



Application Notes for Maximizer CRM 2015 R2 with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services R7.0 using Telephony Web Service – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Maximizer CRM 2015 R2 to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services R7.0 using Telephony Web Service. Maximizer CRM 2015 R2 is a CRM software application.

In the compliance testing, Maximizer CRM 2015 R2 used the Telephony Web Services from Avaya Aura® Application Enablement Services to access to a subset of the third-party call control capabilities provided by Avaya Aura® Communication Manager. The Telephony Web Service supports many requests however only Make Call and Disconnect Active Call were relevant for this testing.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the 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 Maximizer CRM 2015 R2 to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services R7.0 using Telephony Web Service. Maximizer CRM 2015 R2 is CRM software and the click to call feature of this software was tested.

In the compliance testing, Maximizer CRM 2015 R2 used the Telephony Web Service from Avaya Aura® Application Enablement Services (hereafter referred as Application Enablement Services) to make a call from stations on Avaya Aura® Communication Manager (hereafter referred as Communication Manager) to a client phone number configured in their application's address book.

The Telephony Web Service provides high level call control functionality over standard web service interfaces (SOAP/XML). All operations are treated as being independent, and the only parameters required are extension and telephone numbers.

The Telephony Web Service is resident on the Avaya Aura® Application Enablement Services server and enables access to a subset of the third-party call control capabilities provided by Avaya Aura® Communication Manager. The web service allows client applications to control a device's participation in calls on a switch.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of Maximum CRM 2015 R2 (hereafter referred to as Maximizer CRM), the application automatically connects to Application Enablement Services and using the Telephony Web Service can make a call or disconnect an active call.

For the manual part of the testing, a call was initiated by opening the web based client of Maximizer CRM and clicking on a client number from the address book. Also using the same click to call feature, an active call was disconnected too.

The serviceability test cases were performed manually by restarting the server hosting the Maximizer CRM or the client PC that is running the web based client of Maximizer CRM.

The verification of tests included answering the call made and ensure there was proper speech path and also if the call was disconnected correctly. Also the notes section of Maximizer CRM was verified for consistency.

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:

- Making a call using the click to call feature.
- Disconnecting a call using the click to call feature.
- Ensuring that clear speech path is established for an active call.
- Ensure Maximizer CRM can disconnect the call correctly when called number is busy or invalid.
- Ensure that the information in the notes section of Maximizer CRM is correct and valid.

The serviceability testing focused on verifying the ability of Maximizer CRM to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to its server or to a client PC.

2.2. Test Results

All test cases were executed. The following were the observations on Maximizer CRM from the compliance testing.

- The click to call feature can only make active calls or disconnect an active call. Any other features like Transfer, Conference, Hold etc., are not supported.
- The dial plan in Maximizer CRM is hard coded to dial only telephone numbers that are 10 digits or higher.
- Avaya Deskphones of 96x1 types (for example 9641) with SIP firmware are unable to make the call using the Telephony Web Services via Application Enablement Services. Avaya is aware of the issue (JIRA PHONEX6-1448).

2.3. Support

Technical support on Maximizer CRM can be obtained through the following:

- **Phone:** 1-866-275-1254
- **Email:** support@maximizercrmlive.com

3. Reference Configuration

The detailed administration of the basic connectivity between Communication Manager and Application Enablement Services and of the Maximizer CRM are not the focus of these Application Notes and will not be described.

In the compliance testing, both H323 and SIP desk phones were used and therefore Avaya Aura® Session Manager (Session Manager) is shown in the figure below since the SIP desk phones were registered to the Session Manager

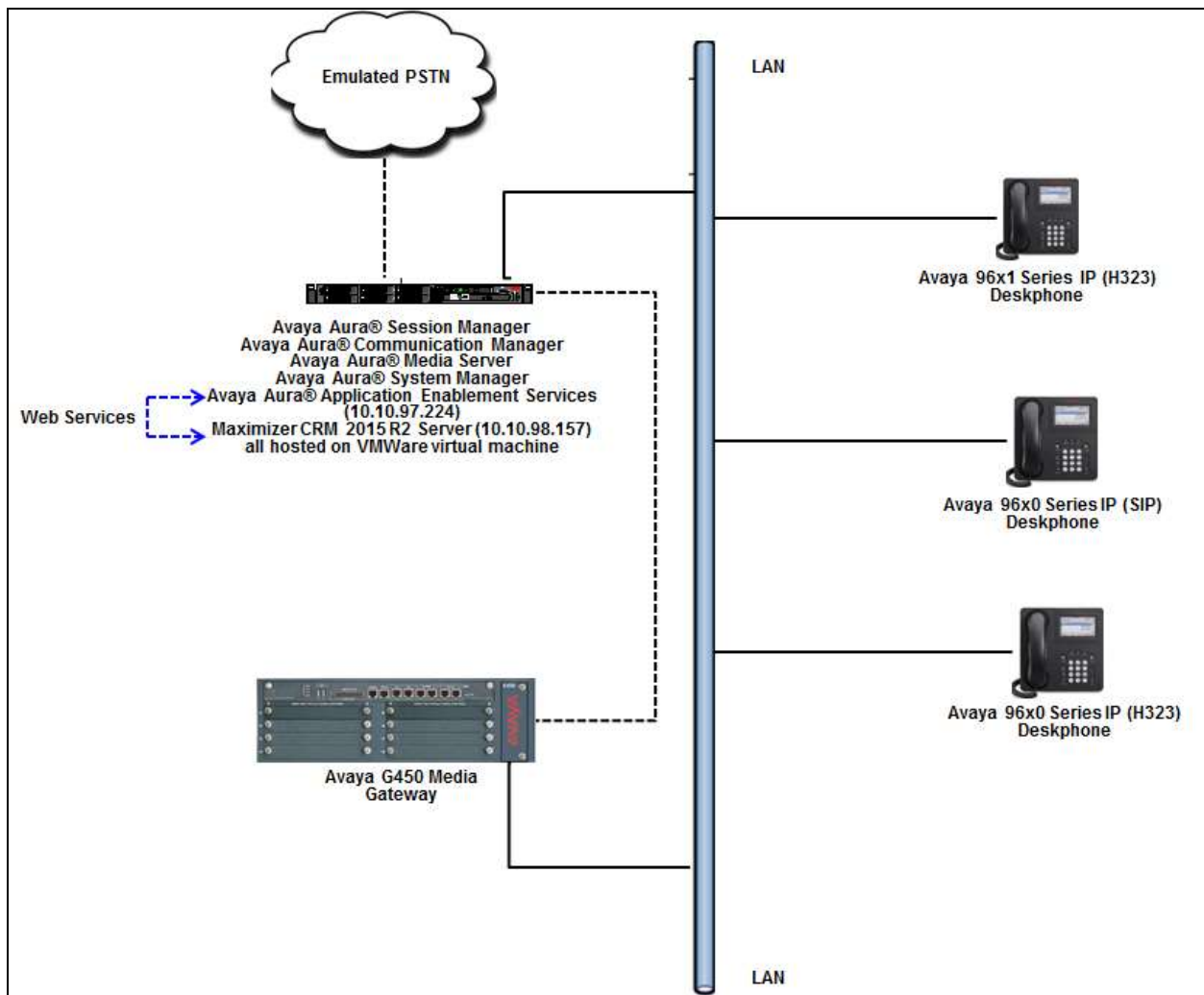


Figure 1: Compliance Testing Configuration

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	7.0.0.1.0-SP1 (R017x.00.0.441.0)
Avaya Aura® Application Enablement Services	7.0.0.0.1.13
Avaya Aura® Session Manager	7.0.0.0.700007
Avaya Aura® System Manager	7.0.0.0
Avaya Aura® Media Server	7.7.0.226
Avaya G450 Media Gateway	37 .19 .0 /1
Avaya IP Deskphones: 9608 (H323) 9641 (H323) 9650 (SIP) 9650 (H323)	6.6115 6.6115 2.6.15 3.250A
Maximizer Server running on VM Ware with Windows Server Standard without Hyper-V SP2 32-bit	Maximizer CRM 2015 R2 Package 13.1

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 a User's Station

5.1. Verify License

Log in to 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 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)?	y	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			

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: 56000
Type: ADJ-IP
Name: DevvmAES                                     COR: 1
```

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 Maximizer CRM.

```
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

      Zip Tone Burst for Callmaster Endpoints: double

ASAI
      Copy ASAI UII 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
      Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```


5.4. Administer a User's Station

Add a desk phone that will be assigned to a user on Maximizer CRM 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.
- **Type:** Any IP telephone type, such as “9608”.
- **Name:** A descriptive name.
- **Security Code:** A desired code.
- **COR:** The COR number.

add station 56101		Page 1 of 5
STATION		
Extension: 56101	Lock Messages? n	BCC: M
Type: 9608	Security Code: *	TN: 1
Port: S00000	Coverage Path 1:	COR: 1
Name: OneOne	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: 56101	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 0	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? y	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? y	

6. Configure Avaya Aura® Application Enablement Services

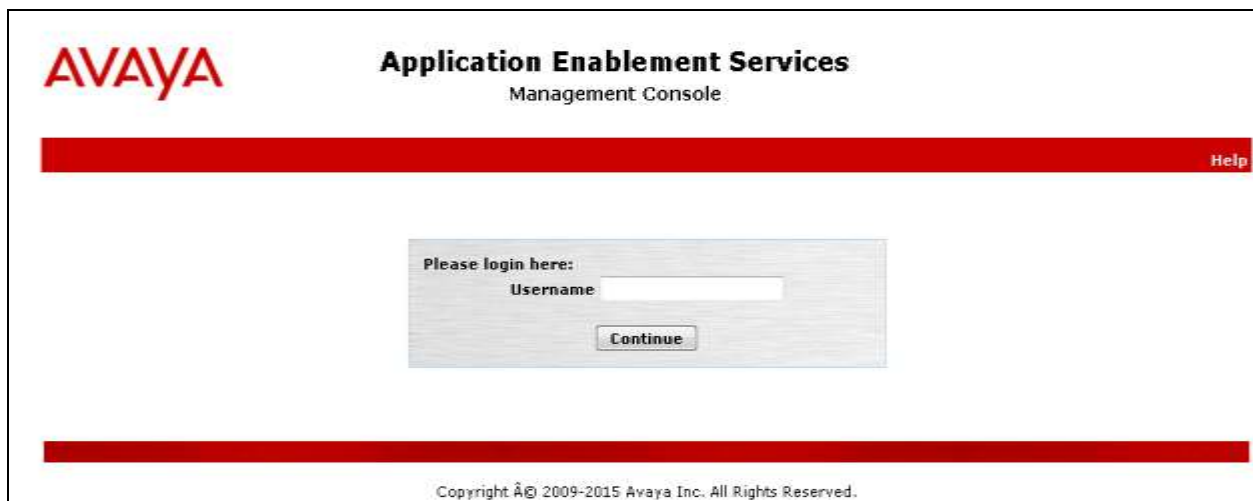
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify License
- Administer TSAPI link
- Administer H.323 gatekeeper
- Disable Security Database
- Restart Services
- Administer Maximizer CRM user
- Enable Call and Device Control for CTI user
- Enable 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 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, with a "Help" link in the top right corner. In the center of the page is a light gray rectangular box containing the text "Please login here:" followed by a "Username" label and a text input field. Below the input field is a "Continue" button. Another thick red horizontal bar is located at the bottom of the page, above the copyright notice: "Copyright © 2009-2015 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, the title "Application Enablement Services Management Console", and a user status bar on the right. The user status bar displays: "Welcome: User admin", "Last login: Thu Jan 7 06:04:12 2016 from 10.10.98.71", "Number of prior failed login attempts: 0", "HostName/IP: DevvmAES/10.10.97.234", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 7.0.0.0.1.13", "Server Date and Time: Fri Jan 08 06:28:47 EST 2016", and "HA Status: Not Configured". Below the header is a red navigation bar with "Home" on the left and "Home | Help | Logout" on the right. The main content area is divided into a left sidebar and a main panel. The sidebar contains a list of menu items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security", "Status", "Utilities", and "Help". The main panel displays the "Welcome to OAM" screen. It includes a red warning message: "This AE Services server is using a default installed server certificate. Default installed certificates should not be used in a production environment. It is highly recommended to replace all default installed certificates." Below this, it states: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:". A bulleted list follows: "• 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.", "• Utilities - Use Utilities to carry out basic connectivity tests.", "• Help - Use Help to obtain a few tips for using the OAM Help system". At the bottom, it notes: "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 **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" menu item selected in the left sidebar. The top header is the same as the previous screenshot. The user status bar now displays: "Welcome: User", "Last login: Tue Dec 17 07:54:36 2013 from 10.32.39.20", "Number of prior failed login attempts: 0", "HostName/IP: aes_125_72/10.64.125.72", "Server Offer Type: VIRTUAL_APPLIANCE_ON_SP", "SW Version: 6.3.1.0.19-0", "Server Date and Time: Tue Dec 17 07:54:58 MST 2013", and "HA Status: Not Configured". The red navigation bar now shows "Licensing" on the left and "Home | Help | Logout" on the right. The main panel displays the "Licensing" screen. It includes the following text: "If you are setting up and maintaining the WebLM, you need to use the following:", a bulleted list with "• WebLM Server Address", "If you are importing, setting up and maintaining the license, you need to use the following:", a bulleted list with "• WebLM Server Access", "If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:", and a bulleted list with "• Reserved Licenses". The left sidebar now shows "AE Services", "Communication Manager Interface", "High Availability", "Licensing" (selected), "WebLM Server Address", "WebLM Server Access", "Reserved Licenses", "Maintenance", and "Networking".

The **Web License Manager** 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** as shown below. Note that the TSAPI license is required for Telephony Web Service.

Application Enablement (CTI) - Release: 7 - SID: 10500000 Standard License File

Has any item: Unlicensed Products + Application_Enablement + View License Capacity

Licenses Installed on: October 13, 2015 5:25:48 AM -05:00

License File Host ID: 13-04-05-02-75-7F

Licensed Features

Item	Feature (License Keyword)	Expirations Date	Licensed capacity	Currently U
	CULAN AS41 VALUE_AES_CULAN_AS41	permanent	16	0
	Unified CC API Desktop Edition VALUE_AES_APC_UNIFIED_CC_DESKTOP	permanent	1000	0
	AES ADVANCED SMALL SWITCH VALUE_AES_APC_SMALL_ADVANCED	permanent	3	0
	CULAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16	0
	Product Notes VALUE_NOTES	permanent		Not count
	AES ADVANCED LARGE SWITCH VALUE_AES_APC_LARGE_ADVANCED	permanent	3	0
	TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000	0

6.3. Administer TSAPI Link

To administer a TSAPI link, select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console**. 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 system information: Welcome: User admin, Last login: Thu Jan 7 06:04:12 2016 from 10.10.98.71, Number of prior failed login attempts: 0, HostName/IP: DevvmAES/10.10.97.224, Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE, SW Version: 7.0.0.0.1.13, Server Date and Time: Fri Jan 08 06:39:08 EST 2016, 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 the following data:

Link	Switch Connection	Switch CTI Link #	ASA Link Version	Security
1	procr	1	5	Both

Below the table are buttons for 'Add Link', 'Edit Link', and 'Delete Link'.

The **Add TSAPI Links** screen is seen next however the screen below shows the screen after the Link has been added.

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 “procr” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.

The screenshot shows the Avaya Application Enablement Services Management Console with the 'Edit TSAPI Links' screen. The left navigation pane is the same as the previous screenshot. The main content area is titled 'Edit TSAPI Links' and contains the following fields:

- Link: 1
- Switch Connection: procr (dropdown)
- Switch CTI Link Number: 1 (dropdown)
- ASA Link Version: 5 (dropdown)
- Security: Both (dropdown)

At the bottom are buttons for 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'.

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 “procr”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Communication Manager Interface' selected, with 'Switch Connections' highlighted. The main area displays a table of switch connections. The table has columns: Connection Name, Processor Ethernet, Msg Period, and Number of Active Connections. One connection named 'procr' is listed with 'Yes' for Processor Ethernet, '30' for Msg Period, and '1' for Number of Active Connections. Below the table are buttons: Edit Connection, Edit PE/CLAN IPs, Edit H.323 Gatekeeper, Delete Connection, and Survivability Hierarchy. The top right shows system information: Welcome! User admin, Last login: Thu Jan 7 06:04:12 2016 from 10.10.98.71, Number of prior failed login attempts: 0, HostName/IP: DevvmAES/10.10.97.224, Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE, SW Version: 7.0.0.0.1.13, Server Date and Time: Fri Jan 08 06:48:29 EST 2016, HA Status: Not Configured.

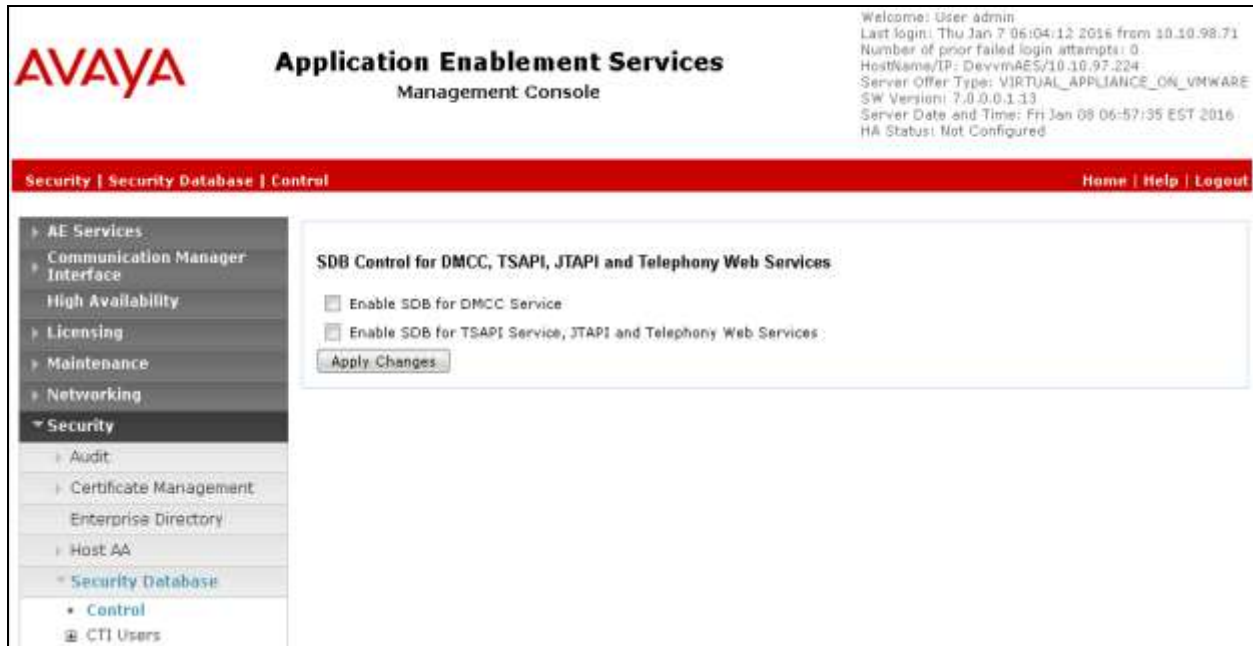
Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> procr	Yes	30	1

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 the H.323 gatekeeper, in this case “10.10.97.222” as shown below, which is the Processor C-LAN on Communication Manager. Click **Add Name or IP**. Screen below shows the already added IP.

The screenshot shows the 'Edit H.323 Gatekeeper - procr' screen. The left navigation pane is the same as the previous screenshot. The main area has a text input field with '10.10.97.222' entered, and buttons for 'Add Name or IP', 'Delete IP', and 'Back'. The top right shows the same system information as the previous screenshot.

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.



6.6. Restart Services

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

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 user 'admin' with login details. A red navigation bar contains "Maintenance | Service Controller" and links for "Home | Help | Logout".

On the left, a sidebar menu lists various sections: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance (selected), Security Database, Service Controller (highlighted), Server Data, Networking, and Security.

The main content area, titled "Service Controller", contains a table with two columns: "Service" and "Controller Status".

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input 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

Below the table, a note states: "For status on actual services, please use [Status and Control](#)". At the bottom, there are several action buttons: Start, Stop, Restart Service, Restart AE Server, Restart Linux, and Restart Web Server.

6.7. Administer Maximizer CRM 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 **Avaya Role**, select “userservice.useradmin” from the drop-down list. For **CT User**, select “Yes” from the drop-down list. Retain the default value in the remaining fields.

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 'User cust' with system details. A red navigation bar contains links for 'User Management', 'User Admin', 'Add User', 'Home', 'Help', and 'Logout'. The left sidebar shows a tree view with 'Status', 'User Management', 'Service Admin', 'User Admin', and 'Help'. Under 'User Admin', 'Add User' is selected. The main content area is titled 'Add User' and contains a form with the following fields: 'User Id' (Test), 'Common Name' (Test), 'Surname' (Test), 'User Password' (masked with asterisks), 'Confirm Password' (empty), 'Admin Note' (empty), 'Avaya Role' (userservice.useradmin), 'Business Category' (empty), 'Car License' (empty), 'CM Home' (empty), 'Css Home' (empty), 'CT User' (Yes), and 'Department Number' (empty). A note indicates that fields marked with an asterisk are required.

6.8. Enable Call and Device Control for CTI User

Select **Security** → **Security Database** → **CTI Users** → **List All Users** from the left pane, to display the **CTI Users** screen in the right pane as shown below. Select the User ID created in **Section 6.7** and click on the **Edit** button.

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 user "admin" with system details. A red navigation bar contains the breadcrumb "Security | Security Database | CTI Users | List All Users" and links for "Home | Help | Logout".

On the left, a sidebar menu lists various services, with "Security" expanded to show "Security Database" and "CTI Users". Under "CTI Users", the options "List All Users" and "Search Users" are visible.

The main content area, titled "CTI Users", features a table with the following data:

User ID	Common Name	Worktop Name	Device ID
Test	Test	NONE	NONE

Below the table are "Edit" and "List All" buttons.

The **Edit CTI User** screen is seen as shown below. Under **Call and Device Control**, select the “Any” option from the drop down for the **Call Origination/Termination and Device Status** field. Under **User Profile**, check the box for the **Unrestricted Access** field. Retain default values for all other field and click on the **Apply Changes** button.

AVAYA Application Enablement Services Management Console

Welcome: User admin
 Last login: Fri Jan 8 06:28:22 2016 from 10.10.98.71
 Number of prior failed login attempts: 0
 HostName/IP: DevvmAES/10.10.97.224
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 7.0.0.1.13
 Server Date and Time: Fri Jan 08 07:50:48 EST 2016
 HA Status: Not Configured

Security | Security Database | CTI Users | List All Users Home | Help | Logout

Edit CTI User

User Profile: User ID: Common Name: Worktop Name: Test: Test: NONE

☒ Unrestricted Access

Call and Device Control: Call Origination/Termination and Device Status: Any

Call and Device Monitoring: Device Monitoring: None
 Calls On A Device Monitoring: None
 Call Monitoring: ☐

Routing Control: Allow Routing on Listed Devices: None

Apply Changes Cancel Changes

6.9. Enable Ports

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

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

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with the following items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking (selected), AE Service IP (Local IP), Network Configure, Ports (highlighted), TCP Settings, and Security. The main content area is titled 'Ports' and displays configuration for CVLAN Ports, DLG Port, and TSAPI Ports. The TSAPI Ports section includes a table with columns for the port name, port number, and a status column with 'Enabled' and 'Disabled' radio buttons. The 'TSAPI Service Port' is set to 450 and is currently enabled, indicated by a red box around the 'Enabled' radio button. Other ports shown include Unencrypted TCP Port (9999), Encrypted TCP Port (9998), and Local TLINK Ports (1024-1039).

Ports		
CVLAN Ports		
Unencrypted TCP Port	9999	Enabled Disabled
Encrypted TCP Port	9998	Enabled Disabled
DLG Port		
TCP Port	5678	
TSAPI Ports		
TSAPI Service Port	450	Enabled Disabled
Local TLINK Ports		
TCP Port Min	1024	
TCP Port Max	1039	

7. Configure Maximizer CRM 2015 R2

This section provides the procedures for configuring Maximizer CRM. The procedure includes the configuration of the “web.config” file in the Maximizer CRM server. It is also assumed that the station configured in **Section 5.4** is assigned to a user on the Maximizer CRM.

The configuration of Maximizer is performed by their installers and dealers. The procedural steps are presented in these Application Notes for informational purposes.

7.1. Administer the Web.Config File

Login to the Maximizer CRM server; navigate to the **C:\Program Files\Maximizer\Portals\Employee\Dialogs\CustomDialogs** directory to edit the **web.config** file as shown below.

Replace the text in yellow with the appropriate values.

Setting	Description
MakeCallDialog_AvayaAESWS_TelephonyServiceService	The URL to the Application Enablement Services web service to be used with the Make Call Dialog
AESCredentialLogin	The login name for the Application Enablement Services web service UserID created in Section 6.7 .
AESCredentialPwd	The password for the Application Enablement Services web service UserID created in Section 6.7 .

```
<applicationSettings>
  <MakeCallDialog.Properties.Settings>
    <setting name="MakeCallDialog_AvayaAESWS_TelephonyServiceService"
      serializeAs="String">
      <value>https://10.10.97.224/axis/services/TelephonyService</value>
    </setting>
    <setting name="AESCredentialLogin" serializeAs="String">
      <value>Test</value>
    </setting>
    <setting name="AESCredentialPwd" serializeAs="String">
      <value>Password</value>
    </setting>
  </MakeCallDialog.Properties.Settings>
</applicationSettings>
```

8. Verification Steps

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

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	5	no	DevvmAES	established	14	14

Verify the registration status of the IP desk phones by using the “list registered-ip-stations” command. Verify that the IP desk phone extension from **Section Error! Reference source not found.4** are displayed along with the IP address of the Communication Manager, as shown below.

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

REGISTERED IP STATIONS						
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	TCP Skt	Station IP Address/ Gatekeeper IP Address		
56101	9608	IP_Phone	y	10.10.5.14		
	1	6.6115		10.10.97.222		
56102	9641	IP_Phone	y	10.10.5.16		
	1	6.6115		10.10.97.222		
56103	9650	IP_Phone	y	10.10.5.12		
	1	3.250A		10.10.97.222		

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**.

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 user "admin" with login details. A red navigation bar contains "Status | Status and Control | TSAPI Service Summary" and links for "Home | Help | Logout".

The left sidebar shows a tree view with categories like "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security", and "Status". Under "Status", the "Status and Control" section is expanded, showing sub-items: "CVLAN Service Summary", "DLG Services Summary", "DMCC Service Summary", "Switch Conn Summary", and "TSAPI Service Summary".

The main content area is titled "TSAPI Link Details". It includes a checkbox for "Enable page refresh every 60 seconds". Below this is a table with the following data:

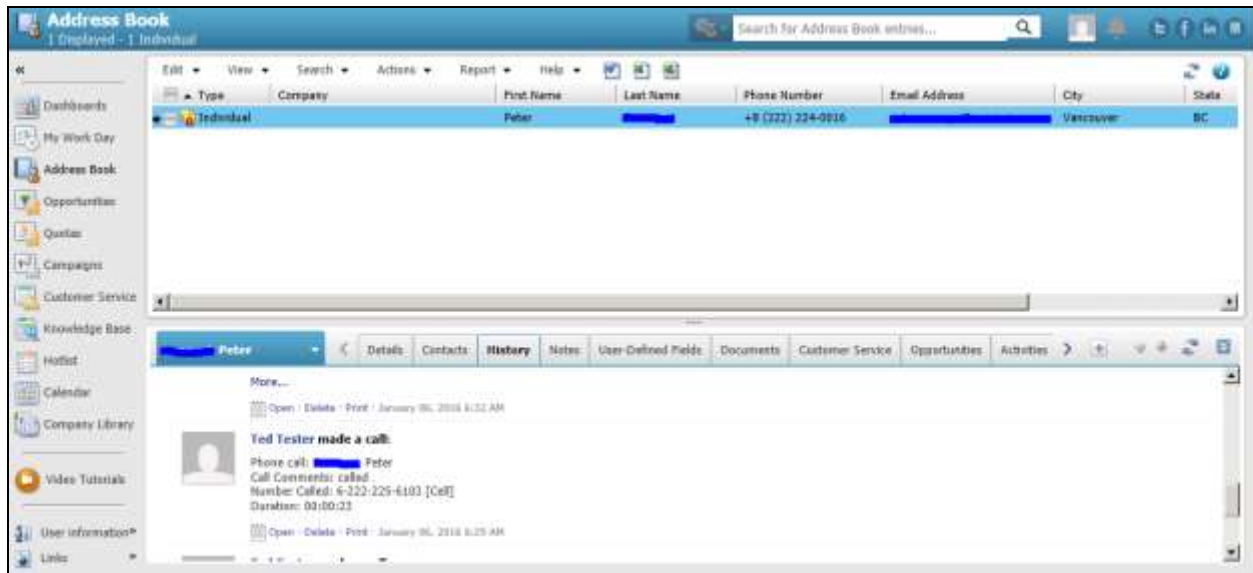
	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
	1	procr	1	Talking	Thu Oct 15 09:14:53 2015	Online	17	0	15	15	30

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

8.3. Verify Maximizer CRM 2015 R2

Log into Maximizer CRM Web Access using one of the supported browsers. Follow the steps to make a call from user's address book to a valid telephone number by clicking the "Make Call" button. The far end telephone rings and answers the call, ensure clear speech path is established and the user is able to add notes in the call comments box and hang up the call by clicking the "Hang Up" button.

Screen below shows the details of the call made after it is completed.



9. Conclusion

These Application Notes describe the configuration steps required for Maximizer CRM 2015 R2 to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services R7.0 using Telephony Web Service. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

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

Avaya

1. *Implementing Avaya Aura® Session Manager* Document ID 03-603473.
2. *Administering Avaya Aura® Session Manager*, Doc ID 03-603324.
3. *Deploying Avaya Aura® System Manager*, Release 7.0.
4. *Administering Avaya Aura® System Manager for Release 7.0*, Release 7.0.
5. *Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager*.
6. *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 7.7.
7. *Administering Avaya Aura® Communication Manager*, Release 7.0, 03-300509.
8. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.0, 555-245-205.
9. *Deploying Avaya Aura® Application Enablement Services in Virtualized Environment*, Release 7.0
10. *Administering and Maintaining Avaya Aura® Application Enablement Services*, Release 7.0

Maximizer CRM

Product information for Maximizer CRM products can be found at <http://www.maximizer.com/>.

Deployment instructions for the Avaya Make Call Dialog can be obtained from Maximizer upon request.

©2016 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.