



Application Notes for BBX Vuesion Multichannel Contact Center with Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services, and Avaya Aura® Session Manager – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for BBX Vuesion Multichannel Contact Center to interoperate with Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services, and Avaya Aura® Session Manager. BBX Vuesion Multichannel Contact Center is a contact center management solution.

In the compliance testing, BBX Vuesion Multichannel Contact Center provided routing, announcements, screen pop, call control, and call reporting by using the Telephony Services Application Programming Interface from Avaya Aura® Application Enablement Services, and the SIP User interface from Avaya Aura® Session Manager.

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 BBX Vuesion Multichannel Contact Center to interoperate with Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services, and Avaya Aura® Session Manager. BBX Vuesion Multichannel Contact Center is a contact center management solution, and the compliance testing focused on the voice channel integration.

In the compliance testing, BBX Vuesion Multichannel Contact Center provided routing, announcements, screen pop, call control, and call reporting by using the Telephony Services Application Programming Interface (TSAPI) from Avaya Aura® Application Enablement Services, and the SIP User interface from Avaya Aura® Session Manager.

The SIP User interface was used by BBX Vuesion Multichannel Contact Center to register virtual SIP users with Avaya Aura® Session Manager. The virtual SIP users were configured in a hunt group on Avaya Aura® Communication Manager, with incoming ACD calls routed over an available virtual SIP user to BBX Vuesion Multichannel Contact Center for IVR treatments such as announcements, digit collections, and routing actions. SIP REFER was used to route incoming ACD calls to available call answering station users (hereafter referred to as agents) on Avaya Aura® Communication Manager.

The TSAPI interface was used by BBX Vuesion Multichannel Contact Center to monitor VDNs, virtual SIP users, and agent users on Avaya Aura® Communication Manager, to provide call control via the agent desktops, and to provide screen pop and call reporting features. The agents have desktop computers running the Vuesion Client application, with BBX Vuesion Multichannel Contact Center providing all ACD related features, such as work modes and availability for ACD calls. Call related actions such as answering of incoming calls can be initiated via the agent telephone, or via the agent desktops.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Vuesion application, the application used TSAPI to request monitoring on VDNs, virtual SIP user stations, and agent user stations. For the manual part of the testing, calls were made to the VDNs. Manual call controls from both the agent telephones and agent desktop computers were exercised.

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

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

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Vuesion:

- Handling of SIP messages in areas of registration, codec negotiation, media shuffling, session refresh, hold/reconnect, inbound DTMF, and transfer.
- Handling of TSAPI messages in areas of event notification and call control.
- Handling of various call scenarios including internal, external, inbound, outbound, answer, hold/resume, drop, blind/attended transfer, blind/attended conference, voicemail coverage, ACD queue, multiple agents, and multiple calls.
- Reporting of basic call scenarios including inbound, outbound, hold/resume, and drop.

The serviceability testing focused on verifying the ability of Vuesion to recover from adverse conditions, such as disconnecting and reconnecting the Ethernet connection to the Vuesion server or to the Vuesion Client.

2.2. Test Results

All test cases were executed and verified. The following was an observation on Vuesion from the compliance testing:

- This release does not support transfer and conference actions from the Vuesion Client application. In the compliance testing, all transfer and conference actions were initiated from the agent telephones, including subsequent drops. Note that when an agent used Vuesion Client to drop from a conference, then all remaining parties will also be dropped per current design.

2.3. Support

Technical support on Vuesion can be obtained through the following:

- **Phone:** (800) 930-4229, option 4
- **Email:** bbxservice@bbxtech.com
- **Web:** www.bbxtech.com

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The Vuesion solution consisted of the Vuesion server, Vuesion Client, and Vuesion Reports. The Vuesion Client application was running on the agent desktops, and the Vuesion Reports application was running on the supervisor desktop.

The detailed administration of basic connectivity between Communication Manager, Application Enablement Services, System Manager, and Session Manager are not the focus of these Application Notes and will not be described. The applicable domain name was “dr220.com”.

In the compliance testing, Vuesion monitored all VDN and station extensions shown in the table below. The supervisor and agent stations were pre-existing. The VDNs, IVR hunt group, and virtual SIP stations were created new and shown in subsequent sections.

Device Type	Extension
VDN	65500, 65501, 65502, 65599
IVR Hunt Group	65551
Virtual SIP Station	66991, 66992
Supervisor Station	65000
Agent Station	65001, 65002

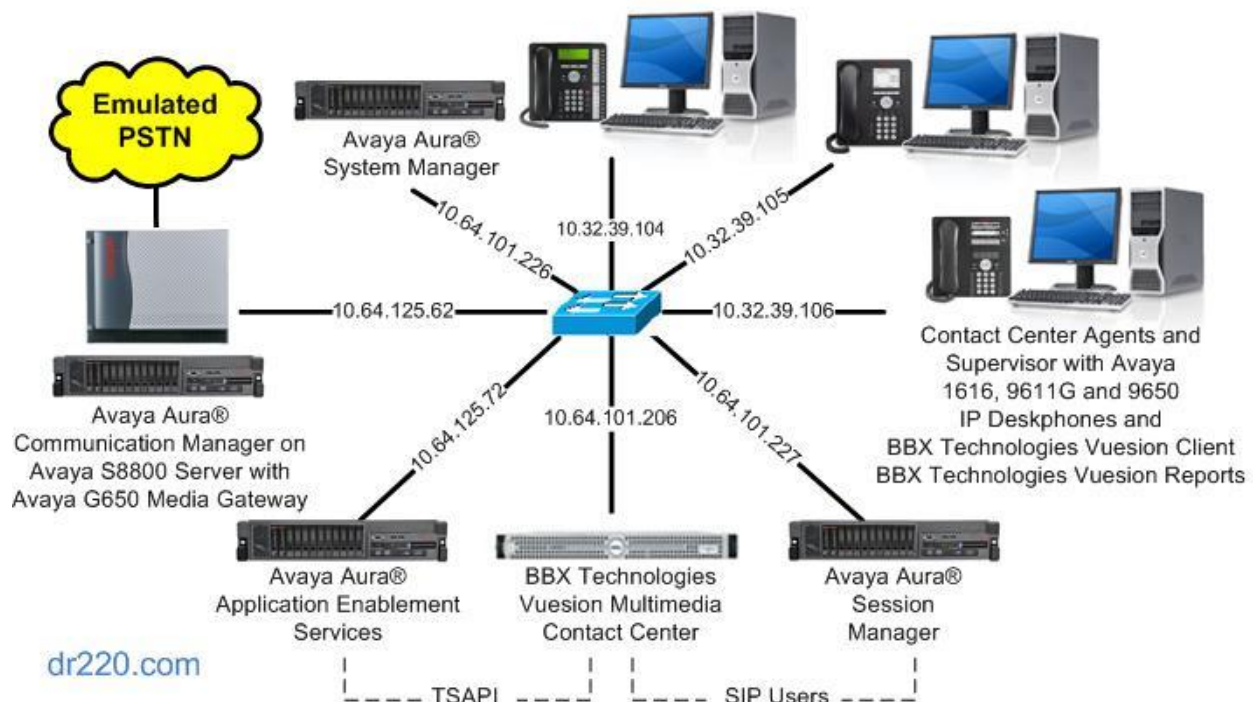


Figure 1: Compliance Testing Configuration

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 S8800 Server with Avaya G650 Media Gateway	6.3.6 (R016x.03.0.124.0-21591)
Avaya Aura® Application Enablement Services	6.3.3 (6.3.3.0.10-0)
Avaya Aura® Session Manager	6.3.8
Avaya Aura® System Manager	6.3.8
Avaya 1616 IP Deskphone (H.323)	1.350B
Avaya 9611G IP Deskphone (H.323)	6.4014
Avaya 9650 IP Deskphone (H.323)	3.230A
BBX Vuesion Multichannel Contact Center on Windows Server 2012 R2 Standard	9.4
• Avaya TSAPI Windows Client (csta32.dll)	6.3.1.502
BBX Vuesion Client	9.4
BBX Vuesion Reports	9.4

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 IP codec set
- Administer hunt group
- Administer vectors and VDNs

5.1. Verify License

Log into 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 there is sufficient capacity for SIP users by comparing the **Maximum Off-PBX Telephones - OPS** field value with the corresponding value in the **USED** column.

The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.

display system-parameters customer-options		Page 1 of 11
OPTIONAL FEATURES		
G3 Version: V16	Software Package: Enterprise	
Location: 2	System ID (SID): 1	
Platform: 28	Module ID (MID): 1	
USED		
Platform Maximum Ports:	65000	162
Maximum Stations:	41000	20
Maximum XMOBILE Stations:	41000	0
Maximum Off-PBX Telephones - EC500:	41000	1
Maximum Off-PBX Telephones - OPS:	41000	4
Maximum Off-PBX Telephones - PBFMC:	41000	0

Navigate to **Page 3**, and verify that the **Computer Telephony Adjunct Links** customer option is set to “y”. If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.

display system-parameters customer-options	Page 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	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? n	DCS Call Coverage? y
ASAI Link Plus Capabilities? n	DCS with Rerouting? y
Async. Transfer Mode (ATM) PNC? n	
Async. Transfer Mode (ATM) Trunking? n	Digital Loss Plan Modification? y
ATM WAN Spare Processor? n	DS1 MSP? y

Navigate to **Page 6**, and verify that the **Vectoring (Basic)** customer option is set to “y”.

display system-parameters customer-options	Page 6 of 11
CALL CENTER OPTIONAL FEATURES	
Call Center Release: 6.0	
ACD? y	Reason Codes? y
BCMS (Basic)? y	Service Level Maximizer? n
BCMS/VuStats Service Level? y	Service Observing (Basic)? y
BSR Local Treatment for IP & ISDN? y	Service Observing (Remote/By FAC)? y
Business Advocate? n	Service Observing (VDNs)? y
Call Work Codes? y	Timed ACW? y
DTMF Feedback Signals For VRU? y	Vectoring (Basic)? y
Dynamic Advocate? n	Vectoring (Prompting)? y
Expert Agent Selection (EAS)? y	Vectoring (G3V4 Enhanced)? y
EAS-PHD? y	Vectoring (3.0 Enhanced)? 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 2	Page 1 of 3
CTI LINK	
CTI Link: 2	
Extension: 60100	
Type: ADJ-IP	
COR: 1	
Name: AES CTI Link	

5.3. Administer System Parameters Features

Use the “change system-parameters features” command, and set **Music (or Silence) on Transferred Trunk Calls** to “call-wait”. This setting will apply music, if administered, to the trunk caller, while waiting for the transfer-to station to answer.

```
change system-parameters features                                     Page 1 of 20
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? n
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y

      Music (or Silence) on Transferred Trunk Calls? call-wait
      DID/Tie/ISDN/SIP Intercept Treatment: attendant
      Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
      Automatic Circuit Assurance (ACA) Enabled? n

      Abbreviated Dial Programming by Assigned Lists? n
      Auto Abbreviated/Delayed Transition Interval (rings): 2
      Protocol for Caller ID Analog Terminals: Bellcore
      Display Calling Number for Room to Room Caller ID Calls? n
```

5.4. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is the codec set number used by the pre-existing SIP trunk to Session Manager. Update the audio codec types in the **Audio Codec** fields as necessary to include G.729, which is the only codec variant supported by Vuesion for the virtual SIP users.

```
change ip-codec-set 1                                             Page 1 of 2
      IP Codec Set

      Codec Set: 3

      Audio      Silence      Frames      Packet
      Codec      Suppression  Per Pkt    Size(ms)
1: G.711MU      n          2          20
2: G.729      n        2        20
3:
```


5.5. Administer Hunt Group

Proceed to **Section 7** to configure Session Manager. After the new virtual SIP users for use by Vuesion have been added in Session Manager, return to this section to configure a hunt group for routing of calls to Vuesion.

Add a hunt group using the “add hunt n” command, where “n” is an available hunt group number. For **Group Name**, enter a descriptive name. For **Group Extension**, enter an available extension number. For **Group Type**, enter “circ”.

add hunt-group 551		Page 1 of 60	
HUNT GROUP			
Group Number: 551			
Group Name: BBX IVR Pilot			
Group Extension: 65551			
Group Type: circ		Coverage Path:	
TN: 1		Night Service Destination:	
COR: 1		MM Early Answer? n	
Security Code:		Local Agent Preference? n	
ISDN/SIP Caller Display:			

Navigate to **Page 3**, and enter all SIP user extensions from **Section 7.2**, as shown below.

add hunt-group 551		Page 3 of 60	
HUNT GROUP			
Group Number: 551		Group Extension: 65551	
Group Type: circ			
Member Range Allowed: 1 - 1500		Administered Members (min/max): 0 /0	
Total Administered Members: 0			
GROUP MEMBER ASSIGNMENTS			
Ext	Name(19 characters)	Ext	Name(19 characters)
1: 66991		14:	
2: 66992		15:	
3:		16:	

5.6. Administer Vectors and VDNs

Administer a set of vectors and VDNs for routing of calls to Vuesion. The number of VDNs and vectors, and the detailed vector steps may vary based on customer needs. In the compliance testing, four VDNs and one vector were created.

The Sales and Support VDNs were used for routing of ACD calls from the PSTN, and the Tenant and IVR Pilot VDNs were used for routing of internal administrative function calls such as retrieval of group announcements and change of emergency announcements.

VDN	Vector	Purpose
65500	501	For delivering Tenant calls to Vuesion
65501	501	For delivering Sales calls to Vuesion
65502	501	For delivering Support calls to Vuesion
65599	501	For delivering IVR Pilot calls to Vuesion

Modify a vector using the “change vector n” command, where “n” is an available vector number. Enter a descriptive **Name** and add a **route-to number** step. Use the hunt group extension from **Section 5.5** as the **route-to number** destination, as shown below.

change vector 501				Page 1 of 6	
CALL VECTOR					
Number: 501		Name: BBX Vector			
Multimedia? n	Attendant Vectoring? n	Meet-me Conf? n	Lock? n		
Basic? y	EAS? y	G3V4 Enhanced? y	ANI/II-Digits? y	ASAI Routing? y	
Prompting? y	LAI? y	G3V4 Adv Route? y	CINFO? y	BSR? y	Holidays? y
Variables? y	3.0 Enhanced? y				
01	route-to	number 65551	with cov n if unconditionally		
02	stop				
03					

Add a VDN using the “add vdn n” command, where “n” is an available extension, in this case “65500”. Associate this VDN with the newly added vector from above.

- **Name:** A descriptive name.
- **Destination:** “Vector Number” along with the vector number from above.

```
add vdn 65500                                     Page 1 of 2
                                         VECTOR DIRECTORY NUMBER
                                         Extension: 65500
                                         Name*: BBX Tenant
                                         Destination: Vector Number      501
Attendant Vectoring? n
Meet-me Conferencing? N
COR: 1
TN*: 1
Measured: none
```

Repeat this section to add all desired VDNs. In the compliance testing, four VDNs were added, as shown below.

```
list vdn 65500 count 4
                                         VECTOR DIRECTORY NUMBERS
                                         Evnt
                                         Noti
Name (22 characters)  Ext/Skills  VDN  Vec  Orig  Adj
Ovr COR TN  PRT Num  Meas Annc
BBX Tenant          65500      n  1   1   V  501  none
BBX Sales          65501      n  1   1   V  501  none
BBX Support        65502      n  1   1   V  501  none
BBX IVR Pilot      65599      n  1   1   V  501  none
```

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
- Disable security database
- Restart TSAPI service
- Obtain Tlink name
- Administer Vuesion user

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 red horizontal bar spans the width of the page, with a "Help" link on the right. In the center, there 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, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2014 Avaya Inc. All Rights Reserved." is displayed.

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

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 with system details: "Welcome: User", "Last login: Tue Oct 14 08:58:28 2014 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: 6.3.3.0.10-0", "Server Date and Time: Tue Oct 14 09:52:17 MDT 2014", and "HA Status: Not Configured". A red navigation bar contains "Home", "Help", and "Logout". On the left, a sidebar lists menu items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The main content area is titled "Welcome to OAM" and contains a paragraph: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:". This is followed by a bulleted list of domains and their functions: "AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.", "Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.", "High Availability - Use High Availability to manage AE Services HA.", "Licensing - Use Licensing to manage the license server.", "Maintenance - Use Maintenance to manage the routine maintenance tasks.", "Networking - Use Networking to manage the network interfaces and ports.", "Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.", "Status - Use Status to obtain server status informations.", "User Management - Use User Management to manage AE Services users and AE Services user-related resources.", "Utilities - Use Utilities to carry out basic connectivity tests.", and "Help - Use Help to obtain a few tips for using the OAM Help system". A final paragraph states: "Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain."


6.2. Verify License

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

The screenshot displays the Avaya Application Enablement Services Management Console with the "Licensing" menu item selected in the left sidebar. The main content area is titled "Licensing" and contains three sections of instructions. The first section, "If you are setting up and maintaining the WebLM, you need to use the following:", lists "WebLM Server Address". The second section, "If you are importing, setting up and maintaining the license, you need to use the following:", lists "WebLM Server Access". The third section, "If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:", lists "Reserved Licenses". The sidebar menu shows "AE Services", "Communication Manager Interface", "High Availability", "Licensing" (selected), "Maintenance", and "Networking". The top header and navigation bar are identical to the previous screenshot.

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.


Web License Manager (WebLM v6.3)
Help | About | Change Password

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

10 Items Show ALL

Feature (License Keyword)	Expiration date	Licensed capacity
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	10000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiS MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_ LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;u TrustedApplications: IPS_001, BasicUnrestrict DMCUnrestricted; 1XP_001, BasicUnrestricted DMCUnrestricted; 1XM_001, BasicUnrestricted DMCUnrestricted; PC_001, BasicUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted DMCUnrestricted; VP_001, BasicUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AEC_UNIFIED_CC_DESKTOP,,, CCE_001, AdvancedUnrestricted, DMCUnrestricted; CSI_001, AdvancedUnrestricted, DMCUnrestricted; CSI_001, AdvancedUnrestricted, DMCUnrestricted; AVA_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, DMCUnrestricted, AgentEvents;
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	10000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16

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 Management Console interface. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows a tree structure with "AE Services" expanded, containing "CVLAN", "DLG", "DMCC", "SMS", "TSAPI" (expanded), "TSAPI Links" (selected), and "TSAPI Properties". The main content area is titled "TSAPI Links" and contains a table with columns: "Link", "Switch Connection", "Switch CTI Link #", "ASAI Link Version", and "Security". Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

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

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection "S8800" 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 "Add TSAPI Links" screen in the Avaya Management Console. The left navigation pane is the same as in the previous screenshot, but "Communication Manager Interface" is also visible under "TSAPI". The main content area is titled "Add TSAPI Links" and contains a form with the following fields: "Link" (value: 1), "Switch Connection" (value: S8800), "Switch CTI Link Number" (value: 2), "ASAI Link Version" (value: 6), and "Security" (value: Unencrypted). Below the form are buttons for "Apply Changes" and "Cancel Changes".

6.4. 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.

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

Welcome: User
Last login: Tue Oct 14 08:58:28 2014 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: 6.3.3.0.10-0
Server Date and Time: Tue Oct 14 09:52:17 MDT 2014
HA Status: Not Configured

Security | Security Database | Control Home | Help | Logout

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

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

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

6.5. Restart TSAPI Service

Select **Maintenance** → **Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check **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 the user. The left navigation pane shows a tree structure with "Maintenance" expanded and "Service Controller" selected. The main content area shows the "Service Controller" page with a table of services and their status. The "TSAPI Service" is checked, and the "Restart Service" button is highlighted.

Welcome: User
Last login: Tue Oct 14 08:58:28 2014 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: 6.3.3.0.10-0
Server Date and Time: Tue Oct 14 09:52:17 MDT 2014
HA Status: Not Configured

Maintenance | Service Controller Home | Help | Logout

Service Controller

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

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

6.6. Obtain Tlink Name

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

In this case, the associated Tlink name is “AVAYA#S8800#CSTA#AES_125_72”. Note the use of the switch connection “S8800” from **Section 6.3** as part of the Tlink name.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The main navigation bar shows "Security | Security Database | Tlinks" and links for "Home | Help | Logout". The left sidebar contains a tree view of the application's structure, with "Security" expanded to show "Security Database" and "Tlinks" selected. The main content area, titled "Tlinks", shows a single Tlink entry with the name "AVAYA#S8800#CSTA#AES_125_72" and a "Delete Tlink" button.

Welcome: User
Last login: Tue Oct 14 08:58:28 2014 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: 6.3.3.0.10-0
Server Date and Time: Tue Oct 14 09:52:17 MDT 2014
HA Status: Not Configured

Security | Security Database | Tlinks Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control
CTI Users
Devices
Device Groups
Tlinks

Tlinks
Tlink Name
AVAYA#S8800#CSTA#AES_125_72
Delete Tlink

6.7. Administer Vuesion User

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

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

AVAYA**Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Oct 14 08:58:28 2014 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: 6.3.3.0.10-0
Server Date and Time: Tue Oct 14 09:52:17 MDT 2014
HA Status: Not Configured

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

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

■ Add User

■ Change User Password

■ List All Users

■ Modify Default Users

■ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Idvuesion

* Common Namevuesion

* Surnamevuesion

* User Password*****

* Confirm Password*****

Admin Note

Avaya RoleNone ▼

Business Category

Car License

CM Home

Css Home

CT UserYes ▼

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

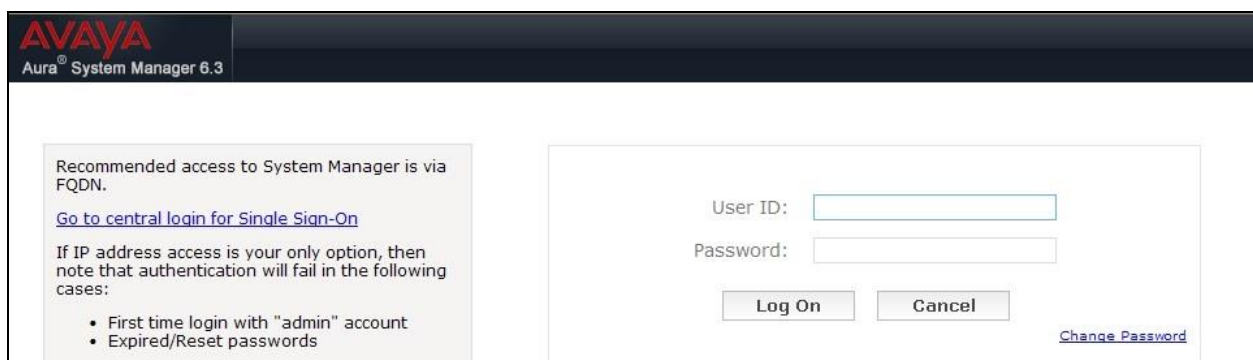
7. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer users

7.1. Launch System Manager

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



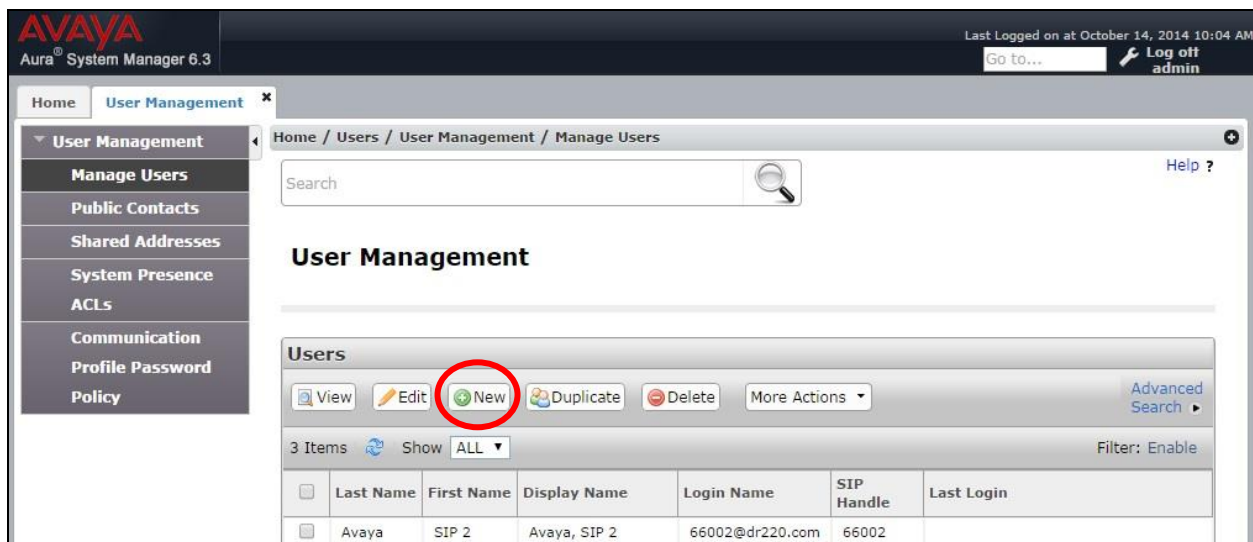
The screenshot shows the Avaya Aura System Manager 6.3 login interface. On the left, there is a text box with the following content: "Recommended access to System Manager is via FQDN. [Go to central login for Single Sign-On](#). If IP address access is your only option, then note that authentication will fail in the following cases:

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

". On the right, there is a login form with fields for "User ID:" and "Password:", a "Log On" button, a "Cancel" button, and a "Change Password" link.

7.2. Administer Users

In the subsequent screen (not shown), select **Users** → **User Management** → **Manage Users** to display the **User Management** screen below. Click **New** to add a user.



The screenshot shows the Avaya Aura System Manager 6.3 User Management screen. The top navigation bar includes "Home", "User Management", and "Manage Users". The left sidebar contains a tree view with "User Management" expanded, showing "Manage Users", "Public Contacts", "Shared Addresses", "System Presence", "ACLs", "Communication", "Profile Password", and "Policy". The main content area has a search bar and a "Help ?" link. Below the search bar, the "User Management" title is displayed. A "Users" section contains a toolbar with "View", "Edit", "New" (circled in red), "Duplicate", "Delete", and "More Actions" buttons. Below the toolbar, there is a table with 3 items. The table has columns: "Last Name", "First Name", "Display Name", "Login Name", "SIP Handle", and "Last Login". The first row shows "Avaya", "SIP 2", "Avaya, SIP 2", "66002@dr220.com", "66002", and an empty "Last Login" field.

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

7.2.1. Identity

The **New User Profile** screen is displayed. For **Last Name**, enter a desired user extension as required by Vuesion, in this case “66991”. For **First Name**, enter “IVR”, as shown below.

For **Login Name**, enter “x@y”, where “x” is the same user extension and “y” is the applicable domain name from **Section 3**. Retain the default values in the remaining fields.

The screenshot displays the Avaya Aura System Manager 6.3 interface. The top header shows the Avaya logo and 'Aura System Manager 6.3'. The right side of the header indicates the user is logged in as 'admin' and shows the last login time as 'October 14, 2014 10:04 AM'. The breadcrumb trail is 'Home / Users / User Management / Manage Users'. The left sidebar contains a 'User Management' menu with options: 'Manage Users' (selected), 'Public Contacts', 'Shared Addresses', 'System Presence', 'ACLs', 'Communication', 'Profile Password', and 'Policy'. The main content area is titled 'New User Profile' and includes buttons for 'Commit & Continue', 'Commit', and 'Cancel'. Below the title is a 'User Provisioning Rule' dropdown menu. The 'Identity' tab is selected, showing the following fields: 'Last Name' (66991), 'Last Name (Latin Translation)' (66991), 'First Name' (IVR), 'First Name (Latin Translation)' (IVR), 'Middle Name' (empty), 'Description' (empty), 'Login Name' (66991@dr220.com), 'Authentication Type' (Basic), 'Password' (empty), and 'Confirm Password' (empty).

7.2.2. Communication Profile

Select the **Communication Profile** tab. For **Communication Profile Password** and **Confirm Password**, enter the password as “VRx” where “x” is the same user extension, as required by Vuesion for the SIP user to use for registration. In this case, the password for SIP user “66991” is “VR66991”.

In the **Communication Address** sub-section, click **New** to add a new address. The sub-section is updated with additional fields, as shown below. For **Type**, retain “Avaya SIP”. For **Fully Qualified Address**, enter and select the SIP user extension and domain name to match the login name from **Section 7.2.1**. Click **Add**.

The screenshot displays the Avaya Aura System Manager 6.3 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 6.3', and a 'Last Logged on' timestamp. The left sidebar shows the 'User Management' menu with options like 'Manage Users', 'Public Contacts', 'Shared Addresses', 'System Presence', 'ACLs', 'Communication', 'Profile Password', and 'Policy'. The main content area is titled 'New User Profile' and contains four tabs: 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is selected, showing fields for 'Communication Profile Password' and 'Confirm Password'. Below these is a 'Communication Address' section with a 'New' button circled in red. The 'New' button is located above a table with columns 'Type', 'Handle', and 'Domain'. The table currently shows 'No Records found'. Below the table, the 'Type' is set to 'Avaya SIP', and the 'Fully Qualified Address' is '66991' with a domain of 'dr220.com'. The 'Add' button is circled in red.

Scroll down to check and expand **Session Manager Profile**. For **Primary Session Manager**, **Origination Sequence**, **Termination Sequence**, and **Home Location**, select the values corresponding to the applicable Session Manager and Communication Manager. Retain the default values in the remaining fields.

Communication Address

New
Edit
Delete

Type	Handle	Domain
Avaya SIP	66991	dr220.com

Select : All, None

☒ **Session Manager Profile**

SIP Registration

* Primary Session Manager
DR220-SMW

Secondary Session Manager
(None)

Survivability Server
(None)

Max. Simultaneous Devices
1

Block New Registration When Maximum Registrations Active?
☐

Primary	Secondary	Maximum
3	0	3

Application Sequences

Origination Sequence
DR220-CMW-APP-Sequence

Termination Sequence
DR220-CMW-APP-Sequence

Call Routing Settings

* Home Location
DR-2C220

Conference Factory Set
(None)

Call History Settings

Enable Centralized Call History?
☐

☐ **Collaboration Environment Profile**

☐ **CM Endpoint Profile**

Scroll down to check and expand **CM Endpoint Profile**. For **System**, select the value corresponding to the applicable Communication Manager. For **Extension**, click and select the SIP user extension from **Section 7.2.1**. For **Template**, select “9620SIP_DEFAULT_CM_6_3”. Retain the default values in the remaining fields.

Click **Endpoint Editor**, as shown below.

The screenshot shows a web interface for configuring a CM Endpoint Profile. The 'Collaboration Environment Profile' section is expanded, showing the 'CM Endpoint Profile' configuration. The 'System' is set to 'DR220-CMW-ES', 'Profile Type' is 'Endpoint', and 'Extension' is '66991'. The 'Template' is '9620SIP_DEFAULT_CM_6_3'. The 'Set Type' is '9620SIP'. The 'Security Code' is empty. The 'Port' is 'IP'. The 'Voice Mail Number' is empty. The 'Preferred Handle' is '(None)'. The 'Enhanced Callr-Info display for 1-line phones' checkbox is unchecked. The 'Delete Endpoint on Unassign of Endpoint from User or on Delete User' checkbox is checked. The 'Override Endpoint Name and Localized Name' checkbox is checked. The 'Endpoint Editor' button is circled in red.

☐ Collaboration Environment Profile ▶

☒ CM Endpoint Profile ▼

* System

* Profile Type

Use Existing Endpoints ☐

* Extension **Endpoint Editor**

Template

Set Type

Security Code

Port

Voice Mail Number

Preferred Handle

Enhanced Callr-Info display for 1-line phones ☐

Delete Endpoint on Unassign of Endpoint from User or on Delete User. ☒

Override Endpoint Name and Localized Name ☒

☐ CS 1000 Endpoint Profile ▶

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

Repeat **Section 7.2** to add the desired number of SIP users. In the compliance testing, two SIP users with extensions “66991” and “66992” were created.

AVAYA
Aura® System Manager 6.3

Last Logged on at October 14, 2014 12:31 PM
Go to... Log off admin

Home Session Manager x User Management x

Home / Users / User Management / Manage Users

Edit Endpoint

Done Cancel [Save As Template]

System DR220-CMW-ES Extension 66991

Template 9620SIP_DEFAULT_CM_6_3 Set Type 9620SIP

Port 500007 Security Code

Name 65991, IVR

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

Button Assignment (B) Group Membership (M)

* Class of Restriction (COR) 1 * Class Of Service (COS) 1

* Emergency Location Ext 66991 * Message Lamp Ext. 66991

* Tenant Number 1

* SIP Trunk Qaar Type of 3PCC Enabled Avaya

Coverage Path 1 Coverage Path 2

Lock Message Localized Display Name 65991, IVR

Multibyte Language Not Applicable

*Required

Done Cancel

8. Configure BBX Vuesion Multichannel Contact Center

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

- Launch Vuesion Manager
- Administer communication setup
- Administer Switch.txt
- Start services
- Administer VMAIL extensions
- Administer local extensions
- Administer ACD members
- Administer ACD groups
- Administer tenants
- Restart services

The configuration of Vuesion server is typically performed by BBX technicians. The procedural steps are presented in these Application Notes for informational purposes. In addition to the shown procedural steps, the application requires the auto attendant and class of service for agents and supervisors be configured by following reference [2].

8.1. Launch Vuesion Manager

From the Vuesion server, double-click the **VuesionManager.exe** icon, which was created as part of installation.



8.2. Administer Communication Setup

The **Vuesion Manager** screen is displayed. Select **Switch Setup** → **Communication Setup** from the top menu.



The **COMMUNICATION SETTINGS** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **PBX IP Addr:** The applicable domain name from **Section 3**.
- **Password:** The Vuesion user credential from **Section 6.7**.
- **Link Name:** The Tlink name from **Section 6.6**.
- **App. UserID:** The Vuesion user credential from **Section 6.7**.
- **This Server IP address:** IP address of the Vuesion server.
- **This Server IP Port:** A unique port number in the range of 62000-62999.
- **IVR Pilot Number:** The IVR Pilot VDN extension from **Section 5.6**.

COMMUNICATION SETTINGS

SWITCH COMMUNICATION INTERFACE

PBX IP Addr: dr220.com Password: ●●●●●●●●

Link Name: AVAYA#S8800#CSTA#AES_125_72

App. Name:

App. UserID: vuesion

NETWORKING SETUP: MASTER SERVER

NetServer IP address:

NetServer IP Port: 65000

Node Index: 0

THIS SERVER DEFINITION

Customer Location Name: Vuesion Aura

This Server IP address: 10.64.101.206

This Server IP Port: 62206

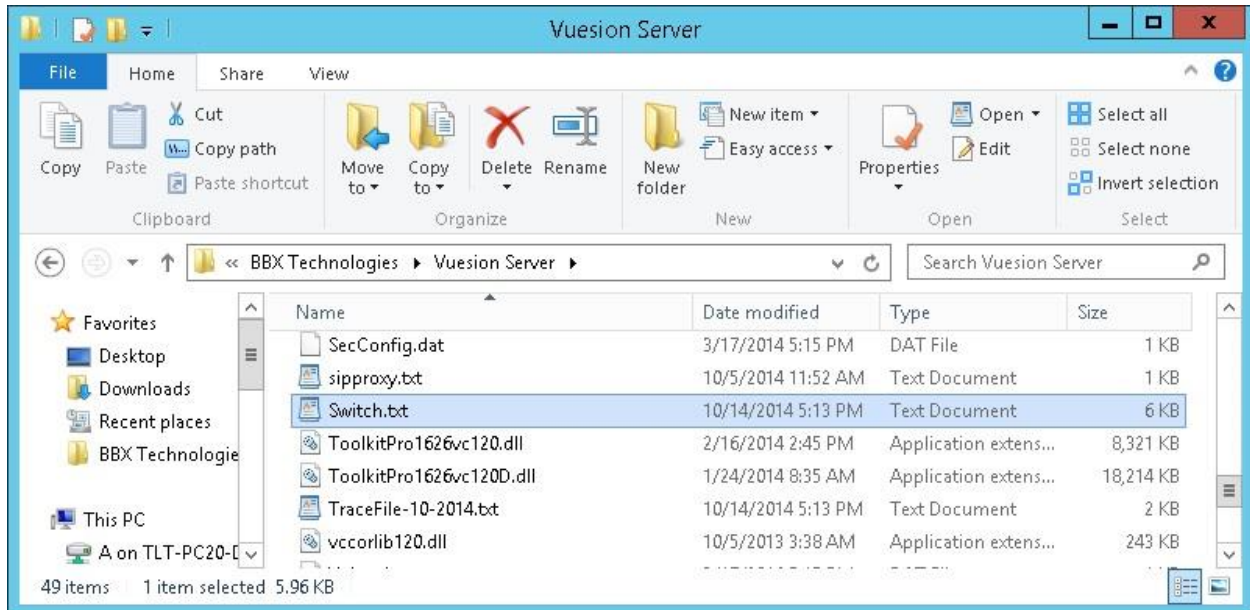
IVR Location: Vuesion Aura

IVR Pilot Number: 65599

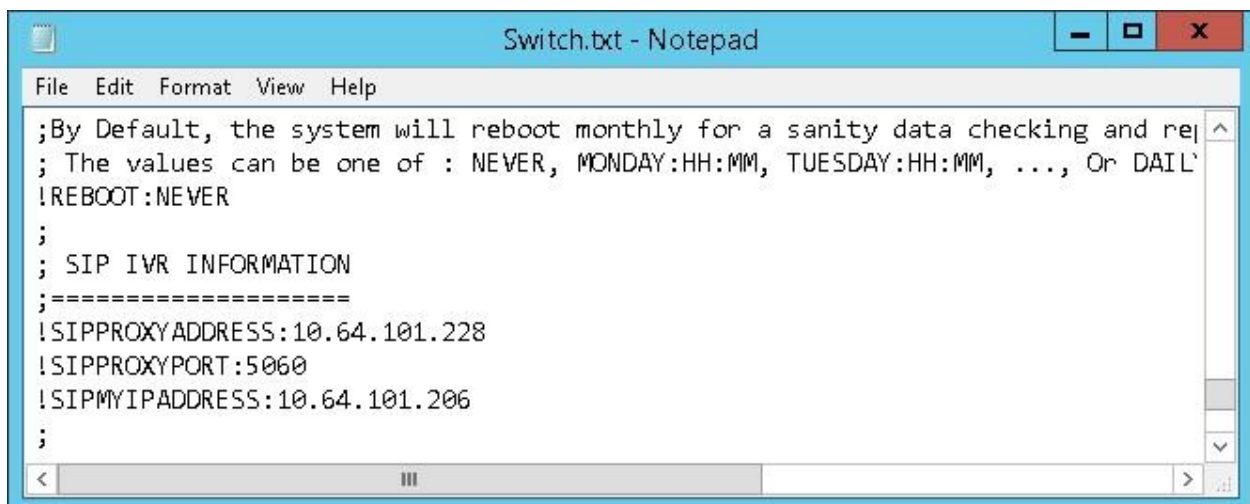
OK

8.3. Administer Switch.txt

From the Vuesion server, navigate to the **C:\Program Files (x86)\BBX Technologies\Vuesion Server** directory to locate the **Switch.txt** file shown below.

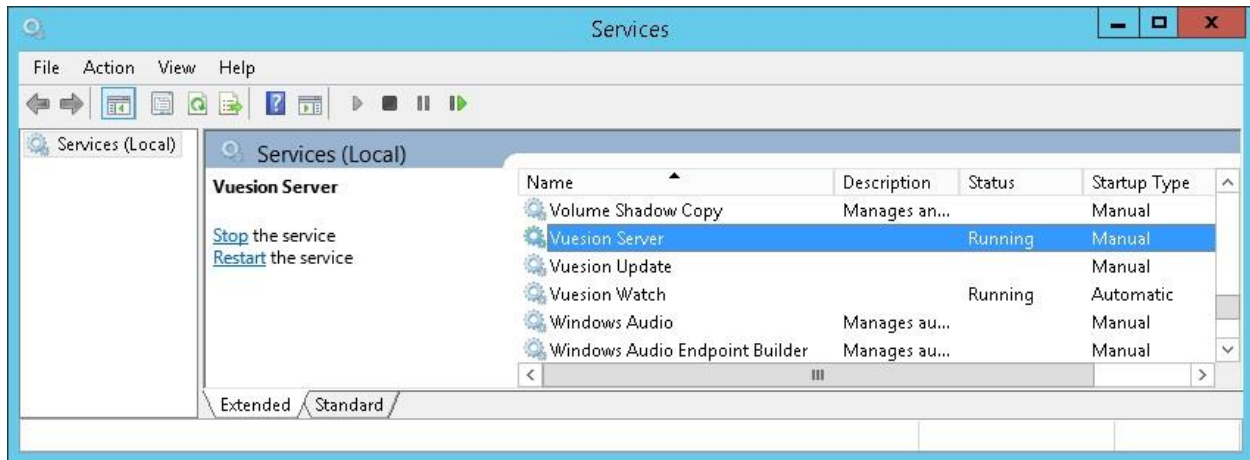


Open the **Switch.txt** file with the Notepad application. Navigate to the **SIP IVR INFORMATION** sub-section. Set **SIPPROXYADDRESS** to the IP address of the Session Manager signaling interface. Set **SIPMYIPADDRESS** to the IP address of the Vuesion server. Retain the default values in the remaining fields.



8.4. Start Services

Select **Start → Control Panel → Administrative Tools → Services**, to display the **Services** screen. Navigate to the **Vuesion Server** entry, right-click on the entry and select **Start**.



8.5. Administer VMAIL Extensions

Follow the procedures in **Section 8.1** to launch Vuesion Manager. From the **Vuesion Manager** screen shown in **Section 8.2**, select **Messaging → VMAIL Extensions** from the top menu, to display the **DIRECTORY CONFIGURATION** screen below.

Follow reference [2] to create an entry for each virtual SIP user from **Section 7.2**. For **FullName**, enter the SIP user name from **Section 7.2.1**. For **Password**, enter the SIP user password from **Section 7.2.2**. Check **SIP IVR**.

Full Name	DN #	Port#
IVR 66991	66991	0
IVR 66992	66992	0

DIRECTORY ASSIGNMENT

Directory #:

FullName:

Title:

PBX:

Account:

Password:

Tenant Name:

Class of Service:

☐ Shared Station ☒ SIP IVR
☐ Virtual/Single Line ☐ Network Advertise
☐ Disable SMDR
☐ Live Record

8.8. Administer ACD Groups

From the **Vuesion Manager** screen shown in **Section 8.2**, select **Contact Center → ACD Groups** from the top menu, to display the **SkillSets Administration** screen. Follow reference [2] to create an entry for each PSTN reachable VDN from **Section 5.6**. Note that the **Queue ID** and **Queue Name** must match the VDN extension and name exactly from **Section 5.6**.

The **Voice Routing Options** sub-section defines parameters used for routing of ACD calls. The **Multichannel Contact Center Members Assignment** sub-section defines the members and their skills level. The **Announcements** sub-section defines the announcement treatments.

The screenshot below shows the values used in the compliance testing.

The screenshot displays the 'SkillSets Administration' window with the following configuration details:

- Queue ID:** 65501, **Queue Name:** BBX Sales, **Parent Group Name:** (empty)
- Enable Schedule:** ☐
- Group Name / ID Table:**

Group Name	ID
BBX Support	65502
BBX Sales	65501
- Voice Routing Options:**
 - ☒ **Enable**, **Priority:** 09, **Longest InQ Thr:** 40s
 - Method:** Skills Based, **Force Priority:** 00
 - Overflow Time:** 25s, **Q Threshold:** 04
 - Overflow Destination:** (empty), **Abandon Filter:** 05s
 - Signed-Out Overflow:** (empty), **Abandon Thr:** 30
 - All Busy Overflow:** (empty), ☒ **Auto/Manual Wrap** 02s
 - Advance Time:** 10s, ☐ **Auto Logout** 11:50:00 PM
- Email Routing Options:**
 - ☐ **Enable**, **Priority:** 00
 - Subject Filter:** (empty)
 - Overflow Time:** 00
 - OVF Destination:** (empty)
 - Signed-Out OVF:** (empty)
 - EmailQ Threshold:** 10
 - Longest InQ Thr:** 300
 - Force Priority:** 0
- Announcements:**

	AA	75503	QPos.	~ Hold	AA	Once	Never
1:	AA	75503	QPos.	~ Hold	AA	Once	Never
2:	AA		QPos.	~ Hold	AA	Repea	Never
3:	AA		QPos.	~ Hold	AA	Repea	Never
- Webchat Routing Options:**
 - ☐ **Enable**, **Priority:** 00
 - Q Threshold:** 4
 - Longest InQ Thr:** 60
 - Force Priority:** 0
- Multichannel Contact Center Members Assignment:**

Voice Skill	Email Skill	Outdial Skill	Webchat Skill	SMS Skill
00	00	00	00	00

Name	ID	Type	Skill
BBX Agent 1	75001	ACD Agent	09
BBX Agent 2	75002	ACD Agent	09
BBX Supervisor	75000	ACD Supervisor	00
- SMS Routing Options:**
 - ☐ **Enable**, **Priority:** 00
 - Q Threshold:** 4
 - Longest InQ Thr:** 60
 - Force Priority:** 0
- Outbound Campaign:** Outdial Campaign OFF
- Buttons:** Add, Remove, Refresh Scripts, Save, Exit

8.9. Administer Tenants

From the **Vuesion Manager** screen shown in **Section 8.2**, select **Messaging → Tenants** from the top menu, to display the **TENANTS/GROUPS** screen.

Follow reference [2] to create an entry for the Tenant VDN from **Section 5.6**. For **Name**, enter the Tenant VDN name from **Section 5.6**. For **ID** and **Password**, enter the Tenant VDN extension, and a desired 4-digits password respectively. Retain the default values in the remaining fields, and click **Edit Members** toward the bottom of the screen (not shown below).

Tenants/Groups		
Name	ID	Pwd
BBX Tenant	65500	6550

Tenant/Group Definition
Name:
ID: Password:
Taxes: %
Discount: %
Long Distance Call Charges: First Minute Add. Minute
International Call Charges: First Minute Add. Minute
☐ Cost Incoming Calls

The **Selected Tenant** screen is displayed next. Select entries associated with agents, supervisors, and PSTN reachable VDNs from the **Available User List** and move to the **Tenant/Group Members List**, as shown below.

Tenant/Group Members List	
Member Name	Member Ext
BBX Agent 1	65001
BBX Agent 2	65002
BBX Sales	65501
BBX Supervisor	65000
BBX Support	65502

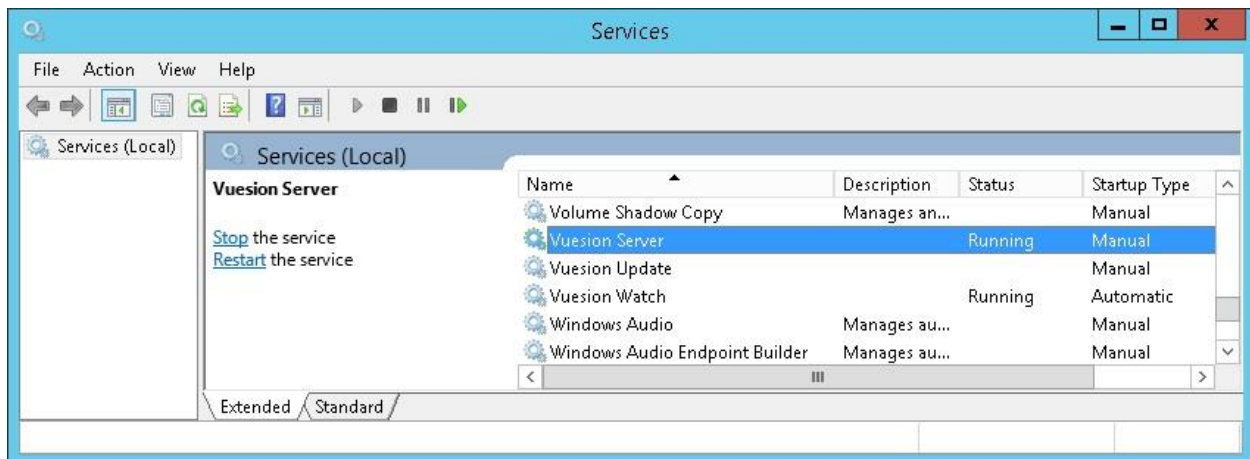
<<--
-->>

Available Users List	
Member Name	Member Ext

8.10. Start Services

Select **Start → Control Panel → Administrative Tools → Services**, to display the **Services** screen. Stop the **Vuesion Watch** service, followed by **Vuesion Server**.

After both services are stopped, start the **Vuesion Server** service, which will automatically start the **Vuesion Watch** service.



9. Verification Steps

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

9.1. Verify Avaya Aura® Communication Manager


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

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
2	6	no	aes_125_72	established	47	22

9.2. 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 total number of monitored VDN and station extensions from **Section 3**.



Application Enablement Services Management Console

Welcome: User
Last login: Wed Oct 15 13:48:13 2014 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: 6.3.3.0.10-0
Server Date and Time: Thu Oct 16 07:19:39 MDT 2014
HA Status: Not Configured

Status | Status and Control | TSAPI Service Summary

Home | Help | Logout

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Log Manager

Logs

Status and Control

CVLAN Service Summary

DLG Services Summary

DMCC Service Summary

Switch Conn Summary

TSAPI Service Summary

TSAPI Link Details

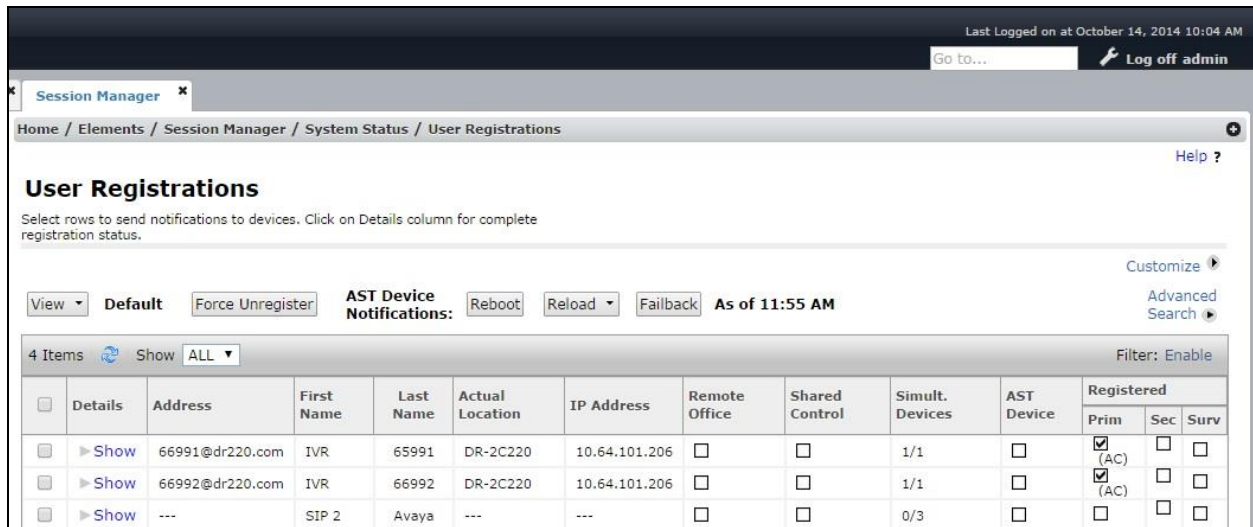
☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	S8800	2	Talking	Fri Sep 26 09:57:29 2014	Online	16	9	22	47	30
<input type="radio"/>	2	S8300D	1	Switch Down	Fri Aug 29 09:00:02 2014	Online	16	0	0	0	30

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

9.3. Verify Avaya Aura® Session Manager

From the System Manager Web interface, select **Elements → Session Manager → System Status → User Registrations** to display the **User Registrations** screen. Verify that all SIP users from **Section 7.2** are registered, as shown below with a check in the **Registered Prim** column.



Session Manager

Home / Elements / Session Manager / System Status / User Registrations

User Registrations

Select rows to send notifications to devices. Click on Details column for complete registration status.

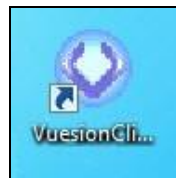
View: Default Force Unregister AST Device Notifications: Reboot Reload Failback As of 11:55 AM

4 Items Show ALL Filter: Enable

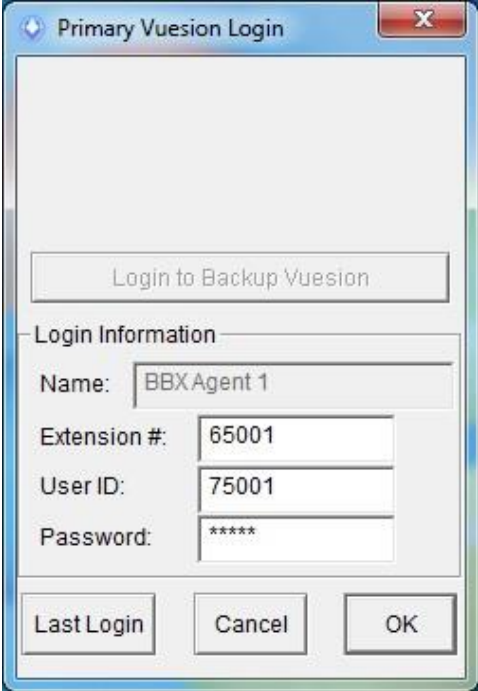
	Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered		
											Prim	Sec	Surv
<input type="checkbox"/>	Show	66991@dr220.com	IVR	65991	DR-2C220	10.64.101.206	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	66992@dr220.com	IVR	66992	DR-2C220	10.64.101.206	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	SIP 2	Avaya	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

9.4. Verify BBX Vuesion Multichannel Contact Center

From the agent user PC running Vuesion Client, double-click on the **VuesionClient.exe** icon shown on the desktop, which was created as part of installation.

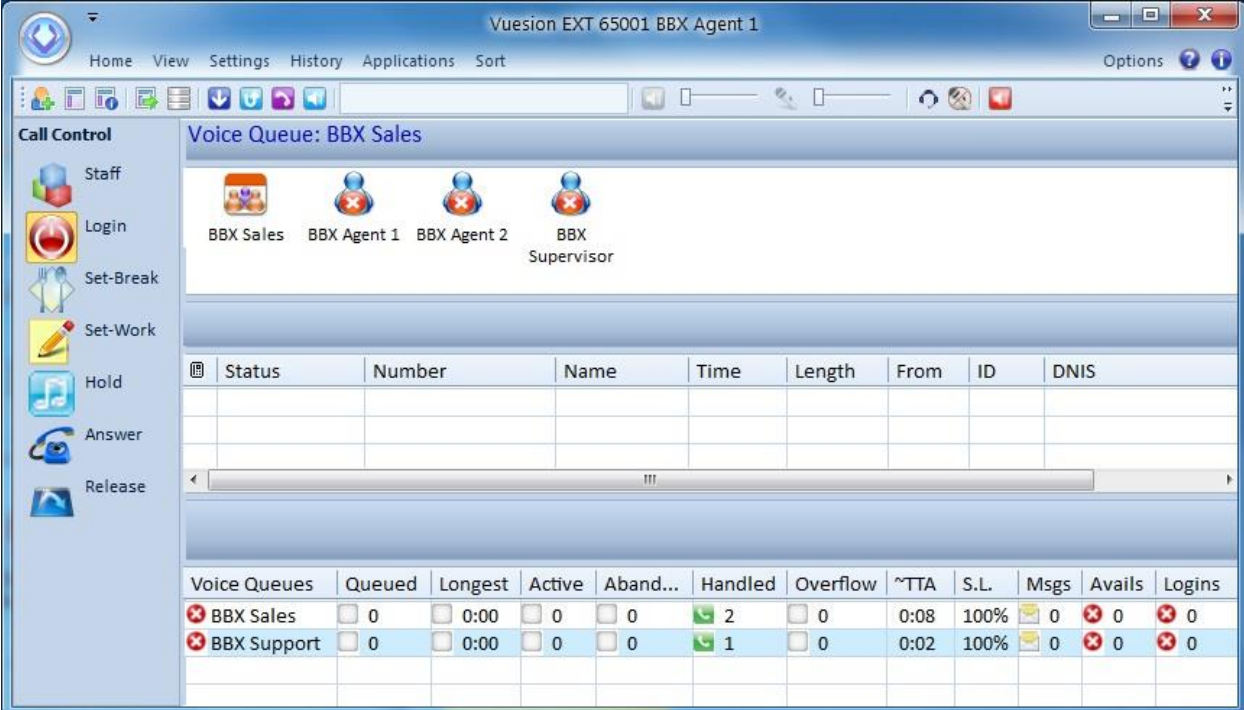


The **Primary Vuesion Login** screen is displayed. Log in using an appropriate agent credentials from **Section 8.7**. For **Extension #**, enter the relevant agent station extension, in this case “65001”.



The image shows a 'Primary Vuesion Login' dialog box. It has a title bar with a close button. Below the title bar is a large empty rectangular area. Underneath that is a button labeled 'Login to Backup Vuesion'. Below the button is a section titled 'Login Information'. This section contains four input fields: 'Name' with the text 'BBX Agent 1', 'Extension #' with the text '65001', 'User ID' with the text '75001', and 'Password' with the text '*****'. At the bottom of the dialog are three buttons: 'Last Login', 'Cancel', and 'OK'.

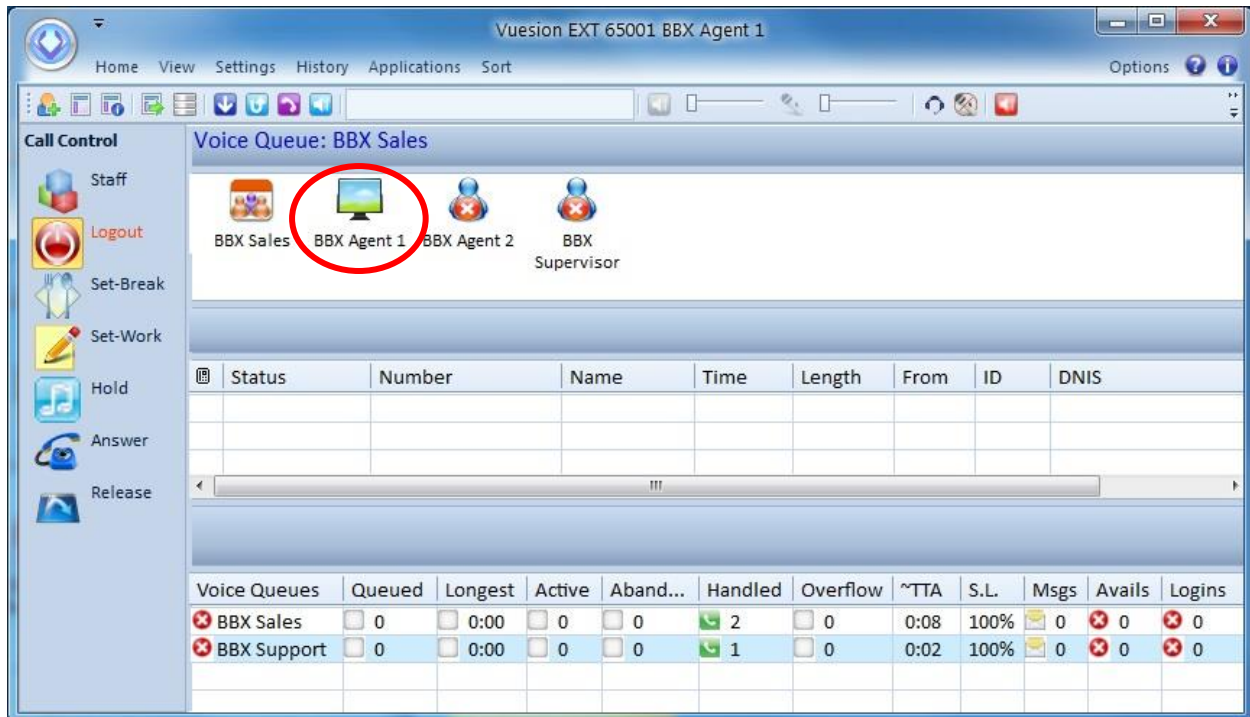
The **Vuesion** screen below is displayed. Click on the **Login** icon from the left pane.



The image shows the 'Vuesion EXT 65001 BBX Agent 1' interface. The title bar includes the application name and standard window controls. The menu bar contains 'Home', 'View', 'Settings', 'History', 'Applications', 'Sort', and 'Options'. The left pane, titled 'Call Control', contains icons for 'Staff', 'Login', 'Set-Break', 'Set-Work', 'Hold', 'Answer', and 'Release'. The main area is titled 'Voice Queue: BBX Sales' and displays four agent icons: 'BBX Sales', 'BBX Agent 1', 'BBX Agent 2', and 'BBX Supervisor'. Below the icons is a table with columns: Status, Number, Name, Time, Length, From, ID, and DNIS. At the bottom of the interface is a summary table with columns: Voice Queues, Queued, Longest, Active, Aband..., Handled, Overflow, ~TTA, S.L., Msgs, Avails, and Logins.

Voice Queues	Queued	Longest	Active	Aband...	Handled	Overflow	~TTA	S.L.	Msgs	Avails	Logins
BBX Sales	0	0:00	0	0	2	0	0:08	100%	0	0	0
BBX Support	0	0:00	0	0	1	0	0:02	100%	0	0	0

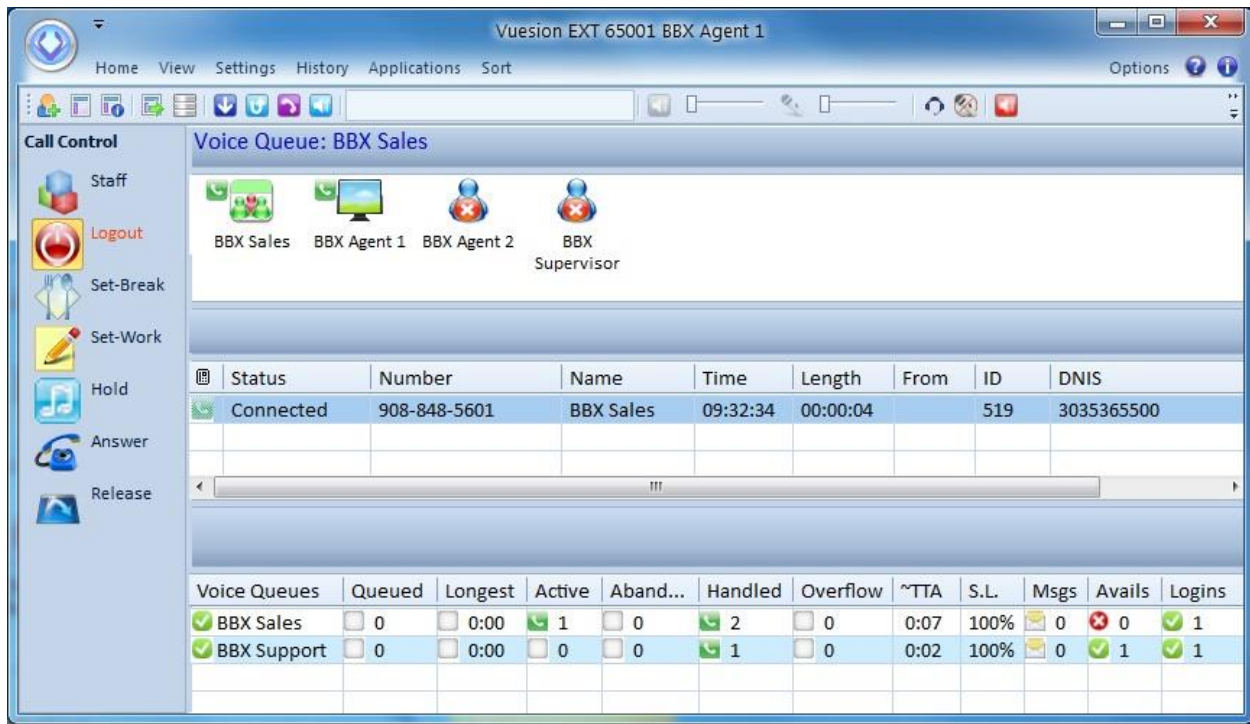
Verify the applicable agent icon is updated in the right pane, as shown below.



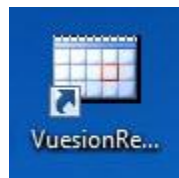
Make an incoming ACD call from the PSTN to the Sales VDN, and verify that the agent screen is updated to reflect a ringing call, as shown below. Also verify that the entry shown in the middle right pane reflects proper information for the call. Click on the **Answer** icon in the left pane to answer the call.



Verify the agent telephone is connected to the caller with two-way talk paths, and that the agent screen is updated to reflect the call being connected, as shown below. Click on the **Release** icon in the left pane to complete the call.



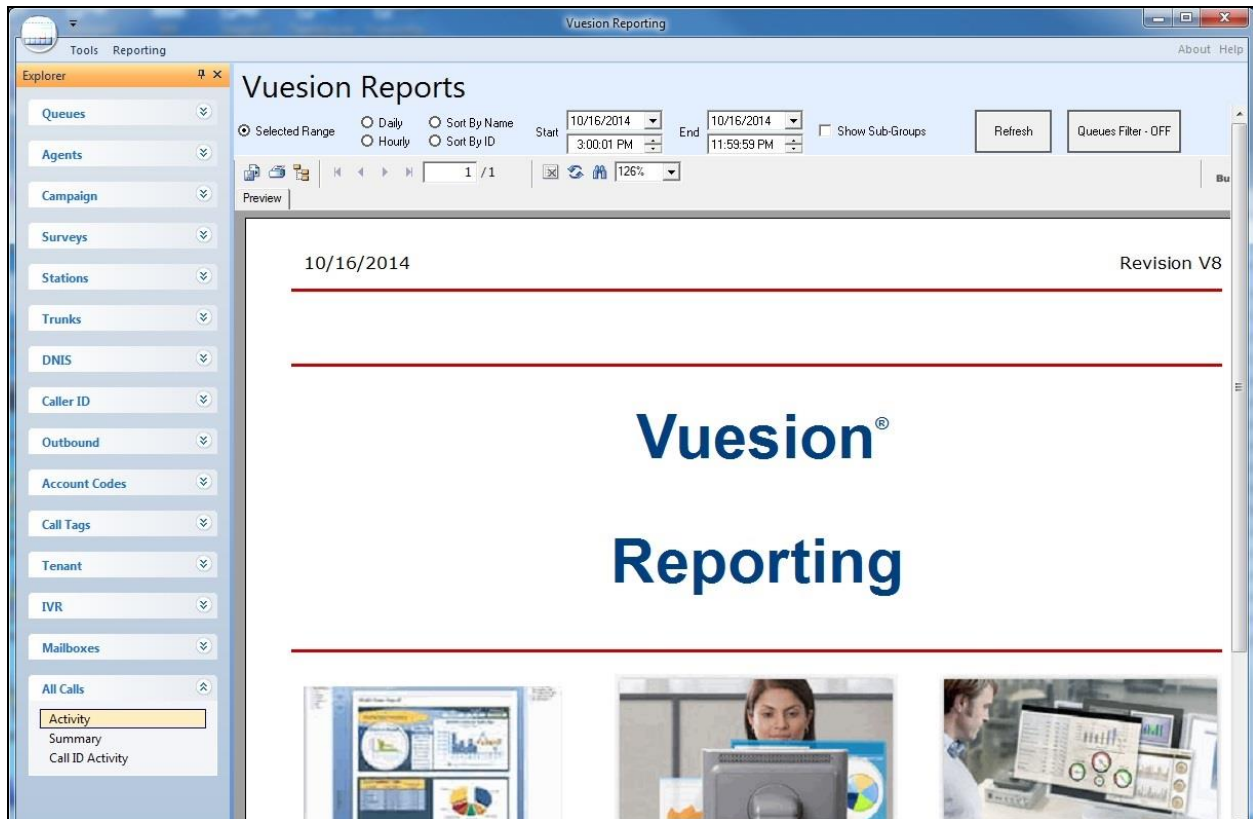
From the supervisor PC running Vuesion Reports, double-click on the **VuesionReports.exe** icon shown on the desktop, which was created as part of installation. In the compliance testing, Vuesion Reports was running on the supervisor PC.



The **Vuesion Reporting** screen is displayed. For **Server IP/Name**, enter the IP address of the Vuesion server. For **TCP/Port**, enter the Vuesion server IP port from **Section 8.2**. For **Supervisor ID** and **Password**, enter the applicable credentials for the supervisor from **Section 8.7**, as shown below.

The **Vuesion Reporting** screen below is displayed. Retain the default values, and click **View Reports** to view reports for the current day.

The **Vuesion Reporting** screen is updated. Select **All Calls** → **Activity** from the left pane.



The **Vuesion Reporting** screen is updated with the **Call Detail Activity** report. Verify that there are entries reflecting the last call with proper information, as shown below.

Date / Time	Ext.	Name	Call Type	ANI / Number Dialed	Name	Call Duration	DNIS	Call ID
10/16/2014								
14:33:04	66991	IVR 66991	Inbound	908.848.5601		00:00:00	303.536.5501	730
14:33:04	65001	BBX Agent 1	Start Ring	908.848.5601		00:00:00	303.536.5501	732
14:33:09	65001	BBX Agent 1	Start Inbound	908.848.5601		00:00:00	303.536.5501	732
14:34:14	65001	BBX Agent 1	CC Inbound	908.848.5601		00:01:04	303.536.5501	732

10. Conclusion

These Application Notes describe the configuration steps required for BBX Vuesion Multichannel Contact Center to successfully interoperate with Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services, and Avaya Aura® Session Manager. All feature and serviceability test cases were completed with an observation noted in **Section 2.2**.

11. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 10, Release 6.3, June 2014, available at <http://support.avaya.com>.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3, 02-300357, June 2014, available at <http://support.avaya.com>.
3. *Administering Avaya Aura® Session Manager*, Release 6.3, Issue 3, October 2013, available at <http://support.avaya.com>.
4. *Vuesion Application Server Contact Center Configuration Guide*, 01/2014 Release V9, available upon request to BBX Support.

©2014 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.