
```

Use **change vector 50** to edit the vector contents and script the queuing of calls to the hunt group added in **Section 5.4**. A line must be added to queue-to skill 1st so that calls are sent to the agents logged into the hunt group set in **Section 5.5**.

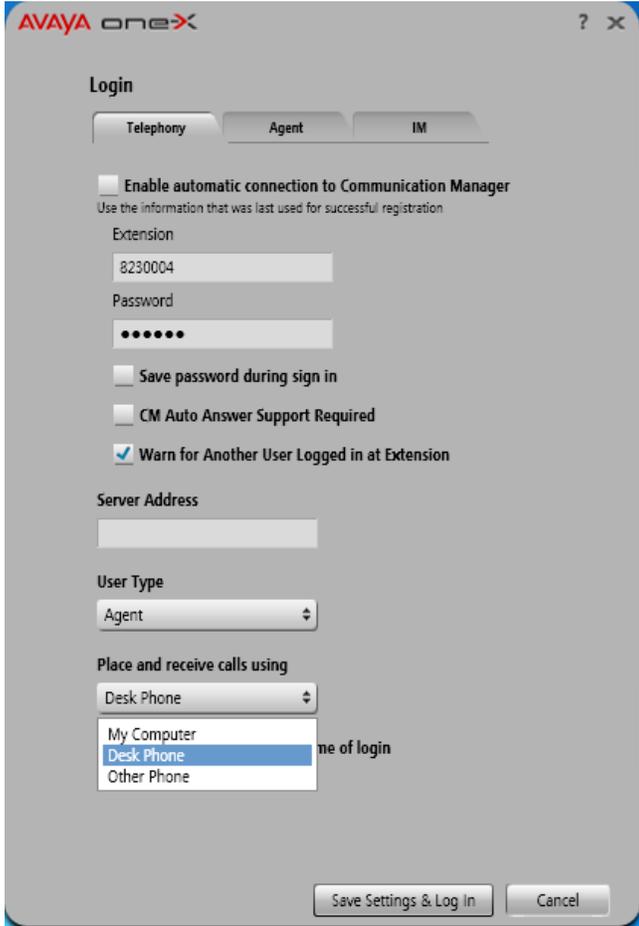
```
change vector 50                                     Page 1 of 6
                                                    CALL VECTOR
Number: 50      Name: Default Agent Route
Multimedia? n  Attendant Vectoring? n  Meet-me Conf? n  Lock? n
Basic? y      EAS? y    G3V4 Enhanced? y  ANI/II-Digits? y  ASAI Routing? y
Prompting? y  LAI? y    G3V4 Adv Route? y  CINFO? y  BSR? y  Holidays? y
Variables? y  3.0 Enhanced? y
01 wait-time  2 secs hearing ringback
02 queue-to  skill 1st pri m
03 wait-time  30 secs hearing ringback
04 goto step  3 if unconditionally
```

6. Configure Avaya one-X Agent

The information in this section describes the steps required to administer Avaya one-X Agent for the solution

6.1. Configure Station settings

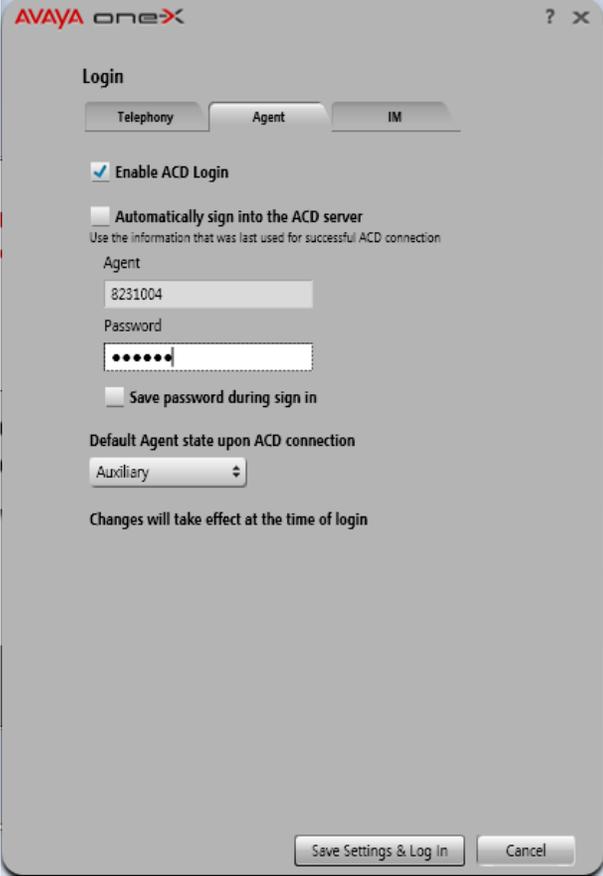
From the one-X agent application, enter the System Settings menu (not shown). On the **Telephony** tab enter the **Extension** and **Password** administered in **Section 5.2**. Set the **User Type** as **Agent** and select the required **Place and receive calls using** setting.



The screenshot shows the Avaya one-X Agent configuration window. The window title is "AVAYA one-X" and it has a standard window control bar with a question mark and a close button. The "Login" section is active, with three tabs: "Telephony", "Agent", and "IM". The "Telephony" tab is selected. Below the tabs, there is a checkbox for "Enable automatic connection to Communication Manager" with a sub-note: "Use the information that was last used for successful registration". Below this are two text input fields: "Extension" containing "8230004" and "Password" with masked characters. There are three more checkboxes: "Save password during sign in", "CM Auto Answer Support Required", and "Warn for Another User Logged in at Extension" (which is checked). Below these is a "Server Address" text input field. The "User Type" is set to "Agent" in a dropdown menu. The "Place and receive calls using" dropdown menu is open, showing three options: "My Computer", "Desk Phone" (which is highlighted), and "Other Phone". At the bottom right, there are two buttons: "Save Settings & Log In" and "Cancel".

6.2. Configure Agent Settings

From the one-X agent application, enter the System Settings menu (not shown). On the Agent tab enter the **Agent LoginID** and **Password** administered in Section 5.3. Set the **Default Agent state upon ACD Connection** to **Auxiliary**. Click on the **Save Settings and Log in** button to proceed.



The screenshot shows the AVAYA one-X Agent Login settings dialog box. The window title is "AVAYA one-X" and it has standard window controls (minimize, maximize, close). The "Login" section has three tabs: "Telephony", "Agent", and "IM", with "Agent" selected. Under "Agent", there are several options: "Enable ACD Login" is checked; "Automatically sign into the ACD server" is unchecked, with a note below it: "Use the information that was last used for successful ACD connection"; the "Agent" field contains "8231004"; the "Password" field is masked with dots; "Save password during sign in" is unchecked. The "Default Agent state upon ACD connection" is set to "Auxiliary" via a dropdown menu. At the bottom, there are two buttons: "Save Settings & Log In" and "Cancel". A note at the bottom states: "Changes will take effect at the time of login".

7. Configure Beta 80 CAD CTI

Once PSAP's positions have been created and enabled for use of the One-X agent API connector, it is possible to configure each CAD client to handshake with the co-resident One-X Agent.

For each CAD client, the relevant "INI" file has to be configured with the following instructions:

```
<!-- Sezione di configurazione dedicata ad Avaya -->
<!-- ACDIntegrationType key value:
1 = ACD with no automatic answer
2 = ACD with automatic answer
-->
<AvayaSection
  RegistryKey="SOFTWARE\Avaya\Avaya one-X Agent\Settings"
  URIBase="http://127.0.0.1:{0}/onexagent/api/"
  URIRegister="{0}registerclient?name={1}"
  URIUnregister="{0}unregisterclient?clientid={1}"
  URINotification="{0}nextnotification?clientid={1}"
  URIMakeCall="{0}voice/makecall?clientid={1}&number={2}"
  URIMute="{0}voice/mute?clientid={1}"
  URIUnmute="{0}voice/unmute?clientid={1}"
  URIAccept="{0}voice/accept?clientid={1}&interactionid={2}"
  URIRelease="{0}voice/release?clientid={1}&interactionid={2}"
  URIHold="{0}voice/hold?clientid={1}&interactionid={2}"
  URIUnhold="{0}voice/unhold?clientid={1}&interactionid={2}"
  NotificationRequestInterval="250"
  RegExCallIdParsing="{&lt;beforePhoneNumber&gt;[\w]{0}} (?&lt;phoneNumber&gt;+[0,1]\d{1,20}) (?&lt;afterPhoneNumber&gt;[\w]{0})"
  ACDIntegrationType="1"
  ExtendedEventLogs="true"
/>
<!-- ***** -->
```

In this file, the One-X Agent's APIs are properly configured (from *URIBase* to *RegExCallIdParsing*); the last two parameters, i.e. "*ACDIntegrationType*" and "*ExtendedEventLogs*", are emma / iO CAD specific values:

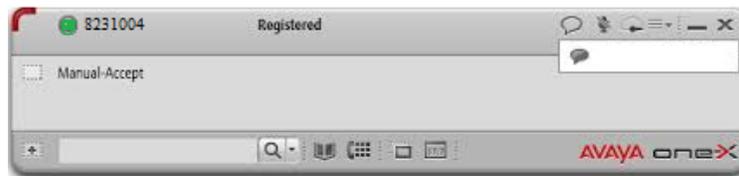
- The *ACDIntegrationType* parameter represents the "auto answer"/"No auto answer" option: the value "1" means that auto answer mode is off, the value "2" means that the auto answer feature is on. This configuration has to match the One-X Agent auto answer settings.
- The *ExtendedEventLogs* parameter enables extended log capture

8. Verification Steps

This section provides the tests that can be performed to verify correct configuration of the Avaya and the Beta80 CAD CTI solution.

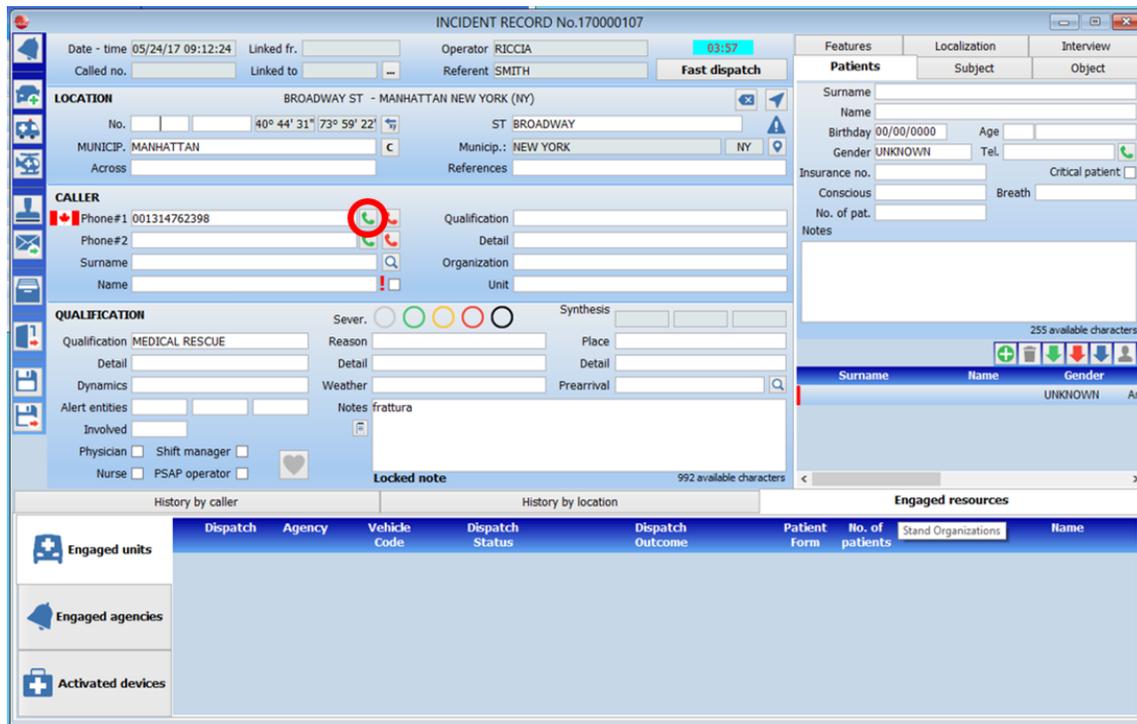
8.1. Verify Avaya one-X agent

The following steps can validate that the Avaya one-X Agent application is logged in and working. The top bar shows the Agent LoginID and shows as Green for Available. A Call should be placed to the VDN number and the call is routed to the Agent.



8.2. Verify Beta 80 CAD CTI

The following shows that the CAD Client is logged in, a call has been answered and the CLI has been correctly imported.



9. Conclusion

These Application Notes describe the configuration steps required for Beta80 CAD CTI to successfully interoperate with Avaya Aura® Communication Manager R7.0 using Avaya one-X Agent 2.5. All feature functionality and serviceability test cases were completed successfully as outlined in **Section 2.2**.

10. Additional References

This section references the Avaya and Beta80 product documentation that are relevant to these Application Notes.

Product documentation for Avaya products may be found at <https://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document ID 555-245-205
- [3] *Avaya one-X Agent Administration and Maintenance Guide Release 2.5*

Product documentation for Beta80 can be obtained as follows:

E-Mail: sales@beta80group.com

Internet: www.beta80group.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.