



Application Notes for Mattersight Call Recording Solution with Avaya Aura® Communication Manager Using Multi Registration with Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Mattersight Call Recording Solution to interoperate with Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services.

Mattersight Call Recording Solution is a call recording solution. In the compliance testing, Mattersight Call Recording Solution used the Device, Media, and Call Control interface from Avaya Aura® Application Enablement Services to monitor skill group and agent station extensions on Avaya Aura® Communication Manager, and to capture the media associated with the monitored agents for call recording.

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 the Mattersight Call Recording Solution to interoperate with Avaya Aura® Communication Manager 7 using Avaya Aura® Application Enablement Services 7.

The Mattersight Call Recording Solution is a call recording solution. In the compliance testing, Mattersight Call Recording Solution used the Device, Media, and Call Control (DMCC) interface from Avaya Aura® Application Enablement Services to monitor skill group and agent station extensions on Avaya Aura® Communication Manager, and to capture the media associated with the monitored agents for call recording.

When there is an active call on the monitored agent, Mattersight Call Recording Solution is informed of the call via event reports from the DMCC interface. Mattersight Call Recording Solution starts the call recording by using Avaya Multi Registration from the DMCC interface to add virtual IP softphone to the active call to obtain the media. The event reports are also used to determine when to stop the call recordings. Multi Registration is only available on H323 phones

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Call Recording Solution application, the application automatically uses DMCC to register the virtual IP softphones to Communication Manager, and to request monitoring on the recording skill group and agent station extensions.

For the manual part of the testing, each call was handled manually on the agent telephone with generation of unique audio content for the recordings. Necessary user actions such as hold and reconnect were performed from the agent telephones to test the different call scenarios. The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to Call Recording Solution.

The verification tests included using the Call Recording Solution logs for proper message exchanges, and using the Retrieval application for proper logging and playback of the calls.

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

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Call Recording Solution:

- Use of DMCC registration services to register and un-register the virtual IP softphones.
- Use of DMCC monitoring services to monitor agent stations and virtual IP softphones.
- Use of DMCC call control service to activate multi registration on an agent phone when a call is active and to obtain the media for call recording.
- Proper recording, logging, and playback of calls for scenarios involving G711, G729, inbound, outbound, internal, external, ACD, non-ACD, hold, reconnect, simultaneous calls, simultaneous agents, conference, transfer and long call duration.

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

2.2. Test Results

All test cases were executed, and the following were observations on Call Recording Solution from the compliance testing:

- The User interface to display recordings is not part of this solution therefore the test audio files created after the call completed were played from Windows File Explorer. Call details such as DNIS, Call Type, Call Direction (Meta data) were reviewed separately.
- Agents must be a member of a specific skill group in order to be recorded.
- If the agent is reskilled without using the Avaya CMS tool the agent will need to log out and log back in for the skill changes to take effect.
- During the call if a user performs actions such as pressing the Transfer button on desk phone and then pressing the Cancel or Clear button this will trigger AES to send a Call Clear event and Mattersight will stop recording the second leg of the call. The first leg of the call will continue to be recorded.
- When an agent is active on a call that is being monitored and recorded, and the agent places another call (by using transfer, conference, or hold) to a destination that is not monitored, the call to the non-monitored destination will not be recorded. Mattersight has indicated that this is working as designed.
- For a call between 2 internal agents, only 1 recording will be created.
- The voice quality of a recorded G729 call is not as clear as a G.711 call.

2.3. Support

Technical support on Mattersight Call Recording Solution can be obtained through the following:

- **Phone:** 877.235.6925
- **Email:** support@mattersight.com

3. Reference Configuration

Call Recording Solution is a SaaS (Software as a service solution) offering. Mattersight will design an appropriately sized solution based on several factors to include concurrent calls, calls per second and concurrent agents. The compliance test used a single server configuration shown in **Figure 1**.

The detailed administration of basic connectivity between Communication Manager, Application Enablement Services and contact center devices is not the focus of these Application Notes and will not be described.

In the compliance testing, the contact center devices consisted of two VDNs, two skill groups, one supervisor, two agents and two H323 stations as shown in the table below.

Device Type	Extension
VDN	56001, 56010
Skill/Hunt Group	56300, 56303
Agent ID	1000, 1004
Agent Station	56101, 56106
Supervisor	56102

A new hunt group will need to be created so the Mattersight CRS application can keep track of the agents that need to be recorded. For testing, skill group 5 with extension 56304 was used. All agents that are in-scope for call recording would need to have this skill assigned to them. For this example agent 1000 and 1004 were added to skill group 5.

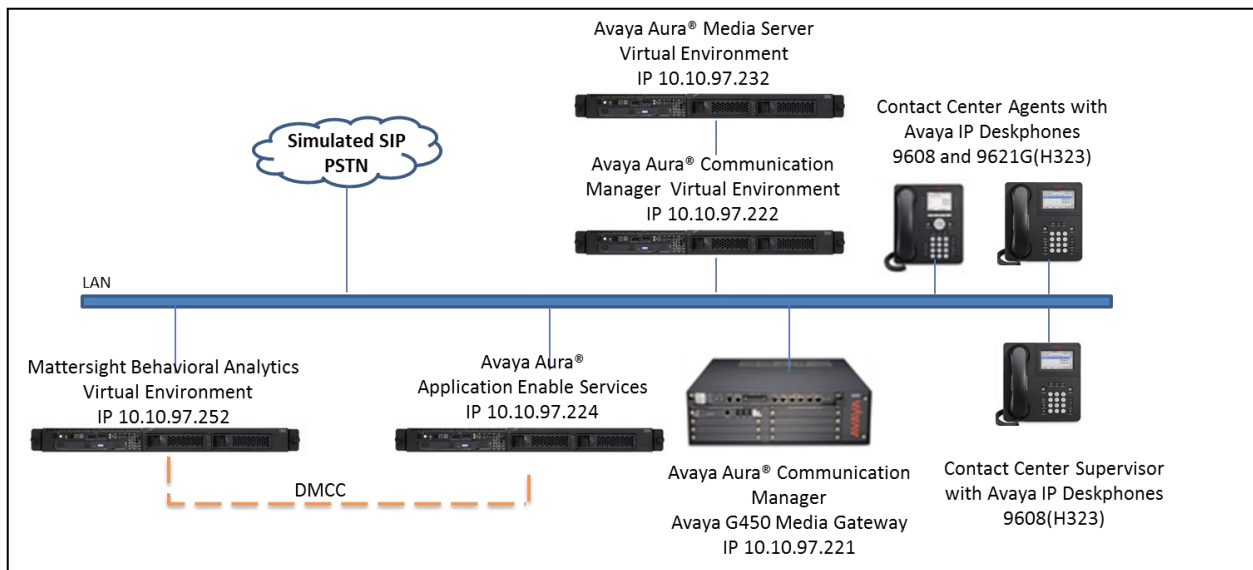


Figure 1: Compliance Testing Configuration

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	7.0.2
Avaya G450 Media Gateway	7.0.1.1
Avaya Aura® Media Server in Virtual Environment	7.7.0.334
Avaya Aura® Application Enablement Services in Virtual Environment	7.0.1 Super Patch 3
Avaya 9608, 9621G IP Deskphone (H.323)	6.6229
MatterSight Call Recording Solution on Windows 2012R2 Server <ul style="list-style-type: none">• Avaya DMCC .NET (ServiceProvider.dll)	4.0 SP 2 6.2.0.29

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
- Administer System Parameters Features
- Administer Recording Hunt Group
- Update Agent's Phone to support Multi-registration

5.1. Verify License

Log in to the System Access Terminal (SAT) 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 to verify that the **Computer Telephony Adjunct Links** customer option is set to “y” on **Page 4**. 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                                         Computer Telephony Adjunct Links? y
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
Async. Transfer Mode (ATM) PNC? n            Digital Loss Plan Modification? y
Async. Transfer Mode (ATM) Trunking? n       DS1 MSP? y
ATM WAN Spare Processor? n                   DS1 Echo Cancellation? y
ATMS? y
Attendant Vectoring? y
(NOTE: You must logoff & login to effect the permission changes.)
```

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: 56001
  Type: ADJ-IP
                                         COR: 1
Name: DevvmAES
```

5.3. 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: 1
```


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

```

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 UUI During Conference/Transfer? n
    Call Classification After Answer Supervision? n
        Send UCID to ASAI? y
    For ASAI Send DTMF Tone to Call Originator? y
    Send Connect Event to ASAI For Announcement Answer? n
  
```

5.4. Administer Hunt Group

A new hunt group will need to be created so the Mattersight CRS application can keep track of the agents that need to be recorded. All agents that are in-scope for call recording would need to have this skill assigned to them. Below is the configuration for **hunt group 5**.

```

display hunt-group 5                                             Page 1 of 4
          HUNT GROUP
    Group Number: 5                                           ACD? y
    Group Name: Basic 3                                       Queue? y
    Group Extension: 56304                                    Vector? y
    Group Type: ucd-mia
        TN: 1
        COR: 1                                           MM Early Answer? n
    Security Code:                                           Local Agent Preference? n
ISDN/SIP Caller Display:
    Queue Limit: unlimited
    Calls Warning Threshold: Port:
    Time Warning Threshold: Port:
  
```

5.5. Update Agent's Phone to support Multi-registration

The agent phone must be assigned to a Class of Restriction that has Service Observe and Service Observer allowed. In addition the IP Softphone and 2-way speakerphone must be enabled to activate multi-registration and capture media. Change the agent's phone using the "change station n" command, where "n" is the agent's extension number. Enable the following values for the specified fields, and retain the default values for the remaining fields.

- **Extension:** The assigned extension number.
- **COR:** Ensure the COR allows Service Observe and Service Observer
- **IP SoftPhone:** Set to "y".
- **Speakerphone:** 2-way

```
add station 56114                                     Page 1 of 5
                                                    STATION
Extension: 56114                                Lock Messages? n                BCC: 0
Type: 9620                                         Security Code: *-              TN: 1
Port: S00067                                       Coverage Path 1:              COR: 1
Name: Agent Phone #1                             Coverage Path 2:              COS: 1
                                                    Hunt-to Station:              Tests: y

STATION OPTIONS
                                                    Time of Day Lock Table:
Loss Group: 19                                     Personalized Ringing Pattern: 1
                                                    Message Lamp Ext: 56114
Speakerphone: 2-way                             Mute Button Enabled? y
Display Language: english                         Expansion Module? n
Survivable GK Node Name:                          Media Complex Ext:
Survivable COR: internal                           IP SoftPhone? y
Survivable Trunk Dest? y                          IP Video Softphone? n
                                                    Short/Prefixed Registration Allowed: default
                                                    Customizable Labels? Y
```

6. Configure Avaya Aura® Application Enablement Services

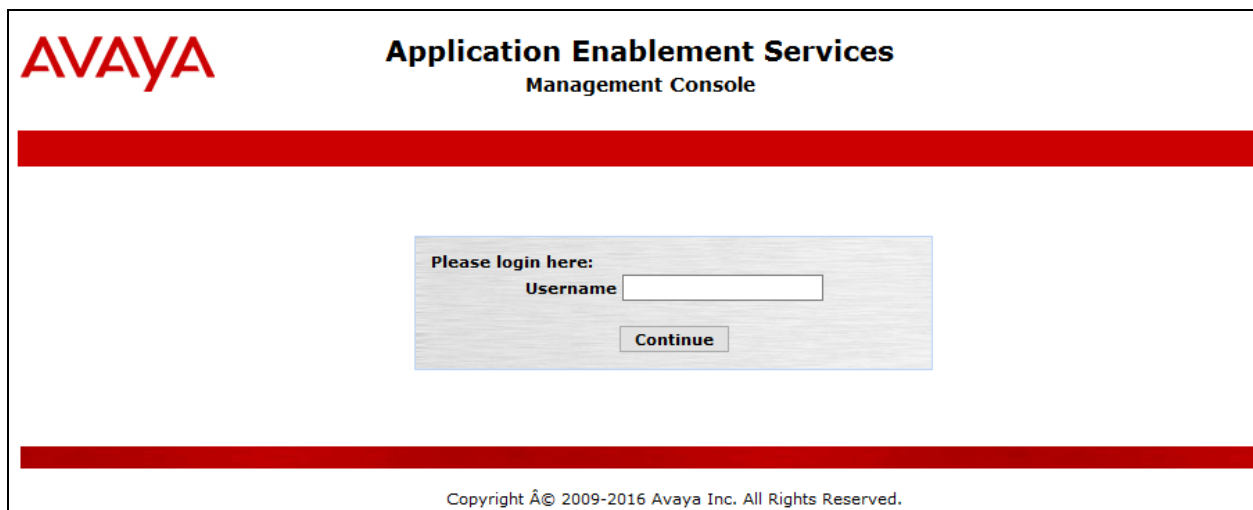
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- Disable security database
- Restart services
- Administer Call Recording Solution user
- Provide Call Recording Solution User unrestricted access
- Administer ports

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 logo on the left and the title "Application Enablement Services Management Console" in the center. Below the title is a red horizontal bar. In the center of the page is a login box with the text "Please login here:" followed by a "Username" label and a text input field. Below the input field is a "Continue" button. At the bottom of the page is another red horizontal bar and the copyright notice "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

The **Welcome to OAM** screen is displayed as below.

The screenshot shows the Avaya Application Enablement Services Management Console. The top left features the Avaya logo. The top center displays the title 'Application Enablement Services Management Console'. The top right corner contains system information: 'Number of prior failed login attempts: 1', 'HostName/IP: devvmaes/135.10.97.224', 'Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE', 'SW Version: 7.0.1.0.3.15-0', 'Server Date and Time: Wed Mar 22 22:01:33 EDT 2017', and 'HA Status: Not Configured'. A red navigation bar at the top contains 'Home' on the left and 'Home | Help | Logout' on the right. On the left side, there is a vertical menu with options: 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 the following text: 'The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:'. Below this text is a bulleted list of administrative domains and their corresponding management tasks.

AVAYA Application Enablement Services Management Console

Number of prior failed login attempts: 1
HostName/IP: devvmaes/135.10.97.224
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Wed Mar 22 22:01:33 EDT 2017
HA Status: Not Configured

Home Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- 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.

6.2. Verify License

Select **Licensing** → **WebLM Server Access** in the left pane to display the **Web License Manager** pop-up screen (not shown), and log in using the appropriate credentials.

The screenshot shows the Avaya Application Enablement Services Management Console with the 'Licensing' section selected. The top left features the Avaya logo. The top center displays the title 'Application Enablement Services Management Console'. The top right corner contains system information: 'Welcome: User cust', 'Last login: Tue Nov 8 10:49:27 2016 from phuongpc252.bvwdev.com', 'Number of prior failed login attempts: 0', 'HostName/IP: devvmaes/135.10.97.224', 'Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE', 'SW Version: 7.0.1.0.2.15-0', 'Server Date and Time: Tue Nov 15 13:13:32 EST 2016', and 'HA Status: Not Configured'. A red navigation bar at the top contains 'Licensing' on the left and 'Home | Help | Logout' on the right. On the left side, there is a vertical menu with options: AE Services, Communication Manager Interface, High Availability, Licensing, WebLM Server Address, WebLM Server Access, Reserved Licenses, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled 'Licensing' and contains the following text: 'If you are setting up and maintaining the WebLM, you need to use the following:'. Below this text is a bulleted list of 'WebLM Server Address'. The next paragraph states: 'If you are importing, setting up and maintaining the license, you need to use the following:'. Below this text is a bulleted list of 'WebLM Server Access'. The third paragraph states: 'If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:'. Below this text is a bulleted list of 'Reserved Licenses'. At the bottom of the main content area, there is a red note: 'NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page'.

AVAYA Application Enablement Services Management Console

Welcome: User cust
Last login: Tue Nov 8 10:49:27 2016 from phuongpc252.bvwdev.com
Number of prior failed login attempts: 0
HostName/IP: devvmaes/135.10.97.224
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Nov 15 13:13:32 EST 2016
HA Status: Not Configured

Licensing Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
WebLM Server Address
WebLM Server Access
Reserved Licenses
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page

The **WebLM** screen below is displayed. 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** and **Device Media and Call Control**, as shown below. Note that the TSAPI license is used for monitoring and call control via DMCC, and the DMCC license is used for the virtual IP softphones.

WebLM Home	Application Enablement (CTI) - Release: 7 - SID: 10503000 Stat																							
Install license	You are here: Licensed Products > Application_Enablement > View License Capacity																							
Licensed products	License installed on: October 13, 2015 6:25:48 AM -04:00																							
APPL_ENAB	<p style="text-align: center;">License File Host IDs: ██████████</p>																							
▼ Application_Enablement	Licensed Features																							
View license capacity	<p>10 Items Show <input type="text" value="All"/> ▼</p> <table border="1"> <thead> <tr> <th>Feature (License Keyword)</th> <th>Expiration date</th> <th>Licensed capacity</th> </tr> </thead> <tbody> <tr> <td>Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP</td> <td>permanent</td> <td>1000</td> </tr> <tr> <td>CVLAN ASAI VALUE_AES_CVLAN_ASAI</td> <td>permanent</td> <td>16</td> </tr> <tr> <td>Device Media and Call Control VALUE_AES_DMCC_DMC</td> <td>permanent</td> <td>1000</td> </tr> <tr> <td>AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED</td> <td>permanent</td> <td>3</td> </tr> <tr> <td>DLG VALUE_AES_DLG</td> <td>permanent</td> <td>16</td> </tr> <tr> <td>TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS</td> <td>permanent</td> <td>1000</td> </tr> </tbody> </table>			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
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																						
View peak usage																								
CCTR																								
▶ ContactCenter																								
CE																								
▶ COLLABORATION_ENVIRONMENT																								
CIE																								
▶ CIE																								
COMMUNICATION_MANAGER																								
▶ Call_Center																								
▶ Communication_Manager																								
Configure Centralized Licensing																								
MESSAGING																								
▶ Messaging																								
PRESENCE_SERVICES																								

6.3. Administer TSAPI Link

To administer a TSAPI link, select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	DevvmCM	1	7	Both

The **Add TSAPI Links** screen is displayed next (not shown), below is example of link created during compliance test.

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 “DevvmCM” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Select “7” for **ASAI Link Version** and select “Both” for **Security**.

Link: 1
Switch Connection: DevvmCM
Switch CTI Link Number: 1
ASAI Link Version: 7
Security: Both

6.4. Administer H.323 Gatekeeper

Select **Communication Manager Interface** → **Switch Connections** from the left pane. The **Switch Connections** screen shows a listing of the existing switch connections.

Locate the connection name associated with the relevant Communication Manager, in this case “S8300D”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

Communication Manager Interface | Switch Connections Home | Help | Logout

Switch Connections

Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> DevvmCM	Yes	30	1

The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to be used as H.323 gatekeeper, click **Add Name or IP**. Example below is **H323 Gatekeeper** already created with IP address of Communication Manager 10.10.97.222

AE Services

Communication Manager Interface

Switch Connections

Dial Plan

High Availability

Licensing

Edit H.323 Gatekeeper - DevvmCM

Name or IP Address

10.10.97.222

6.5. Disable 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. Uncheck both fields below, and click **Apply Changes**.

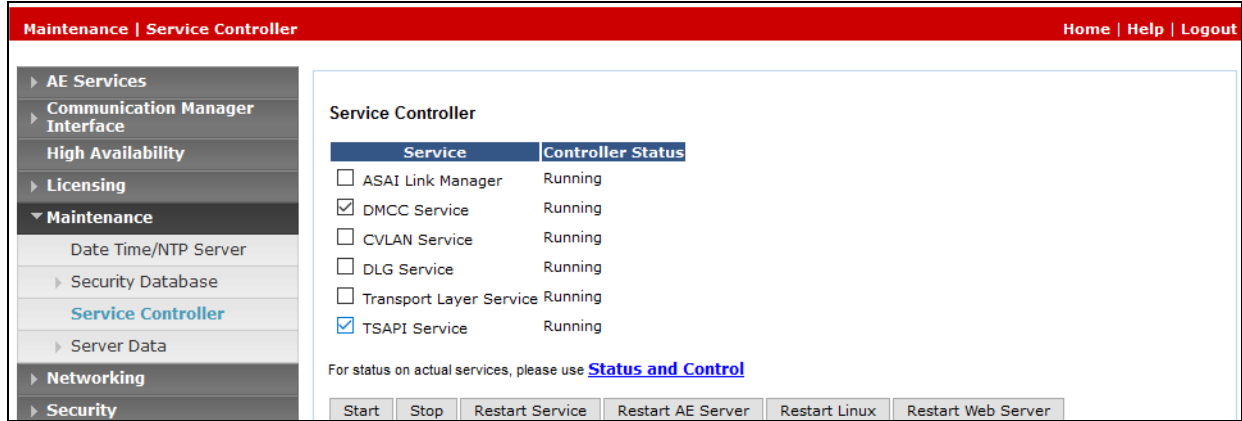
The screenshot displays the Avaya Application Enablement Services Management Console. The top left features the Avaya logo. The top center shows the title "Application Enablement Services Management Console". The top right contains system information: "Welcome: User cust", "Last login: Tue Nov 15 13:56:37 2016 from 135.10.98.75", "Number of prior failed login attempts: 0", "HostName/IP: devvmaes/135.10.97.224", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 7.0.1.0.2.15-0", "Server Date and Time: Tue Nov 15 13:57:21 EST 2016", and "HA Status: Not Configured".

A red navigation bar at the top contains "Security | Security Database | Control" on the left and "Home | Help | Logout" on the right. The left sidebar is a tree view with categories: 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), and Control (selected).

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". Below these is an "Apply Changes" button.

6.6. 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 shows a web interface for the Service Controller. The top navigation bar is red and contains the text "Maintenance | Service Controller" on the left and "Home | Help | Logout" on the right. On the left side, there is a vertical menu with several categories: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance" (expanded), "Date Time/NTP Server", "Security Database", "Service Controller" (highlighted in blue), "Server Data", "Networking", and "Security". The main content area is titled "Service Controller" and contains a table with two columns: "Service" and "Controller Status". The table lists several services, each with a checkbox and a status of "Running". The "DMCC Service" and "TSAPI Service" checkboxes are checked. Below the table, there is a note: "For status on actual services, please use [Status and Control](#)". At the bottom of the main content area, there is a row of buttons: "Start", "Stop", "Restart Service", "Restart AE Server", "Restart Linux", and "Restart Web Server".

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

6.7. Administer Call Recording Solution 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 values in the remaining fields. Click **Apply** at the bottom of the screen. Below is screenshot of user mattersight created during compliance tested.

The screenshot displays the 'User Management | User Admin | List All Users' interface. On the left is a navigation pane with a tree view. The 'User Management' folder is expanded, and 'User Admin' is selected. Under 'User Admin', 'List All Users' is highlighted. The main area on the right is titled 'Edit User' and contains a form with the following fields:

- * User Id: mattersight
- * Common Name: mattersight
- * Surname: mattersight
- User Password: (empty)
- Confirm Password: (empty)
- Admin Note: (empty)
- Avaya Role: None (dropdown)
- Business Category: (empty)
- Car License: (empty)
- CM Home: (empty)
- Css Home: (empty)
- CT User: Yes (dropdown)
- Department Number: (empty)
- Display Name: (empty)
- Employee Number: (empty)
- Preferred Language: English
- Room Number: (empty)
- Telephone Number: (empty)

At the bottom of the form are two buttons: 'Apply Changes' and 'Cancel Changes'.

6.8. Provide Call Recording Solution User unrestricted access

Select **Security** → **Security Database** → **CTI Users** → **List All Users** from the left pane to display the list of CTI users in the right pane (not shown). Under the user list select the user created in the previous step and click on Edit at the bottom of the page. In the User Profile section check the box for the Unrestricted Access.

This will allow the CTI user access to all devices on this AES server.

6.9. Administer Ports

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

In the **DMCC Server Ports** sub-section, select the radio button for **Unencrypted Port** under the **Enabled** column, and make a note of the port value to be used later to configure Call Recording Solution. Retain the default values in the remaining fields. Click **Apply Changes** at the bottom of the screen (not shown below).

High Availability ▶ Licensing ▶ Maintenance ▼ Networking AE Service IP (Local IP) Network Configure Ports TCP/TLS Settings ▶ Security ▶ Status ▶ User Management ▶ Utilities ▶ Help	CVLAN Ports			Enabled Disabled
	Unencrypted TCP Port	9999		<input checked="" type="radio"/> <input type="radio"/>
	Encrypted TCP Port	<input type="text" value="9998"/>		<input checked="" type="radio"/> <input type="radio"/>
	<hr/>			
	DLG Port	TCP Port	5678	
	TSAPI Ports			Enabled Disabled
	TSAPI Service Port	450		<input checked="" type="radio"/> <input type="radio"/>
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	<input type="text" value="1050"/>		
	TCP Port Max	<input type="text" value="1065"/>		
	Encrypted TLINK Ports			
TCP Port Min	<input type="text" value="1066"/>			
TCP Port Max	<input type="text" value="1081"/>			
<hr/>				
DMCC Server Ports			Enabled Disabled	
Unencrypted Port	<input type="text" value="4721"/>		<input checked="" type="radio"/> <input type="radio"/>	
Encrypted Port	<input type="text" value="4722"/>		<input checked="" type="radio"/> <input type="radio"/>	
TR/87 Port	<input type="text" value="4723"/>		<input checked="" type="radio"/> <input type="radio"/>	

7. Configure Mattersight Call Recording Solution

This section provides the procedures for configuring Call Recording Solution. The procedures include the configuration of the WorkerSetting.config file.

The configuration of Call Recording Solution is performed by Mattersight technicians. The procedural steps are presented in these Application Notes are for informational purposes.

7.1. Administer WorkerSettings

In the WorkerSettings file configure the following parameters in order for Mattersight to communicate with Application Enablement Service:

- **CmIpAddress:** Enter IP address of Communication Manager.
- **RtpIpAddress:** Enter IP address of Mattersight server
- **AesIpAddress:** Enter IP address of Application Enablement Service.
- **AesSocketPort:** Enter port in **Section 6.9**
- **DmccUserName:** Enter user name create in **Section 6.7.**
- **DmccPassword:** Enter password created in **Section 6.7.**
- **Codec:** Enter codec used for recording
- **Mode:** Enter the interface mode in this case it is MR.

```
<workerSettings>
<add key="EndpointsToPublishTo" value="tcp://127.0.0.1:56000" />
<add key="EndpointsToSubscribeTo" value="tcp://127.0.0.1:56001" />
<add key="ExtensionsWhitelist" value="" />
<add key="RecordingExtensions" value="56114-56115" />
<add key="CmIpAddress" value="10.10.97.222" />
<add key="StartPort" value="4800" />
<add key="RtpIpAddresses" value="10.10.97.252" />
<add key="AesIpAddress" value="10.10.97.224" />
<add key="AesSocketPort" value="4721" />
<add key="DmccUserName" value="mattersight" />
<add key="DmccPassword" value="mattersight" />
<add key="ProtocolVersion" value="http://www.ecma-international.org/standards/ecma-323/csta/ed3/priv6" />
<add key="RecordOnlyAgentToAgent" value="false" />
<add key="Codec" value="g711U" /><!--g711U, g729, g711A-->
<add key="Mode" value="MR" /><!--MR (multi registration), SSC (single step conf), SO (Service Observe)-->
<add key="StationPassword" value="1234" />
<add key="FAC" value="*43" /><!--feature access code for service observe-->
<add key="ServerPingIntervalInSecs" value="10" />
<add key="ReconnectDelayInMins" value="2" />
</workerSettings>
```

Close the file and save all of the configuration changes.

7.2. Administer Service

In Services window, verify Mattersight Dmcc Avaya Interface is running as shown below (this is performed by the Mattersight team):

Mattersight Dmcc Avaya interface	ChangeMe	Running	Automatic	Local System
Mattersight Predictive Routing Proc...	Mattersight Predictive Rout...	Running	Automatic	Local System
Mattersight Real Time Bus	Mattersight Real Time Bus	Running	Automatic	Local System
Mattersight Route Skill Filter	Mattersight Route Skill Filter	Running	Automatic	Local System
Mattersight Routing Heartbeat	Mattersight Routing Heart...	Running	Automatic	Local System
Mattersight RtpCaptureEngine	Captures RTP and writes it ...		Disabled	Local System
Microsoft iSCSI Initiator Service	Manages Internet SCSI (iSC...		Manual	Local System
Microsoft Software Shadow Copy Pr...	Manages software-based v...		Manual	Local System
Microsoft Storage Spaces SMP	Host service for the Micros...		Manual	Network Service

8. Verification Steps

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

8.1. 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	devaes	established	26	20

Verify the registration status of the phones by using the “list registered-ip-stations” command. Verify that all H323 extensions from **Section 3** are displayed, as shown below.

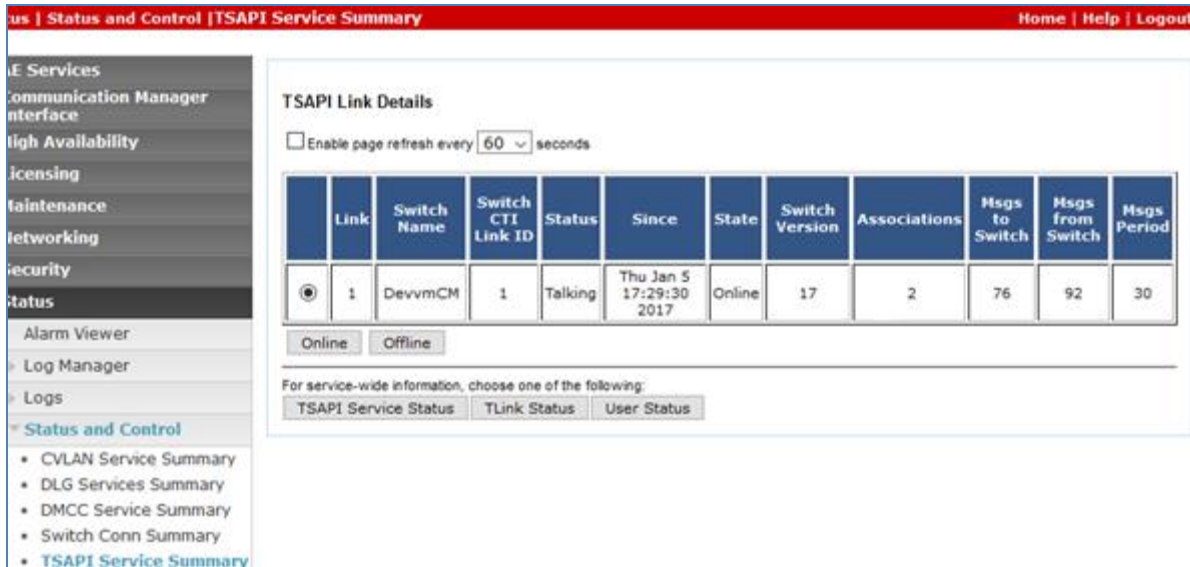
```
list registered-ip-stations
```

REGISTERED IP STATIONS						
Station or Orig	Ext Port	Set Net	Type/ Rgn	Prod ID/ Release	Station Skt	IP Address/ Gatekeeper IP Address
56101		9608	1	IP Phone 6.6229	tcp	10.33.5.29
56106		9608	1	IP Phone 6.6229	tcp	10.33.5.30

8.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the TSAPI link by selecting **Status** → **Status and Control** → **TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify the **Status** is “Talking” for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the number of monitored skill group and agent station extensions from **Section 3**.



The screenshot displays the 'TSAPI Link Details' screen in the Avaya Aura® Application Enablement Services (AES) interface. The page title is 'us | Status and Control | TSAPI Service Summary' and it includes navigation links for 'Home | Help | Logout'.

The left navigation pane shows the following menu items:

- 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

The main content area displays the 'TSAPI Link Details' for a single link. It includes a checkbox for 'Enable page refresh every 60 seconds' and a table with the following data:

	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	DevvmCM	1	Talking	Thu Jan 5 17:29:30 2017	Online	17	2	76	92	30

Below the table, there are buttons for 'Online' and 'Offline'. At the bottom, there is a section for 'For service-wide information, choose one of the following:' with buttons for 'TSAPI Service Status', 'TLink Status', and 'User Status'.

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

Verify the **User** column shows an active session with the Call Recording Solution user name from **Section 6.7**, and that the **# of Associated Devices** column reflects the number of monitored skill group, agent station extensions, and virtual IP softphone extensions.

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 seconds

Session Summary [Device Summary](#)
Generated on Fri Mar 24 19:27:17 EDT 2017

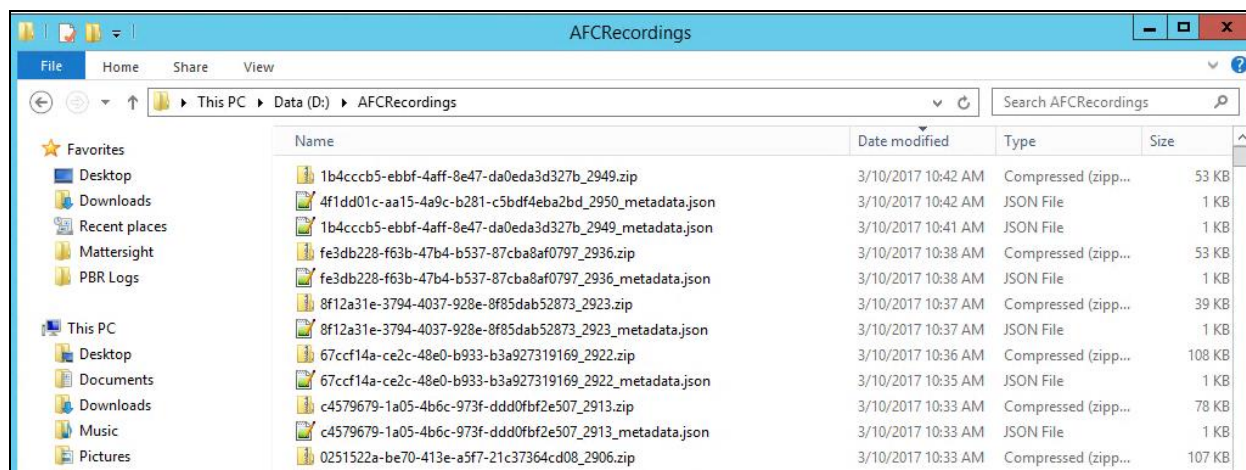
Service Uptime: 16 days, 7 hours 43 minutes
 Number of Active Sessions: 3
 Number of Sessions Created Since Service Boot: 40
 Number of Existing Devices: 16
 Number of Devices Created Since Service Boot: 197

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	9F3A17A0C790AED36 1EF24E5B89B2471-1	mattersight	Avaya Dmcc Interface	10.10.97.252	XML Unencrypted	7

Item 1-3 of 3

8.3. Verify Mattersight Call Recording Solution

In the AFCRecordings folder, select the entry and verify that the call recording can be played back and play the correct media.



9. Conclusion

These Application Notes describe the configuration steps required for Mattersight Call Recording Solution 4.0 to successfully interoperate with Avaya Aura® Communication Manager 7.0.2 using Avaya Aura® Application Enablement Services 7.0.1 SP3. All feature and serviceability test cases were completed successfully with observations noted in **Section 2.2**.

10. Additional References

This section references the product documentation relevant to these Application Notes can be found on support.avaya.com:

1. *Administering Avaya Aura® Communication Manager*, Release 7.0.1 555-245-205 Issue 3 October 2016.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 7.0.1 Issue 2 August 2016.

Mattersight document is available upon request.

©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.