DevConnect Program

Application Notes for Imperium Inaipi Hospitality Application 2.0 running on Avaya Vantage™ Release 3 with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Session Manager R10.1 - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Imperium Inaipi Hospitality Application 2.0 running on Avaya Vantage™ Release 3 with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Session Manager R10.1.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the Avaya DevConnect Program.

1. Introduction

The Imperium Inaipi Hospitality Application runs on Avaya Vantage™ (hereafter referred to as Vantage). In these compliance testing, Avaya Vantage™ Release 3.x devices are Compliance tested specifically on K175 model. Vantage K155 model is not supported because of the screen size difference.

The Inaipi Hospitality Application is using Avaya Client SDK for the call service and all the application control can be done from the dedicated web control panel. The application is design to map the hotel room numbers enter on the Vantage to the extension on Avaya Aura® Communication Manager which also includes the Vantage server configurations and speed dial numbers. When the device is configured, the home screen will be displayed and the guest can use Vantage with customizable screen for theme, welcome message, speed dial buttons, call features, incoming call log and event push notification. Once configured, user cannot exit the screen unless she has the administration password.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on placing calls to and from the Vantage, and verifying two-way audio. The call types included calls to local extensions, and to the PSTN. Mute/un-mute, and volume are also tested in those scenarios. Feature testing also includes abbreviated dialing.

The serviceability testing focused on verifying the usability after restarting Vantage device.

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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and endpoints utilized enabled capabilities of TLS/SRTP.

2.1. Interoperability Compliance Testing

All test cases were performed manually. The following features were verified:

- Placing calls to internal extensions to verify two-way audio.
- Placing calls to the PSTN to verify two-way audio.
- Hearing ringing tone for incoming and ring back for outgoing calls.
- Answering and ending calls using the call control buttons on the application or the Bluetooth handset.
- Using the volume control buttons on the Vantage to adjust the audio volume.
- Using the mute control buttons on the application to mute and un-mute the audio.
- Switching between the handset, 3.5mm headset and the phone Bluetooth handset while in conversation.
- Basic telephony features, including redial and long duration calls.
- Screen display for rejected or unanswered inbound calls.
- Screen display for rejected outbound calls for invalid numbers.
- Label (abbreviated dialing) calls to places such as Operator, Laundry, Spa, Front desk etc.

For the serviceability testing, making calls were made for inbound and outbound after the reboot was completed.

2.2. Test Results

All test cases are completed successfully. The following observation was made:

- Customized Inaipi app for local configuration is used for Compliance Testing.
- Inaipi supports one outbound or inbound call at any one time as per design. Second inbound call will get a busy tone.
- There is no headset icon/button on the application to switch from handsets or speakers as per design.

2.3. Support

For support on this Inaipi Hospitality application solution, contact Imperium Support at:

- Phone: +97 142443417
- Website: http://www.imperiumapp.com
- Email: sales@imperiumapp.com

3. Reference Configuration

Figure 1 illustrates the test configuration used to verify Inaipi Hospitality App running on Avaya Vantage™ with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Note that Avaya Vantage™ K175 Release 3.x devices is supported only. Avaya Vantage™ Bluetooth handset is used.

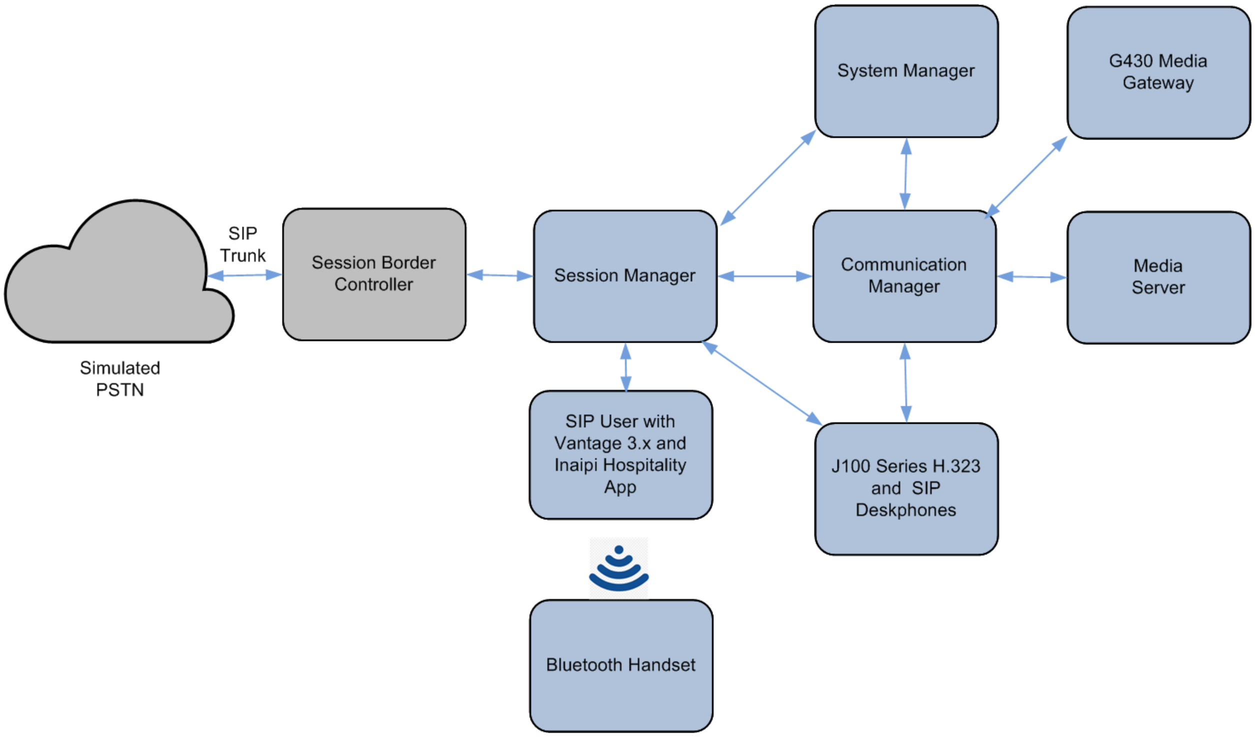


Figure 1: Test Configuration

4. Equipment and Software Validated

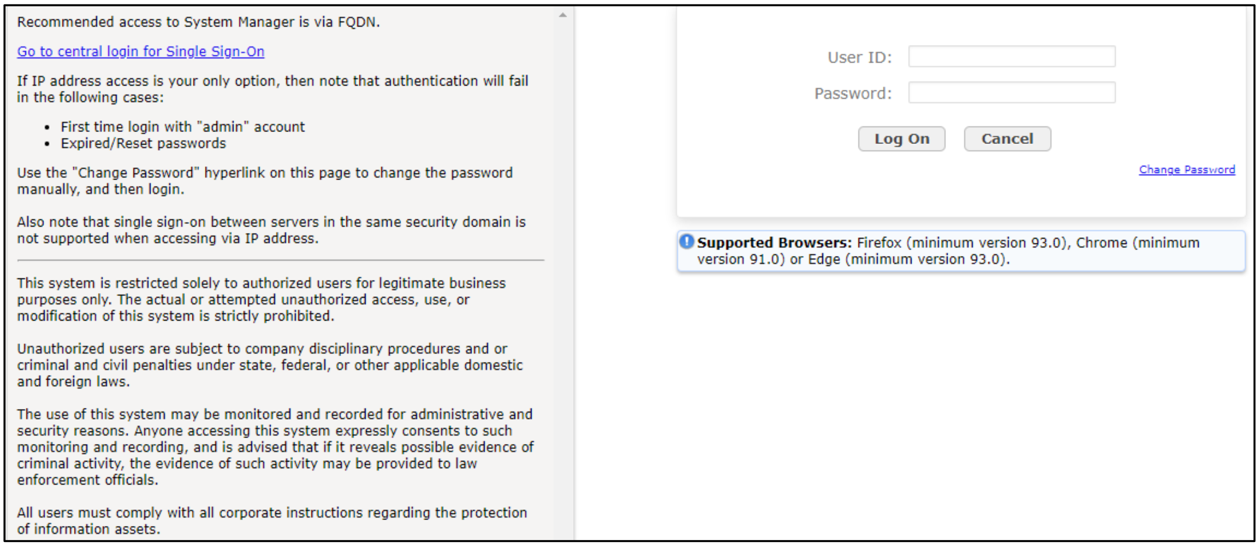
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Session Border Controller	10.1.0.0-32-21432
Avaya Aura® Communication Manager	10.1 SP3 (10.1.0.3.0.0.974.27867)
Avaya G430 Media Gateway • MGP	FW 42.22.0
Avaya Aura® System Manager	10.1 FP 3 Build 10.1.3.0.0715713
Avaya Aura® Session Manager	10.1 SP3 (10.1.3.0.1013007) Patch 91132
Avaya Aura® Media Server	10.1.0.147
Avaya J100 Series H.323 Deskphones	6.8541
Avaya J100 Series SIP Deskphones	4.1.1.3
Avaya Vantage™ K175 device running on Android Version 9	3.1.1.2
Imperium Inaipi Hospitality Application	2.0.10

6. Configure Avaya Aura® Session Manager

This section describes aspects of the Session Manager configuration required for Vantage to register. It is assumed that the Domains, Locations, SIP entities, Entity Links, Routing Policies, Dial Patterns and Application Sequences have been configured where appropriate for Communication Manager, and Session Manager.

Session Manager is managed via System Manager. Using a web browser, access **https://<ip-addr of System Manager>/SMGR**. In the **Log On** screen, enter appropriate **User ID** and **Password** and click the **Log On** button.


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

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

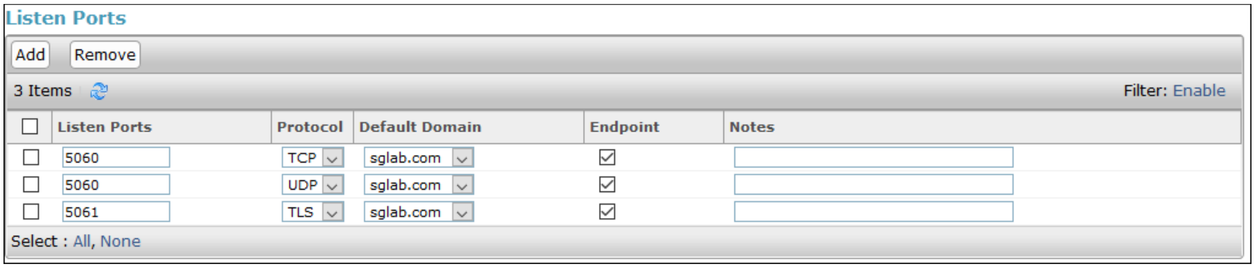
User ID:

Password:

Supported Browsers: Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0).

6.1. Verify Session Manager Ports for SIP endpoint registration

Each Session Manager Entity must be configured so that the SIP Endpoint can register to it. From the home page, under **Elements**, click **Routing → SIP Entities** (not shown) and select the Session Manager entity used for registration. Make sure that **TCP**, **UDP** and **TLS** entries are present under **Listen Ports**. During the compliance test, Vantage registered to the Session Manager using TLS transport are tested.


Listen Ports

3 Items

Filter: Enable

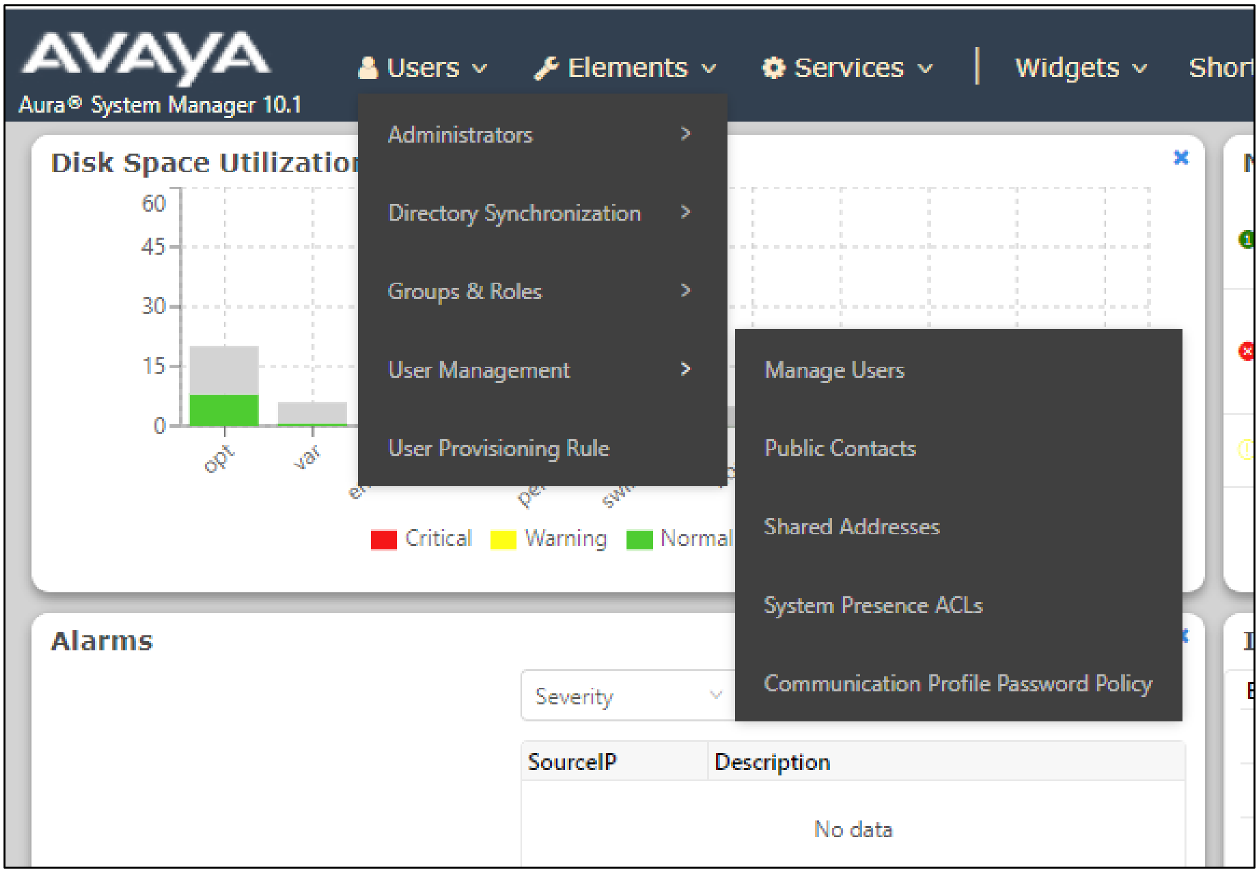
□	Listen Ports	Protocol	Default Domain	Endpoint	Notes
□	5060	TCP	sglab.com	☑	
□	5060	UDP	sglab.com	☑	
□	5061	TLS	sglab.com	☑	

Select : All, None

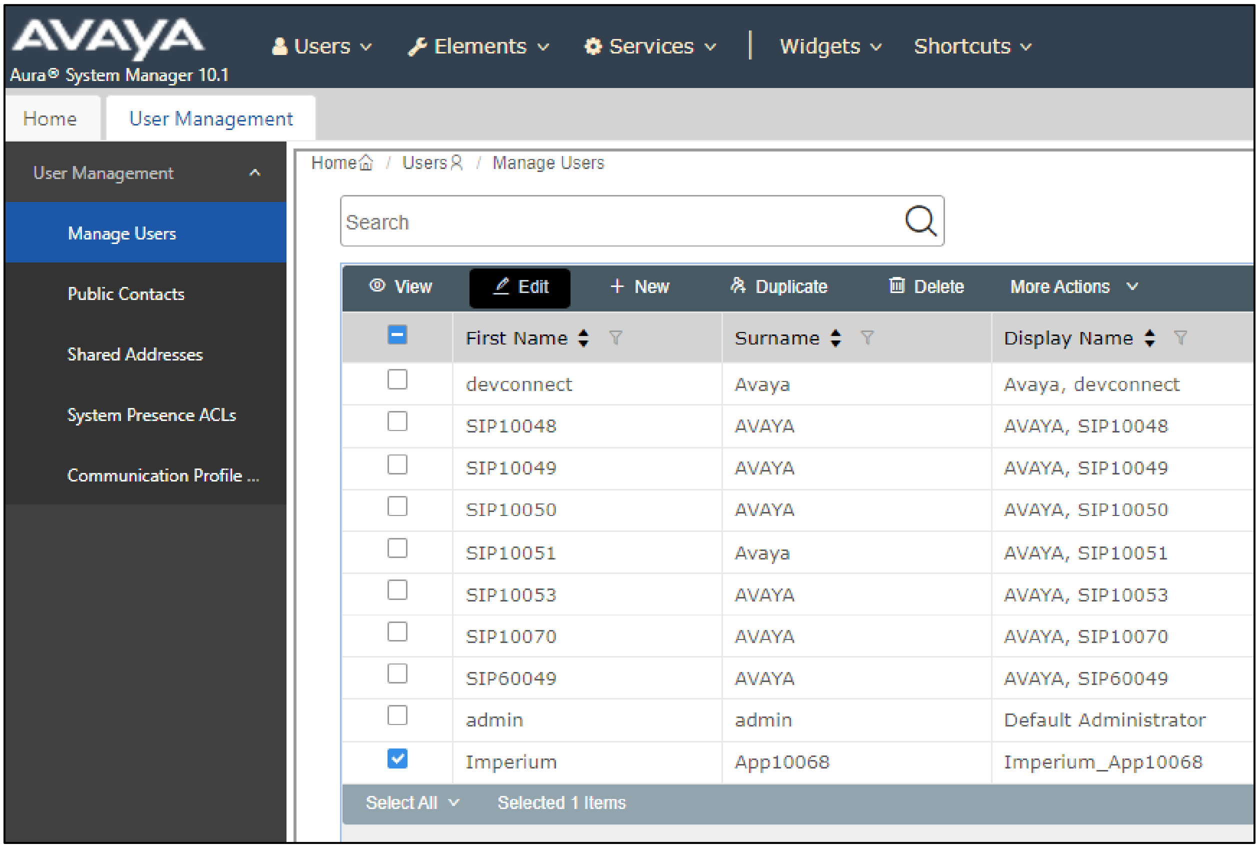
6.2. Add SIP User

The addition of SIP User will be assumed to be already created. The following highlight the abbreviated dialing configuration to be configured. Refer to details in administration document for Avaya Aura® Session Manager in **[2]** on adding SIP User.

From the System Manager dashboard, select **Users → User Management → Manage Users.**

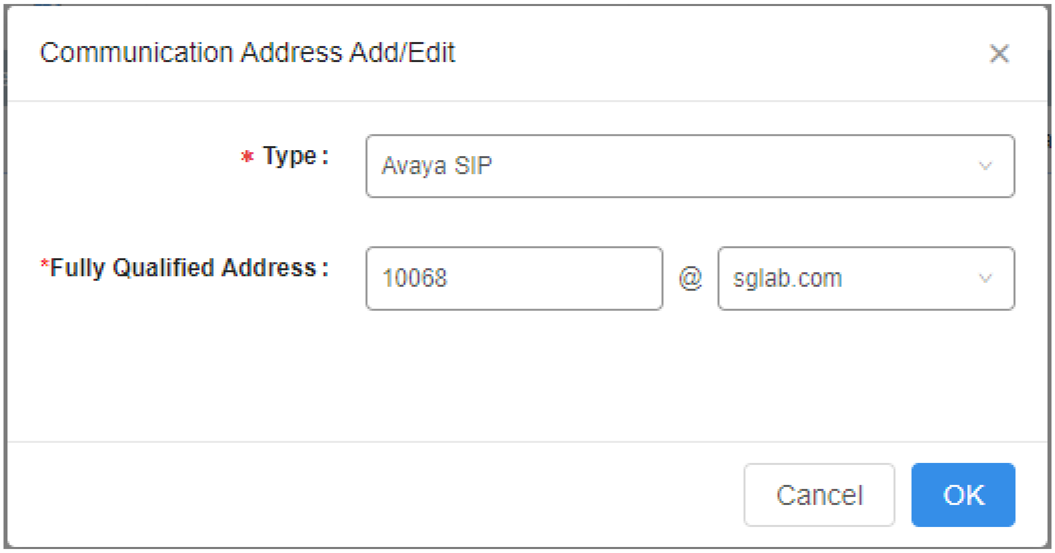


Click on the user and select **Edit.** The user screen configuration screen will be displayed.



☐	First Name	Surname	Display Name
☐	devconnect	Avaya	Avaya, devconnect
☐	SIP10048	AVAYA	AVAYA, SIP10048
☐	SIP10049	AVAYA	AVAYA, SIP10049
☐	SIP10050	AVAYA	AVAYA, SIP10050
☐	SIP10051	Avaya	AVAYA, SIP10051
☐	SIP10053	AVAYA	AVAYA, SIP10053
☐	SIP10070	AVAYA	AVAYA, SIP10070
☐	SIP60049	AVAYA	AVAYA, SIP60049
☐	admin	admin	Default Administrator
☑	Imperium	App10068	Imperium_App10068

Click on the **Communication Profile** tab and the **Communication Address**. Verify the User had **Avaya SIP** as **Type** for the Communication Address as sample below with **Fully Qualified Address**:

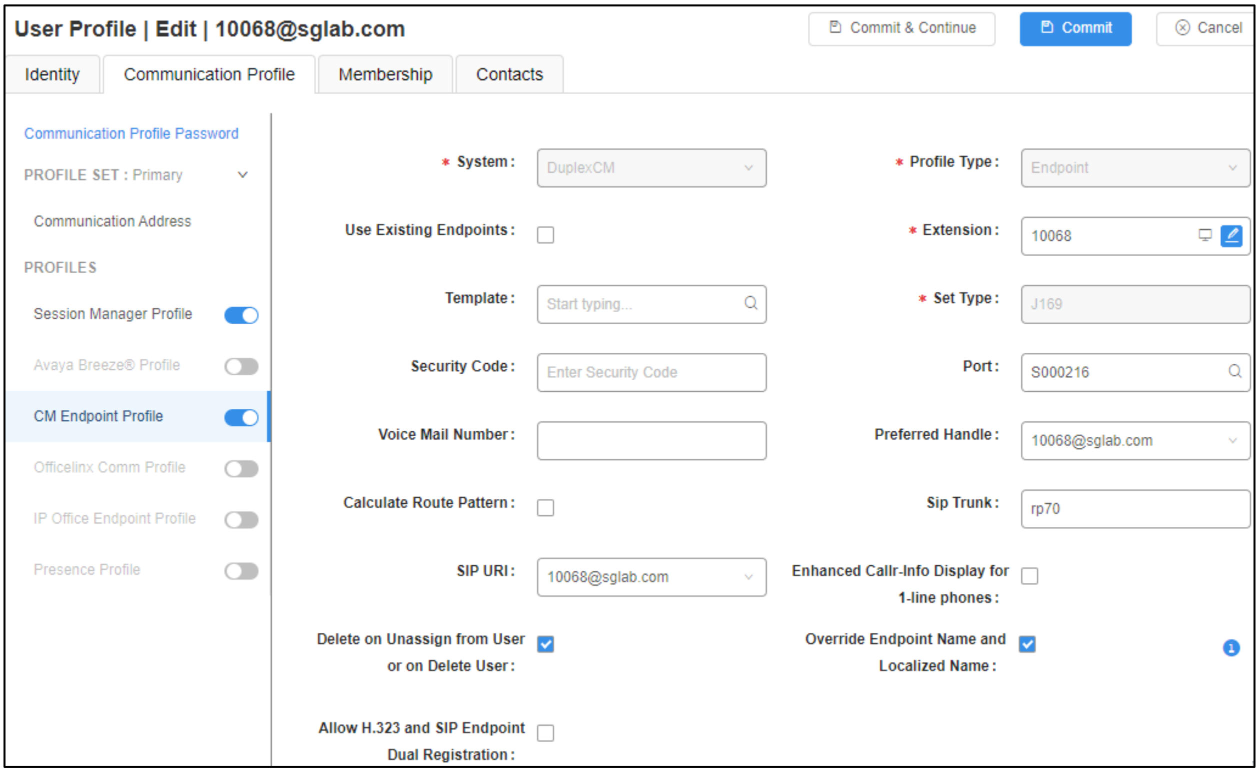


Communication Address Add/Edit

* Type : Avaya SIP

*Fully Qualified Address : 10068 @ sglab.com

Scroll down the page and select **CM Endpoint Profile** section. Click on the endpoint editor symbol beside the **Extension** below.



User Profile | Edit | 10068@sglab.com

* System : DuplexCM

* Profile Type : Endpoint

Use Existing Endpoints : □

* Extension : 10068

Template : Start typing...

* Set Type : J169

Security Code : Enter Security Code

Port : S000216

Voice Mail Number :

Preferred Handle : 10068@sglab.com

Calculate Route Pattern : □

Sip Trunk : rp70

SIP URI : 10068@sglab.com

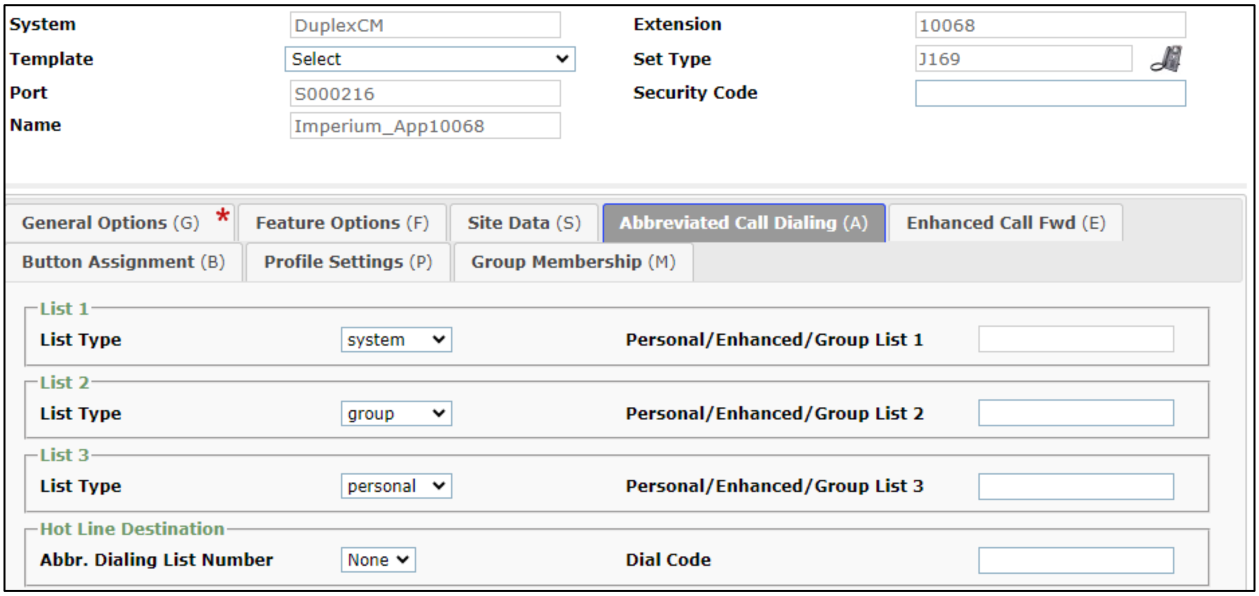
Enhanced Callr-Info Display for 1-line phones : □

Delete on Unassign from User or on Delete User : ☑

Override Endpoint Name and Localized Name : ☑

Allow H.323 and SIP Endpoint Dual Registration : □

From the editor screen, click on **Abbreviated Call Dialing** tab (not shown). Verify the abbreviated dialing **List** for **1**, **2** and **3** are configured for **system**, **group** and **personal**. Other features maybe subsequently added as required.



System	DuplexCM	Extension	10068
Template	Select	Set Type	J169
Port	S000216	Security Code	
Name	Imperium_App10068		

List 1

List Type	system	Personal/Enhanced/Group List 1	

List 2

List Type	group	Personal/Enhanced/Group List 2	

List 3

List Type	personal	Personal/Enhanced/Group List 3	

Hot Line Destination

Abbr. Dialing List Number	None	Dial Code	

7. Configure Avaya Aura® Communication Manager

It is implied a working Communication Manager system is already in place, including dial plans and SIP trunks to Session Manager. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 11**.

8. Configure Inaipi Hospitality Application

8.1. Installation of Inaipi Application

The Inaipi application is pushed automatically from the file server hosting the 46xxsettings file to the Vantage as apk application file, since Vantage runs on Android. In Vantage Release 3.x devices, the Android is running on version 9.

The following highlight are the essential configuration of the 46xxsettings file for the apk application file to be pushed and configuration to be pinned. For other settings particular to Vantage, refer to [**4**] in **Section 11**.

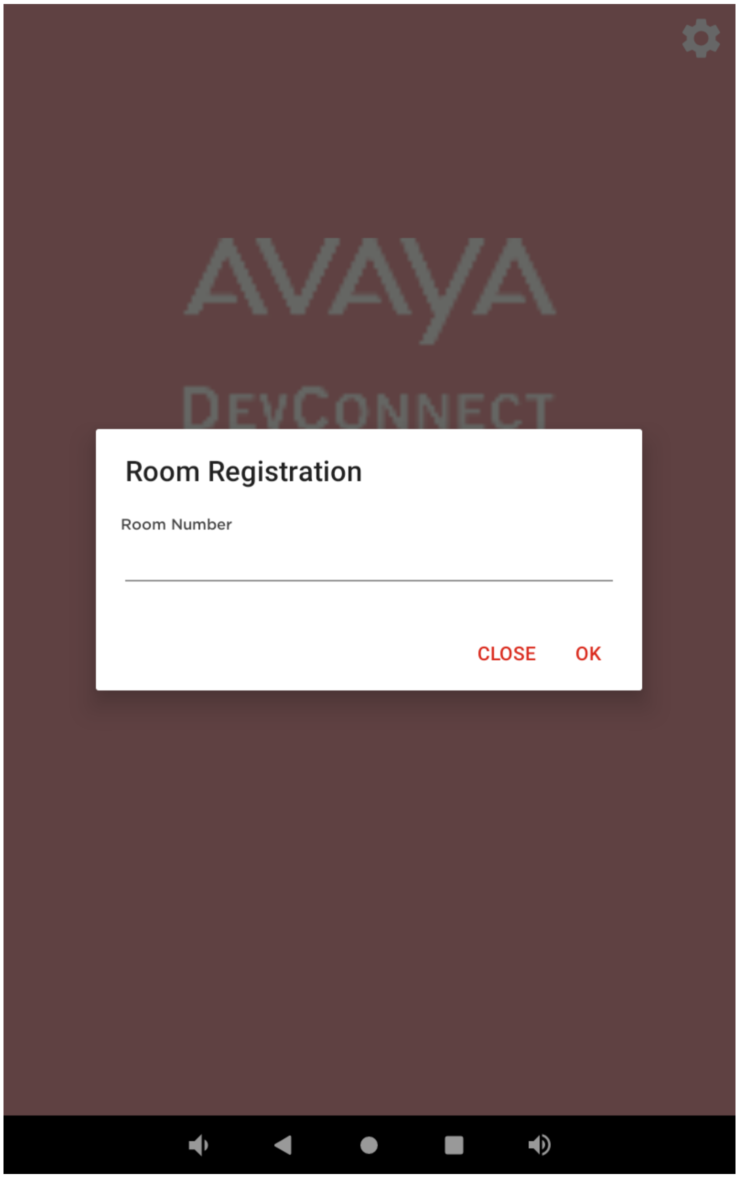
```
##################  APPLICATIONS SETTINGS (SIP)  ################
##
## ACTIVE_CSDK_BASED_PHONE_APP specifies the Android package name (as defined in the
application APK manifest file) of active phone application.
SET ACTIVE_CSDK_BASED_PHONE_APP "com.avaya.jumeirah.commpackage"

## PUSH_APPLICATION specifies a list of third party applications (APKs) for installation on
Avaya Vantage devices.
SET PUSH_APPLICATION "devconnect-app-release-test-4.apk"
##
## PIN_APP specifies the Android package name (as defined in the application APK manifest file)
of the application to be pinned after boot up.
SET PIN_APP "com.avaya.jumeirah.commpackage"

## DEFAULT_PIN_APP specifies which application out of the applications to be pinned shall be
presented after reboot/powerup. The android package name of this application shall be
configured.
SET DEFAULT_PIN_APP "com.avaya.jumeirah.commpackage"
```

If the application had been previously installed, clear the cache and stored data before rebooting Vantage to install a new version. Below is the steps to clear the cache and stored data.

1. Select the Inaipi application from the list of apps and hold it.
2. Select the **App Info** that pops up.
3. Select **Storage → Clear Storage** or **Clear Cache**.

8.2. Configuration of Inaipi Application

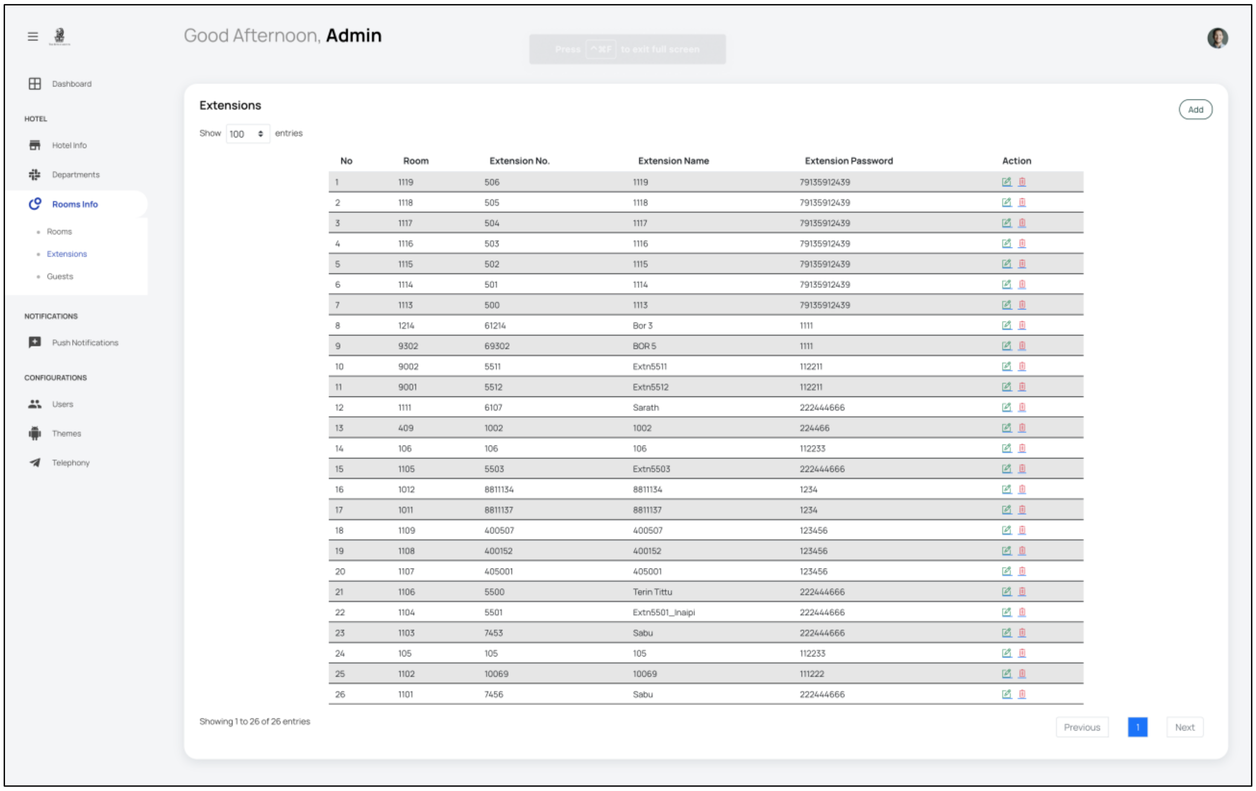
In field operation, the configuration is performed by logging into an assigned **Room Registration** number provided by the administrator during installation, where the application is being executed for the first time. The relevant information for the Vantage to be configured were obtained from the cloud web UI (as opposed to a localized configuration used for Compliance Testing).



Room Registration

Room Number

The web configuration is administered by Imperium and will not be detailed here. Below is a screen capture for a sample of the web UI in general with configuration link to the room number and telephony portion.

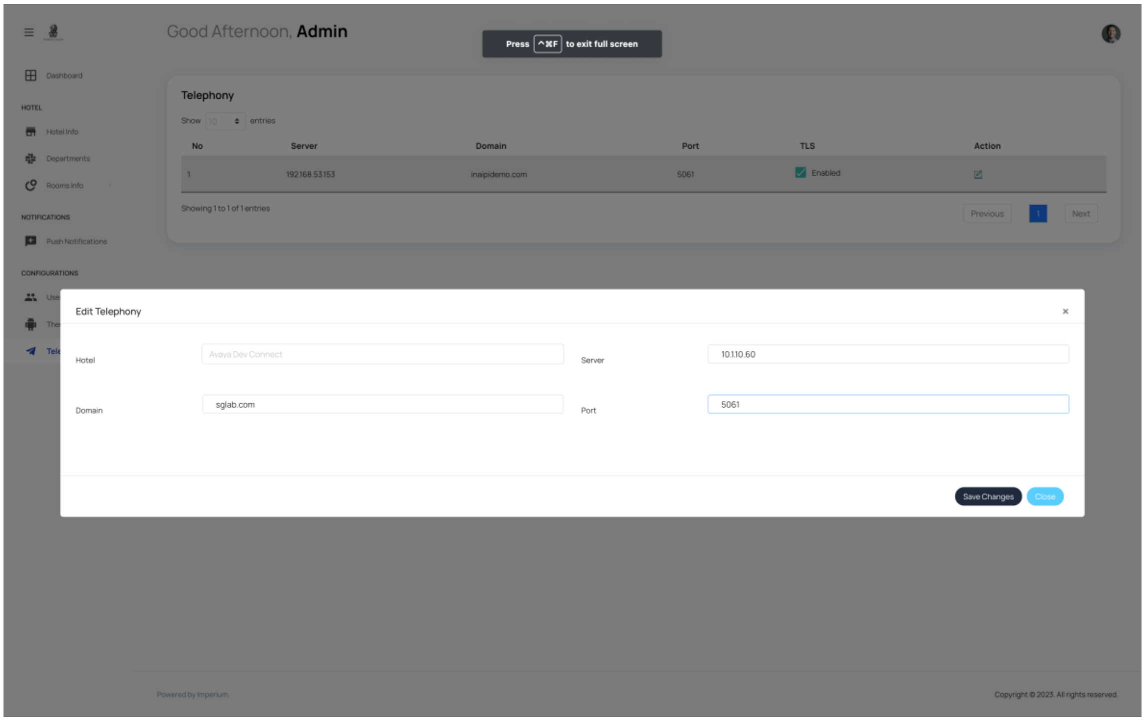


Extensions

Show 100 entries

No	Room	Extension No.	Extension Name	Extension Password	Action
1	1119	506	1119	79135912439	
2	1118	505	1118	79135912439	
3	1117	504	1117	79135912439	
4	1116	503	1116	79135912439	
5	1115	502	1115	79135912439	
6	1114	501	1114	79135912439	
7	1113	500	1113	79135912439	
8	1214	61214	Bor 3	1111	
9	9302	69302	BOR 5	1111	
10	9002	5511	Extn5511	112211	
11	9001	5512	Extn5512	112211	
12	1111	6107	Sarath	222444666	
13	409	1002	1002	224466	
14	106	106	106	112233	
15	1105	5503	Extn5503	222444666	
16	1012	8811134	8811134	1234	
17	1011	8811137	8811137	1234	
18	1109	400507	400507	123456	
19	1108	400152	400152	123456	
20	1107	405001	405001	123456	
21	1106	5500	Terin Tittu	222444666	
22	1104	5501	Extn5501_Inaipi	222444666	
23	1103	7453	Sabu	222444666	
24	105	105	105	112233	
25	1102	10069	10069	111222	
26	1101	7456	Sabu	222444666	

Showing 1 to 26 of 26 entries



Telephony

Show 10 entries

No	Server	Domain	Port	TLS	Action
1	192.168.53.153	inaipidemo.com	5061	☑ Enabled	

Showing 1 to 1 of 1 entries

Edit Telephony

Hotel: Avaya Dev Connect

Server: 10.1.10.60

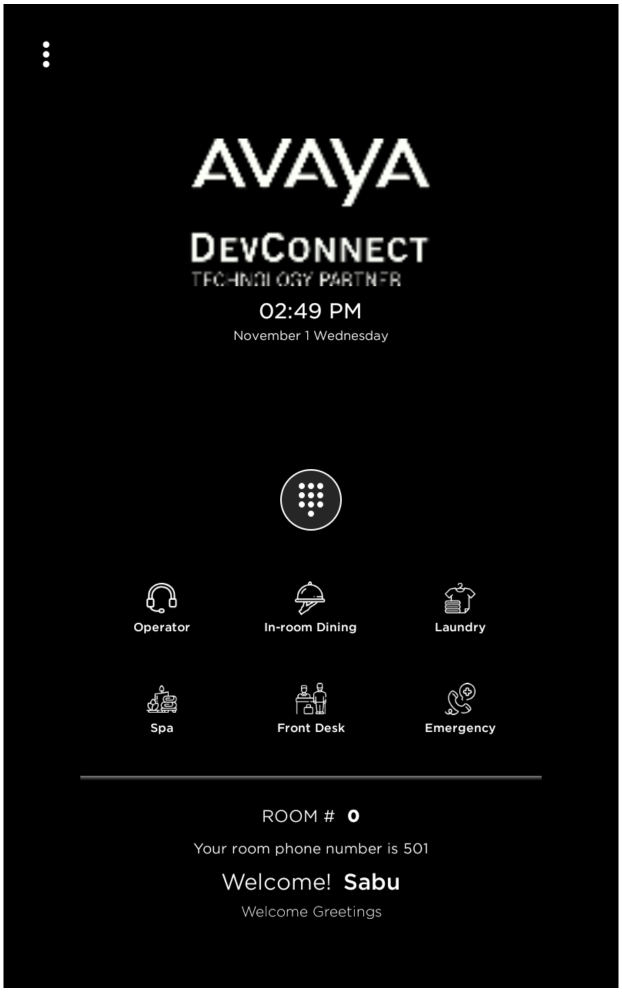
Domain: sglab.com

Port: 5061

As the compliance test is using localized configuration settings, the configuration screen will be displayed (not shown) after the application is started for the first time and the following information are required:

1. **Address** – Registration server IP address and the Session Manager is configured.
2. **Domain** – SIP domain applicable to the Aura environment.
3. **Port** – SIP port for registration.
4. **TLS** – Turn on for registration if applicable.
5. **use_certificate** – Turn on for registration with certificate already imported or pushed.
6. **Extensions Username/Password** – Enter the appropriate room extensions.
7. **Room Number –** Enter the room extensions assigned by administrator.
8. **User –** Enter appropriate user name.
9. **Speed Dial** – Enter Speed Dial number for testing purpose.

Below is a sample of the home screen after successfully configured with the information above.



02:49 PM

November 1 Wednesday

ROOM # 0

Your room phone number is 501

Welcome! Sabu

Welcome Greetings

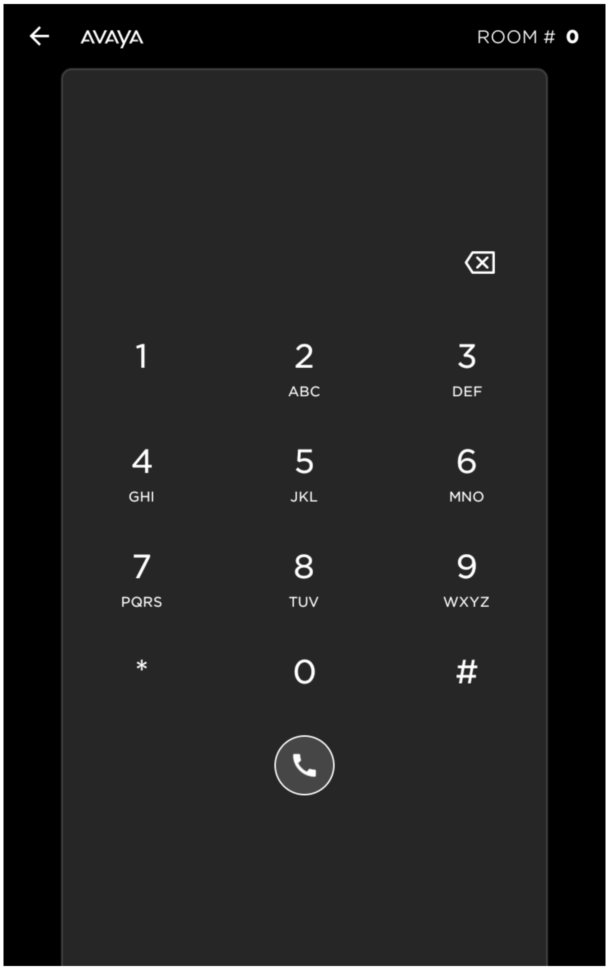
9. Verification Steps

This section verifies that Imperium Inaipi application has been successfully integrated with Vantage.

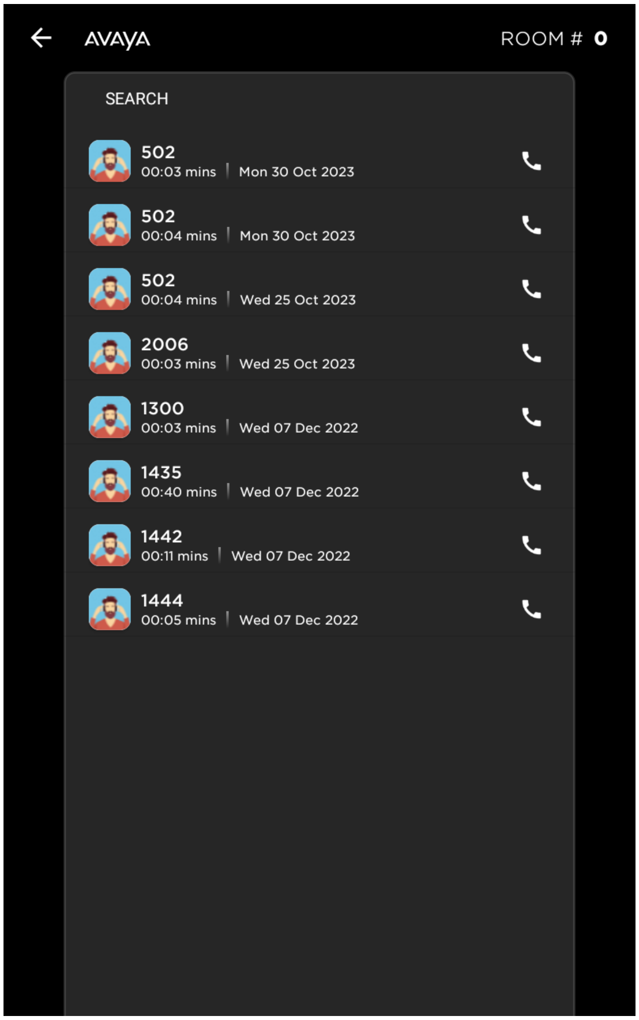
9.1. Inaipi Hospitality Application

Below are the steps to verify the functionality of the Inaipi application.

- Click to start the application assuming it is already configured. If the application is registered successfully for the first time, a registration message will be flashed at the bottom of the home screen.
- On the Vantage home screen shown in bottom of **Section 8.2**, click the dial pad icon on the top. Verify dial tone can be heard from the speaker (or by lifting the handset) by selecting the off-hook icon.



- Swipe from the right side of the screen from right to left, and verify dialer and call history can be seen as below.

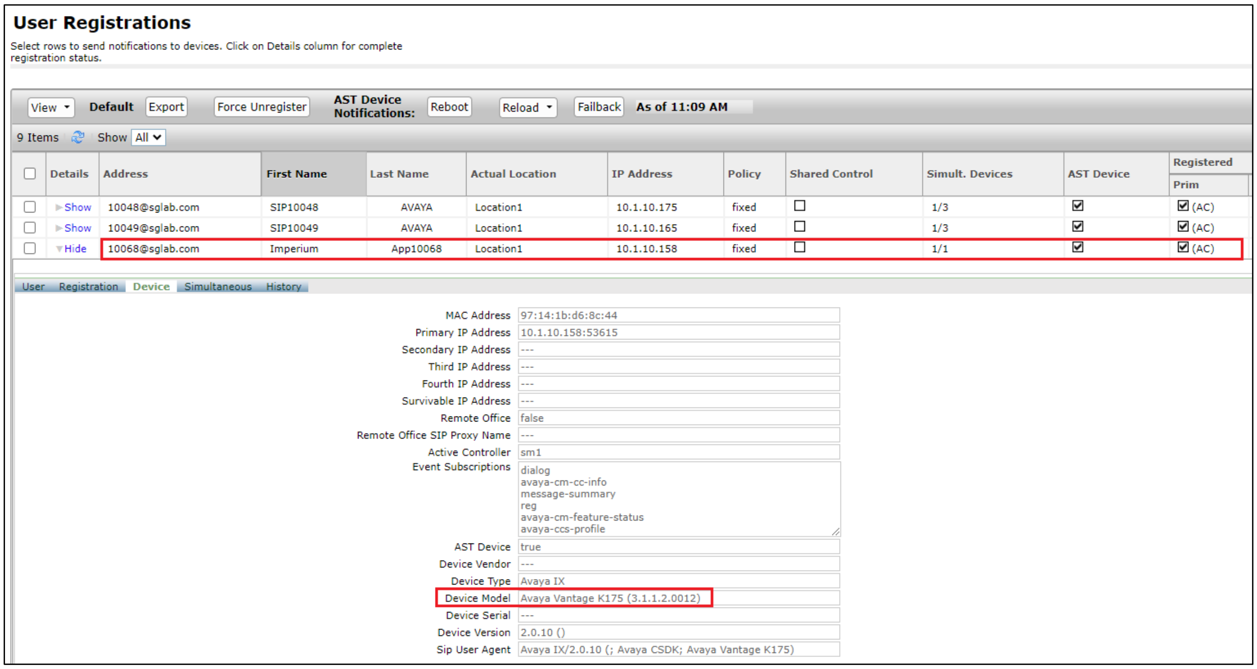


502	00:03 mins	Mon 30 Oct 2023
502	00:04 mins	Mon 30 Oct 2023
502	00:04 mins	Wed 25 Oct 2023
2006	00:03 mins	Wed 25 Oct 2023
1300	00:03 mins	Wed 07 Dec 2022
1435	00:40 mins	Wed 07 Dec 2022
1442	00:11 mins	Wed 07 Dec 2022
1444	00:05 mins	Wed 07 Dec 2022

- Make incoming and outgoing calls and verify that calls can be established with two-way audio. For incoming calls, answer the call by pressing the **Accept** message.
- End the call by pressing the **ONHOOK** icon on application.
- Verify also that call control call functions such as mute/un-mute and adjust the volume can be performed on the Vantage with speaker or handset mode.

9.2. SIP registration to Avaya Aura® Session Manager

Using a web browser, access **https://<ip-addr of System Manager>/SMGR**. From the home page, under **Elements**, click **Session Manager → System Status → User Registration**. Verify the user is registered with the appropriate device.



User Registrations

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

☐	Details	Address	First Name	Last Name	Actual Location	IP Address	Policy	Shared Control	Simult. Devices	AST Device	Registered
											Prim
☐	▸ Show	10048@sglab.com	SIP10048	AVAYA	Location1	10.1.10.175	fixed	☐	1/3	☑	☑ (AC)
☐	▸ Show	10049@sglab.com	SIP10049	AVAYA	Location1	10.1.10.165	fixed	☐	1/3	☑	☑ (AC)
☐	▾ Hide	10068@sglab.com	Imperium	App10068	Location1	10.1.10.158	fixed	☐	1/1	☑	☑ (AC)

MAC Address	97:14:1b:d6:8c:44
Primary IP Address	10.1.10.158:53615
Secondary IP Address	---
Third IP Address	---
Fourth IP Address	---
Survivable IP Address	---
Remote Office	false
Remote Office SIP Proxy Name	---
Active Controller	sm1
Event Subscriptions	dialog avaya-cm-cc-info message-summary reg avaya-cm-feature-status avaya-ccs-profile
AST Device	true
Device Vendor	---
Device Type	Avaya IX
Device Model	Avaya Vantage K175 (3.1.1.2.0012)
Device Serial	---
Device Version	2.0.10 ()
Sip User Agent	Avaya IX/2.0.10 (; Avaya CSDK; Avaya Vantage K175)

10. Conclusion

These Application Notes describe the integration of Imperium Inaipi Hospitality Application 2.0 running on Avaya Vantage™ with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Session Manager R10.1. All test cases were completed successfully with observations noted in **Section 2.2**.

11. Additional References

This section references the Avaya documentation that are relevant to these Application Notes.

The following Avaya product documentation can be found at http://support.avaya.com.

[1] *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 5, Mar 2023.

[2] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 5, Feb 2023.

[3] *Using Avaya Vantage™*, Release 3.1.1, Issue 3, Nov 2022.

[4] *Installing and Administering Avaya Vantage™ in an Avaya Aura® or IP Office Environment*, Release 3.1.1, Issue 5, Sep 2022.

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.