



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for configuring Komutel SIT2 SIP Console Version 2.5.11 with Avaya Aura® Communication Manager Release 10.1 and Avaya Aura® Session Manager Release 10.1 – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps for provisioning the Komutel SIT2 SIP Console to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

Readers should pay particular attention to the scope of testing as outlined in **Section 2.1**, as well as 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 steps required to integrate the Komutel SIT2 SIP Console (Solution for Integrated Telecommunications) with Avaya Aura® Session Manager (Session Manager) and Avaya Aura® Communication Manager (Communication Manager). The SIT2 SIP Console provides a desktop communications center with enhanced control of call handling features. It provides the ability to handle a high volume of calls and offers tools designed to manage telephony functions. In the compliance test, the SIT2 SIP Console successfully registered with Session Manager, established calls with other telephones, and executed telephony features such as Hold, Transfer, and Conference.

Komutel SIT2 SIP Console registers to Session Manager and is able to work as a SIP agent in Avaya Call Center Elite environment, by using Avaya's Advanced SIP Telephone (AST). Support for this solution is restricted solely to deployments with Canadian Emergency 911 PSAPs and is not supported by Avaya for general enterprise deployments or for use in emergency services call centers in other geographies.

## 2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on establishing calls between the SIT2 SIP Console and Avaya SIP, H.323, and digital stations and exercising common telephony features, such as hold, transfer, and conference.

The serviceability testing focused on verifying that the SIT2 SIP Console comes back into service after re-connecting the Ethernet connection or rebooting the PC on which the SIT2 SIP Console is running.

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 this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products only (private network side). 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 Komutel SIT2 SIP Console did not include use of any specific encryption features as requested by Komutel.

## 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 phones, H.323 phones, Digital phones and PSTN endpoints.

- Successful registration of the SIT2 IP Console with Session Manager.
- Calls between SIT2 SIP Console and Avaya SIP, H.323, digital stations and PSTN.
- G.711Mulaw, G.711Alaw and G.722 codecs support.
- Caller ID display on Avaya and SIT2 SIP Console.
- Proper recognition of DTMF tones.
- Basic telephony features including Hold, Mute, Transfer, and Conference.
- Extended telephony features using Communication Manager Feature Access Code (FAC) such as Call Park and Call Pickup.
- Contact center features including agent login, agent logout, various agent states and receiving the contact center call.
- Multi Device Access.
- Proper system recovery after a restart of the SIT2 SIP Console and loss of IP connectivity.

## 2.2. Test Results

All test cases passed successfully with the following observation.

- Komutel SIT2 SIP Console does not support codec G.729
- Komutel SIT2 SIP Console does not support Call Forward and Call Park at the time of testing.

## 2.3. Support

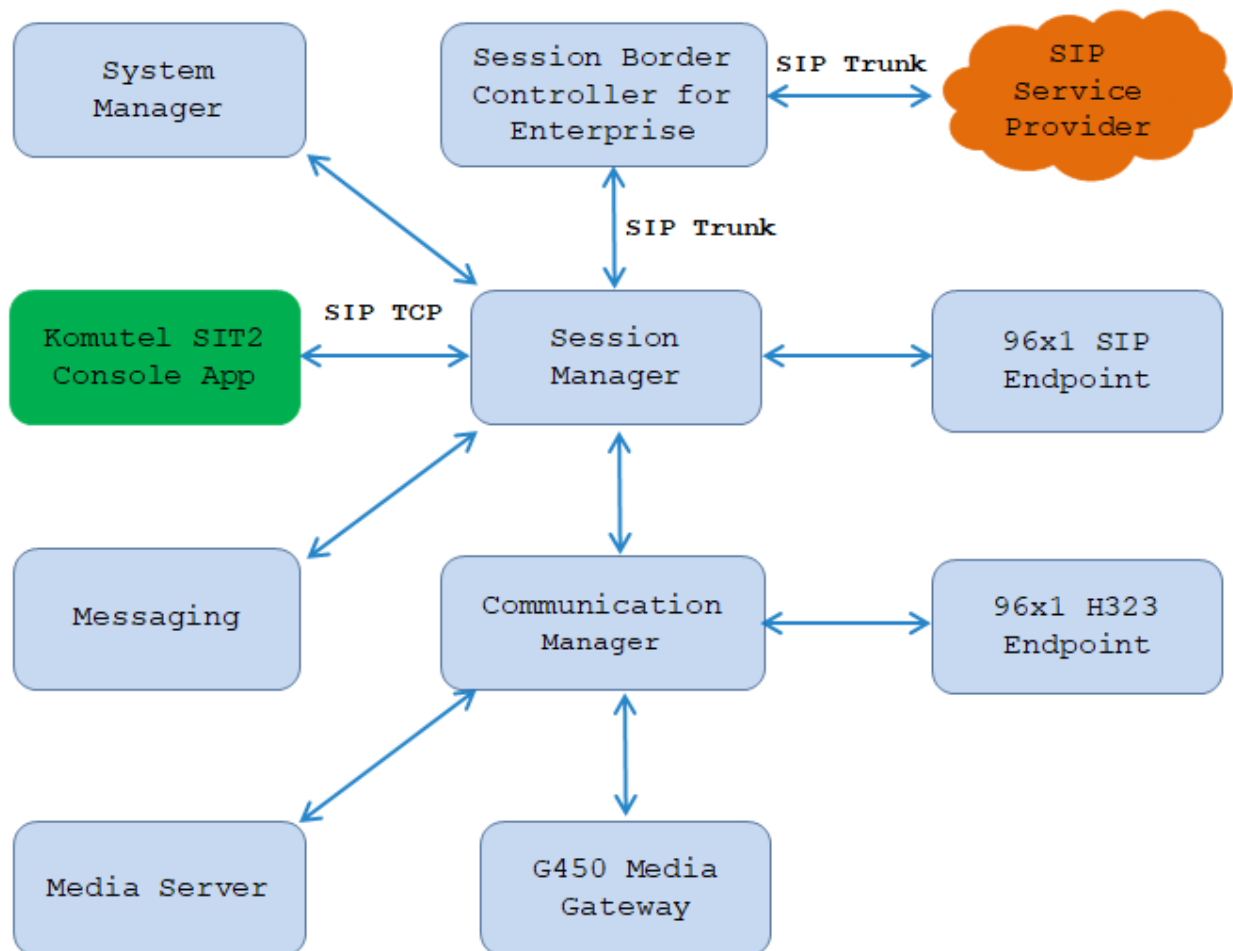
For technical support on the SIT2 SIP Console, contact Komutel Support via phone, email, or website.

- **Phone:** +1(877) 225-9988
- **Email:** [service@komutel.com](mailto:service@komutel.com)
- **Web:** <https://www.komutel.com/fr/a-propos-de-komutel/services/>

### 3. Reference Configuration

**Figure 1** illustrates a sample configuration with an Avaya SIP-based network that includes the following Avaya products:

- Avaya Aura® Communication Manager running on a virtualized environment with a G450 Media Gateway.
- Avaya Aura® Session Manager connected to Communication Manager via a SIP trunk and acting as a Registrar/Proxy for SIP telephones.
- Avaya Aura® System Manager used to configure Session Manager.
- Enterprise has SIP trunk connected to PSTN through Avaya Session Border Controller.
- Komutel SIT2 IP Console registered with Session Manager with Advanced SIP Telephony (AST) and acted as a SIP agent for Call Center Elite in Communication Manager.



**Figure 1:** Avaya SIP Network with Komutel SIT2 SIP Console

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on virtualized environment	10.1 (10.1.0.1.0.974.27372)
Avaya Messaging	11.1
Avaya Aura® Session Manager running on virtualized environment	10.1 (10.1.0.0.1010019)
Avaya Aura® System Manager running on virtualized environment	10.1 (10.1.0.0.0614119)
Avaya Aura® Media Server running on virtualized environment	8.0 (8.0.2.163)
Avaya Session Border Controller for Enterprise	8.1.3
Avaya G450 Media Gateway	42.07.0
Avaya IP Deskphones <ul style="list-style-type: none"><li>• 9608 (H.323)</li><li>• 9621 (H.323)</li><li>• 9641GS (SIP)</li><li>• J189 (SIP)</li></ul>	6.8.304 6.8.304 7.1.9.0.8 4.0.7.1.5
Komutel SIP2 Console Application	2.5.11.61095
modAdvancedSearch.dll	1.1.3.60837
modDisplayGroupButton.dll	1.1.0.51798

## 5. Configure Avaya Aura® Communication Manager

Configuration and verification operations on Communication Manager illustrated in this section were all performed using Avaya Site Administrator Emulation Mode. The information provided in this section describes the configuration of Communication Manager for this solution. It is implied a working system is already in place, including SIP trunks to a Session Manager. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

**Note:** Any settings not in **Bold** in the following screen shots may be left as Default.

### 5.1. Verify System Capacity

The license file installed on the system controls these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative. Use the **display system-parameters customer-options** command to determine these values. On **Page 1**, verify that the **Maximum Off-PBX Telephones** allowed in the system is sufficient. One OPS station is required per SIP device.

```
display system-parameters customer-options                               Page 1 of 10
                                OPTIONAL FEATURES

G3 Version: V16                                     Software Package: Enterprise
Location: 2                                           System ID (SID): 1
Platform: 28                                          Module ID (MID): 1

                                USED
Platform Maximum Ports: 65000 290
Maximum Stations: 41000 44
Maximum XMOBILE Stations: 41000 0
Maximum Off-PBX Telephones - EC500: 41000 0
Maximum Off-PBX Telephones - OPS: 41000 14
Maximum Off-PBX Telephones - PBFMC: 41000 0
Maximum Off-PBX Telephones - PVFMC: 41000 0
Maximum Off-PBX Telephones - SCCAN: 41000 0
Maximum Survivable Processors: 313 0

(NOTE: You must logoff & login to effect the permission changes.)
```

On **Page 2** of the **system-parameters customer-options form**, verify that the number of **Maximum Administered SIP Trunks** supported by the system is sufficient.

display system-parameters customer-options	Page	2 of 10
OPTIONAL FEATURES		
IP PORT CAPACITIES	USED	
Maximum Administered H.323 Trunks:	12000	16
Maximum Concurrently Registered IP Stations:	18000	2
Maximum Administered Remote Office Trunks:	12000	0
Maximum Concurrently Registered Remote Office Stations:	18000	0
Maximum Concurrently Registered IP eCons:	414	0
Max Concur Registered Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	41000	1
Maximum Video Capable IP Softphones:	18000	4
<b>Maximum Administered SIP Trunks:</b>	<b>24000</b>	<b>180</b>
Maximum Administered Ad-hoc Video Conferencing Ports:	24000	0
Maximum Number of DS1 Boards with Echo Cancellation:	522	0
Maximum TN2501 VAL Boards:	128	0
Maximum Media Gateway VAL Sources:	250	0
Maximum TN2602 Boards with 80 VoIP Channels:	128	0
Maximum TN2602 Boards with 320 VoIP Channels:	128	0
Maximum Number of Expanded Meet-me Conference Ports:	300	0
(NOTE: You must logoff & login to effect the permission changes.)		

On **Page 8** of the **system-parameters customer-options form**, verify that the number of **Logged-In ACD Agents** supported by the system is sufficient.

```

display system-parameters customer-options
                                Page      8 of 12
                                CALL CENTER OPTIONAL FEATURES

VDN of Origin Announcement? y
VDN Return Destination? y
                                VuStats? y
                                VuStats (G3V4 Enhanced)? y


                                USED
Logged-In ACD Agents: 10000      5
    Logged-In Advocate Agents: 10000      0
    Logged-In IP Softphone Agents: 10000    0
    Logged-In SIP EAS Agents: 10000      1
(NOTE: You must logoff & login to effect the permission changes.)

```

## 5.2. Administer Hunt Group

This section provides the Hunt Group configuration for the call center agents. Agents will log into Hunt Group 1 configured below. Provide a descriptive name and set the **Group Extension** field to a valid extension. Enable the **ACD**, **Queue**, and **Vector** options. This hunt group will be specified in the **Agent LoginIDs** configured in **Section 5.5**.

add hunt-group 1		Page 1 of 4
HUNT GROUP		
Group Number: 1	ACD? y	
Group Name: Skill-1	Queue? y	
Group Extension: 3320	Vector? y	
Group Type: ucd-mia		
TN: 1		
COR: 1	MM Early Answer? n	
Security Code:	Local Agent Preference? n	
ISDN/SIP Caller Display:		
Queue Limit: unlimited		
Calls Warning Threshold:	Port:	
Time Warning Threshold:	Port:	
SIP URI:		

On **Page 2** of the Hunt Group form, enable the **Skill** option and **Both** in the **Measured** field.

add hunt-group 1		Page 2 of 4
HUNT GROUP		
Skill? y	Expected Call Handling Time (sec): 180	
AAS? n	Service Level Target (% in sec): 80 in 20	
Measured: both		
Supervisor Extension:		
Controlling Adjunct: none		
VuStats Objective:		
Multiple Call Handling: none		
Timed ACW Interval (sec):	After Xfer or Held Call Drops? n	



### 5.3. Administer Vector

Use the command “**change vector n**” while “n” is the vector number from 1-8000. The example of the vector 1 with the basic scripting is shown below. The vector 1 is used for the configuration of VDN in the next step.

```
change vector 1                                     Page 1 of 6
                                     CALL VECTOR
Number: 1                      Name: Contact Center
Multimedia? n      Attendant Vectoring? n      Meet-me Conf? n      Lock? n
Basic? y      EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing? y
Prompting? y      LAI? y      G3V4 Adv Route? y      CINFO? y      BSR? y      Holidays? y
Variables? y      3.0 Enhanced? y
01 wait-time      10 secs hearing 1100      then silence
02 queue-to      skill 1      pri m
03 wait-time      5 secs hearing ringback
04 check      skill 1      pri m if expected-wait      < 30
05 announcement 1104
06 queue-to      skill 1      pri m
07 stop
```

### 5.4. Administer VDN

Use the “**add vdn <ext>**” command to add a VDN number. In the **Destination** field, enter **Vector Number 1** as configured in **Section 5.3** above and keep other fields at their default values.

```
add vdn 3340                                     Page 1 of 3
                                     VECTOR DIRECTORY NUMBER
                                     Extension: 3340
                                     Name*: Contact Center 1
                                     Destination: Vector Number      1
Attendant Vectoring? n
Meet-me Conferencing? n
Allow VDN Override? n
COR: 1
TN*: 1
Measured: both      Report Adjunct Calls as ACD*? n
Acceptable Service Level (sec): 20
VDN of Origin Annc. Extension*:
1st Skill*:
2nd Skill*:
3rd Skill*:
```

## 5.5. Administer Agent Login ID

To add an **Agent LoginID**, use the command “**add agent-loginID <agent ID>**” for each agent. In the compliance test, three agent login IDs 1000, 1001, and 1002 were created.

add agent-loginID 1000		Page 1 of 2
AGENT LOGINID		
Login ID: 1000	AAS? n	
Name: Agent 1000	AUDIX? n	
TN: 1		
COR: 1		
Coverage Path:	LWC Reception: spe	
Security Code: 1234	LWC Log External Calls? n	
Attribute:	AUDIX Name for Messaging:	
LoginID for ISDN/SIP Display? n		
Password:		
Password (enter again):		
Auto Answer: station		
MIA Across Skills: system		
AUX Agent Considered Idle (MIA)? system	ACW Agent Considered Idle: system	
Aux Work Reason Code Type: system		
Logout Reason Code Type: system		
Maximum time agent in ACW before logout (sec): system		
Forced Agent Logout Time: :		
WARNING: Agent must log in again before changes take effect		

On **Page 2** of the **Agent LoginID** form, set the skill number (**SN**) to hunt group 1, which is the hunt group (skill) and Skill Level (**SL**) to 1 that the agents will log into.

add agent-loginID 1000		Page 2 of 2
AGENT LOGINID		
Direct Agent Skill:		Service Objective? n
Call Handling Preference: skill-level		Local Call Preference? n
<b>SN</b>	<b>RL</b>	<b>SL</b>
1: 1		1
2:		16:
3:		17:
4:		18:
5:		19:
6:		20:
7:		
8:		
9:		
10:		
11:		
12:		
13:		
14:		
15:		

## 5.6. Define the Dial Plan

Use the **change dialplan analysis** command to define the dial plan used in the system. This includes all telephone extensions. In the sample configuration, telephone extensions are 4 digits long and begin with **33** and **34**.

change dialplan analysis						Page 1 of 12		
DIAL PLAN ANALYSIS TABLE								
Location: all						Percent Full: 1		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
33	4	ext						
34	4	ext						
*	3	fac						
#	3	fac						

## 5.7. Administer IP-Codec Set

Use “**change ip-codec set n**” where **n** is the chosen value of the configuration for the enterprise endpoint. Enter the list of audio codec’s eligible to be used in order of preference. For the interoperability test the codec supported by Komutel SIT2 Console were configured, namely **G.722-64K**, **G.711Mu** and **G.711A**.

Note that the **Media Encryption** is defined here for use between Avaya IP endpoints. Komutel SIT2 Console did not use any media encryption during the compliance test; therefore the media encryption between Komutel SIT2 Console and Avaya IP endpoint is not utilized.

change ip-codec-set 1

Page1 of 2

IP MEDIA PARAMETERS

Codec Set: 1

Audio	Silence	Frames	Packet
Codec	Suppression	Per Pkt	Size (ms)
1: <b>G.722-64K</b>		<b>2</b>	<b>20</b>
2: <b>G.711MU</b>	<b>n</b>	<b>2</b>	<b>20</b>
3: <b>G.711A</b>	<b>n</b>	<b>2</b>	<b>20</b>
4:			
5:			
6:			
7:			

Media Encryption

Encrypted SRTCP: best-effort

1: 1-srtp-aescml28-hmac80
2: none
3:
4:
5:

## 6. Configure Avaya Aura® Session Manager

This section describes aspects of the Session Manager configuration required for interoperating with Komutel SIT2 IP Console. It is assumed that the Domains, Locations, SIP entities, Entity Links, Routing Policies, Dial Patterns and Application Sequences have been configured where appropriate for Communication Manager, Session Manager and Aura Messaging.

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

Recommended access to System Manager is via FQDN.  
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

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

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

---

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

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

User ID:

Password:

[Change Password](#)

**Supported Browsers:** Internet Explorer 11.x or Firefox 65.0, 66.0 and 67.0.

## 6.1. Check Avaya Aura® Session Manager ports for SIP Endpoint Registration

Each Session Manager Entity must be configured so that the SIT2 SIP Console can register to it using UDP/TCP. From the web interface click **Routing** → **SIP Entities** (not shown) and select the Session Manager entity used for registration. Make sure that **TCP** and **UDP** listen ports are present. The TCP and UDP port and SIP domain name are highlighted below.

The screenshot shows the Avaya Aura System Manager 10.1 web interface. The left sidebar contains a navigation menu with options: Home, Routing, Domains, Locations, Conditions, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled "SIP Entity Details" and includes a "General" tab. The "General" tab contains the following fields:

- Name: SM10
- IP Address: 10.33.1.42
- SIP FQDN: (empty)
- Type: Session Manager
- Notes: (empty)
- Location: Session Manager
- Outbound Proxy: (empty)
- Time Zone: America/Denver
- Minimum TLS Version: Use Global Setting
- Credential name: (empty)

Below the "General" tab is the "Monitoring" section, which includes:

- SIP Link Monitoring: Use Session Manager Configuration
- CRLF Keep Alive Monitoring: Use Session Manager Configuration

Buttons for "Commit" and "Cancel" are located at the top right of the "SIP Entity Details" section.

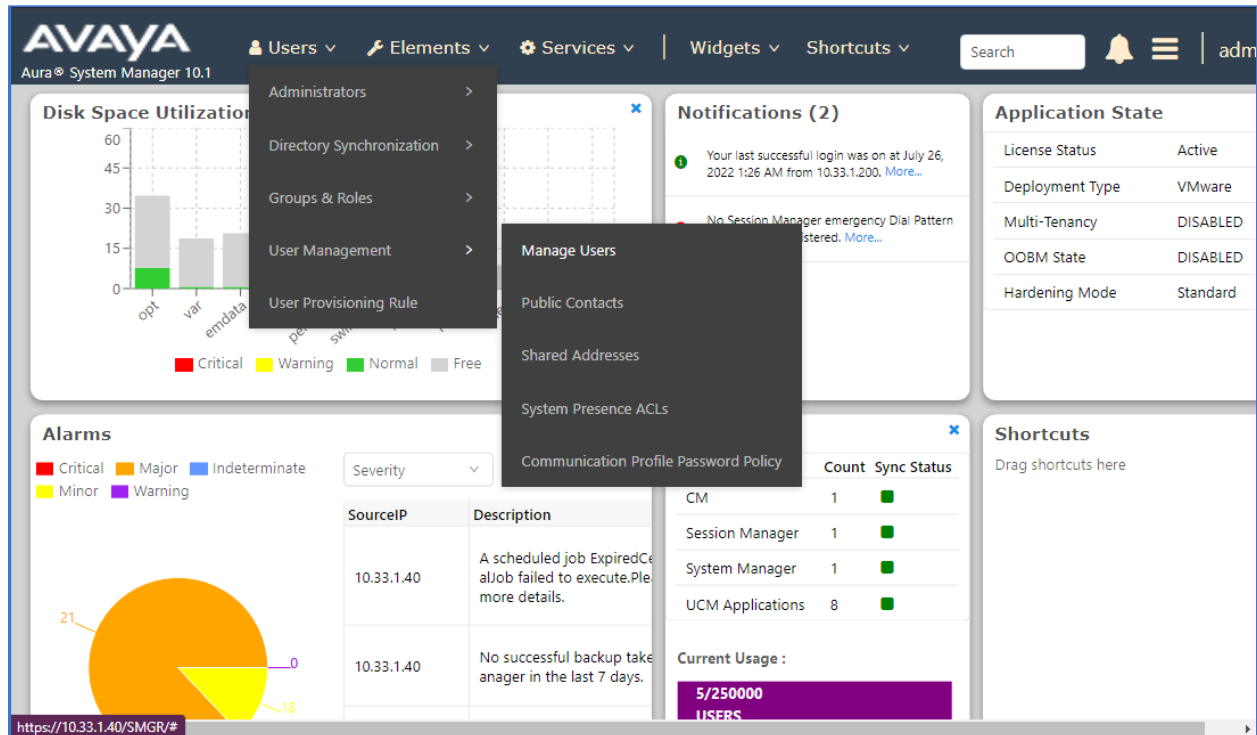
The screenshot shows the "Listen Ports" configuration page for the selected SIP Entity (SM10). The page includes a "Failover Ports" section with fields for "TCP Failover port" and "TLS Failover port". Below this is the "Listen Ports" section, which contains a table with 4 items. The table has columns: Listen Ports, Protocol, Default Domain, Endpoint, and Notes. The first two rows are highlighted with a red box, indicating the TCP and UDP ports for the domain avayalab.com.

Listen Ports	Protocol	Default Domain	Endpoint	Notes
5060	TCP	avayalab.com	<input checked="" type="checkbox"/>	
5060	UDP	avayalab.com	<input checked="" type="checkbox"/>	
5061	TLS	avayalab.com	<input checked="" type="checkbox"/>	
5067	TLS	avayalab.com	<input type="checkbox"/>	

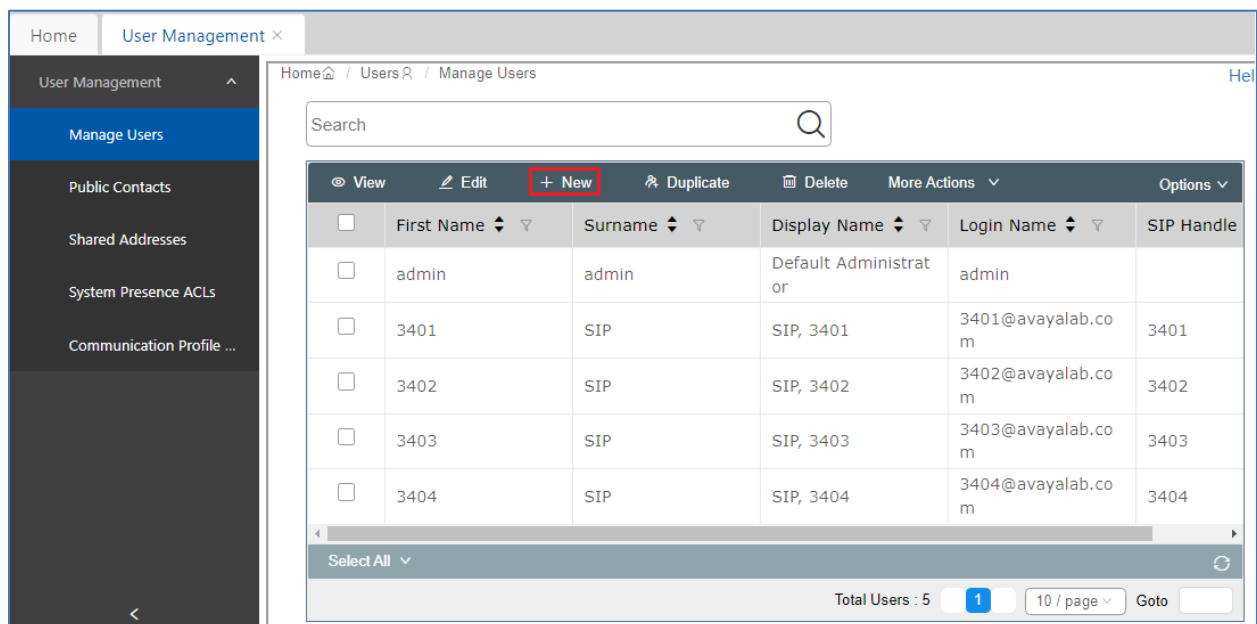
Buttons for "Add" and "Remove" are located above the table. A "Filter: Enable" button is located at the bottom right of the table. The "Select" dropdown at the bottom left is set to "All, None".

## 6.2. Administer SIP User

The Komutel SIT2 SIP Console application registers to a SIP user in Session Manager, to create a SIP user navigate to **Users → User Management → Manage Users**.



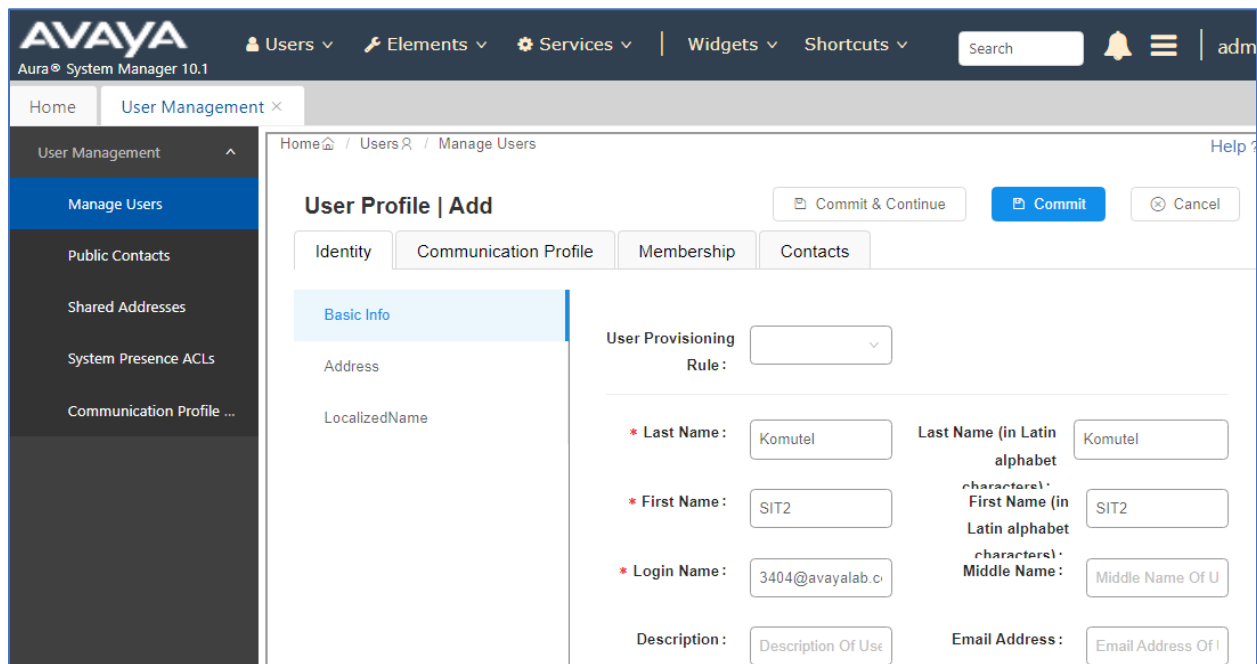
Select **+New** button from the **Manage Users** page in the right hand side to add a new SIP user.



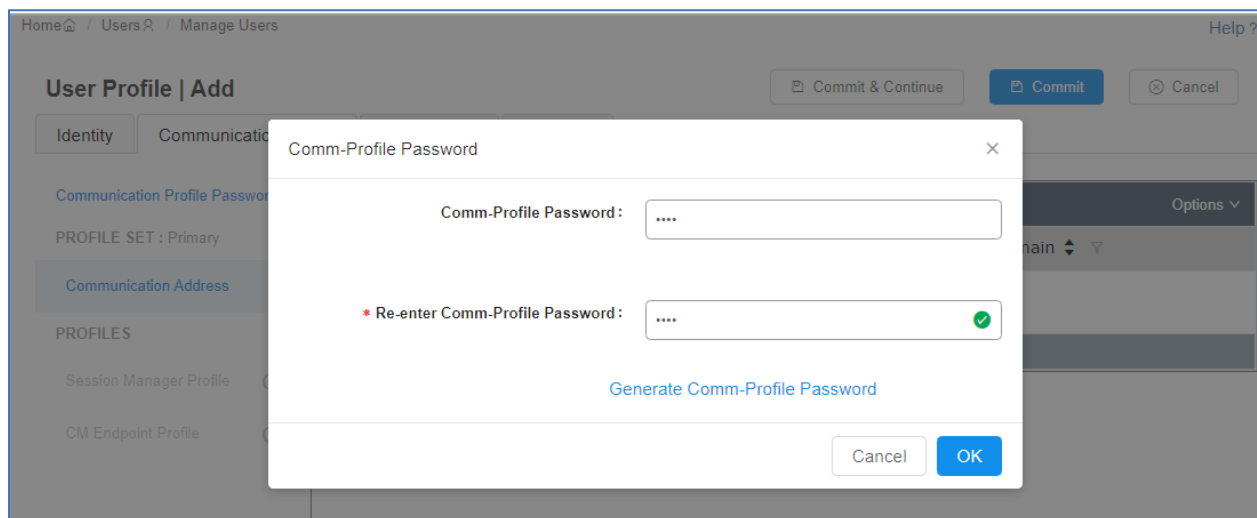
In the **Identity** tab enter the basic information for the SIP user; the fields with asterisk are mandatory.

- **First Name** Enter a descriptive name
- **Last Name** Enter an descriptive name
- **Login Name** Enter the extension number followed by the domain

Leave other fields at default values



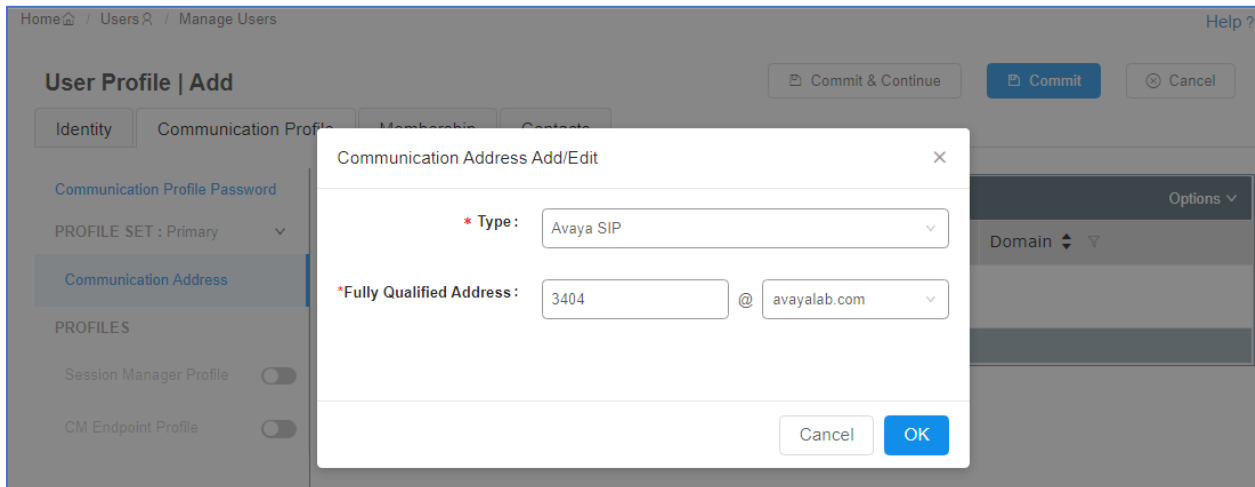
Select **Communication Profile** → **Communication Profile Password**. The **Comm-Profile Password** window displays, enter the same password in the **Comm-Profile Password** and **Re-enter Comm-Profile Password** fields. Click on **OK** button to save the configuration.



Select **Communication Profile** → **Communication Address** and then select “+ New” button (not shown) to add a new communication address; enter the information as shown in the picture below.

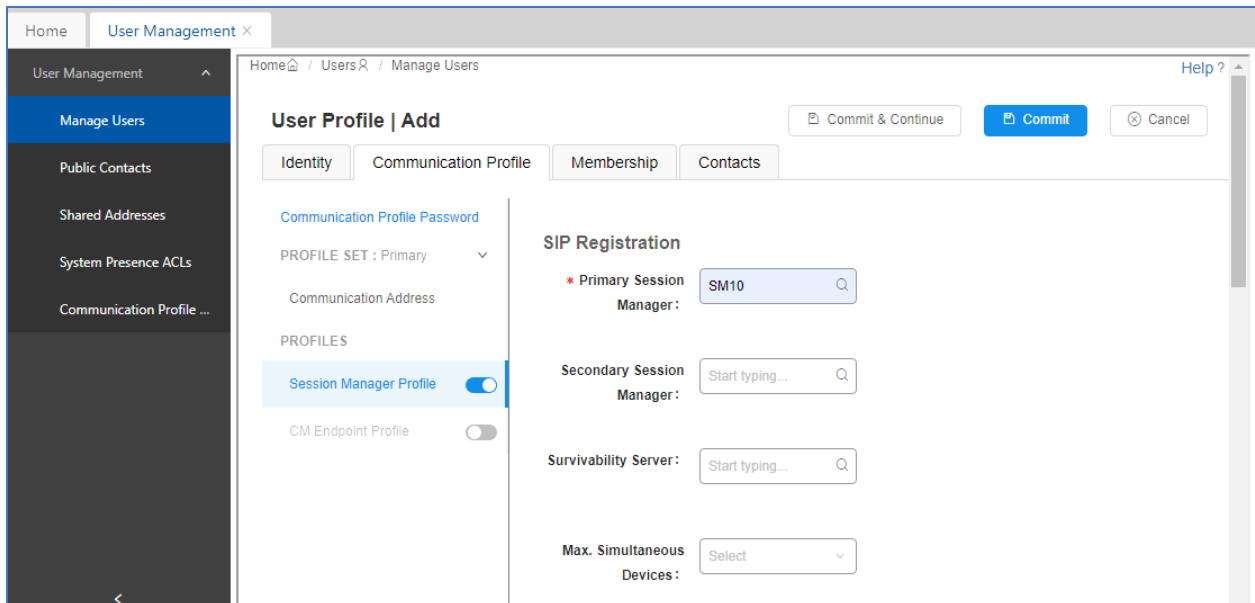
- **Type** Select “**Avaya SIP**” in the dropdown menu
- **Fully Qualified Address** Enter the number **3404** and select SIP domain **avayalab.com**” in the dropdown menu

Click **OK** button to save the configuration.



The screenshot shows a web interface for managing users. A modal dialog titled "Communication Address Add/Edit" is open. It has two main fields: "Type" with a dropdown menu showing "Avaya SIP", and "Fully Qualified Address" with a text input containing "3404" and a domain dropdown showing "avayalab.com". At the bottom of the dialog are "Cancel" and "OK" buttons. The background shows the "User Profile | Add" page with tabs for Identity, Communication Profile, Membership, and Contacts. The "Communication Profile" tab is active, and the "Communication Address" section is highlighted in the left sidebar.

Enable **Session Manager Profile** in the **Communication Profile** tab. In the **SIP Registration** section, select the Session Manager SIP entity **SM10** as shown in the picture below.



The screenshot shows the "User Profile | Add" page with the "Communication Profile" tab selected. On the left, under "PROFILES", the "Session Manager Profile" toggle is turned on. On the right, the "SIP Registration" section is visible. It contains four fields: "Primary Session Manager" with a dropdown showing "SM10", "Secondary Session Manager" with a search input, "Survivability Server" with a search input, and "Max. Simultaneous Devices" with a dropdown showing "Select". The "Commit" button is highlighted in blue.



In the **Application Sequences** section of **Session Manager Profile**, select the previously created **CM10\_Seq** in the **Origination Sequence** and **Termination Sequence** fields.

In the **Call Routing Settings** section, select the previously created **Thornton** in the **Home Location** field.

The screenshot displays the 'User Management' interface with a sidebar on the left containing 'Manage Users', 'Public Contacts', 'Shared Addresses', 'System Presence ACLs', and 'Communication Profile ...'. The main content area is divided into two sections. The top section, 'Application Sequences', contains two dropdown menus: 'Origination Sequence' and 'Termination Sequence', both set to 'CM10\_Seq'. The bottom section, 'Emergency Calling Application Sequences', contains two dropdown menus: 'Emergency Calling Origination Sequence' and 'Emergency Calling Termination', both set to 'Select'. The bottom section, 'Call Routing Settings', contains a dropdown menu for 'Home' set to 'Thornton'.

Application Sequences	
Origination Sequence :	CM10_Seq
Termination Sequence :	CM10_Seq


Emergency Calling Application Sequences	
Emergency Calling Origination Sequence :	Select
Emergency Calling Termination	Select

Call Routing Settings	
* Home	Thornton

Enable **CM Endpoint Profile** in the **Communication Profile** tab. Enter the following values as shown in the picture below.

- **System** Select the previously created *cm10*
- **Profile Type** Select *Endpoint*
- **Extension** Enter the extension *3404*
- **Template** Select the template *9641SIPCC\_DEFAULT\_CM*

The screenshot shows the 'User Profile | Add' form with the 'Communication Profile' tab selected. The 'CM Endpoint Profile' toggle is enabled. The following fields are populated: System (cm10), Profile Type (Endpoint), Extension (3404), Template (9641SIPCC\_DEF), Set Type (9641SIPCC), Port (IP), and Sip Trunk (aar). The 'Security Code' field is empty, and the 'Voice Mail Number' field is also empty.

Select **Editor**  icon next to the **Extension** field. The New Endpoint window displays, in the **General Options (G)** tab, make sure the **Type of 3PCC Enabled** is set to *Avaya*.

The screenshot shows the 'New Endpoint' form with the 'General Options (G)' tab selected. The 'Type of 3PCC Enabled' dropdown is set to 'Avaya'. Other fields include: System (cm10), Template (9641SIPCC\_DEFAULT\_CM\_10\_1), Port (IP), Extension (3404), Set Type (9641SIPCC), Security Code, Class of Restriction (COR) (1), Emergency Location Ext (3404), Tenant Number (1), SIP Trunk (aar), Coverage Path 1, Class of Service (COS) (1), Message Lamp Ext. (3404), and Coverage Path 2.

Select the **Button Assignment (B)** tab, in the Main Buttons sub-tab, add 5 buttons for the contact center agent: **agnt-login**, **auto-in**, **manual-in**, **aux-work**, and **after-call**.

Endpoint Configurations		Button Configurations			
Favorite	Button Label	Button Feature	Argument-1	Argument-2	Argument-3
<input type="checkbox"/>		call-appr			
<input type="checkbox"/>		call-appr			
<input type="checkbox"/>		call-appr			
<input type="checkbox"/>		agnt-login			
<input type="checkbox"/>		auto-in	auto-in Grp		
<input type="checkbox"/>		manual-in	manual-in Grp		
<input type="checkbox"/>		aux-work	Reason Code	Hunt Grp	
<input type="checkbox"/>		after-call	after-call Grp		

Click on **Done** button (not shown) on the **New Endpoint** window and then click on **Commit** button to save the configuration for the new user created.

Home / Users / Manage Users

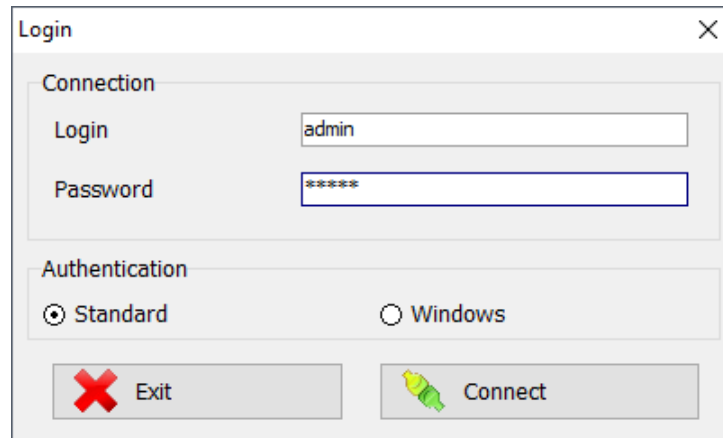
User Profile | Add

Identity Communication Profile Membership Contacts

Commit & Continue **Commit** Cancel

## 7. Komutel SIT2 Console Application

Launch the SIT2 SIP Console application and login in with the appropriate credentials.



To configure the console's lines, navigate to the **Tools → Options → Phone Settings** tab. Depending on the number of lines that are available, choose *Automatic Line* in the **Functions** column, enter the **DN** in the **Description** column and type the text that will be displayed on the line's button in the **Label** column. As shown below, the console was configured with three line appearances with extension 3404.

Phone's functions identification					
	Label	Functions	Description	Receive c	Can make
1	3404	Automatic line	3404	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	3404	Automatic line	3404	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	3404	Automatic line	3404	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
11				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
12				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
13				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
14				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
15				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
16				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
17				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
18				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
19				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
20				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
21				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
22				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
23				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
24				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

In the **Connection** tab, configure the SIP parameters, including:

- Enter **Username** and **Password** as configured in **Section 6.2** to register with Session Manager.
- Enter the SIP domain **avayalab.com** in the **Domain** field.
- Enter the IP address of Session Manager in the **Outbound proxy list** field.

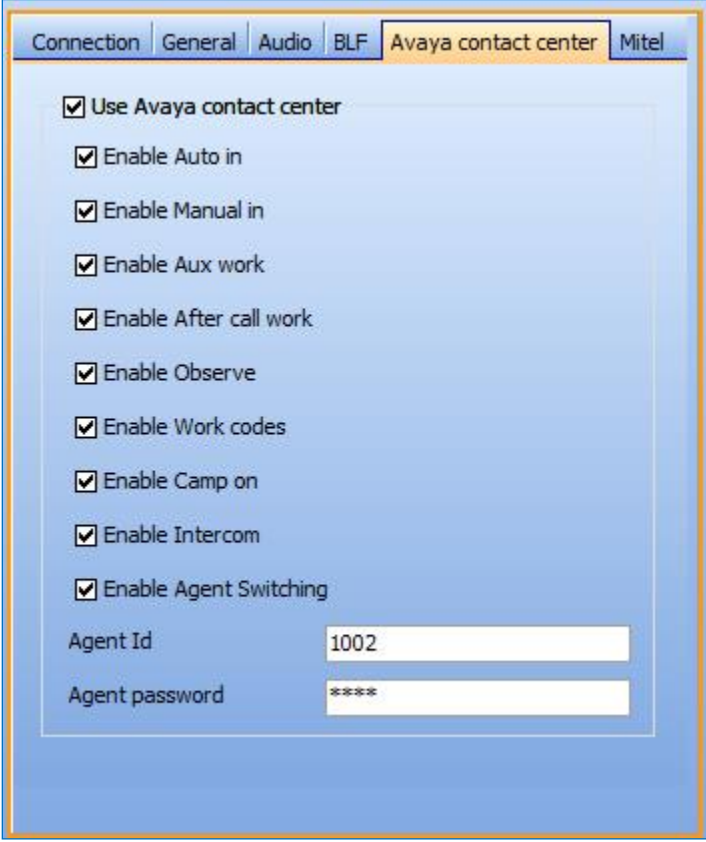
The screenshot shows the 'SIT Options' window with the 'Connection' tab selected. The window is divided into several sections:

- Phone's functions identification:** A table with 24 rows. The first three rows are labeled '3404' and 'Automatic line'. The 'Receive c' and 'Can make' columns are checked for all rows.
- System settings:** Fields for Country (Canada), Local prefix, Long distance prefix (9), Local area code, National code (1), and International code (011).
- Connection tab:** Fields for Username (3404), Password (\*\*\*\*), Domain (avayalab.com), Outbound proxy list (10.33.1.42), External IP (NAT), DNS server, Transport (TCP), RTP port (5004), Local SIP port (5060), and Register type (User and lines). The 'Register with proxy' checkbox is checked.
- Status monitoring:** A checkbox for 'Control status button of logged user' is checked, and the 'Phone ID' is 3404.

In the **Audio** tab, specify the audio device or headset that will be used with the console.

The screenshot shows the 'Audio' tab configuration. The 'Speaker' is set to 'Headset Earphone (Plantronic)', the 'Microphone' is set to 'Headset Microphone (Plantronic)', and the 'Ring' is set to 'Headset Earphone (Plantronic)'.

In the **Avaya contact center** tab, check on the **Use Avaya contact center** check box and its features such as **Enable Auto in**, **Enable Manual in**, **Enable Aux work**, **Enable After call work** and enter the **Agent Id** and **Agent password** as configured in **Section 5.5**.



The screenshot shows a configuration window with several tabs: Connection, General, Audio, BLF, Avaya contact center (selected), and Mitel. The Avaya contact center tab contains a list of checkboxes, all of which are checked: Use Avaya contact center, Enable Auto in, Enable Manual in, Enable Aux work, Enable After call work, Enable Observe, Enable Work codes, Enable Camp on, Enable Intercom, and Enable Agent Switching. Below the checkboxes are two text input fields: Agent Id with the value 1002, and Agent password with the value \*\*\*\*.

Click on the **Save** button  in the **Options** window to save the configuration.

## 8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of the Komutel SIT2 SIP Console with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

1. Verify that the SIT2 SIP Console is successfully registered with Session Manager and acquire the AST feature as well as subscribe the contact center events such as “*avaya-cm-feature-status*” and “*avaya-ccs-profile*”.

### User Registrations

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

View ▾ Default Export Force Unregister

AST Device Notifications: Reboot Reload ▾ Failback As of 9:54 AM

Customize ▾ Advanced Search ▾

4 Items Show All ▾ Filter: Enable

<input type="checkbox"/>	Details	Address	First Name	Last Name	Actual Location	IP Address	Policy	Shared Control	Simult. Devices	AST Device	Registered					
											Prim	Sec	3rd	4th	Surv	Visiting
<input checked="" type="checkbox"/>	▼ Hide	3404@avayalab.com	SIT2	Komutel	---	192.168.11.16	fixed	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

User Registration Device Simultaneous History

Registration Address

IP Address

Actual Location

Active Controller

PPM Subscription Time (AC)

Event Subscriptions

Instance Id

Primary Registration Time

Primary Registration Interrupted Time

3404@avayalab.com

192.168.11.16:56080

---

SM10

Wed Jul 27 11:10:04 MDT 2022

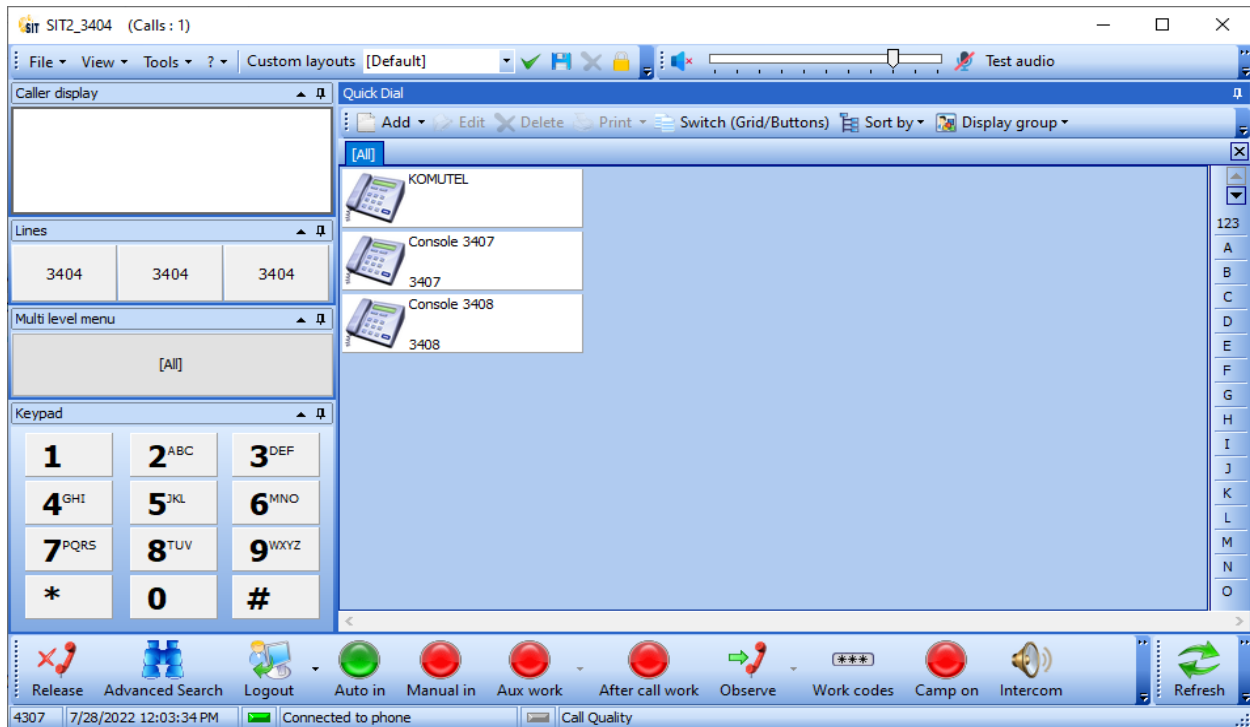
dialog  
message-summary  
reg  
avaya-cm-feature-status  
avaya-ccs-profile

"<urn:uuid:00000000-0000-0000-0000-000096e78cf1>"

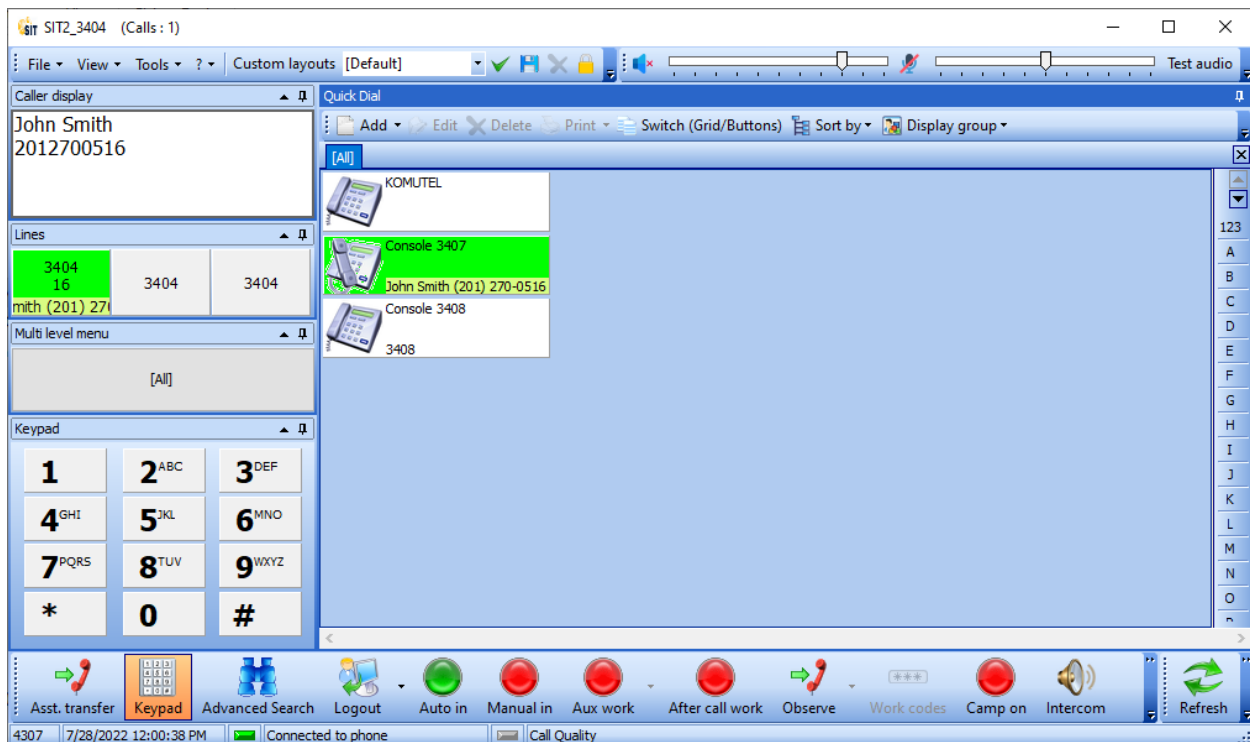
Wed Jul 27 11:09:46 MDT 2022

---

2. Verify SIT2 SIP Console is able to login an agent and set it to the **Ready** status..



3. Verify SIT2 SIP Console was able to receive an inbound call center ACD call.





## 9. Conclusion

These Application Notes describe the configuration steps for provisioning the Komutel SIT2 SIP Console as a SIP agent in Call Center Elite using Advanced SIP Telephony to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Please refer to **Section 2.2** for test results and observations.

## 10. Additional References

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

- [1] *Administering Avaya Aura® Communication Manager*, Release 10.1, Issue 1, December 2021.
- [2] *Administering Avaya Aura® Session Manager*, Release 10.1, Issue 1, April 2021.
- [3] *Administering Avaya Aura® Application Enablement Services*, Release 10.1, Issue 4, April 2022.

---

**©2022 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](mailto:devconnect@avaya.com).