



Avaya Solution & Interoperability Test Lab

Application Notes for Computer Instruments e-IVR with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP Users – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Computer Instruments e-IVR to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP users. Computer Instruments e-IVR is an IVR development platform that includes a number of self-service IVR and Web applications.

In the compliance testing, Computer Instruments e-IVR used SIP users to Avaya Aura® Session Manager to support inbound and outbound IVR applications.

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 Computer Instruments e-IVR to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP users. Computer Instruments e-IVR is an IVR development platform that includes a number of self-service IVR and Web applications.

In the compliance testing, Computer Instruments e-IVR used SIP users to Avaya Aura® Session Manager to support inbound and outbound IVR applications. The SIP users were registered to Avaya Aura® Session Manager.

The Computer Instruments e-IVR server used in the testing included the Dialogic Host Media Processing Software for support of SIP protocol.

2. General Test Approach and Test Results

The feature test cases were performed manually. The e-IVR inbound application was tested by manually placing calls from users on the PSTN and on Communication Manager to the e-IVR inbound application. The associated e-IVR inbound application played greeting announcements and collected DTMF input from the caller to decide on the feature to provide, such as transfer to internal or external destinations.

The e-IVR outbound application was tested by manually requesting callbacks to users on the PSTN and on Communication Manager. The callback requests were initiated from the Web page associated with the e-IVR outbound application.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet connection to e-IVR.

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 included registration, G.711MU, codec negotiation, media shuffling, session refresh, hold/reconnect, inbound DTMF, invalid number, busy destination, and outgoing call screening.

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

2.2. Test Results

All test cases were executed and passed.

2.3. Support

Technical support on e-IVR can be obtained through the following:

- **Phone:** (888) 451-0851
- **Email:** support@instruments.com

3. Reference Configuration

As shown in **Figure 1**, SIP users were used between e-IVR and Session Manager, and the applicable domain name used was “br110.com”.

The configuration of Session Manager is performed via the web interface of System Manager. The detailed administration of basic connectivity between Communication Manager, System Manager, Session Manager, and routing of SIP user extensions is not the focus of these Application Notes and will not be described.

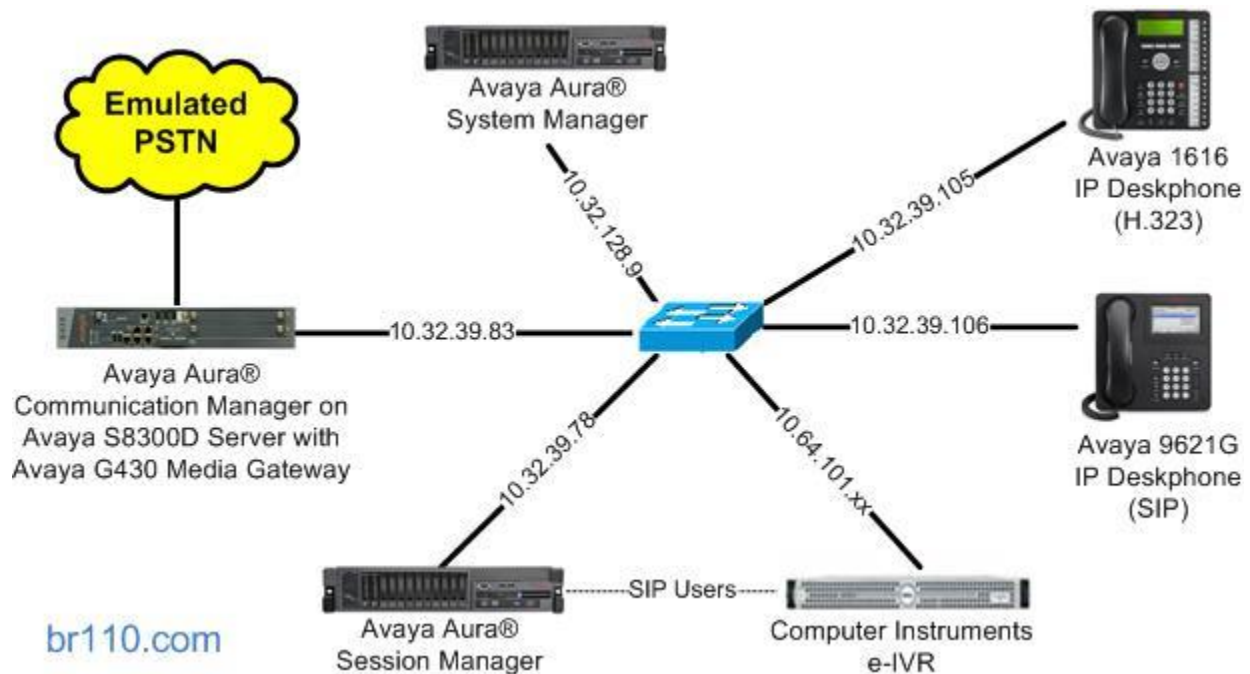


Figure 1: Compliance Testing Configuration

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 | 6.3.5 (R016x.03.0.124.0-21460) 6.3.5 (35.8.0) |
| Avaya Aura® Session Manager | 6.3.7 |
| Avaya Aura® System Manager | 6.3.5 |
| Avaya 1616 IP Deskphone (H.323) | 1.350B |
| Avaya 9621G IP Deskphone (SIP) | 6.3.1.22 |
| Computer Instruments e-IVR on Windows Server 2012 <ul style="list-style-type: none">eIVRMenuAPI.dlleIVRMenuVA.dllDialogic Host Media Processing Software | 5.0.0 1.0.0.35 1.0.0.89 3.0 Service Update 349 |

5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer IP codec set
- Administer hunt group

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: 6400 | | 158 |
| Maximum Stations: 2400 | | 19 |
| Maximum XMOBILE Stations: 2400 | | 0 |
| Maximum Off-PBX Telephones - EC500: 9600 | | 1 |
| Maximum Off-PBX Telephones - OPS: 9600 | | 9 |
| Maximum Off-PBX Telephones - PBFMC: 9600 | | 0 |

5.2. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is the codec set number used by the existing SIP trunk to Session Manager. Update the audio codec types in the **Audio Codec** fields as necessary to include G.711. Note that e-IVR only supports the G.711 codec variant.

change ip-codec-set 1

Page1 of 2

IP Codec Set

Codec Set: 3

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

5.3. Administer Hunt Group

Proceed to **Section 6** to configure Session Manager. After the new SIP users for use by e-IVR have been added in Session Manager, return to this section to configure a hunt group for routing of calls to the e-IVR inbound application.

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.

| | | | |
|---------------------------|--|----------------------------|--|
| add hunt-group 46 | | Page 1 of 60 | |
| HUNT GROUP | | | |
| Group Number: 46 | | ACD? n | |
| Group Name: e-IVR Inbound | | Queue? n | |
| Group Extension: 46000 | | Vector? n | |
| Group Type: ucd-mia | | 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 the SIP user extensions from **Section 6.2** that are associated with the e-IVR inbound application, as shown below.

| | | | | |
|--------------------------------|---------------------|--------------------------------------|--------------|---------------------|
| add hunt-group 46 | | | Page 3 of 60 | |
| HUNT GROUP | | | | |
| Group Number: 46 | | Group Extension: 46000 | | Group Type: ucd-mia |
| 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: 46101 | | | 14: | |
| 2: 46102 | | | 15: | |
| 3: | | | 16: | |

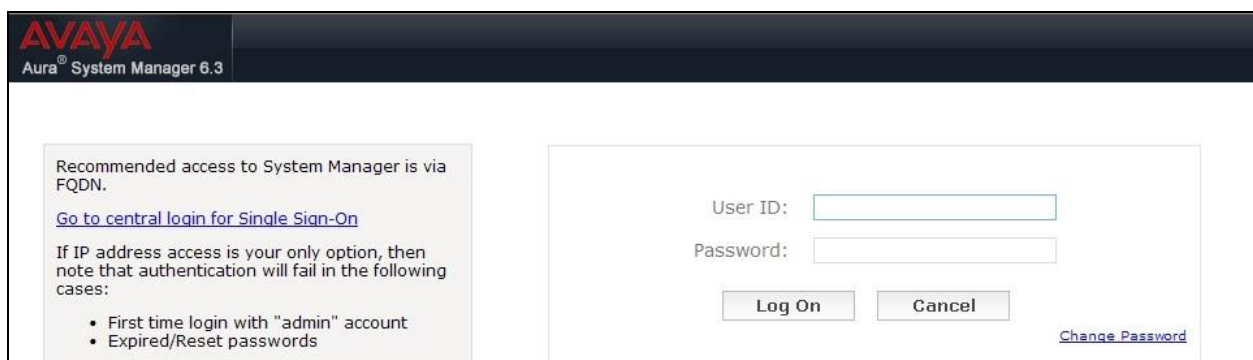
6. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer users

6.1. Launch System Manager

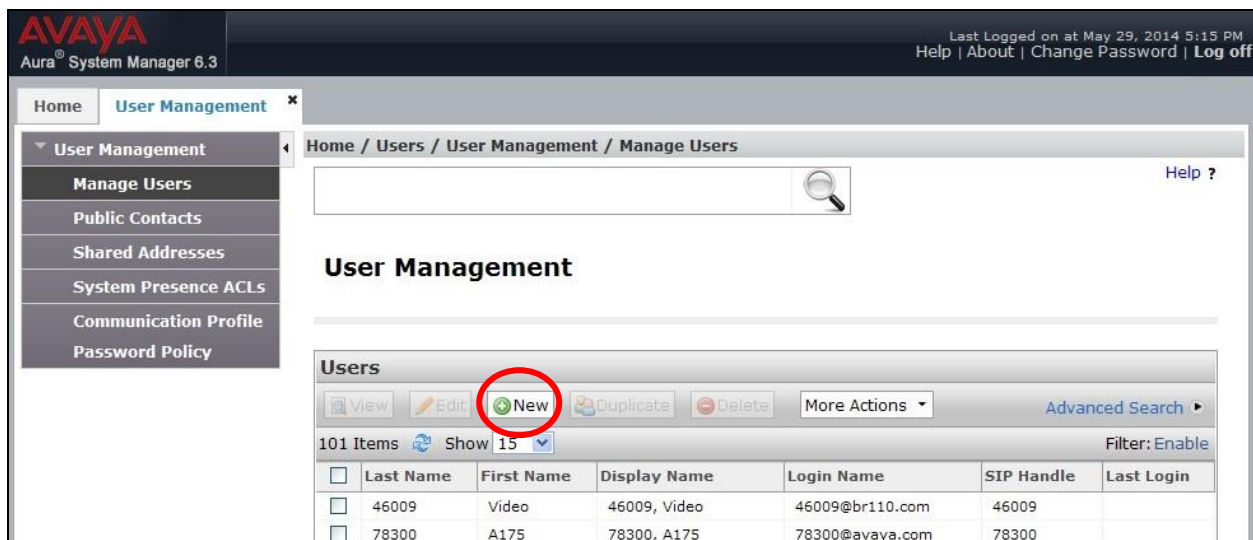
Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.



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.

6.2. 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" and "User Management". The left sidebar lists "User Management", "Manage Users", "Public Contacts", "Shared Addresses", "System Presence ACLs", "Communication Profile", and "Password Policy". The main content area shows the "User Management" title and a "Users" table. The "Users" table has a toolbar with buttons for "View", "Edit", "New" (circled in red), "Duplicate", "Delete", and "More Actions". Below the toolbar, it says "101 Items" and "Show 15". The table has columns for "Last Name", "First Name", "Display Name", "Login Name", "SIP Handle", and "Last Login". The table contains two rows of data: one for "46009 Video" and one for "78300 A175".

| | Last Name | First Name | Display Name | Login Name | SIP Handle | Last Login |
|--------------------------|-----------|------------|--------------|-----------------|------------|------------|
| <input type="checkbox"/> | 46009 | Video | 46009, Video | 46009@br110.com | 46009 | |
| <input type="checkbox"/> | 78300 | A175 | 78300, A175 | 78300@avaya.com | 78300 | |

6.2.1. Identity

The **New User Profile** screen is displayed. Enter desired **Last Name** and **First Name**. For **Login Name**, enter “n@x”, where “n” is the desired user extension and “x” 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 header indicates 'Last Logged on at May 29, 2014 5:15 PM' and provides links for 'Help', 'About', 'Change Password', and 'Log off'. The left sidebar contains a 'User Management' menu with options: 'Manage Users', 'Public Contacts', 'Shared Addresses', 'System Presence ACLs', 'Communication Profile', and 'Password Policy'. The main content area is titled 'New User Profile' and includes a breadcrumb trail: 'Home / Users / User Management / Manage Users'. There are three buttons at the top right: 'Commit & Continue', 'Commit', and 'Cancel'. Below these are four tabs: 'Identity' (marked with a red asterisk), 'Communication Profile', 'Membership', and 'Contacts'. The 'Identity' tab is selected, showing a 'User Provisioning Rule' dropdown and an 'Identity' section with the following fields:

- * Last Name: CI
- Last Name (Latin Translation): CI
- * First Name: eIVR Inb-1
- First Name (Latin Translation): eIVR Inb-1
- Middle Name: (empty)
- Description: (empty)
- * Login Name: 46101@br110.com
- * Authentication Type: Basic
- Password: (empty)
- Confirm Password: (empty)

6.2.2. Communication Profile

Select the **Communication Profile** tab. For **Communication Profile Password** and **Confirm Password**, enter the desired password for the SIP user to use for registration.

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 6.2.1**. Click **Add**.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The top navigation bar includes 'Home', 'User Management', and a breadcrumb trail: 'Home / Users / User Management / Manage Users'. The left sidebar lists various management options, with 'Communication Profile Password Policy' selected. The main content area is titled 'New User Profile' and contains several tabs: 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active, displaying fields for 'Communication Profile Password' and 'Confirm Password'. Below these fields are buttons for 'New', 'Delete', 'Done', and 'Cancel'. The 'Name' section shows 'Primary' as the selected name. The 'Communication Address' section is expanded, showing a table with columns 'Type', 'Handle', and 'Domain'. The 'New' button in this section is circled in red. Below the table, the 'Type' is set to 'Avaya SIP', and the 'Fully Qualified Address' is '46101@br110.com'. The 'Add' button is also circled in red. At the bottom, there is a checkbox for 'Session Manager Profile'.

Scroll down to check and expand **Session Manager Profile**. For **Primary Session Manager**, **Origination Application Sequence**, **Termination Application 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

| <input type="checkbox"/> | Type | Handle | Domain |
|--------------------------|-----------|--------|-----------|
| <input type="checkbox"/> | Avaya SIP | 46101 | br110.com |

Select : All, None

☒ **Session Manager Profile**

SIP Registration

* Primary Session Manager
BR110-SMH

Secondary Session Manager
(None)

Survivability Server
(None)

Max. Simultaneous Devices
1

Block New Registration When Maximum Registrations Active?
☐

| Primary | Secondary | Maximum |
|---------|-----------|---------|
| 7 | 0 | 7 |

Application Sequences

Origination Sequence
BR110-G430-APP-Sequence

Termination Sequence
BR110-G430-APP-Sequence

Call Routing Settings

* Home Location
BR-1C110

Conference Factory Set
(None)

☐ **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 6.2.1**. For **Template**, select “9630SIP_DEFAULT_CM_6_3”. Retain the default values in the remaining fields.

Repeat **Section 6.2** to add the desired number of SIP users, using the same password for all SIP users as required by e-IVR. In the compliance testing, two SIP users with extensions “46101” and “46102” were created for association with one inbound IVR application, and two SIP users with extensions “46201” and “46201” were created for association with two outbound IVR applications.

The screenshot shows a web-based configuration interface for a Collaboration Environment Profile. The 'CM Endpoint Profile' section is expanded, showing various fields for configuring a SIP endpoint. The 'System' is set to 'BR110-G430-ES' and the 'Profile Type' is 'Endpoint'. The 'Extension' is '46101' and the 'Template' is '9630SIP_DEFAULT_CM_6_3'. Other fields like 'Set Type', 'Security Code', 'Port', 'Voice Mail Number', and 'Preferred Handle' are also visible. There are checkboxes for 'Use Existing Endpoints', 'Enhanced Callr-Info display for 1-line phones', 'Delete Endpoint on Unassign of Endpoint from User or on Delete User.', and 'Override Endpoint Name and Localized Name'.

☐ Collaboration Environment Profile ▶

☒ CM Endpoint Profile ▼

* System

* Profile Type

Use Existing Endpoints ☐

* Extension

* 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 ▶

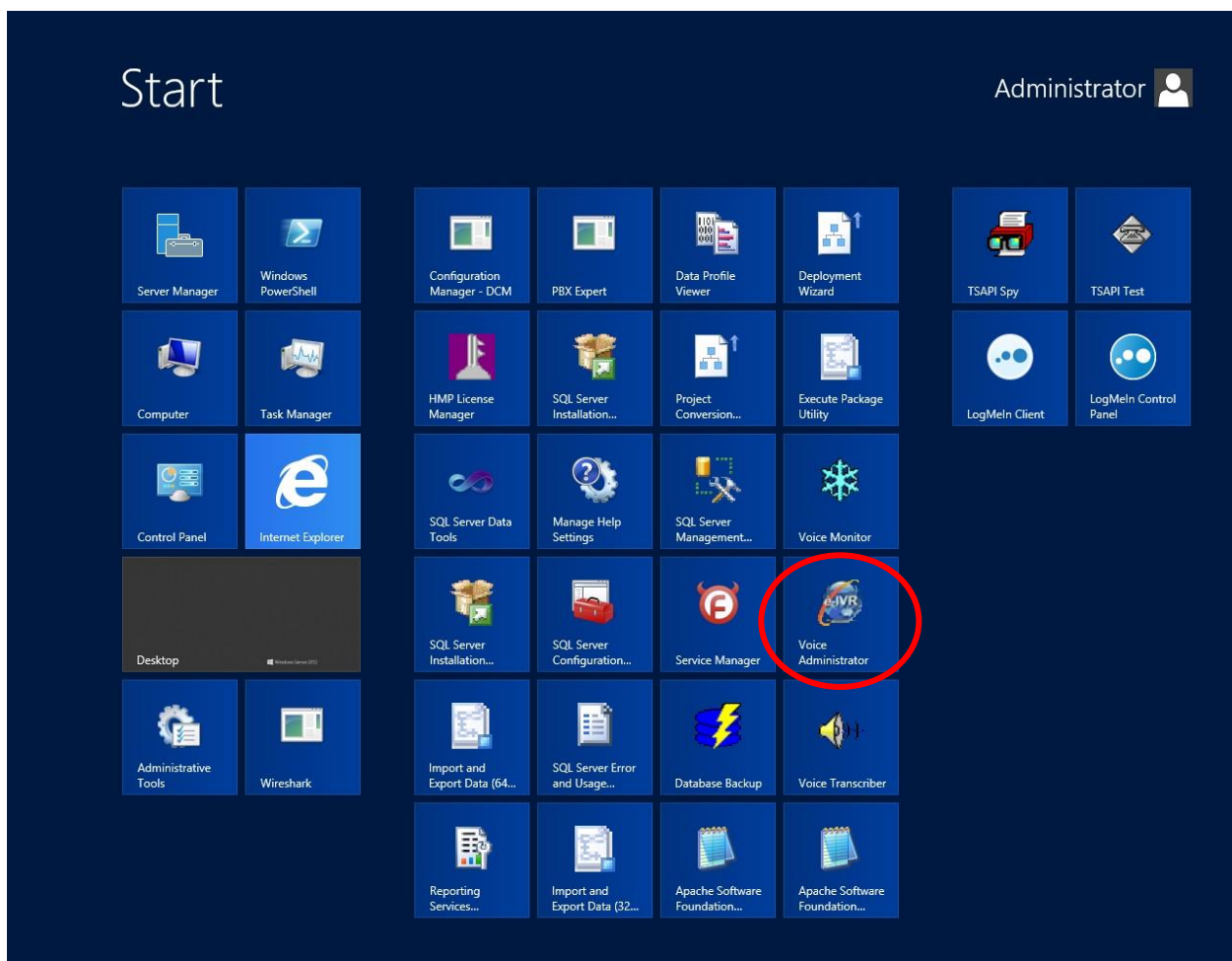
7. Configure Computer Instruments e-IVR

This section provides the procedures for configuring e-IVR. The procedures include the following areas:

- Administer system config
- Administer EIVR.ini
- Restart service

7.1. Administer System Config

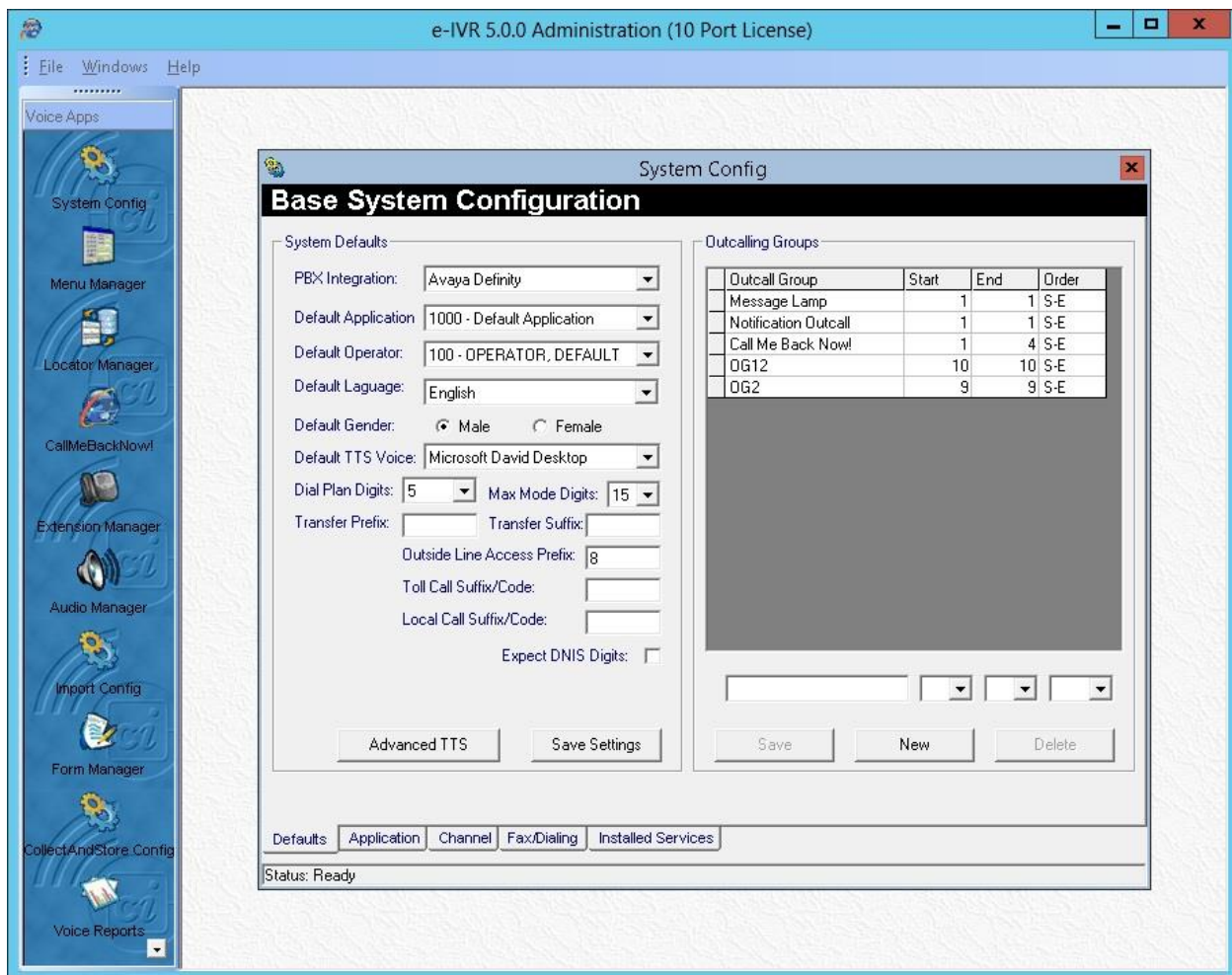
From the e-IVR server, select **Start → Voice Administrator** as shown below.



In the subsequent screen, select **System Config** from the left pane to display the **System Config** pop-up screen shown below.

In the **System Defaults** sub-section, select “Avaya Definity” for **PBX Integration**. For **Dial Plan Digits**, enter the maximum length of internal extensions on Communication Manager. For **Outside Line Access Prefix**, enter the applicable prefix for calls to the PSTN, as required by Communication Manager. For outbound calls to the PSTN, e-IVR will automatically prepend the **Outside Line Access Prefix** value defined below, plus the digit “1”.

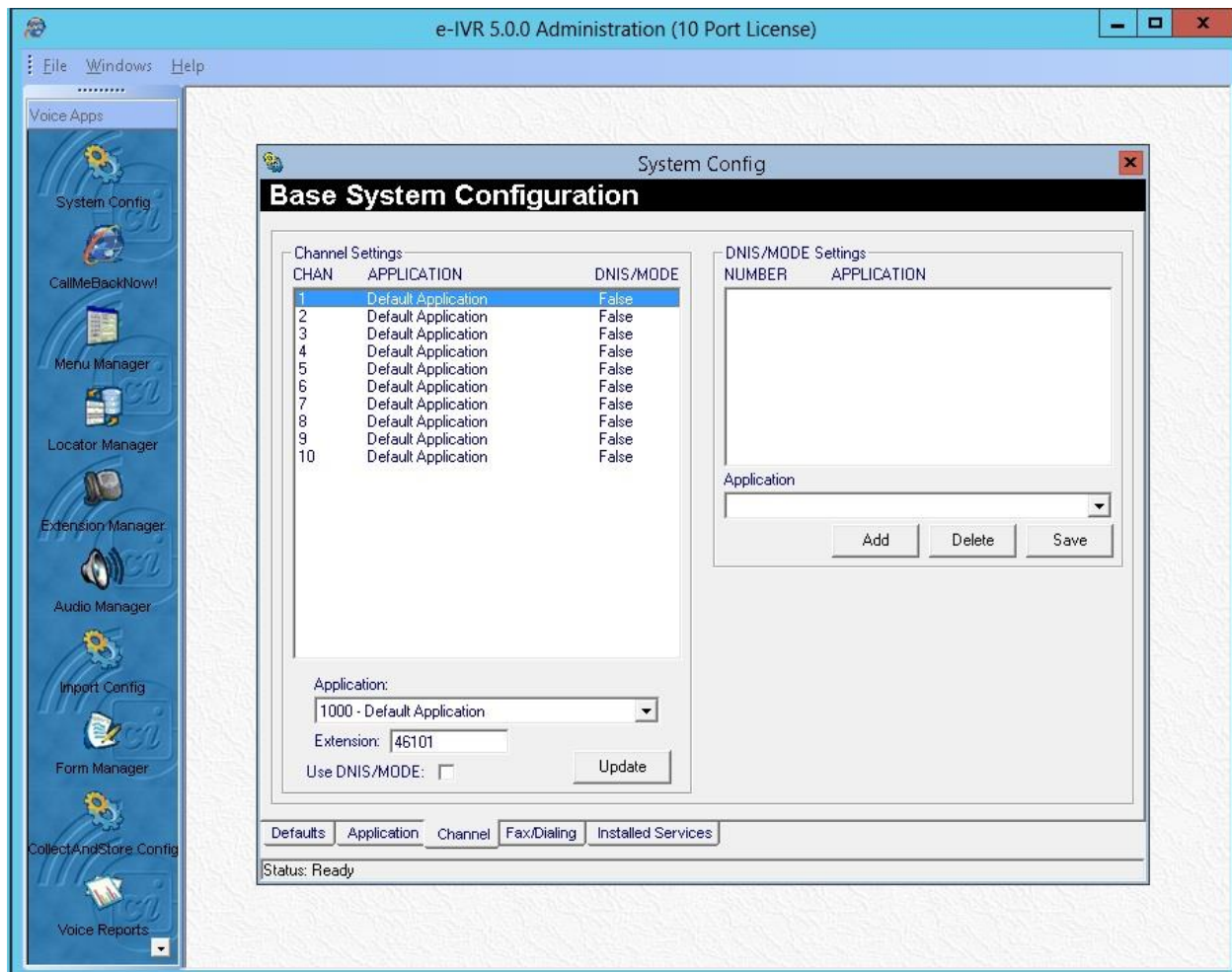
In the **Outcalling Groups** sub-section, the first three groups were the default groups, and the last two groups were pre-configured groups used for testing outbound applications.



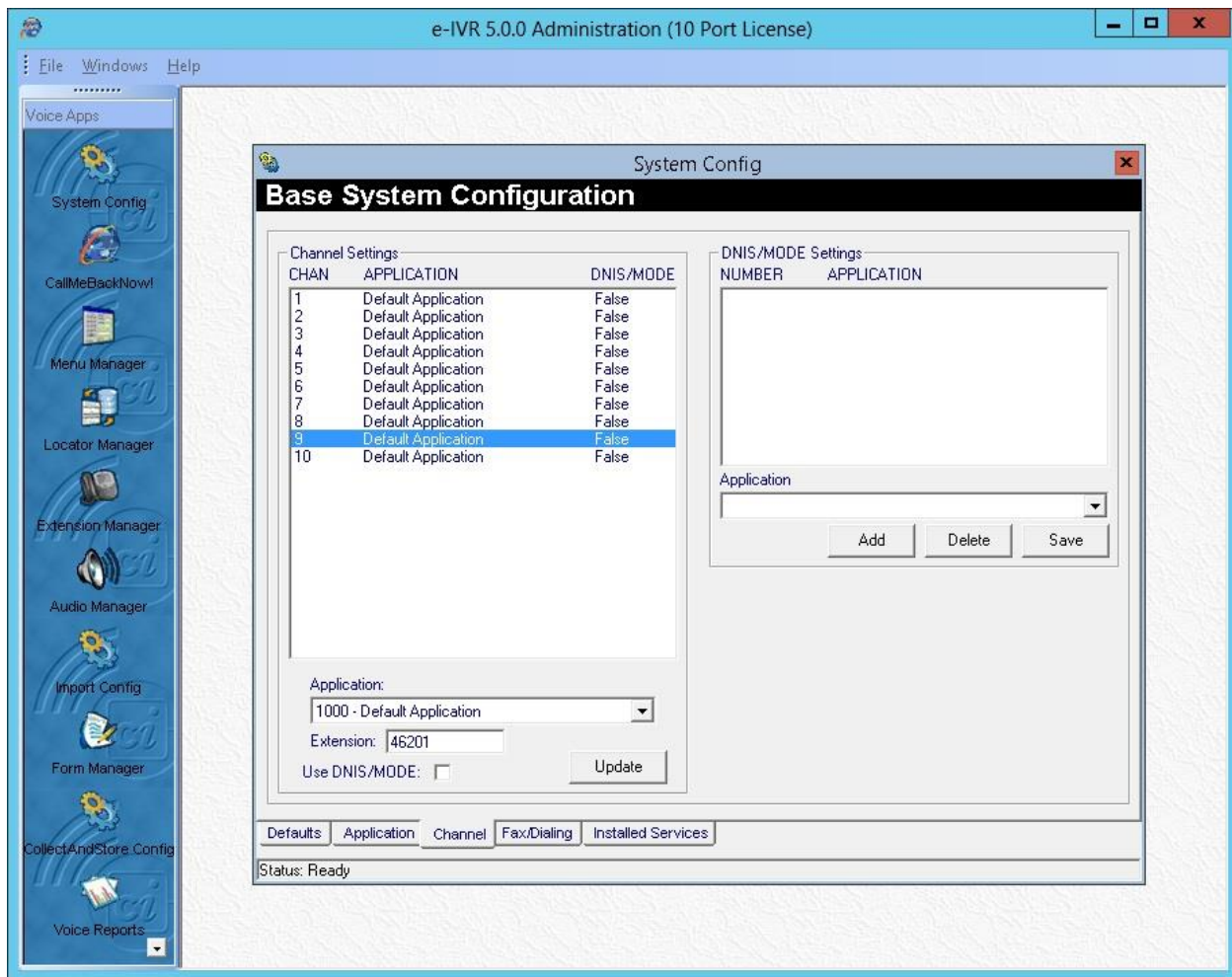
Select the **Channel** tab from the bottom of the **System Config** pop-up screen.

In the **Channel Setting** sub-section, select the first channel entry. For **Extension**, enter the first SIP user extension from **Section 6.2** used for the inbound application, in this case “46101”. By default, all third party channel resources are used for inbound applications unless otherwise specified. Note that the compliance testing used ten channel resources, which is governed by the Dialogic license.

In the compliance testing, two SIP users were associated with the one inbound application and were mapped to the first two channel resources.

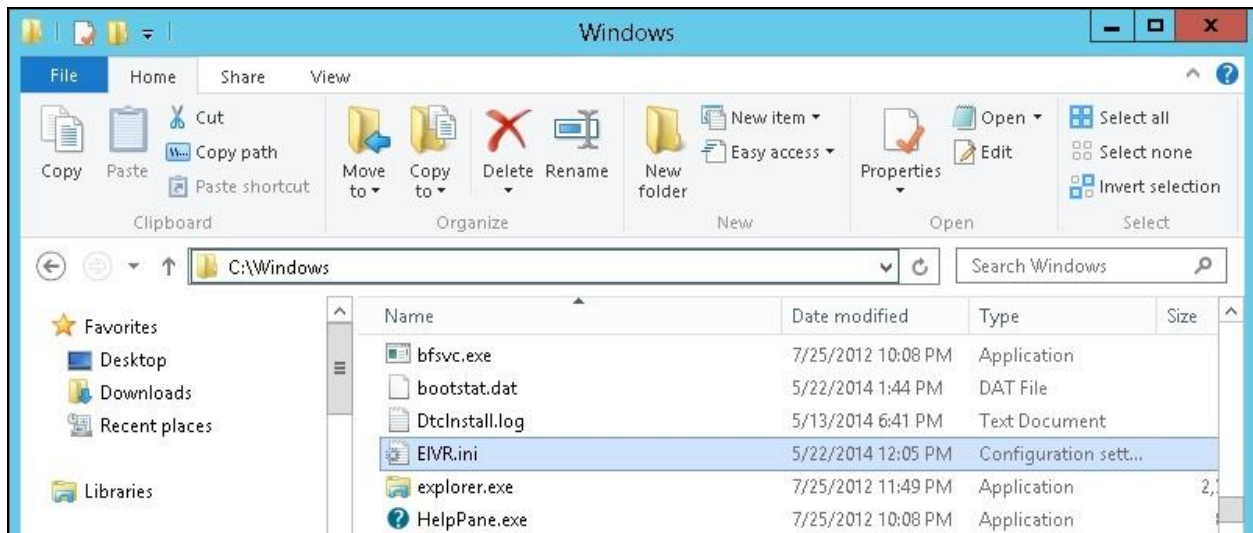


Repeat to map extensions associated with the outbound applications. In the compliance testing, channels 9 and 10 were used for two outbound applications and were mapped to SIP user extensions “46201” and “46202” from **Section 6.2** respectively.



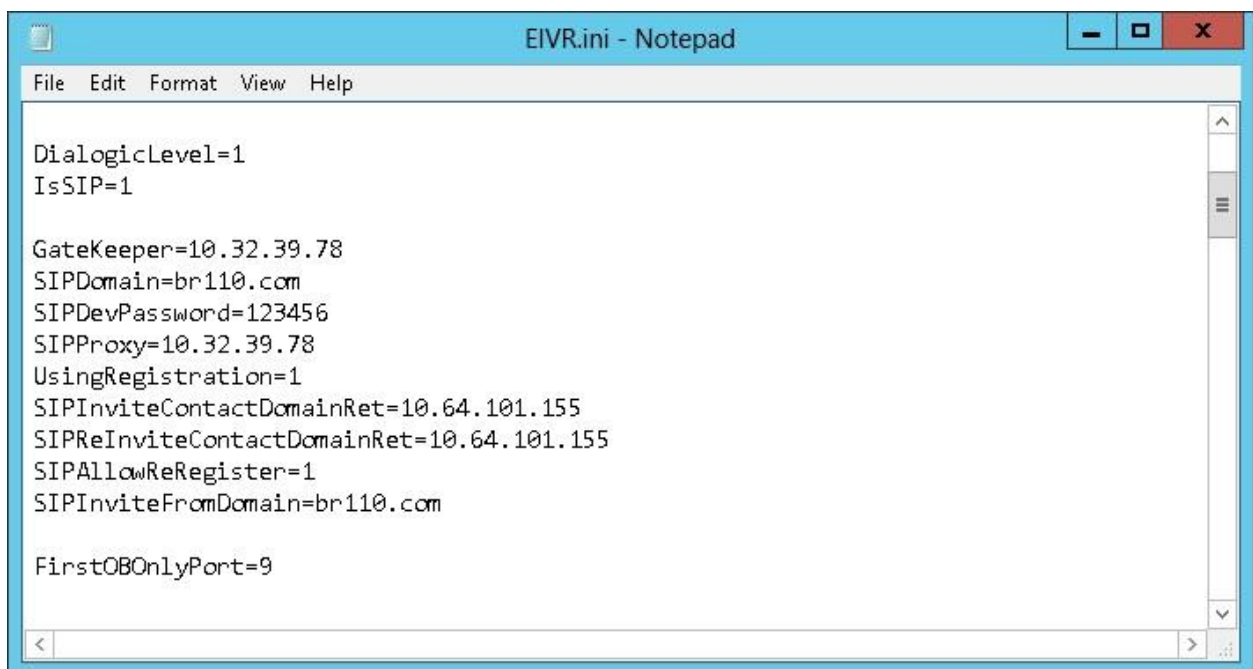
7.2. Administer EIVR.ini

From the e-IVR server, navigate to the **C:\Windows** directory to locate the **EIVR.ini** file.



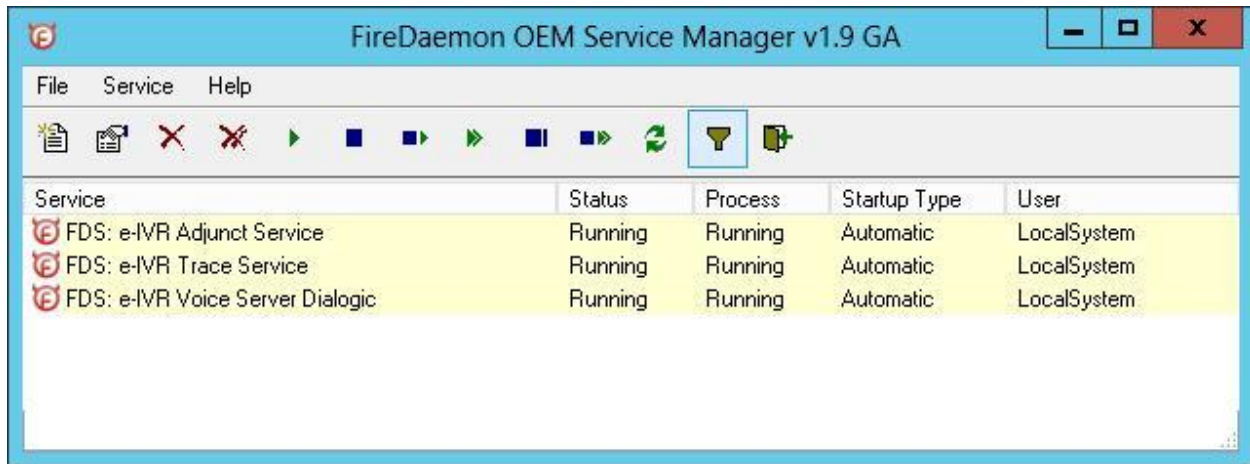
Open the **EIVR.ini** file with the Notepad application. Configure the parameters as shown below, where "10.32.39.78" is the IP address of the Session Manager signaling interface, "10.64.101.155" is the IP address of the e-IVR server, and "br110.com" is the domain name from **Section 3**. For **SIPDevPassword**, enter the common SIP user password from **Section 6.2**.

For **FirstOBOnlyPort**, enter the first channel resource reserved for outbound applications, in this case "9".



7.3. Restart Service

From the **Start** screen shown in **Section 7.1**, select **Service Manager** to display the screen below. Restart the **e-IVR Voice Server Dialogic** service.



8. Verification Steps

This section provides tests that can be performed to verify proper configuration of Session Manager and e-IVR.

8.1. 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 the user from **Section 6.2** is registered, as shown below with a check in the **Registered Prim** column.

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

Help ?

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 10:59 AM

Customize ▸

Advanced Search ▸

104 Items Show 15 ▾

Filter: Enable

| <input type="checkbox"/> | 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 | 46002@br110.com | SIP 2 | Avaya | BR-1C110 | 20.32.39.106:5061 | <input type="checkbox"/> | <input type="checkbox"/> | 1/3 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> (AC) | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | ► Show | 46101@br110.com | eIVR Inb-1 | CI | CI-Loc | 10.64.101.155:5060 | <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 | 46102@br110.com | eIVR Inb-2 | CI | CI-Loc | 10.64.101.155:5060 | <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 | 46201@br110.com | eIVR Outb-1 | CI | CI-Loc | 10.64.101.155:5060 | <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 | 46202@br110.com | eIVR Outb-2 | CI | CI-Loc | 10.64.101.155:5060 | <input type="checkbox"/> | <input type="checkbox"/> | 1/1 | <input type="checkbox"/> | <input checked="" type="checkbox"/> (AC) | <input type="checkbox"/> | <input type="checkbox"/> |

8.2. Verify Computer Instruments e-IVR

From the **Start** screen shown in **Section 7.1**, select **Voice Monitor** to display the **e-IVR Voice Monitor** screen. Verify that the **Status** for all ports is “Line is Idle”, as shown below.

| System Name | Port | Datestamp | Status |
|-----------------|------|----------------------|--------------|
| CI-EIVR-TEST-VM | 01 | 5/30/2014 9:57:22 AM | Line is Idle |
| CI-EIVR-TEST-VM | 02 | 5/30/2014 9:57:22 AM | Line is Idle |
| CI-EIVR-TEST-VM | 03 | 5/30/2014 9:57:22 AM | Line is Idle |
| CI-EIVR-TEST-VM | 04 | 5/30/2014 9:57:22 AM | Line is Idle |
| CI-EIVR-TEST-VM | 05 | 5/30/2014 9:57:22 AM | Line is Idle |
| CI-EIVR-TEST-VM | 06 | 5/30/2014 9:57:22 AM | Line is Idle |
| CI-EIVR-TEST-VM | 07 | 5/30/2014 9:57:22 AM | Line is Idle |
| CI-EIVR-TEST-VM | 08 | 5/30/2014 9:57:22 AM | Line is Idle |
| CI-EIVR-TEST-VM | 09 | 5/30/2014 9:57:22 AM | Line is Idle |
| CI-EIVR-TEST-VM | 10 | 5/30/2014 9:57:22 AM | Line is Idle |

9. Conclusion

These Application Notes describe the configuration steps required for Computer Instruments e-IVR to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP users. All feature and serviceability test cases were completed.

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 9, Release 6.3, October 2013, available at <http://support.avaya.com>.
2. *Administering Avaya Aura® Session Manager*, Release 6.3, Issue 3, October 2013, available at <http://support.avaya.com>.
3. *Installing e-IVR*, available from <http://www.instruments.com>.
4. *e-IVR Application Server*, available from <http://www.instruments.com>.

©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.