



Avaya Solution & Interoperability Test Lab

Application Notes for Tenacity ipTTY with Avaya Aura[®] Session Manager and Avaya Aura[®] Communication Manager - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring the Tenacity ipTTY to interoperate with Avaya Aura[®] Session Manager 7.0 and Avaya Aura[®] Communication Manager 7.0.

The overall objective of the interoperability compliance testing was to verify Tenacity ipTTY functionalities in an environment comprised of Avaya Aura[®] Session Manager, Avaya Aura[®] Communication Manager, and various SIP and H.323 IP Deskphones.

Readers should pay attention to **Section** Error! Reference source not found., in particular the scope of testing as outlined in **Section** Error! Reference source not found. as well as any observations noted in **Section** Error! Reference source not found., 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 procedure for configuring Tenacity ipTTY to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

Tenacity ipTTY is engineered to enable TTY communications using an existing VoIP/Hybrid PBX infrastructure. The only requirement from the infrastructure is support for 3rd party SIP devices. With Tenacity ipTTY, there is no longer a need for outdated TTY machines or expensive computer modems. Most importantly, with ipTTY, analog telephone lines are not required to facilitate TTY communications. Additionally, the ipTTY supports Hearing Carry Over (HCO), Voice Carry Over (VCO), includes a multi-lined display (versus a single lined display like standard TTY machines) and offers a recent calls list.

2. General Test Approach and Test Results

The focus of the interoperability compliance testing was to verify the ability of the Tenacity ipTTY solution to interoperate with an Avaya SIP-enabled IP Telephony environment comprised of Avaya Aura® Session Manager, Avaya Aura® Communication Manager and various Avaya phones including SIP and H.323.

The feature test cases were performed manually by making calls to/from ipTTY devices, and verify features of ipTTY devices.

The serviceability test cases were performed manually by disconnecting/reconnecting Ethernet connection to ipTTY installed PC, and stop/restarting the ipTTY application.

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 features and serviceability. The focus of the interoperability compliance testing was primarily on verifying call establishment on the Tenacity ipTTY with Avaya devices and PSTN. The feature testing focused on verifying the following on ipTTY:

- Register to Session Manager
- Send/receive text accuracy, inbound voice calls (call connection and termination)
- Inbound/outbound voice calls (call connection and termination)
- Call transfer
- Call forward
- DTMF
- Leaving/retrieving voicemail

The serviceability testing introduced failure scenarios to see if Tenacity ipTTY can recover from failures.

2.2. Test Results

All test cases were executed, and the following was observed on ipTTY:

During process of retrieving voicemail, an issue was noticed intermittently where the ipTTY did not display the message to enter a password. The user could still send the password to Avaya Aura Messaging and retrieve his messages by looking at the log screen below. This happened infrequently and is not expected to be a highly used feature. It was reported to Tenacity.

2.3. Support

Technical support for Tenacity ipTTY solution can be obtained by contacting Tenacity:

- Email – support@accessaphone.com
- Phone – (866) 756-0321

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of Communication Manager, an Avaya G450 Media Gateway (and/or Avaya Aura® Media Server), Session Manager, System Manager, various Avaya IP deskphones, and Tenacity ipTTY. Communication Manager, Session Manager, System Manager, and Avaya Aura® Media Server were all installed in a virtual environment. Tenacity ipTTY was installed on Windows 7. The solution described herein is also extensible to other Avaya Servers and Media Gateways.

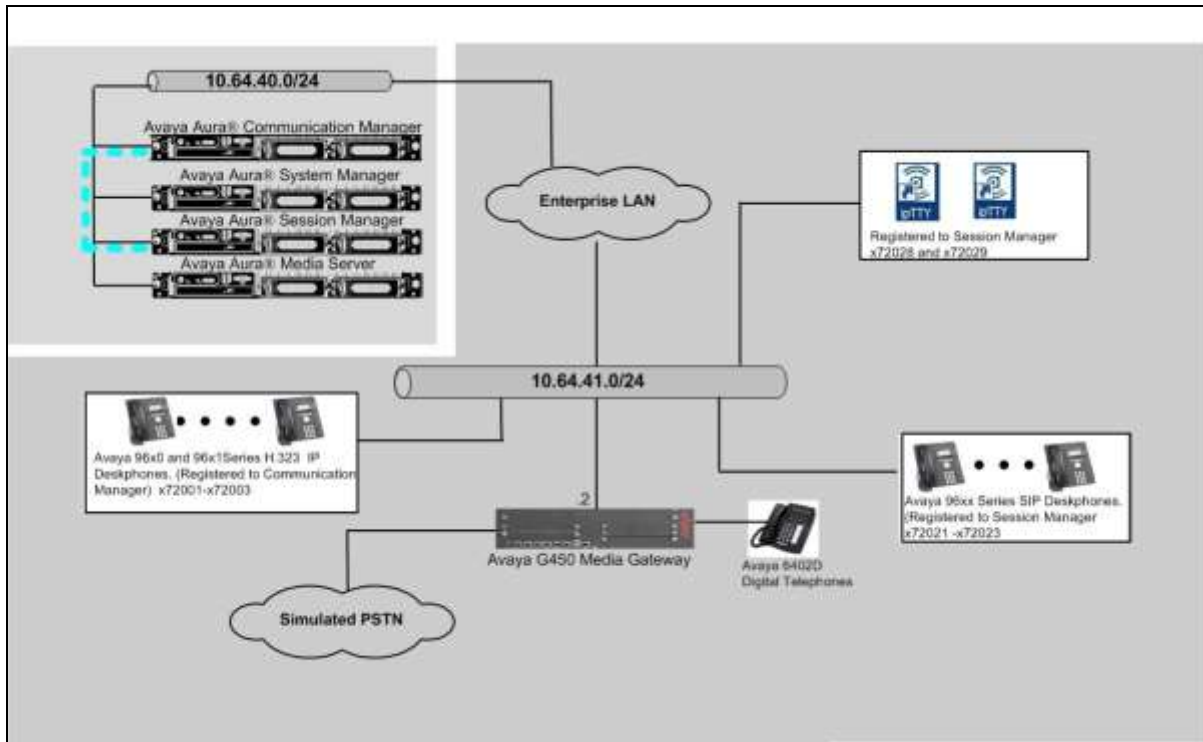


Figure 1: Test Configuration of Tenacity ipTTY

4. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya Aura® Communication Manager		7.0.1.0 FP1 (R017x.00.0.441.0-23012)
Avaya G450 Media Gateway		37.19
Avaya Aura® Media Server		7.7.0.226
Avaya Aura® System Manager		7.0.1 (7.0.1.0.64859)
Avaya Aura® Session Manager		7.0
Avaya 96x1 Series SIP Telephones		
	9641 (SIP)	7.0.0.39
	9611 (SIP)	7.0.0.39
Avaya 9600 Series IP Telephones		
	9621G (H.323)	6.6.115
	9650C (H.323)	3.25
Tenacity ipTTY		2.0.3.3

5. Configure Avaya Aura® Communication Manager

During the compliance test, assumptions were made that the following were already installed, and the basic configuration, included below, was performed:

- Communication Manager License
- IP Codec Set
- IP Network Region
- IP Node Name
- SIP Signaling Group (between Communication Manager and Session Manager)
- SIP Trunk Group (between Communication Manager and Session Manager)
- Route Pattern
- Private Numbering
- AAR Analysis

6. Configure Avaya Aura® Session Manager

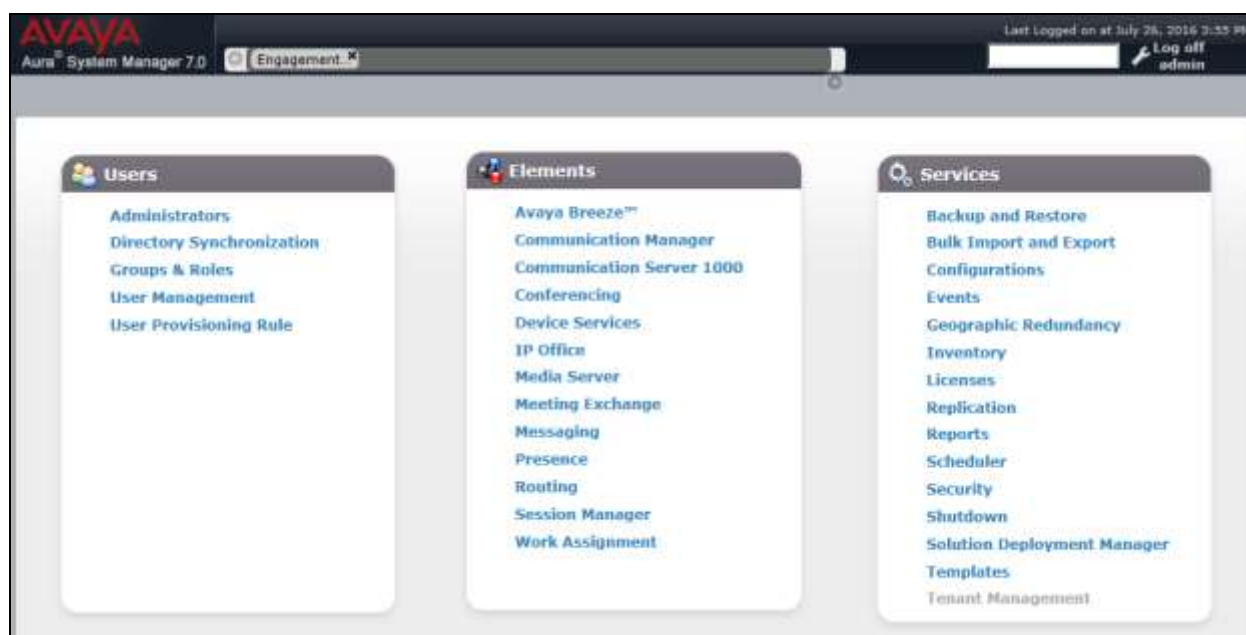
Session Manager is comprised of two functional components: the Session Manager server and the System Manager server. All SIP call provisioning for Session Manager is performed through the System Manager Web interface. System Manager delivers a set of shared, secure management services and a common console across multiple products in the Avaya Aura® network, including the central administration of routing policies, and a common format for logs and alarms.

This section assumes that Session Manager and System Manager have been installed, network connectivity exists between the two platforms, and the following basic configuration was performed.

- SIP Domains
- Locations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policy
- Dial Patterns
- Manage Element
- Applications
- Application Sequence

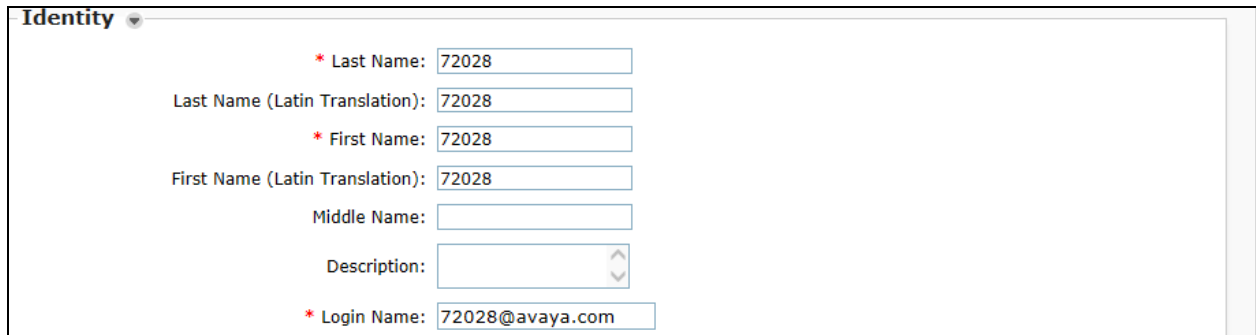
Thus, this section only provides the procedures for configuring users for ipTTY devices.

Using a web browser, access <https://<ip-addr of System Manager>/SMGR>. Log in using appropriate credentials. The main page for the web interface is shown below.



To add new SIP users, Navigate to **Home / Users / User Management / Manage Users**. Click **New (not shown)** and provide the following information:

- Identity section
 - **Last Name** – Enter last name of user.
 - **First Name** – Enter first name of user.
 - **Login Name** – Enter extension number@sip domain.

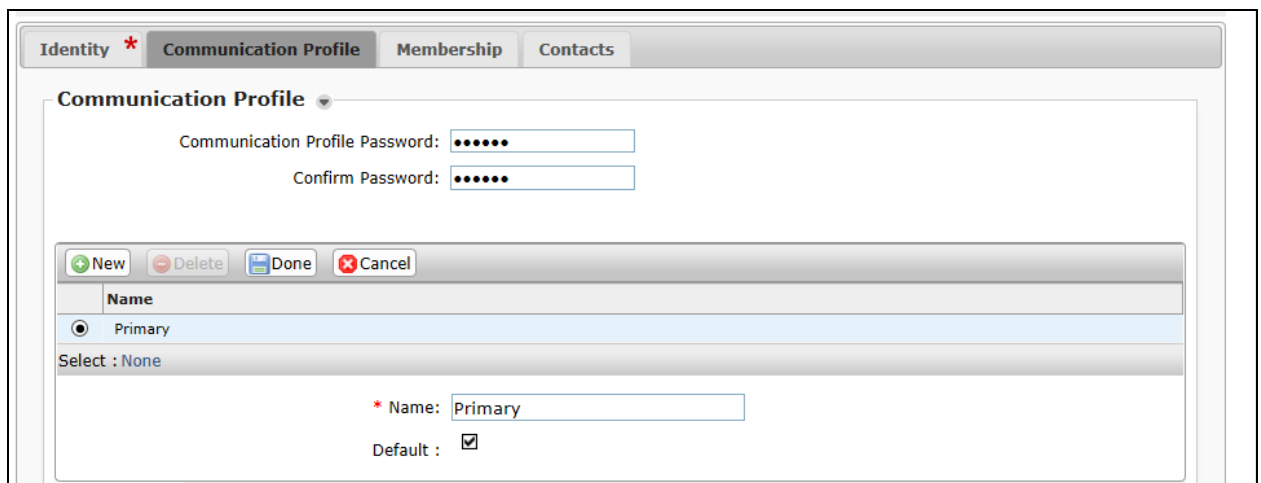


The screenshot shows the 'Identity' section of a user management interface. It contains several input fields: 'Last Name' (72028), 'Last Name (Latin Translation)' (72028), 'First Name' (72028), 'First Name (Latin Translation)' (72028), 'Middle Name' (empty), 'Description' (empty), and 'Login Name' (72028@avaya.com). Each field is preceded by an asterisk indicating it is required.

- Communication Profile section
 - **Communication Profile Password** – Enter a numeric value used to logon to SIP telephone.
 - **Confirm Password** – Repeat numeric password.

Verify there is a default entry identified as the **Primary** profile for the new SIP user. If an entry does not exist, select **New** and enter values for the following required attributes:

- **Name** – Enter **Primary**.
- **Default** – Enter



The screenshot shows the 'Communication Profile' section of a user management interface. It includes tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active. It contains two password fields: 'Communication Profile Password' and 'Confirm Password', both masked with dots. Below these is a table with columns for 'Name' and 'Select'. The 'Primary' entry is selected. Below the table, there is a 'Name' field with the value 'Primary' and a 'Default' checkbox which is checked.

- Communication Address sub-section

Select **New** to define a **Communication Address** for the new SIP user, and provide the following information.

 - **Type** – Select **Avaya SIP** using the drop-down menu.
 - **Full Qualified Address** – Enter same extension number and domain used for Login Name, created previously.

Click the **Add** button to save the Communication Address for the new SIP user.

- Session Manager Profile section
 - **Primary Session Manager** – Select one of the Session Managers.
 - **Secondary Session Manager** – Select **(None)** from drop-down menu.
 - **Origination Application Sequence** – Select Application Sequence defined for Communication Manager in System Manager.
 - **Termination Application Sequence** – Select Application Sequence defined for Communication Manager in System Manager.
 - **Survivability Server** – Select **(None)** from drop-down menu.
 - **Home Location** – Select Location defined in **Home → Routing → Locations**.

- Endpoint Profile section
 - **System** – Select Managed Element defined for Communication Manager in System Manager.
 - **Profile Type** – Select “Endpoint”.
 - **Use Existing Endpoints** - Leave unchecked to automatically create new endpoint when new user is created. Or else, check the box if endpoint is already defined in Communication Manager.
 - **Extension** - Enter same extension number used for Login Name previously.
 - **Template** – Select template for type of SIP phone.
 - **Security Code** – Enter numeric value used to logon to SIP telephone. (**Note:** this field must match the value entered for the Shared Communication Profile Password field.
 - **Port** – Select **IP** from drop down menu.
 - **Voice Mail Number** – Enter Pilot Number for Avaya Modular Messaging if installed. Or else, leave field blank.

- Use the default value for remaining fields.

CM Endpoint Profile ▼

* System ▼

* Profile Type ▼

Use Existing Endpoints

* Extension

Template ▼

Set Type

Security Code

Port

Voice Mail Number

Preferred Handle ▼

Calculate Route Pattern

Sip Trunk

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

Allow H.323 and SIP Endpoint Dual Registration

Click **Commit** to save definition of new user. The following screen shows the created users during the compliance test. The highlight shows users created for the ipTTY endpoints.

The screenshot shows the Avaya System Manager 7.0 User Management interface. The breadcrumb trail is Home / Users / User Management / Manage Users. The main content area displays a table of users with the following data:

Last Name	First Name	Display Name	Login Name	SIP Handle	Last Login
admin	admin	Default Administrator	admin		July 20, 2016 9:57:21 AM -06:00
72028	72028	72028	72028@avaya.com	72028	
72029	72029	72029	72029@avaya.com	72029	
SIP	72023	SIP, 72023	72023@avaya.com	72023	
SIP	station1	SIP, station1	72021@avaya.com	72021	
SIP	Station2	SIP, Station2	72022@avaya.com	72022	

7. Configure Avaya Aura® Messaging

In Avaya Aura® Messaging, there are two ways to test the ipTTY solution. One is to make users as ipTTY compatible. The other is, creating a site for ipTTY. For the compliance test, the latter is used. To enable ipTTY on Avaya Aura® Messaging, a language pack called “en-US TTY” needs to be installed on Avaya Aura® Messaging.

The following screen shows the language pack is downloaded. Select the language pack for the site. Select “en-US TTY” for the **System Language** and **Default Subscriber UI Language** fields.

The screenshot shows the Avaya Aura® Messaging System Management Interface (SMI) Administration page for Languages. The page is titled "Languages" and is part of the "Administration / Messaging" section. The left sidebar contains a navigation menu with categories like Reports (Storage), Server Information, Server Settings, and IMAP/SMTP Settings (Storage). The main content area is divided into several sections:

- Language Packs:** A table showing installed language packs. The table has two columns: "Name" and "User Selectable".
- Language Settings:** Fields for "System Language:" and "Default Subscriber UI Language:", both set to "en-US TTY (American English)".
- Language Packs (Current Application software release):** Shows the current software release as "6.3.141.348-1.258129" and an "Add Language Pack:" section with a "Browse..." button and an "Upload" button.
- Delete Language Pack:** A section with a dropdown menu set to "en-US TTY (American English)" and a "Delete" button.

Name	User Selectable
en-US (American English) 6.3.3.2	<input type="checkbox"/>
en-US TTY (American English) 6.3.3.5.3	<input checked="" type="checkbox"/>

Navigate to **Managing System (Storage) → User Management** on the left pane, and create a user, 72028. Select **TTY** for the **Class of Service** field, as shown below.

AVAYA Avaya Aura® Messaging System Management Interface (SMI)

Help Log Off Administration This Server: server1

Administration / Messaging

Managing System (Storage)

- User Management
- Class of Service
- Sites
- Topology
- Storage Destinations
- System Policies
- Enhanced List Management
- System Mailboxes
- System Administration
- User Activity Log Configuration

Reports (Storage)

- Users
- Info Mailboxes
- Remote Users
- Uninitialized Mailboxes
- Login Failures
- Locked Out Users
- Sites
- Dormant Mailboxes
- Full Mailboxes
- Web Access

Server Information

- System Status
- Alarm Summary
- Voice Channels (Application)
- Cache Statistics (Application)
- Outbound Fax (Storage)

Server Settings

- Server Role / AxC Address

Server Settings (Storage)

- External Hosts
- Trusted Servers
- Networked Servers
- Request Remote Update

Server Settings (Application)

- Dial Rules
- Cluster
- System Parameters
- Languages
- Log Configuration

IMAP/SMTP Settings (Storage)

- General Options
- Mail Options
- IMAP/SMTP Status

Telephony Settings

- Telephony Integration
- Telephony Domains

Advanced (Application)

User Management > Properties for test 72028

User Properties

First name: test

Last name: 72028

Display name: test

ASCII name: test72028

Site: Default

Mailbox number: 72028

Email address: 72028@server1

Numeric address: 72028

Extension: 72028

Include in Auto Attendant directory

Additional extension 1:

Additional extension 2:

Additional extension 3:

Additional extension 4:

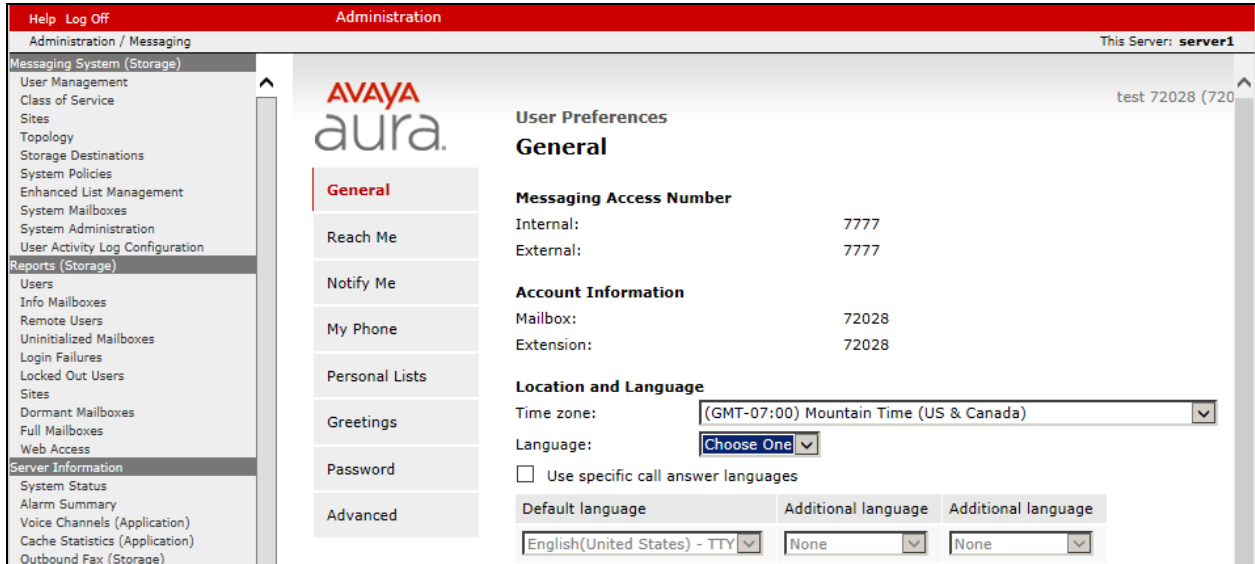
Additional extension 5:

Additional extension 6:

Additional extension 7:

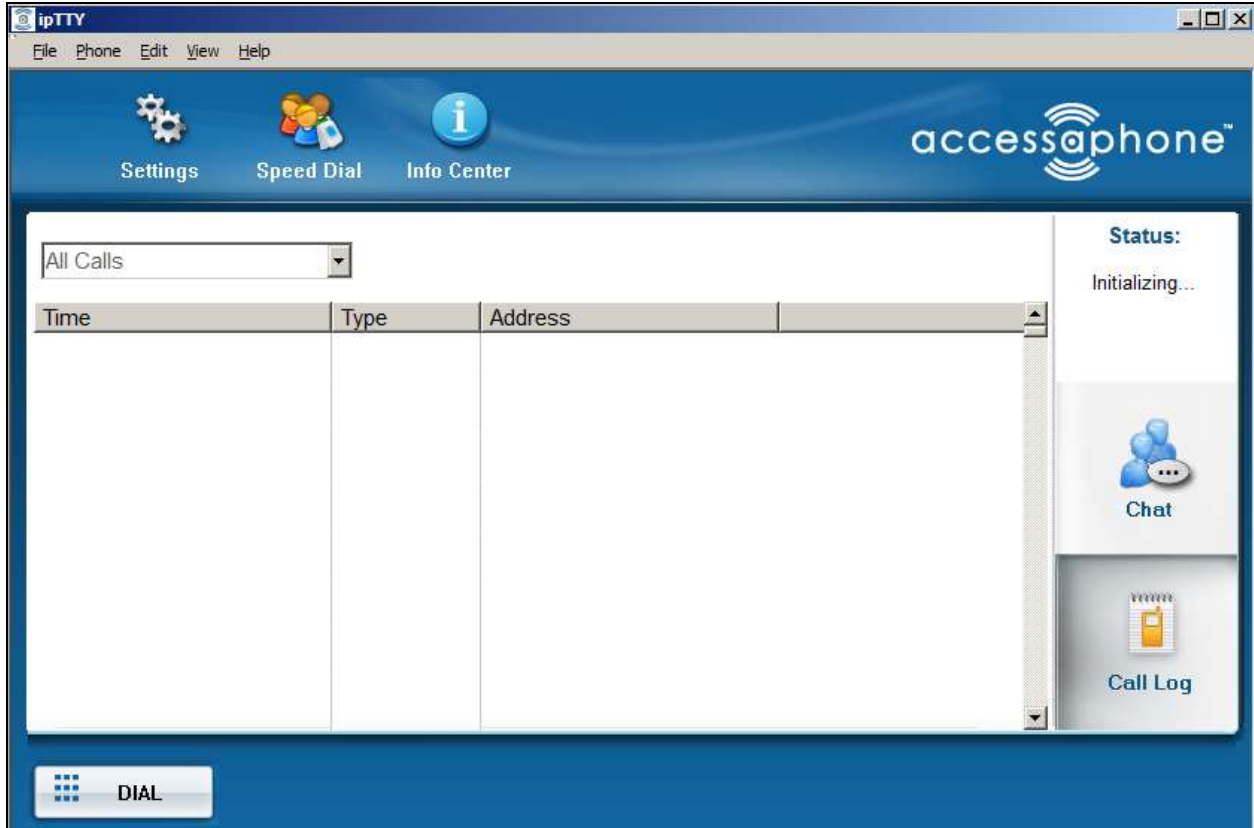
Class of Service: TTY

Navigate to **Reports (Storage) → Users**. On the **Report** page (not shown), select the user created previously (not shown). On the **User Management > Properties for test 72028** page, select “Open User Preference for test 72028” under the **User Preference** section. The User Preferences page is displayed. Verify “English(United States) – TTY” is set for **Default Language**.



8. Configure Tenacity ipTTY

This section provides steps to configure Tenacity ipTTY. The latest firmware was provided by Tenacity. To start the Tenacity ipTTY application, double click the ipTTY icon (📞). Select the **Settings** button to configure the ipTTY for interfacing with Session Manager.

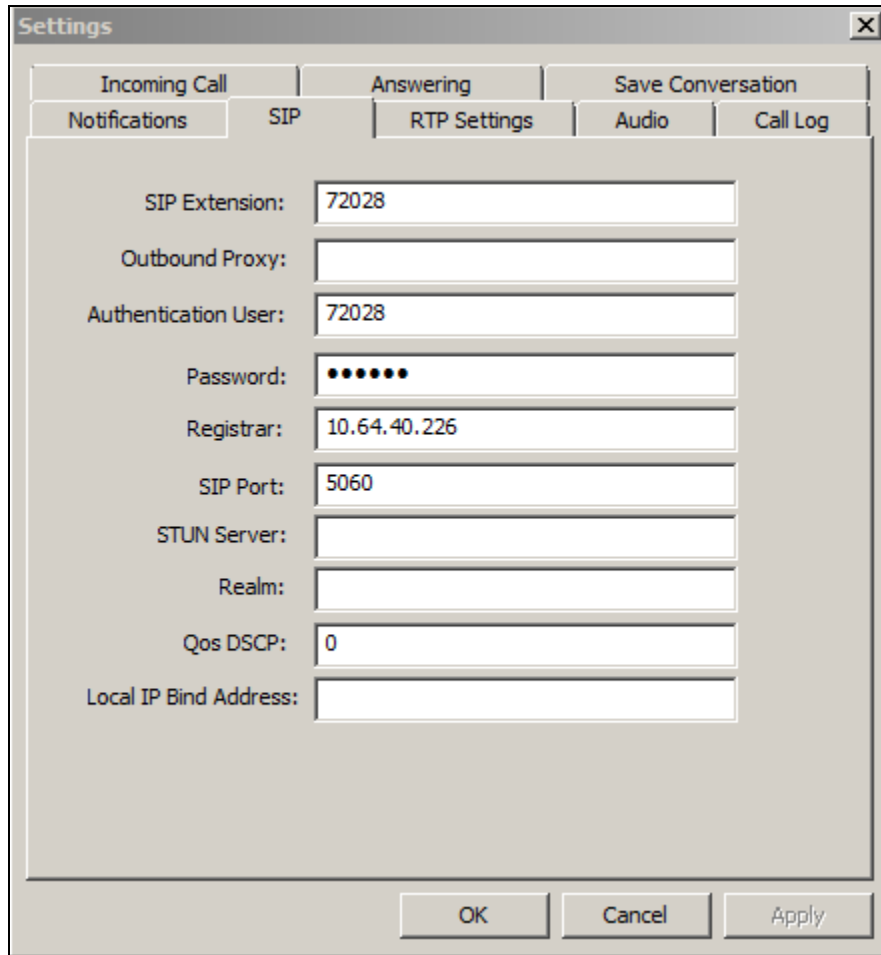


On the **Settings** page, select the **SIP** tab, and provide the following information:

- SIP Extension – Enter the user extension created in **Section 6**.
- Authentication User – username (usually the same as the SIP Extension).
- Password – Enter the password created in **Section 6**.
- Registrar – Enter the IP address of Session Manager.
- SIP Port – The default port is utilized.

Click on the **OK** button, after the completion.

Note: In order for the settings to take effect, the ipTTY must be closed and reopened.

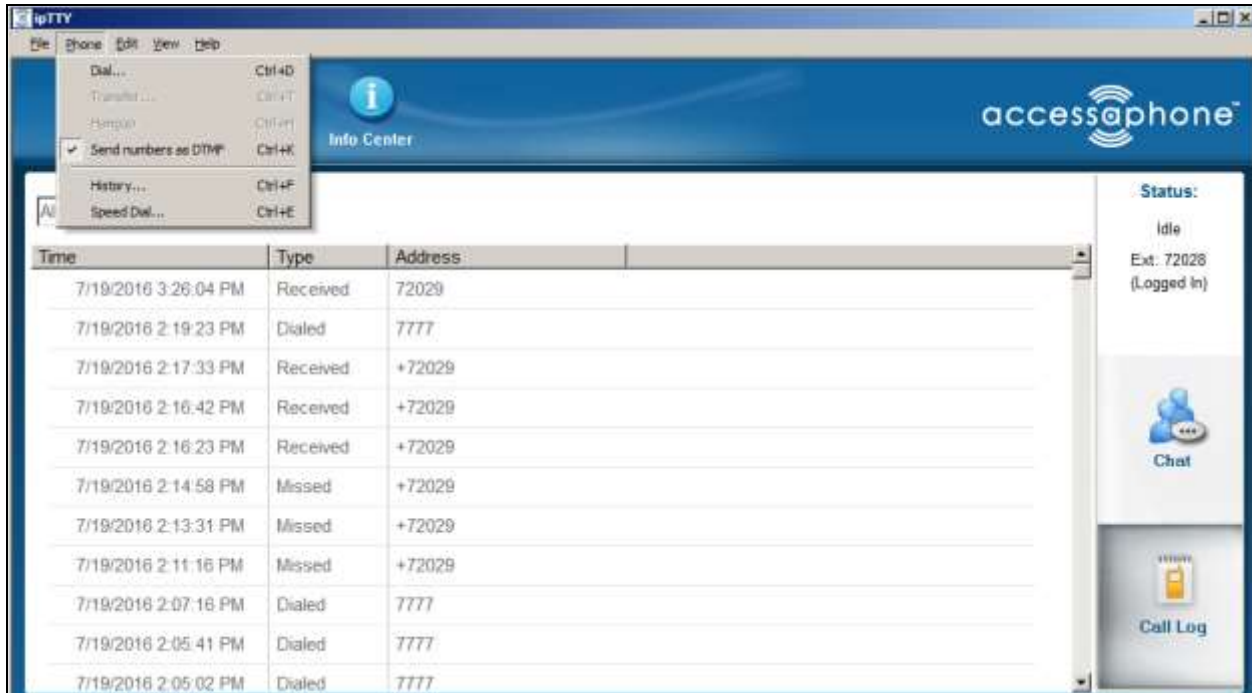


The screenshot shows a 'Settings' dialog box with a close button (X) in the top right corner. The dialog has several tabs: 'Incoming Call', 'Answering', 'Save Conversation', 'Notifications', 'SIP', 'RTP Settings', 'Audio', and 'Call Log'. The 'SIP' tab is selected. The settings are as follows:

SIP Extension:	72028
Outbound Proxy:	
Authentication User:	72028
Password:	••••••
Registrar:	10.64.40.226
SIP Port:	5060
STUN Server:	
Realm:	
Qos DSCP:	0
Local IP Bind Address:	

At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

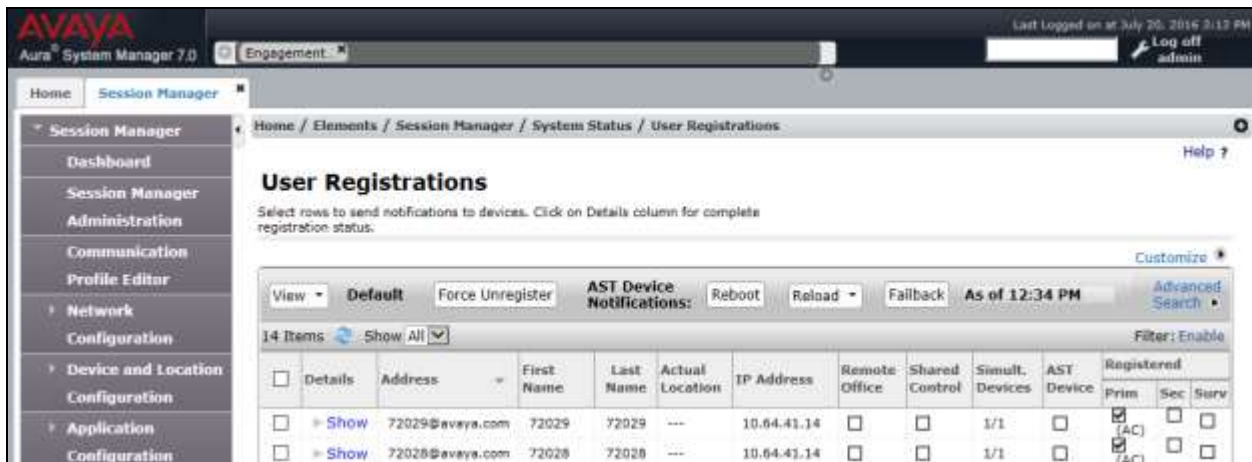
From the **Phone** menu select the “Send Numbers as DTMF” option.



9. Verification Steps

The following steps may be used to verify the configuration:

- Verify that Tenacity ipTTY successfully registered with Session manager by following the **Elements → Session Manager → System Status → User Registrations** link on the System Manager Web Interface.



- Place calls to and from Tenacity ipTTY and verify that the calls are successfully established with two-way talk path.
- Place text messages between Tenacity ipTTYs and verify that each ipTTY can send and receive.

10. Conclusion

Tenacity ipTTY was successfully compliance tested with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Session Manager 7.0. Tenacity ipTTY successfully registered with Session Manager, sent/received text messages, placed and received calls to and from SIP and H.323 deskphones, and executed other telephony features like transfer, forward, DTMF, and voicemail. Some observations are noted in **Section 2**.

11. Additional References

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

[1] *Administering Avaya Aura® Communication Manager* Release 7.0.1, Issue 2, May 2016, Document Number 03-300509.

[2] *Administering Avaya Aura® System Manager*, Release 7.0.1, June 20106.

©2016 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.