



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for HigherGround Capture911 with Avaya Aura® Communication Manager Using Avaya Aura® Application Enablement Services – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for HigherGround Capture911 to interoperate with Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services.

HigherGround Capture911 is a call recording solution. In the compliance testing, HigherGround Capture911 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.

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 HigherGround Capture911 to interoperate with Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services.

HigherGround Capture911 is a call recording solution. In the compliance testing, HigherGround Capture911 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, HigherGround Capture911 is informed of the call via event reports from the DMCC interface. HigherGround Capture911 starts the call recording by using the Single Step Conference feature from the DMCC interface to add a 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.

## 2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Capture911 application, the application automatically uses DMCC to register the virtual IP softphones to Communication Manager, and to request monitoring on the 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 Capture911.

The verification of tests included using the Capture911 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 Capture911:

- Use of DMCC registration services to register and un-register the virtual IP softphones.
- Use of DMCC monitoring services to monitor skill group, agent stations, and virtual IP softphones.
- Use of DMCC call control services to activate Single Step Conference for the virtual IP softphones and to obtain the media for call recording.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, reconnect, simultaneous calls, simultaneous agents, conference, and transfer.

The serviceability testing focused on verifying the ability of Capture911 to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to the Capture911 server.

## 2.2. Test Results

All test cases were executed, and the following were observations on Capture911 from the compliance testing:

- Agents are required to log in after Capture911 starts.
- Only one skill group can be monitored by Capture911. Agents that do not belong to the monitored skill group can still be monitored with ACD calls recorded, and the recording entries for those calls will be associated with the agent station instead of agent ID extension.
- Non-ACD calls to the agents are recorded and reported using the agent ID extension. The called parameter from those recording entries can be used to identify the non-ACD calls.
- The hold and reconnect scenario with held period under the system MaxRecordSilence interval produced one recording entry, and the same scenario with held period over the MaxRecordSilence interval produced two recording entries with blank call type, calling, called, and answer values in the second recording entry. This is by design, and the MaxRecordSilence parameter is configurable with a default of 15 seconds.
- Two back-to-back calls with inter-call interval below the MaxRecordSilence interval are lumped into one recording entry, with information from the second call used for calling, called, and answer.
- For the blind transfer scenario, the recording entry associated with the transfer-from agent can have a call type of OUT or IN, depending on whether the transfer-to destination is a monitored agent or a non-monitored supervisor respectively.
- For the attended transfer scenario, the recording entry associated with the transfer-from agent can have a call type of INTERN or OUT, depending on whether the transfer-to destination is a monitored agent or a non-monitored supervisor respectively. In addition, the recording entry for the transfer-to agent contained blank values for calling, called, and answer.
- For the conference scenarios, the recording entry for the conference-from agent showed call information from the call with the conference-to destination. In addition, the recording entry for the conference-to agent contained blank values for calling, called, and answer.

## 2.3. Support

Technical support on Capture911 can be obtained through the following:

- **Phone:** (818) 456-1600
- **Email:** [support@highergroundinc.com](mailto:support@highergroundinc.com)

### 3. Reference Configuration

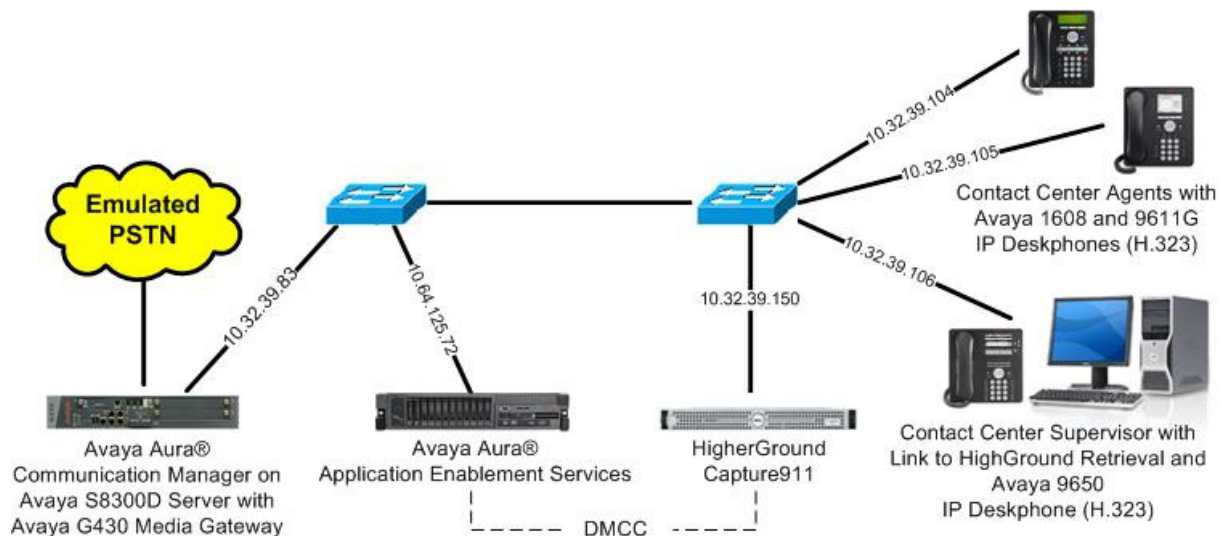
Capture911 can be configured on a single server or with components distributed across multiple servers. The compliance test used a single server configuration shown in **Figure 1**.

Capture911 has a Retrieval application that can be used to review and playback the call recordings. In the compliance testing, the supervisor has a shortcut to the Retrieval application that physically resides on the Capture911 server.

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

In the compliance testing, the contact center devices consisted of two VDNs, two skill groups, one supervisor, and two agents shown in the table below. Capture911 requested monitoring on the first skill group and on both agent station extensions.

Device Type	Extension
VDN	48001, 48002
Skill Group	48101, 48102
Supervisor	45000
Agent ID	45881, 45882
Agent Station	45001, 45002



**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 on Avaya S8300D Server with Avaya G430 Media Gateway	6.3 SP1 (R016x.03.0.124.0-20850)
Avaya Aura® Application Enablement Services	6.3 (6.3.0.0.212-0)
Avaya 1608 IP Deskphone (H.323)	1.330D
Avaya 9611G IP Deskphone (H.323)	6.2209
Avaya 9650 IP Deskphone (H.323)	3.105S
HigherGround Capture911 on Windows 2008 Server <ul style="list-style-type: none"><li>DMCC Integrator Service</li><li>Avaya DMCC .NET (ServiceProvider.dll)</li></ul>	2.1 SP 2 2.1.0.1 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 virtual IP softphones

### 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 3**. 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	3 of	11
OPTIONAL FEATURES				
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y	
Access Security Gateway (ASG)?	n	Authorization Codes?	y	
Analog Trunk Incoming Call ID?	y	CAS Branch?	n	
A/D Grp/Sys List Dialing Start at 01?	y	CAS Main?	n	
Answer Supervision by Call Classifier?	y	Change COR by FAC?	n	
ARS?	y	<b>Computer Telephony Adjunct Links?</b>	<b>y</b>	
ARS/AAR Partitioning?	y	Cvg Of Calls Redirected Off-net?	y	
ARS/AAR Dialing without FAC?	y	DCS (Basic)?	y	
ASAI Link Core Capabilities?	n	DCS Call Coverage?	y	
ASAI Link Plus Capabilities?	n	DCS with Rerouting?	y	
Async. Transfer Mode (ATM) PNC?	n			

### 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			
<b>Extension:</b>	40001			
<b>Type:</b>	ADJ-IP			
<b>Name:</b>	CTI Link			
		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 Capture911.

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

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

  Reporting for PC Non-Predictive Calls? n

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

ASAI
  Copy ASAI UII During Conference/Transfer? n
  Call Classification After Answer Supervision? 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 Virtual IP Softphones

Add a virtual softphone 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 “4620”.
- **Name:** A descriptive name.
- **Security Code:** A desired code.
- **IP SoftPhone:** “y”

add station 45991		Page 1 of 5
STATION		
<b>Extension: 45991</b>	Lock Messages? n	BCC: 0
<b>Type: 4620</b>	<b>Security Code: 45991</b>	TN: 1
Port: IP	Coverage Path 1:	COR: 1
<b>Name: Capture911 Virtual #1</b>	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests: y
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
Speakerphone: 2-way	Message Lamp Ext: 45991	
Display Language: english	Mute Button Enabled? y	
Survivable GK Node Name:	Expansion Module? n	
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	<b>IP SoftPhone? y</b>	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? Y	

Repeat this section to administer the desired number of virtual IP softphones, using sequential extension numbers. In the compliance testing, two virtual IP softphones were administered as shown below, to allow for simultaneous recording of two monitored agents in **Section 3**.

list station 45991 count 2									
STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ TN	Jack	
<b>45991</b>	<b>S00036</b>	<b>Capture911 Virtual #1</b>				<b>1</b>			
	<b>4620</b>		<b>no</b>			<b>1</b>	<b>1</b>		
<b>45992</b>	<b>S00039</b>	<b>Capture911 Virtual #2</b>				<b>1</b>			
	<b>4620</b>		<b>no</b>			<b>1</b>	<b>1</b>		

## 6. Configure Avaya Aura® Application Enablement Services

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

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- Disable security database
- Restart services
- Administer Capture911 user
- 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 Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. A thick red horizontal bar separates the header from the main content area. In the center of the page is a login box with a light gray background. Inside this box, the text "Please login here:" is followed by two input fields: "Username" and "Password". Below these fields is a blue "Login" button. Another thick red horizontal bar is located below the login box. At the bottom of the page, centered, is the copyright notice: "© Copyright © 2009-2012 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 welcome message for the user. The left sidebar contains a menu with options: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area displays the "Welcome to OAM" screen, which explains the purpose of the OAM web interface and lists the administrative domains it manages: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. It also mentions that these domains can be managed by a single administrator or separate administrators.

Welcome: User  
Last login: Tue Sep 3 10:41:39 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: 6.3.0.0.212-0  
Server Date and Time: Tue Sep 3 10:48:28 MDT 2013

Home | Help | Logout

Home

AE Services  
Communication Manager Interface  
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.
- 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.
- Help - Use Help to obtain a few tips for using the OAM Help system

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" section selected in the left sidebar. The main content area displays the "Licensing" screen, which provides instructions on how to set up and maintain the WebLM, import licenses, and administer reserved licenses. It lists the following steps: WebLM Server Address, WebLM Server Access, and Reserved Licenses.

Welcome: User  
Last login: Tue Sep 3 10:41:39 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: 6.3.0.0.212-0  
Server Date and Time: Tue Sep 3 10:49:22 MDT 2013

Home | Help | Logout

Licensing

AE Services  
Communication Manager Interface  
Licensing  
Maintenance  
Networking  
Security

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

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** 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.


Web License Manager (WebLM v6.3)
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

WebLM Home  
Install license  
Licensed products  
APPL\_ENAB  
▼ Application\_Enablement  
View license capacity  
View peak usage  
Uninstall license  
Server properties  
Manage users  
Shortcuts  
Help for Installed Product

Application Enablement (CTI) - Release: 6 - SID: 10503000 (Standard License file)

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

License installed on: May 11, 2012 7:07:47 PM -04:00

License File Host IDs: 00-16-3E-48-ED-82

Licensed Features

Feature (Keyword)	Expiration date	Licensed	Acquired
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	16	0
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	10000	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	16	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	16	0
Product Notes (VALUE_NOTES)	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AEC_UNIFIED_CC_DESKTOP,; CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents;	Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	16	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	10000	0
DLG (VALUE_AES_DLG)	permanent	16	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	10000	0
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	permanent	16	0

### 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**.

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 welcome message for the user. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area displays the "TSAPI Links" table with one link listed. Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	S8800	2	4	Both

Buttons: Add Link, Edit Link, Delete Link

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

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection "S8300D" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields, and click **Apply Changes**.

The screenshot shows the "Add TSAPI Links" screen in the Avaya Application Enablement Services Management Console. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area displays the "Add TSAPI Links" form with fields for Link, Switch Connection, Switch CTI Link Number, ASAI Link Version, and Security. The "Apply Changes" and "Cancel Changes" buttons are at the bottom.

Form fields:

- Link: 2
- Switch Connection: S8300D
- Switch CTI Link Number: 1
- ASAI Link Version: 4
- Security: Unencrypted

Buttons: Apply Changes, Cancel Changes



## 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**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Communication Manager Interface' and 'Switch Connections'. The main content area displays a table of switch connections. The table has four columns: Connection Name, Processor Ethernet, Msg Period, and Number of Active Connections. There are two entries: S8300D and S8800. The S8300D entry is selected with a radio button. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'. A top right status bar shows user information and server details.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> S8300D	No	30	1
<input type="radio"/> S8800	No	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, in this case “10.32.39.83” as shown below. Click **Add Name or IP**.

The screenshot shows the 'Edit H.323 Gatekeeper - S8300D' screen. The left navigation pane is the same as the previous screenshot. The main content area has a text input field containing '10.32.39.83' and an 'Add Name or IP' button. Below the input field are 'Delete IP' and 'Back' buttons. A top right status bar shows user information and server details.

## 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 shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Security' expanded, with 'Security Database' and 'Control' selected. The main content area is titled 'SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services'. It 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. The top right corner displays user information: 'Welcome: User', 'Last login: Tue Sep 3 10:41:39 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: 6.3.0.0.212-0', and 'Server Date and Time: Tue Sep 03 10:56:36 MDT 2013'. The top navigation bar includes 'Security | Security Database | Control' and 'Home | Help | Logout'.

## 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 the Avaya Application Enablement Services Management Console. The left navigation pane has 'Maintenance' expanded, with 'Service Controller' selected. The main content area is titled 'Service Controller'. It contains a table with two columns: 'Service' and 'Controller Status'. The table lists several services, with 'DMCC Service' and 'TSAPI Service' checked. Below the table is a link to 'Status and Control' and a row of buttons: 'Start', 'Stop', 'Restart Service', 'Restart AE Server', 'Restart Linux', and 'Restart Web Server'. The top right corner displays user information: 'Welcome: User', 'Last login: Tue Sep 3 10:41:39 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: 6.3.0.0.212-0', and 'Server Date and Time: Tue Sep 3 10:57:59 MDT 2013'. The top navigation bar includes 'Maintenance | Service Controller' and 'Home | Help | Logout'.

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 Capture911 User

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

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select “Yes” from the drop-down list. Retain the default value in the remaining fields. Click **Apply** at the bottom of the screen (not shown below).

**AVAYA**

**Application Enablement Services**  
Management Console

Welcome: User  
Last login: Tue Sep 3 10:48:22 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: 6.3.0.0.212-0  
Server Date and Time: Tue Sep 3 11:31:31 MDT 2013

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

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with \* can not be empty.

\* User Idcapture911

\* Common Namecapture911

\* Surnamecapture911

\* User Password●●●●●●●●

\* Confirm Password●●●●●●●●

Admin Note

Avaya RoleNone

Business Category

Car License

CM Home

Css Home

CT UserYes

Department Number

Display Name

Employee Number

Employee Type



## 6.8. 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 Capture911. Retain the default values in the remaining fields. Click **Apply Changes** at the bottom of the screen (not shown below).

**AVAYA**

**Application Enablement Services**  
Management Console

Welcome: User  
Last login: Tue Sep 3 10:48:22 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: 6.3.0.0.212-0  
Server Date and Time: Tue Sep 3 11:27:49 MDT 2013

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▼ Networking

AE Service IP (Local IP)

Network Configure

Ports

TCP Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999

Enabled Disabled

Encrypted TCP Port9998

DLG Port

TCP Port5678

TSAPI Ports

TSAPI Service Port450

Enabled Disabled

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Enabled Disabled

Encrypted Port4722

TR/87 Port4723

## 7. Configure HigherGround Capture911

This section provides the procedures for configuring Capture911. The procedures include the following areas:

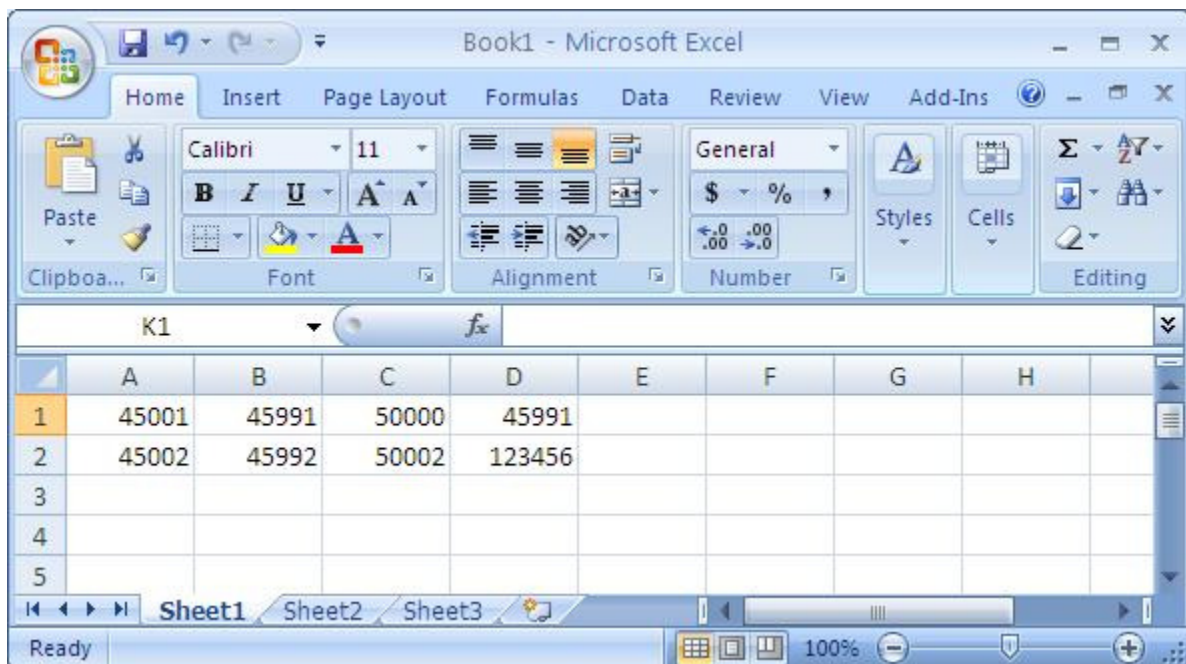
- Administer extensions
- Administer DMCC integrator service
- Administer VoIP channels
- Administer station utility

The configuration of Capture911 is performed by HigherGround technicians. The procedural steps are presented in these Application Notes for informational purposes.

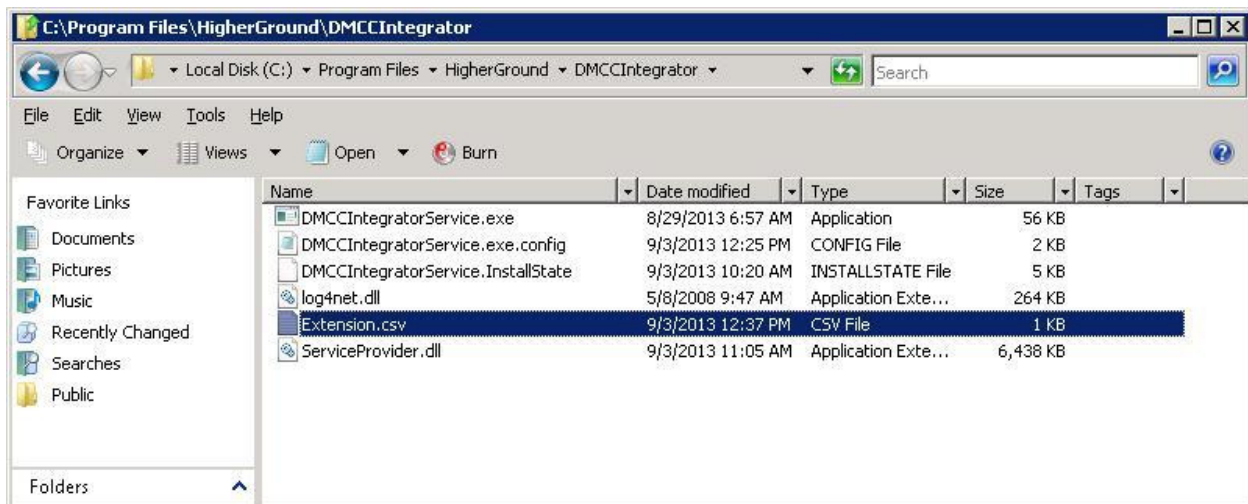
### 7.1. Administer Extensions

From any PC running the Microsoft Excel application, create a worksheet containing an entry for each monitored agent from **Section 3**. Enter the following values for the specified fields, as shown below.

- **Cell A:** The agent station extension from **Section 3**.
- **Cell B:** An available virtual IP softphone extension from **Section 5.4**.
- **Cell C:** An available even RTP port number in the range of 50000-65535.
- **Cell D:** The security code for the available virtual IP softphone from **Section 5.4**.

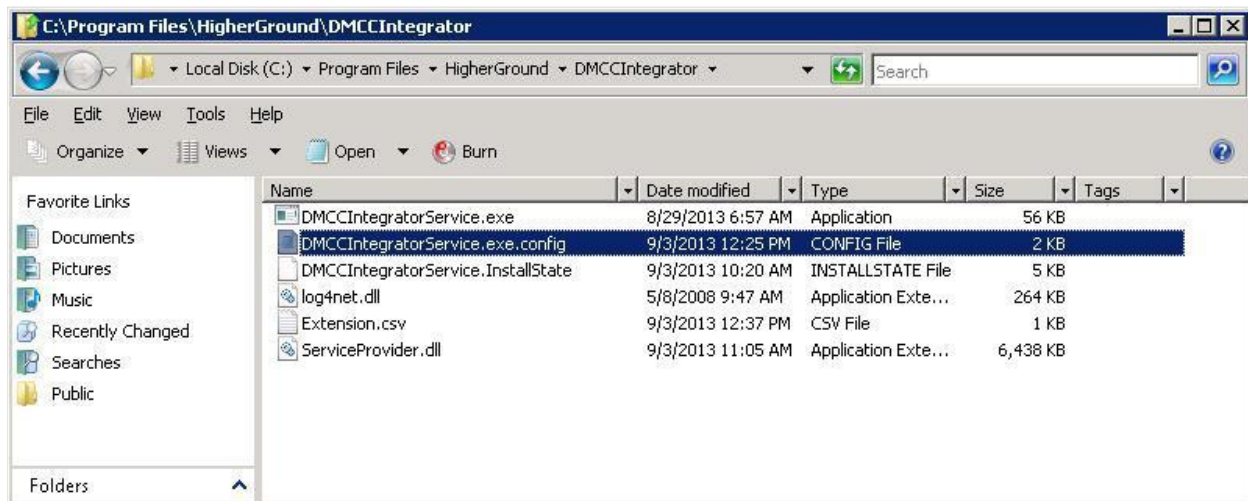


Save the worksheet using **Extension** as file name, and **CSV** as file type. Manually copy the resultant **Extension.csv** file to the Capture911 server running the Recorder component, in this case under directory **C:\Program Files\HigherGround\DMCCIntegrator**, as shown below.



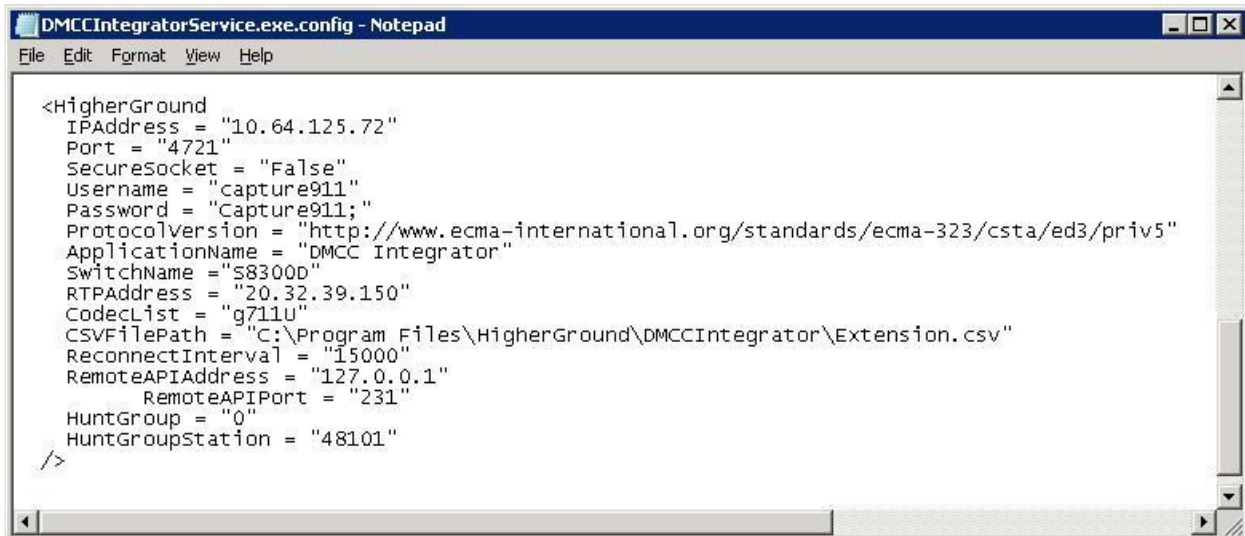
## 7.2. Administer DMCC Integrator Service

From the Capture911 server running the Recorder component, navigate to the **C:\Program Files\HigherGround\DMCCIntegrator** directory to locate the **DMCCIntegratorService.exe.config** file shown below.



Open the **DMCCIntegratorService.exe.config** file with the Notepad application. Navigate to the **HigherGround** sub-section. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **IPAddress:** IP Address of Application Enablement Services.
- **Port:** The DMCC unencrypted port value from **Section 6.8**.
- **Username:** The Capture911 user credentials from **Section 6.7**.
- **Password:** The Capture911 user credentials from **Section 6.7**.
- **ProtocolVersion:** "http://www.ecma-international.org/standards/ecma-323/csta/ed3/priv5"
- **SwitchName:** The relevant switch connection name from **Section 6.3**.
- **RTPAddress:** IP address of Capture911 server running the Recorder component.
- **CSVFilePath:** The path to the manually installed Extension.csv file.
- **RemoteAPIAddress:** "127.0.0.1"
- **HuntGroupStation:** The skill group extension to be monitored from **Section 3**.



```
<HigherGround
  IPAddress = "10.64.125.72"
  Port = "4721"
  SecureSocket = "False"
  Username = "capture911"
  Password = "capture911;"
  ProtocolVersion = "http://www.ecma-international.org/standards/ecma-323/csta/ed3/priv5"
  ApplicationName = "DMCC Integrator"
  SwitchName = "S8300D"
  RTPAddress = "20.32.39.150"
  CodecList = "g711u"
  CSVFilePath = "C:\Program Files\HigherGround\DMCCIntegrator\Extension.csv"
  ReconnectInterval = "15000"
  RemoteAPIAddress = "127.0.0.1"
    RemoteAPIPort = "231"
  HuntGroup = "0"
  HuntGroupStation = "48101"
/>
```

### 7.3. Administer VoIP Channels

From the Capture911 server running the Management Portal application, double click on the **HigherGround Management Portal** icon, which was created as part of installation.



The **HigherGround Capture911** screen is displayed. Log in using the appropriate credentials.

The window title is 'HigherGround Capture911 - HgManage Login [DEVCONNE-841693]'. It features the 'Next Generation capture911 incident re-creation' logo on the left. On the right, there are input fields for 'User Name:' and 'Password:', followed by 'Log In' and 'Cancel' buttons.

Next Generation  
**capture911**<sup>TM</sup>  
incident re-creation

User Name:

Password:

**Log In** **Cancel**

The **HigherGround Capture911 Control Tower – User/Channel Table** screen is displayed next. Select the first **VoIP Channel** entry on the left portion of the screen.

The window title is 'HigherGround Capture911 Control Tower - User/Channel Table'. It has tabs for 'Settings', 'Database', 'Table', 'Utility', and 'Run'. Below the tabs are two checked checkboxes: 'Show interactive users' and 'Show recorder channels'. The main area contains a table with columns: System ID, Record Type, User Name, Station, Station Name, and User Level. The first 'VoIP Channel' entry is highlighted in red.

HigherGround Capture911 Control Tower - User/Channel Table

Settings Database Table Utility Run

☒ Show interactive users

☒ Show recorder channels

System ID	Record Type	User Name	Station	Station Name	User Level
DEVCONNE-841693	Interactive User	ADMIN	99		Admin
DEVCONNE-841693	Interactive User	UNIT1	1		Station Only
DEVCONNE-841693	Interactive User	UNIT2	2		Station Only
DEVCONNE-841693	VoIP Channel	CLU1-001	1		
DEVCONNE-841693	VoIP Channel	CLU1-002	2		
DEVCONNE-841693	VoIP Channel	CLU1-003	3		
DEVCONNE-841693	VoIP Channel	CLU1-004	4		



In the right portion of the screen shown below, enter the following values for the specified fields in the **Connection** sub-section, and retain the default values for the remaining fields.

- **Station:** The first agent station extension from **Section 3**.
- **VoIP IP:** IP address of Capture911 server running the Recorder component.
- **Port:** The corresponding RTP port number for the agent from **Section 7.1**.

The screenshot shows a configuration window with two main sections: Identification and Connection.

**Identification Section:**

- Record Type: VoIP Channel
- Recorder Unit: 1
- User Name: CLU1-001
- Channel: 1
- Recording Group: Automatic
- Location: (empty)
- System ID: DEVCONNE-841693

**Connection Section:**

- Station: 45001
- Picker: 45001
- Station Name: (empty)
- Department: (empty)
- Division: (empty)
- VoIP IP: 20.32.39.150
- Port: 50000 0 0
- VoIP MAC: 00:00:00:00:00:00

Repeat this section to administer a VoIP channel for each agent station extension from **Section 3**. In the compliance testing, two VoIP channels were configured as shown below.

The screenshot shows a table titled "HigherGround Capture911 Control Tower - User/Channel Table". The table has the following columns: System ID, Record Type, User Name, Station, Station Name, User Level, Trigger, VoIP IP, and VoIP MAC. The table contains several rows, with two rows highlighted in red, representing VoIP channels.

System ID	Record Type	User Name	Station	Station Name	User Level	Trigger	VoIP IP	VoIP MAC
DEVCONNE-841693	Interactive User	ADMIN	99		Admin	ROD DNR		
DEVCONNE-841693	Interactive User	UNIT1	1		Station Only			
DEVCONNE-841693	Interactive User	UNIT2	2		Station Only			
DEVCONNE-841693	VoIP Channel	CLU1-001	45001			VoIP	20.32.39.150	00:00:00:00:00:00
DEVCONNE-841693	VoIP Channel	CLU1-002	45002			VoIP	20.32.39.150	00:00:00:00:00:00
DEVCONNE-841693	VoIP Channel	CLU1-003	3			VoIP	0.0.0.0	00:00:00:00:00:00
DEVCONNE-841693	VoIP Channel	CLU1-004	4			VoIP	0.0.0.0	00:00:00:00:00:00

## 7.4. Administer Station Utility

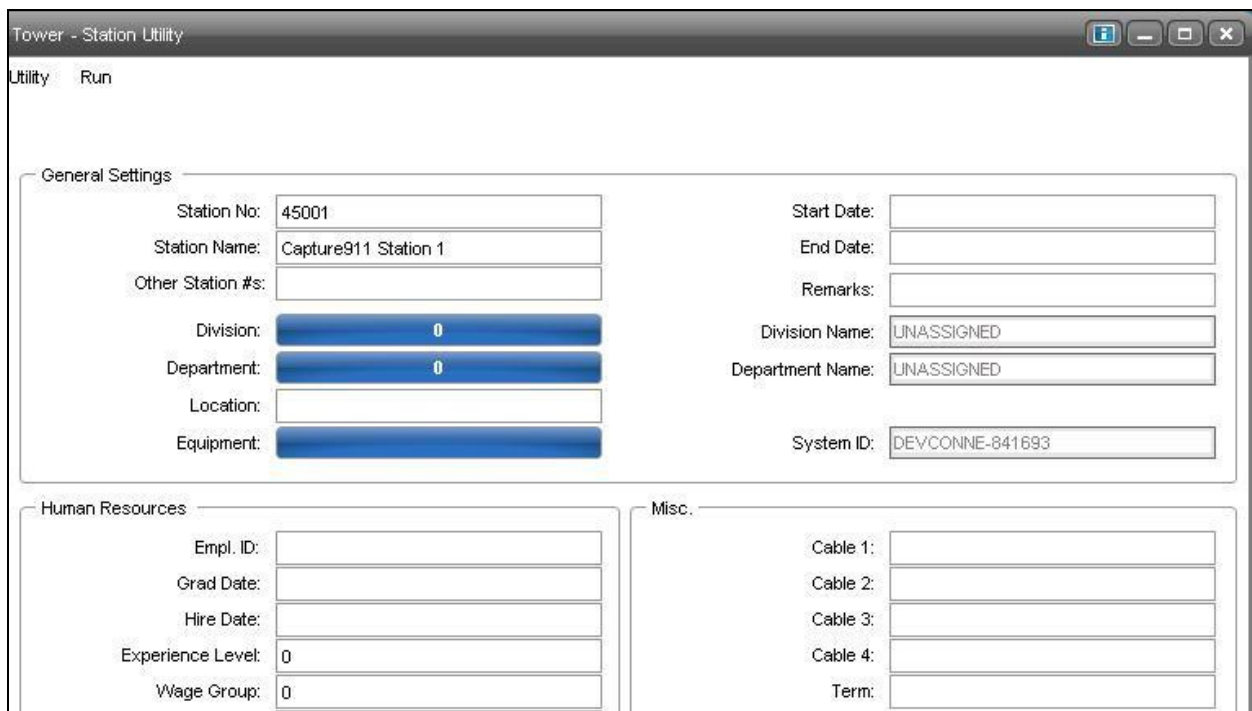
Select **Utility** → **Station Utility** from the top menu to display the **HigherGround Capture911 Control Tower – Station Utility** screen. Click **Add** in the bottom left portion of the screen (not shown).



System ID	Station	Name	Division	Division Name
DEVCONNE-841693	9999	Test Phone	0	UNASSIGNED

In the right portion of the screen shown below, enter the following values for the specified fields in the **General Settings** sub-section, and retain the default values for the remaining fields.

- **Station No:** The first agent station extension from **Section 3**.
- **Station Name:** A desired station name.



Tower - Station Utility

Utility Run

General Settings

Station No: 45001

Station Name: Capture911 Station 1

Other Station #s:

Division: 0

Department: 0

Location:

Equipment:

Start Date:

End Date:

Remarks:

Division Name: UNASSIGNED

Department Name: UNASSIGNED

System ID: DEVCONNE-841693

Human Resources

Empl. ID:

Grad Date:

Hire Date:

Experience Level: 0

Wage Group: 0

Misc.

Cable 1:

Cable 2:

Cable 3:

Cable 4:

Term:

Repeat this section to create a station utility entry for each agent station and agent ID extension from **Section 3**. In the compliance testing, four station utility entries were configured as shown below.

HigherGround Capture911 Control Tower - Station Utility

Settings Database Table Utility Run

☒ Show expired Stations

☒ Show older versions of Stations

System ID	Station	Name	Division	Division Name	Department	Department
DEVCONNE-841693	9999	Test Phone	0	UNASSIGNED	0	UNASSIGNED
DEVCONNE-841693	45001	Capture911 Station 1	0	UNASSIGNED	0	UNASSIGNED
DEVCONNE-841693	45002	Capture911 Station 2	0	UNASSIGNED	0	UNASSIGNED
DEVCONNE-841693	45881	Agent1	0	UNASSIGNED	0	UNASSIGNED
DEVCONNE-841693	45882	Agent2	0	UNASSIGNED	0	UNASSIGNED

Save Cancel Add Remove Copy Apply To Report



## 8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, and Capture911.

### 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
<b>1</b>	<b>4</b>	<b>no</b>	<b>aes_125_72</b>	<b>established</b>	<b>16</b>	<b>17</b>

Verify the registration status of the virtual softphones by using the “list registered-ip-stations” command. Verify that all extensions from **Section 5.4** are displayed, 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		
45000	9650	IP_Phone	y	10.32.39.104		
	1	3.105S		10.32.39.83		
45001	1608	IP_Phone	y	10.32.39.105		
	1	1.330D		10.32.39.83		
45002	9611	IP_Phone	y	10.32.39.106		
	1	6.2209		10.32.39.83		
<b>45991</b>	<b>4620</b>	<b>IP_API_A</b>	<b>y</b>	<b>10.64.125.72</b>		
	<b>1</b>	<b>3.2040</b>		<b>10.32.39.83</b>		
<b>45992</b>	<b>4620</b>	<b>IP_API_A</b>	<b>y</b>	<b>10.64.125.72</b>		
	<b>1</b>	<b>3.2040</b>		<b>10.32.39.83</b>		

## 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**.

**Application Enablement Services**  
Management Console

Welcome: User  
Last login: Tue Sep 3 13:13:34 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: 6.3.0.0.212-0  
Server Date and Time: Wed Sep 4 07:52:37 MDT 2013

Status | Status and Control | TSAPI Service Summary

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ 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



▶ User Management

▶ Utilities

▶ Help

TSAPI Link Details

☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
	1	S8800	2	Talking	Mon Aug 19 09:35:30 2013	Online	16	2	15	15	30
	2	S8300D	1	Talking	Wed Sep 4 07:21:02 2013	Online	16	3	23	23	30

Online

Offline

For service-wide information, choose one of the following:


TSAPI Service Status

TLink Status

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 Capture911 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.



**Application Enablement Services**  
Management Console

Welcome: User  
Last login: Tue Sep 3 13:13:34 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: 6.3.0.0.212-0  
Server Date and Time: Wed Sep 4 07:52:59 MDT 2013

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

▶ AE Services  
▶ Communication Manager Interface  
▶ 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  
▶ User Management  
▶ Utilities  
▶ Help

DMCC Service Summary - Session Summary

☐ Enable page refresh every 60 seconds

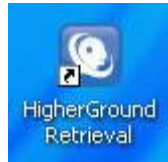
Session Summary [Device Summary](#)  
Generated on Wed Sep 04 07:52:54 MDT 2013  
Service Uptime: 0 days, 18 hours 37 minutes  
Number of Active Sessions: 1  
Number of Sessions Created Since Service Boot: 8  
Number of Existing Devices: 5  
Number of Devices Created Since Service Boot: 25

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	41C58A00745D3D7D0 226603FD64D8486-7	capture911	DMCC Integrator	20.32.39.150	XML Unencrypted	5

Item 1-1 of 1

### 8.3. Verify HigherGround Capture911

Log an agent in to the monitored skill group to handle and complete an ACD call. From the agent PC, double click on the shortcut of the HigherGround Retrieval application that resides on the Capture911 server.



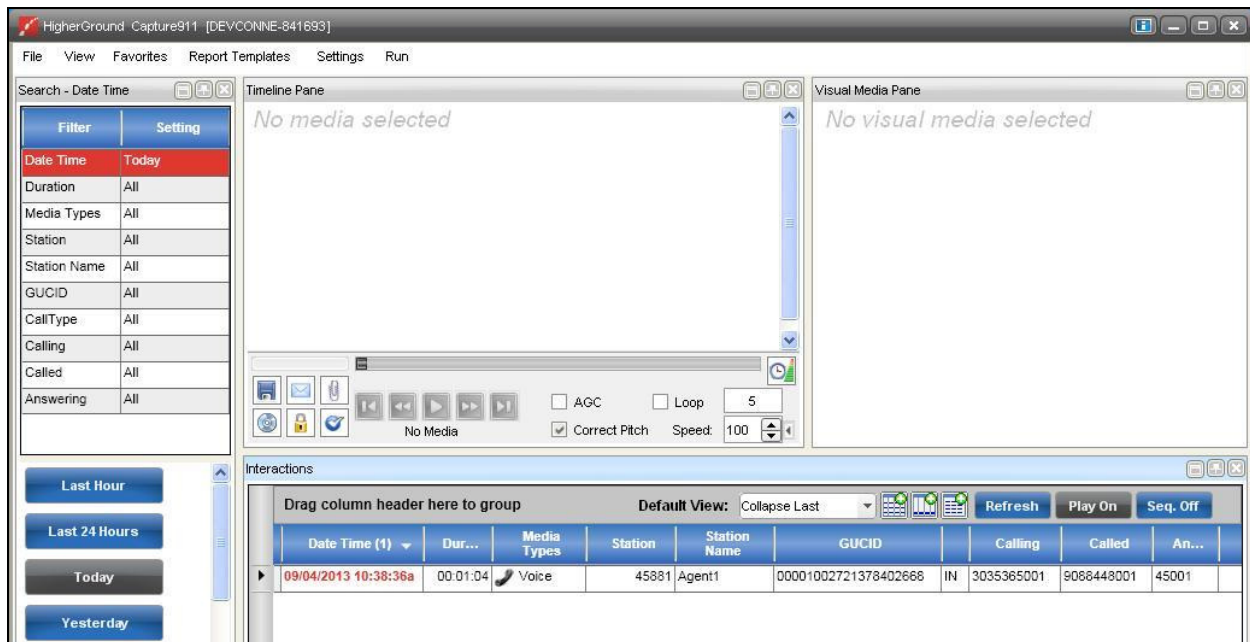
The screen below is displayed. Log in using the appropriate credentials.

A screenshot of a login window titled 'HigherGround Capture911 - HgRetrieval Login [DEVCONNE-841693]'. The window features the 'capture911' logo with the tagline 'incident re-creation'. To the right of the logo are two input fields labeled 'User Name:' and 'Password:'. Below these fields are two buttons: 'Log In' and 'Cancel'.

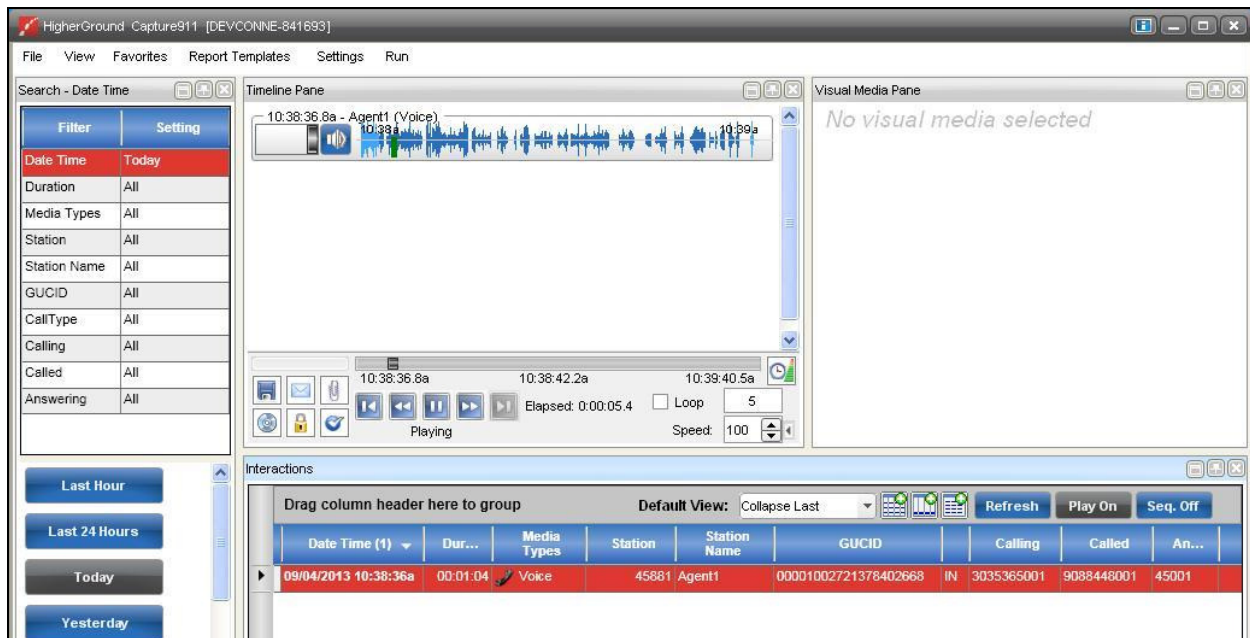
The screen below is displayed briefly while the forms are loading.



The **HigherGround Capture911** screen below is displayed next with a list of the call recordings for today. Verify that there is an entry reflecting the last call, with proper values in the relevant fields.



Select the entry and verify that the call recording can be played back.



## 9. Conclusion

These Application Notes describe the configuration steps required for HigherGround Capture911 to successfully interoperate with Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

## 10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 8, Release 6.3, May 2013, available at <http://support.avaya.com>.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3, Issue 1, May 2013, available at <http://support.avaya.com>.
3. *Capture911 Administrator Manual, Version 8.1*, available as part of Capture911 installation.
4. *Avaya DMCC Based Call Monitoring Installation Manual, Version 1.1, 4/2009*, Version v.2.1, 2013, available as part of Capture911 installation.
5. *Capture911 User Manual*, Version v.2.1, 2013, available as part of Capture911 installation.

---

**©2013 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).