Avaya Solution & Interoperability Test Lab

Application Notes for Sytel Softdial Contact Center® (SCC) with Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Sytel Softdial Contact Center® (SCC) v11.1 with Avaya Aura® Application Enablement Services R10.1 and Avaya Aura® Communication Manager R10.1. Sytel SCC integrates with Avaya Aura® Application Enablement Services using the connection to Avaya Aura® Application Enablement Services Telephony Server Application Programming Interface (TSAPI) and the System Management Service (SMS) Web Service to initiate outbound calls and move skills to and from Call Center Elite agents.

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

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required to integrate Sytel Softdial Contact Center® (SCC) v11.1 with Avaya Aura® Application Enablement Services (AES) R10.1 and Avaya Aura® Communication Manager R10.1, using the connection to Avaya Aura® Application Enablement Services Telephony Server Application Programming Interface (TSAPI) and the System Management Service (SMS) Web Service to initiate outbound calls and move skills to and from Call Center Elite agents.

The System Management Service (SMS) Web Service is hosted on the Application Enablement Services server and exposes management features of Avaya Aura® Communication Manager to client SOAP applications. The web service enables client applications to display, list, add, change and remove specific managed objects on Communication Manager. This service provides programmatic access to a subset of the administration objects available via Communication Manager's System Access Terminal (SAT) screens.

When an agent logs in, SCC checks if this agent has the *outbound* skill. If it does, it removes all other skills and adds the agent to the outbound dialer pool of agents. Sytel SCC uses:

- TSAPI to request makePredictiveCall() and transfer the call to the selected agent
- SMS interface to manage skills for the selected agent

SCC monitors all VDNs associated with the predefined *outbound* skill (and inbound Hunt Group) and mirrors their states. The SCC dialer algorithm selects the best agent to take the outbound call. Once the outbound call is placed and offered to the VDN, the VDN performs an Adjunct Route step in the vector, and SCC returns the selected agent for the call. The VDN then routes the call to the selected agent.

If an inbound call is connected to a VDN, this call will be connected to the outbound agent following the VDN rules. The outbound agent does not receive outbound calls when connected to an inbound call. As soon as the inbound call disconnects, the outbound agent becomes eligible to receive outbound calls.

Both Avaya Agent for Desktop and a J189 phone were used for the solution to manage the voice extension. Sytel's Agent Desktop web application was used to:

- Pop up the customer data to the agent
- Provide an agent screen script to support the agent on the call
- Control login, logout, call disposition and agent breaks

All PBX functions will remain available in Avaya Agent for Desktop or J189.

2. General Test Approach and Test Results

The general test approach was to ensure the connection to Application Enablement Services was successful and to manually run through a number of scenarios to prove this to be the case. The connections to Application Enablement Services were tested by:

- Starting the Sytel SCC campaign
- Observing the outbound calls being made successfully
- Placing incoming calls to inbound VDN's
- Allowing the Sytel's Agent Desktop to answer and process the calls

Serviceability testing was carried out to observe the response of Sytel's Agent Desktop when various LAN failures were simulated.

For compliance testing, Avaya Agent for Desktop was set up to register its extension automatically, and both the J100 Series phone and Avaya Agent for Desktop were configured to answer the calls automatically (as required for this integration). The outbound agents logged in/ out using Sytel's Agent Desktop. Sytel synchronized the login with Avaya's AES using the TSAPI connection. Avaya agents logged into both Avaya Agent for Desktop, and the J189 SIP deskphone were used in an Avaya Call Center Elite environment. The Sytel's Agent Desktop utilized these agents and the Avaya Agent for Desktop when making outbound calls to a simulated PSTN.

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 that 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 Softdial Contact Center did not include the use of any specific encryption features as requested by Sytel.

2.1. Interoperability Compliance Testing

Interoperability compliance testing included feature and serviceability testing. The feature testing focused on the following functionality:

- Agents Login and Logout
- Agent states: Ready, Not Ready, and observing the skills associated
- Make Outbound Campaign calls (Predictive, Progressive, and Preview)
- Receive inbound skillset calls
- Hold/transfer/conference phone calls (using the Avaya endpoints only)
- Serviceability testing by simulating LAN failures

The serviceability testing focused on verifying the ability of the Softdial Contact Center solution to recover from adverse conditions, such as power failures and network disconnects.

2.2. Test Results

All test cases were executed and verified. All test cases passed successfully, with the following observations noted.

1. Application Enablement Services, Service Pack 2 (10.1.0.2), was applied to rectify an issue previously observed with the SMS connection.
2. Agents must login to outbound campaigns using Sytel's Agent Desktop, and the outbound campaign needs to be active. If agents are already logged in, and the outbound campaign is reset or restarted, the agents need to logout to prevent failing to be nailed up for the outbound campaign and blending operation.
3. All telephony functionality such as hold, retrieve, transfer, conference, and forward is done on the Avaya endpoint only and is not part of Sytel's Agent Desktop.
4. The information on the screen pop is not transferred when a "transfer" or "conference" is made to/with another agent. This is as per design.

2.3. Support

For technical support on the Softdial Contact Center, contact Sytel via phone, email, or the internet.

- Phone: +44 (0) 1296 381200
- Web: www.sytel.com
- Email: support@sytel.com

3. Reference Configuration

Figure 1 shows the network topology during compliance testing. The SCC Dialer server was placed on the Avaya Telephony LAN. SCC Outbound Dialer uses TSAPI to do a makePredictiveCall() followed by the SMS interface to manage agent skills and TSAPI to transfer the call to the actual agent. Once the outbound call is placed and offered to the VDN, the VDN does an Adjunct Route step in the vector, and the application (SCC) returns the selected agent for the call. The VDN then routes the call to the selected agent.

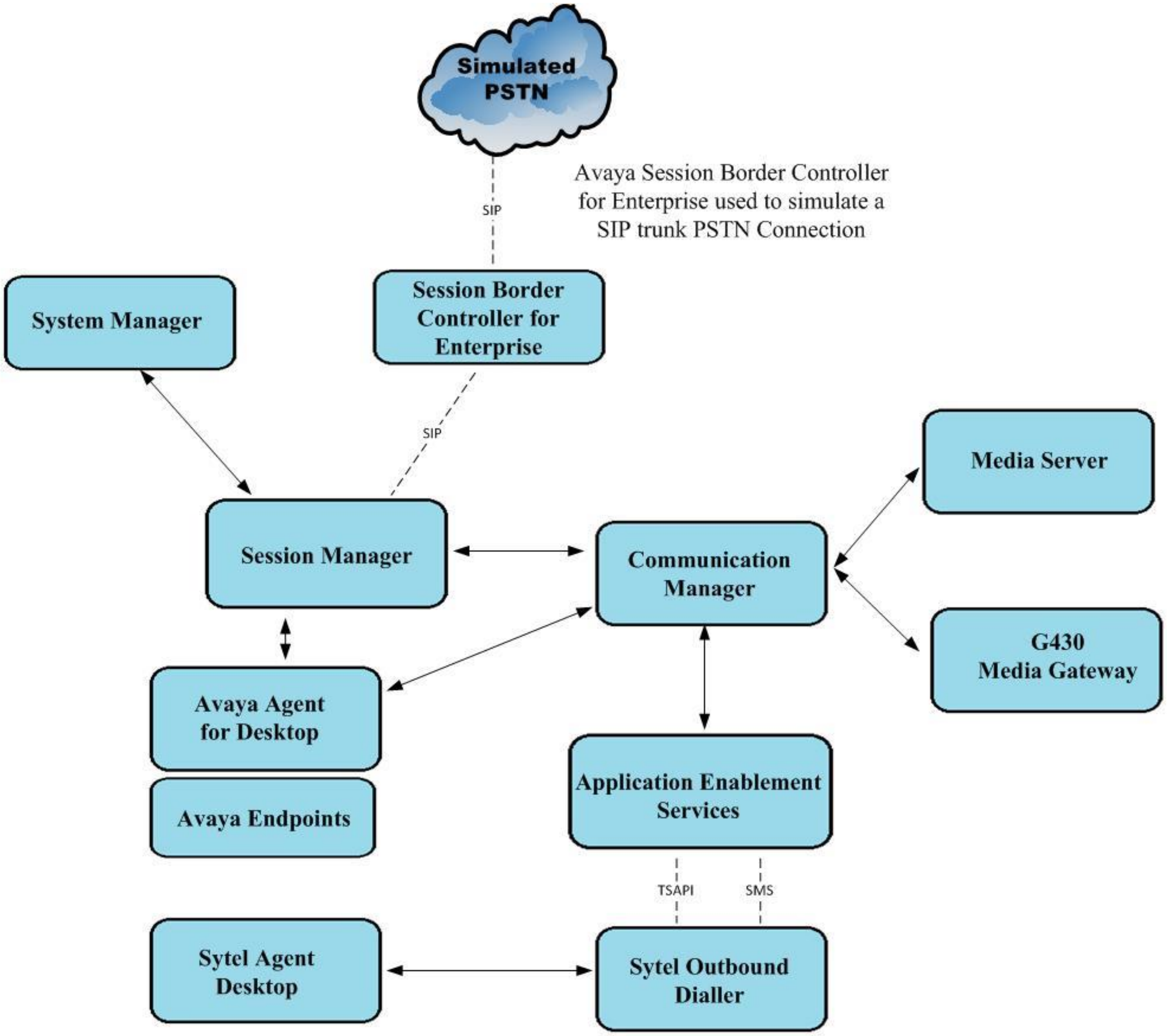


Figure 1: Network solution of Sytel Softdial Contact Center Dialer with Avaya Aura® Application Enablement Services R10.1

4. Equipment and Software Validated

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

Avaya Equipment	Software / Firmware Version
Avaya Aura® Application Enablement Services running on a virtual server	10.1.0.2.0.12-0
Avaya Aura® Communication Manager running on a virtual server	10.1 Update ID 01.0.974.0-27293
Avaya G430 Media Gateway	41.16.0/1
Avaya Aura® System Manager running on a virtual server	10.1.0.0 Build No. – 10.1.0.0.537353 SW Update Revision No: 10.1.0.0.0614254
Avaya Aura® Session Manager running on a virtual server	10.1 Build No. – 10.1.0.0.1010019
Avaya Session Border Controller for Enterprise running on a virtual server	8.1.3.0-31-21052
Avaya Agent for Desktop	2.0.6.23.3005
Avaya J100 Series SIP Deskphone	4.0.7.1.5
Sytel Equipment	**Software / Firmware Version**
Softdial Contact Center (SCC) – Main Platform Softdial Avaya Telephony Gateway (SATG) - The integration module	11.1.745 11.1.814.2

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. Some screens in this section have been abridged and highlighted for brevity and clarity in the presentation. The general installation of the servers and Avaya G430 Media Gateway is presumed to have been previously completed and is not discussed here. For all other provisioning information, such as initial installation and configuration, please refer to the product documentation in **Section 10**.

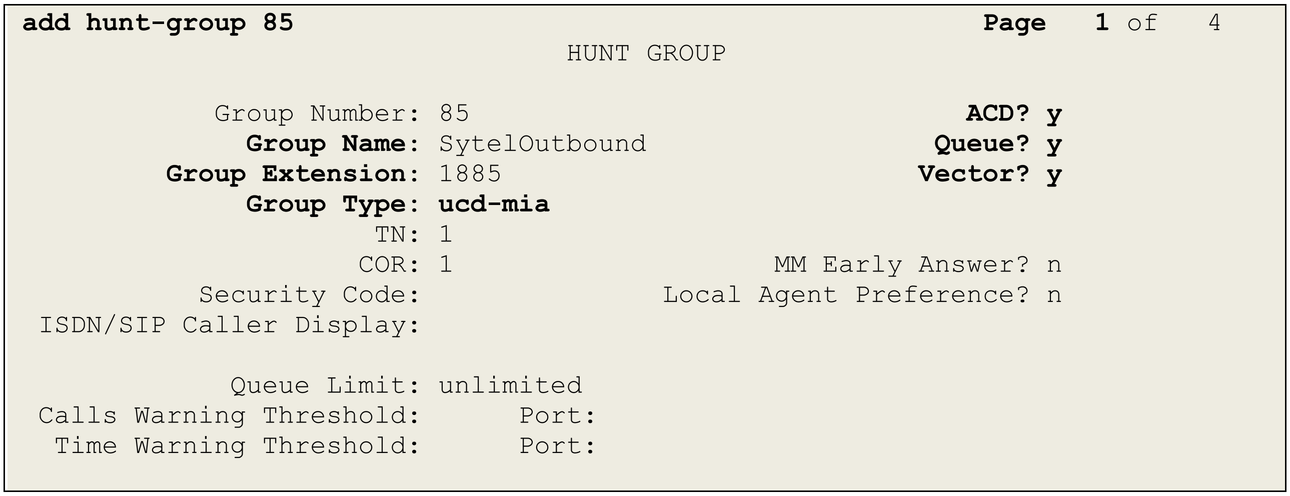
5.1. Configuration of the VDN, Vector, and Agent

A new VDN, Vector, and Hunt Group (skill) were created for Outbound calls that are made using the Sytel Outbound Dialer. The following sections show these configurations and the agent setup required for Outbound Dialer to operate successfully with the Avaya platform. For blended-type calls where there is a mixture of outbound calls and inbound calls to the Elite agent, other VDN's Vector and Hunt Groups must be in operation to facilitate inbound calls to skills associated with the same agent.

5.1.1. Hunt Group

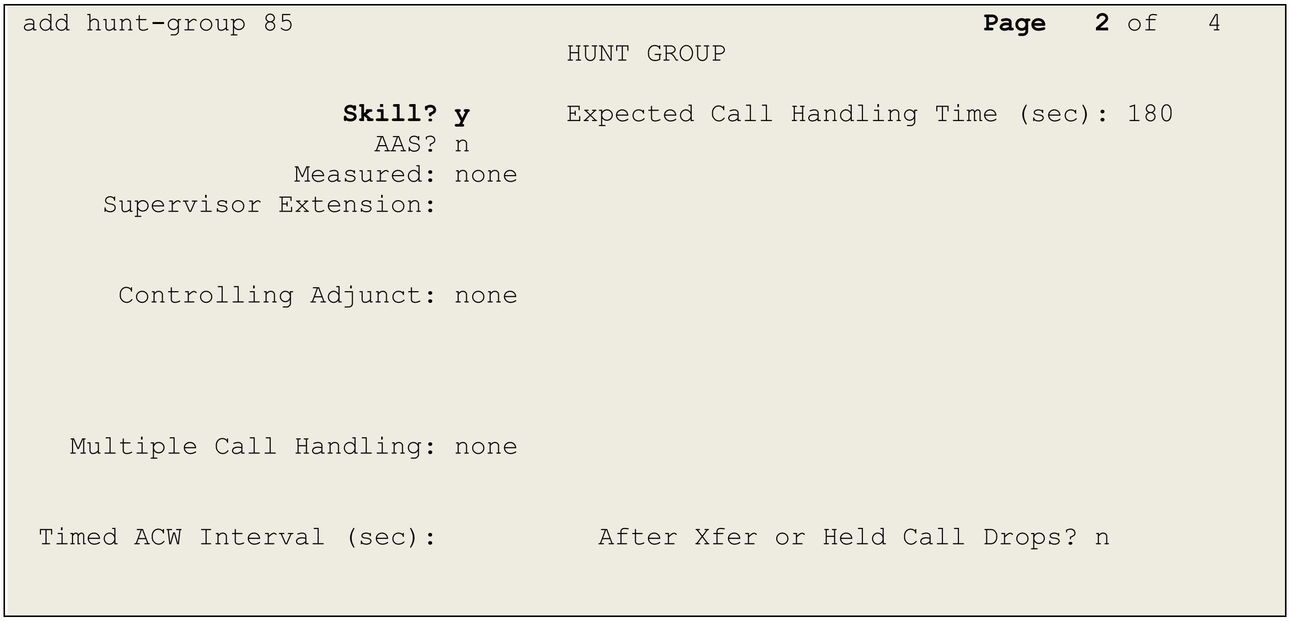
A hunt group is set up for outbound calls. Enter the **add hunt-group n** command where **n** in the example below is **85**. On **Page 1** of the **hunt-group** form, assign a **Group Name** and **Group Extension** valid under the provisioned dial plan. Set the following options to **y**, as shown below.

- **Group Type** to **ucd-mia**
- **ACD** to **y**
- **Queue** to **y**
- **Vector** to **y**



```
add hunt-group 85                                           Page   1 of   4
                                  HUNT GROUP

            Group Number: 85                               ACD? y
              Group Name: SytelOutbound                  Queue? y
         Group Extension: 1885                          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 the **Skill** field to **y**, as shown below.

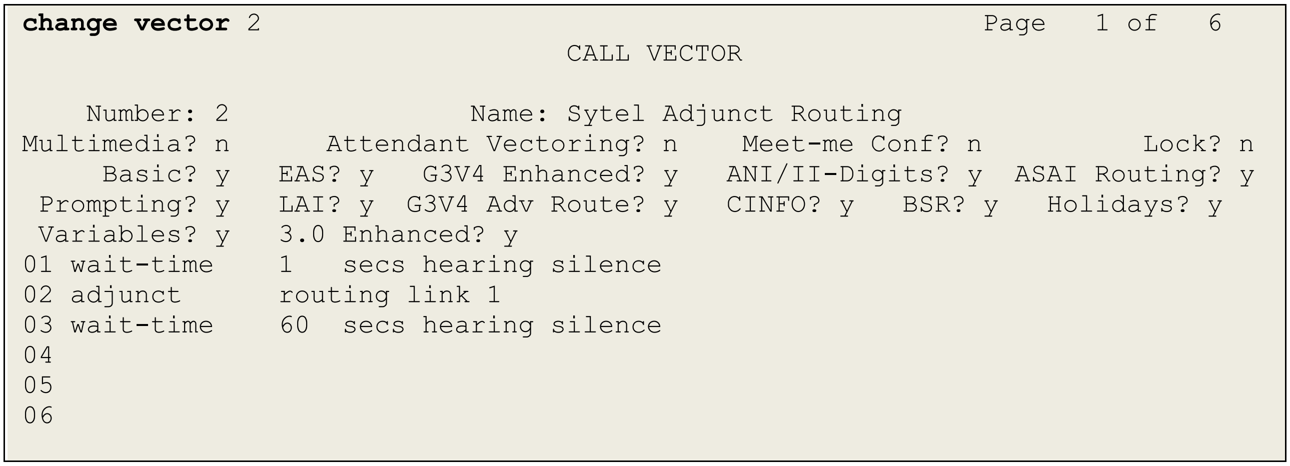


```
add hunt-group 85                                              Page   2 of   4
                                  HUNT GROUP

                    Skill? y      Expected Call Handling Time (sec): 180
                      AAS? n
                 Measured: none
     Supervisor Extension:


      Controlling Adjunct: none




   Multiple Call Handling: none


 Timed ACW Interval (sec):          After Xfer or Held Call Drops? n
```

Repeat the above steps to create hunt groups for other inbound services, should they be required. For compliance testing, two hunt groups, 81 and 82, were already in existence for inbound skills Sales and Support.

5.1.2. Vectors

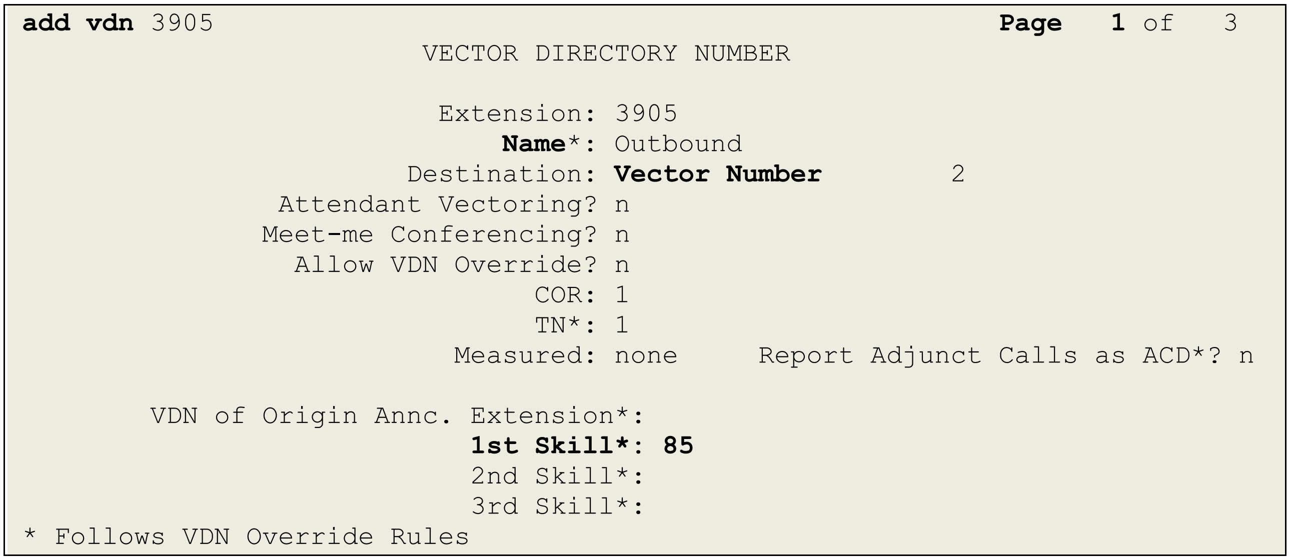
Enter the **change vector n** command, where **n** is the vector number. For this test, simple routing was used to get the call to the agent. The call is sent to the adjunct routing link, so Sytel SCC handles the call.



```
change vector 2                                                Page   1 of   6
                                  CALL VECTOR

    Number: 2               Name: Sytel Adjunct 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    1   secs hearing silence
02 adjunct      routing link 1
03 wait-time    60  secs hearing silence
04
05
06
```

5.1.3. Vector Directory Numbers (VDN)

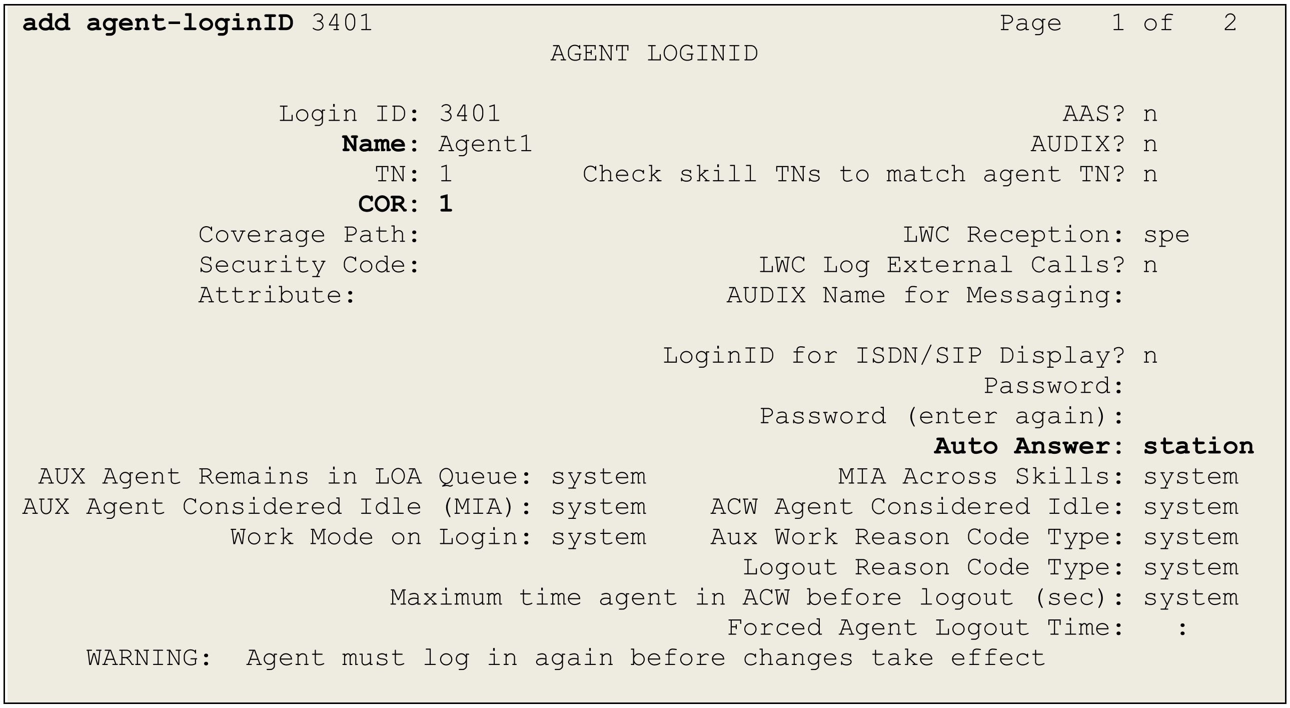
Enter the **add vdn n** command, where **n** is an available extension number. On **Page 1**, assign a **Name** for the VDN and set the **Vector Number** to that created in **Section 5.1.2**. The **1st Skill** should be set to that hunt group configured in **Section 5.1.1**.



```
add vdn 3905                                                 Page   1 of   3
                         VECTOR DIRECTORY NUMBER

                          Extension: 3905
                              Name*: Outbound
                        Destination: Vector Number        2
                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*: 85
                            2nd Skill*:
                            3rd Skill*:
* Follows VDN Override Rules
```

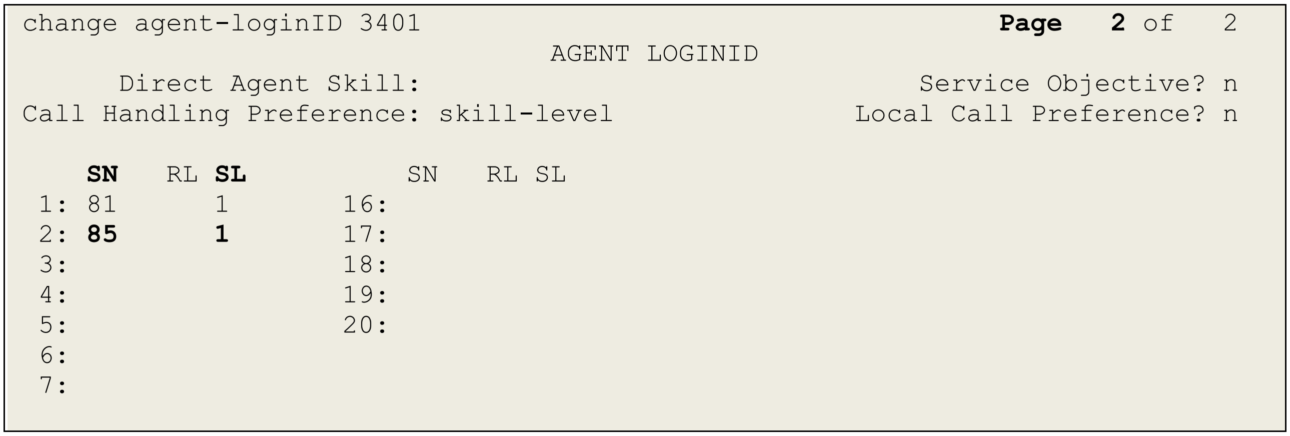
5.1.4. Administer Agent Logins

Enter the **add agent-loginID n** command, where **n** is an available extension number. Enter a descriptive name for the agent in the **Name** field. The **Auto Answer** field is set to **station**. Configure a password as required.



```
add agent-loginID 3401                                       Page   1 of   2
                                 AGENT LOGINID

                Login ID: 3401                                   AAS? n
                    Name: Agent1                               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:
                                              Password (enter again):
                                                         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**, assign the skills to the agent by entering the relevant hunt group numbers created in **Section 5.1.1** for **SN** and entering a skill level of **1** for **SL**. In this case, an agent able to handle both inbound and outbound calls is created.



```
change agent-loginID 3401                                       Page   2 of   2
                                 AGENT LOGINID
      Direct Agent Skill:                                Service Objective? n
Call Handling Preference: skill-level                Local Call Preference? n

    SN   RL SL          SN   RL SL
 1: 81      1       16:
 2: 85      1       17:
 3:                 18:
 4:                 19:
 5:                 20:
 6:
 7:
```

Repeat this task accordingly for any additional inbound agents required.

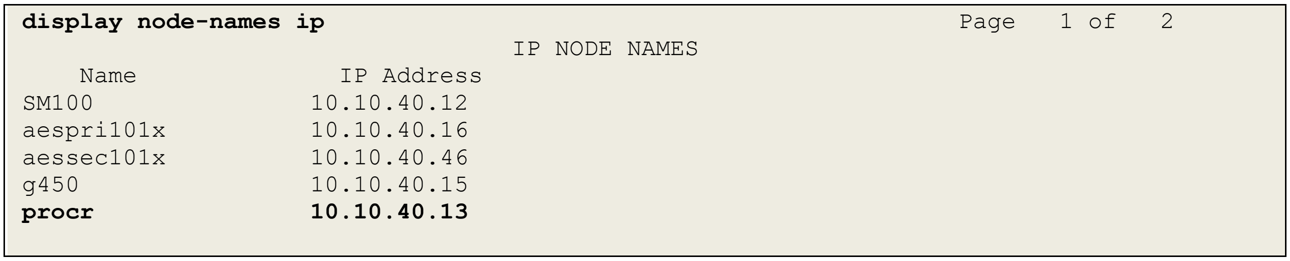
5.2. Configuration of the connection to the Avaya Aura® Application Enablement Services

The configuration operations described in this section can be summarized as follows:

- Note procr IP Address
- Configure Transport Link
- Configure CTI Link for TSAPI Service

5.2.1. Note procr IP Address for Avaya Aura® Application Enablement Services Connectivity

Display the procr IP address by using the command **display node-names ip** and noting the IP address for the **procr** and Application Enablement Services.



```
display node-names ip                                            Page   1 of   2
                              IP NODE NAMES
    Name              IP Address
SM100               10.10.40.12
aespri101x          10.10.40.16
aessec101x          10.10.40.46
g450                10.10.40.15
procr               10.10.40.13
```

5.2.2. Configure Transport Link for Avaya Aura® Application Enablement Services Connectivity

To administer the transport link to Application Enablement Services, use the **change ip-services** command. On **Page 1**, add an entry with the following values:

- **Service Type:** should be set to **AESVCS**
- **Enabled:** set to **y**
- **Local Node:** set to the node name assigned for the **procr** in **Section 5.2.1**
- **Local Port:** Retain the default value of **8765**

```
change ip-services                                                Page   1 of   3

                                   IP SERVICES
 Service      Enabled     Local        Local       Remote      Remote
  Type                    Node         Port        Node        Port
AESVCS         y          procr        8765
```

Go to **Page 4** of the **ip-services** form and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case **aespri101x**
- **Password:** Enter a password to be administered on the AES server
- **Enabled:** Set to **y**

Note: The password entered for **Password** field must match the password on the AES server in **Section 6.2**. The **AE Services Server** should match the administered name for the AES server; this is created as part of the AES installation and can be obtained from the AES server by typing **uname –n** at the Linux command prompt.

```
change ip-services                                                Page   4 of   4
                            AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:        aespri101x         ********          y          in use
      2:        aessec101x         ********          y          in use
      3:
```

5.2.3. Configure CTI Link for TSAPI Service

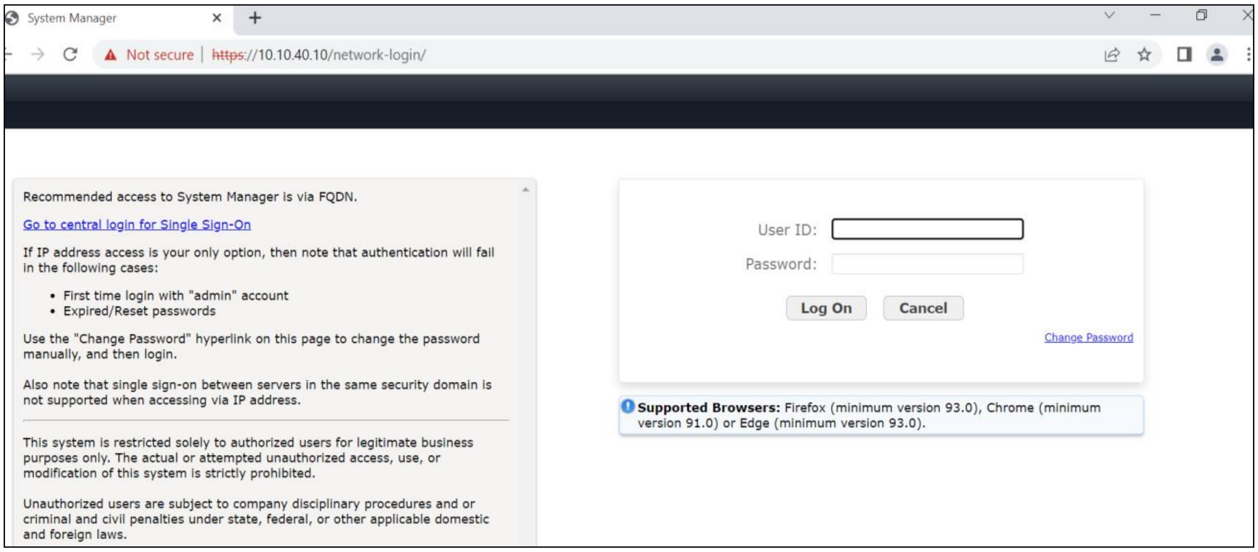
Add a CTI link using the **add cti-link n** command. Enter an available extension number in the **Extension** field. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field.

```
add cti-link 1                                                   Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 3990
     Type: ADJ-IP
                                                                          COR: 1
     Name: aespri101x
```

5.3. Configure SIP Agent Stations

Each Avaya SIP endpoint will need to have Auto Answer configured correctly. 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 to a SIP extension and assumes that the SIP extension has been programmed correctly and is fully functioning.



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.

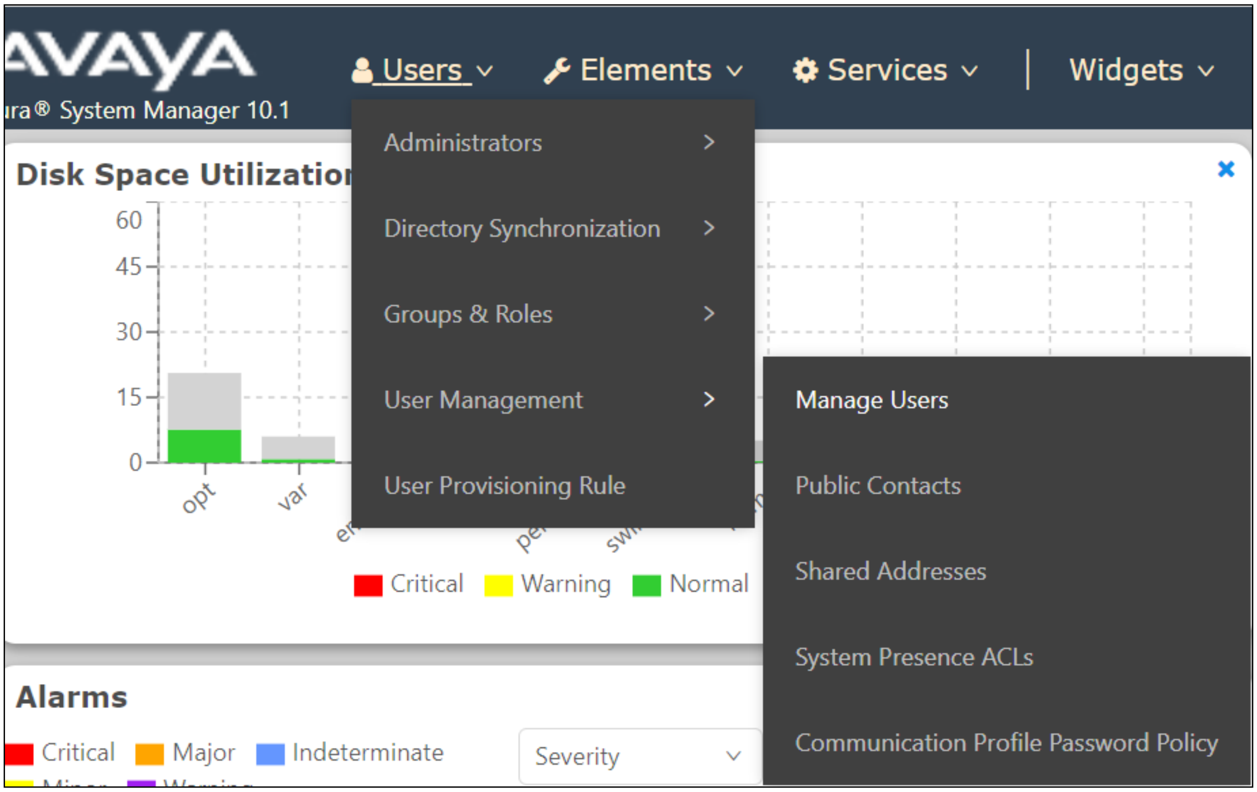
Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

User ID:

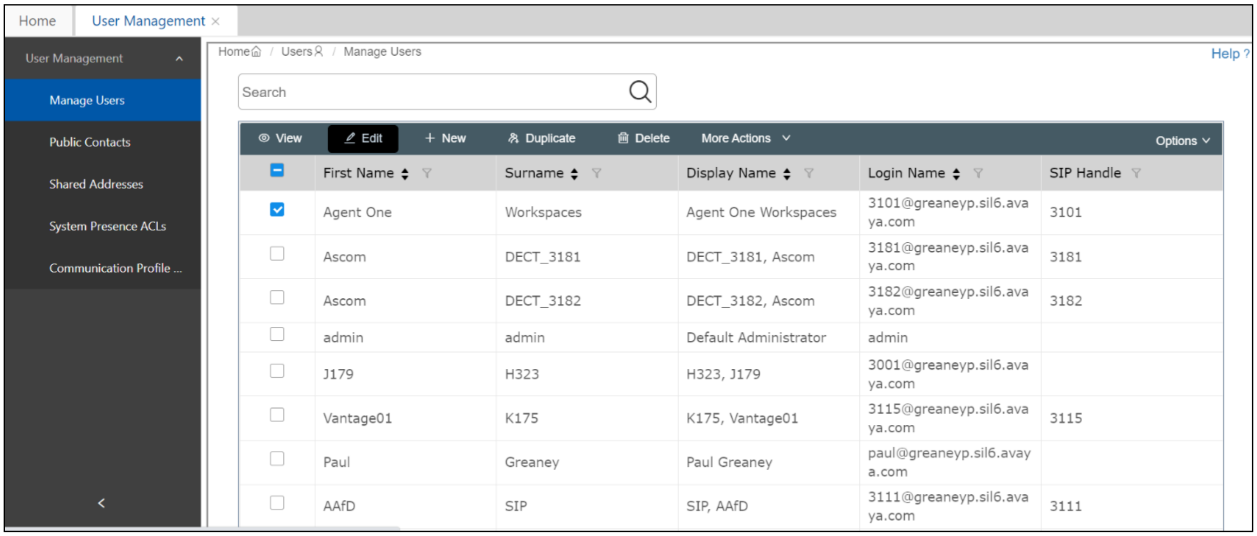
Password:

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.

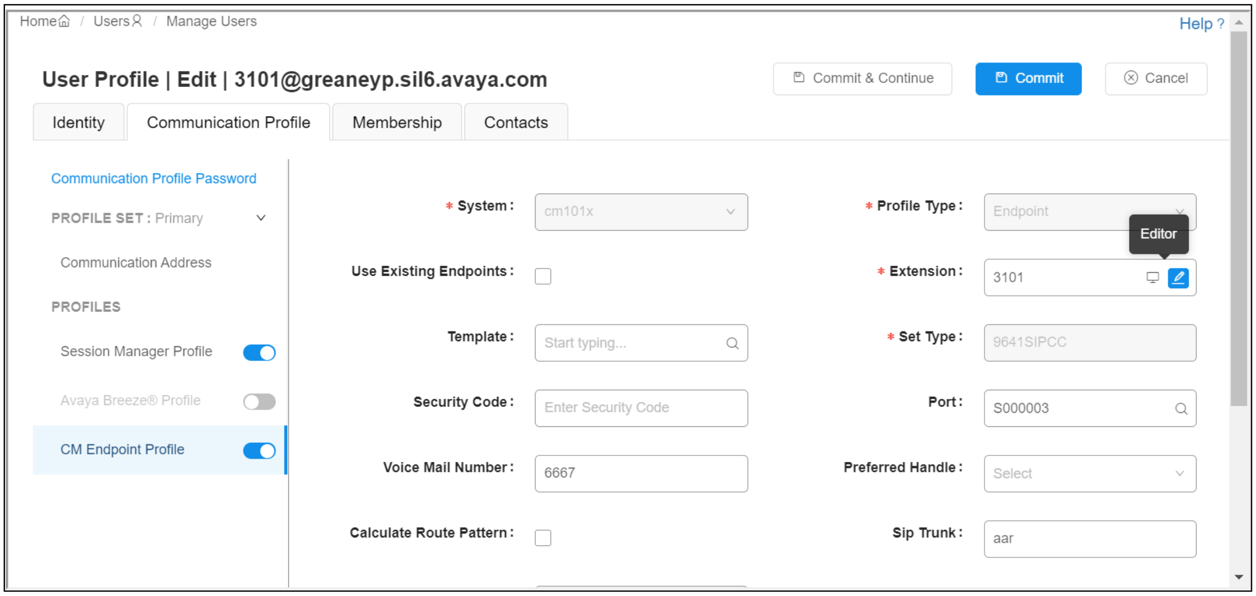


Click on **Manager Users** in the left window. Select the station to be edited and click on **Edit**.



	First Name	Surname	Display Name	Login Name	SIP Handle
☑	Agent One	Workspaces	Agent One Workspaces	3101@greaneyp.sil6.avaya.com	3101
□	Ascom	DECT_3181	DECT_3181, Ascom	3181@greaneyp.sil6.avaya.com	3181
□	Ascom	DECT_3182	DECT_3182, Ascom	3182@greaneyp.sil6.avaya.com	3182
□	admin	admin	Default Administrator	admin	
□	J179	H323	H323, J179	3001@greaneyp.sil6.avaya.com	
□	Vantage01	K175	K175, Vantage01	3115@greaneyp.sil6.avaya.com	3115
□	Paul	Greaney	Paul Greaney	paul@greaneyp.sil6.avaya.com	
□	AAfD	SIP	SIP, AAfD	3111@greaneyp.sil6.avaya.com	3111

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



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

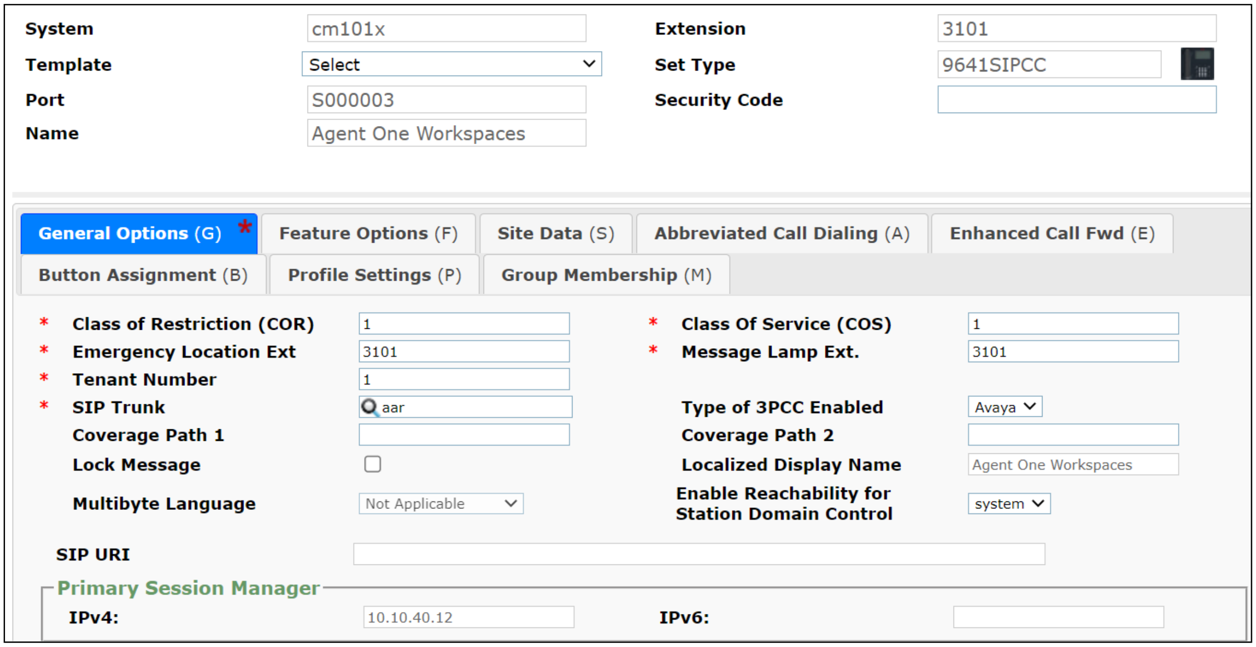
PROFILE SET : Primary

Session Manager 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**.



System	cm101x	Extension	3101
Template	Select	Set Type	9641SIPCC
Port	S000003	Security Code	
Name	Agent One Workspaces		

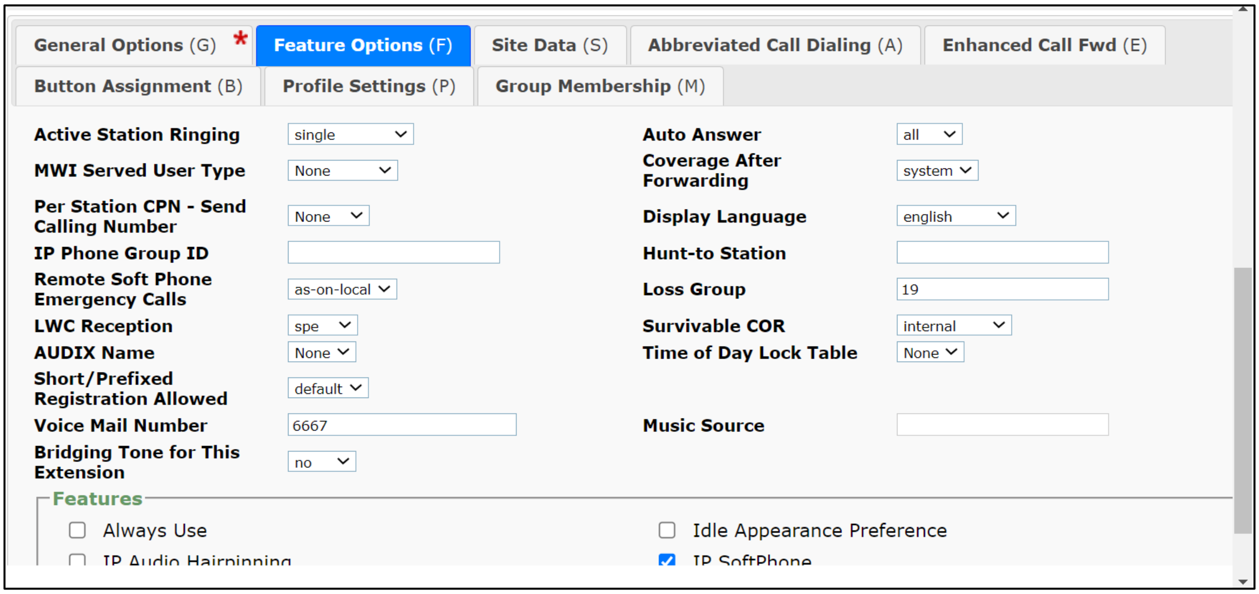
* Class of Restriction (COR)	1	* Class Of Service (COS)	1
* Emergency Location Ext	3101	* Message Lamp Ext.	3101
* Tenant Number	1		
* SIP Trunk	aar	Type of 3PCC Enabled	Avaya
Coverage Path 1		Coverage Path 2	
Lock Message	□	Localized Display Name	Agent One Workspaces
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system

SIP URI

Primary Session Manager

IPv4: 10.10.40.12 IPv6:

On the **Feature Options** tab, **Auto Answer** was set to **all**, this setting is required to allow the correct operation with SCC Dialer.



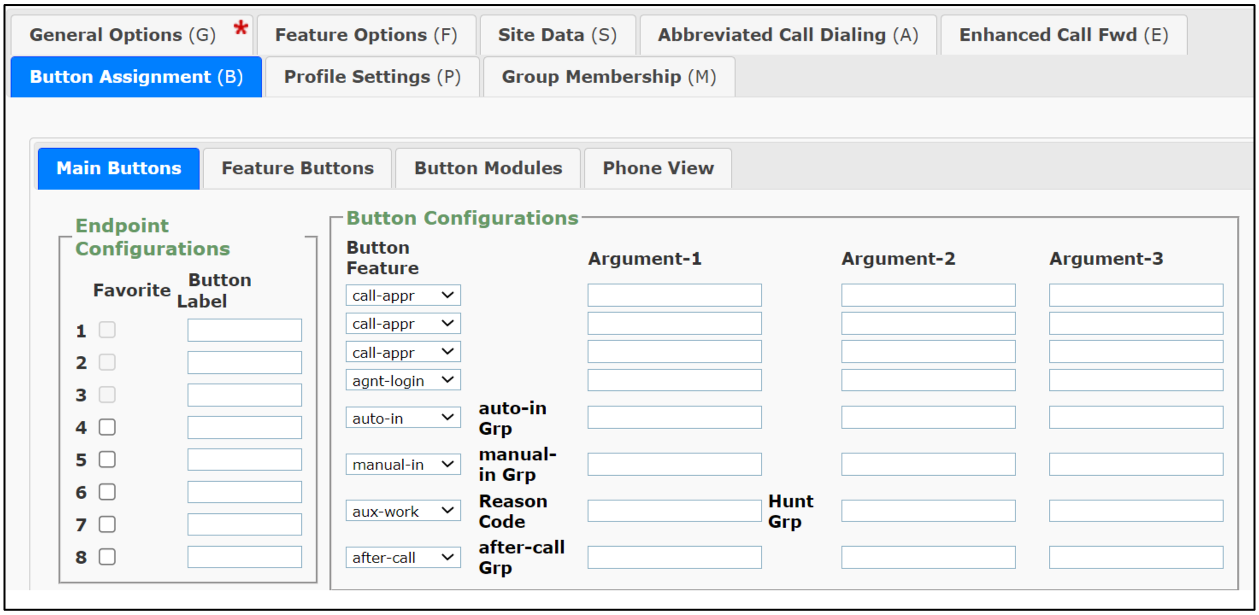
Active Station Ringing	single	Auto Answer	all
MWI Served User Type	None	Coverage After Forwarding	system
Per Station CPN - Send Calling Number	None	Display Language	english
IP Phone Group ID		Hunt-to Station	
Remote Soft Phone Emergency Calls	as-on-local	Loss Group	19
LWC Reception	spe	Survivable COR	internal
AUDIX Name	None	Time of Day Lock Table	None
Short/Prefixed Registration Allowed	default		
Voice Mail Number	6667	Music Source	
Bridging Tone for This Extension	no		

Features

☐ Always Use ☐ Idle Appearance Preference

☐ IP Audio Hairpinning ☑ IP SoftPhone

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



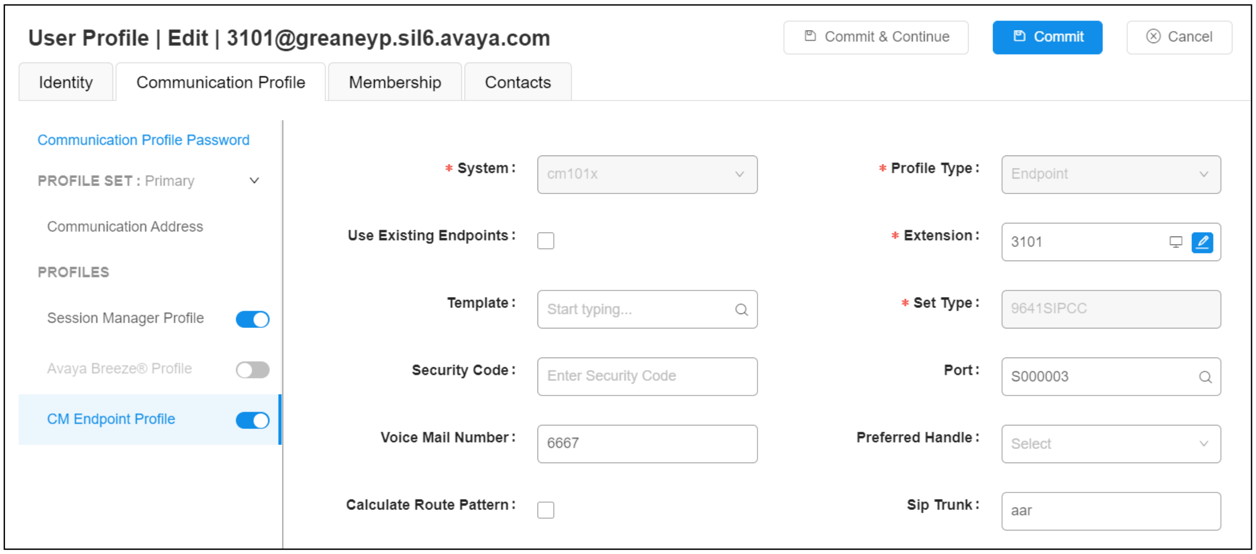
Endpoint Configurations

	Favorite	Button Label
1	☐	
2	☐	
3	☐	
4	☐	
5	☐	
6	☐	
7	☐	
8	☐	

Button Configurations

Button Feature		Argument-1		Argument-2	Argument-3
call-appr					
call-appr					
call-appr					
agnt-login					
auto-in	auto-in Grp				
manual-in	manual-in Grp				
aux-work	Reason Code		Hunt Grp		
after-call	after-call Grp				

Click on **Commit** to save the changes.



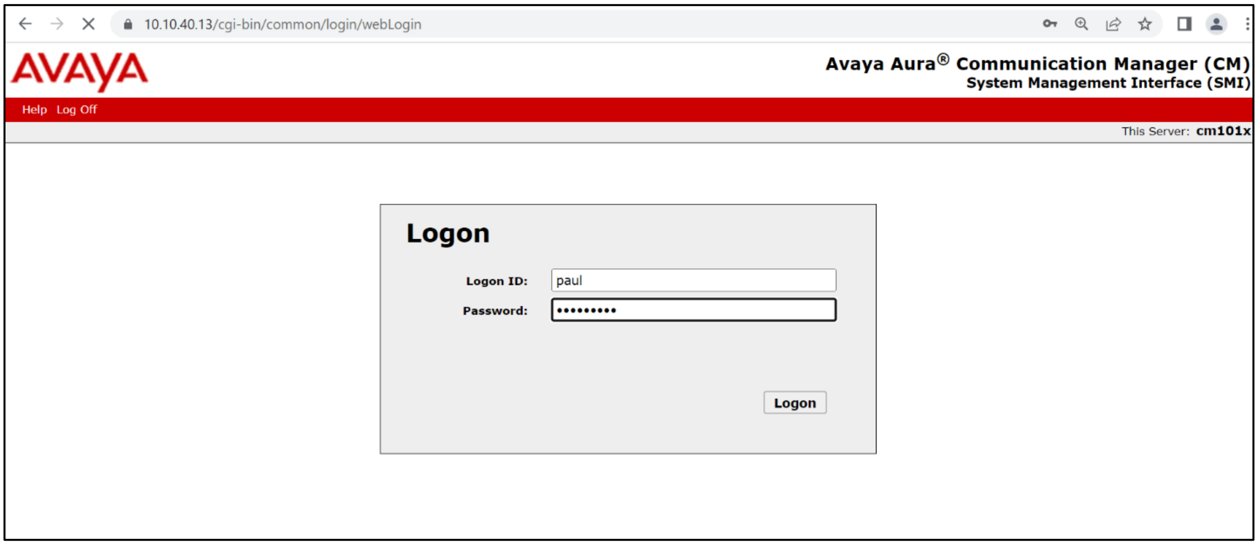
User Profile | Edit | 3101@greaneyp.sil6.avaya.com

* 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

5.4. Adding a user on Avaya Aura® Communication Manager for Sytel

A user on Communication Manager must be added to allow the SCC Dialer to make changes to the agents on Communication Manager. These changes are facilitated using a connection to the SMS on AES. This connection then uses this user that will be created to carry out the necessary changes on Communication Manager.

Open the web browser to Communication Manager and log in using the appropriate credentials.



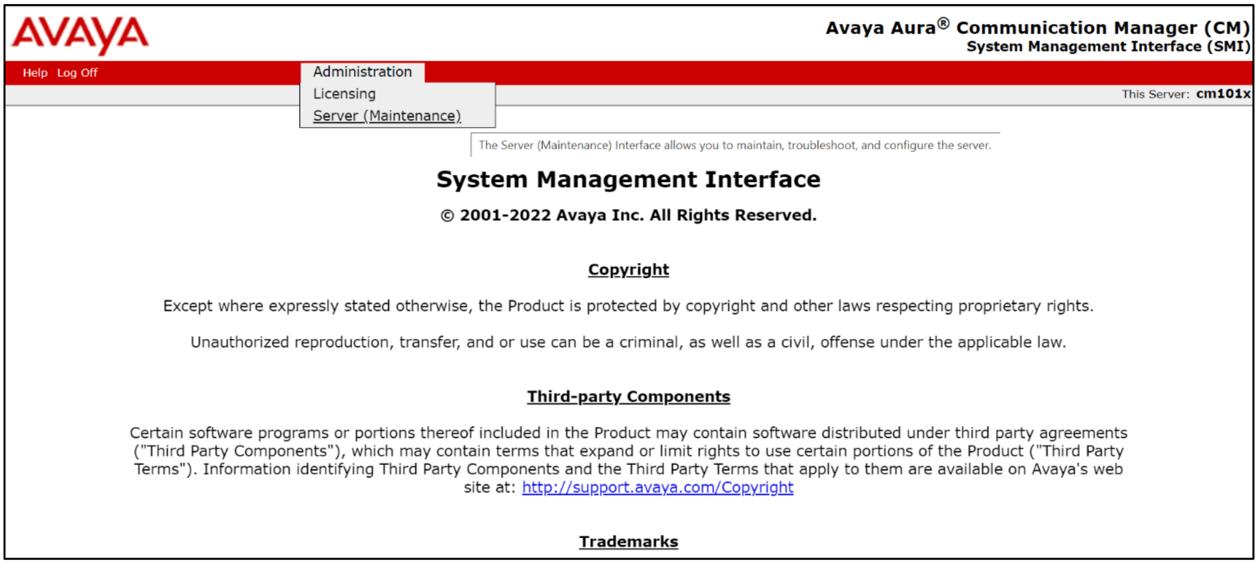
10.10.40.13/cgi-bin/common/login/webLogin

AVAYA
Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)
Help Log Off
This Server: cm101x

Logon

Logon ID:	paul
Password:	•••••••••

Once logged in, navigate to **Server (Maintenance)** as shown below.



The Server (Maintenance) Interface allows you to maintain, troubleshoot, and configure the server.

System Management Interface

© 2001-2022 Avaya Inc. All Rights Reserved.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

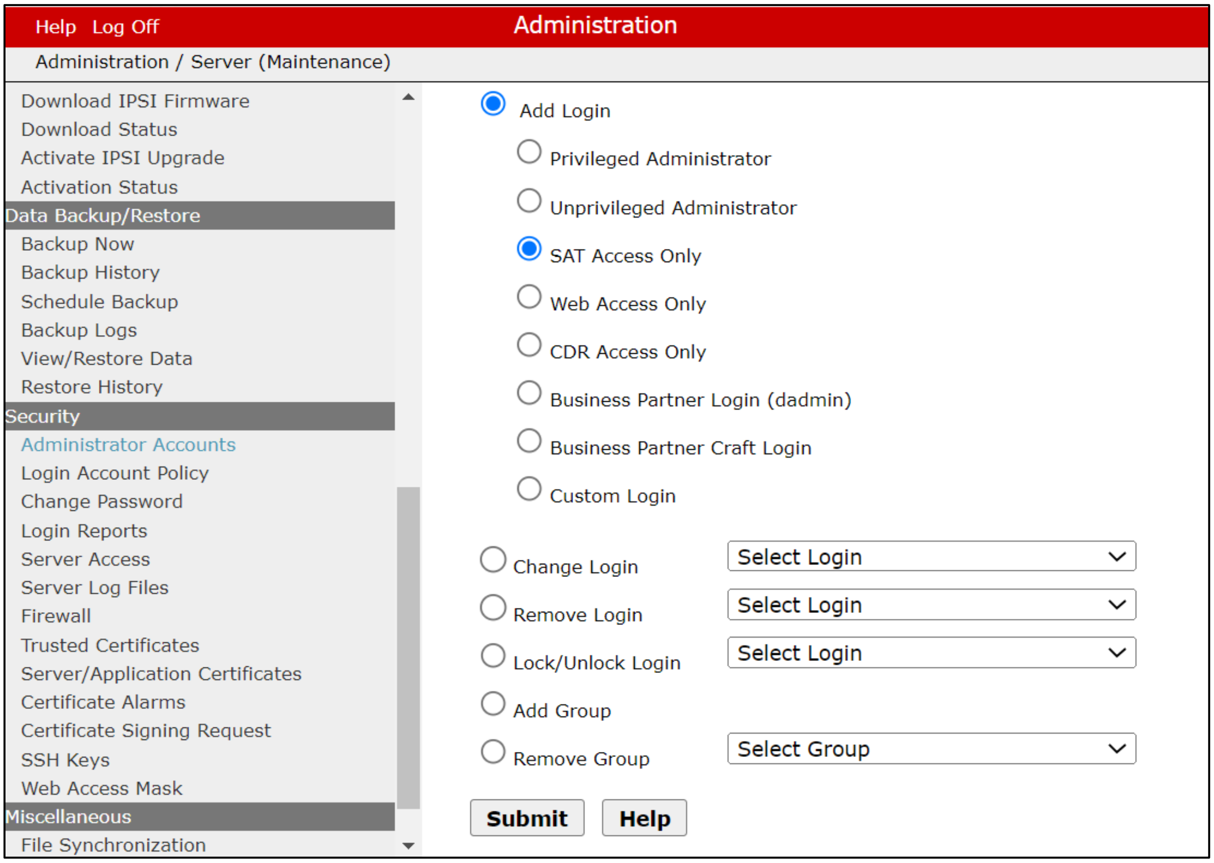
Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at: http://support.avaya.com/Copyright

Trademarks

Navigate to **Security → Administrator Accounts** in the left window, select **Add Login**, and choose the **SAT Access Only**, as this is all that is required to allow the Sytel user to make the necessary changes to the agents using the SMS connection. Click on **Submit**.



● Add Login

○ Privileged Administrator

○ Unprivileged Administrator

● SAT Access Only

○ Web Access Only

○ CDR Access Only

○ Business Partner Login (dadmin)

○ Business Partner Craft Login

○ Custom Login

○ Change Login — Select Login

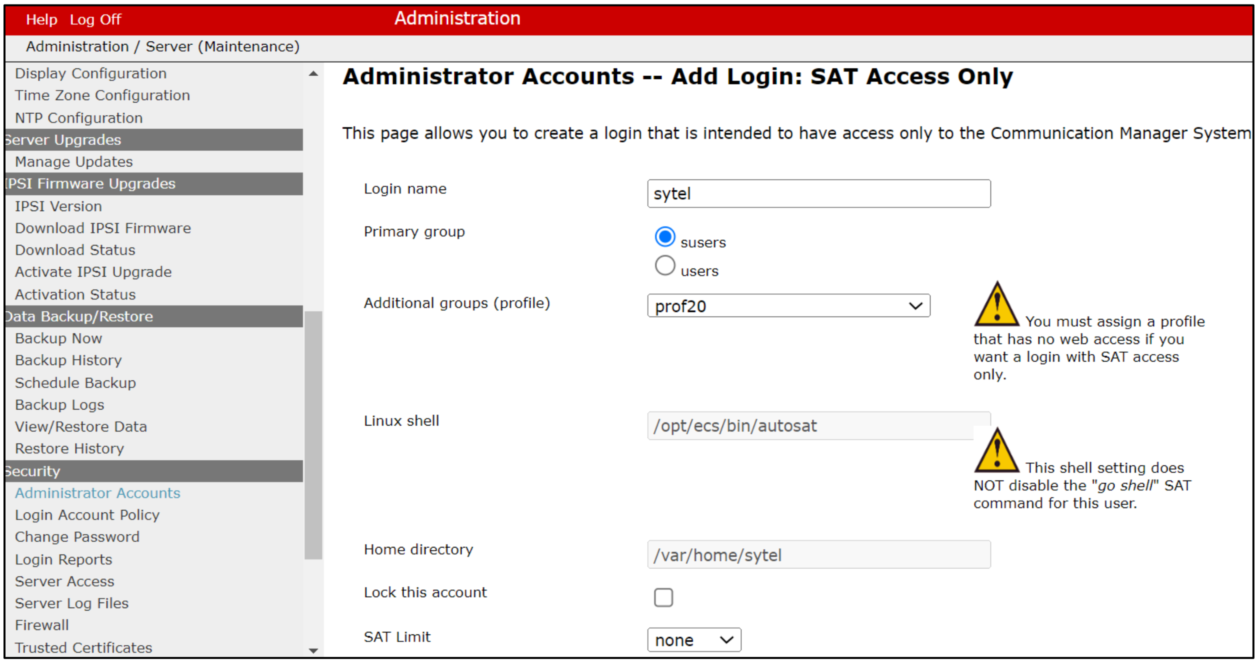
○ Remove Login — Select Login

○ Lock/Unlock Login — Select Login

○ Add Group

○ Remove Group — Select Group

Enter a suitable **Login name** and the rest can be left as default.



Administrator Accounts -- Add Login: SAT Access Only

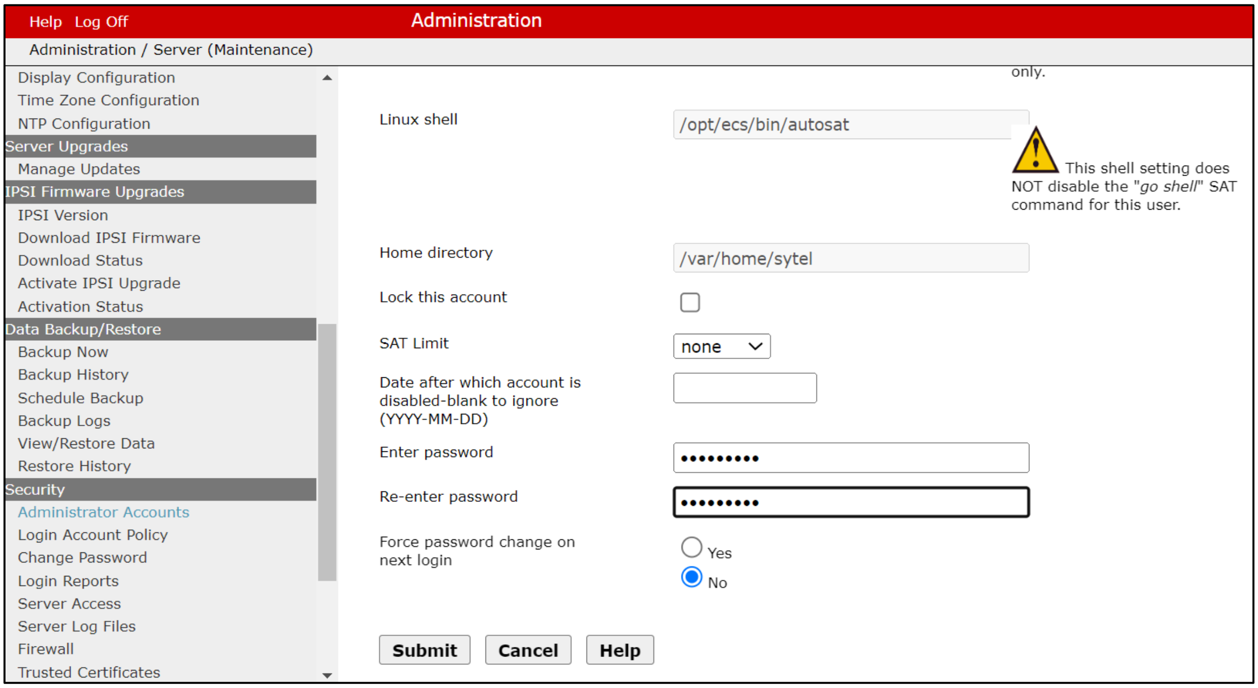
This page allows you to create a login that is intended to have access only to the Communication Manager System

Login name	sytel
Primary group	● susers ○ users
Additional groups (profile)	prof20
Linux shell	/opt/ecs/bin/autosat
Home directory	/var/home/sytel
Lock this account	□
SAT Limit	none

You must assign a profile that has no web access if you want a login with SAT access only.

This shell setting does NOT disable the "*go shell*" SAT command for this user.

Enter a new **password**, and again the rest can be left as default. Click on **Submit** to finish.



only.

Linux shell	/opt/ecs/bin/autosat
Home directory	/var/home/sytel
Lock this account	□
SAT Limit	none
Date after which account is disabled-blank to ignore (YYYY-MM-DD)	
Enter password	•••••••••
Re-enter password	•••••••••
Force password change on next login	○ Yes ● No

This shell setting does NOT disable the "*go shell*" SAT command for this user.

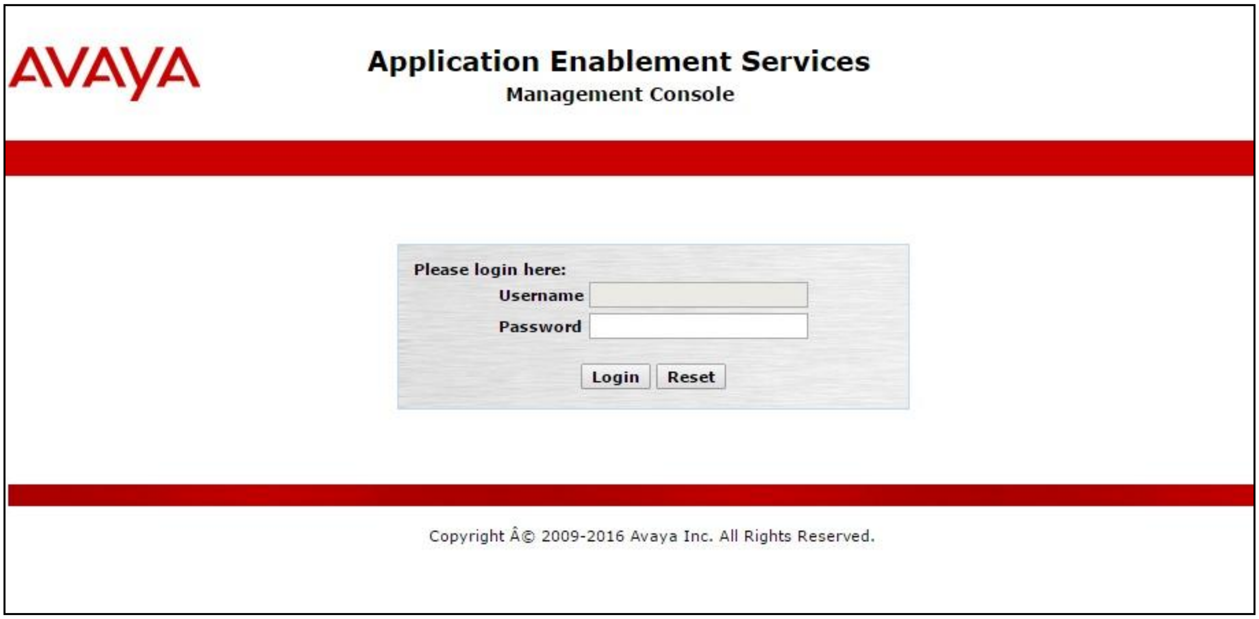
6. Configure Avaya Aura® Application Enablement Services

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

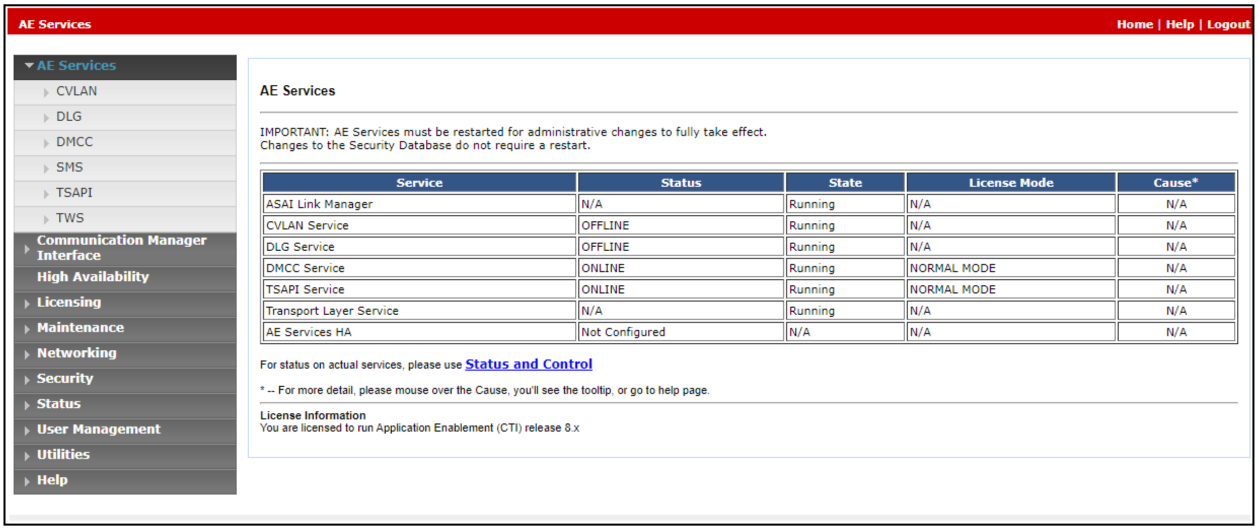
- Verify Licensing
- Switch Connection
- Administer TSAPI Link
- Identify Tlinks
- Enable TSAPI Ports
- Create CTI User
- Configure Security
- Configure System Management Service (SMS)
- Restart AE Server

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 AES. Log in with the appropriate credentials at the login screen and then select the **Login** button.


AVAYA
Application Enablement Services
Management Console
Please login here:
Username
Password
Login
Reset
Copyright Â© 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.



AE Services

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect.
Changes to the Security Database do not require a restart.

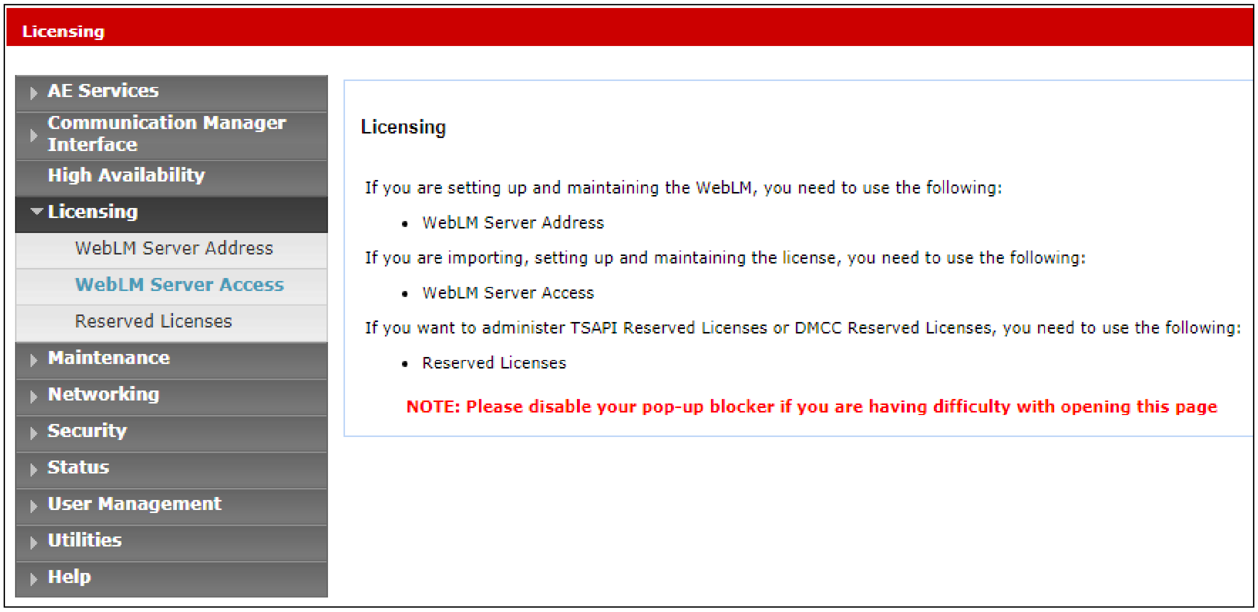
Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A
AE Services HA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

For status on actual services, please use Status and Control

* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

License Information
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.



Licensing

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:

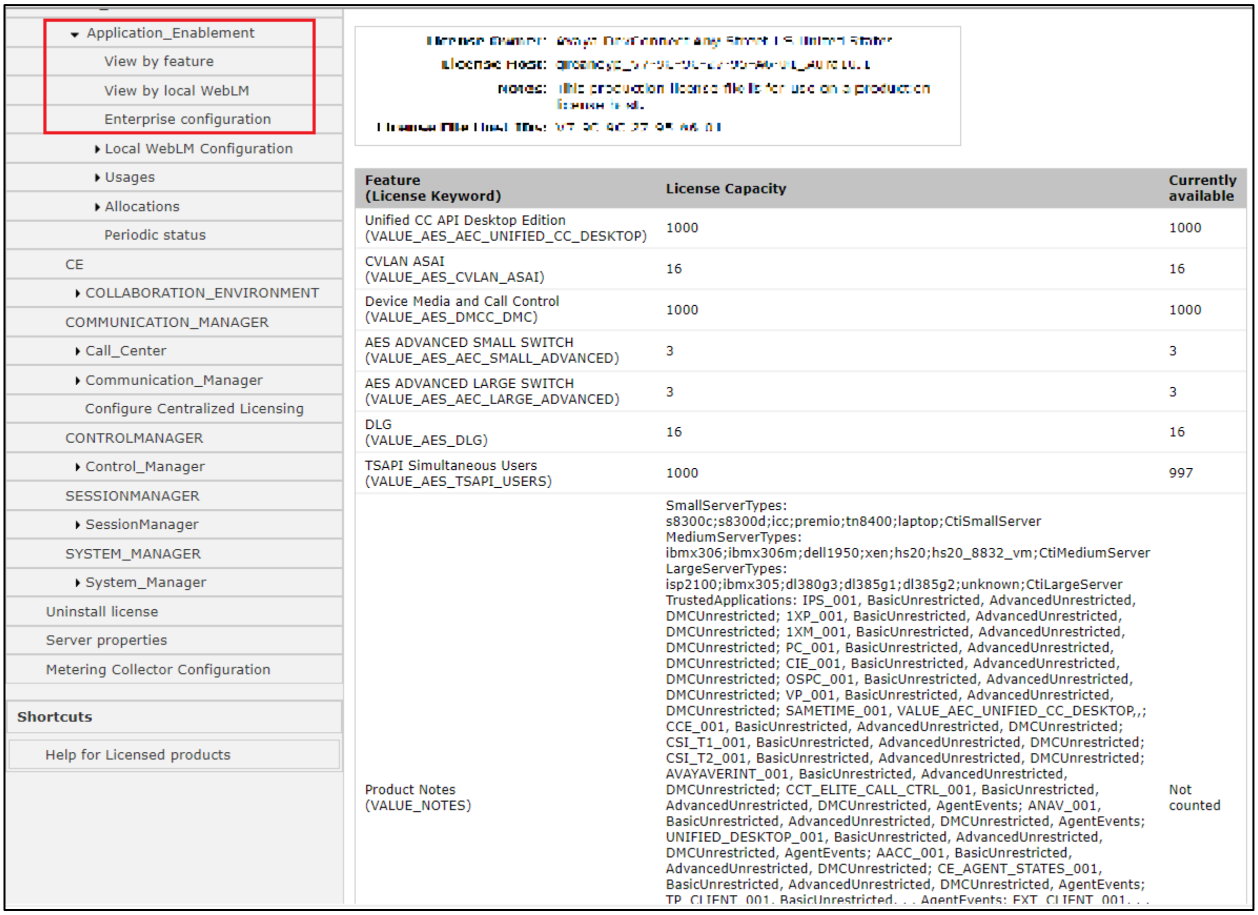
- WebLM Server Access

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.

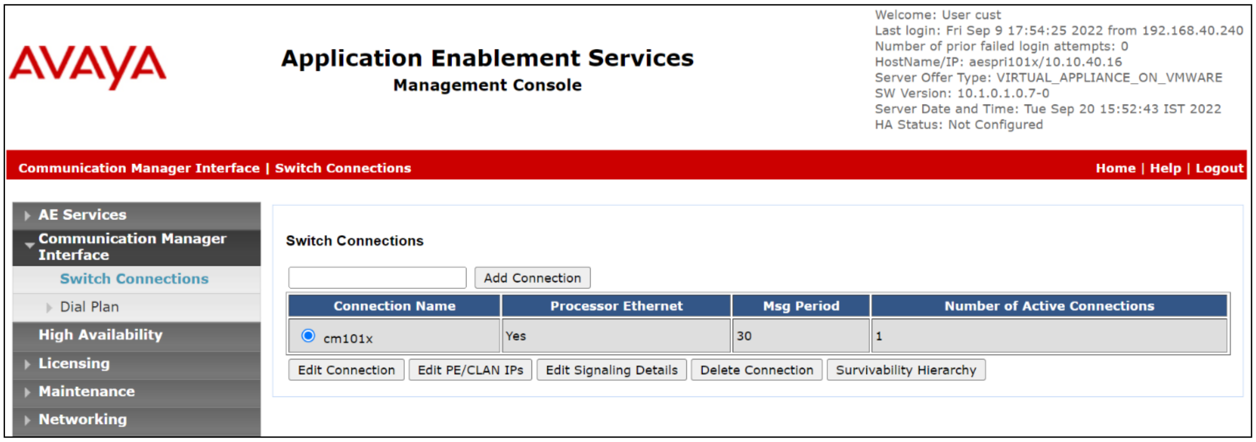


License Owner: [redacted]
License Host: [redacted]
Notes: This production license file is for use on a production license host.
License File Host IDs: [redacted]

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; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AEC_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_CLIENT_001, BasicUnrestricted, . . AgentEvents; EXT_CLIENT_001, . .	Not counted

6.2. Switch Connection to Avaya Aura® Communication Manager

Typically, the connection between the AES and Communication Manager is set up as part of the initial installation and would not usually be outlined in these Application Notes. The following screenshots show the setup that was used for compliance testing. From the AES Management Console, navigate to **Communication Manager Interface → Switch Connections**, the connection to Communication Manager should be present as shown below but if one is not present one can be added by clicking on **Add Connection**.

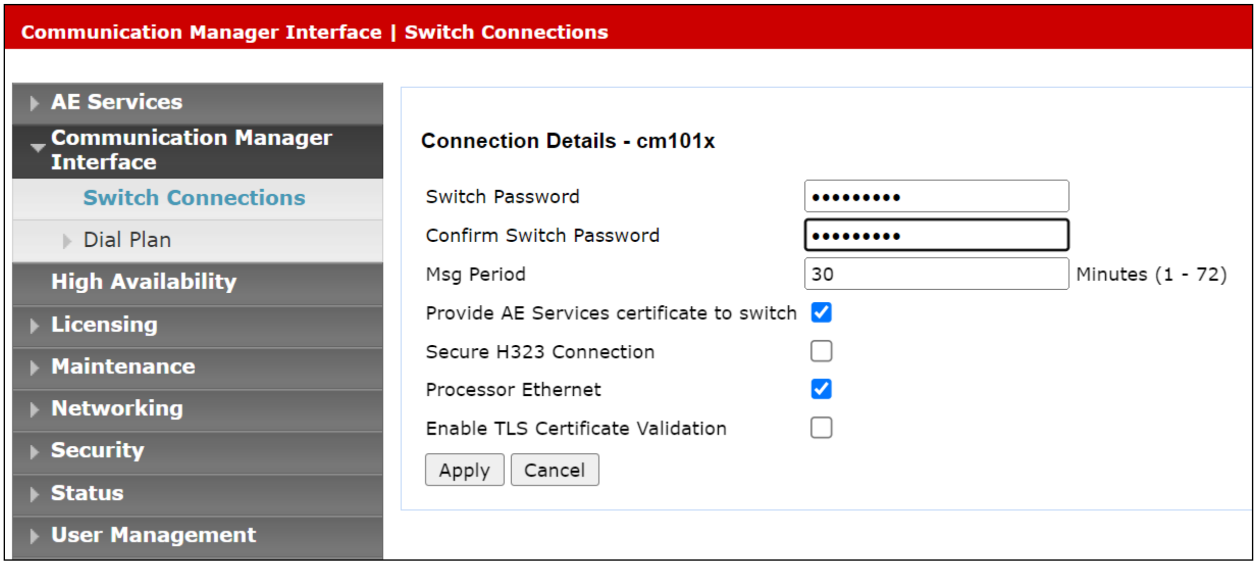


Welcome: User cust
Last login: Fri Sep 9 17:54:25 2022 from 192.168.40.240
Number of prior failed login attempts: 0
HostName/IP: aespri101x/10.10.40.16
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.1.0.7-0
Server Date and Time: Tue Sep 20 15:52:43 IST 2022
HA Status: Not Configured

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● cm101x	Yes	30	1

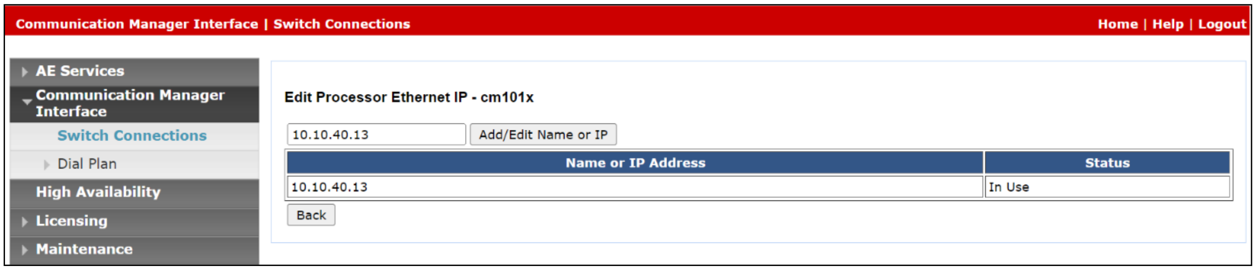
In the resulting screen, enter the **Switch Password**; the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.2.2**. **Secure H323 Connection** was left unticked, as shown below. Click **Apply** to save changes.



Connection Details - cm101x

Switch Password	•••••••••
Confirm Switch Password	•••••••••
Msg Period	30 Minutes (1 - 72)
Provide AE Services certificate to switch	☑
Secure H323 Connection	□
Processor Ethernet	☑
Enable TLS Certificate Validation	□

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit PE/CLAN IPs** button (not shown), see screen at the bottom of the previous page. In the resulting screen, enter the IP address of the procr as shown in **Section 5.2.1** that will be used for the AES connection and select the **Add/Edit Name or IP** button.

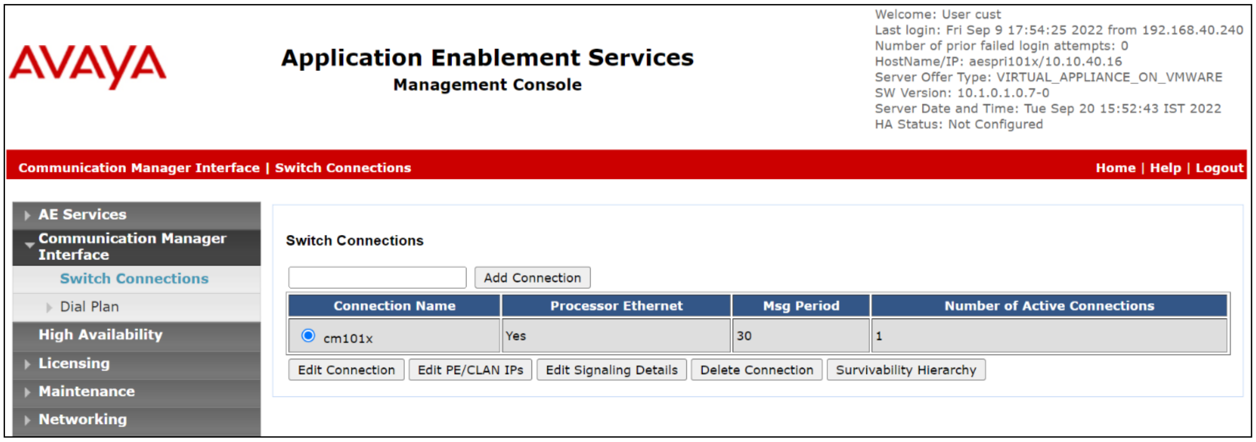


Edit Processor Ethernet IP - cm101x

10.10.40.13

Name or IP Address	Status
10.10.40.13	In Use

Clicking on **Edit Signaling Details** below brings up the H.323 Gatekeeper page.

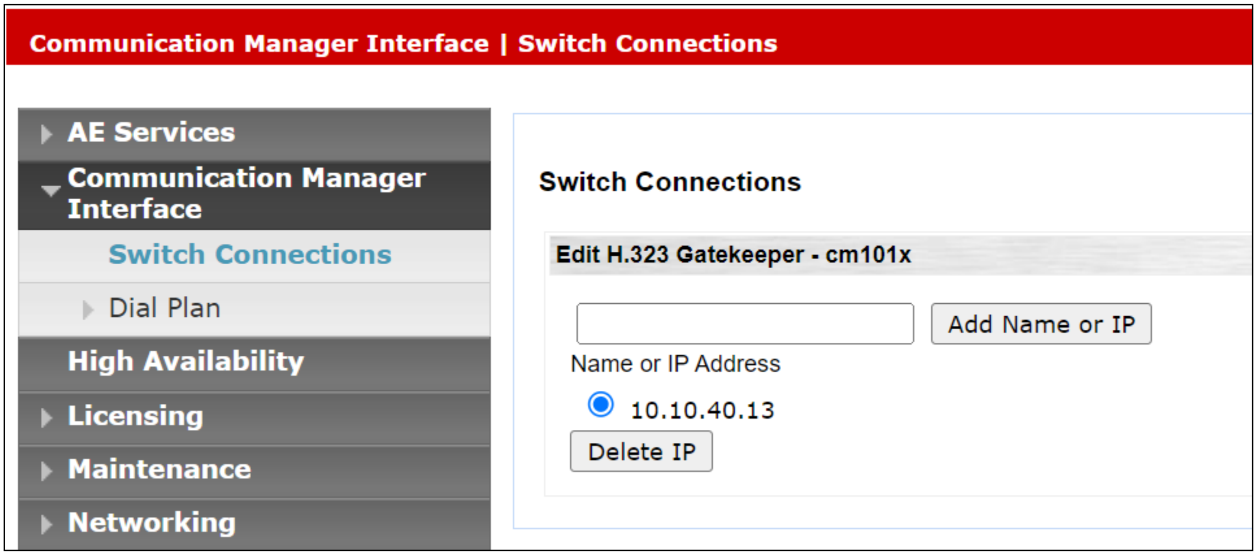


Welcome: User cust
Last login: Fri Sep 9 17:54:25 2022 from 192.168.40.240
Number of prior failed login attempts: 0
HostName/IP: aespri101x/10.10.40.16
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.1.0.7-0
Server Date and Time: Tue Sep 20 15:52:43 IST 2022
HA Status: Not Configured

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● cm101x	Yes	30	1

The IP address of Communication Manager is set for the **H.323 Gatekeeper**, as shown below.



Switch Connections

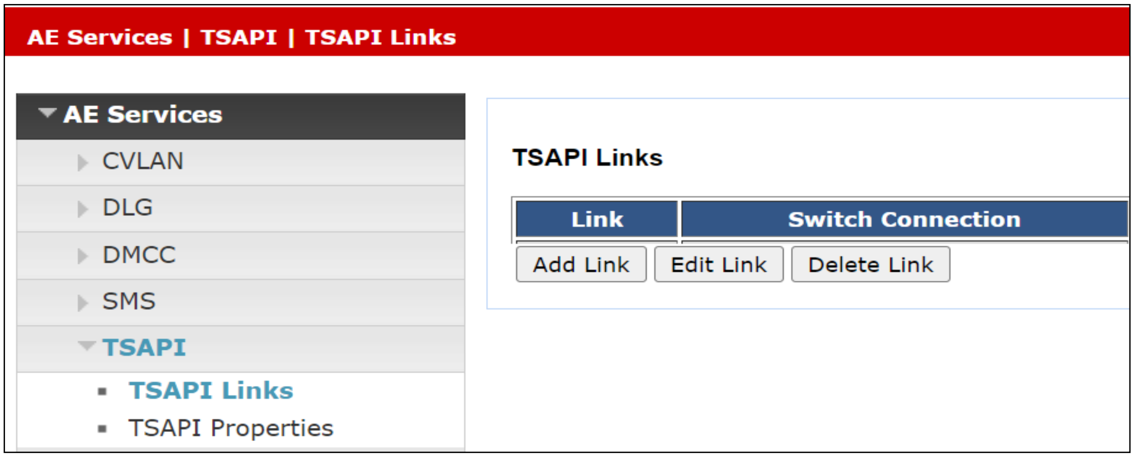
Edit H.323 Gatekeeper - cm101x

Name or IP Address

● 10.10.40.13

6.3. Administer TSAPI link

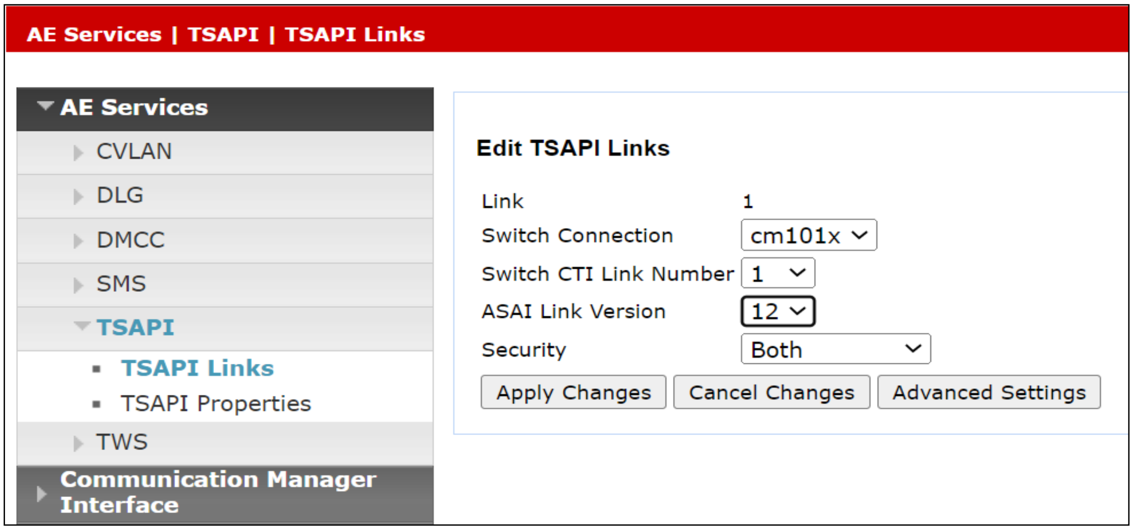
From the Application Enablement Services Management Console, select **AE Services** → **TSAPI** → **TSAPI Links**. Select **Add Link** button as shown in the screen below.



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:

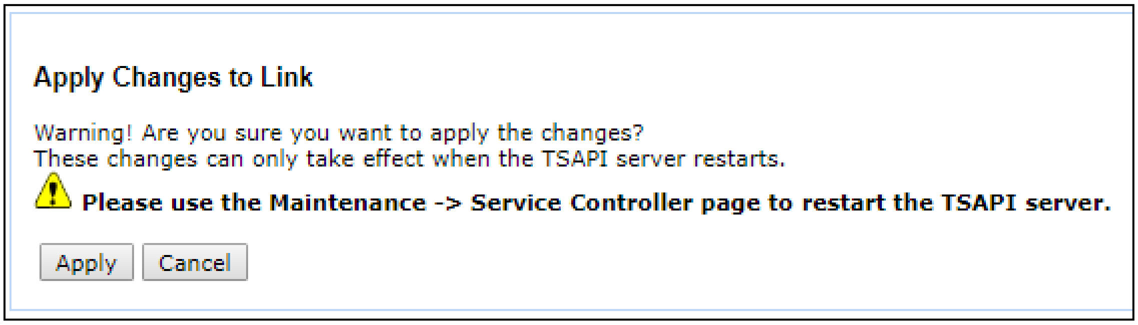
- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **cm101x**, which has already been configured in **Section 6.2** from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.2.3**Error! Reference source not found. which is **1**.
- **ASAI Link Version: 12** was used for compliance testing but the latest version available can be chosen).
- **Security:** This can be left at the default value of **both**.

Once completed, select **Apply Changes**.



Link	1
Switch Connection	cm101x
Switch CTI Link Number	1
ASAI Link Version	12
Security	Both

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

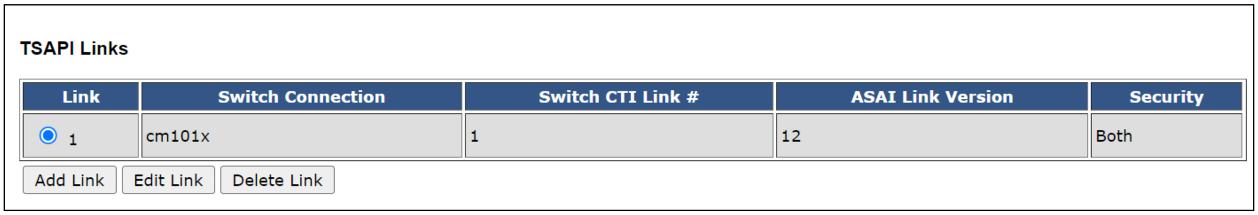


Apply Changes to Link

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.

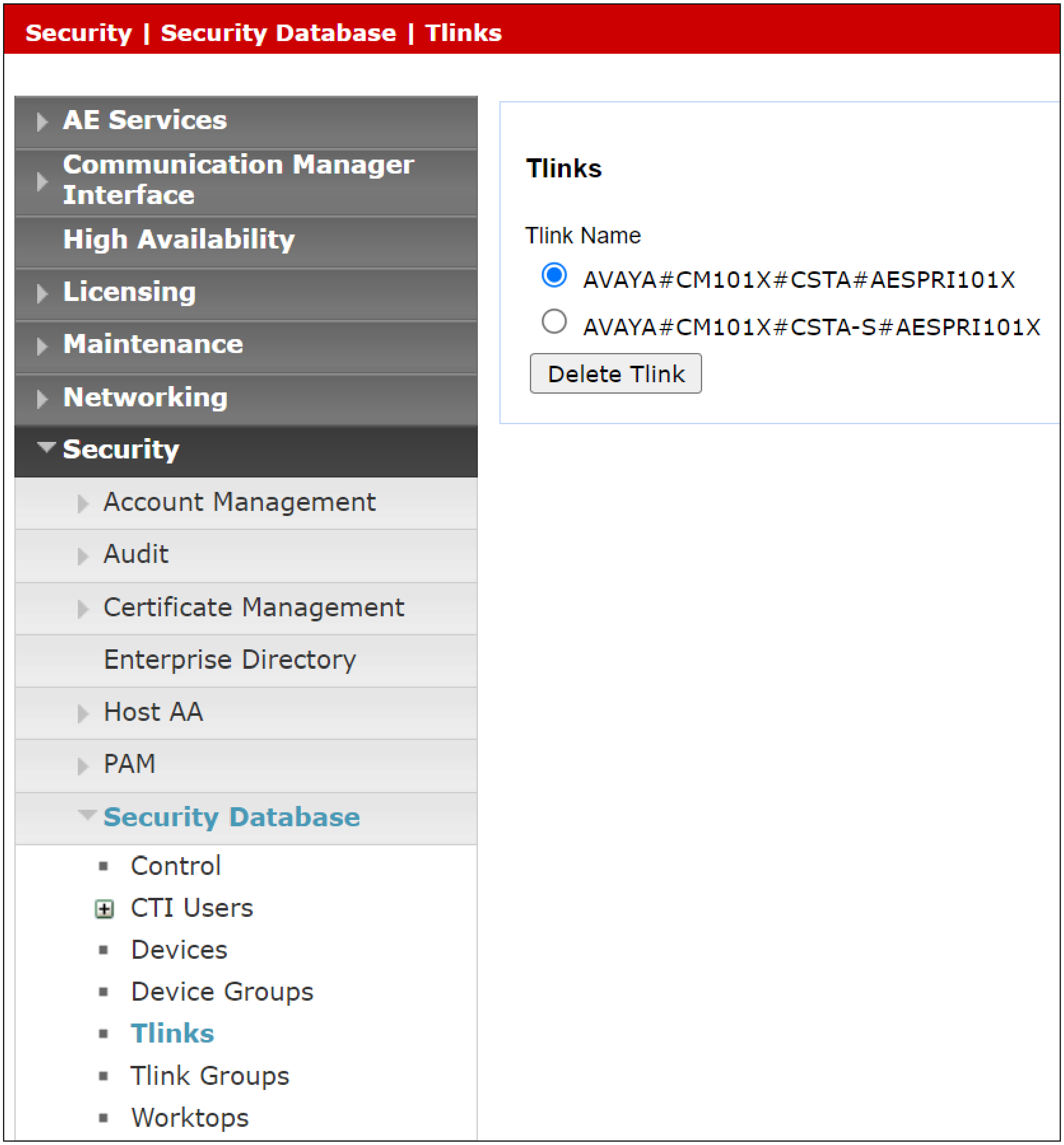


TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
● 1	cm101x	1	12	Both

6.4. Identify Tlinks

Navigate to **Security** → **Security Database** → **Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure/verify the TSAPI Client in **Section 7.1**.



Tlinks

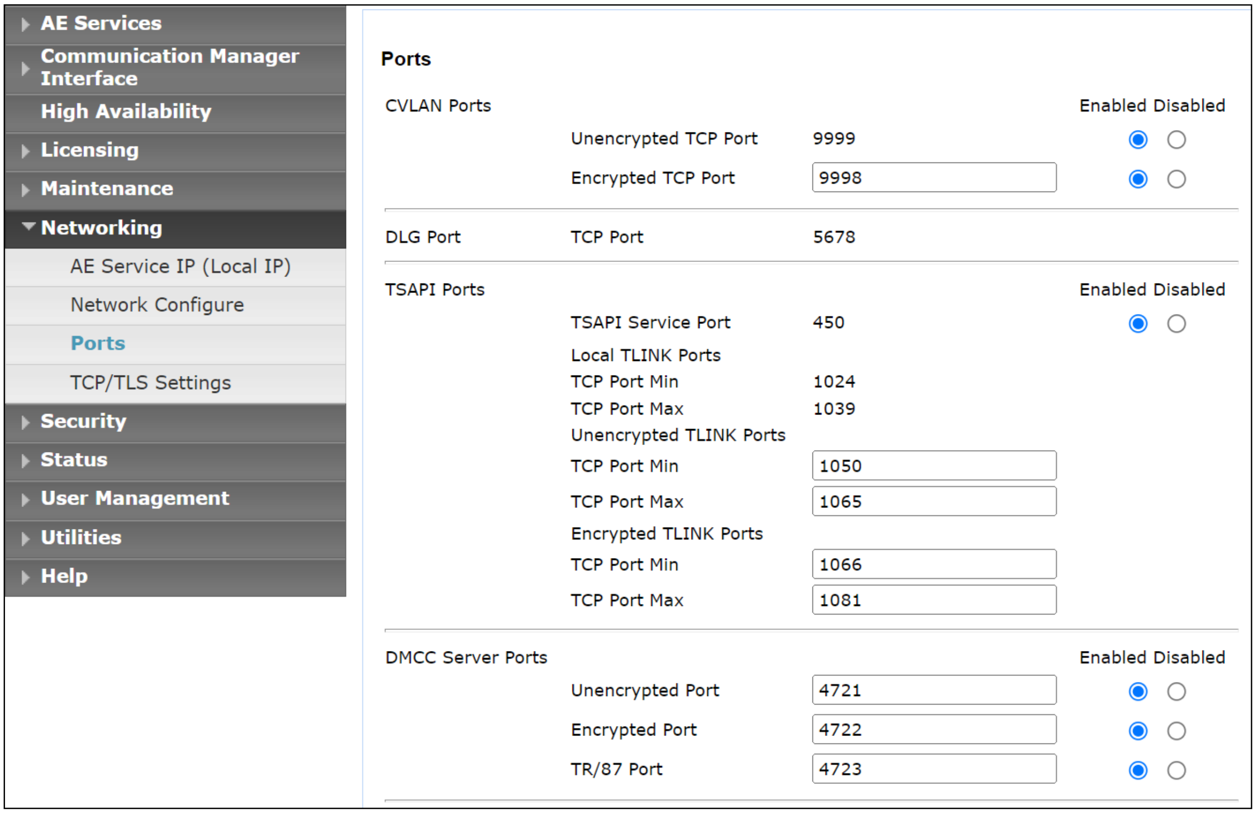
Tlink Name

● AVAYA#CM101X#CSTA#AESPRI101X

○ AVAYA#CM101X#CSTA-S#AESPRI101X

6.5. 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, also note the port number, the default port is 450 and this will be used in the configuration of the TSAPI client in **Section 7.1**.

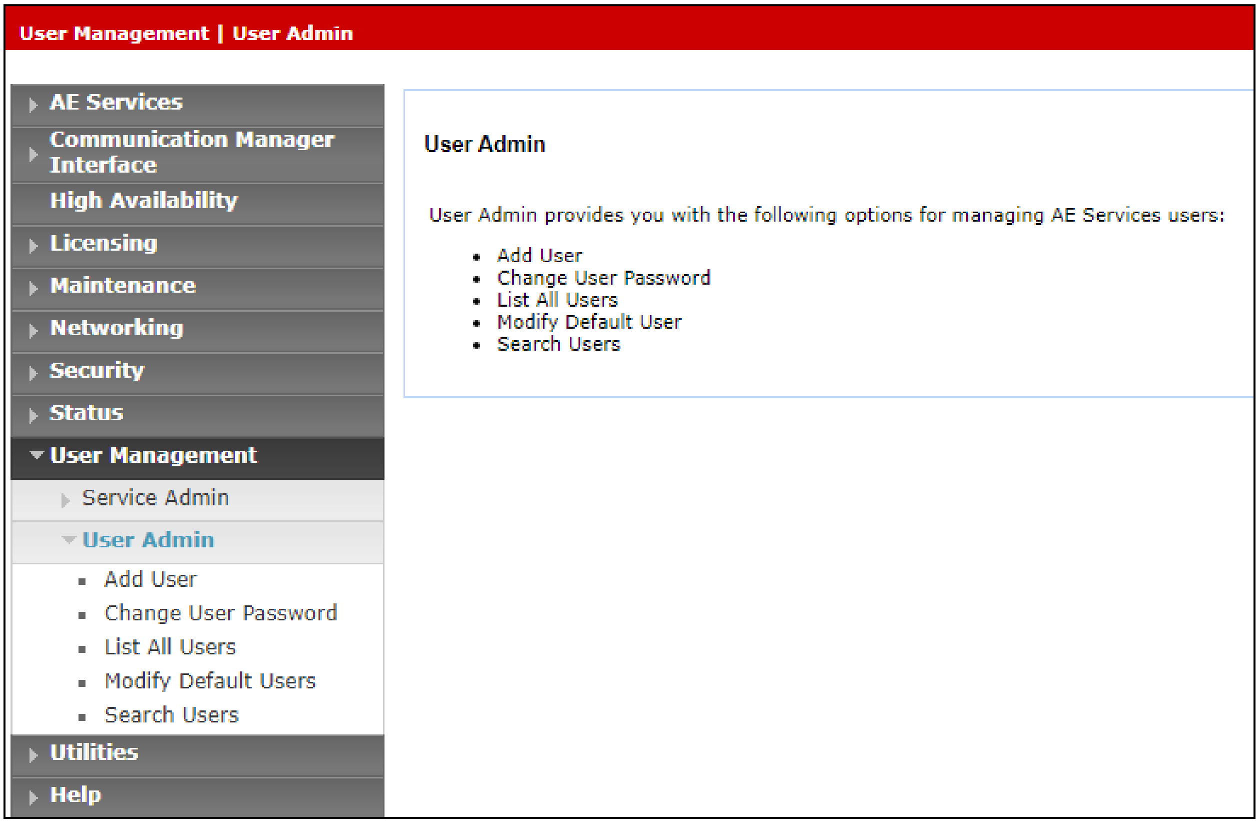


Ports

			Enabled	Disabled
CVLAN Ports			Enabled	Disabled
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports			Enabled	Disabled
	TSAPI Service Port	450	●	○
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	1050		
	TCP Port Max	1065		
	Encrypted TLINK Ports			
	TCP Port Min	1066		
	TCP Port Max	1081		
DMCC Server Ports			Enabled	Disabled
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	●	○

6.6. Create CTI User

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



User Admin

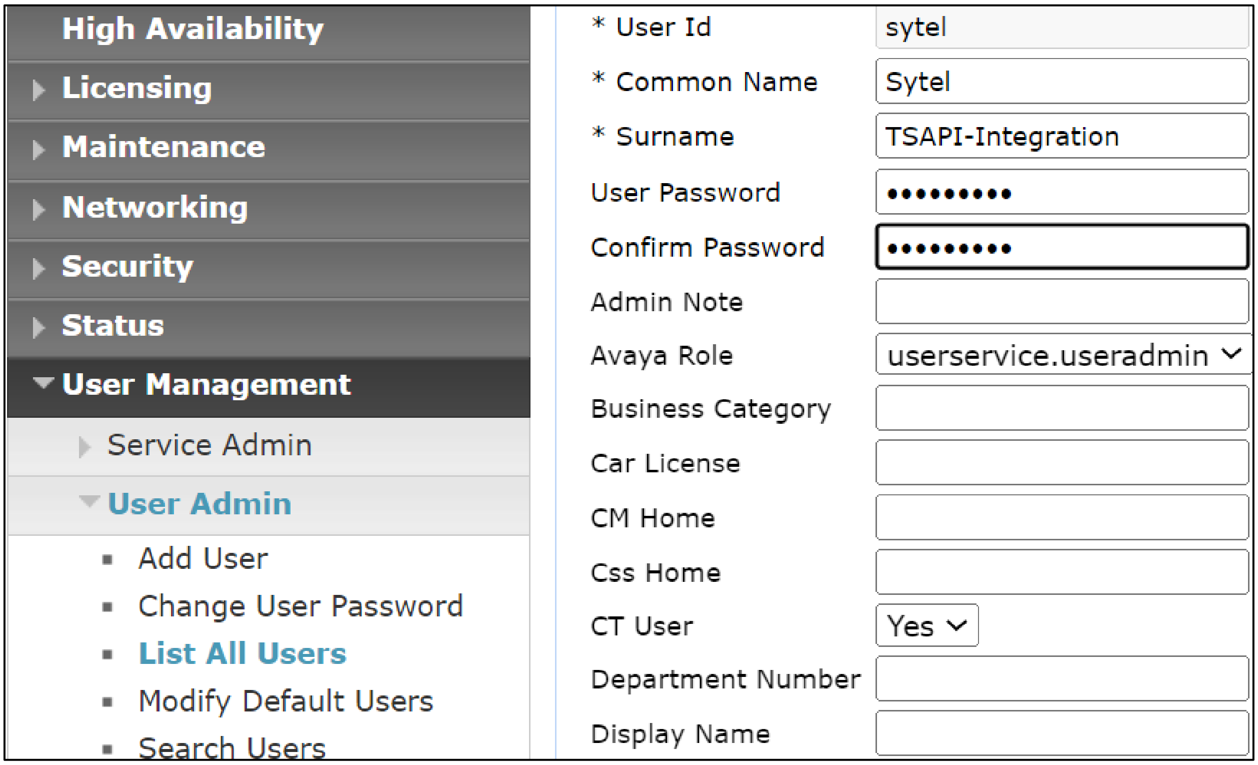
User Admin provides you with the following options for managing AE Services users:

- Add User
- Change User Password
- List All Users
- Modify Default User
- Search Users

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

- **User Id -** This will be used by the Outbound Dialer setup in **Section 7.1**.
- **Common Name** and **Surname -** Descriptive names need to be entered.
- **User Password** and **Confirm Password -** This will be used with the Outbound Dialer setup in **Section 7.1**.
- **CT User -** Select **Yes** from the drop-down menu.

Click on **Apply Changes** at the bottom of the screen (not shown).



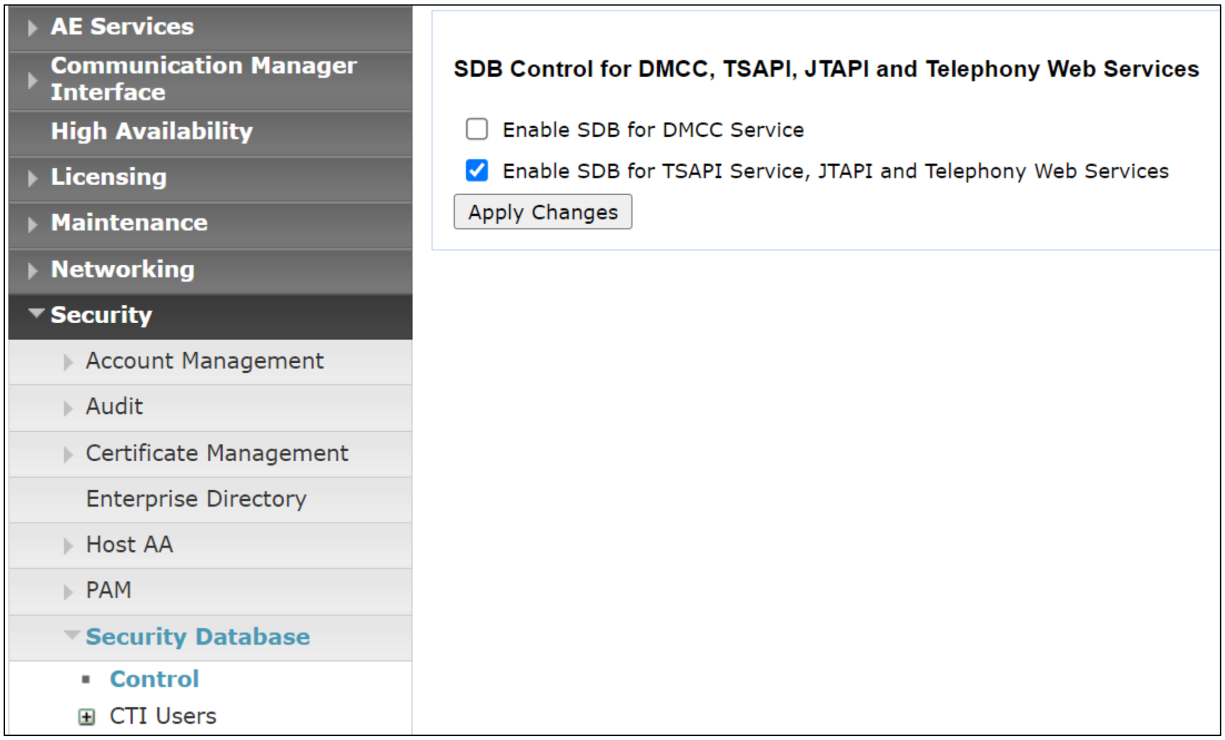
* User Id	sytel
* Common Name	Sytel
* Surname	TSAPI-Integration
User Password	•••••••••
Confirm Password	•••••••••
Admin Note	
Avaya Role	userservice.useradmin
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	

6.7. Configure Security

The CTI user and the database security are set.

6.7.1. Configure Database Control

Open **Control** and ensure that the **SDB Control** is set as shown below.



SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

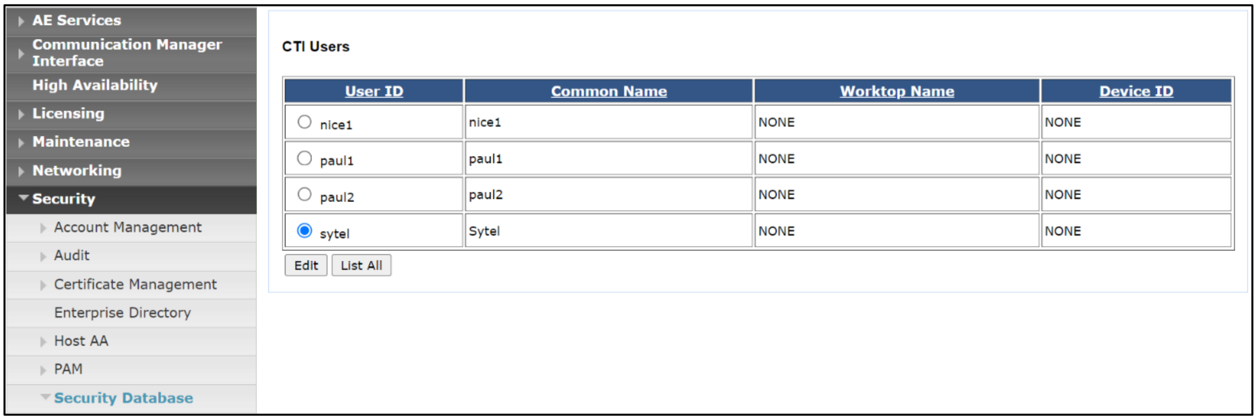
☐ Enable SDB for DMCC Service

☑ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

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 10** for more information on this.

6.7.2. Associate Devices with CTI User

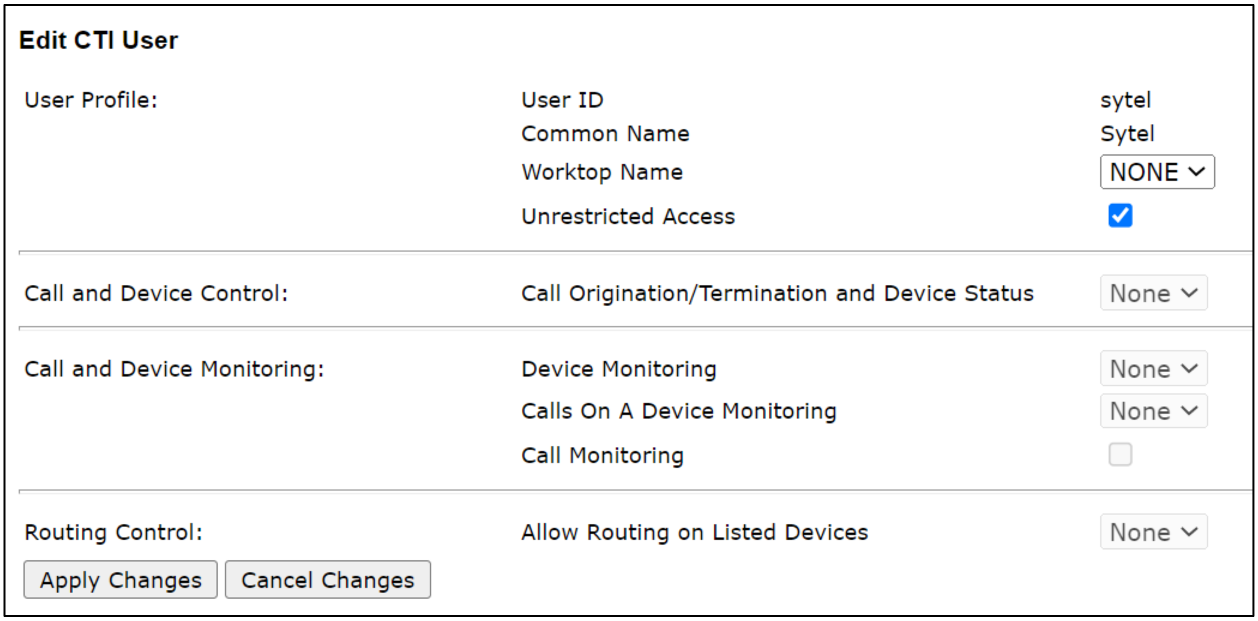
Navigate to **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the CTI user added in **Section 6.6** and click on **Edit Users**.



CTI Users

	User ID	Common Name	Worktop Name	Device ID
○	nice1	nice1	NONE	NONE
○	paul1	paul1	NONE	NONE
○	paul2	paul2	NONE	NONE
●	sytel	Sytel	NONE	NONE

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

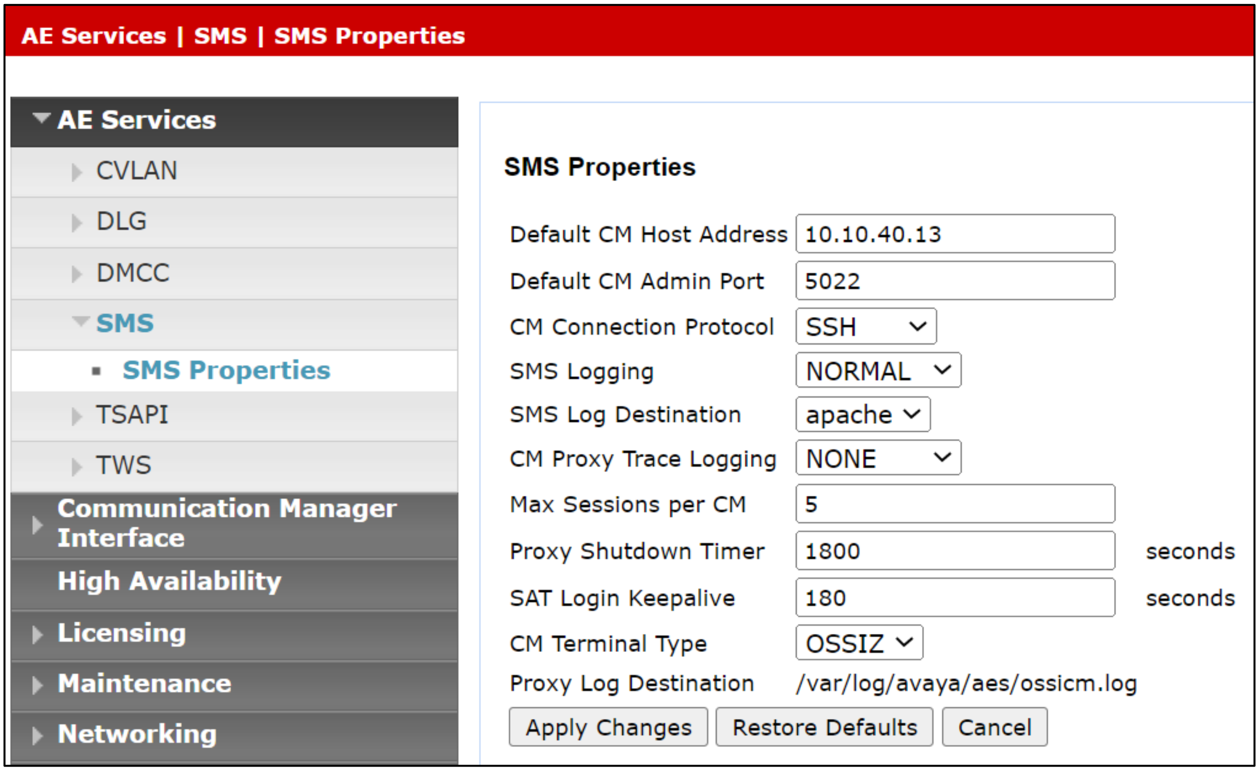


Edit CTI User

User Profile:	User ID	sytel
	Common Name	Sytel
	Worktop Name	NONE
	Unrestricted Access	☑
Call and Device Control:	Call Origination/Termination and Device Status	None
Call and Device Monitoring:	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	☐
Routing Control:	Allow Routing on Listed Devices	None

6.8. 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.

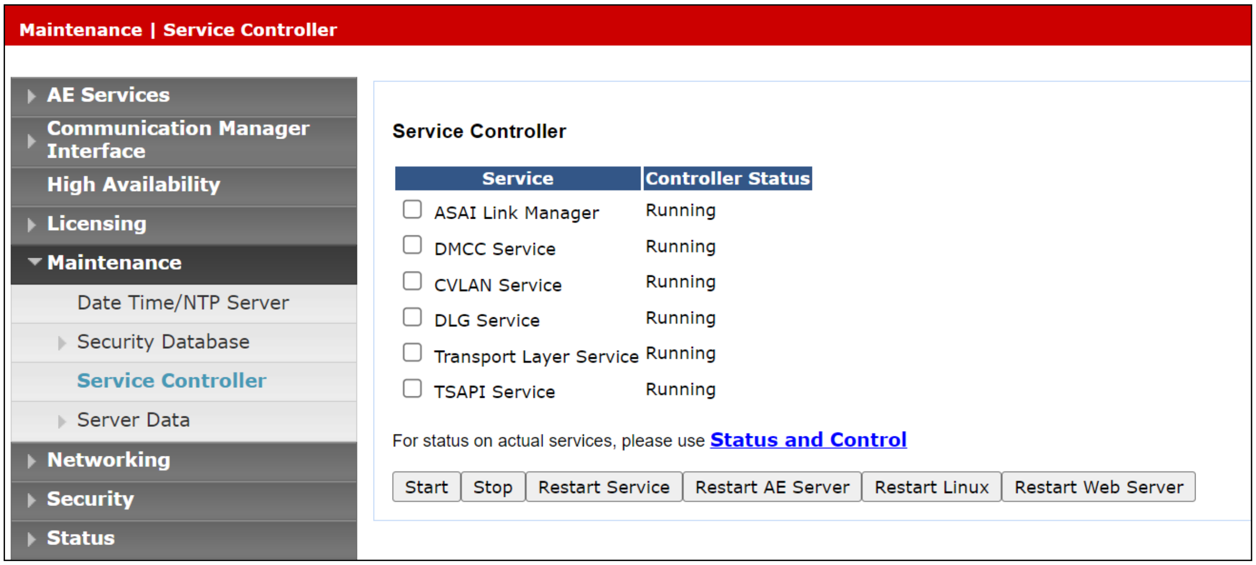


SMS Properties

Default CM Host Address	10.10.40.13	
Default CM Admin Port	5022	
CM Connection Protocol	SSH	
SMS Logging	NORMAL	
SMS Log Destination	apache	
CM Proxy Trace Logging	NONE	
Max Sessions per CM	5	
Proxy Shutdown Timer	1800	seconds
SAT Login Keepalive	180	seconds
CM Terminal Type	OSSIZ	
Proxy Log Destination	/var/log/avaya/aes/ossicm.log	

6.9. 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.

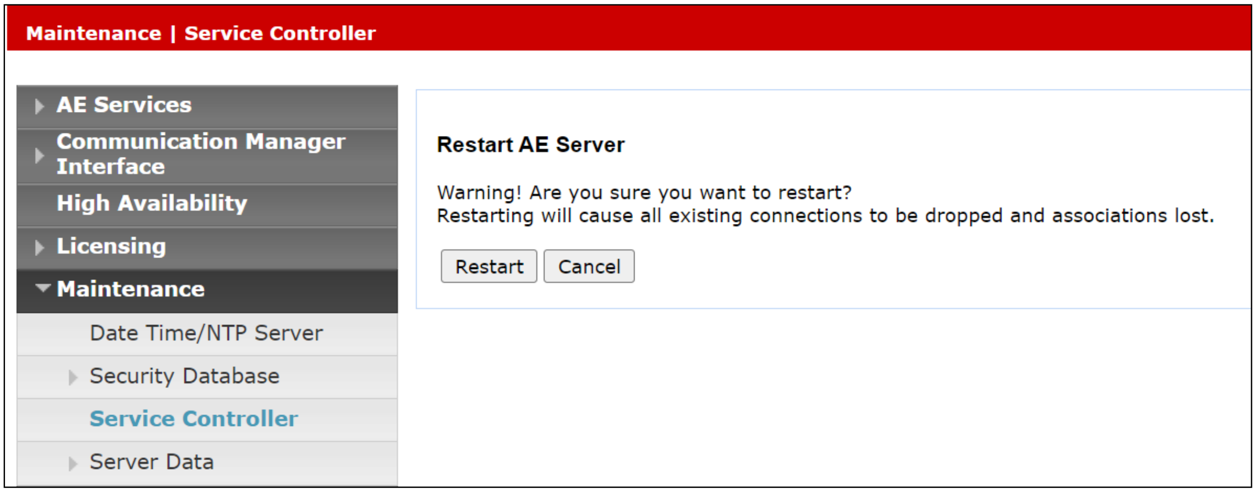


Service Controller

Service	Controller Status
□ ASAI Link Manager	Running
□ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
□ TSAPI Service	Running

For status on actual services, please use Status and Control

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



Restart AE Server

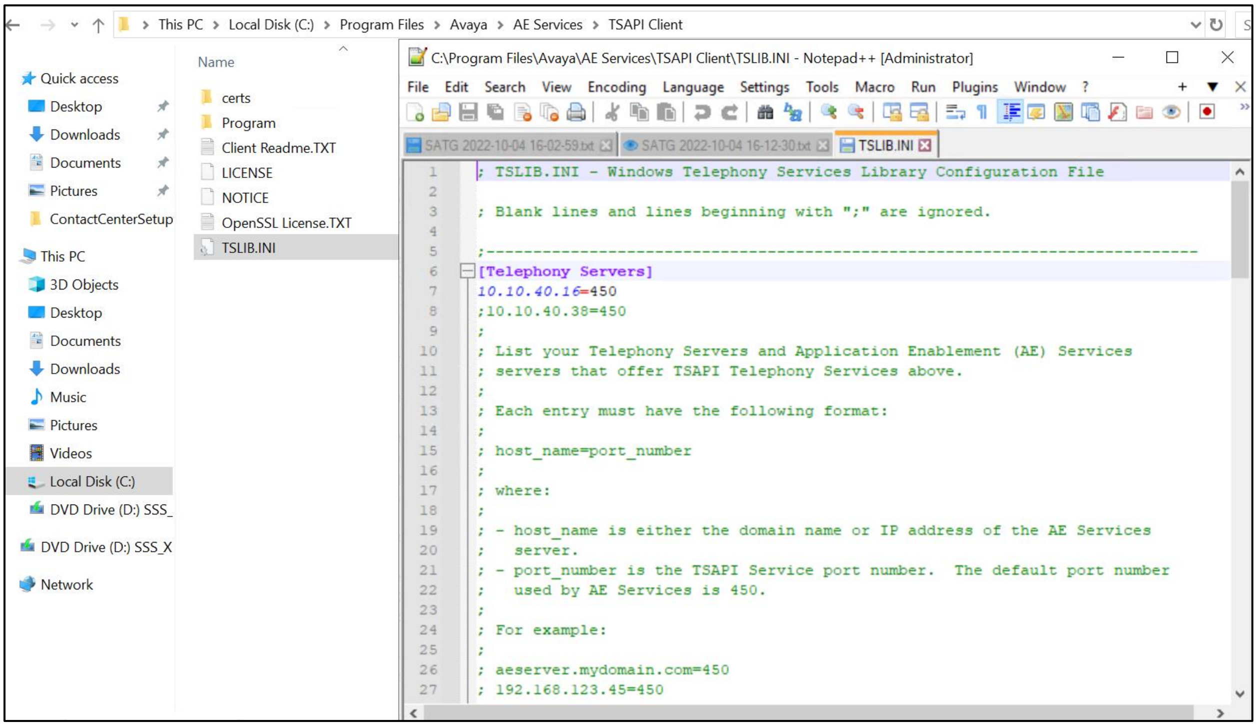
Warning! Are you sure you want to restart?
Restarting will cause all existing connections to be dropped and associations lost.

7. Configure Sytel Softdial Contact Center

The configuration of the SCC server consists of amending a TSAPI client.ini file to ensure the correct IP address is given, and to configure the outbound campaign on the SCC Campaign Manager module. Please consult Sytel's Support using the contact information from **Section 2.3** above to explore all outbound campaign management options or any other SCC options.

7.1. Configure the Avaya TSAPI Client running on SCC Server

Navigate to **Program Files → Avaya → AE Services → TSAPI Client**, as shown below. The **TSLIB.ini** file needs to be edited to add the IP address and port of the AES server, that being **10.10.40.16** and port **450**, as shown below.


This PC › Local Disk (C:) › Program Files › Avaya › AE Services › TSAPI Client
Quick access
Desktop
Downloads
Documents
Pictures
ContactCenterSetup
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) SSS_
DVD Drive (D:) SSS_X
Network
Name
certs
Program
Client Readme.TXT
LICENSE
NOTICE
OpenSSL License.TXT
TSLIB.INI
C:\Program Files\Avaya\AE Services\TSAPI Client\TSLIB.INI - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
SATG 2022-10-04 16-02-59.txt
SATG 2022-10-04 16-12-30.txt
TSLIB.INI

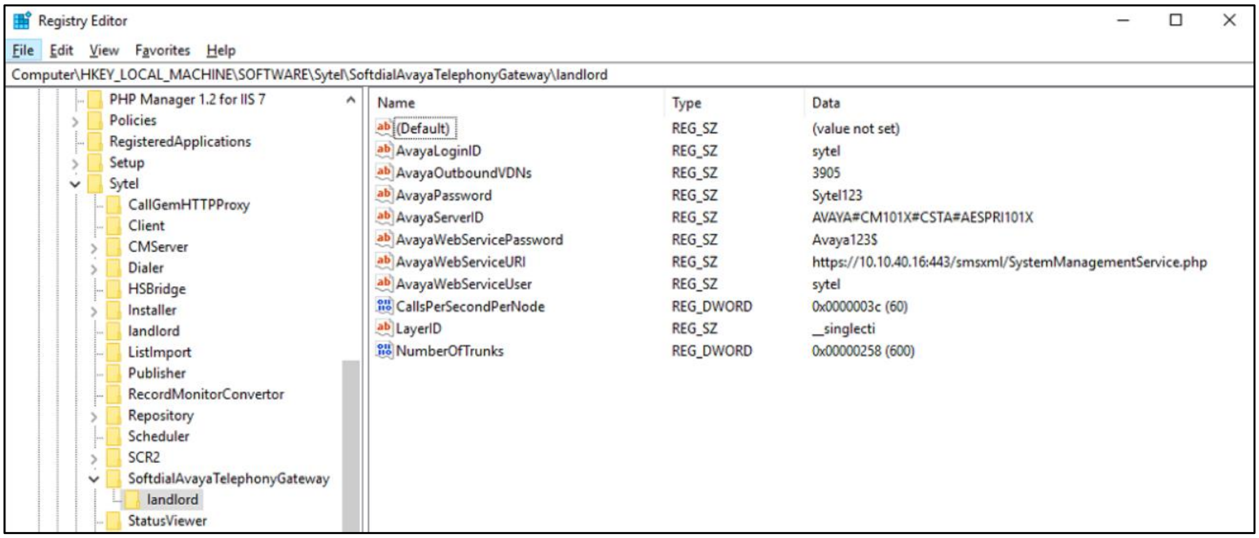
```
; TSLIB.INI - Windows Telephony Services Library Configuration File

; Blank lines and lines beginning with ";" are ignored.

;---------------------------------------------------------------------------
[Telephony Servers]
10.10.40.16=450
;10.10.40.38=450
;
; List your Telephony Servers and Application Enablement (AE) Services
; servers that offer TSAPI Telephony Services above.
;
; Each entry must have the following format:
;
; host_name=port_number
;
; where:
;
; - host_name is either the domain name or IP address of the AE Services
;   server.
; - port_number is the TSAPI Service port number.  The default port number
;   used by AE Services is 450.
;
; For example:
;
; aeserver.mydomain.com=450
; 192.168.123.45=450
```

7.2. Configure Sytel Avaya Telephony gateway on SCC Server

Sytel’s integration service (SATG) configuration parameters are stored in the Windows Registry. Open Windows Registry Editor to the registry path **HKEY_LOCAL_MACHINE\SOFTWARE\Sytel\SoftdialAvayaTelephonyGateway\landlord**

The configuration parameters were set as shown for compliance testing. The following parameters should be configured:

AvayaWebServiceURI: SMS address
AvayaWebServiceUser: SMS user
AvayaWebServicePassword: SMS Password
AvayaServerID: TSAPI Server Instance
AvayaLogindID: TSAPI User
AvayaPassword: TSAPI Password
AvayaOutboundVDNs: Outbound VDN
NumberOfTrunks: Maximum number of simultaneous outbound calls. Use the ratio of 2:5 trunks per agent when using Predictive campaigns—default 600.
CallsPerSecondPerNode: Maximum number of calls per second for all outbound campaigns. Default 60.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Sytel\SoftdialAvayaTelephonyGateway\landlord

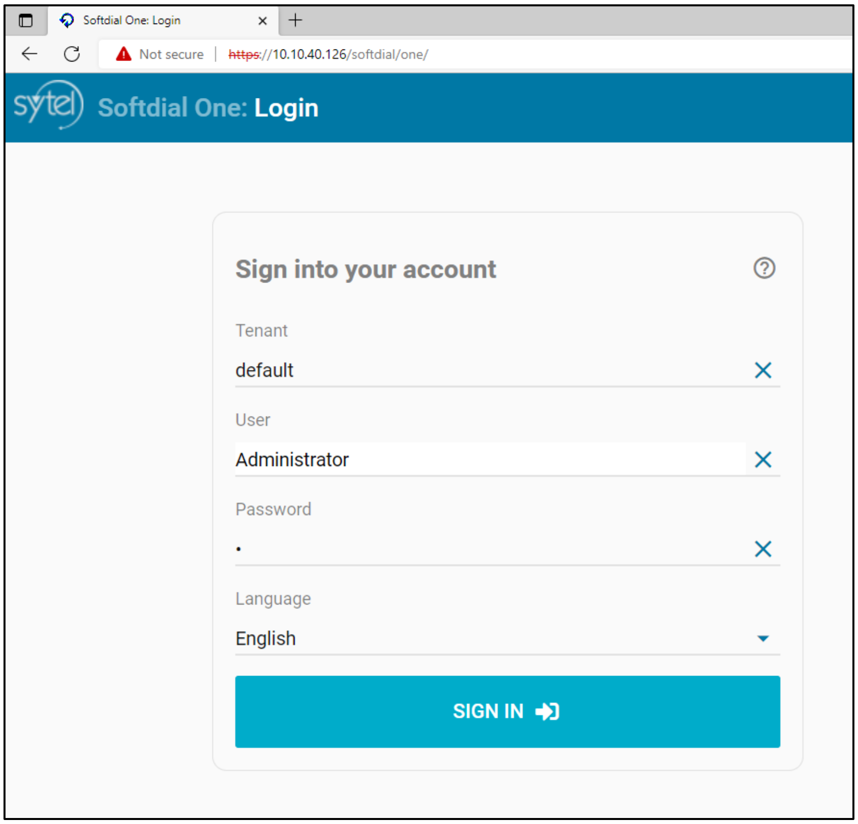
Name	Type	Data
(Default)	REG_SZ	(value not set)
AvayaLoginID	REG_SZ	sytel
AvayaOutboundVDNs	REG_SZ	3905
AvayaPassword	REG_SZ	Sytel123
AvayaServerID	REG_SZ	AVAYA#CM101X#CSTA#AESPRI101X
AvayaWebServicePassword	REG_SZ	Avaya123$
AvayaWebServiceURI	REG_SZ	https://10.10.40.16:443/smsxml/SystemManagementService.php
AvayaWebServiceUser	REG_SZ	sytel
CallsPerSecondPerNode	REG_DWORD	0x0000003c (60)
LayerID	REG_SZ	_singlecti
NumberOfTrunks	REG_DWORD	0x00000258 (600)

Note: The parameters not listed above are for internal use and should not be changed.

Note: Restart the service Softdial Avaya Telephony Gateway after changing any of the parameters.

7.3. Configure the Outbound Campaign

Open a web browser to the IP address of the Softdial Contact Center server. Enter the appropriate credentials and click on **Sign In**.



Sign into your account

Tenant: default

User: Administrator

Password: •

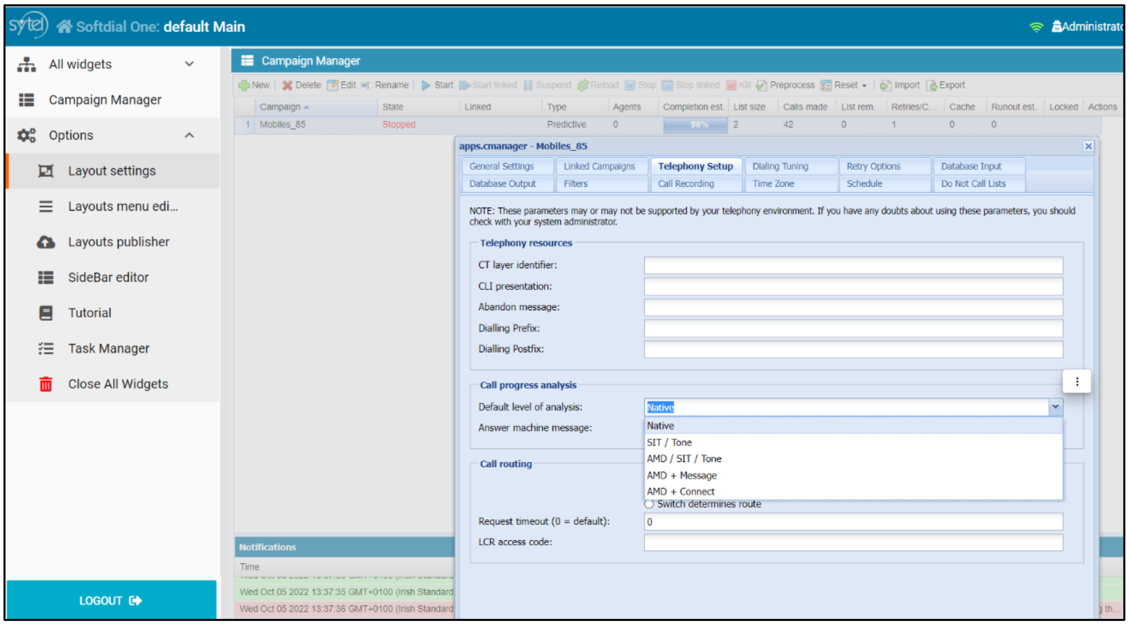
Language: English

For a complete set of instructions on creating an outbound campaign and loading data for outbound dialing, please contact Sytel's support, as per **Section 2.3**.

Please note that the campaign name format is key to relating an outbound campaign in SCC with an outbound skill in Avaya.

Following the screenshot example, the campaign "*Mobiles_85*" will use skill 85 as its outbound skill in AES. This is a required configuration for SCC Dialer integration.

Open **Campaign Manager** by clicking on it in the left window, and the existing outbound campaign should be displayed. Double-click on the campaign, and a new window will open, as shown below. Click on the **Telephony Setup** tab. Note that the **Default level of analysis** was set to **Native**, as shown. This will ensure that Answering Machine Detection was not set to that on Communication Manager.



	Campaign	State	Linked	Type	Agents	Completion est.	List size	Calls made	List rem.	Retries/C...	Cache	Runout est.	Locked	Actions
1	Mobiles_85	Stopped		Predictive	0	98%	2	42	0	1	0	0		

NOTE: These parameters may or may not be supported by your telephony environment. If you have any doubts about using these parameters, you should check with your system administrator.

Telephony resources

CT layer identifier:

CLI presentation:

Abandon message:

Dialling Prefix:

Dialling Postfix:

Call progress analysis

Default level of analysis: Native

Answer machine message:

Call routing

○ Switch determines route

Request timeout (0 = default): 0

LCR access code:

Wed Oct 05 2022 13:37:35 GMT+0100 (Irish Standard

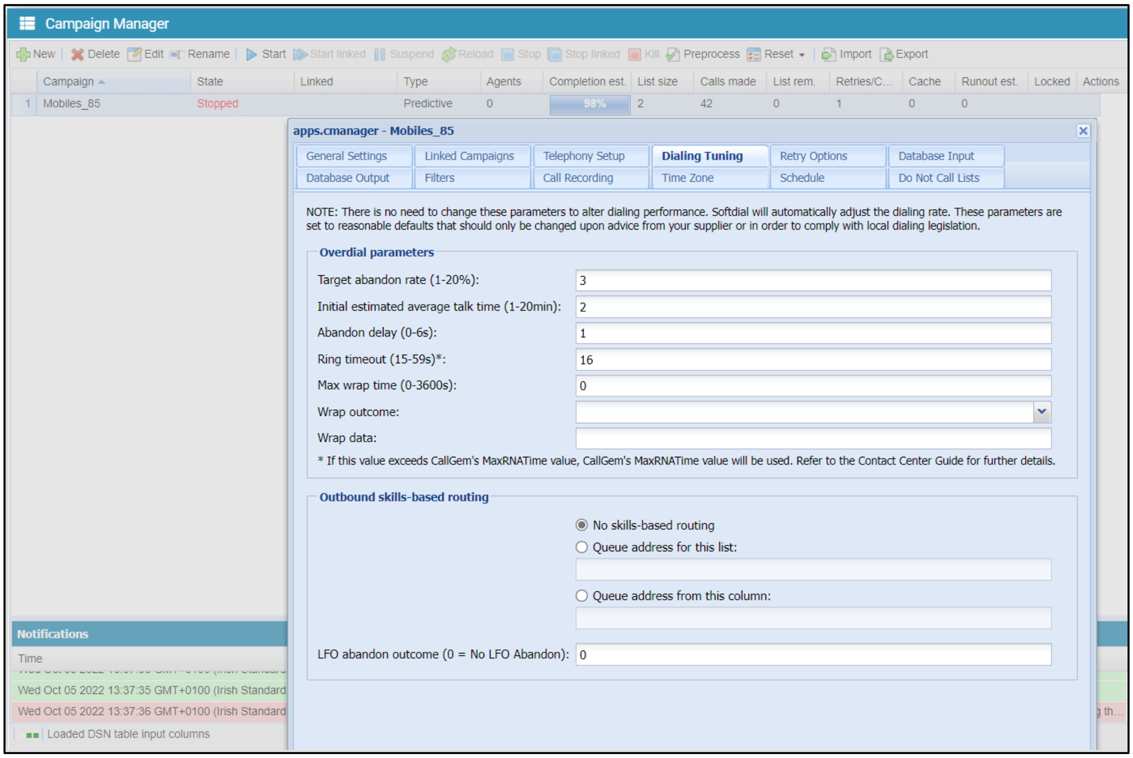
Wed Oct 05 2022 13:37:36 GMT+0100 (Irish Standard

Communication Manager performs the Answer Machine actions in this integration scenario. It can be optionally enabled by changing the Default level of analysis in an SCC campaign to enable/disable it as follows:

- **Native**: AMD is disabled. This is the TSAPI option AT_NO_TREATMENT
- **SIT / Tone**: AMD is managed by what is the default option in Avaya Communications Manager. This is TSAPI option AT_NONE
- **AMD + Connect**: AMD is enabled for the campaign. This is TSAPI option AT_CONNECT
- **All other options**: AMD is enabled. If detected as AMD, the call is dropped. This is TSAPI option AT_DROP

Note: Avaya's AMD configuration and tunning are not in the scope of this document.

Click on the **Dialing Tuning** tab. These options were set as shown for compliance testing.



	Campaign	State	Linked	Type	Agents	Completion est.	List size	Calls made	List rem.	Retries/C...	Cache	Runout est.	Locked	Actions
1	Mobiles_85	Stopped		Predictive	0	98%	2	42	0	1	0	0		

apps.cmanager - Mobiles_85

NOTE: There is no need to change these parameters to alter dialing performance. Softdial will automatically adjust the dialing rate. These parameters are set to reasonable defaults that should only be changed upon advice from your supplier or in order to comply with local dialing legislation.

Overdial parameters

Target abandon rate (1-20%): 3

Initial estimated average talk time (1-20min): 2

Abandon delay (0-6s): 1

Ring timeout (15-59s)*: 16

Max wrap time (0-3600s): 0

Wrap outcome:

Wrap data:

* If this value exceeds CallGem's MaxRNATime value, CallGem's MaxRNATime value will be used. Refer to the Contact Center Guide for further details.

Outbound skills-based routing

● No skills-based routing

○ Queue address for this list:

○ Queue address from this column:

LFO abandon outcome (0 = No LFO Abandon): 0

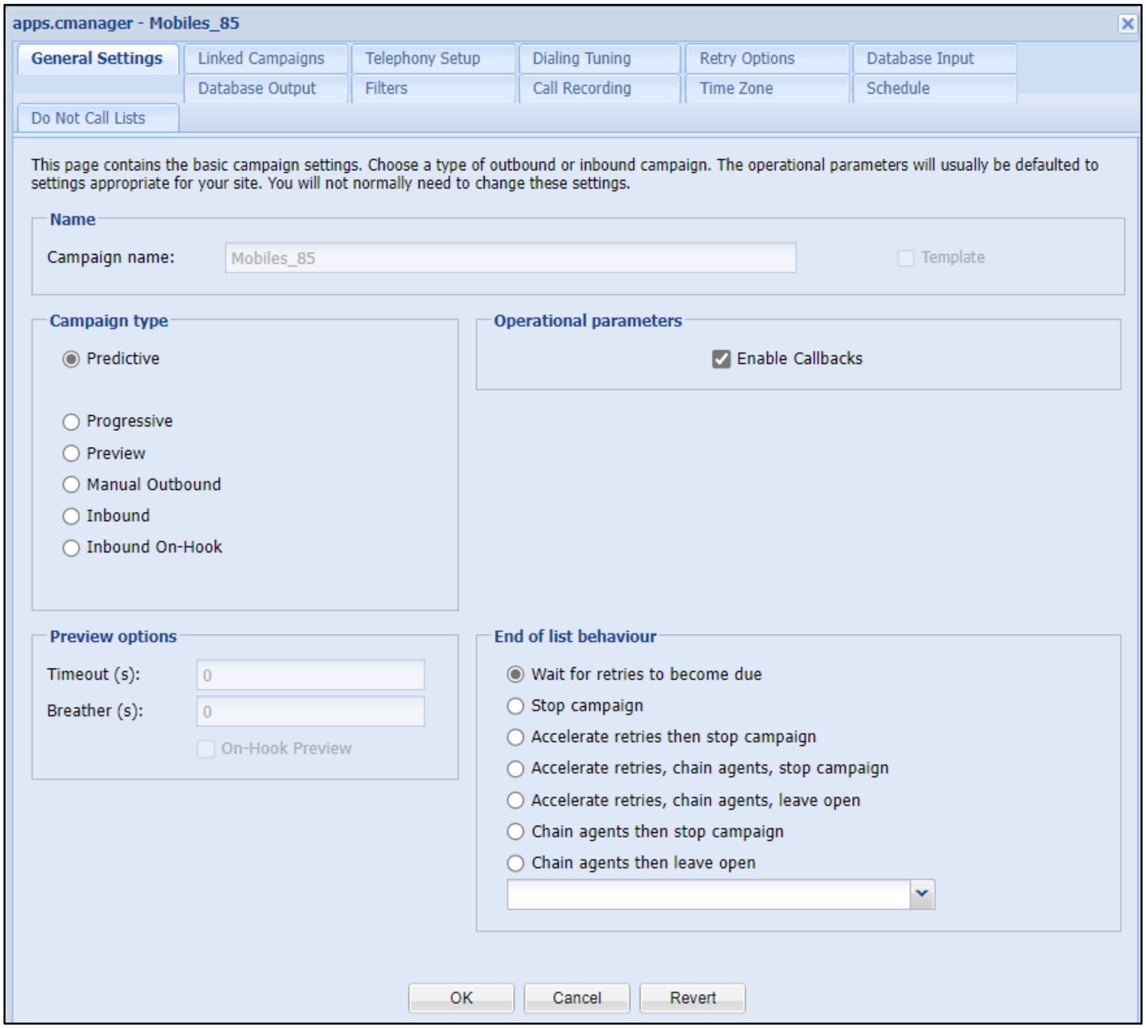
Time

Wed Oct 05 2022 13:37:35 GMT+0100 (Irish Standard

Wed Oct 05 2022 13:37:36 GMT+0100 (Irish Standard

Loaded DSN table input columns

Under the **General Settings** tab, the **Campaign type** can be chosen. For compliance testing, **Predictive**, **Progressive**, and **Preview** campaigns were run.



This page contains the basic campaign settings. Choose a type of outbound or inbound campaign. The operational parameters will usually be defaulted to settings appropriate for your site. You will not normally need to change these settings.

Name

Campaign name: Mobiles_85 □ Template

Campaign type

● Predictive

○ Progressive

○ Preview

○ Manual Outbound

○ Inbound

○ Inbound On-Hook

Operational parameters

☑ Enable Callbacks

Preview options

Timeout (s): 0

Breather (s): 0

□ On-Hook Preview

End of list behaviour

● Wait for retries to become due

○ Stop campaign

○ Accelerate retries then stop campaign

○ Accelerate retries, chain agents, stop campaign

○ Accelerate retries, chain agents, leave open

○ Chain agents then stop campaign

○ Chain agents then leave open

8. Verification Steps

The connection to Application Enablement Services can be verified on the Application Enablement Services side, on the SCC Dialer side, and by using the desktop to make an outbound call.

8.1. 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.

- Verify CTI Service State on Communication Manager
- Verify TSAPI link and user on Application Enablement Services
- Verify SMS on Application Enablement Services

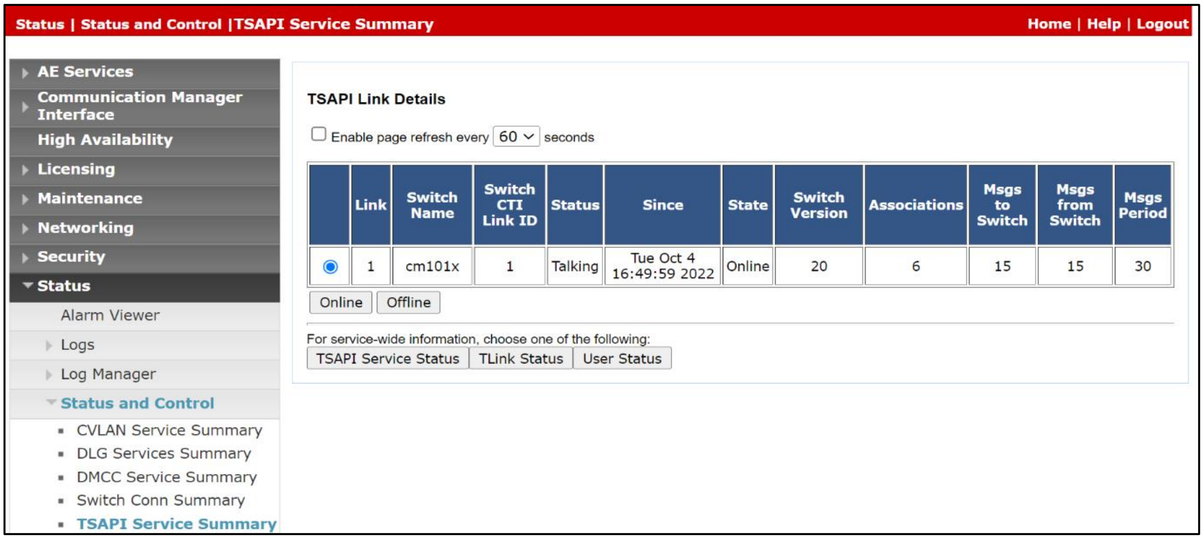
8.1.1. Verify Avaya Aura® Communication Manager CTI Service State

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

```
status aesvcs cti-link

                             AE SERVICES CTI LINK STATUS

CTI    Version      Mnt    AE Services              Service      Msgs      Msgs
Link                Busy      Server                State        Sent      Rcvd

1          12       no       aespri101x             established  865       865
```

8.1.2. Verify TSAPI 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**.



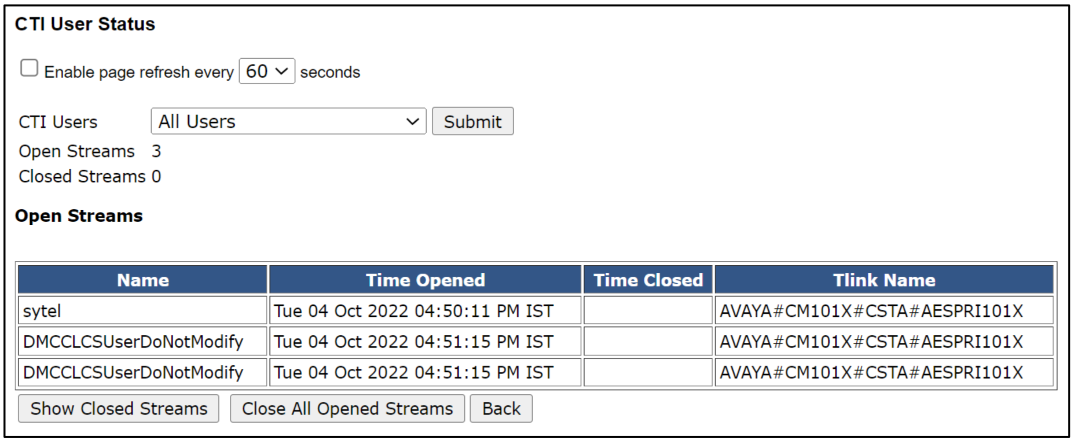
TSAPI Link Details

☐ 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
●	1	cm101x	1	Talking	Tue Oct 4 16:49:59 2022	Online	20	6	15	15	30

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

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



CTI User Status

☐ Enable page refresh every 60 seconds

CTI Users: All Users [Submit]

Open Streams 3

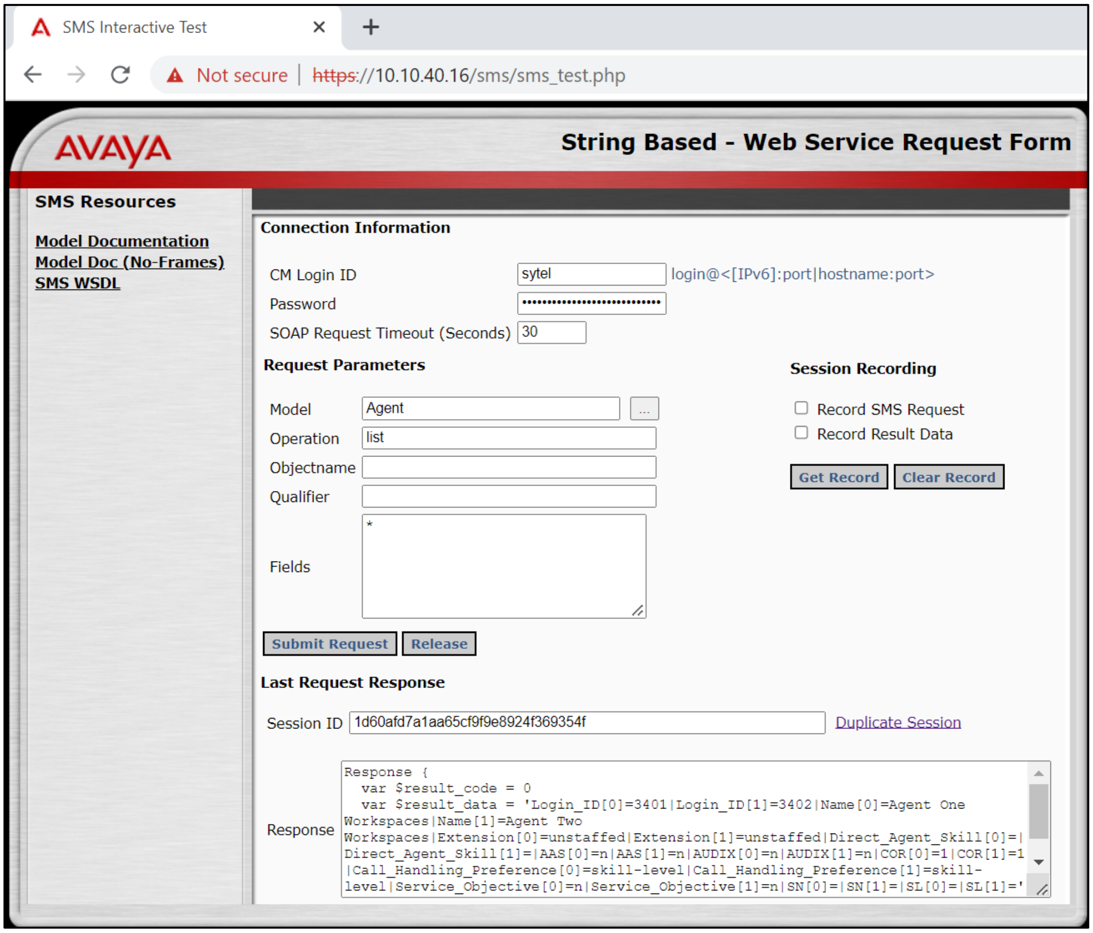
Closed Streams 0

Open Streams

Name	Time Opened	Time Closed	Tlink Name
sytel	Tue 04 Oct 2022 04:50:11 PM IST		AVAYA#CM101X#CSTA#AESPRI101X
DMCCLCSUserDoNotModify	Tue 04 Oct 2022 04:51:15 PM IST		AVAYA#CM101X#CSTA#AESPRI101X
DMCCLCSUserDoNotModify	Tue 04 Oct 2022 04:51:15 PM IST		AVAYA#CM101X#CSTA#AESPRI101X

8.1.3. Verify SMS link

Open a web page to **https://<AESIP>/sms/sms-test.php**, as shown below. Enter the Communication Manager login details and a **Reques**t, such as List Agent, is entered as shown below, this should return a **Response** as shown.



Connection Information

CM Login ID: sytel (login@<[IPv6]:port|hostname:port>)

Password: ••••••••••••••••••••••••••••

SOAP Request Timeout (Seconds): 30

Request Parameters

Model: Agent

Operation: list

Objectname:

Qualifier:

Fields: *

Session Recording

☐ Record SMS Request

☐ Record Result Data

Last Request Response

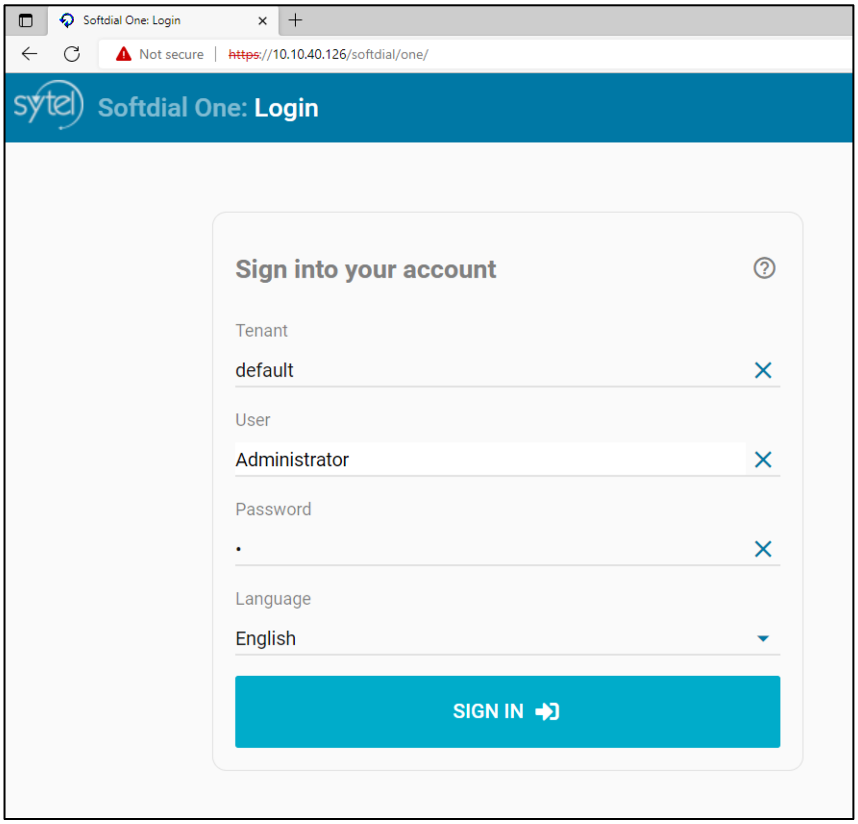
Session ID: 1d60afd7a1aa65cf9f9e8924f369354f

Response:

```
Response {
  var $result_code = 0
  var $result_data = 'Login_ID[0]=3401|Login_ID[1]=3402|Name[0]=Agent One
Workspaces|Name[1]=Agent Two
Workspaces|Extension[0]=unstaffed|Extension[1]=unstaffed|Direct_Agent_Skill[0]=|
Direct_Agent_Skill[1]=|AAS[0]=n|AAS[1]=n|AUDIX[0]=n|AUDIX[1]=n|COR[0]=1|COR[1]=1
|Call_Handling_Preference[0]=skill-level|Call_Handling_Preference[1]=skill-
level|Service_Objective[0]=n|Service_Objective[1]=n|SN[0]=|SN[1]=|SL[0]=|SL[1]='
```

8.2. Verify Connection from Sytel SCC

Log into the Softdial Contact Center by opening a web session to the IP address of the dialer as shown below. Enter the appropriate credentials and click on **Sign In**.



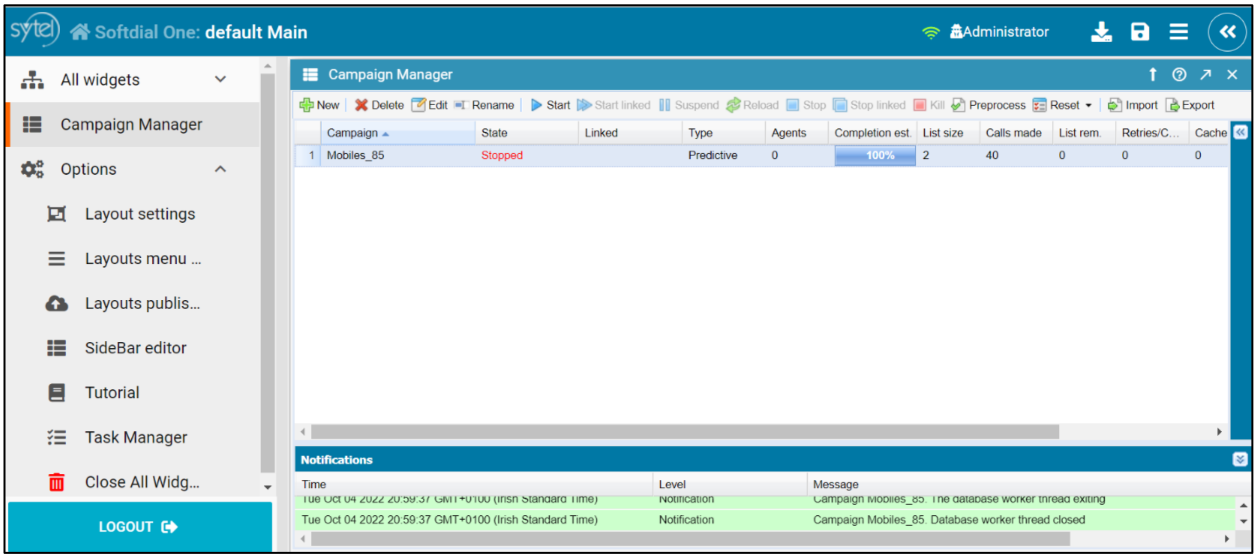
Tenant
default

User
Administrator

Password
•

Language
English

Navigate to **Campaign Manager** in the left window and start the campaign by highlighting the configured outbound campaign in the main window and clicking on **Start** above it. The outbound Campaign should be running before any agent login.

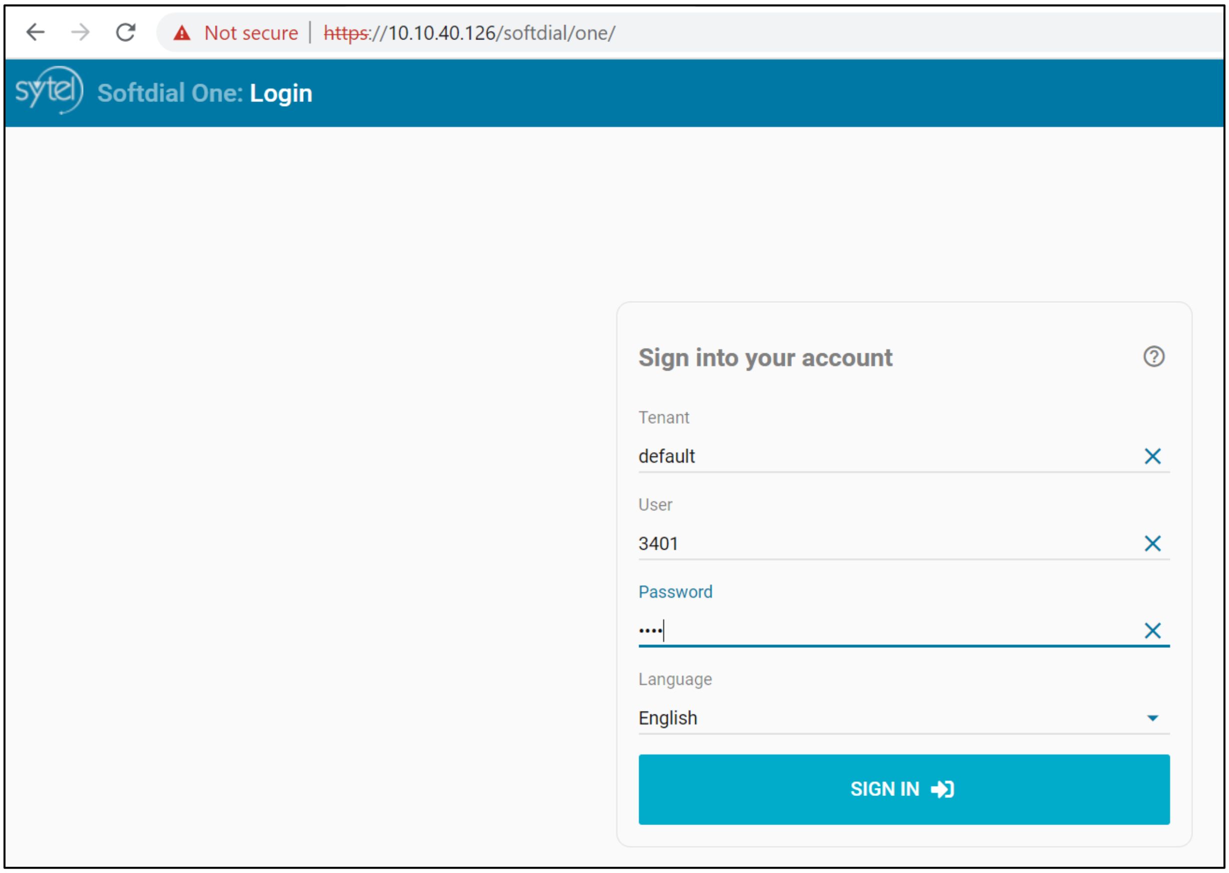


	Campaign	State	Linked	Type	Agents	Completion est.	List size	Calls made	List rem.	Retries/C...	Cache
1	Mobiles_85	Stopped		Predictive	0	100%	2	40	0	0	0

Notifications

Time	Level	Message
Tue Oct 04 2022 20:59:37 GMT+0100 (Irish Standard Time)	Notification	Campaign Mobiles_85. The database worker thread exiting
Tue Oct 04 2022 20:59:37 GMT+0100 (Irish Standard Time)	Notification	Campaign Mobiles_85. Database worker thread closed

From a client PC, open a web browser to the SCC as shown, and enter the desired Agent ID (**User**) and **Password**. Ensure that **Tenant** is set to **default**, as shown below.



Not secure | ~~https~~://10.10.40.126/softdial/one/

Softdial One: Login

Sign into your account

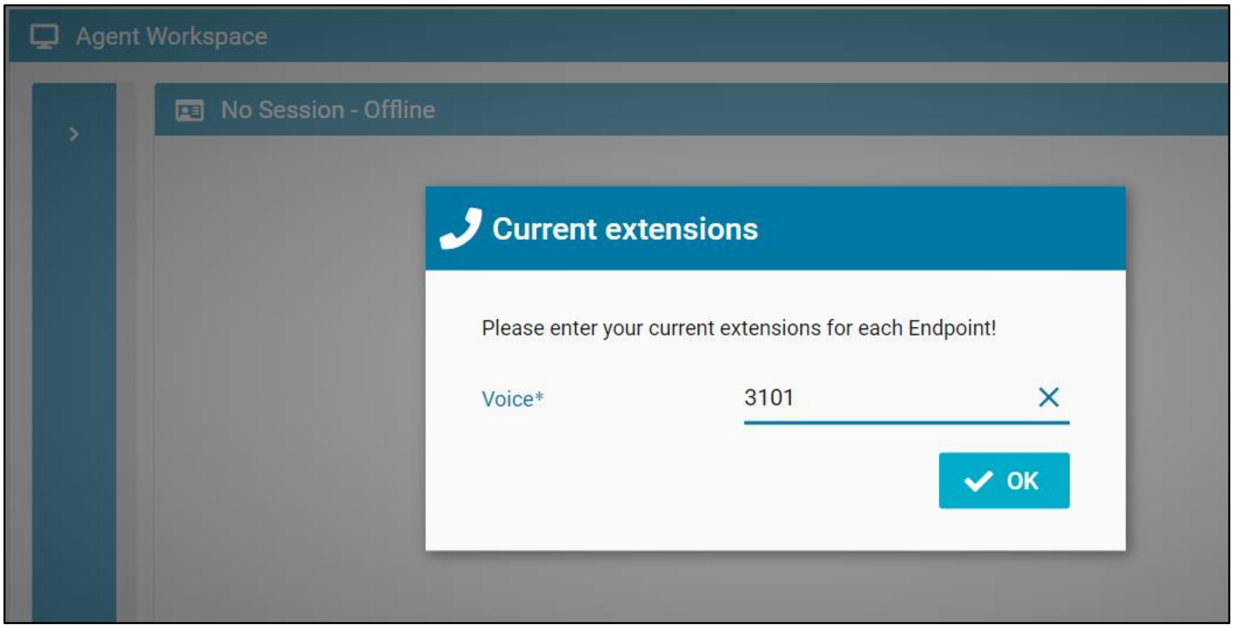
Tenant: default

User
3401

Password: ••••

Language: English

Enter the Avaya extension to be used and click on **OK**.

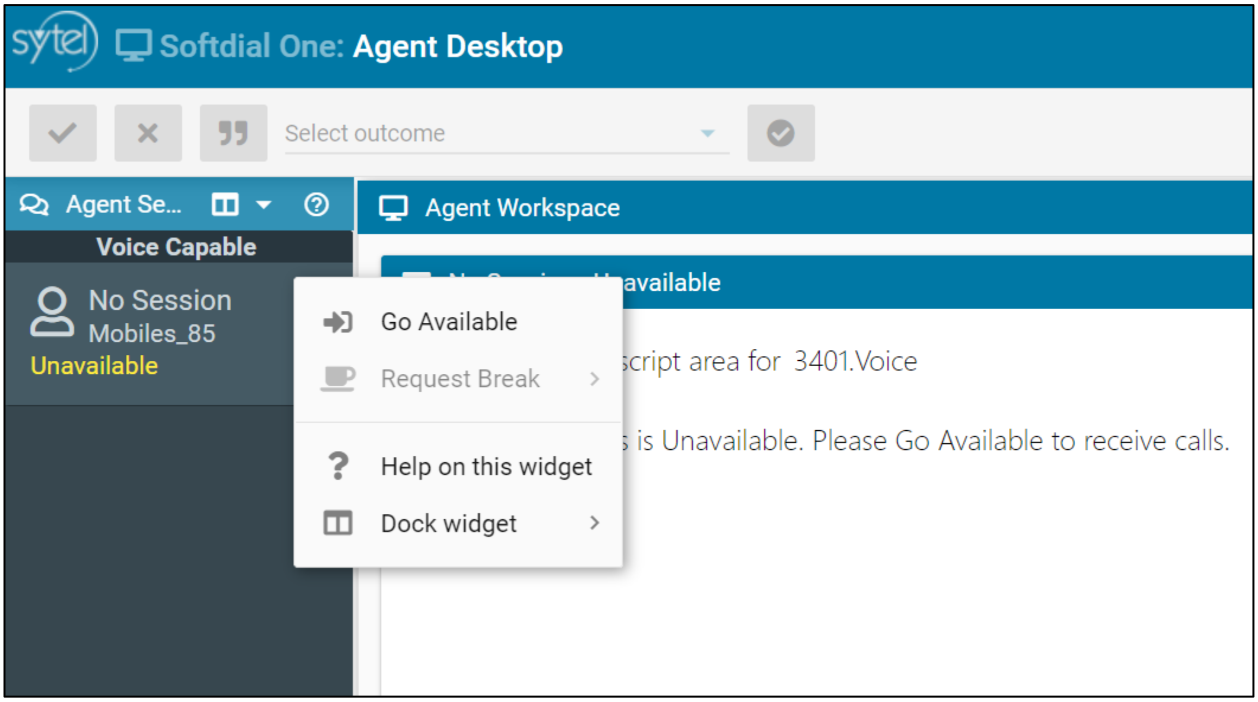


Current extensions

Please enter your current extensions for each Endpoint!

Voice*: 3101

Once logged in, the agent can **Go Available** by right-clicking on the left window area, as shown.



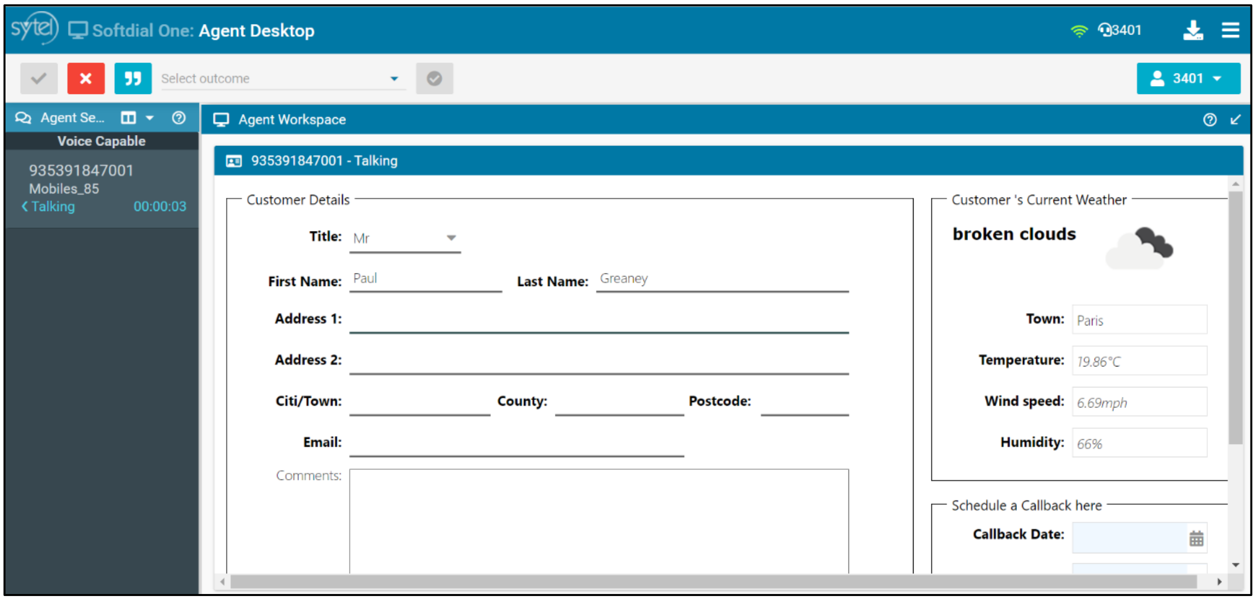
No Session
Mobiles_85
Unavailable

...available

...script area for 3401.Voice

...s is Unavailable. Please Go Available to receive calls.

Once the call is answered (and this is done automatically), a screen pop like the one below should be populated on the agent's screen.



935391847001
Mobiles_85
Talking 00:00:03

935391847001 - Talking

Title: Mr

First Name: Paul Last Name: Greaney

Address 1:

Address 2:

Citi/Town: County: Postcode:

Email:

Comments:

broken clouds

Town: Paris

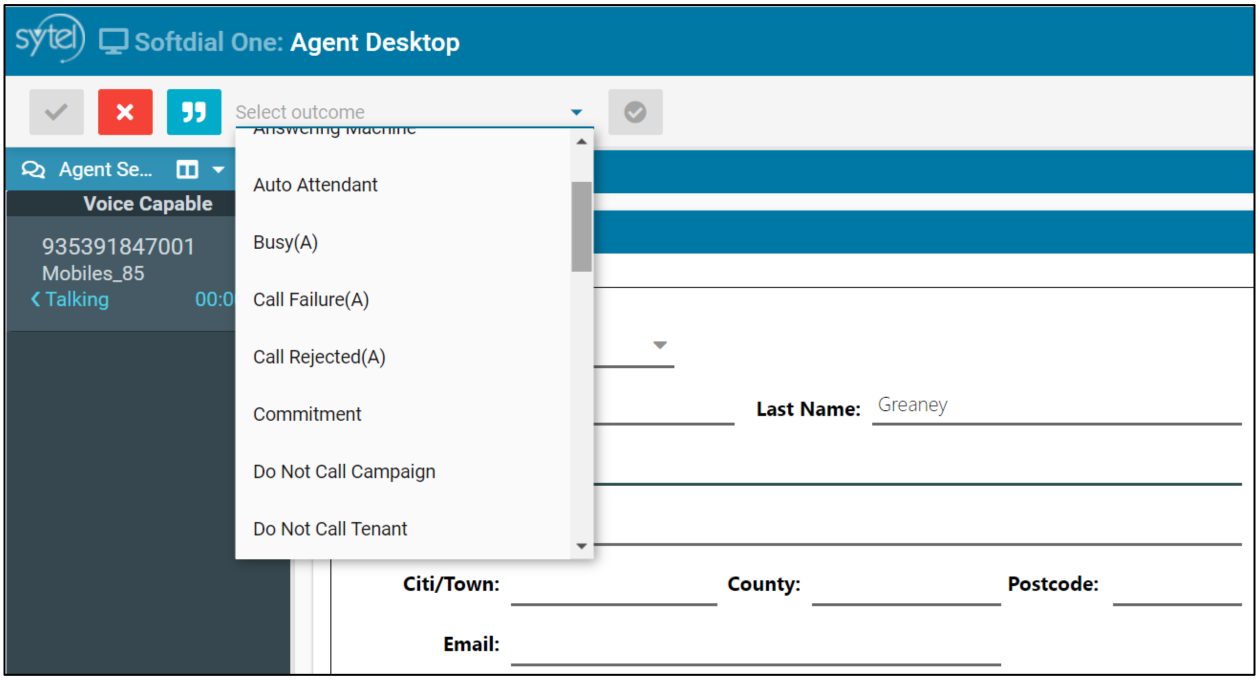
Temperature: 19.86°C

Wind speed: 6.69mph

Humidity: 66%

Callback Date:

Once the agent is finished with the caller, the agent can choose the outcome as shown below.



935391847001
Mobiles_85
Talking 00:0

Last Name: Greaney

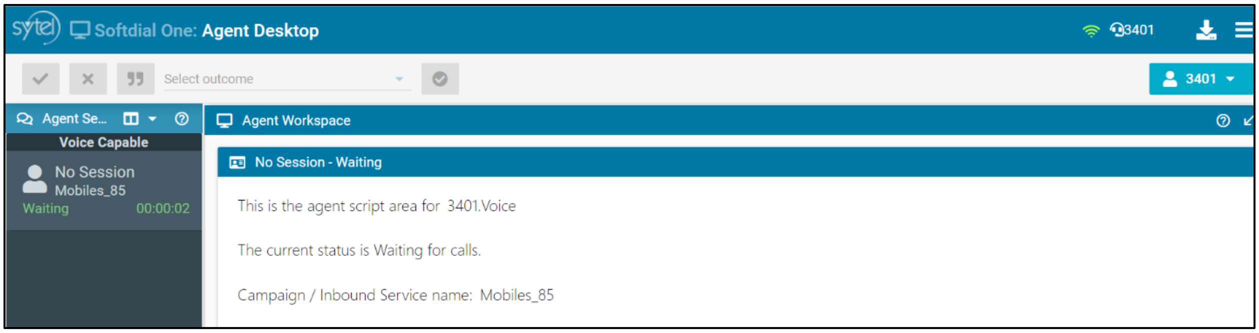
Citi/Town:

County:

Postcode:

Email:

Once the call is complete, the agent is waiting for the next outbound or inbound call to arrive.



No Session
Mobiles_85
Waiting 00:00:02

No Session - Waiting

This is the agent script area for 3401.Voice

The current status is Waiting for calls.

Campaign / Inbound Service name: Mobiles_85

9. Conclusion

These Application Notes describe the configuration steps required to integrate Sytel Softdial Contact Center v11.1 with Avaya Aura® Application Enablement Services R10.1 and Avaya Aura® Communication Manager R10.1. All feature and serviceability test cases were completed successfully, with all observations listed in **Section 2.2**.

10. Additional References

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

Documentation for Avaya products may be obtained via http://support.avaya.com.

[1] *Administering Avaya Aura® Communication Manager*, Release 10.1, Issue 1, December 2021.

[2] *Administering Avaya Aura® Application Enablement Services,* Release 10.1.x, Issue 4, April 2022.

Documentation related to Softdial Contact Center may be obtained directly from Sytel or via Sytel Help Web Portal *(*https://help.sytel.com/*)*

[3] *Softdial Contact Center Documentation,* Release 11.1.745+, Issue 15, August, 2022.

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.