



Avaya Solution & Interoperability Test Lab

Application Notes for Workforce Connect Voice Client running on TC51 Touch Computer from Zebra Technologies with Avaya Aura® Communication Manager and Avaya Aura® Session Manager - Issue 1.0

Abstract

These Application Notes describe the integration of the Workforce Connect Voice Client running on TC51 touch computer with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. The Workforce Connect Voice Client runs on Android based Voice enabled touch computers. Workforce Connect Voice Client on TC51 registers with Avaya Aura® Session Manager as a SIP endpoint through the enterprise wireless LAN.

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 integration of the Workforce Connect (WFC) Voice Client running on an TC51 touch computer with Avaya Aura® Communication Manager (Communication Manager) and Avaya Aura® Session Manager (Session Manager). The WFC Voice Client runs on Android based Voice enabled touch computers. The WFC Voice Client registers with Avaya Aura® Session Manager as a SIP endpoint through the enterprise wireless LAN.

The WFC Voice Client provides the capability to customize its user interface by adding telephony feature buttons.

Feature buttons that are associated with telephony features are supported locally by WFC Voice Client such as Do Not Disturb, Hold, and Call Transfer etc. Refer to WFC Voice Client documentation for a full list of feature buttons supported, and button configuration and operation.

The features tested by this solution are listed below.

Automatic Redial	Call Forward (All/Busy/Do not Answer)
Call Hold/Resume	Call Park/Unpark
Consultation Hold	Do Not Disturb
Transfer	Call Pickup
Conference	Extended Call Pickup
Message Waiting Indicator	Directed Call Pickup
Speed Dial Buttons	Exclusion
Automatic Call back	Priority Calling

2. General Test Approach and Test Results

This section details the general approach to the testing, what was covered, and results of the testing. If the testing was successfully concluded but it was necessary to implement workarounds or certain non-critical features did not work, it should be noted in **Section 2.2**.

The interoperability compliance test included feature and serviceability testing. The feature testing focused on establishing calls between the WFC Voice Client and Avaya SIP, H.323, and digital telephones and exercising basic telephony features, such as hold, mute, transfer, and conference. Additional telephony features, such as call forward, coverage, call park/unpark, call pickup etc., were also verified.

The serviceability testing focused on verifying that the WFC Voice Client comes back into service after rebooting it or the wireless LAN 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 the Zebra Technologies did not include use of any specific encryption features as requested by Zebra Technologies.

Avaya's formal testing and Declaration of Conformity is provided only on the headsets/Smartphones that carry the Avaya brand or logo. Avaya may conduct testing of non-Avaya headset/handset to determine interoperability with Avaya phones. However, Avaya does not conduct the testing of non-Avaya headsets/Smartphones for: Acoustic Pressure, Safety, Hearing Aid Compliance, EMC regulations, or any other tests to ensure conformity with safety, audio quality, long-term reliability or any regulation requirements. As a result, Avaya makes no representations whether a particular non-Avaya headset will work with Avaya's telephones or with a different generation of the same Avaya telephone.

Since there is no industry standard for handset interfaces, different manufacturers utilize different handset/headset interfaces with their telephones. Therefore, any claim made by a headset vendor that its product is compatible with Avaya telephones does not equate to a guarantee that the headset will provide adequate safety protection or audio quality.

Avaya's formal testing and Declaration of Conformity is provided only on the headsets/handsets that carry the Avaya brand or logo. Avaya may conduct testing of non-Avaya headset/handset to determine interoperability with Avaya phones. However, Avaya does not conduct the testing of non-Avaya headsets/handsets for: Acoustic Pressure, Safety, Hearing Aid Compliance, EMC regulations, or any other tests to ensure conformity with safety, audio quality, long-term reliability or any regulation requirements. As a result, Avaya makes no representations whether a particular non-Avaya headset will work with Avaya's telephones or with a different generation of the same Avaya telephone.

Since there is no industry standard for handset interfaces, different manufacturers utilize different handset/headset interfaces with their telephones. Therefore, any claim made by a headset vendor that its product is compatible with Avaya telephones does not equate to a guarantee that the headset will provide adequate safety protection or audio quality.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- SIP registration of WFC Voice Client with Avaya Aura® Session Manager.
- Calls between WFC Voice Client and Avaya SIP, H.323, and digital telephones with Direct IP Media (Shuffling) enabled and disabled.
- Calls between WFC Voice Client and PSTN.
- G.711MU/A and G.729 codec support.
- Proper recognition of DTMF tones.
- Basic telephony features, including hold, mute, redial, multiple calls, call display, blind and supervised transfer, and attended conference.
- Extended telephony features using TC51 feature buttons as mentioned in **Section 1**.
- Telephony features using Multi-Device Access.
- Voicemail coverage, MWI support, and logging into voicemail system to retrieve messages.
- Proper system recovery after a restart of the WFC Voice Client and loss of wireless connectivity.

2.2. Test Results

All test cases passed with the following observations noted:

- Zebra Technologies products currently do not support encryption, so for this solution to work encryption protocols had to be disabled between the Avaya products.
- During compliance testing only TCP was used for signaling protocol.
- WFC Voice Client currently does not provide any notification when Long Hold Recall Timer expires. Zebra Technologies is aware of this and working towards an enhancement.
- When more than one voice message is delivered to WFC Voice Client, the WFC Voice Client visual notification only shows “1” message, however all delivered messages can be retrieved when WFC Voice Client dials the voice mail system. Zebra Technologies is aware of this issue and working towards a resolution.
- When an incoming call is presented to a WFC Voice Client and if the handset is in idle state (blank screen), after the client answers the call and taps the Transfer button to transfer a call, the client is not presented with a dial pad. Instead the main screen is presented with the call being on hold. User needs to resume the call and then tap the transfer button again to be presented with a dial pad to continue the transfer operation. This sequence is only seen when the handset is in idle state. Zebra Technologies is aware of this issue and working towards a resolution.
- Automatic Callback button in WFC Voice Client is only presented if the called number has Call Waiting or a Coverage path enabled. The Automatic Callback button is not presented if the called number returns SIP Busy message.

2.3. Support

For technical support on the Workforce Connect Voice Client, contact Zebra Technologies support via phone or website.

- **Phone:** 1.800.653.5350
- **Web:** <http://www.zebra.com>

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of TC51 Workforce Connect Voice Clients with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. In this configuration, the WFC Voice Client runs on the TC51 touch computer and connects to the enterprise wireless network. The WFC Voice Client registers with Session Manager via SIP.

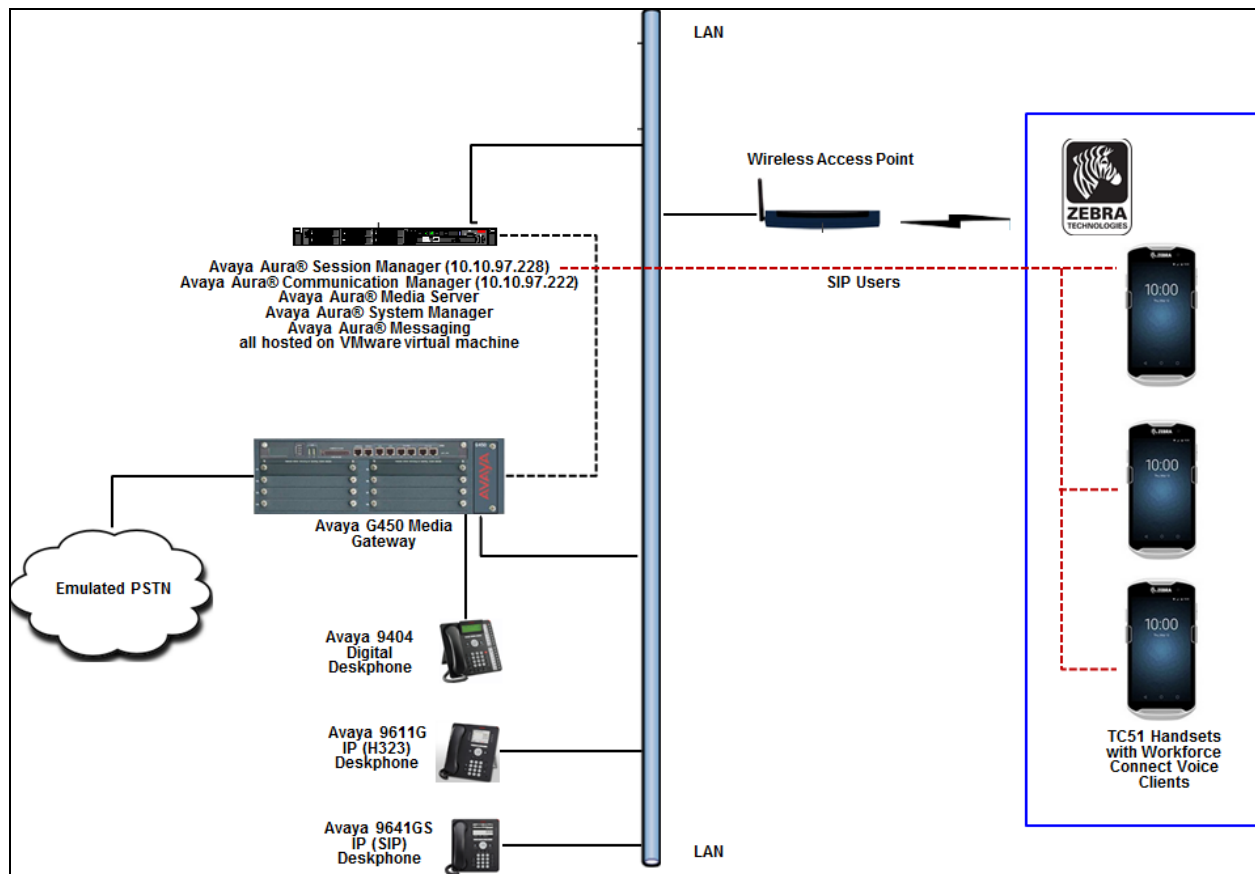


Figure 1: TC51 Workforce Connect Voice Client with Avaya Aura® Communication Manager and Avaya Aura® Session Manager

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura [®] System Manager running on virtual machine	7.1 FP2 (7.1.2.0.0.57353)
Avaya Aura [®] Communication Manager running on virtual machine	7.1.2.0.0-FP2
Avaya Aura [®] Session Manager running on virtual machine	7.1.2.0.712004
Avaya Aura [®] Media Server running on virtual machine	7.8.0.333
Avaya Aura [®] Messaging running on virtual machine	7.0.1.2.0-FP1SP2
Avaya G450 Media Gateway	38.21.0/1
Avaya IP Phones: Avaya 9611G (H.323) Avaya 9641GS (SIP)	6.6401 7.0.1.2.9
Avaya 9404 Digital Deskphone	18.0
Workforce Connect Voice Client running on TC51 Wireless handset	8.2.738

5. Configure Avaya Aura® Communication Manager

It is assumed that a fully functioning Communication Manager is in place with the necessary licensing with a SIP Trunk in place to Session Manager. For further information on the configuration of Communication Manager please see **Section 10** of these Application Notes. The following sections go through the following.

- Configure Dial Plan Analysis
- Configure IP Interfaces
- Configure Network Region
- Configure IP Codec Set
- Configure Signalling Group

5.1. Configure Dial Plan Analysis

Use the **change dialplan analysis** command to configure the dial plan using the parameters shown below. Extension numbers (**ext**) are those beginning with **56**.

change dialplan analysis			DIAL PLAN ANALYSIS TABLE			Page 1 of 12		
			Location: all			Percent Full: 7		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
56	5	ext						

5.2. Configure IP Interfaces

Shown below is an example of the nodes names used in the compliance testing. Note that TC51 Workforce Voice Connect does not feature in this setup and only the name and IP address of Session Manager and Communication Manager processor is added. Use the **change node-names ip** command to configure the IP address of Session Manager and Communication Manager processor. **SM-VM** is the **Name** used for Session Manager and **10.10.97.228** is the **IP Address**. **procr** is the **Name** used for Communication Manager processor and **10.10.97.222** is the **IP Address**. The IP address of Session Manager will be required in **Section 7** while configuring the WFC Voice Client application.

change node-names ip		IP NODE NAMES	
Name	IP Address		
SM-VM	10.10.97.228		
procr	10.10.97.222		

5.3. Configure Network Region

Use the **change ip-network-region x** (where x is the network region to be configured) command to assign an appropriate domain name to be used by Communication Manager. In the example below **bvwdev.com** is used. Note this domain is also configured in **Section 6.1** of these Application Notes.

```
change ip-network-region 1                                     Page 1 of 20

                                IP NETWORK REGION

Region: 1
Location: 1           Authoritative Domain: bvwdev.com
Name:
Stub Network Region: n
MEDIA PARAMETERS
Codec Set: 1          Intra-region IP-IP Direct Audio: yes
UDP Port Min: 2048    Inter-region IP-IP Direct Audio: yes
UDP Port Max: 3329    IP Audio Hairpinning? n
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5    AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS          RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

5.4. Configure IP-Codec-Set

Use the **change ip-codec-set x** (where x is the ip-codec set used) command to designate a codec set compatible with TC51 Workforce Voice Connect clients, which supports **G.711MU**, **G.729**, and **G.711A**.

```
change ip-codec-set 1                                         Page 1 of 2

                                IP CODEC SET

Codec Set: 1

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

5.5. Configure SIP Signaling Group

For the compliance test, a signaling group and the associated SIP trunk group and route was used for connecting Communication Manager with Session Manager. The configuration of SIP trunk group and route is outside the scope of these Application Notes. Only the configuration of the SIP Signaling Group is shown below. For further details on other fields refer to **Section 10**.

Use the **change signaling-group x** (where x is the signaling-group used) command to configure the SIP Signaling Group

- The **Group Type** was set to **sip**.
- The **Transport Method** was set to **tcp**. As a result, the **Near-end Listen Port** and **Far-end Listen Port** are automatically set to **5060**.
- The **Near-end Node Name** was set to **procr**, the node name that maps to the IP address of the circuit pack used to connect to Session Manager. Node names are defined using the **change node-names ip** command (see **Section 5.2**).
- The **Far-end Node Name** was set to **SM-VM**. This node name maps to the IP address of the Session Manager server as defined using the **change node-names ip** command (see **Section 5.2**).
- The **Far-end Network Region** was set to **1**. This is the IP network region which contains Session Manager (see **Section 5.3**).
- The **Far-end Domain** was set to **bvwdev.com**. This domain is sent in the headers of SIP INVITE messages for calls originating from and terminating to Session Manager using this signaling group.
- **Direct IP-IP Audio Connections** was set to **y**. This field must be set to **y** to enable Media Shuffling on the trunk level.
- **Initial IP-IP Direct Media** was set to **y**.

Retain default values for all other fields.

```

display signaling-group 1
                                     Page 1 of 2
                                     SIGNALING GROUP

Group Number: 1                     Group Type: sip
IMS Enabled? n                      Transport Method: tcp
  Q-SIP? n
  IP Video? n                      Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
  Near-end Node Name: procr          Far-end Node Name: SM-VM
  Near-end Listen Port: 5060         Far-end Listen Port: 5060
                                     Far-end Network Region: 1

Far-end Domain: bwvdev.com

Incoming Dialog Loopbacks: eliminate Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload           RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3 Direct IP-IP Audio Connections? y
  Enable Layer 3 Test? y            IP Audio Hairpinning? y
H.323 Station Outgoing Direct Media? n Initial IP-IP Direct Media? y
                                     Alternate Route Timer(sec): 6

```

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager as shown in the reference configuration. All provisioning for Session Manager is performed via the System Manager web interface.

The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

The WFC Voice Clients are added to Session Manager as SIP Users.

Access the System Manager Administration web interface by entering <https://<ip-address>/SMGR> as the URL in an Internet browser, where *<ip-addr>* is the IP address of the System Manager server.

Log in using appropriate credentials.

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.

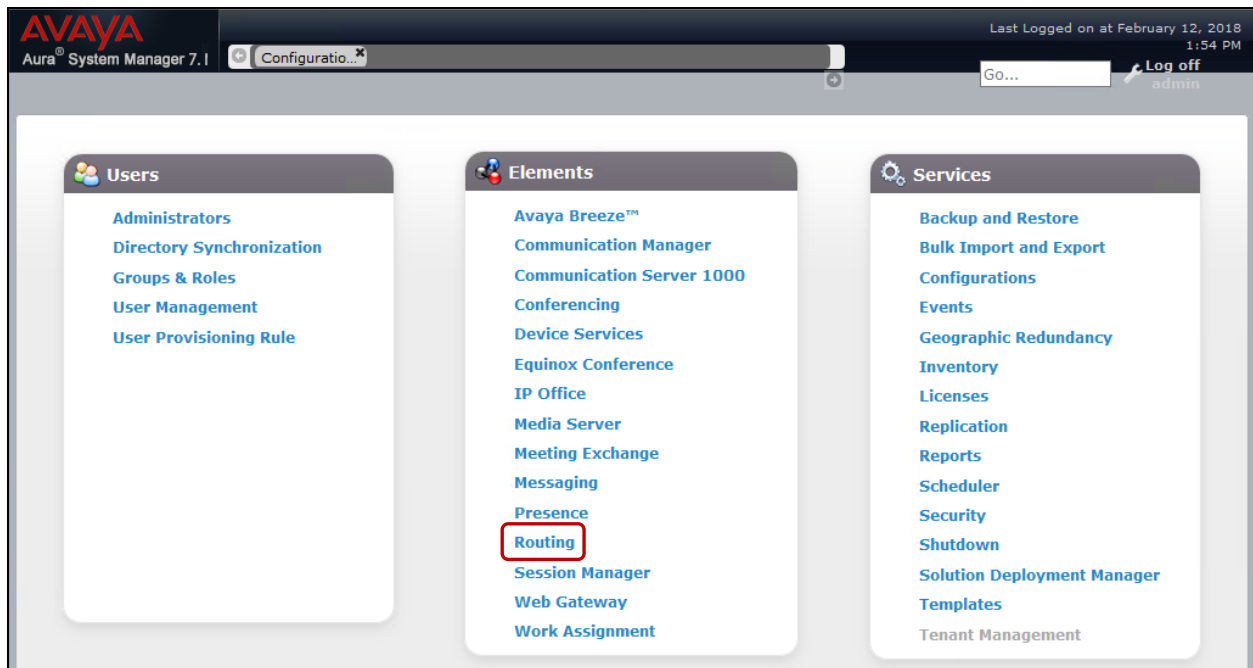
User ID:

Password:

[Change Password](#)

Supported Browsers: Internet Explorer 11.x or Firefox 48.0, 49.0 and 50.0.

The main page for the administrative interface is shown below. Navigate to **Elements** → **Routing** as shown below.



6.1. Configuration of a Domain

Navigate to **Elements → Routing → Domains**, and click the **New** button (not shown) to add the SIP domain with the following:

- **Name:** **bvwdev.com** (as set in **Section 5.3**).
- **Type:** **sip**.
- **Notes:** Optional descriptive text.

Click **Commit** to save the configuration.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The top navigation bar includes the Avaya logo and the text 'Aura System Manager 7.1'. The main navigation menu on the left lists various configuration options: Home, Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The 'Routing' menu is expanded, showing 'Domains' as the selected option. The main content area is titled 'Domain Management' and contains a table with one item, 'bvwdev.com', of type 'sip'. The table has columns for Name, Type, and Notes. The 'Name' column contains 'bvwdev.com', the 'Type' column contains 'sip', and the 'Notes' column is empty. The table is filtered by 'Enable'. The interface also includes 'Commit' and 'Cancel' buttons at the bottom right.

Name	Type	Notes
* bvwdev.com	sip	

6.2. Add Location

Locations identify logical and/or physical locations where SIP entities reside. Only one Location was configured for compliance testing.

Navigate to **Elements → Routing → Locations** and click the **New** button (not shown) to add the Location. Enter the following information:

Under **General**:

- **Name:** A descriptive name
- **Notes:** Optional descriptive text

The Location Pattern is used to identify call routing based on IP address. Session Manager matches the IP address against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern then Session Manager uses the location administered for the SIP Entity.

Under **Location Pattern**, click the **Add** button to add a new line:

- **IP Address Pattern:** Enter the logical pattern used to identify the location. During compliance testing **10.10.5.*** and **10.10.97.*** was used.
- **Notes:** Optional descriptive text.

Click on the **Commit** (not shown) button to save the configuration.

AVAYA
 Aura® System Manager 7.1

Configuratio...

[Home](#)
[Routing](#)

Routing
 Domains
 Locations
 Adaptations
 SIP Entities
 Entity Links
 Time Ranges

Home / Elements / Routing / Locations

Location Details

General

* **Name:**

Notes:

Location Pattern

4 Items
 [Filter: Enable](#)

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.10.5.*	Phones and Servers on private lab network
<input type="checkbox"/>	* 10.10.97.*	Lab PBX

6.3. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP-based telephony system supported by it using SIP trunks. In the sample configuration a SIP Entity is added for the Session Manager and Communication Manager.

Note, the Session Manager SIP Entity is assumed to have already been configured. Navigate to **Elements → Routing → SIP Entities**, check the checkbox for the Session Manager SIP Entity, and click the **Edit** button (not shown). Under the **Port** section, verify the required Session Manager listening ports are configured (i.e. **Port 5060 / Protocol TCP**). If necessary, click the **Add** button to add a listening port and then click **Commit** to save the changes (not shown).

<input type="checkbox"/>	Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input checked="" type="checkbox"/>	5060	TCP	bwvdev.com	<input checked="" type="checkbox"/>	

To add a SIP Entity, navigate to **Elements → Routing → SIP Entities** and click the **New** button (not shown).

The configuration details for the SIP Entity defined for Communication Manager are below:

Under **General**:

- **Name:** A descriptive name.
- **FQDN or IP Address:** **10.10.97.222** is the IP address of the procr used during compliance testing.
- **Type:** Select **CM**.
- **Location:** Select the location configured in **Section 6.2**.
- **SIP Link Monitoring:** Retain the default value, **Use Session Manager Configuration** from the drop down menu.
- **Entity Links:** This was added in a subsequent edit to the Entity record using the **Add** button but is described here for brevity purposes. See **Section 6.4** for how the Entity Link was created.

Default settings can be used for the remaining fields. Click **Commit** to save the SIP Entity definition.

AVAYA
Aura® System Manager 7.1

Configuratio...

HomeRouting

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

* Name:

DevvmCM

* FQDN or IP Address:

10.10.97.222

Type:

CM

Notes:

Lab CM

Adaptation:

Location:

Belleville

Time Zone:

America/Fortaleza

* SIP Timer B/F (in seconds):

4

Minimum TLS Version:

Use Global Setting

Credential name:

Securable:

☐

Call Detail Recording:

both

Loop Detection

Loop Detection Mode:

On

Loop Count Threshold:

5

Loop Detection Interval (in msec):

200

Monitoring

SIP Link Monitoring:

Use Session Manager Configuration

Entity Links

Override Port & Transport with DNS SRV: ☐

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* LinktoDevvmCM_TCP	DevvmSM	TCP	* 5060	DevvmCM	* 5060	trusted	<input type="checkbox"/>

Select : All, None

6.4. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity link. One Entity Link was created:

- Session Manager ↔ Communication Manger

Navigate to **Elements → Routing → Entity Links**, and click the **New** button (not shown) to add a new Entity Link. The screen below shows the configuration details for the Entity Link connecting Session Manager with Communication Manager.

- **Name:** A descriptive name.
- **SIP Entity 1:** Select the Session Manager SIP Entity.
- **Protocol:** Select **TCP** as the transport protocol.
- **Port:** **5060**. This is the port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the Communication Manager SIP Entity.
- **Port: 5060.** This is the port number on which the other system receives SIP requests.
- **Connection Policy:** Select **Trusted**.
- **Notes:** Optional descriptive text.

Click **Commit** to save the configuration.

AVAYA
Aura® System Manager 7.1

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item Filter: Enable

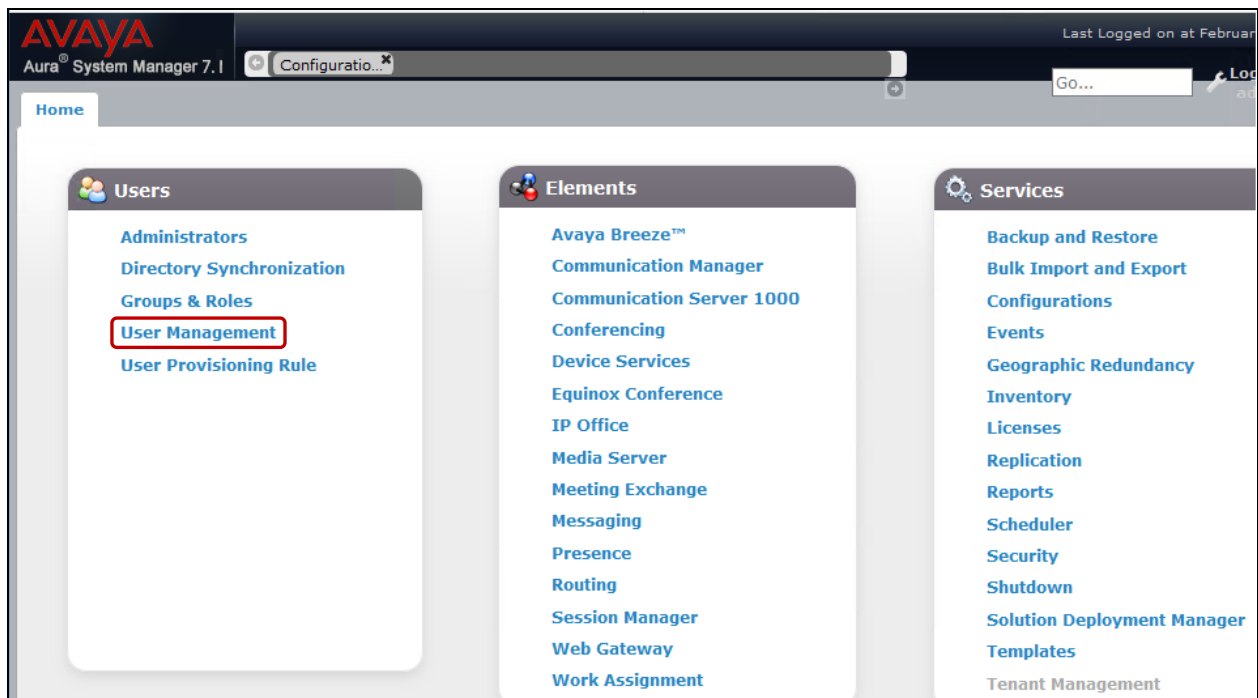
<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy
<input type="checkbox"/>	* LinktoDevvmCM_TCP	* DevvmSM	TCP	* 5060	* DevvmCM	* 5060	<input type="checkbox"/>	trusted

Select : All, None

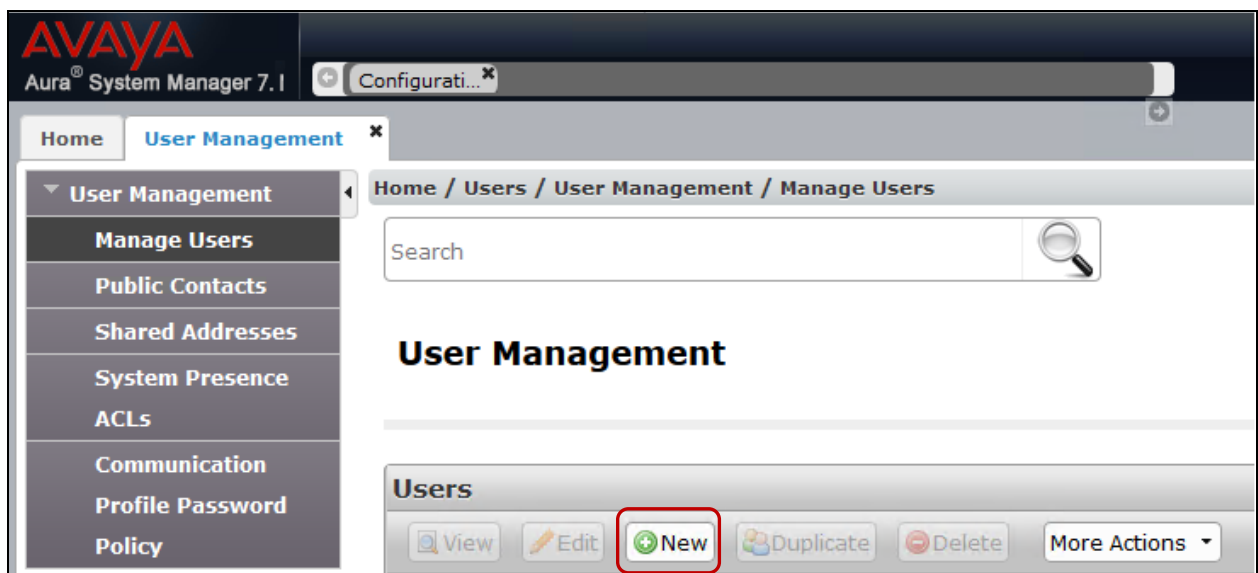
Commit Cancel

6.5. Adding Workforce Connect Voice Client as SIP User

From the main page for the administrative interface of System Manager as shown below, navigate to **Elements** → **User Management**.



Click on **Manage Users** and click on **New** as highlighted below to add a new SIP user.



Under the **Identity** tab, fill in the user's **Last Name** and **First Name** as shown below. Enter the **Login Name** and the **Change Password** configuration is optional. Retain default values for all other fields.

The screenshot shows a web interface with four tabs: Identity (marked with a red asterisk), Communication Profile, Membership, and Contacts. The Identity tab is active, showing a 'User Provisioning Rule' dropdown and an 'Identity' section. The Identity section contains several input fields: Last Name (56217), Last Name (Latin Translation) (56217), First Name (Thirdparty SIP), First Name (Latin Translation) (Thirdparty SIP), Middle Name (empty), Description (empty), Update Time (February 12, 2018 1:56:), Login Name (56217@bvwdev.com), Email Address (empty), and User Type (Basic). A 'Change Password' link is at the bottom.

Identity * Communication Profile Membership Contacts

User Provisioning Rule ▼

User Provisioning Rule: ▼

Identity ▼

* Last Name: 56217

Last Name (Latin Translation): 56217

* First Name: Thirdparty SIP

First Name (Latin Translation): Thirdparty SIP

Middle Name:

Description:

Update Time : February 12, 2018 1:56:

* Login Name: 56217@bvwdev.com

Email Address:

User Type: Basic ▼

[Change Password](#)

Under the **Communication Profile** tab, enter a suitable **Communication Profile Password**. Note that this password is required when configuring the WFC Voice Client in **Section 7**. Under **Communication Address** click on **New** to add a new communication address. Select **Type** as **Avaya SIP** and enter the extension number and the domain for the **Fully Qualified Address** and click on **Add** once finished.

The screenshot shows a web-based configuration interface with four tabs: Identity, Communication Profile, Membership, and Contacts. The 'Communication Profile' tab is active. It contains a 'Communication Profile' section with fields for 'Communication Profile Password' and 'Confirm Password', both masked with dots. A 'Generate' link is next to the confirm password field. Below this is a 'Communication Address' section. It has a toolbar with 'New', 'Delete', 'Done', and 'Cancel' buttons. A table below the toolbar has a single row with 'Primary' selected. Below the table, there is a 'Name' field with 'Primary' entered and a 'Default' checkbox which is checked. At the bottom of the 'Communication Address' section, there is a 'New' button (highlighted with a red box), 'Edit', and 'Delete' buttons. Below these is a table with columns 'Type', 'Handle', and 'Domain'. The table is empty, showing 'No Records found'. Below the table, there is a 'Type' dropdown menu set to 'Avaya SIP'. Below that is a 'Fully Qualified Address' field with '56217' entered, followed by an '@' symbol and a 'Domain' dropdown menu set to 'bvwddev.com'. At the bottom right of this section are 'Add' and 'Cancel' buttons.

Identity * Communication Profile Membership Contacts

Communication Profile

Communication Profile Password: Password:

Confirm Password: [Generate](#)

Communication Address

Name
Primary

Select : None

* Name: Primary

Default : ☒

Communication Address

Type	Handle	Domain
No Records found		

Type: Avaya SIP

* Fully Qualified Address: 56217 @ bvwddev.com

Ensure **Session Manager Profile** is checked and enter the **Primary Session Manager** details, enter the **Origination Sequence**, the **Termination Sequence** and the **Home Location** as highlighted below. Note that **DevvmCM_AppSeq** is an application sequence that corresponds to the Communication Manager in the test configuration and has been configured in the system previously. In the screen below, **Max. Simultaneous Devices** is set at the default value. Administrator can change this depending on how many simultaneous devices want to register as the same user.

☒ **Session Manager Profile**

SIP Registration

* Primary Session Manager

Secondary Session Manager

Survivability Server

Max. Simultaneous Devices

1

Block New Registration When Maximum Registrations Active?

☐

Primary	Secondary	Maximum
20	0	20

Application Sequences

Origination Sequence

Termination Sequence

Emergency Calling Application Sequences

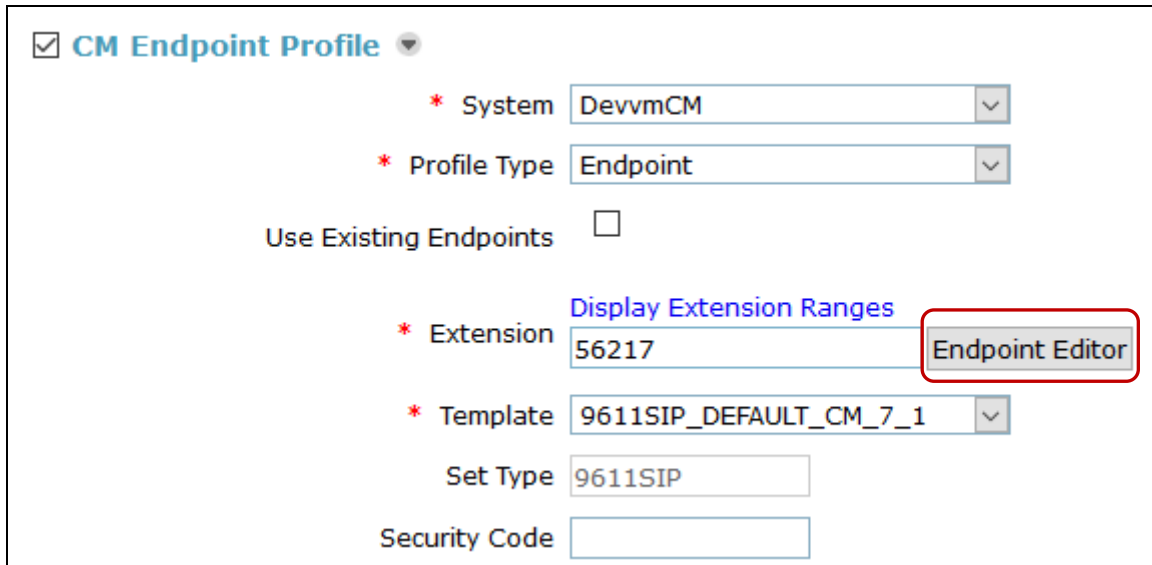
Emergency Calling Origination Sequence

Emergency Calling Termination Sequence

Call Routing Settings

* Home Location

Ensure that **CM Endpoint Profile** is selected. Select **DevvmCM** as **System** and **Endpoint** for **Profile Type**. Enter **56217** for **Extension** and choose the **9611SIP_DEFAULT_CM_7_1** as the **Template**. Click **Endpoint Editor** to configure the buttons and features for that handset on Communication Manager.




The screenshot shows a web-based configuration form for a 'CM Endpoint Profile'. At the top, there is a checked checkbox labeled 'CM Endpoint Profile' with a dropdown arrow. Below this, the form contains several fields and a button:

- A red asterisk followed by the label 'System' and a dropdown menu showing 'DevvmCM'.
- A red asterisk followed by the label 'Profile Type' and a dropdown menu showing 'Endpoint'.
- The text 'Use Existing Endpoints' followed by an unchecked checkbox.
- A red asterisk followed by the label 'Extension' and a text input field containing '56217'. Above this field is a blue link 'Display Extension Ranges'. To the right of the input field is a button labeled 'Endpoint Editor', which is highlighted with a red rectangular border.
- A red asterisk followed by the label 'Template' and a dropdown menu showing '9611SIP_DEFAULT_CM_7_1'.
- The text 'Set Type' followed by a text input field containing '9611SIP'.
- The text 'Security Code' followed by an empty text input field.

Edit Endpoint

[\[Save As Template\]](#)

System	<input type="text" value="DevvmCM"/>	Extension	<input type="text" value="56217"/>
Template	<input type="text" value="9611SIP_DEFAULT_CM_7_1"/> ▼	Set Type	<input type="text" value="9611SIP"/> 
Port	<input type="text" value="IP"/>	Security Code	<input type="text"/>
Name	<input type="text" value="56217,ThirdParty SIP"/>		

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

Button Assignment (B)
Profile Settings (P)
Group Membership (M)


Main Buttons
Feature Buttons
Button Modules

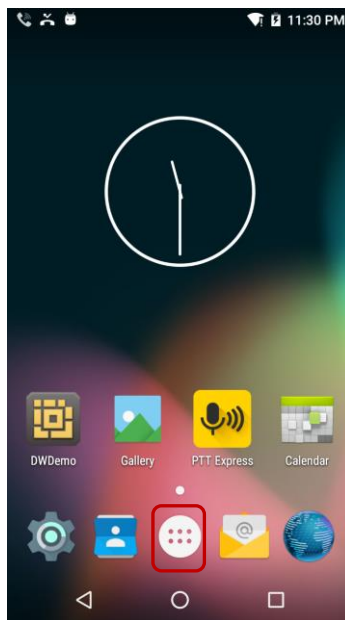
Endpoint Configurations		Button Configurations			
Favorite	Button Label	Button Feature	Argument-1	Argument-2	Argument-3
9 <input type="checkbox"/>	<input type="text"/>	auto-cback ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
10 <input type="checkbox"/>	<input type="text"/>	call-fwd ▼ Extension	<input type="text"/>	<input type="text"/>	<input type="text"/>
11 <input type="checkbox"/>	<input type="text"/>	cfwd-bsyda ▼ Extension	<input type="text"/>	<input type="text"/>	<input type="text"/>
12 <input type="checkbox"/>	<input type="text"/>	call-park ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
13 <input type="checkbox"/>	<input type="text"/>	call-unpk ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
14 <input type="checkbox"/>	<input type="text"/>	call-pkup ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
15 <input type="checkbox"/>	<input type="text"/>	dir-pkup ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
16 <input type="checkbox"/>	<input type="text"/>	ext-pkup ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
17 <input type="checkbox"/>	<input type="text"/>	exclusion ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>
18 <input type="checkbox"/>	<input type="text"/>	priority ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>

7. Configure Workforce Connect Voice Client

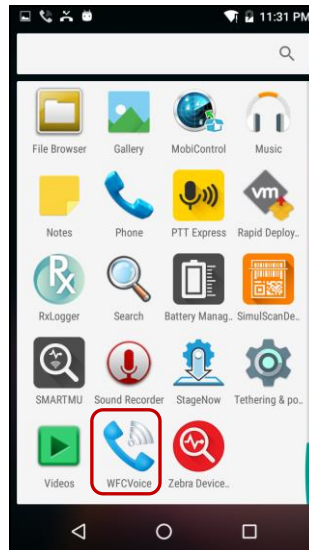
This section provides the procedures for configuring the WFC Voice Client for SIP connectivity to Avaya Aura® Communication Manager and Avaya Aura® Session Manager.


Note: Connecting the TC51 Android-based voice-enabled touch computer to the wireless network and configuring feature buttons on the WFC Voice Client are outside the scope of these Application Notes.

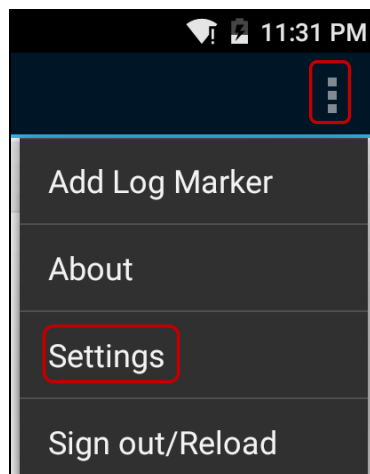
Power on the WFC Voice Client and unlock the TC51 Android-based voice-enabled touch computer. The following screen is displayed. Tap on the  button, highlighted below.




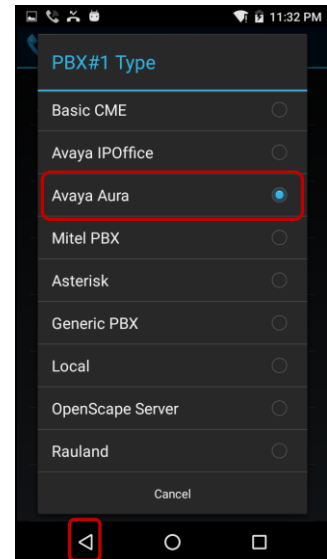
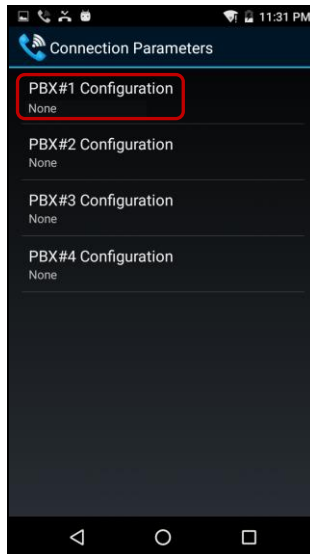
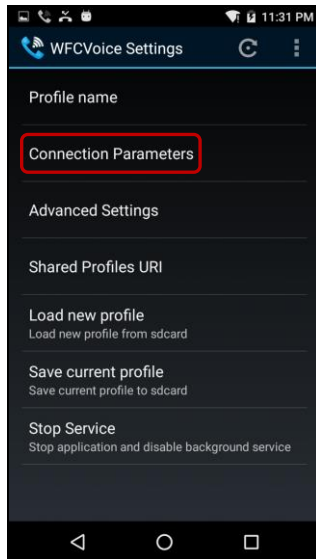
Scroll through the applications until the **WFCVoice** application is seen. Tap the **WFCVoice** button.



From the **WFCVoice** screen shown below, tap the  button on the TC51 Android-based voice-enabled touch computer to display the menu below. From the menu presented, tap on the **Settings** option.



The **WFCVoice Settings** screen is displayed. Tap on the **Connection Parameters** and then on the **PBX#1 Configuration** option. In the **PBX#1 Type** screen select **Avaya Aura** as shown below and then tap on the  button.



In the resulting **PBX#1 Configuration** screen shown below, tap on the following fields and configure them as follows. Tap on the ◀ button until the main screen of WFC Voice client is seen to complete the configuration.

Field Name	Description
User ID	Specify the SIP extension configured in Section 6.5 . In this example, the SIP extension was 56217 . This is the SIP extension that WFC Voice client will use to register with Session Manager.
Password	Specify the SIP password configured on Session Manager in Section 6.5 . WFC Voice client will use this password to register with Session Manager.
SIP transport	Select TCP .
Server Address	This is the IP address of Session Manager. In this example, the address is 10.10.97.228 .

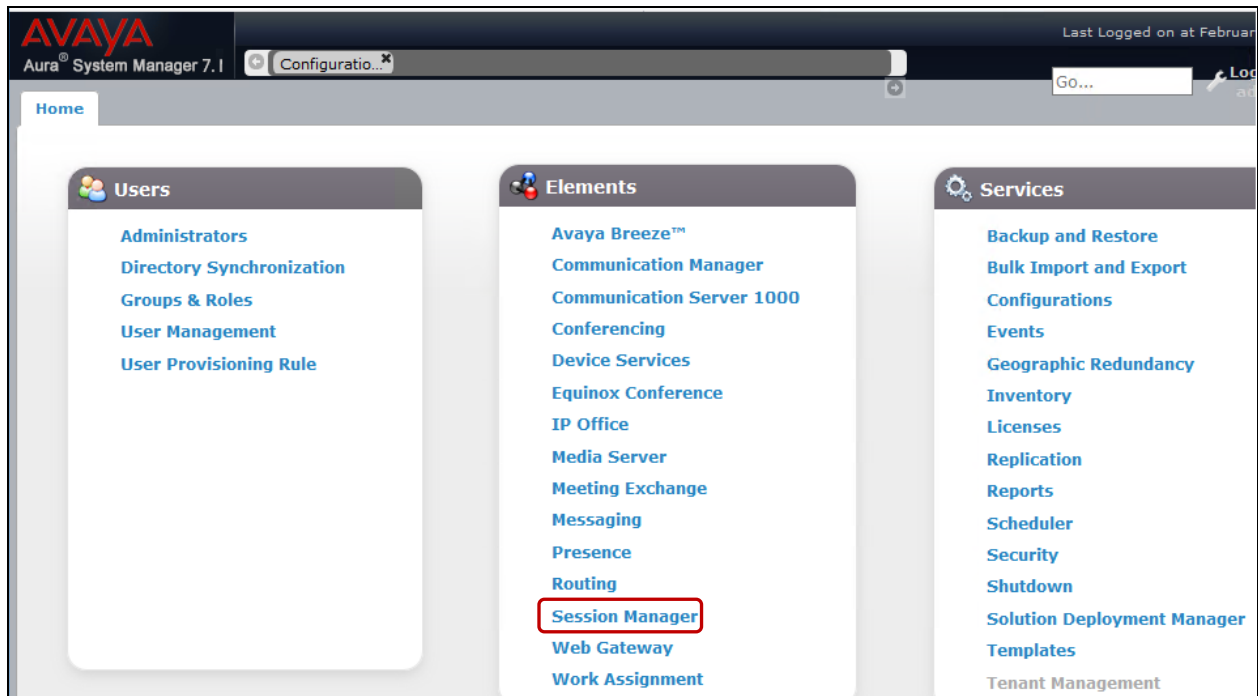
The screenshot displays the 'PBX#1 Configuration' screen. The fields and their values are as follows:

- PBX#1 Type:** Avaya Aura
- PBX Line Logo:** (empty field)
- SIP ID:** (empty field)
- User ID:** 56217
- Password:** *****
- SIP transport:** TCP
- Device MAC:** (empty field)
- Server Address:** 10.10.97.228

8. Verification Steps

The following steps can be taken to ensure that connections between WFC Voice Client and Session Manager and Communication Manager are up.

Log into System Manager as done previously in **Section 6** and navigate to **Elements → Session Manager** as shown below.



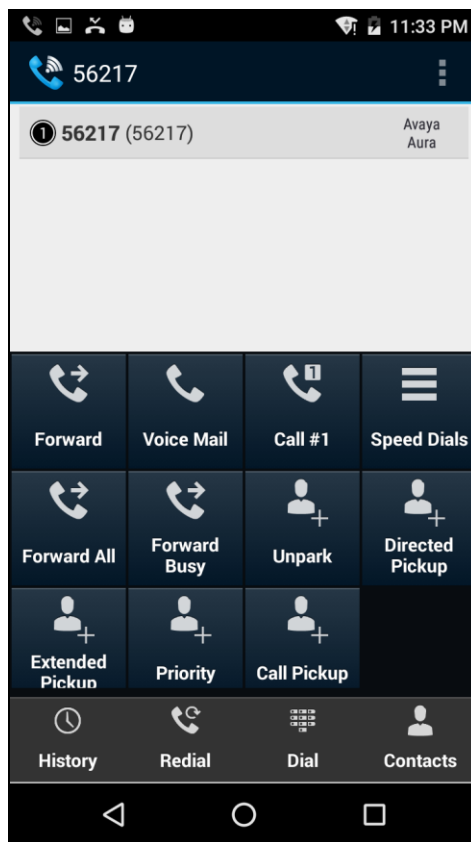
Navigate to **System Status → User Registrations** in the left column. This screen displays the users that are currently registered with Session Manager. The WFC Voice client user **56217** is shown below as being registered.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The left sidebar contains a navigation menu with the following items: Session Manager (expanded), Dashboard, Session Manager Administration, Global Settings, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, System Status (expanded), SIP Entity Monitoring, Managed Bandwidth Usage, Security Module Status, SIP Firewall Status, Registration Summary, and User Registrations (selected). The main content area is titled "User Registrations" and includes a sub-header "Select rows to send notifications to devices. Click on Details column for complete registration status." Below this is a table with 19 items. The table has columns: Details, Address, First Name, Last Name, Actual Location, IP Address, Remote Office, Shared Control, Simult. Devices, AST Device, Registered Prim, and Registered Sec. The first row shows a user with ID 56217, address 56217@bvwddev.com, first name Thirdparty, last name SIP, actual location Belleville, IP address 10.10.5.53, remote office checkbox, shared control checkbox, simultaneous devices 1/1, AST device checkbox, and registered status Prim (checked) and Sec (unchecked). The table also includes a "Show" button and a "Filter: Enable" dropdown.

Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered Prim	Registered Sec
Show	56217@bvwddev.com	Thirdparty	SIP	Belleville	10.10.5.53	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>

Launch WFCVoice application and verify that the SIP extension has been registered. When WFCVoice application is registered with Session Manager, it would display the SIP extension as shown below without any other error status information along with the feature buttons configured.

Verify basic telephony features by establishing incoming and outgoing calls with the WFC Voice Client and also verify that the feature buttons that were mentioned in **Section 1** are working as intended.



9. Conclusion

These Application Notes describe the integration of the Zebra Technologies Workforce Connect Voice Client running on a TC51 touch computer with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. The Workforce Connect Voice Client registered successfully with Avaya Aura® Session Manager as a SIP endpoint through the enterprise wireless LAN.

Incoming and outgoing calls were placed to/from the WFC Voice Clients and telephony features were exercised. All test cases passed with observations noted in **Section 2.2**.

10. References

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

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

1. *Deploying Avaya Aura® Session Manager*, Release 7.1.2, Issue 4 December 2017
2. *Administering Avaya Aura® Session Manager*, Release 7.1.2, Issue 3 December 2017
3. *Deploying Avaya Aura® System Manager*, Release 7.1.2, Issue 5 January 2018
4. *Administering Avaya Aura® System Manager for Release 7.1.2*, Release 7.1.2, Issue 10 January 2018
5. *Deploying Avaya Aura® communication Manager*, Release 7.1.2, Issue 3 December 2017
6. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.1.2, Issue 4 January 2018

Product Documentation for Zebra Technologies can be obtained from a product supplier or may be accessed at <https://www.zebra.com/> (login required).

1. *TC51 Touch Computer Quick Start Guide*.
2. *TC51 Touch Computer User Guide for Android™*.

©2018 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.