



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Yealink's SIP T32G Deskphone with Avaya Aura® Communication Manager R6.2 and Avaya Aura® Session Manager R6.2 – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning Yealink's SIP T32G Deskphone to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

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 steps required to connect Yealink's SIP T32G Gigabit deskphone (T32G) to a SIP infrastructure consisting of Avaya Aura® Session Manager R6.2 and Avaya Aura® Communication Manager R6.2. Yealink's T32G is a colour display handset with 3 line appearances, 4 soft keys and 16 feature buttons. Also described is how Avaya Aura® Communication Manager features can be made available in addition to the standard features supported on Yealink's T32G. In this configuration, the Off-PBX Stations (OPS) feature set is extended from Avaya Aura® Communication Manager to Yealink's T32G providing the T32G with enhanced calling features.

2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of Yealink's T32G to make and receive calls to and from Avaya H.323 and SIP deskphones. Avaya Aura® Messaging was used to allow users leave voicemail messages and to demonstrate Message Waiting Indication and DTMF control on the T32G.

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 compliance testing included the test scenarios shown below. Note that when applicable, all tests were performed with Avaya SIP deskphones, Avaya H.323 deskphones, Yealink's T32G and PSTN endpoints.

- Basic Calls
- Hold and Retrieve
- Attended and Blind Transfer
- Call Forwarding Unconditional, No Reply and Busy
- Call Waiting
- Call Park/Pickup
- Conference
- Do Not Disturb
- Calling Line Name/Identification
- Codec Support
- DTMF Support
- Message Waiting Indication

2.2. Test Results

The following observations were noted during testing.

- When using Busy Lamp Field (BLF) key for Call Pickup this needs to be set so DSS Key TYPE = Direct Pickup Call pickup on Yealink.
- Yealink supports up to 3-way audio conference.

2.3. Support

Support from Avaya is available by visiting the website <http://support.avaya.com> and a list of product documentation can be found in **Section 11** of these Application Notes. Technical support for the Yealink deskphones can be obtained as follows:

- <http://www.yealink.co.uk/support/>
- email: support@yealink.co.uk
- Tel: +44 (0) 161 763 2060

3. Reference Configuration

Figure 1 shows the network topology during compliance testing. Yealink's T32G is placed on the Telephony LAN. The T32G registers as a third-party SIP user with Session Manager in order to be able to make/receive calls to and from the Avaya H.323 and SIP deskphones on Communication Manager. System Manager is used to configure Session Manager.

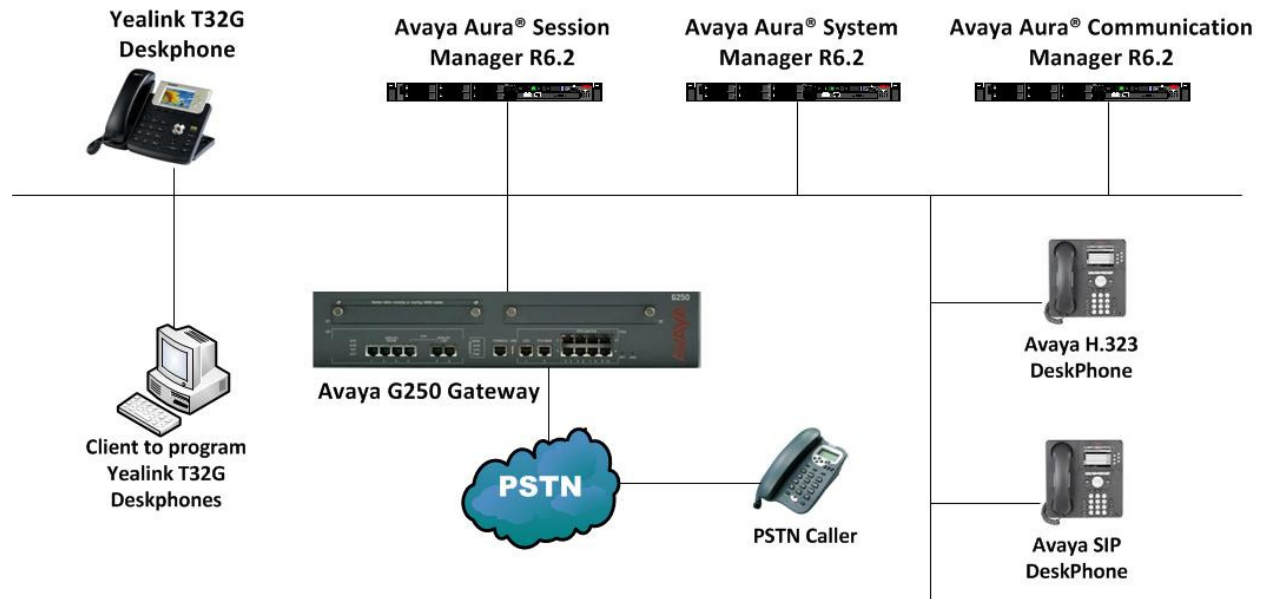


Figure 1: Network Solution of Yealink T32G SIP Deskphone with Avaya Aura® Communication Manager R6.2 and Avaya Aura® Session Manager R6.2

4. Equipment and Software Validated

The following equipment and software was used for the compliance test.

Equipment/Software	Release/Version
Avaya Aura® System Manager running on Avaya S8800 Server	R6.2 SP4 (6.2.0.0.15669)
Avaya Aura® Communication Manager running on Avaya S8800 Server	R6.2 SP4 (R016x.02.0.823.0)
Avaya Aura® Session Manager running on Avaya S8800 Server	R6.2 SP3 (6.2.3.0.623006)
Avaya Aura® Messaging running on S8800 Server	R6.1
Avaya 96xx Series IP Deskphone (with Avaya one-X® H.323 firmware)	96xx H.323 Release 3.1 SP2
Avaya 96xx Series IP Deskphone (with Avaya one-X® SIP firmware)	96xx SIP Release 2.6 SP3
Yealink T32G	SW Ver 32.70.0.105 HW Ver 22.0.2.32.0.0.0

5. Configure Avaya Aura® Communication Manager

It is assumed that a fully functioning Communication Manager is in place with the necessary licensing and a SIP Trunk to Session Manager. For further information on the configuration of Communication Manager please see **Section 11** of these Application Notes. The following sections go through the following.

- Dial Plan Analysis
- Feature Access Codes
- IP Interfaces
- Network Region
- IP Codec
- Hunt Group
- Off-PPX Stations

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 **2, 3, 4** and **5**. Feature Access Codes (**fac**) use digits **8** and **9** or **#**.

change dialplan analysis			DIAL PLAN ANALYSIS TABLE			Page 1 of 12		
			Location: all			Percent Full: 1		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
2	4	ext						
3	4	ext						
4	4	ext						
5	4	ext						
8	1	fac						
9	1	fac						
*	3	dac						
#	3	fac						

5.2. Configure Feature Access Codes

Use the **change feature-access-codes** command to configure access codes which can be entered from the Yealink T32G to initiate Communication Manager call features. These access codes must be compatible with the dial plan described in **Section 5.1**. The following access codes need to be setup.

- **Answer Back Access Code** : **#22**
- **Auto Alternate Routing (AAR) Access Code** : **8**
- **Auto Route Selection (ARS) - Access Code 1** : **9**
- **Call Park Access Code** : **#11**

change feature-access-codes		Page 1 of 10
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:		
Abbreviated Dialing List2 Access Code:		
Abbreviated Dialing List3 Access Code:		
Abbreviated Dial - Prgm Group List Access Code:		
Announcement Access Code:		
Answer Back Access Code: #22		
Attendant Access Code:		
Auto Alternate Routing (AAR) Access Code: 8		
Auto Route Selection (ARS) - Access Code 1: 9		
		Access Code 2:
Automatic Callback Activation:		Deactivation:
Call Forwarding Activation Busy/DA: All:		Deactivation:
Call Forwarding Enhanced Status: Act:		Deactivation:
Call Park Access Code: #11		
Call Pickup Access Code:		
CAS Remote Hold/Answer Hold-Unhold Access Code:		
CDR Account Code Access Code:		
Change COR Access Code:		
Change Coverage Access Code:		
Conditional Call Extend Activation:		Deactivation:
Contact Closure Open Code:		Close Code:
CDR Account Code Access Code:		
Change COR Access Code:		
Change Coverage Access Code:		
Conditional Call Extend Activation:		Deactivation:
Contact Closure Open Code:		Close Code:

5.3. Configure Node-Names IP

Shown below is an example of the nodes names used in the compliance testing. Use the **change node-names ip** command to configure the IP address of Session Manager. **SM100** is the **Name** used for Session Manager Security Module and **192.168.50.16** is the **IP Address**.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
SM100	192.168.50.16	
default	0.0.0.0	
g250-dcp	192.168.50.18	
procr	192.168.50.13	
procr6	::	

5.4. 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, **devcon.avaya** is used. Note this domain is also configured in **Section 6.1**.

```
change ip-network-region 1                                     Page 1 of 20
                                                             IP NETWORK REGION
    Region: 1
    Location: 1          Authoritative Domain: devcon.avaya
    Name: default NR
MEDIA PARAMETERS                                           Intra-region IP-IP Direct Audio: yes
    Codec Set: 1                                           Inter-region IP-IP Direct Audio: yes
    UDP Port Min: 2048                                     IP Audio Hairpinning? y
    UDP Port Max: 3329
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
```

5.5. Configure IP-Codec

Use the **change ip-codec-set x** (where x is the ip-codec set used) command to designate a codec set compatible with the T32G, which supports **G.711A**, **G.711U** and **G.729A**.

```
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.711A      n             2         20
2: G.711U      n             2         20
3: G.729A      n             2         20
```


5.6. Configuration of Coverage Path and Hunt Group for voicemail

The coverage path setup used for compliance testing is illustrated below. Note the following:

- **Don't Answer** is set to **y** The coverage path will be used in the event the phone set is not answered.
- **Number of Rings** is set to **4** The coverage path will be used after 4 rings.
- **Point 1:** is set to **h59** Hunt Group 59 is utilised by this coverage path.

```
display coverage path 1

                                COVERAGE PATH

                                Coverage Path Number: 59
                                Cvg Enabled for VDN Route-To Party? n
                                Next Path Number:           Hunt after Coverage? n
                                                Linkage

COVERAGE CRITERIA
  Station/Group Status   Inside Call   Outside Call
      Active?            n             n
      Busy?              y             y
      Don't Answer?      y             y      Number of Rings: 4
      All?                n             n
      DND/SAC/Goto Cover? y             y
      Holiday Coverage?  n             n

COVERAGE POINTS
  Terminate to Coverage Pts. with Bridged Appearances? n
Point1: h59           Rng:   Point2:
Point3:                Point4:
Point5:                Point6:
```

The hunt group used for compliance testing is shown below. Note on **Page 1** the **Group Extension** is **5999** which is the voicemail number for Messaging and on **Page 2, Message Center** is set to **sip-adjunct**.

```
display hunt-group 59                                     Page 1 of 60

                                HUNT GROUP

                                Group Number: 59
                                Group Name: Voicemail
                                Group Extension: 5999
                                Group Type: ucd-mia
                                TN: 1
                                COR: 1
                                Security Code:
                                ISDN/SIP Caller Display: mbr-name
                                ACD? n
                                Queue? n
                                Vector? n
                                Coverage Path:
                                Night Service Destination:
                                MM Early Answer? n
                                Local Agent Preference? n
```

```
display hunt-group 59                                     Page 2 of 60

                                HUNT GROUP

                                Message Center: sip-adjunct

Voice Mail Number   Voice Mail Handle   Routing Digits
                    (e.g., AAR/ARS Access Code)
5999                5999                8
```

5.7. Verify Off PBX Station Mapping

Use the **display off-pbx-telephone station-mapping** command to verify that SIP Endpoints, added to Session Manager in **Section 6.3**, have been administered in Communication Manager. The example below shows that Station Extensions **3000** to **3012** are configured as **OPS**.

display off-pbx-telephone station-mapping							Page 1 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode
2000	OPS	-		2000	1	1	
2000	EC500	-		3000	1	1	
2001	OPS	-		2001	aar	1	
2011	EC500	-		3001	1	1	
2013	EC500	-		3006	1	1	
3000	OPS	-		3000	1	1	
3001	OPS	-		3001	1	1	
3002	OPS	-		3002	1	1	
3003	OPS	-		3003	1	1	
3005	OPS	-		3005	1	1	
3006	OPS	-		3006	1	1	
3007	OPS	-		3007	1	1	
3008	OPS	-		3008	1	1	
3010	OPS	-		3010	1	1	
3011	OPS	-		3011	1	1	
3012	OPS	-		3012	1	1	

6. Configure Avaya Aura® Session Manager

Yealink's T32G is added to Session Manager as a SIP User. In order to make changes in Session Manager a web session to System Manager is opened.

6.1. Configuration of a Domain

Navigate to <http://<System Manager IP Address>/SMGR>, enter the appropriate credentials and click on **Log On** as shown below.

System Manager - Windows Internet Explorer provided by Avaya IT

https://192.168.50.8/network-login/

File Edit View Favorites Tools Help

System Manager

AVAYA Avaya Aura® System Manager 6.2

Home / Log On

Log On

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:

Log On Cancel

[Change Password](#)

Once logged in, click on **Routing** highlighted below.

AVAYA Avaya Aura® System Manager 6.2

Help | About | Change Password | Log off

Users	Elements	Services
Administrators Manage Administrative Users	B5800 Branch Gateway Manage B5800 Branch Gateway 6.2 elements	Backup and Restore Backup and restore System Manager database
Directory Synchronization Synchronize users with the enterprise directory	Communication Manager Manage Communication Manager 5.2 and higher elements	Bulk Import and Export Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others
Groups & Roles Manage groups, roles and assign roles to users	Conferencing Manage Conferencing Multimedia Server objects	Configurations Manage system wide configurations
User Management Manage users, shared user resources and provision users	Inventory Manage, discover, and navigate to elements, update element software	Events Manage alarms, view and harvest logs
	Meeting Exchange Manage Meeting Exchange and Avaya Aura Conferencing 6.0 elements	Licenses View and configure licenses
	Messaging Manage Avaya Aura Messaging, Communication Manager Messaging, and Modular Messaging	Replication Track data replication nodes, repair replication nodes
	Presence Presence	Scheduler Schedule, track, cancel, update and delete jobs
	Routing Network Routing Policy	Security Manage Security Certificates
		Templates Manage Templates for Communication

Click on **Domains** in the left window. If there is not a domain already configured click on **New** highlighted below and enter a suitable domain name. Note the domain **Name** used in the compliance testing was **devcon.avaya**. Note this domain is also referenced in **Section 5.4**.

AVAYA Avaya Aura® System Manager 6.2 Help | About

Home / Elements / Routing / Domains

Domain Management

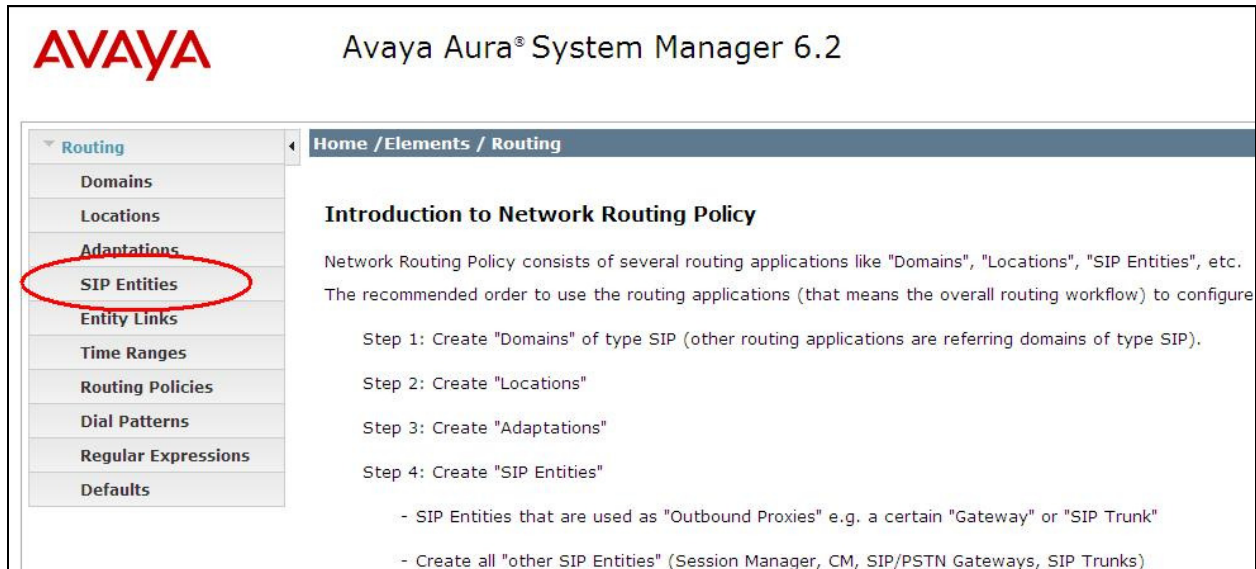
1 Item Refresh

<input type="checkbox"/>	Name	Type	Default	Notes
<input type="checkbox"/>	devcon.avaya	sip	<input type="checkbox"/>	

Select : All, None

6.2. Configuration of SIP Entities

Log into System Manager as described in **Section 6.1** above, click on **SIP Entities** highlighted below.



The screenshot shows the Avaya Aura System Manager 6.2 interface. On the left, a navigation menu is visible with the following items: Routing, Domains, Locations, Adaptations, SIP Entities (highlighted with a red circle), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area displays the 'Introduction to Network Routing Policy' page, which includes a breadcrumb trail 'Home / Elements / Routing' and a list of steps for configuring the routing policy.

Introduction to Network Routing Policy

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc. The recommended order to use the routing applications (that means the overall routing workflow) to configure

Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).

Step 2: Create "Locations"

Step 3: Create "Adaptations"

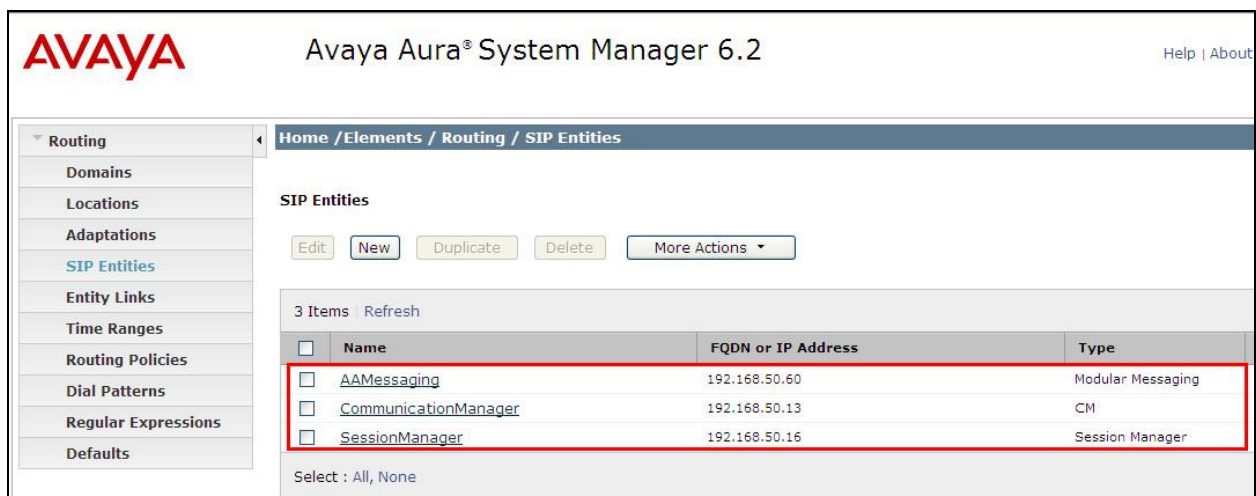
Step 4: Create "SIP Entities"

- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)

Clicking on **SIP Entities** shows what SIP Entities have been added to the system and allows the addition of any new SIP Entity that may be required. Please note the SIP Entities present for the Compliance Testing of Yealink T32G Deskphone.

- Communication Manager SIP Entity
- Session Manager SIP Entity
- Messaging SIP Entity

Note: There is no SIP Entity present or required for Yealink.



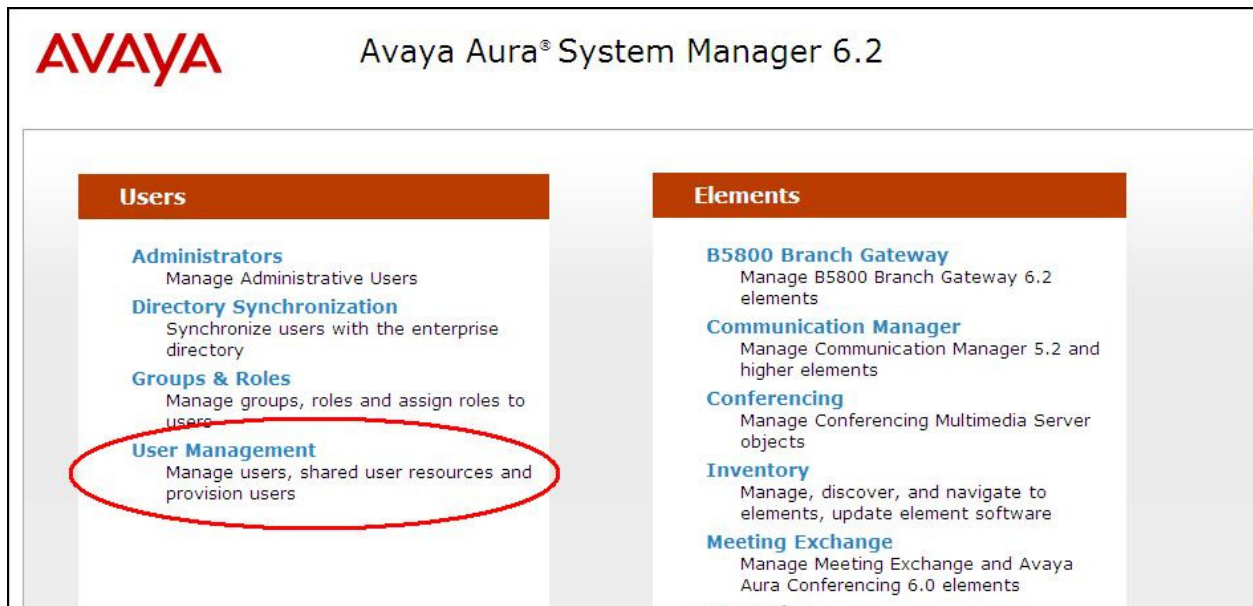
The screenshot shows the Avaya Aura System Manager 6.2 interface with the 'SIP Entities' page selected. The breadcrumb trail is 'Home / Elements / Routing / SIP Entities'. The page title is 'SIP Entities'. There are buttons for 'Edit', 'New', 'Duplicate', 'Delete', and 'More Actions'. Below these buttons, it says '3 Items Refresh'. A table lists the SIP Entities:

<input type="checkbox"/>	Name	FQDN or IP Address	Type
<input type="checkbox"/>	AAmessaging	192.168.50.60	Modular Messaging
<input type="checkbox"/>	CommunicationManager	192.168.50.13	CM
<input type="checkbox"/>	SessionManager	192.168.50.16	Session Manager

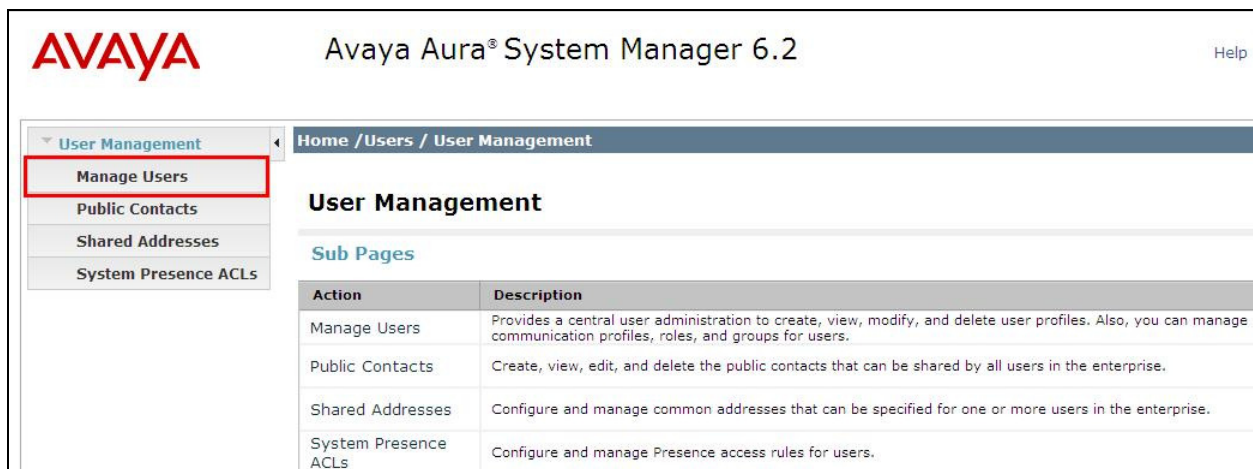
Below the table, it says 'Select : All, None'.

6.3. Adding Yealink T32G SIP Users

From the home page click on **User Management** highlighted below.



Click on **Manage Users**.



Click on **New** highlighted to add a new SIP user.

AVAYA Avaya Aura® System Manager 6.2 Help

Home /Users / User Management / Manage Users

User Management

Users

View Edit **New** Duplicate Delete More Actions ▾

13 Items Refresh Show ALL ▾

<input type="checkbox"/>	Last Name	First Name	Display Name	Login Name	E164 Handle
--------------------------	-----------	------------	--------------	------------	-------------

Under the **Identity** tab fill in the user's **Last Name** and **First Name** as shown below. Enter the **Login Name** and ensure **Authentication Type** is set to **Basic**. The ID password (not shown) also needs to be added.

Manage Users Public Contacts Shared Addresses System Presence ACLs

User Profile Edit: 3000@devcon.avaya Commit & Continue Commit

Identity * Communication Profile * Membership Contacts

Identity ▾

* Last Name: T32

* First Name: 3000

Middle Name:

Description:

Status: Offline

Update Time: February 19, 2013 10:00

* Login Name: 3000@devcon.avaya

* Authentication Type: Basic ▾

[Change Password](#)

Source: local

Localized Display Name: T32 3000

Endpoint Display Name: T32 3000

Under the **Communication Profile** tab enter a suitable **Communication Profile Password** and click on **Done** when added, note that this password is required when configuring the Yealink T32G in **Section 8**. Click on **New** to add a new **Communication Address**.

Enter the extension number and the domain defined in **Section 6.1** for the **Fully Qualified Address** and click on **Add** once finished.

Ensure **Session Manager Profile** is checked and select the **Primary Session Manager**, select the previously defined **Origination Application Sequence** and the **Termination Application Sequence** and the **Home Location** as highlighted below.

The screenshot shows the 'Session Manager Profile' configuration page. The following fields are highlighted with red boxes:

- ☒ **Session Manager Profile**
- * **Primary Session Manager**: SessionManager
- Secondary Session Manager**: (None)
- Origination Application Sequence**: CMAPPSEQ
- Termination Application Sequence**: CMAPPSEQ
- Conference Factory Set**: (None)
- Survivability Server**: (None)
- * **Home Location**: DevconLAB

Two tables are visible on the right side of the page:

Primary	Secondary	Maximum
12	0	12

Primary	Secondary	Maximum

Ensure that **CM Endpoint Profile** is selected and choose the **DEFAULT_9620SIP_CM_6_2** as the **Template** and ensure **Port** is set to **IP**. Click **Endpoint Editor** to configure the buttons and features for that handset on Communication Manager.

The screenshot shows the 'CM Endpoint Profile' configuration page. The following fields are highlighted with red boxes:

- ☒ **CM Endpoint Profile**
- * **System**: CommunicationManager62
- * **Profile Type**: Endpoint
- Use Existing Endpoints**: ☐
- * **Extension**: 3000 (with 'Endpoint Editor' button)
- Template**: DEFAULT_9620SIP_CM_6_2
- Set Type**: 9620SIP
- Security Code**: (empty)
- * **Port**: IP
- Voice Mail Number**: (empty)
- Preferred Handle**: (None)
- Delete Endpoint on Unassign of Endpoint from User or on Delete User.**: ☐
- Override Endpoint Name**: ☒

Under the **General Options** tab ensure that **Coverage Path 1** is set to that configured in **Section 5.6**. Also ensure that **Message Lamp Ext.** is showing the correct extension number.

General Options (G) *		Feature Options (F)		Site Data (S)		Abbreviated Call Dialing (A)		Enhanced Call Fwd (E)	
Button Assignment (B)		Group Membership (M)							
* Class of Restriction (COR)	1	* Class Of Service (COS)	1						
* Emergency Location Ext	3000	* Message Lamp Ext.	3000						
* Tenant Number	1	* SIP Trunk	Qaar						
Type of 3PCC Enabled	None	Native Name	T32 3000						
Coverage Path 1	1	Coverage Path 2							
Lock Message	<input type="checkbox"/>	Multibyte Language	Not Applicable						

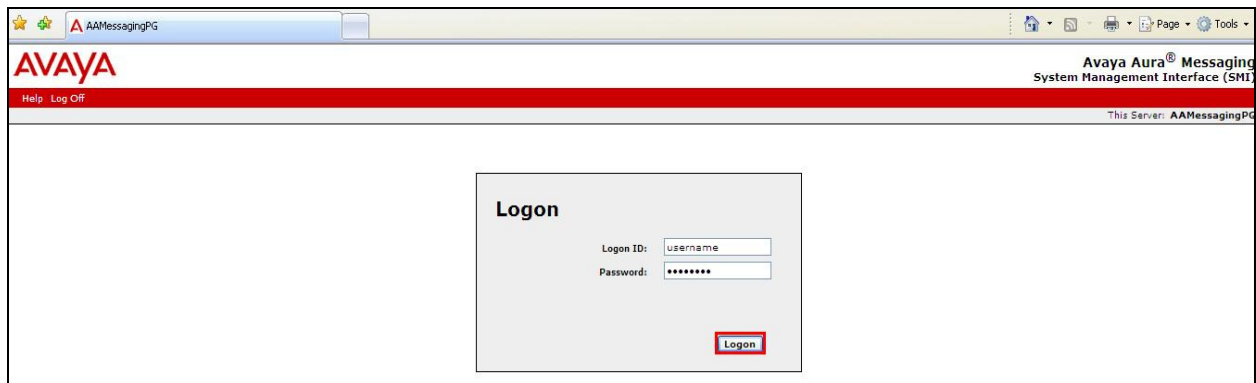
*Required

Done

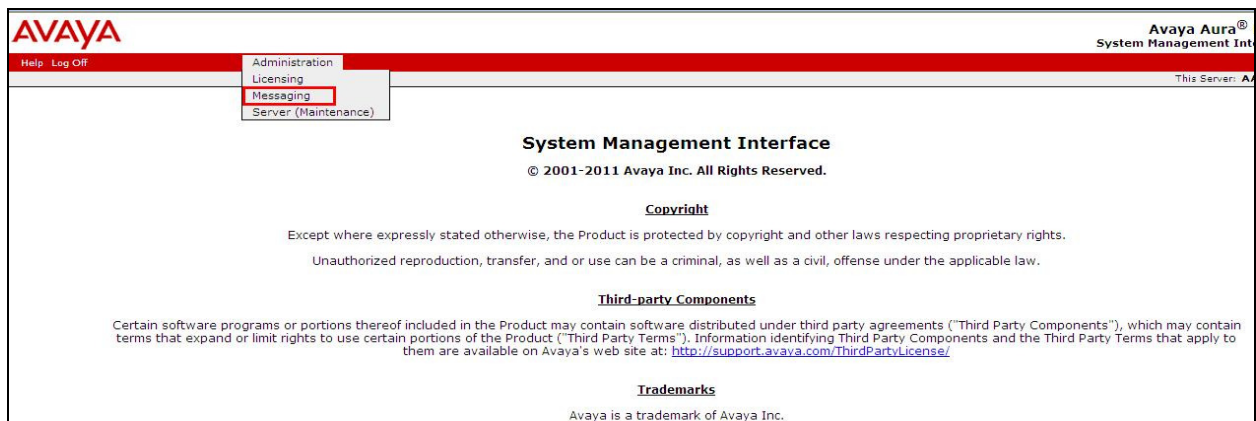
7. Configure Avaya Aura® Messaging

It is assumed that a fully working messaging system is in place and the necessary configuration for Communication Manager and Session Manager has already been done. For further information on the installation and configuration of Messaging please refer to **Section 11** of these Application Notes.

Navigate to <http://<Messaging IP Address>>. Enter the appropriate credentials and click on **Logon** highlighted below.



Once logged on select **Messaging** under **Administration** as shown below.



Click on **User Management** in the left hand column and click on **Add** under **Add User/Info Mailbox** as highlighted below.

The screenshot shows the Avaya Administration web interface. The top navigation bar includes 'Help' and 'Log Off'. The left sidebar lists various system components, with 'User Management' highlighted. The main content area is titled 'User Management' and contains three sections: 'License Status' (License mode: Normal), 'Edit User/Info Mailbox' (with an 'Identifier' input field and an 'Edit' button), and 'Add User/Info Mailbox' (with an 'Add' button highlighted by a red box).

Enter a suitable **First Name** and **Last Name**. Select the appropriate **Site** from the drop down box. Enter the correct **Mailbox number** and **Extension**. Select the appropriate **Class of Service**.

The screenshot shows the 'User Management > Properties for New User' form in the Avaya Administration interface. The left sidebar has 'User Management' highlighted. The main content area contains the following fields and options:

- User Properties**
- First name:** Yealink3000
- Last name:** T32
- Display name:** YealinkT32, 3000
- ASCII name:** (empty field)
- Site:** Messaging_PG (dropdown menu)
- Mailbox number:** 3000
- Extension:** 3000
- ☒ **Include in Auto Attendant directory**
- Additional extensions:** (three empty input fields)
- Class of Service:** Standard (dropdown menu)

Ensure that **MWI Enabled** is set to **Yes**. Enter a suitable **password** and click on **Save** once finished.

The screenshot shows the Avaya Administration web interface. The left sidebar contains a navigation tree with categories like 'Messaging System (Storage)', 'Reports (Storage)', 'Server Information', and 'Server Settings (Storage)'. The main content area is titled 'Administration' and shows configuration options for a 'Class of Service'. The 'MWI enabled' dropdown is set to 'Yes' and is highlighted with a red box. Below it, 'Miscellaneous 1' and 'Miscellaneous 2' are empty text fields. Further down, 'New password' and 'Confirm password' fields are both filled with six dots and are also highlighted with a red box. At the bottom, there are three checkboxes: 'User must change voice messaging password at next login' (checked), 'Voice messaging password expired' (unchecked), and 'Locked out from voice messaging' (unchecked). A 'Save' button is highlighted with a red box, and a 'Delete' button is next to it.

AVAYA

Help Log Off Administration

Administration / Messaging

Messaging System (Storage)

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

Reports (Storage)

- Users
- Info Mailboxes
- Remote Users
- Uninitialized Mailboxes
- Login Failures
- Locked Out Users

Server Information

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

Server Settings (Storage)

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

Class of Service: Standard

Pronounceable name:

MWI enabled: Yes

Miscellaneous 1:

Miscellaneous 2:

New password:

Confirm password:

☒ User must change voice messaging password at next login

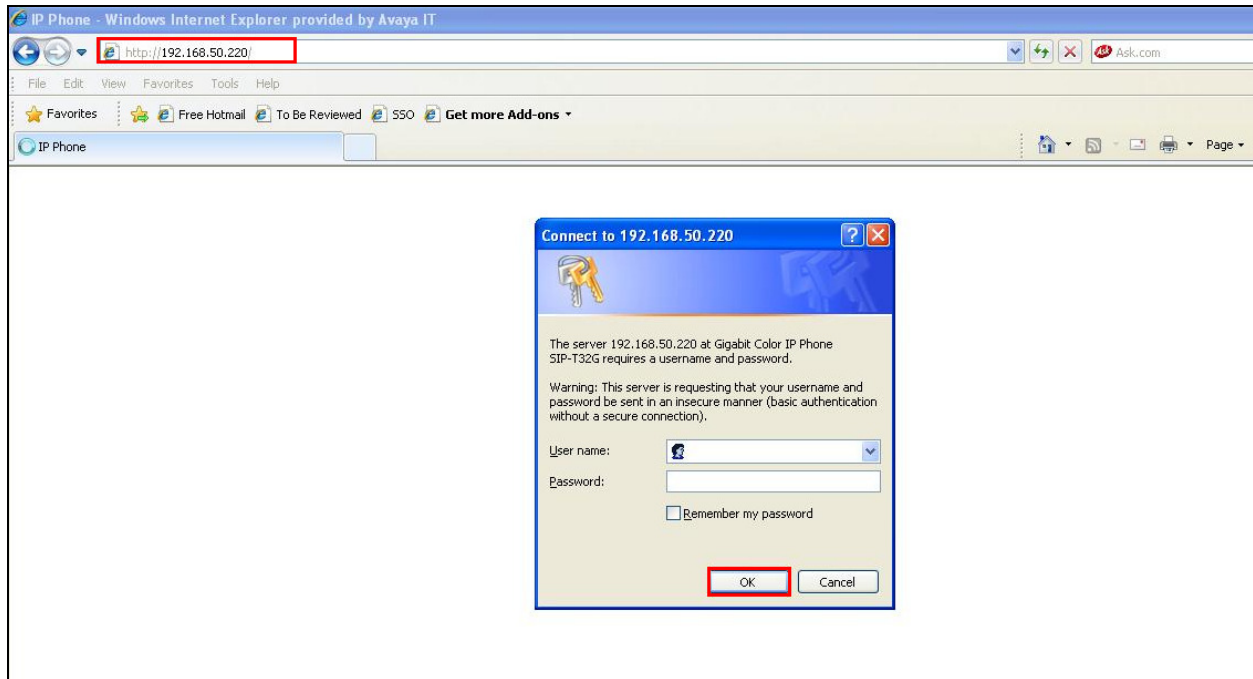
☐ Voice messaging password expired

☐ Locked out from voice messaging

Save Delete

8. Configure Yealink T32G SIP Deskphone

The configuration of Yealink T32G is achieved by opening a web browser. To obtain the IP address of the phone press the **OK** button located at the centre of the directional keys (not shown). Open a web browser and enter the IP address of the T32G. Enter the proper credentials and press **OK** as shown below.



Click on the **Basic** tab in the left window. Click on the **Account** tab in the main window and enter all the credentials as shown below. Note the **SIP Server** IP address is the SM100 IP address as shown in **Section 5.4**. The **User Name** and **Password** entered is that of the Communication Manager Profile username and password which was created in **Section 6.3**. Click **Confirm** once all the information has been entered correctly. Enter all the credentials as shown.

Yealink

Status **Account** Network DSS Key Phone Directory Security

Basic Codec Advanced

Account Account 1

Register Status: Registered

Account Active: Enabled

Label: 3000

Display Name: 3000

Register Name: 3000

User Name: 3000

Password:

SIP Server: 192.168.50.16 Port: 5060

Enable Outbound Proxy Server: Disabled

Outbound Proxy Server: Port: 5060

Transport: UDP

Backup Outbound Proxy Server: Port: 5060

NAT Traversal: Disabled

STUN Server: Port: 3478

Voice Mail: 5999

Proxy Require:

Anonymous Call: Off

On Code:

Off Code:

Anonymous Call Rejection: Off

On Code:

Off Code:

Missed Call Log: Enabled

Auto Answer: Disabled

XML Idle Screen: Disabled

XML Idle Screen URL:

Ring Tones: common

Confirm **Cancel**

Copyright © 1998-2011 **Inc. All Rights Reserved

NOTE

Display Name
SIP service subscriber's name which will be used for Caller ID display.

Register Name
SIP service subscriber's ID used for authentication.

User Name
User account, provided by VoIP service provider.

NAT Traversal
Defines the STUN server will be active or not.

Proxy Require
A special parameter just for Nortel server. If you login to Nortel server, the value should be: com.nortelnetworks.firewall

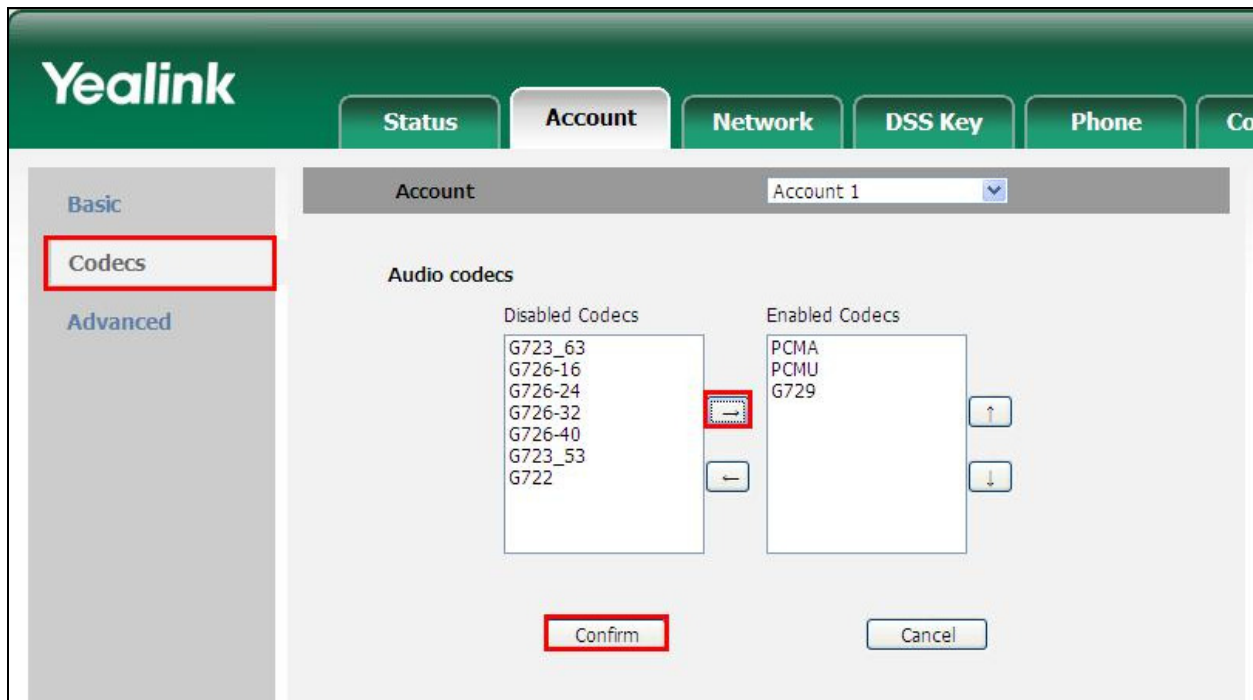
Codecs
Choose the codecs you want to use.

Advanced
The Advanced parameters for administrator.

Click on the **Advanced** tab in the left window and ensure the **Subscribe for MWI** is **Enabled** and the **MWI Subscription Period** set to **120**.

Basic	Account	Account 1	
Codecs	UDP Keep-alive Message	Enabled	?
Advanced	UDP Keep-alive Interval (seconds)	30	
	Login Expire (seconds)	3600	?
	Local SIP Port	5060	?
	Rport	Enabled	?
	SIP Session Timer (seconds) T1	0.5	?
	SIP Session Timer (seconds) T2	4	
	SIP Session Timer (seconds) T4	5	
	Subscribe Period (seconds)	180	?
	DTMF Type	RFC2833	?
	How to INFO DTMF	Disabled	
	DTMF Payload	101	
	100 Reliable Retransmission	Disabled	?
	Enable Precondition	Disabled	?
	Subscribe Register	Disabled	?
	Subscribe for MWI	Enabled	?
	MWI Subscription Period (Scope:0~84600) (seconds)	120	
	Caller ID Header	FROM	?

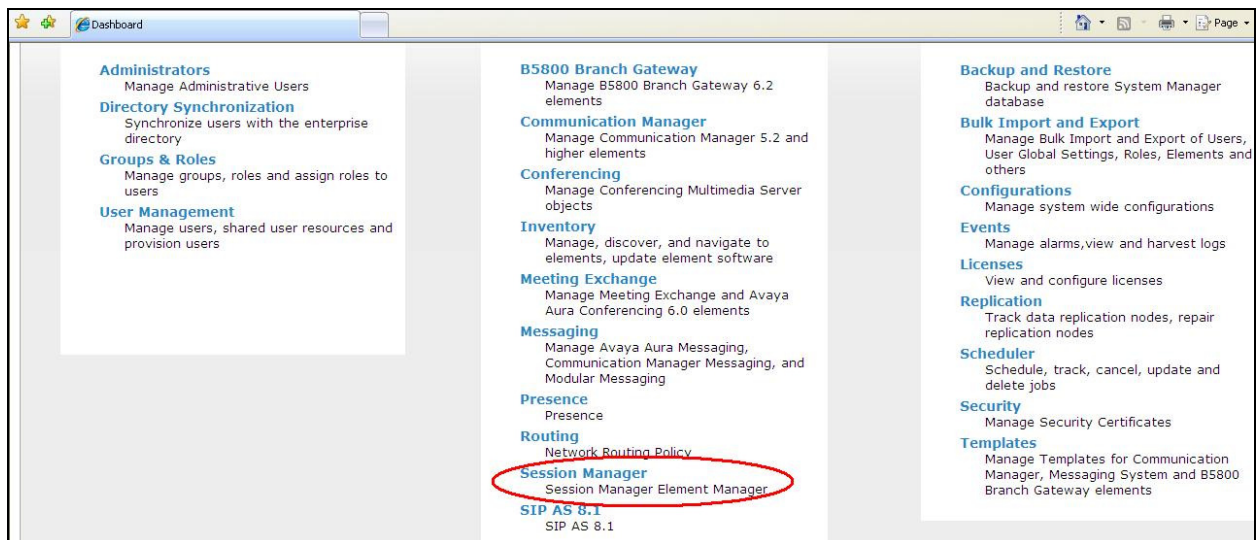
Click on the **Codec** tab in the left windows and select the necessary **Audio Codecs** consistent with IP Codec Set defined in **Section 5.5** in the main window.



9. Verification Steps

The following steps can be taken to ensure that connection between the Yealink T32G and Session Manager are up.

Log into System Manager as done previously in **Section 6.1**, select **Session Manager** as highlighted below.



Select **System Status** and **User Registrations** in the left column. This displays the users that are currently registered with Session Manager. The T32G should show as being registered when the **Address** and the **IP Address** columns are populated with the T32G user information as shown below.

The screenshot shows the 'User Registrations' page. On the left, the 'System Status' and 'User Registrations' menu items are highlighted with red boxes. The main area displays a table of registered users. The third row of the table is highlighted with a red box, showing the following details:

	Details	Address	Login Name	First Name	Last Name	Location	IP Address	AST Device	Registered
<input type="checkbox"/>	» Show	---	3005@devcon.avaya	WLESS3005	Ascom	DevconLAB	---	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	» Show	---	3007@devcon.avaya	WLESS3007	Ascom	DevconLAB	---	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	» Show	3002@devcon.avaya	3002@devcon.avaya	3002	VP 530	DevconLAB	192.168.50.71:5060	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	» Show	---	3015@devcon.avaya	TestSet	9641SIP	DevconLAB	---	<input type="checkbox"/>	<input type="checkbox"/>

The 'IP Address' column for the highlighted row contains the value '192.168.50.71:5060'. The page also includes a left sidebar with navigation options, a top navigation bar, and a bottom status bar showing 'Page 2 of 2'.

10. Conclusion

These Application Notes describe the configuration steps required for Yealink's SIP T32G Deskphone to successfully interoperate with Avaya Aura® Communication Manager R6.2 and Avaya Aura® Session Manager R6.2 by registering the T32G with Session Manager as a third-party SIP phone. Please refer to **Section 2.2** for test results and observations.

11. Additional References

This section references documentation relevant to these Application Notes. The Avaya product documentation is available at <http://support.avaya.com> where the following documents can be obtained.

- [1] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document ID 555-245-205
- [3] *Implementing Avaya Aura® Session Manager* Document ID 03-603473
- [4] *Administering Avaya Aura® Session Manager*, Doc ID 03-603324

Please refer to **Section 2.3** of these Application Notes for information on Yealink support. Product documentation can be found at www.yealink.com

©2013 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.