



DevConnect Program

Application Notes for Tetherfi Multimedia Agent Client with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Tetherfi Multimedia Agent Client 5.1 to interoperate with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Application Enablement Services R10.1 using the TSAPI and SMS interface. Tetherfi Multimedia Agent Client is a web-based CTI solution. This thin client provides a single unified CTI desktop capable of servicing Voice, SMS, Email, Chat, Video and Social Media Channels.

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

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

1. Introduction

These Application Notes describe the configuration steps required for Tetherfi Multimedia Agent Client 5.1 to interoperate with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Application Enablement Services R10.1 using the Telephony Service Application Programming Interface (TSAPI) and the System Management Service (SMS) Web Service. Tetherfi Multimedia Agent Client (TMAC) is a web-based CTI solution. This thin client provides a single unified CTI desktop capable of servicing Voice, SMS, Email, Chat, Video and Social Media Channels.

TMAC is an Agent/User desktop application that allows users to control Telephony functions via their desktops PC instead of physical hard phone. It empowers agents/users to interact with customers across multiple channels. TMAC implements TSAPI to provide Computer Telephony Integration (CTI) call control and monitoring functionality, and through the System Management Service (SMS) for dynamic update of wallboard skills list and real-time skill statistics. Contact Center agents log into this desktop to handle all interactions across channels for inbound calls.

Note: Tetherfi Multimedia Agent Client may also be referred to as ‘TMAC’, or ‘Agent Desktop’ throughout these Application Notes.

2. General Test Approach and Test Results

The general test approach was to validate the ability of TMAC to connect to Application Enablement Services and handle and control various Communication Manager endpoints in a variety of call scenarios. Two agents were logged into TMAC, each agent was assigned to a specific Avaya endpoint, a SIP and H.323 endpoint was used during compliance testing. Calls were made to and from these endpoints using TMAC to control the calls.

TMAC makes use of the TSAPI protocol in Application Enablement Services and Application Enablement Services requires ‘Basic licensing’ to support basic features and call monitoring supported methods.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member’s solution.

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

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products. For the testing associated with these Application Notes, the interface between Avaya systems and Tetherfi Multimedia Agent Client did not include use of any specific encryption features as requested by Tetherfi.

2.1. Interoperability Compliance Testing

Interoperability compliance testing consisted of using Multimedia Agent Client to verify successful handling and control of a variety of endpoints as follows:

- Agent Log In/Log Out
- Set Status for ACD Agents
- Non-ACD calls to and from Agent telephones
- ACD/Skillset calls to Agents
- Call Hold/Unhold
- Call Transfers: Blind and Supervised
- Call Conferencing: Blind and Supervised
- Calls from Agent to Agent
- Observing wallboard skills list and real-time skill statistics
- Serviceability Testing by simulating LAN failures

2.2. Test Results

All test cases were executed successfully, with the following observations:

1. There appears to be a two second lag when any of the Agent Desktop functions are used. For example, when the “answer call” icon is pressed, it takes another 2 secs before the call is actually answered and another 1 – 2 secs before the widgets are loaded to view the allowed call functions. This was consistent throughout the testing for all telephony functions. However, if the phone is manually changed state, the result is instantaneous on the Agent Desktop. Tetherfi are aware of this issue.
2. During a consultative/supervised transfer, if the original caller hangs up, the Agent Desktop shows that the original caller is now on hold, this is not the case, it should show that the Agent is on a call with the person they initiated the call to. This is an issue as the call cannot be hung up from the agent desktop. It comes back into sync once the caller hangs up or the call is hung up manually from the phone. Tetherfi are aware of this issue.
3. If an existing call is hung up manually when there is a LAN break between the Tetherfi Server and the Application Enablement Services, this call remains on the Agent Desktop after the LAN is reconnected and it cannot be cleared until the CTI service is restarted. Tetherfi are aware of this issue.

2.3. Support

Technical support on Tetherfi can be obtained through the following:

- Phone: +65-6715 7048 (Singapore), +1-415 9157048 (US)
- Email: support@tetherfi.com
- Web: <https://www.tetherfi.com>

3. Reference Configuration

Figure 1 below shows Avaya Aura® Communication Manager serving both SIP and H.323 endpoints with Avaya Aura® Application Enablement Services providing a TSAPI interface to which the Tetherfi Multimedia Agent Client application connects to. Avaya Aura® Session Manager provides the point of registration for Avaya SIP endpoints. Avaya Aura® System Manager provides a means to manage and configure Session Manager. An SMS connection to AES provides the means to list various components on Avaya Aura® Communication Manager.

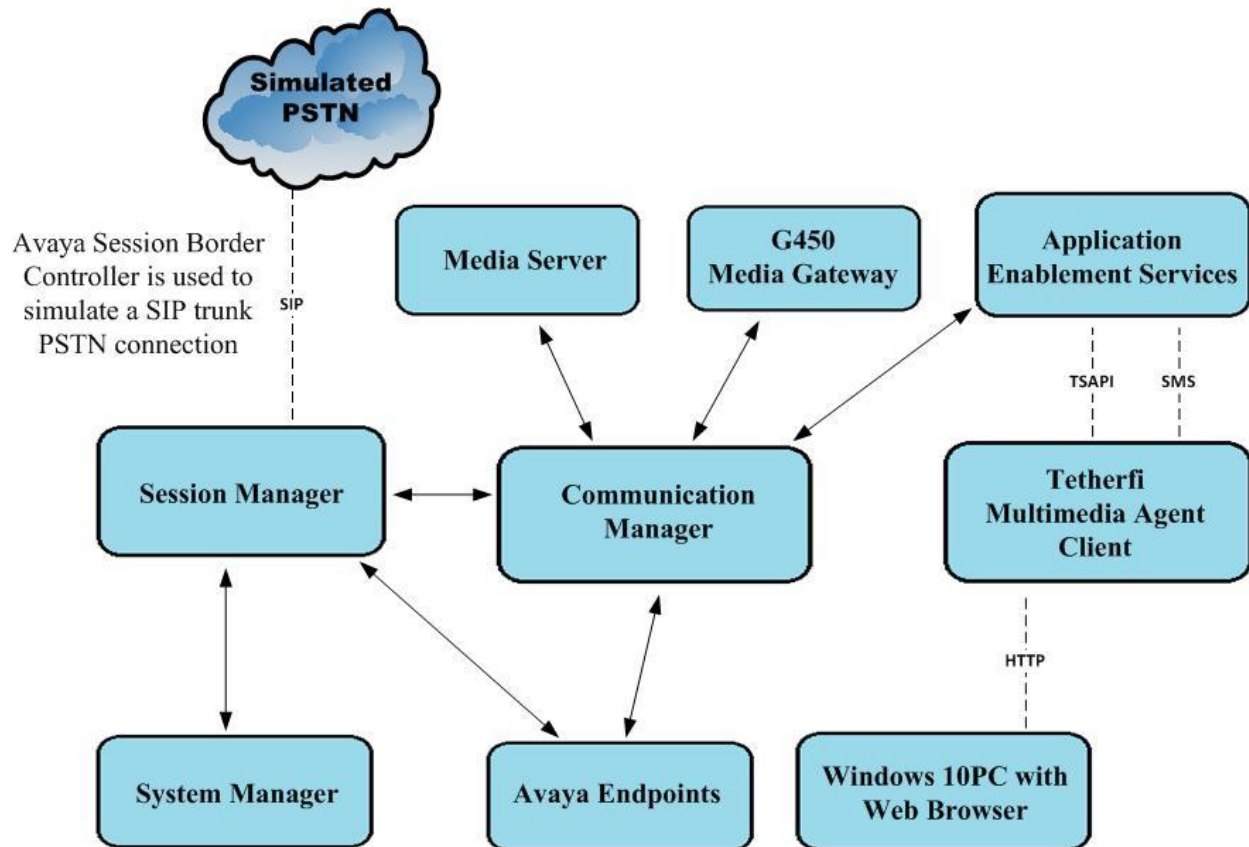


Figure 1: Connection of Tetherfi Multimedia Agent Client with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Application Enablement Services R10.1

4. Equipment and Software Validated

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

Avaya Equipment/Software	Firmware/Version
Avaya Aura® System Manager	System Manager 10.1.3.0 Feature Pack 3 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.3.0.0715713
Avaya Aura® Session Manager	Session Manager R10.1 Build No. – 10.1.3.0.1013007
Avaya Aura® Communication Manager	R10.1.3.0 – FP3 R020x.01.0.974.0 Update ID 01.0.974.0-27893
Avaya Aura® Application Enablement Services	10.1.3 R10.1.3.0.0.11-0
Avaya Aura® Media Server	10.1.0.101
Avaya Media Gateway G450	42.7.0 /2
Avaya J100 Series (H323) Deskphone	6.8.5.3.2
Avaya J100 Series (SIP) Deskphone	4.0.14.0.7
Avaya 9404 Digital Deskphone	17.0
Avaya Session Border Controller (to facilitate simulated PSTN)	10.1
Tetherfi Equipment/Software	Firmware/Version
Tetherfi Multimedia Agent Client Server	5.1
Tetherfi Agent Desktop UI	5.2
Tetherfi CTI Server	6.0
Tetherfi SMS API Server	5.1
Windows 10 PC running a Web Browser	Windows 10/Chrome 119.0.6045.160

All equipment are virtual servers running on VMware.

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section are performed using the Communication Manager System Access Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation as referenced in **Section 10**. The configuration operations described in this section can be summarized as follows:

- Configure TSAPI Interface to Avaya Aura® Application Enablement Services
- Configure Call Center Features
- Configure Avaya SIP Endpoints for Third Party Call Control

5.1. Configure TSAPI Interface to Avaya Aura® Application Enablement Services

The following sections illustrate the steps required to create the TSAPI link between Communication Manager and Application Enablement Services. It is assumed that the switch link (IP Services Interface) between Communication Manager and Application Enablement Services has already been setup as part of the installation of Application Enablement Services.

5.1.1. Verify System Features

Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 4**, ensure that **Computer Telephony Adjunct Links?** is set to **y** as shown below.

display system-parameters customer-options		Page	4 of 12
OPTIONAL FEATURES			
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y
Access Security Gateway (ASG)?	y	Authorization Codes?	y
Analog Trunk Incoming Call ID?	y	CAS Branch?	n
A/D Grp/Sys List Dialing Start at 01?	y	CAS Main?	n
Answer Supervision by Call Classifier?	y	Change COR by FAC?	n
ARS?	y	Computer Telephony Adjunct Links?	y
ARS/AAR Partitioning?	y	Cvg Of Calls Redirected Off-net?	y
ARS/AAR Dialing without FAC?	y	DCS (Basic)?	y
ASAI Link Core Capabilities?	y	DCS Call Coverage?	y
ASAI Link Plus Capabilities?	y	DCS with Rerouting?	y
Async. Transfer Mode (ATM) PNC?	n	Digital Loss Plan Modification?	y
Async. Transfer Mode (ATM) Trunking?	n	DS1 MSP?	y
ATM WAN Spare Processor?	n	DS1 Echo Cancellation?	y
ATMS?	y		
Attendant Vectoring?	y		
(NOTE: You must logoff & login to effect the permission changes.)			

5.1.2. Configure CTI Link for TSAPI Service

Add a CTI link using the **add cti-link n** command, where n is the n is the cti-link number as shown in the example below this is **1**. Enter an available extension number in the **Extension** field. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

add cti-link 1		Page 1 of 3
CTI LINK		
CTI Link: 1		
Extension: 1990		
Type: ADJ-IP		
Name: aespri101x		COR: 1

5.2. Configure Call Center Features

The following were set to allow inbound ACD calls to the Agents logged into Multimedia Agent Client.

- Configure Hunt Group
- Configure Vector
- Configure Vector Directory Number (VDN)
- Configure Agents

5.2.1. Configure Hunt Group

Enter the command **add hunt-group x** where **x** is an appropriate hunt group number and configure as follows:

- **Group Number** – this is the Skill Number when configuring the agent and vector.
- **Group Name** – enter an appropriate name.
- **Group Extension** – enter an extension appropriate to the dialplan.
- **Group Type** – set to **ucd-mia**.
- **ACD?** – set to **y**.
- **Queue?** – set to **y**.
- **Vector?** – set to **y**.

add hunt-group 90		Page 1 of 4
HUNT GROUP		
Group Number: 90		ACD? y
Group Name: Support		Queue? y
Group Extension: 1800		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:

On **Page 2**, set **Skill** to **y**. **Measured** was set to **internal**, to allow the monitoring of skillsets by Communication Manager using the ‘monitor bcms’ command.

add hunt-group 90		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: internal		
Supervisor Extension:		
Controlling Adjunct: none		
VuStats Objective:		
Multiple Call Handling: none		
Timed ACW Interval (sec): After Xfer or Held Call Drops? n		

5.2.2. Configure Vector

Enter the command **change vector x** where **x** is the required vector number. Configure as shown below so that calls **queue-to skill 1st**. Skill 1st is the hunt group configured in the VDN in **Section 5.2.3**.

change vector 1		Page 1 of 6
CALL VECTOR		
Number: 1	Name: Basic Routing	
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	2 secs hearing ringback	
02 queue-to	skill 1st prim	
03 wait-time	100 secs hearing music	
04 goto step	3 if unconditionally	
05 stop		
06		
07		
08		
09		

5.2.3. Configure Vector Directory Number (VDN)

Enter the command **add vdn x** where **x** is the required VDN number appropriate to the dialplan. Configure the VDN to send calls to the vector configured in the previous section as follows:

- **Extension** – note the VDN extension number which will be used to place calls to the Skill vector and on to the Skill.
- **Name** – enter an appropriate name.
- **Destination** – enter the **Vector Number** configured in the previous section.
- **1st Skill** – enter the hunt group created in **Section 5.2.1**.

add vdn 3901	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 3901	Unicode Name? n
Name*: Support	
Destination: Vector Number	1
Attendant Vectoring? n	
Meet-me Conferencing? n	
Allow VDN Override? n	
COR: 1	
TN*: 1	
Measured: none	Report Adjunct Calls as ACD*? n
VDN of Origin Annc. Extension*:	
	1st Skill*: 90
	2nd Skill*:
	3rd Skill*:
SIP URI:	
* Follows VDN Override Rules	

5.2.4. Configure Agents

Agents must be configured with the appropriate Skill Number. Enter the command **add agent-loginID x** where **x** is an agent extension number appropriate to the dialplan and configure as follows:

- **Login ID** – take a note of the configured **Login ID**.
- **Name** – enter an identifying name.
- **Password** – enter a suitable password of the agent.

```
add agent-loginID 3411                                     Page 1 of 2
                                     AGENT LOGINID

      Login ID: 3411                                     Unicode Name? n   AAS? n
      Name: Agent One                                     AUDIX? n
      TN: 1                                           Check skill TNs to match agent TN? n
      COR: 1
      Coverage Path:                                     LWC Reception: spe
      Security Code:                                     LWC Log External Calls? n
      Attribute:                                         AUDIX Name for Messaging:

                                     LoginID for ISDN/SIP Display? n
                                     Password:1234
                                     Password (enter again):1234
                                     Auto Answer: station
      AUX Agent Remains in LOA Queue: system           MIA Across Skills: system
      AUX Agent Considered Idle (MIA): system          ACW Agent Considered Idle: system
      Work Mode on Login: 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**, enter the hunt group number configured in **Section 5.2.1** in the **SN** (Skill Number) column and enter an appropriate **SL** (skill level).

```
add agent-loginID 3411                                     Page 2 of 2
                                     AGENT LOGINID

      Direct Agent Skill: 90                               Service Objective? n
      Call Handling Preference: skill-level                Local Call Preference? n

      SN   RL  SL           SN   RL  SL
      1: 90    1           16:
      2:                   17:
      3:                   18:
      4:                   19:
      5:                   20:
      6:
      7:
      8:
```

5.3. Configure Avaya SIP Endpoints for Third Party Call Control

Each Avaya SIP endpoint or station that needs to be monitored and used for 3rd party call control will need to have “Type of 3PCC Enabled” is set to “Avaya”. Changes to SIP phones on Communication Manager must be carried out by System Manager. Access the System Manager using a Web Browser by entering **http://<FQDN>/network-login**, where <FQDN> is the fully qualified domain name of System Manager, or the IP address of System Manager can be used as an alternative to the FQDN. Log in using the appropriate credentials.

Note: The following shows changes a SIP extension and assumes that the SIP extension has been programmed correctly and is fully functioning.

System Manager

Not secure | <https://10.10.40.10/network-login/>

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.

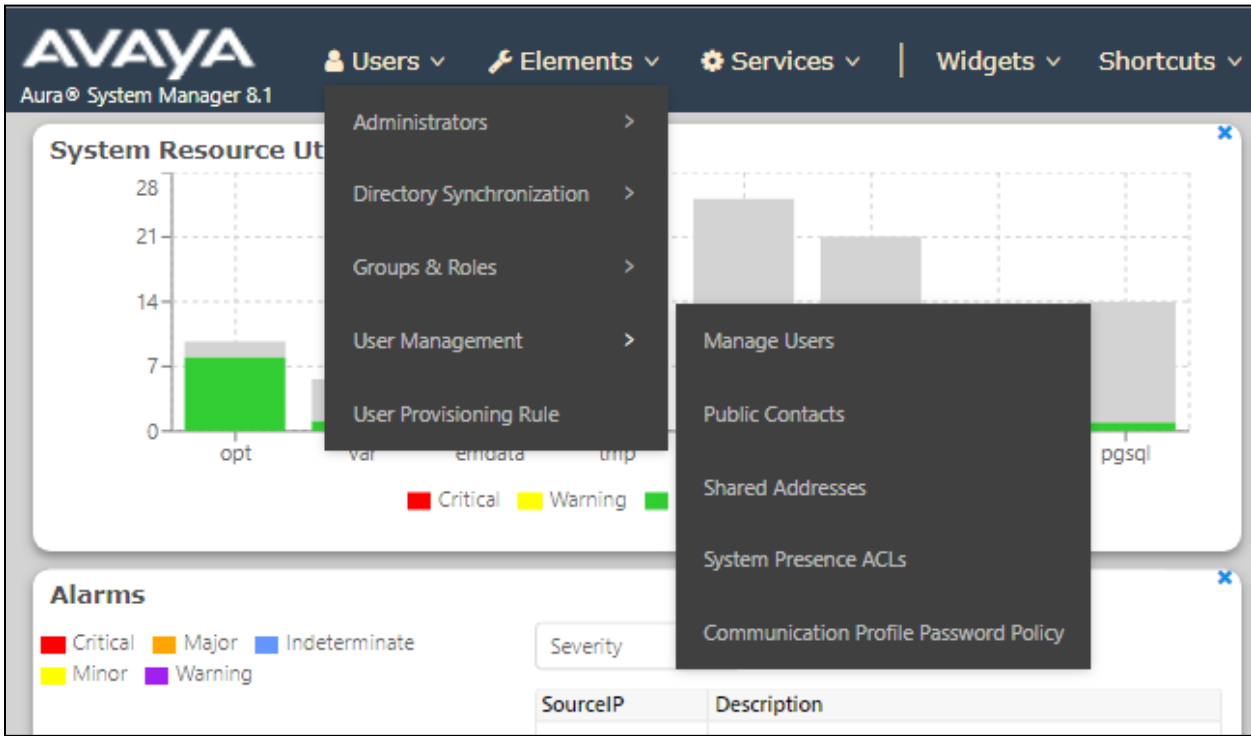
User ID:

Password:

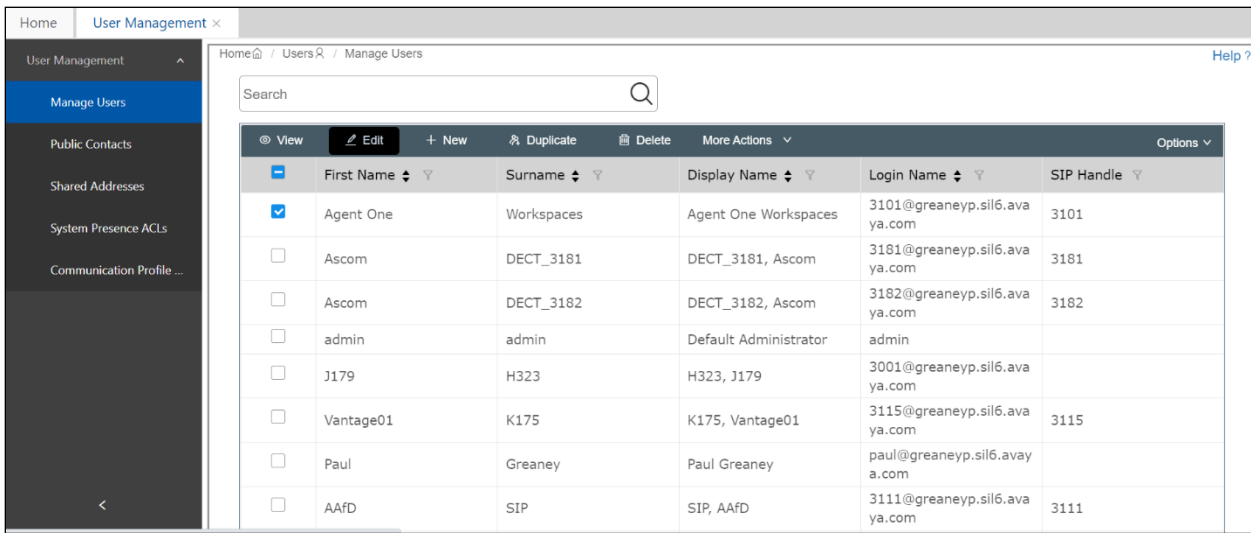
[Change Password](#)

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

From the home page, click on **Users** → **User Management** → **Manage Users**, as shown below.



Click on **Manager Users** in the left window. Select the station to be edited and click on **Edit**.



Click on the **CM Endpoint Profile** tab in the left window. Click on **Endpoint Editor** to make changes to the SIP station.

Home / Users / Manage Users

User Profile | Edit | 3101@greanep.sil6.avaya.com

Commit & Continue Commit Cancel

Identity Communication Profile Membership Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile

Avaya Breeze Profile

CM Endpoint Profile

* System : cm101x

* Profile Type : Endpoint

Use Existing Endpoints :

* Extension : 3101

Template : Start typing...

* Set Type : 9641SIPCC

Security Code : Enter Security Code

Port : S000003

Voice Mail Number : 6667

Preferred Handle : Select

Calculate Route Pattern :

Sip Trunk : aar

In the **General Options** tab ensure that **Type of 3PCC Enabled** is set to **Avaya** as is shown below.

System : cm101x

Extension : 3101

Template : Select

Set Type : 9641SIPCC

Port : S000003

Security Code :

Name : Agent One Workspaces

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

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

* Class of Restriction (COR) : 1

* Emergency Location Ext : 3101

* Tenant Number : 1

* SIP Trunk : aar

Coverage Path 1 :

Lock Message :

Multibyte Language : Not Applicable

* Class Of Service (COS) : 1

* Message Lamp Ext. : 3101

Type of 3PCC Enabled : Avaya

Coverage Path 2 :

Localized Display Name : Agent One Workspaces

Enable Reachability for Station Domain Control : system

SIP URI :

Primary Session Manager

IPv4 : 10.10.40.12

IPv6 :

The buttons were set as shown below but these are not critical to the overall operation of Multimedia Agent Client. Click on **Done** at the bottom of the screen (not shown).

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

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

Main Buttons **Feature Buttons** **Button Modules** **Phone View**

Endpoint Configurations

Favorite	Button Label	Button Feature	Argument-1	Argument-2	Argument-3
1 <input type="checkbox"/>		call-appr			
2 <input type="checkbox"/>		call-appr			
3 <input type="checkbox"/>		call-appr			
4 <input type="checkbox"/>		agnt-login			
5 <input type="checkbox"/>		auto-in			
6 <input type="checkbox"/>		manual-in			
7 <input type="checkbox"/>		aux-work			
8 <input type="checkbox"/>		after-call			

Button Configurations

auto-in Grp

manual-in Grp

Reason Code

after-call Grp

Hunt Grp

Click on **Commit** once this is done to save the changes.

User Profile | Edit | 3101@greanep.sil6.avaya.com

Identity **Communication Profile** **Membership** **Contacts**

Communication Profile Password

PROFILE SET: Primary

Communication Address

PROFILES

Session Manager Profile ☒

Avaya Breeze® Profile ☐

CM Endpoint Profile ☒

*** System:** cm101x

*** Profile Type:** Endpoint

Use Existing Endpoints: ☐

*** Extension:** 3101

Template: Start typing...

*** Set Type:** 9641SIPCC

Security Code: Enter Security Code

Port: S000003

Voice Mail Number: 6667

Preferred Handle: Select

Calculate Route Pattern: ☐

Sip Trunk: aar

Commit & Continue **Commit** **Cancel**

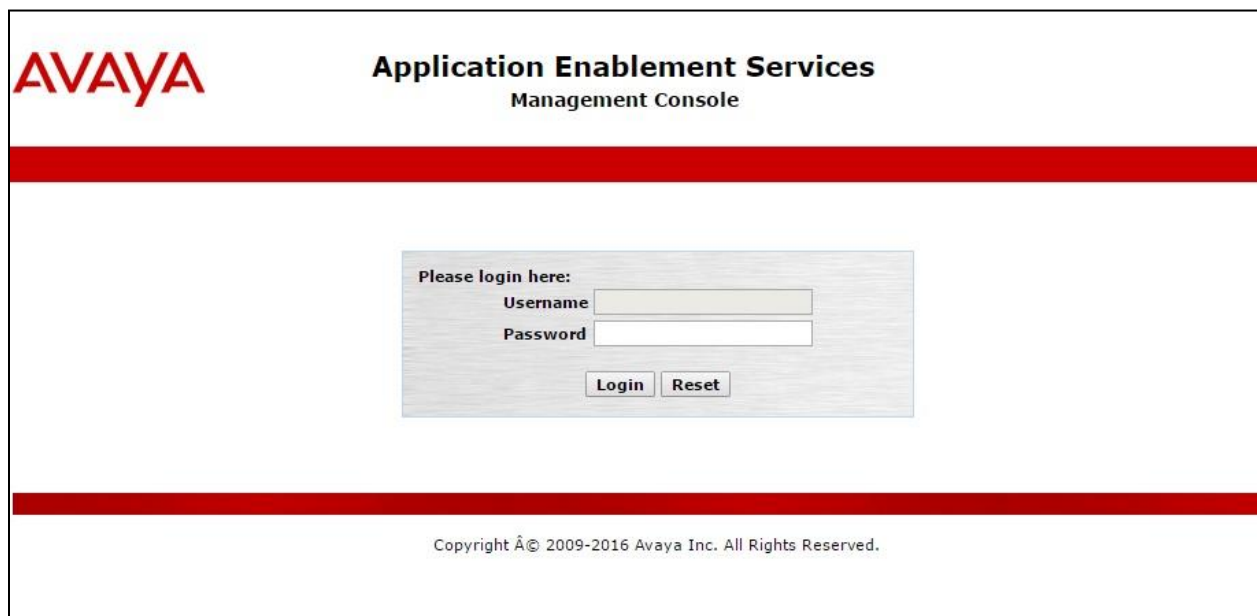
6. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Application Enablement Services. The procedures fall into the following areas:

- Verify Licensing
- Administer TSAPI Link
- Identify Tlinks
- Enable TSAPI Ports
- Create CTI User
- Configure Security
- Configure System Management Service (SMS)
- Restart AE Server

6.1. Verify Licensing

To access the AES Management Console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the IP address of the AES. At the login screen displayed, log in with the appropriate credentials and then select the **Login** button.



The screenshot shows the Avaya Application Enablement Services Management Console login page. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A thick red horizontal bar spans the width of the page below the header. In the center of the page is a light gray rectangular box containing the login form. The form has the text "Please login here:" followed by two input fields: "Username" and "Password". Below these fields are two buttons: "Login" and "Reset". Another thick red horizontal bar is located below the login form. At the bottom of the page, centered, is the copyright notice: "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI Service is licensed by ensuring that **TSAPI Service** is in the list of **Services** and that the **License Mode** is showing **NORMAL MODE**. If not, contact an Avaya support representative to acquire the appropriate license.

The screenshot shows the 'AE Services' management console. On the left is a navigation menu with options like CVLAN, DLG, DMCC, SMS, TSAPI, TWS, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The 'Licensing' option is selected. The main content area is titled 'AE Services' and contains an important note: 'IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.' Below this is a table with the following data:

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A
AE Services HA	Not Configured	N/A	N/A	N/A

Below the table, there is a link to 'Status and Control' and a note: '* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.' At the bottom, there is a 'License Information' section stating: 'You are licensed to run Application Enablement (CTI) release 8.x'.

The TSAPI license is a user licenses issued by the Web License Manager to which the Application Enablement Services server is pointed to. From the left window open **Licensing** and click on **WebLM Server Access** as shown below.

The screenshot shows the 'Licensing' management console. On the left is a navigation menu with options like AE Services, Communication Manager Interface, High Availability, Licensing, WebLM Server Address, WebLM Server Access, Reserved Licenses, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The 'Licensing' option is selected. The main content area is titled 'Licensing' and contains the following text:

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page

The following screen shows the available licenses for **TSAPI** users.

Application_Enablement

View by feature

View by local WebLM

Enterprise configuration

Local WebLM Configuration

Usages

Allocations

Periodic status

CE

COLLABORATION_ENVIRONMENT

COMMUNICATION_MANAGER

Call_Center

Communication_Manager

Configure Centralized Licensing

CONTROLMANAGER

Control_Manager

SESSIONMANAGER

SessionManager

SYSTEM_MANAGER

System_Manager

Uninstall license

Server properties

Metering Collector Configuration

Shortcuts

Help for Licensed products

License Summary: Avaya DevConnect Any Edition 15 United States

License Host: 00000000000000000000000000000000

Notes: This production license file is for use on a production license host.

License File Path: /etc/opt/avaya/

Feature (License Keyword)	License Capacity	Currently available
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	1000	1000
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	16	16
Device Media and Call Control (VALUE_AES_DMCC_DMC)	1000	1000
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	3	3
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	3	3
DLG (VALUE_AES_DLG)	16	16
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	1000	997
Product Notes (VALUE_NOTES)	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSCP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP,,; CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; ANAV_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; UNIFIED_DESKTOP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; AACC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CE_AGENT_STATES_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; TP_CITFNT_001, BasicUnrestricted, . . . AgentEvents: EXT_CITFNT_001, . . .	Not counted

6.2. Administer TSAPI link

From the Application Enablement Services Management Console, select **AE Services** → **TSAPI** → **TSAPI Links**. Select **Add Link** button as shown in the screen below.

The screenshot shows the 'AE Services | TSAPI | TSAPI Links' interface. On the left, a sidebar lists 'AE Services' with sub-items: CVLAN, DLG, DMCC, SMS, TSAPI (expanded), TSAPI Links (selected), and TSAPI Properties. The main area is titled 'TSAPI Links' and contains a table with two columns: 'Link' and 'Switch Connection'. Below the table are three buttons: 'Add Link', 'Edit Link', and 'Delete Link'.

On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the appropriate switch connection **cm101x**, which has already been configured from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.1.2** which is **1**.
- **ASAI Link Version:** This should be set to the highest version available.
- **Security:** This should be set to **Both** allowing both secure and nonsecure connections.

Once completed, select **Apply Changes**.


The screenshot shows the 'AE Services | TSAPI | TSAPI Links' interface. On the left, a sidebar lists 'AE Services' with sub-items: CVLAN, DLG, DMCC, SMS, TSAPI (expanded), TSAPI Links (selected), TSAPI Properties, TWS, and Communication Manager Interface. The main area is titled 'Edit TSAPI Links' and contains the following fields:

- Link: 1
- Switch Connection: cm101x (dropdown)
- Switch CTI Link Number: 1 (dropdown)
- ASAI Link Version: 12 (dropdown)
- Security: Both (dropdown)

At the bottom are three buttons: 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'.

Another screen appears for confirmation of the changes made. Choose **Apply**.

Apply Changes to Link

Warning! Are you sure you want to apply the changes?
These changes can only take effect when the TSAPI server restarts.
 **Please use the Maintenance -> Service Controller page to restart the TSAPI server.**

When the TSAPI Link is completed, it should resemble the screen below.

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<input checked="" type="radio"/> 1	cm101x	1	12	Both

6.3. Identify Tlinks

Navigate to **Security** → **Security Database** → **Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure TMAC in **Section 7.1.2**.

Security | Security Database | Tlinks

▶ **AE Services**

▶ **Communication Manager Interface**

High Availability

▶ **Licensing**

▶ **Maintenance**

▶ **Networking**

▼ **Security**

▶ Account Management

▶ Audit

▶ Certificate Management

Enterprise Directory

▶ Host AA

▶ PAM

▼ **Security Database**

▪ Control

⊕ CTI Users

▪ Devices

▪ Device Groups

▪ **Tlinks**

▪ Tlink Groups

▪ Worktops

Tlinks

Tlink Name

☒ AVAYA#CM101X#CSTA#AESPRI101X

☐ AVAYA#CM101X#CSTA-S#AESPRI101X

Delete Tlink

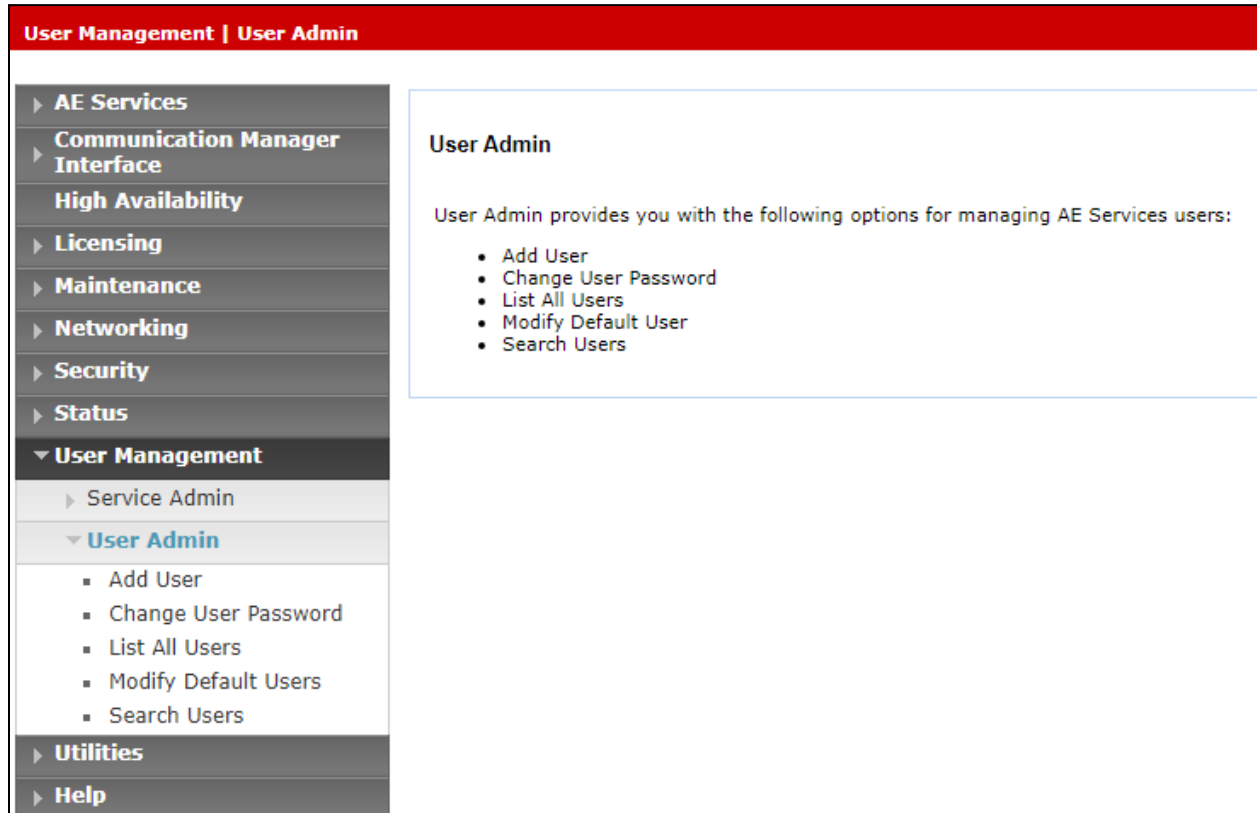
6.4. Enable TSAPI Ports

To ensure that TSAPI ports are enabled, navigate to **Networking → Ports**. Ensure that the TSAPI ports are set to **Enabled** as shown below.

Networking Ports				
<ul style="list-style-type: none"> AE Services Communication Manager Interface High Availability Licensing Maintenance Networking AE Service IP (Local IP) Network Configure Ports TCP/TLS Settings Security Status User Management Utilities Help 	Ports			
	CVLAN Ports			Enabled Disabled
	Unencrypted TCP Port	9999	<input checked="" type="radio"/>	<input type="radio"/>
	Encrypted TCP Port	<input type="text" value="9998"/>	<input checked="" type="radio"/>	<input type="radio"/>
	DLG Port	TCP Port	5678	
	TSAPI Ports			Enabled Disabled
	TSAPI Service Port	450	<input checked="" type="radio"/>	<input type="radio"/>
	Local TLINK Ports			
	TCP Port Min	1024		
TCP Port Max	1039			
Unencrypted TLINK Ports				
TCP Port Min	<input type="text" value="1050"/>			
TCP Port Max	<input type="text" value="1065"/>			
Encrypted TLINK Ports				
TCP Port Min	<input type="text" value="1066"/>			
TCP Port Max	<input type="text" value="1081"/>			
DMCC Server Ports			Enabled Disabled	
Unencrypted Port	<input type="text" value="4721"/>	<input checked="" type="radio"/>	<input type="radio"/>	
Encrypted Port	<input type="text" value="4722"/>	<input checked="" type="radio"/>	<input type="radio"/>	
TR/87 Port	<input type="text" value="4723"/>	<input checked="" type="radio"/>	<input type="radio"/>	
H.323 Ports				
TCP Port Min	<input type="text" value="20000"/>			
TCP Port Max	<input type="text" value="29999"/>			
Local UDP Port Min	<input type="text" value="20000"/>			
Local UDP Port Max	<input type="text" value="29999"/>			
Server Media			Enabled Disabled	
			<input checked="" type="radio"/> <input type="radio"/>	

6.5. Create CTI User

A user ID and password needs to be configured for the Tetherfi to communicate with the Application Enablement Services server. Navigate to the **User Management** → **User Admin** screen then choose the **Add User** option.



In the **Add User** screen shown below, enter the following values:

- **User Id** - This will be used by the TMAC setup in **Section 7.1.2**.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with TMAC setup in **Section 7.1.2**.
- **CT User** - Select **Yes** from the drop-down menu.

Click on **Apply Changes** at the bottom of the screen.

Edit User	
* User Id	<input type="text" value="devconnect"/>
* Common Name	<input type="text" value="devconnect"/>
* Surname	<input type="text" value="devconnect"/>
User Password	<input type="password" value="....."/>
Confirm Password	<input type="password" value="....."/>
Admin Note	<input type="text"/>
Avaya Role	<input type="text" value="None"/>
Business Category	<input type="text"/>
Car License	<input type="text"/>
CM Home	<input type="text"/>
Css Home	<input type="text"/>
CT User	<input type="text" value="Yes"/>
Department Number	<input type="text"/>
Display Name	<input type="text"/>
Employee Number	<input type="text"/>
Employee Type	<input type="text"/>
Enterprise Handle	<input type="text"/>
Given Name	<input type="text"/>
Home Phone	<input type="text"/>
Home Postal Address	<input type="text"/>
Initials	<input type="text"/>
Labeled URI	<input type="text"/>

6.6. Configure Security

The CTI user permissions and the database security are set under **Security Database**.

6.6.1. Configure Database Control

The security database can be set differently depending on the requirements of the customer in question. For compliance testing, the DevConnect lab was setup as shown below, however this may be changed by opening **Control** and ticking the boxes shown.

The screenshot displays the Avaya DevConnect configuration interface. On the left is a navigation pane with a tree structure. The 'Security' folder is expanded, showing sub-items: Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database (expanded), Control (selected), and CTI Users. The main content area on the right is titled 'SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services'. It contains two checkboxes: 'Enable SDB for DMCC Service' (unchecked) and 'Enable SDB for TSAPI Service, JTAPI and Telephony Web Services' (checked). Below these is an 'Apply Changes' button.

SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services	
<input type="checkbox"/>	Enable SDB for DMCC Service
<input checked="" type="checkbox"/>	Enable SDB for TSAPI Service, JTAPI and Telephony Web Services
<button>Apply Changes</button>	

Note: The AES Security Database (SDB) provides the ability to control a user's access privileges. The SDB stores information about Computer Telephony (CT) users and the devices they control. The DMCC service, the TSAPI service, and Telephony Web Services use this information for permission checking. Please look to **Section Error! Reference source not found.** for more information on this.

6.6.2. Configure Access of Tetherfi CTI User

Navigate to **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the CTI user added in **Section 6.5** and click on **Edit**.

Security | Security Database | CTI Users | List All UsersHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▶ Certificate Management

Enterprise Directory

▶ Host AA

▶ PAM

▼ Security Database

▪ Control

▣ CTI Users

▪ List All Users

▪ Search Users

▪ Devices

▪ Device Groups

CTI Users

User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> asc	asc	NONE	NONE
<input type="radio"/> centricity	centricity	NONE	NONE
<input checked="" type="radio"/> devconnect	devconnect	NONE	NONE
<input type="radio"/> mitel	mitel	NONE	NONE
<input type="radio"/> nice1	nice1	NONE	NONE
<input type="radio"/> paul1	paul1	NONE	NONE
<input type="radio"/> paul2	paul2	NONE	NONE
<input type="radio"/> qfiniti	qfiniti	NONE	NONE
<input type="radio"/> smoke	smoke	NONE	NONE
<input type="radio"/> sytel	Sytel	NONE	NONE
<input type="radio"/> voxtronic	voxtronic	NONE	NONE

EditList All

In the main window ensure that **Unrestricted Access** is ticked. Once this is done click on **Apply Changes**.

Edit CTI User

User Profile:

User ID
Common Name
Worktop Name
Unrestricted Access

devconnect
devconnect
NONE ▼
☒

Call and Device Control:

Call Origination/Termination and Device Status

None ▼

Call and Device Monitoring:

Device Monitoring
Calls On A Device Monitoring
Call Monitoring

None ▼
None ▼
☐

Routing Control:

Allow Routing on Listed Devices

None ▼

Apply Changes

Cancel Changes

Click on **Apply** when asked again to **Apply Changes** (not shown).

6.7. Configure System Management Service (SMS)

Navigate to **AE Services** → **SMS** → **SMS Properties**. The only change that should be necessary is the value set in the **Default CM Host Address**, this should be set to the IP address of Communication Manager. Everything else should be as default, or as shown below. Click on **Apply Changes** to ensure that all is saved correctly.

AE Services | SMS | SMS Properties

▼ **AE Services**

▶ CVLAN

▶ DLG

▶ DMCC

▼ **SMS**

▪ **SMS Properties**

▶ TSAPI

▶ TWS

▶ **Communication Manager Interface**

▶ **High Availability**

▶ **Licensing**

▶ **Maintenance**

▶ **Networking**

SMS Properties

Default CM Host Address10.10.40.13

Default CM Admin Port5022

CM Connection ProtocolSSH ▼

SMS LoggingNORMAL ▼

SMS Log Destinationapache ▼

CM Proxy Trace LoggingNONE ▼

Max Sessions per CM5

Proxy Shutdown Timer1800seconds

SAT Login Keepalive180seconds

CM Terminal TypeOSSIZ ▼

Proxy Log Destination/var/log/avaya/aes/ossicm.log

Apply Changes

Restore Defaults

Cancel

6.8. Restart AE Server

Once everything is configured correctly, it is best practice to restart AE Server (if possible), this will ensure that the new connections are brought up correctly. Click on the **Restart AE Server** button at the bottom of the screen.

Maintenance | Service Controller

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

Start

Stop

Restart Service

Restart AE Server

Restart Linux

Restart Web Server

A message confirming the restart will appear, click on **Restart** to proceed.

Maintenance | Service Controller

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

Restart AE Server

Warning! Are you sure you want to restart?
Restarting will cause all existing connections to be dropped and associations lost.

Restart

Cancel

7. Configure Tetherfi Multimedia Agent Client

This section provides the procedures for configuring Multimedia Agent Client. The following two connections to Application Enablement Services must be configured on Multimedia Agent Client, as well as the Users/Agents on OCM.

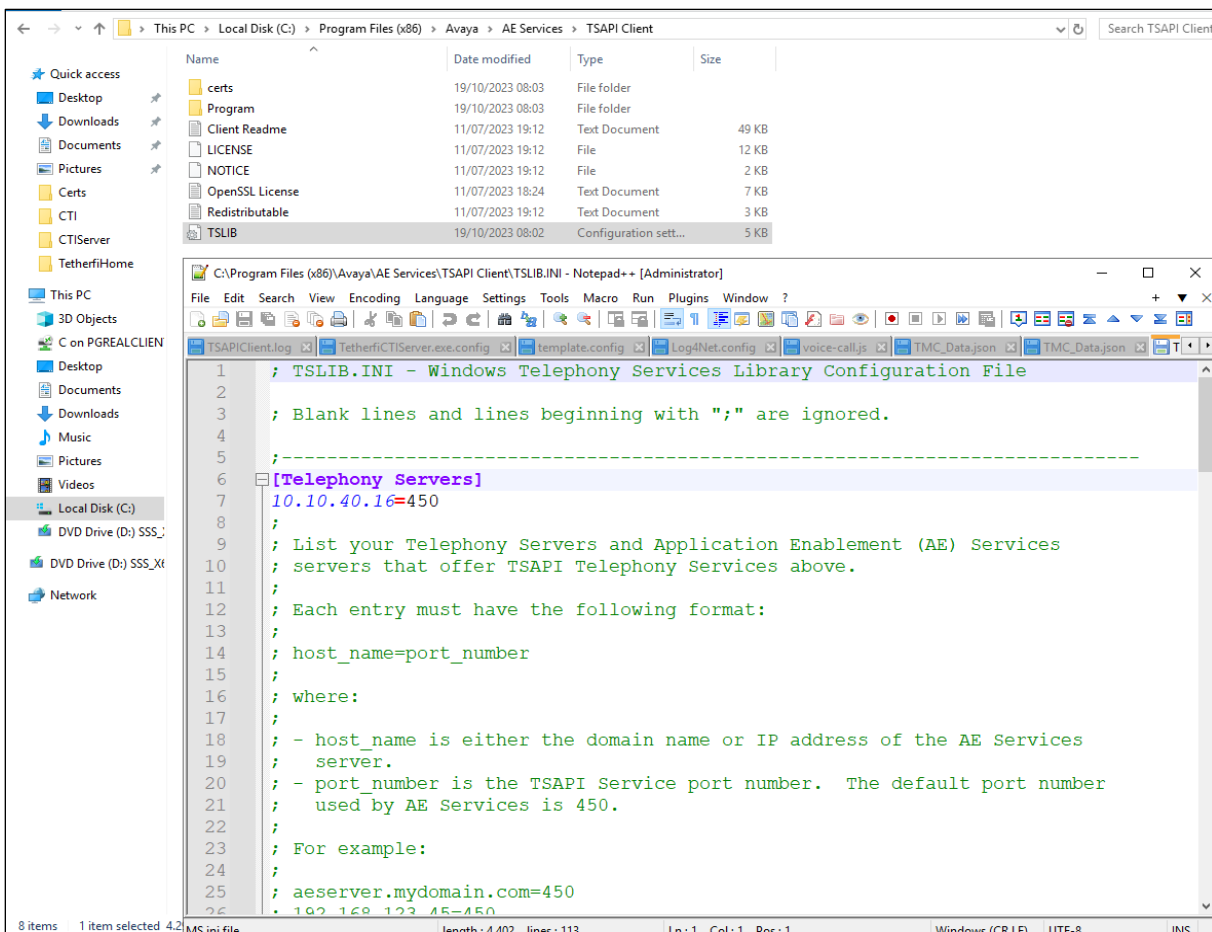
- Telephony Service Application Programming Interface
- System Management Service (SMS) Web Service

7.1. Configure the Telephony Service Application Programming Interface connection to Avaya Aura® Application Enablement Services

Both the TSAPI client connection and the TSAPI credentials must be configured.

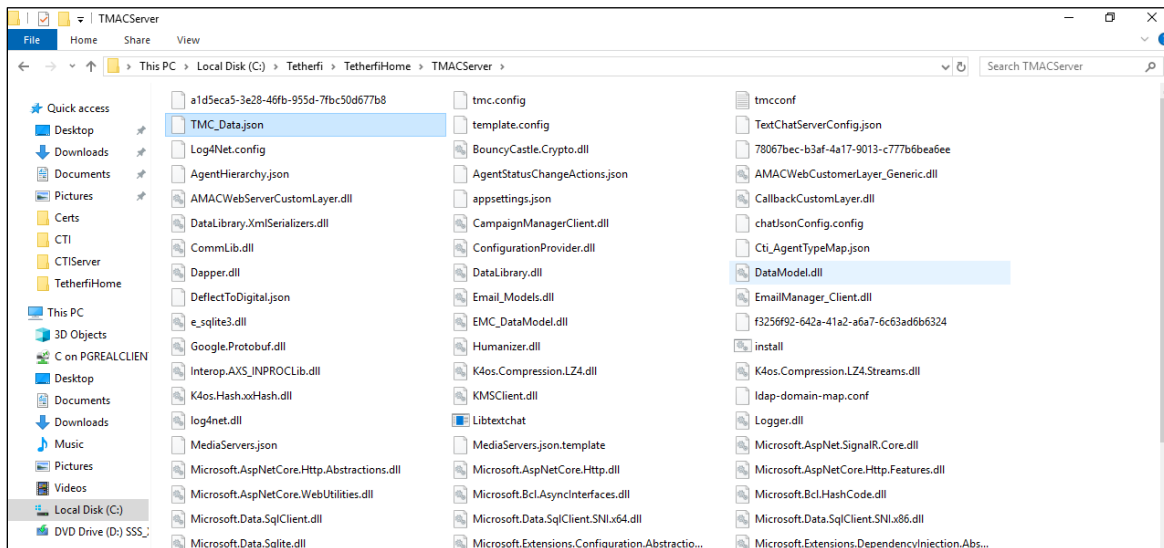
7.1.1. Configure TSAPI Client

The TSAPI client must be installed on the TMAC server, this is part of the overall installation and it not shown here. Once installed the TSLIB.ini file is located and edited. Enter the IP address of the Application Enablement Services server along with the port number as per **Section 6.4**.

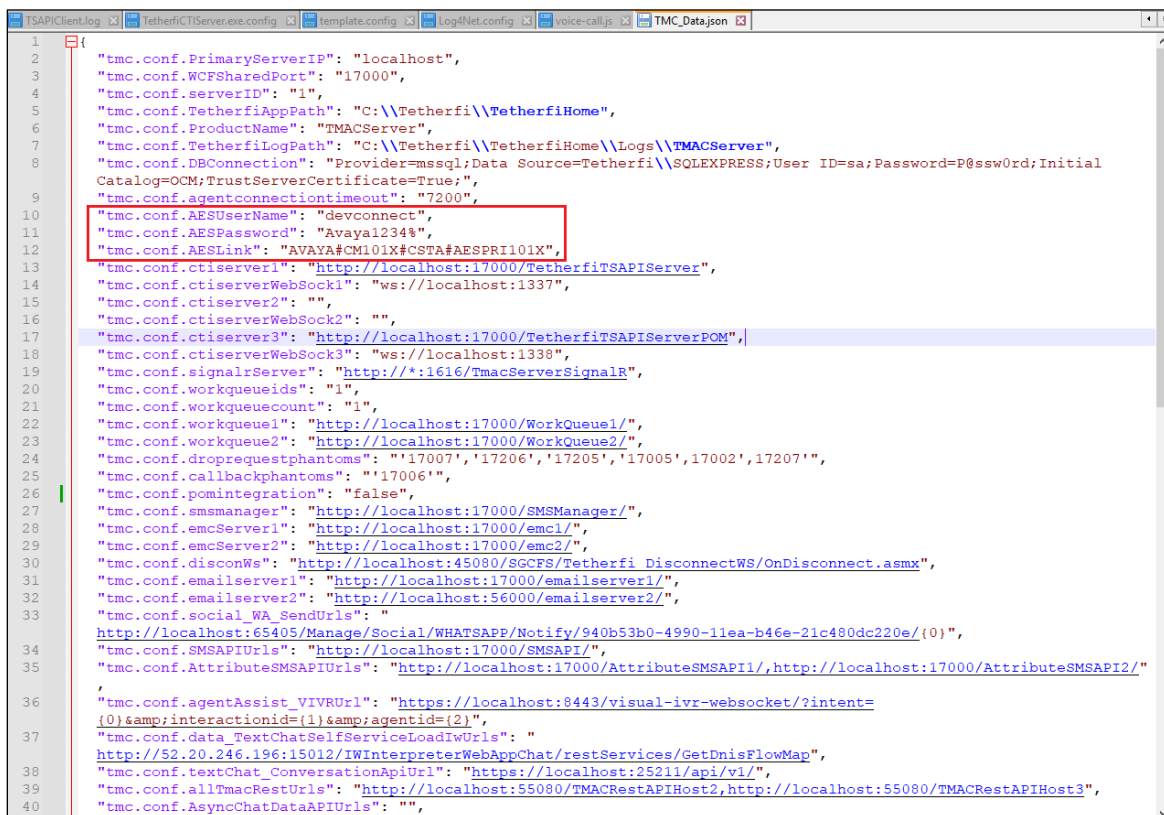


7.1.2. Configure TSAPI credentials

Open the file **TMC_data.json** which should be located as shown below.

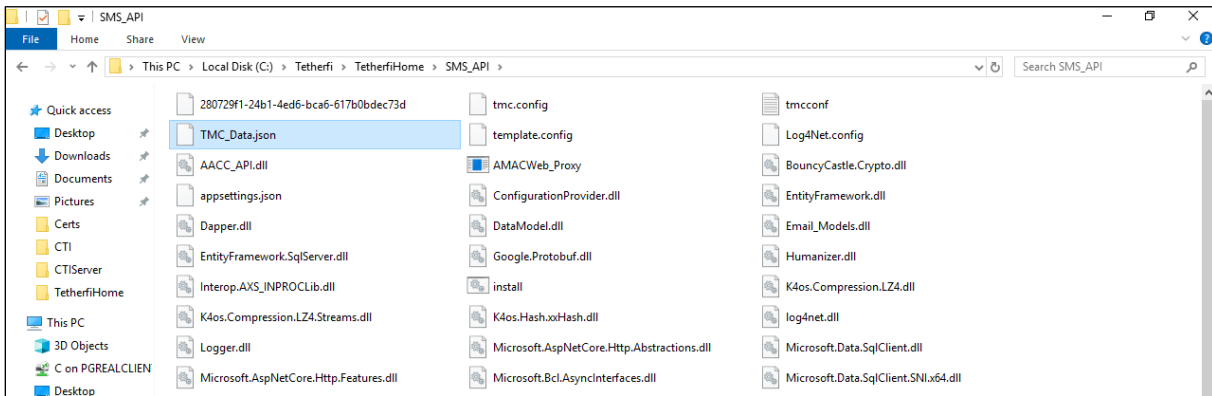


The highlighted information shows the credentials that were used to connect to Application Enablement Services TSAPI, and these should match that of **Section 6.5** and **Section 6.3**.

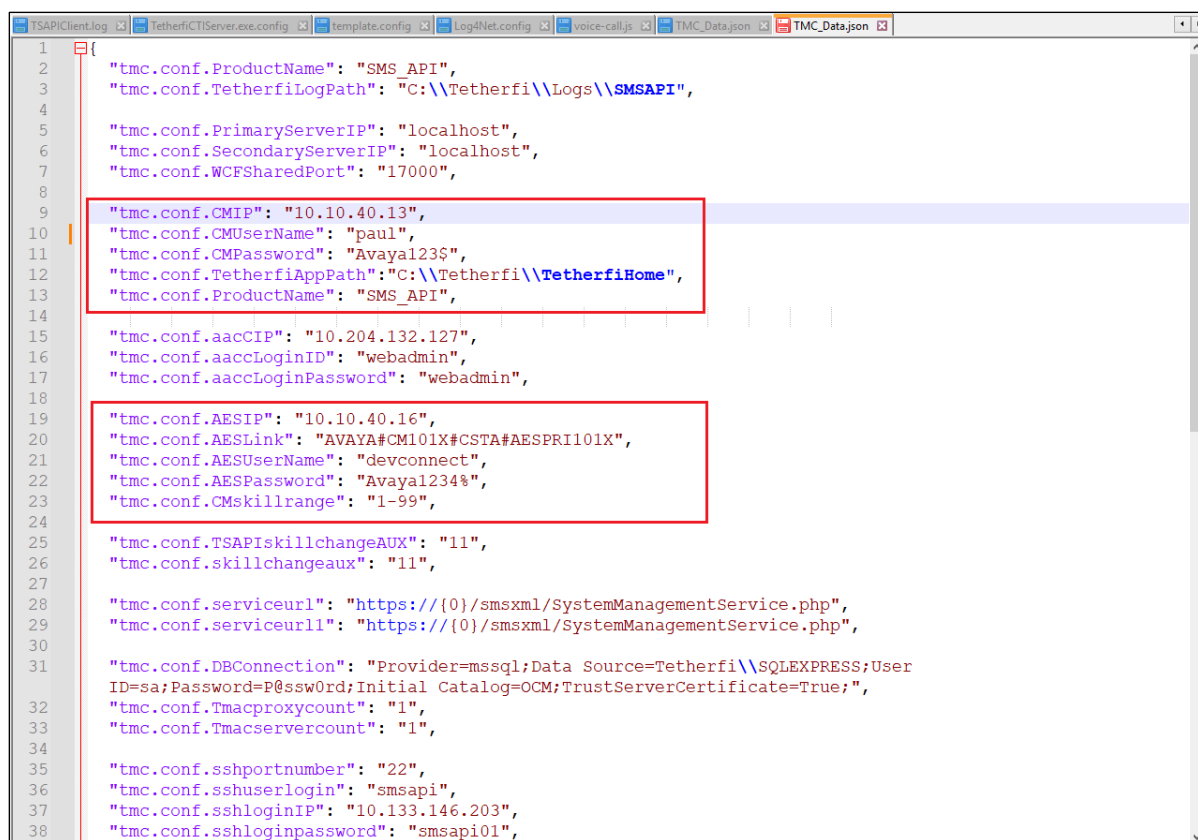


7.2. Configure the SMS connection to Avaya Aura® Application Enablement Services

Open the **TMC_Data.json** file located as shown below.

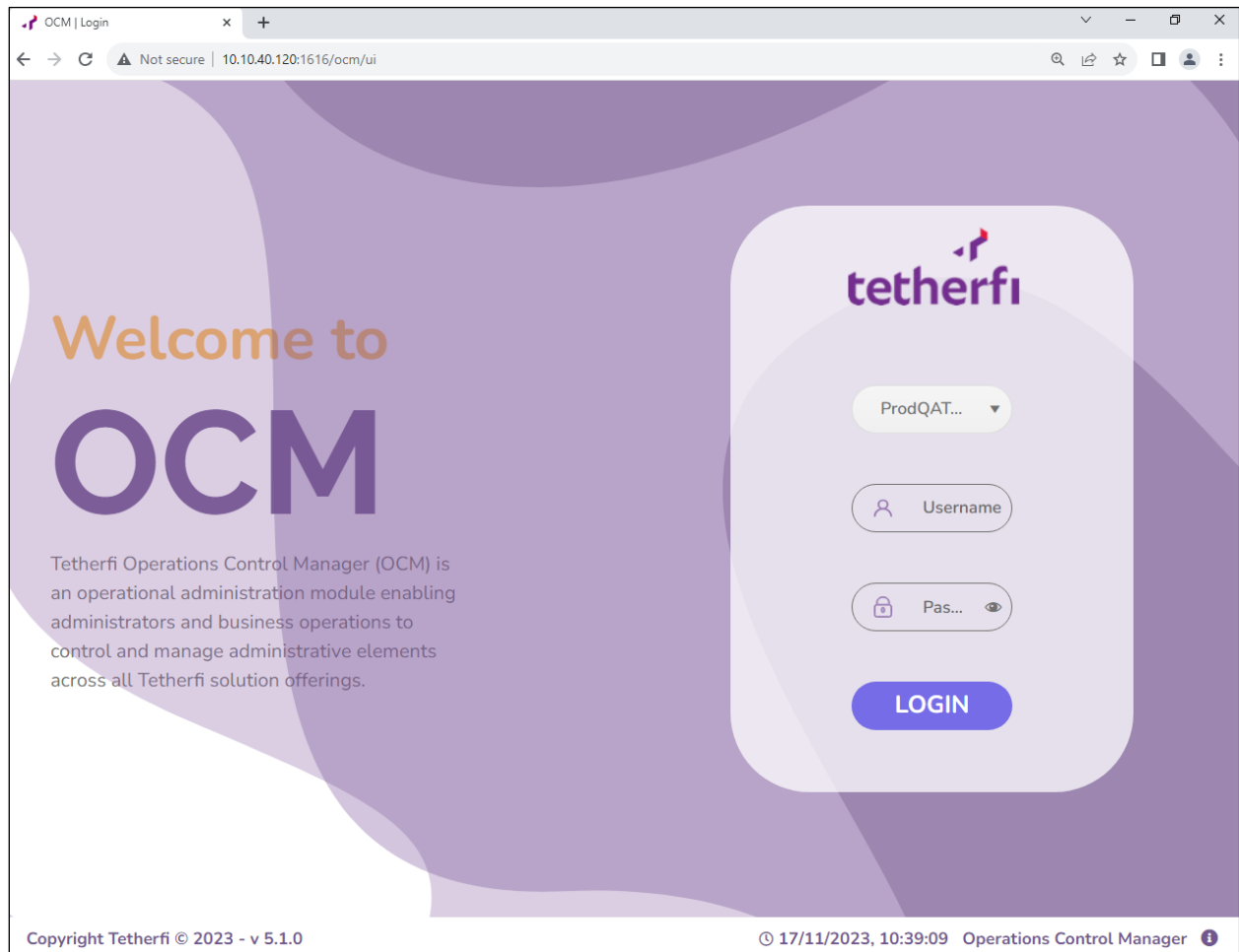


The highlighted sections below are relevant to the connection to Application Enablement Services to gather the skillset and agent details for real-time displays. Note that an existing user/password for Communication Manager was used for compliance testing and the IP address of Communication Manager was also added. The same details for the TSAPI user on Application Enablement Services is also added as shown.

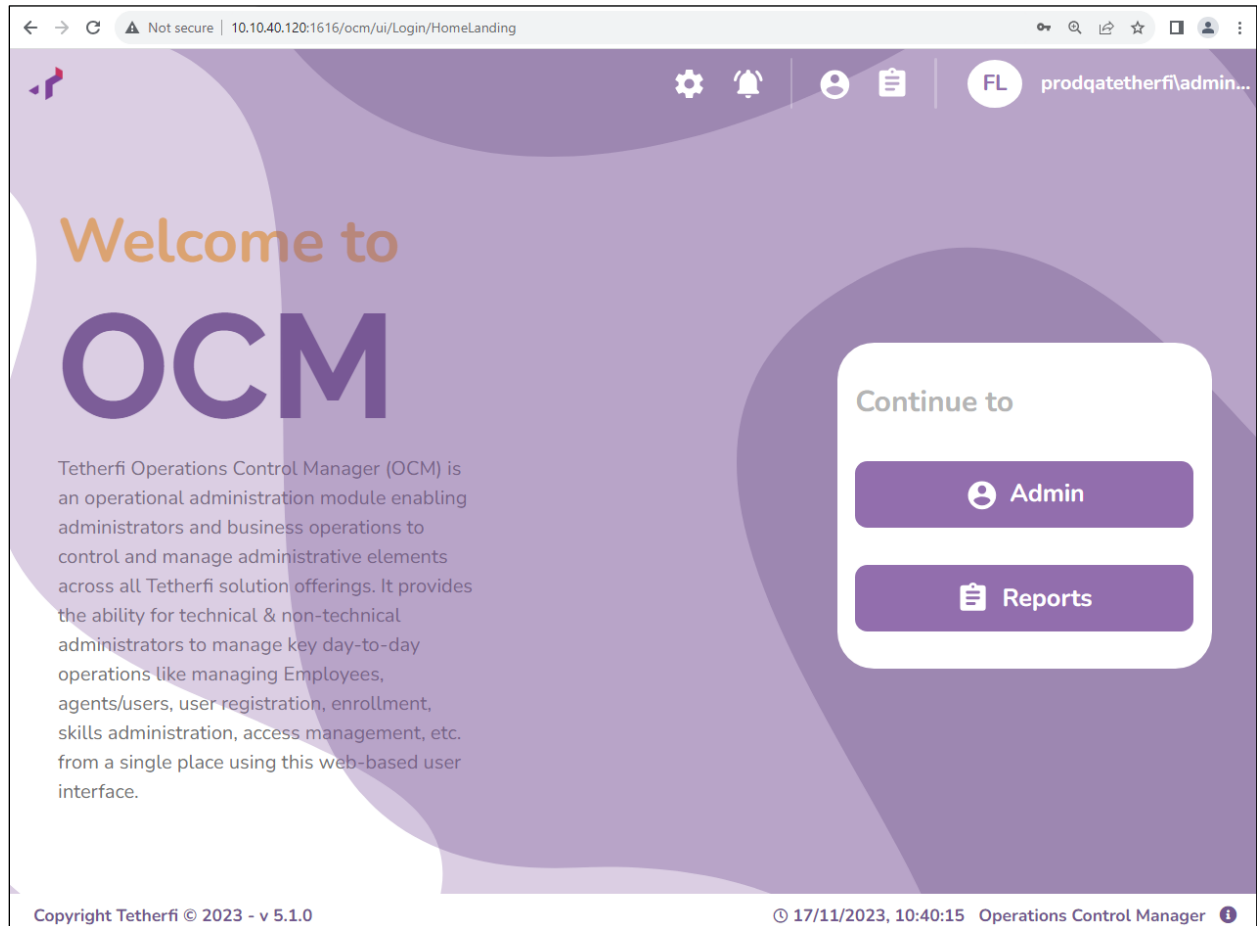


7.3. Configure the Users/Agents on Tetherfi Operations Control Manager

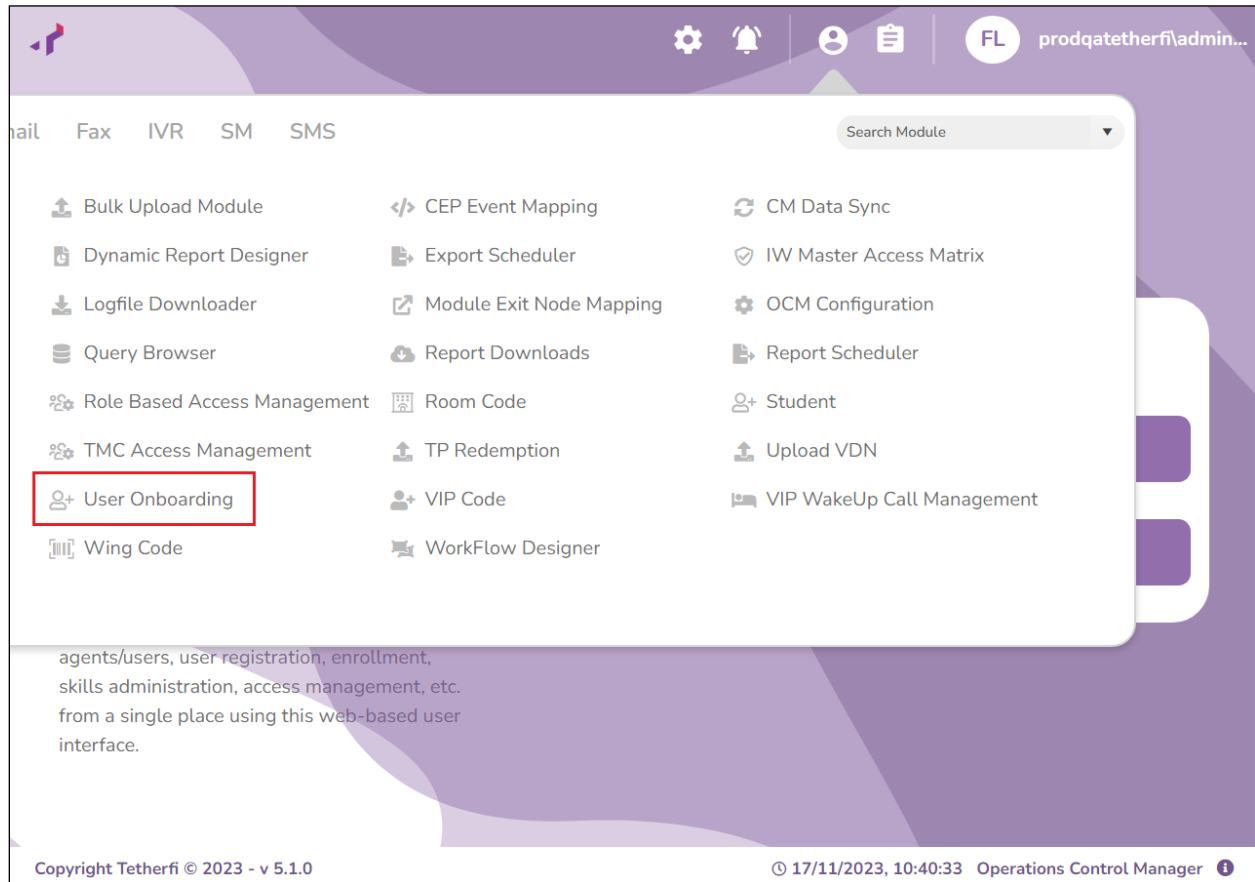
Open the Tetherfi Operations Control Manager (OCM) by opening a browser session to the <server IP address>:1616/ocm/ui, as shown.



Once logged in click on **Admin**.



Select **User Onboarding** as highlighted below.



The following users were created for DevConnect testing. However, to create a new user, click on + **Add New User Onboarding Record**.

The screenshot shows the 'User Onboarding' page in the OCM interface. It includes a header with the OCM logo and navigation icons. Below the header, there are buttons for '+ Add New User Onboarding Record', 'Invite User', and 'Select Action...'. A search bar and 'Export to Excel' button are also present. The main content area displays a table of users. The table has columns for Profile, Lan ID, First Name, Last Name, Agent ID, PBX ID, Profile, and Supervisor. Three users are listed: 'Administr...', 'devconne...', and 'devconne...'. Each user row has a checkbox, a pencil icon for editing, and a trash icon for deletion.

			Profi...	Lan ID	First ...	Last ...	Agent...	PBX ID	Profile	Superv
▶	<input type="checkbox"/>			Administr...	FirstName	LastName	50001	50001	Supervisor	NA
▶	<input type="checkbox"/>			devconne...	dev	connect1	3411	3411	Supervisor	NA
▶	<input type="checkbox"/>			devconne...	dev	connect2	3412	3412	Supervisor	NA

The following screen shows the information for the existing user **devconnect1** which is associated with Communication Manager Elite agent **3411**, as per **Section 5.2.4**. The same screen would be present for a new user where the information added should resemble something like shown below. The **Lan ID** may be used to match up with a local LDAP server and this is then associated with both the **Agent ID** and **PBX ID** which should be that of the Communication Manager Elite agent. Click on **Next** to continue.

User Onboarding

Personal Info

Profile Picture

Secondary Profil...

Channel Count

Features

Role Mapping

Access Role

Miscellaneous

Lan ID*

devconnect1

Last Name*

connect1

PBX ID*

3411

Profile*

Superv...

Is Active*

☒

First Name*

dev

Agent ID*

3411

Org. Unit*

Tet... X

Superviso

NA

Step 1 of 8

Next

Clicking **Next** until the **Channel Count** tab appears, where the types of channels are associated with the agent. For compliance testing only **Voice** was used and so this was ticked, and two channels were associated to this agent. Click on **Next** again to move on.

The screenshot shows the 'User Onboarding' window at Step 4 of 8, titled 'Channel Count'. On the left is a vertical navigation menu with icons and labels: Personal Info, Profile Picture, Secondary Profil..., Channel Count (highlighted with a gear icon), Features, Role Mapping, Access Role, and Miscellaneous. The main content area contains several channel types with checkboxes and numeric input fields:

- Voice**: Checked, value 2
- Text Chat**: Unchecked, value 0
- Audio Chat**: Unchecked, value 0
- Video Chat**: Unchecked, value 0
- Fax**: Unchecked, value 0
- SMS**: Unchecked, value 0
- Email Channel**: Unchecked, value 0

 At the bottom, it says 'Step 4 of 8' and has 'Previous' and 'Next' buttons.

The **Features** are added here. These are the features that were ticked for compliance testing.

The screenshot shows the 'User Onboarding' window at Step 5 of 8, titled 'Features'. The left navigation menu is the same as in Step 4, with 'Features' now highlighted with a magnifying glass icon. The main content area lists various features with checkboxes and input fields:

- Allow Supervisor to CapturePicture**: Unchecked
- Allow Supervisor to interaction notification**: Checked, with 'Enter Feature Value' below it
- Allow Supervisor to logout**: Checked, with 'Enter Feature Value' below it
- Allow Supervisor to send notification**: Checked, with 'Enter Feature Value' below it
- Auto Answer All ACD Calls**: Checked, with 'Enter Feature Value' below it
- Go ACW After Each ACD Calls**: Checked, with 'Enter Feature Value' below it
- Go ACW After Any Calls**: Checked, with 'Enter Feature Value' below it
- Text Chat Auto Answer**: Checked, with 'Enter Feature Value' below it
- Text Chat Auto ACW Enabled**: Checked, with 'Enter Feature Value' below it
- TRS POPUP PROGRAM GAMIFICATION TRACK**: Unchecked

 At the bottom, it says 'Step 5 of 8' and has 'Previous' and 'Next' buttons.

Click on Next to fill in any other information that may need to be added. Once everything is configured as required, click on **Save** at the bottom of the screen.

User Onboarding

Profile Picture

Secondary Profil...

Channel Count

Features

Role Mapping

Access Role

Miscellaneous

CRM Name

Select

Text Template

Select

Step 8 of 8

Previous

Modify Reason*

Save

Cancel

8. Verification Steps

The correct configuration of the solution can be verified as follows.

8.1. Verify Tetherfi Multimedia Agent Client

Open a browser session to **http://<serverIP:1616/agent-desktop/login** and enter the appropriate credentials. The example below shows that **devconnect1**, which is associated with Agent ID 3411, will be logging into extension **3001**. Note this agent can log into any extension that is being monitored correctly by AES.

Agent Desktop

Not secure | 10.10.40.120:1616/agent-desktop/login

Welcome to Agent Desktop!

tetherfi

devconnect1

....

3001

☒ Login to PBX?

☐ Login to Webphone?

LOGIN

Copyright Tetherfi | UI: 5.2.7.3004 - Server: 5.1.11.3009 | TmacServer1

Once logged in, the agent can be made **Available**, as shown.

The screenshot displays the Avaya DevConnect application interface. At the top, the browser address bar shows "Not secure | 10.10.40.120:1616/agent-desktop/main/3411". The user profile "dev connect1 Default" is visible in the top right corner. A dropdown menu is open, showing the following options:

- Available (checked)
- 1 - Break
- 2 - Outbound
- 3 - Logout
- 4 - Meeting/Training

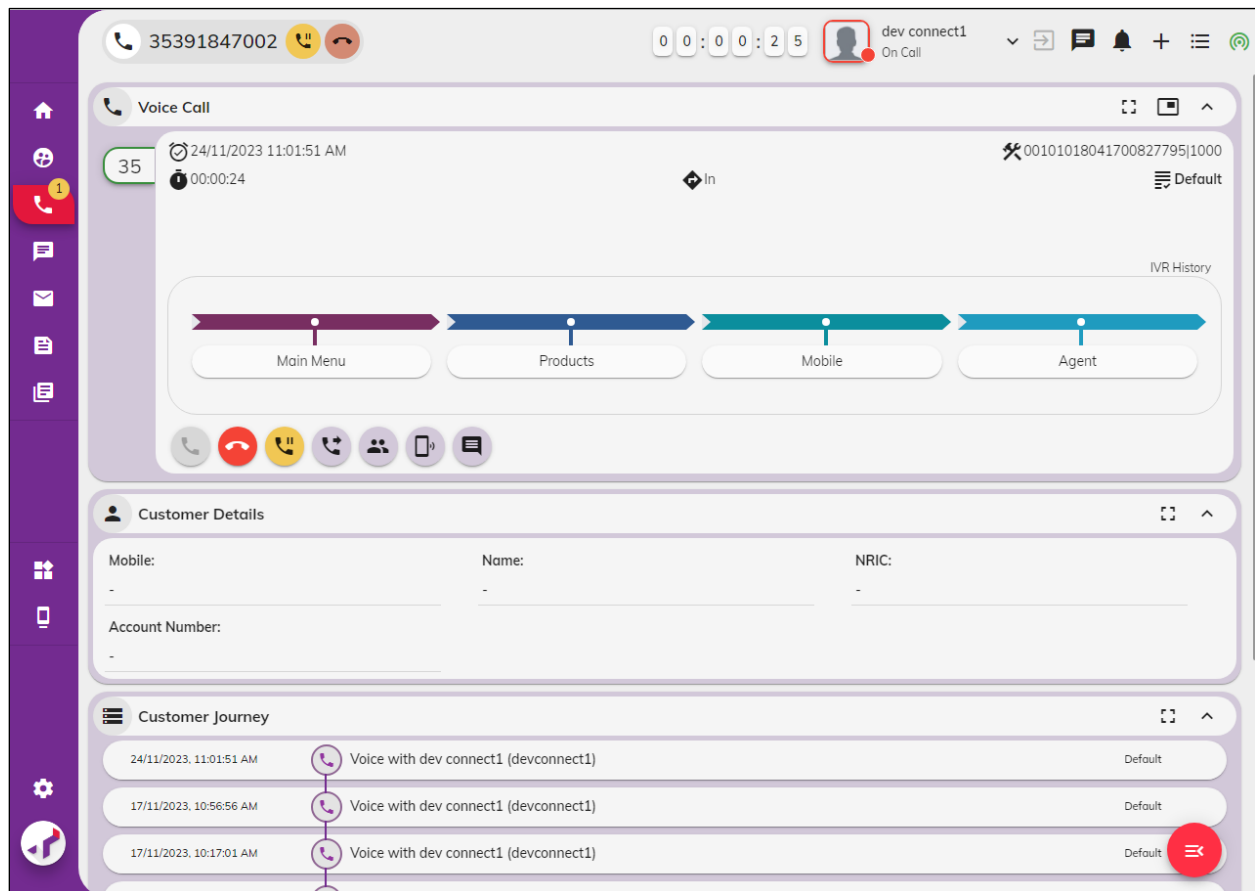
The main dashboard contains several widgets:

- Wallboard:** A table with the following data:

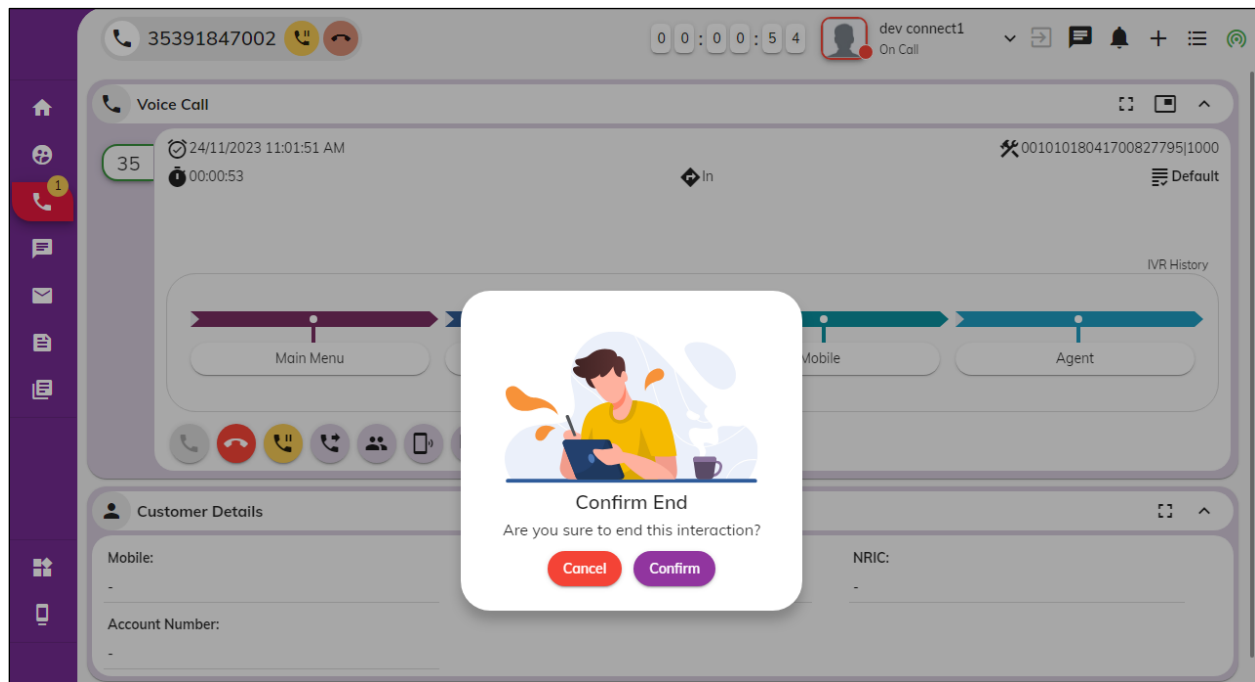
Skill Name	Stf	Avl	CIQ ↓	SL %
WorkSpaces	1	0	0	NA
Outbound	1	0	0	NA
MainOutbound	1	0	0	NA
Support	1	0	0	NA
- All Interactions:** Displays "No data available" with an illustration of two people working on a computer.
- Aux Status:** Displays "No data available" with the same illustration.
- Calendar:** Shows "November 2023" with a calendar icon.
- Interaction Details:** Displays "No data available".

The interface also features a vertical sidebar on the left with various icons and a red circular button with a white plus sign in the bottom right corner.

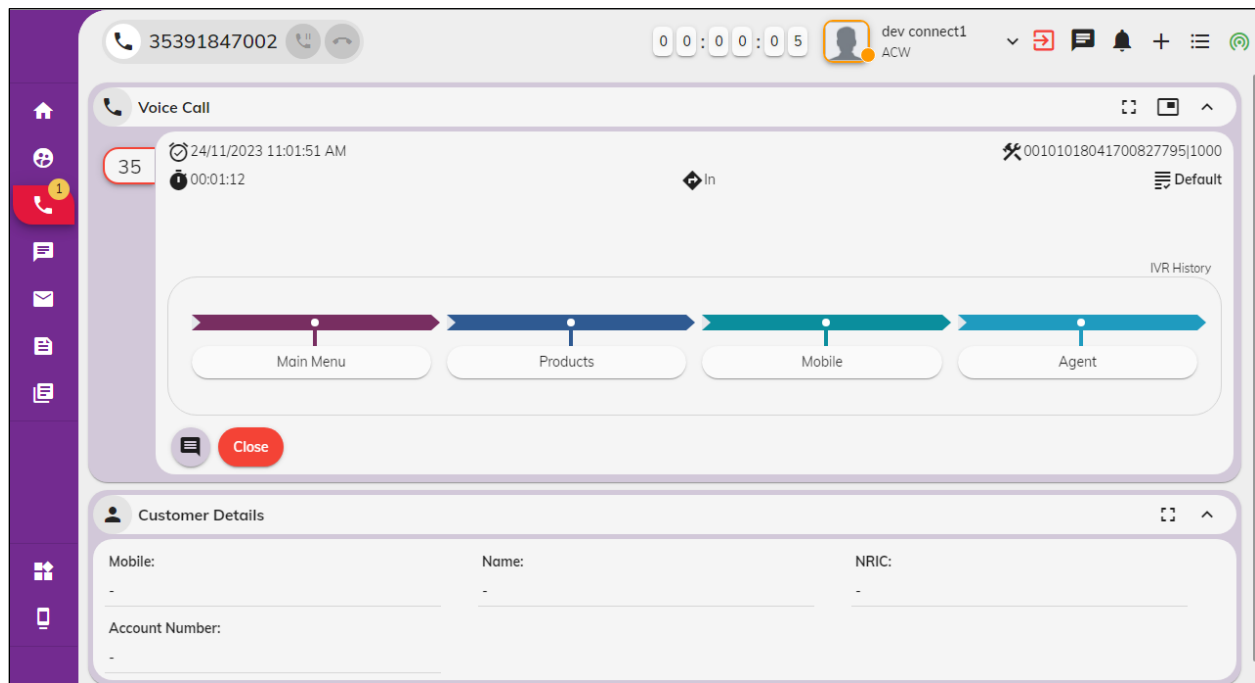
A call is then made from PSTN **35391847002** to the Support skillset 3901. The Voice widget is called upon and the telephony functions can be seen at the bottom of the main window. Functions such as hold, transfer, conference, and disconnect are shown.



Once the call has ended the session must also be closed. Pressing the disconnect or hang up button will result in the window below popping up to confirm the ending of the interaction. Click on **Confirm** to end the call completely.



Once the call is ended, click on **Close** to complete the session, and return the agent to **Available** again to get ready for the next call.



8.2. Verify connection from Avaya platform

There are a number of checks that can be performed to ensure that a connection is present from the Avaya products. These are some of the key checks that can be performed.

- Verify CTI Service State on Communication Manager
- Verify Telephony Service Application Programming Interface link and user on Application Enablement Services
- Verify System Management Service on Application Enablement Services

8.2.1. Verify Avaya Aura® Communication Manager CTI Service State

Check the connection between Communication Manager and AES. Check the AESVCS link status by using the command **status aescvs cti-link**. Verify the **Service State** of the CTI link is **established**.

status aescvs cti-link						
AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	12	no	aespril01x	established	865	865

8.2.2. Verify Telephony Service Application Programming Interface Link

On the AES Management Console, verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** to display the **TSAPI Link Details** screen. Verify the TSAPI link by checking that the **Status** is **Talking** and the **State** is **Online**.

Status | Status and Control | TSAPI Service Summary

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▶ Log Manager

▼ Status and Control

■ CVLAN Service Summary

■ DLG Services Summary

■ DMCC Service Summary

■ Switch Conn Summary

■ TSAPI Service Summary

TSAPI Link Details

☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	cm101x	1	Talking	Thu Nov 16 14:13:34 2023	Online	20	0	2883	2883	30

Online Offline

For service-wide information, choose one of the following:

TSAPI Service Status TLink Status User Status

Clicking on **User Status** from the screen on the previous page should display something similar to that shown below, where the **Multimedia Agent Client** user and corresponding **Tlink Name** are shown.

CTI User Status

☐

Enable page refresh every

60

seconds

CTI Users

All Users

Submit

Open Streams

3

Closed Streams

10

Open Streams

Name	Time Opened	Time Closed	Tlink Name
devconnect	Fri 17 Nov 2023 04:04:12 AM GMT		AVAYA#CM101X#CSTA#AESPRI101X
DMCCLCSUserDoNotModify	Thu 16 Nov 2023 01:15:02 PM GMT		AVAYA#CM101X#CSTA#AESPRI101X
DMCCLCSUserDoNotModify	Thu 16 Nov 2023 02:15:02 PM GMT		AVAYA#CM101X#CSTA#AESPRI101X

Show Closed Streams

Close All Opened Streams

Back

8.2.3. Verify System Management Service on Application Enablement Services

Open a web session to **https://AESIP/sms/sms_test.php** and enter the same credentials as **Section 7.2**. Enter some command such as ‘list agent’ as shown below, and it should return something like shown.

← → ↺ ⚠ Not secure | https://10.10.40.16/sms/sms_test.php

🔍 📄 ★ 🛑

AVAYA

String Based - Web Service Request Form

SMS Resources

Model Documentation
Model Doc (No-Frames)
SMS WSDL

Connection Information

CM Login IDlogin@<[IPv6]:port|hostname:port>
Password
SOAP Request Timeout (Seconds)

Request Parameters

Agent...
Operation
Objectname
Qualifier

Fields

*

Submit Request

Release

Session Recording

☐ Record SMS Request
☐ Record Result Data

Get Record

Clear Record

Last Request Response

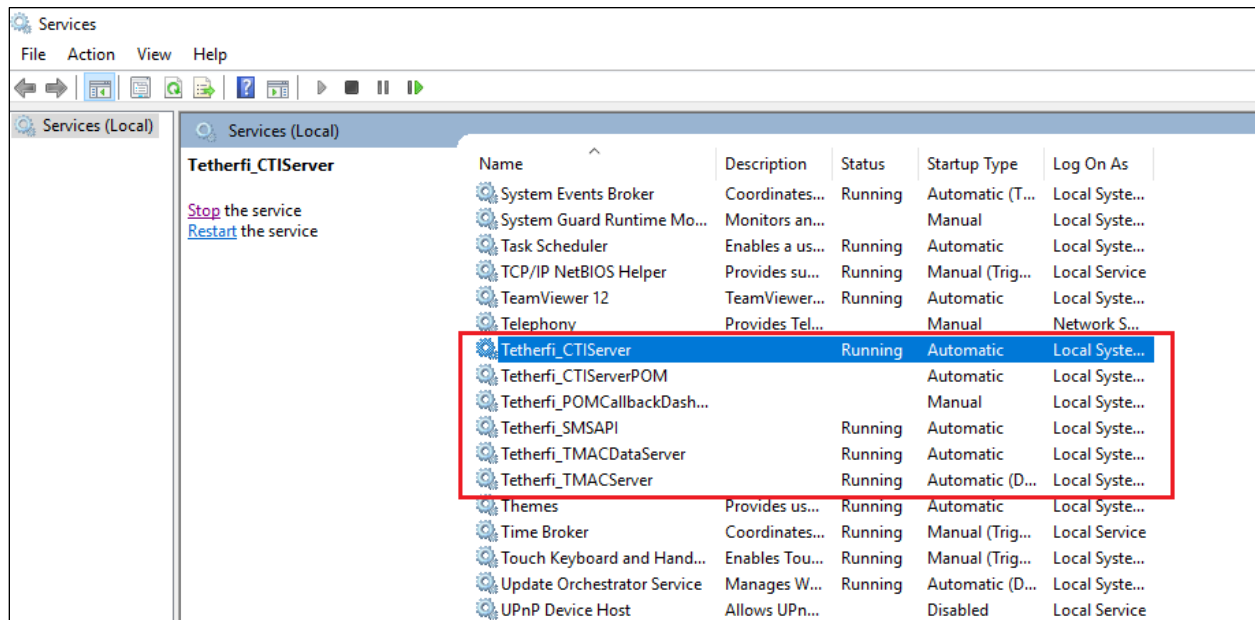
Session ID[Duplicate Session](#)

Response

```
Response {
  var $result_code = 0
  var $result_data =
'Login_ID[0]=3401|Login_ID[1]=3402|Login_ID[2]=3403|Login_ID[3]=3404|Login_ID[4]=3
411|Login_ID[5]=3412|Login_ID[6]=3413|Name[0]=Agent One|Name[1]=Agent
Two|Name[2]=Agent Three|Name[3]=Agent Four|Name[4]=Workspaces Agt
1|Name[5]=Workspaces Agt 2|Name[6]=Workspaces Agt
3|Extension[0]=unstaffed|Extension[1]=unstaffed|Extension[2]=unstaffed|Extension[3]
```

8.3. Verify Tetherfi services are running

From the TMAC server, check on the services that are running for Tetherfi_*. Note the following were running for compliance testing, for the connection to AES.



9. Conclusion

These Application Notes describe the compliance testing of Tetherfi Multimedia Agent Client 5.1 to interoperate with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Application Enablement Services R10.1 using the Telephony Service Application Programming Interface and the System Management Service. All test cases were executed successfully with any observations noted in **Section 2.2**.

10. Additional References

This section references the product documentations that are relevant to these Application Notes.

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

- [1] *Administering Avaya Aura® Communication Manager, Release 10.1.x, Issue 5, March 2023.*
- [2] *Administering Avaya Aura® Application Enablement Services, Release 10.1.x, Issue 6, Feb 2023.*
- [3] *Avaya Aura® Communication Manager Feature Description and Implementation, Release 10.1.x, Issue 8, March 2023.*
- [4] *Administering Avaya Aura® Session Manager, Release 10.1.x Issue 5, Feb 2023.*

Product documentation for Multimedia Agent Client can be found by contacting Tetherfi as per **Section 2.3**.

©2023 Avaya LLC. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. 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.