



DevConnect Program

Application Notes for OpenText Qfiniti 22.4 with Avaya Proactive Outreach Manager 4.0.2 and Avaya Aura® Application Enablement Services 10.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for OpenText Qfiniti 22.4 to interoperate with Avaya Proactive Outreach Manager 4.0.2 and Avaya Aura® Application Enablement Services 10.1 using Service Observing to records calls.

OpenText Qfiniti connected to the Avaya solution to allow recording of outbound calls generated by Avaya Proactive Outreach Manager and used the Service Observing feature via the Avaya Aura® Application Enablement Services Device, Media, and Call Control interface to capture media associated with the monitored agent stations for call recording.

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 for OpenText Qfiniti 22.4 to interoperate with Avaya Proactive Outreach Manager 4.0.2 and Avaya Aura® Application Enablement Services 10.1 using Service Observing to records calls.

The primary focus of these Application Notes is the connection to Proactive Outreach Manager (POM) in order to record outbound campaign calls from agent phones. OpenText Qfiniti made use of the Call Recorder Application Programming Interface (API) on POM and used the Service Observing feature via the Application Enablement Services Device, Media, and Call Control (DMCC) interface to capture media associated with the monitored agent stations for call recording.

A number of blended calls were also recorded that being a mixture of both outbound calls using POM and inbound calls to a VDN. To facilitate the recording of both the outbound and inbound calls, a separate connection to Application Enablement Services was established. Qfiniti used the Telephony Services Application Programming Interface (TSAPI) from Application Enablement Services to monitor skill groups and agent stations on Communication Manager, along with the Service Observing feature via the Application Enablement Services (DMCC) for call recording of inbound calls.

DMCC works by allowing software vendors to create soft phones, in memory on a recording server, and use them to monitor and record other phones. This is purely a software solution and does not require telephony boards or any wiring beyond a typical network infrastructure. The DMCC API associated with Application Enablement Services monitors the digital and VoIP stations or extensions. The application uses the DMCC service to register itself as a recording device at the target extension. When the target extension joins a call, the application automatically receives the call's aggregated RTP media stream via the recording device by using Service Observing and records the call.

Note: The primary focus of these Application Notes is the connection to the POM recording API for recording of outbound calls. Although a connection to TSAPI was made to allow for blended calls, this connection has previously been certified and the resulting Application Notes are titled *Application Notes for OpenText Qfiniti 20.4 with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 Using Service Observing*.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of Qfiniti, the application automatically performed device queries and requested monitoring of POM agents using the POM Call Recorder API. Qfiniti also registered the virtual IP softphones using DMCC.

For the manual part of the testing, each call was handled manually using the POM Agent Desktop application for user actions such as hold, resume, transfer and conference.

When there was an active call at a monitored agent station, Qfiniti was informed of the call either by reports from POM via the Call Recorder API during an outbound call or by event reports from the TSAPI interface only for an inbound call as part of a blended call. It started call recording using Service Observing via the DMCC interface to add a virtual IP softphone to the active call and obtain the media. The event reports were also used to determine when to stop the call recordings.

The primary focus of the compliance testing was on the recording of outbound calls using POM to generate calls from a list associated with a campaign. Both Preview and Progressive campaigns were used during testing. Some blended calls were made using the POM agent desktop to transfer callers to incoming VDN's. All calls were expected to be recorded.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to Qfiniti.

The verification of tests included use of Application Enablement Services and Qfiniti logs for proper message exchanges and use of Qfiniti's web interface (Qfiniti Web Access) for proper logging and playback of calls.

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 Application Enablement Services and Qfiniti did not include use of any specific encryption features as requested by OpenText.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing focused on verifying the following on Qfiniti.

- **Handling of POM messaging** in areas of event notification and value queries.
- **Use of DMCC services** to register virtual IP softphones, and to activate Service Observing via button press to obtain the media for call recording.
- **Outbound calls in a Preview Campaign** – Test call recording for outbound calls in a preview campaign created on POM made to PSTN endpoints over a SIP trunk.
- **Outbound calls in a Progressive Campaign** - Test call recording for outbound calls in a progressive campaign created on POM made to both QSIG and SIP PSTN endpoints.
- **Hold/Transferred/Conference calls** – Test call recording of outbound calls in a preview campaign on hold, transferred and conferenced.
- **Blended calls** – The recording of both inbound and outbound calls together using an agent associated with “outbound” and another associated with “inbound”.
- **Serviceability testing** - The behaviour of Qfiniti under different simulated failure conditions.

The serviceability testing focused on verifying the ability of Qfiniti to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to Qfiniti.

2.2. Test Results

All test cases were executed. The following observations were noted on POM from the compliance testing.

1. There was a known issue with POM 4.0.2 running a Progressive Campaign where there is one-way audio and the customer can hear the agent, but the agent cannot hear the customer; this is reflected in the recordings as well. Avaya created a patch with a fix, and the fix was verified.
2. The POM Call Recorder API sends a Media Info message specifying the agent’s state to be “Active” instead of “Hold” (as Qfiniti thought) when a call is placed on hold. To identify whether a customer is on hold because of consult or actual hold (by pressing hold button), in case of actual hold there will be two participants in the message; for the consult case, there will be three participants. This is as per design.

2.3. Support

Technical support on Qfiniti can be obtained through the following.

- **Phone:** +1 (800) 540-7292
- **Web:** <https://www.opentext.com/contact>

3. Reference Configuration

The configuration in **Figure 1** was used to compliance test Qfiniti with POM, Communication Manager and Application Enablement Services.

During compliance testing, Qfiniti monitored the skill groups and agent stations shown in the table below.

Device Type	Extension
VDN	3900, 3901
Skill Group	81, 82
Supervisor	3172
Agent Station	3101 (SIP), 3001 (H.323), 3063 (Digital), 3111 (Avaya Agent for Desktop)
Agent ID	3401, 3402, 3403
Virtual DMCC Stations	18901, 18902, 18903, 18904

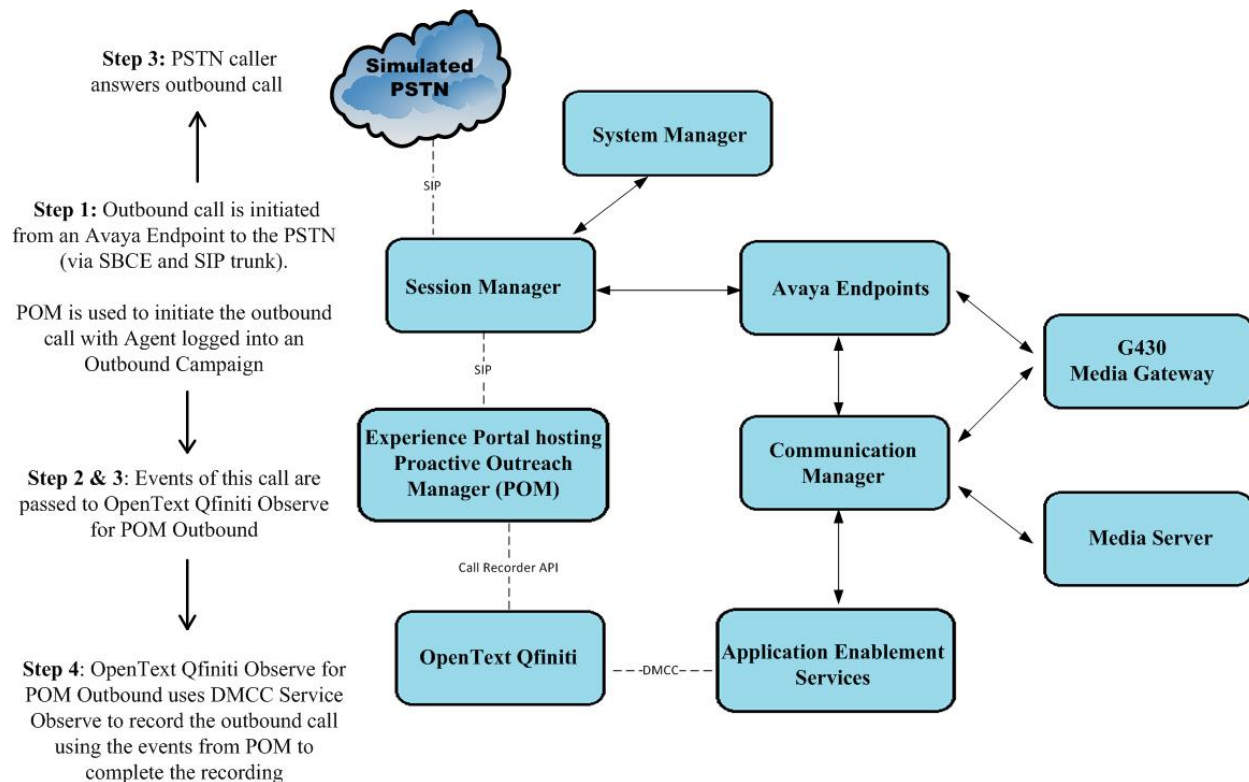


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Avaya Equipment/Software	Release/Version
Avaya Aura® Experience Portal used to host POM Avaya Proactive Outreach Manager -EPM (Experience Portal Manager) -MPP (Media Processing Platform)	R8.1.2 R4.0.2 R8.1.2.0.0347 R8.1.2.0.0346
Avaya Aura® Application Enablement Services	10.1.0 Build 10.1.0.2.0.12-0
Avaya Aura® Session Manager	Session Manager R10.1 Build No. – 10.1.0.2.1010219
Avaya Aura® Communication Manager	R10.1.0 – FP2 R018x.00.0.890.0 Update ID 01.0.890.0-26095
Avaya Aura® System Manager	System Manager 10.1.0.2 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.0.2.0715160 Service Pack 2
Avaya Aura® Media Server	10.1.0.101
Avaya Media Gateway G430	42.7.0 /2
Avaya 9404 Digital	17.0
Avaya J100 Series (SIP)	7.1.2.0.14
Avaya J100 Series (H323)	7.0.14.0.7
Avaya Agent for Desktop (SIP)	2.0.6.23.3005
Avaya Session Border Controller for Enterprise (to facilitate simulated PSTN)	10.1.0
OpenText Equipment/Software	Release/Version
OpenText Qfiniti running on Windows 2019 server with MS SQL 2019	22.4.0
• Avaya TSAPI Windows Client (csta32.dll)	10.1.0
• Avaya DMCC XML	10.1.0

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify license
- Administer CTI link
- Administer IP codec set
- Administer system parameters features
- Administer class of restriction
- Administer agent stations (H.323)
- Administer virtual IP softphones
- Administer agent stations (SIP)

5.1. Verify License

Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the **display system-parameters customer-options** command to verify that the **Computer Telephony Adjunct Links** customer option is set to **y** on **Page 4**. If this option is not set to **y**, then contact the Avaya sales team or business partner for a proper license file.

display system-parameters customer-options		Page	4 of 12
OPTIONAL FEATURES			
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y
Access Security Gateway (ASG)?	n	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?	n	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		
Async. Transfer Mode (ATM) Trunking?	n	Digital Loss Plan Modification?	y
ATM WAN Spare Processor?	n	DS1 MSP?	y

Navigate to **Page 7** and verify that the **Service Observing (Basic)** customer option is set to **y**.

display system-parameters customer-options		Page	7 of 12
CALL CENTER OPTIONAL FEATURES			
Call Center Release: 7.0			
ACD?	y	Reason Codes?	y
BCMS (Basic)?	y	Service Level Maximizer?	n
BCMS/VuStats Service Level?	y	Service Observing (Basic)?	y
BSR Local Treatment for IP & ISDN?	y	Service Observing (Remote/By FAC)?	y
Business Advocate?	n	Service Observing (VDNs)?	y
Call Work Codes?	y	Timed ACW?	y
DTMF Feedback Signals For VRU?	y	Vectoring (Basic)?	y
Dynamic Advocate?	n	Vectoring (Prompting)?	y

5.2. Administer CTI Link

Add a CTI link using the **add cti-link n** command, where “n” is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. 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		COR: 1	
Name: aes81xvmpg			

5.3. Administer IP Codec Set

Use the **change ip-codec-set n** command, where “n” is an existing codec set number used for integration with Qfiniti.

For customer network that use encrypted media, make certain that **none** is included for **Media Encryption**, and that **Encrypted SRTP** is set to **best-effort**, these settings are needed for support of non-encrypted media from the virtual IP softphones used by Qfiniti.

In the compliance testing, this IP codec set was assigned to the virtual IP softphones used by Qfiniti.

change ip-codec-set 1		Page 1 of 2	
		IP Codec Set	
Codec Set: 1			
Audio	Silence	Frames	Packet
Codec	Suppression	Per Pkt	Size (ms)
1: G.711A	n	2	20
2: G.711MU			
3: G.729			
4:			
5:			
6:			
7:			
Media Encryption		Encrypted SRTP: best-effort	
1: 1-srtp-aescm128-hmac80			
2: none			
3:			
4:			
5:			

5.4. Administer System Parameters Features

Use the **change system-parameters features** command and navigate to **Page 11**. Set **Service Observing: Warning Tone** to the needed setting per customer requirement, and enable **Allow Two Observers in Same Call**, as shown below.

```
change system-parameters features                                     Page 11 of 19
                                FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
  EAS
    Expert Agent Selection (EAS) Enabled? y
    Minimum Agent-LoginID Password Length:
    Direct Agent Announcement Extension:          Delay:
    Message Waiting Lamp Indicates Status For: station
    Work Mode On Login: aux
  VECTORING
    Converse First Data Delay: 0          Second Data Delay: 2
    Converse Signaling Tone(msec): 100      Pause (msec): 70
    Prompting Timeout(secs): 10
    Interflow-qpos EWT Threshod: 2
    Reverse Star/Pound Digit For Collect Step? n
    Available Agent Adjustments for BSR? n
    BSR Tie Strategy: 1st-found
    Store VDN Name in Station's Local Call Log? n
  SERVICE OBSERVING
    Service Observing: Warning Tone? n      or Conference Tone? n
    Allowed with Exclusion: Service Observing? n      SSC? n
    Allow Two Observers in Same Call? y
```

5.5. Administer Class of Restriction

Enter the **change cor n** command, where “n” is the class of restriction (COR) number used for integration with Qfiniti. Set the **Can Be Service Observed** and **Can Be A Service Observer** fields to **y**, as shown below. For the compliance testing, this COR was assigned to the agent stations and virtual IP softphones.

If desired, separate COR can be used for enablement of each parameter. The COR with **Can Be Service Observed** enabled needs to be assigned to the agent stations, and the COR with **Can Be A Service Observer** enabled needs to be assigned to the virtual IP softphones.

```
change cor 2                                                         Page 1 of 23
                                CLASS OF RESTRICTION

                                COR Number: 2
                                COR Description: OpenText

                                FRL: 0          APLT? y
    Can Be Service Observed? y      Calling Party Restriction: none
    Can Be A Service Observer? y    Called Party Restriction: none
    Time of Day Chart: 1          Forced Entry of Account Codes? n
    Priority Queuing? n          Direct Agent Calling? n
    Restriction Override: none    Facility Access Trunk Test? n
    Restricted Call List? n      Can Change Coverage? n
```

5.6. Administer Agent Stations (H.323)

Use the **change station n** command, where n is the first H.323 agent station extension from **Section 3**. For **COR**, enter the COR number from **Section 5.5**.

Repeat this section to administer all agent stations from **Section 3**. In the compliance testing, one agent station was administered as shown below.

change station 1001		Page	1 of	5
STATION				
Extension: 1001	Lock Messages? n	BCC: 0		
Type: 9611	Security Code: *	TN: 1		
Port: S00102	Coverage Path 1: 1	COR: 2		
Name: CM Station 1	Coverage Path 2:	COS: 1		
	Hunt-to Station:	Tests? y		

5.7. Administer Virtual IP Softphones

Add a virtual IP softphone using the **add station n** command, where “n” is an available extension number. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Extension:** The available extension number
- **Type:** Any IP telephone type, such as **4620**
- **Name:** A descriptive name
- **Security Code:** A desired code
- **COR:** The COR number from **Section 5.5**
- **IP SoftPhone:** y

add station 18901		Page	1 of	5
STATION				
Extension: 18901	Lock Messages? n	BCC: 0		
Type: 4620	Security Code: 1234	TN: 1		
Port: IP	Coverage Path 1:	COR: 2		
Name: Qfiniti DMCC 1	Coverage Path 2:	COS: 1		
	Hunt-to Station:	Tests: y		
STATION OPTIONS				
Location:	Time of Day Lock Table:			
Loss Group: 19	Personalized Ringing Pattern: 1			
	Message Lamp Ext: 18901			
Speakerphone: 2-way	Mute Button Enabled? y			
Display Language: english	Expansion Module? n			
Survivable GK Node Name:	Media Complex Ext:			
Survivable COR: internal	IP SoftPhone? y			
Survivable Trunk Dest? y	IP Video Softphone? n			
	Short/Prefixed Registration Allowed: default			

Navigate to **Page 4** and add **serv-obsrv** to the 6th button as shown below.

add station 18901		Page 4 of 5
STATION		
SITE DATA		
Room:	Headset?	n
Jack:	Speaker?	n
Cable:	Mounting:	d
Floor:	Cord Length:	0
Building:	Set Color:	
ABBREVIATED DIALING		
List1:	List2:	List3:
BUTTON ASSIGNMENTS		
1: call-appr	5:	
2: call-appr	6: serv-obsrv	
3: call-appr	7:	
4:	8:	

5.8. Administer Agent Stations (SIP)

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” set to “Avaya”. Changes of SIP phones must be carried out from System Manager by entering **http://<FQDN>/network-login**, where <FQDN> is the fully qualified domain name of System Manager or **Error! Hyperlink reference not valid. Address >/network-login**. Log in using 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.

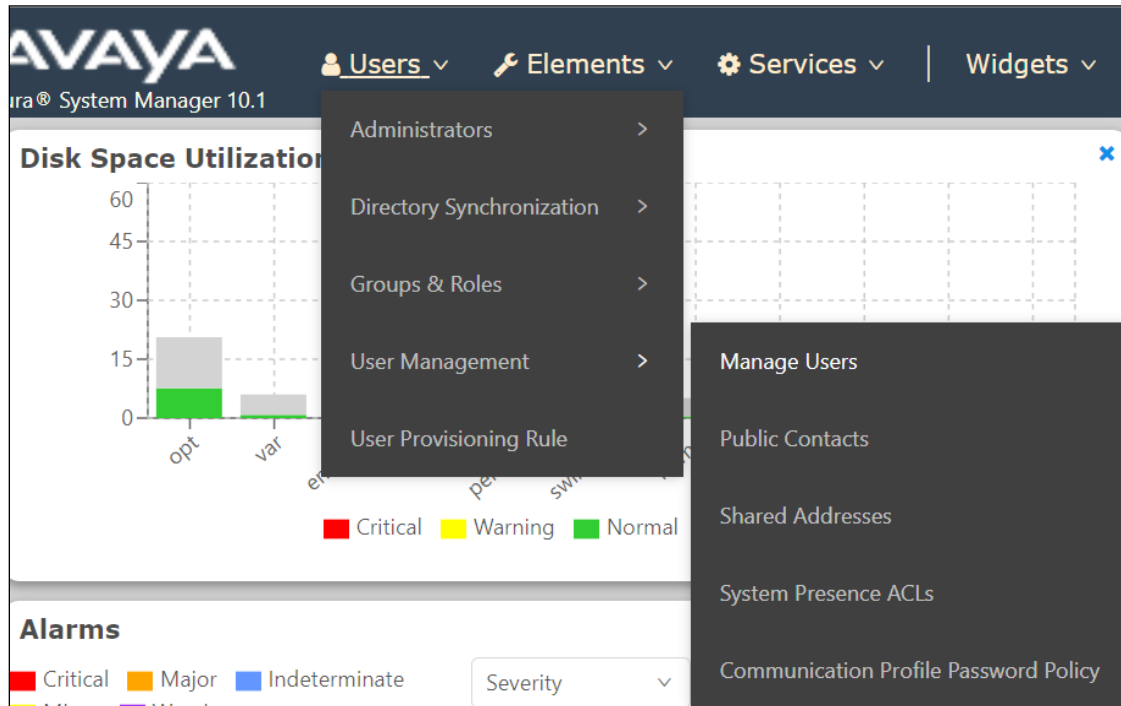
User ID:

Password:

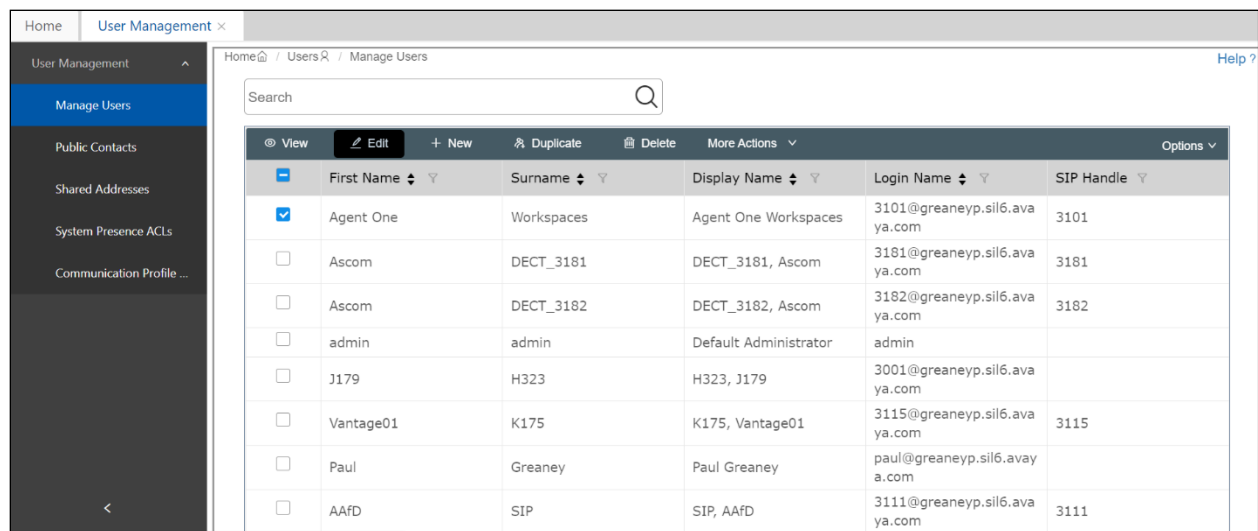
[Change Password](#)

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. Click on **Done**, at the bottom of the screen once this is set.

System cm101x

Extension 3101

Template Select

Set Type 9641SIPCC

Port S000003

Name Agent One Workspaces

Security Code

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

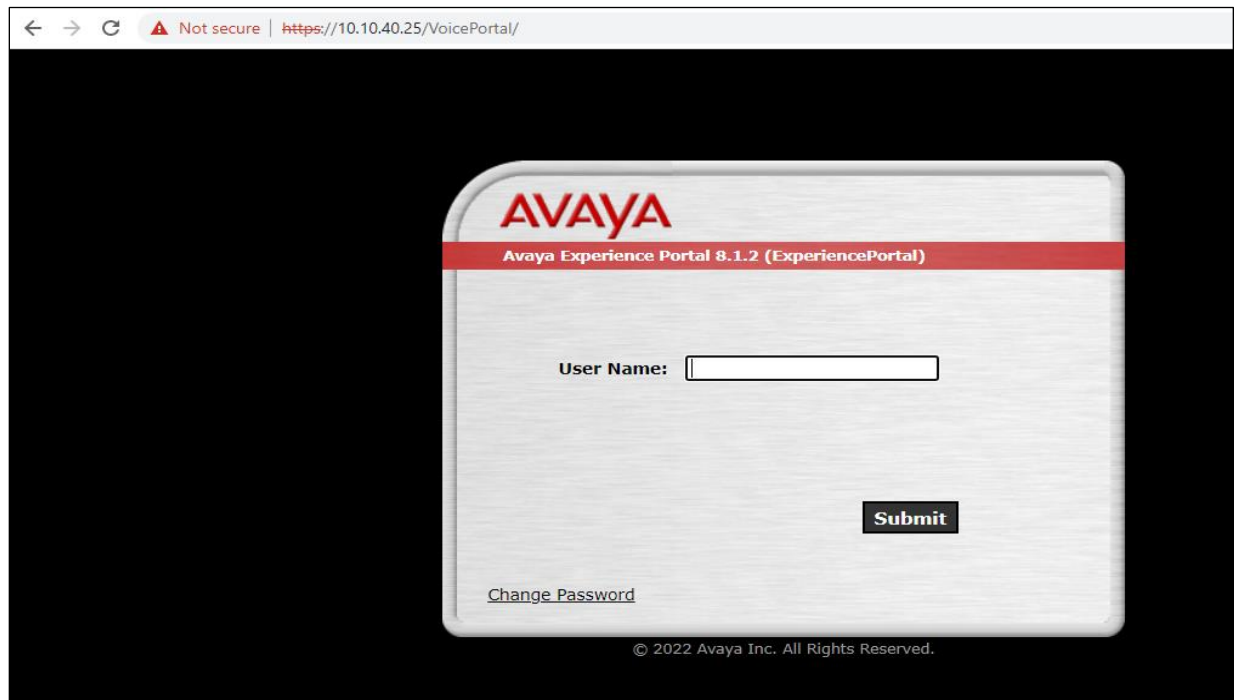
IPv6:

Click on **Commit**, on the resulting page (not shown), to save the changes.

6. Configure Avaya Aura® Experience Portal and Avaya Proactive Outreach Manager

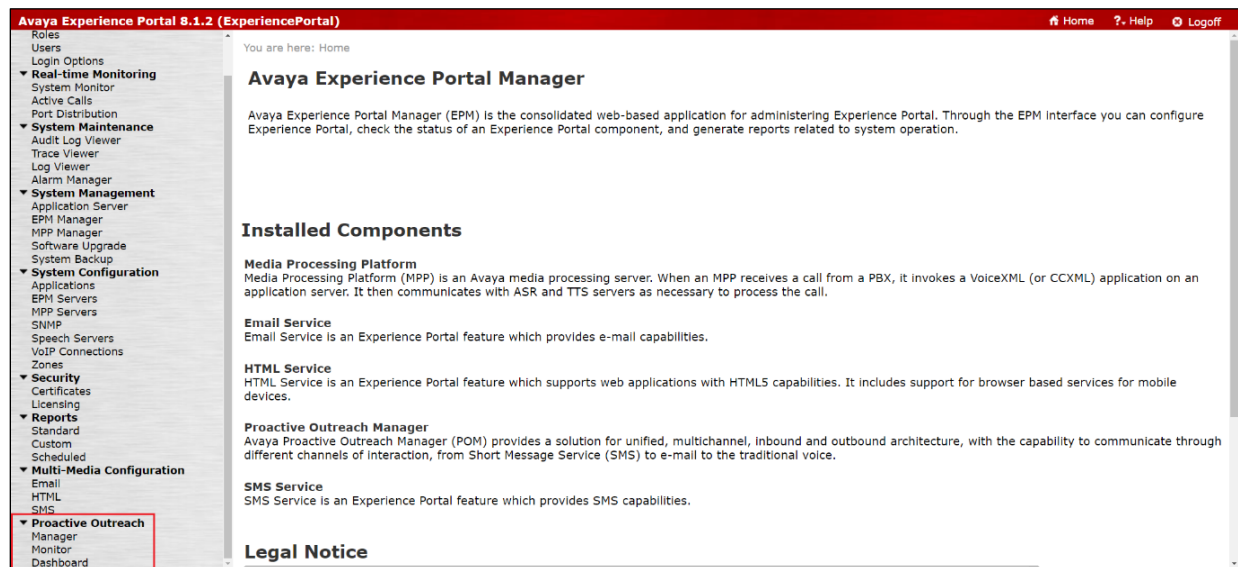
Avaya Proactive Outreach Manager is installed on top of an existing Avaya Aura® Experience Portal installation. It is assumed that both Experience Portal and POM are fully installed and configured. This section will go through the changes that are necessary to allow Qfiniti to connect and receive call events from the POM Call Recorder API.

Open a web browser and navigate to **https://<IPAddressofEP>/VoicePortal/** as shown below, enter the appropriate credentials and click on **Logon**.

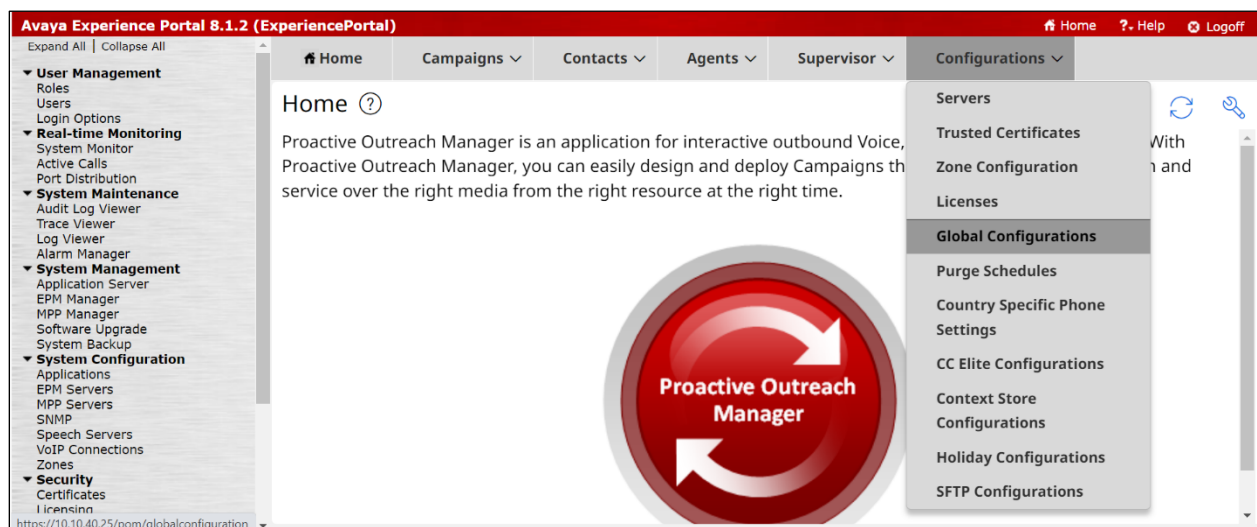


6.1. Configure Proactive Outreach Manager

Select **Proactive Outreach** → **Manager** from the bottom of the left window.



Select **Global Configurations** as shown below.



Click on the **Recorder Settings** tab and ensure that **Enable Recorder** is ticked and the default port of **7999** is selected. The **Nailup call CLID** can be set at any figure, and it was set as shown below. Click **Apply** at the bottom of the screen (not shown).

Global Configurations ?

This page displays configuration parameters. Depending on your user role, you can view or modify these configuration parameters.

<

Call Settings

Campaign Settings

Callback Settings

Pacing Settings

Contact Settings

DNC Settings

Recorder Settings

Agent Settings

Recorder Settings

☒ **Enable Recorder**

☐ **Enable Secured Connection**

Recorder port *

7999

Valid values are from 1024 through 65535.

☐ **Send MediaComplete event every time**

Select to send the MediaComplete event if busy or no answer is received for preview calls.

Agent Settings

Maximum job waiting duration(min) *

20

Valid values are from 10 through 60.

Minimum job attachment period(min) *

15

Valid values are from 1 through 480.

Nailing retry interval(sec) *

20

Valid values are from 10 through 1800.

Nailup call CLID *

98765

The sender's address to be displayed in the nail up call of an agent.

Maximum record waiting duration for attribute dialing(min) *

10

Valid values are from 10 through 60.

ANI for external consult calls

☒ **Nailup call CLID**

☐ Agent Extension

☐ Use campaign ANI

☐ Free form Text

The ANI to be used for external consult calls.

98675

☐ **Call queue**

Select to queue calls if the agent is unavailable.

☐ **Override PAI for External Consult Calls**

Select to use the value selected in the ANI for external consult calls parameter for external consult calls instead of PAI.

☐ **Enable Time Restriction for preview dial and redial**

6.2. Create a POM User for Qfiniti

A user must be created to allow Qfiniti access to web services for call events. This user will be configured during the Qfiniti setup in **Section 8.3**. Click on **Users** in the left window and **Add** in the main window.

Avaya Experience Portal 8.1.2 (ExperiencePortal)

You are here: [Home](#) > User Management > Users

Users

This page displays the list of EPM user accounts. Depending on your user role, you can add, modify, and delete user accounts. You can also configure parameters under LDAP Settings to enable the EPM to access user accounts in your corporate directory.

<input type="checkbox"/>	Name	Enable	Type	Assigned Roles/Features	Last Login	Failed Attempts	Locked	Password Longevity (days)
<input checked="" type="checkbox"/>	epadmin	Yes	EP (Password)	Administration, Auditor, Maintenance, Operations, Privacy Manager, User Manager, Web Services	27-Apr-2023 16:12:04 IST			Not enforced
<input checked="" type="checkbox"/>	init	Yes	EASG	Service Account	Never			N/A
<input type="checkbox"/>	paul	Yes	EP (Password)	Administration, Auditor, User Manager	07-Feb-2022 18:33:25 GMT			354 (System)
<input type="checkbox"/>	pom	Yes	EP (Password)	Administration, campaignmanager, contactattributesunmask, Maintenance, Operations, pomadmin, supervisor, User Manager, Web Services	17-Feb-2022 11:00:25 GMT			Not enforced

Add **Delete** **Help**

Ensure that **Web Services** and **campaignmanager** are ticked, enter a suitable **Name** and **Password** and click on **Save**.

You are here: [Home](#) > User Management > [Users](#) > Change User

Change User

Use this page to modify a EPM user account. You can change the user role and password.

Name: opentextpom

Enable: ☒ Yes ☐ No

Roles:

<input type="checkbox"/> Administration	<input type="checkbox"/> Auditor	<input checked="" type="checkbox"/> campaignmanager
<input type="checkbox"/> contactattributesunmask	<input type="checkbox"/> Maintenance	<input type="checkbox"/> Operations
<input type="checkbox"/> pomadmin	<input type="checkbox"/> Privacy Manager	<input type="checkbox"/> Reporting
<input type="checkbox"/> supervisor	<input type="checkbox"/> User Manager	<input checked="" type="checkbox"/> Web Services

Created: 14/03/23 17:24

Password:

Verify Password:

Enforce Password Longevity: ☐

Save **Apply** **Cancel** **Help**

6.3. Starting the Outbound Campaign

Before any outbound calls can be made, the outbound campaign (configured in the **Appendix**) must be started. Open **Campaign Manager** as shown below.



All campaigns that are configured are shown. To start a campaign, click on the play icon highlighted below.

A screenshot of the 'Campaign Manager' page. It features a 'New Campaign' button, a search bar, and a table of campaigns. The table has columns for Name, Contact List - Filter Template, Type, Campaign Strategy, Last Executed, and Waiting ...

Campaign Manager ⓘ					
This page displays Campaigns and actions associated with Campaigns depending on your user role.					
<div>New Campaign</div> <div>Search Campaign</div>					
Name	Contact List - Filter Template	Type	Campaign Strategy	Last Executed	Waiting ...
<div>Preview</div>	OnetoPSTN - None	Finite	Preview	09/03/2023 10:30:09	0
<div>Progressive</div>	OnetoPSTN - None	Finite	Progressive	09/03/2023 10:31:09	0

Select the appropriate campaign to run, right click on the three dots to the left of the campaign in question and select **Run Now**.

HomeCampaignsContactsAgentsSupervisorConfigurations

Campaign Manager ?

This page displays Campaigns and actions associated with Campaigns depending on your user role.

New Campaign

Search Campaign

⋮

Edit

Run Now

Schedule

Campaign Summary

Rule Association

Holiday Association

Campaign Linking

Save As

Export Files

1-2

Delete

Contact List - Filter Temp...	T...	Campaign St...	Last Executed	Wa...
OnetoPSTN - None	Fin...	Preview	09/03/2023 10:3...	0
OnetoPSTN - None	Fin...	Progressive	09/03/2023 10:3...	0

←

1

→

Show: 10

The campaign should now be displayed as **In Progress**.

Campaign Manager ?

This page displays Campaigns and actions associated with Campaigns depending on your user role.

New Campaign

Search Campaign

Name	Contact List - Filter Temp...	T...	Campaign St...	Last Executed	Wa...
<div>⋮</div> Preview	OnetoPSTN - None	Fin...	Preview	In Progress	0
<div>⋮</div> Progressive	OnetoPSTN - None	Fin...	Progressive	09/03/2023 10:3...	0

PG; Reviewed:
SPOC 6/16/2023

Solution & Interoperability Test Lab Application Notes
©2023 Avaya Inc. All Rights Reserved.

19 of 73
Qfiniti-POM402

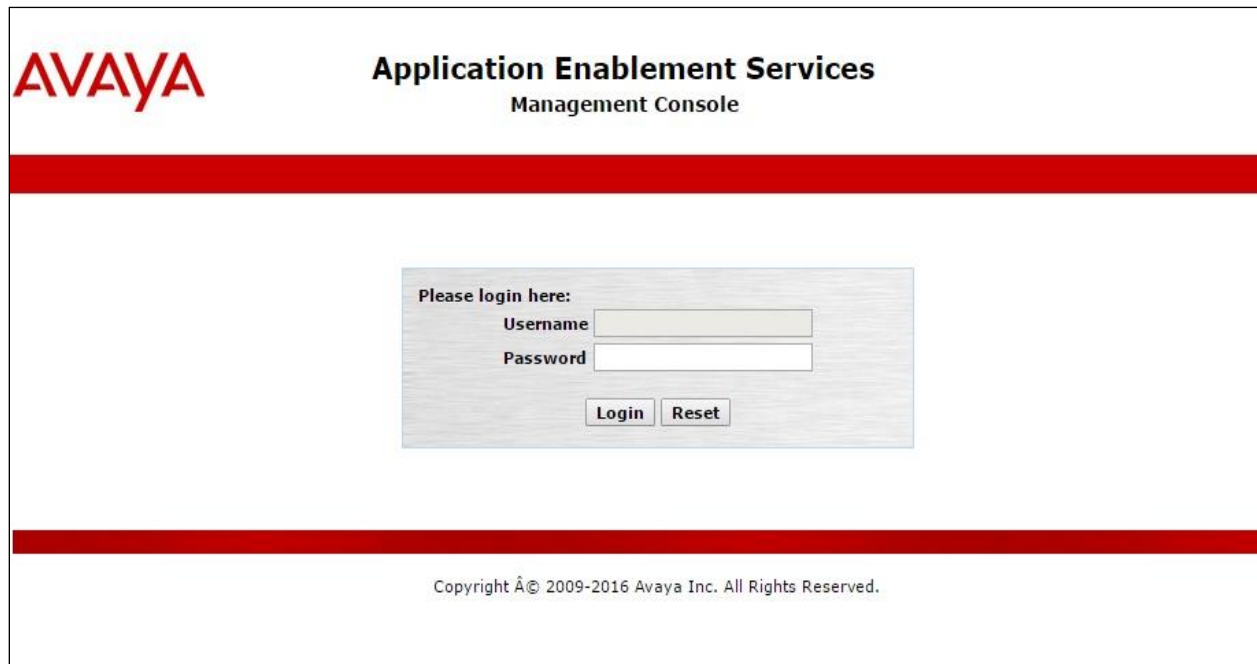
7. Configure Avaya Aura® Application Enablement Services

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 and DMCC Ports
- Create CTI User
- Administer Security
- Restart AE Services

7.1. 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 interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. Below this is a red horizontal bar. The main content area contains a login box with the text "Please login here:" followed by "Username" and "Password" labels, each with a corresponding text input field. Below the input fields are "Login" and "Reset" buttons. Another red horizontal bar is located below the login box. At the bottom of the page, the copyright notice "Copyright © 2009-2016 Avaya Inc. All Rights Reserved." is visible.

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 proper 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 main content area is titled 'AE Services' and includes 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 listing services and their status.

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, 'License Information' states: 'You are licensed to run Application Enablement (CTI) release 8.x'.

The TSAPI and DMCC licenses are user licenses issues by the Web License Manager to which the Application Enablement Services (AES) server is pointed to. The following screen shows the available licenses for both DMCC and TSAPI users.

The screenshot shows the 'Application_Enablement' section of the Web License Manager. It lists various license features with their keywords, expiration dates, and licensed capacities. Two specific licenses are highlighted with red boxes: 'Device Media and Call Control' (VALUE_AES_DMCC_DMC) and 'TSAPI Simultaneous Users' (VALUE_AES_TSAPI_USERS), both with permanent expiration dates and a capacity of 44.

Feature (License Keyword)	Expiration date	Licensed capacity
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	44
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	44
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	44
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	4
DLG VALUE_AES_DLG	permanent	44
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	44
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	4
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	44

At the bottom, there is a section for 'SmallServerTypes', 'MediumServerTypes', 'LargeServerTypes', and 'TrustedApplications' with their respective values.

7.2. 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, 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 switch connection which has already been configured from the drop-down list, in the example below this was **cm101x**.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.2** which is **1**.
- **ASAI Link Version:** This should be set to the highest version available.
- **Security:** This was 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, TSAPI Properties, TWS, and Communication Manager Interface. The main area is titled 'Edit TSAPI Links' and contains a form with the following fields: Link (1), Switch Connection (cm101x), Switch CTI Link Number (1), ASAI Link Version (12), and Security (Both). Below the form 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	cm81xvmpg	1	11	Both

7.3. Identify Tlinks

Navigate to **Security** → **Security Database** → **Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure Qfiniti in **Section 8.4**. The unsecure link (top link) was used for compliance testing.

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

7.4. Enable TSAPI and DMCC Ports

To ensure that the TSAPI and DMCC ports are enabled, navigate to **Networking → Ports**. Ensure that the ports are set to **Enabled** as shown below. The ports used in compliance testing were TSAPI port **450** and DMCC port **4721**.

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 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		<input checked="" type="radio"/>	<input type="radio"/>

7.5. Create CTI User

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

User Management | User Admin

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 Qfiniti setup in **Section 8.2** and **8.4**.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with Qfiniti setup in **Section 8.2** and **8.4**.
- **CT User** - Select **Yes** from the drop-down menu.

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

High Availability	* User Id	devconnect
► Licensing	* Common Name	devconnect
► Maintenance	* Surname	devconnect
► Networking	User Password	••••••••
► Security	Confirm Password	•••••••• 
► Status	Admin Note	
▼ User Management	Avaya Role	None ▼
► Service Admin	Business Category	
▼ User Admin	Car License	
▪ Add User	CM Home	
▪ Change User Password	Css Home	
▪ List All Users	CT User	Yes ▼
▪ Modify Default Users	Department Number	
▪ Search Users	Display Name	
► Utilities	Employee Number	
► Help	Employee Type	
	Enterprise Handle	
	Given Name	
	Home Phone	
	Home Postal Address	
	Initials	

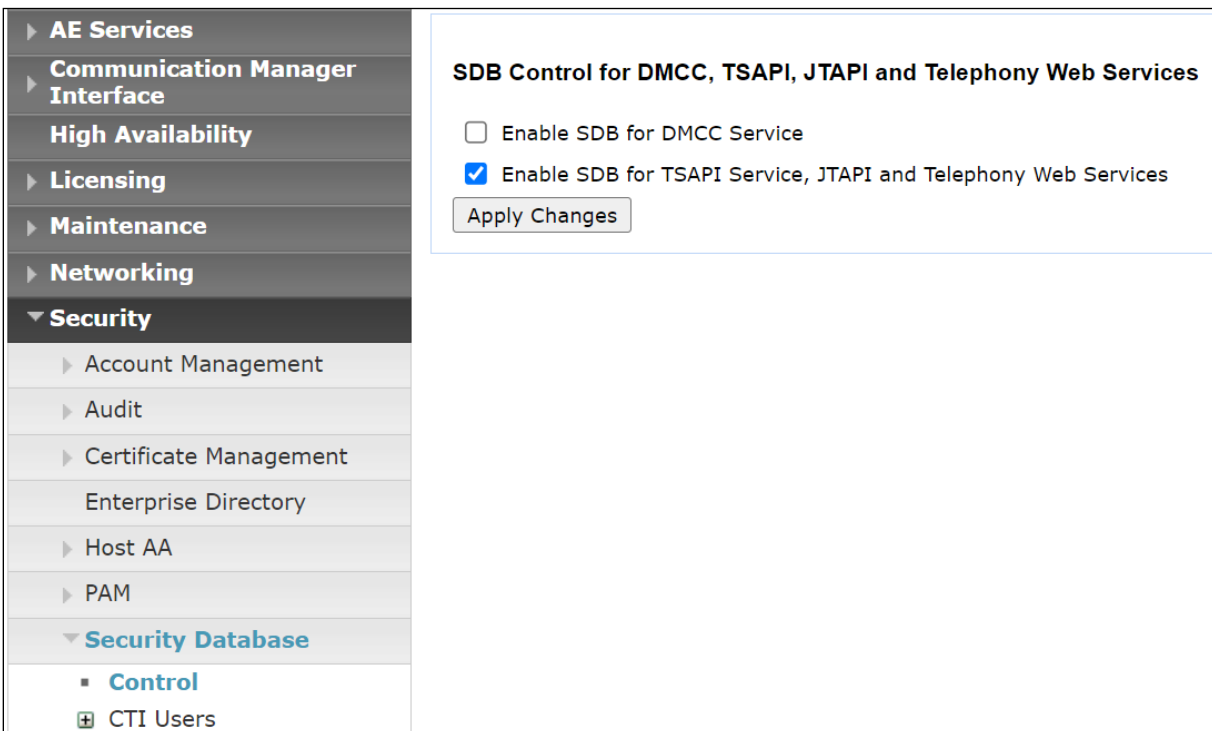
7.6. Administer Security

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

7.6.1. 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.

Note: Since the CTI user was given unrestricted access, as per **Section 7.6.2** these values set here do not impact the overall setup.



The screenshot shows a web-based configuration interface. On the left is a navigation menu with the following items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security (expanded), Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database (expanded), Control (selected), and CTI Users. The main content area 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 the checkboxes is an '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.

In the event that the security database is used by the customer with parameters already enabled, then follow reference [2] to configure access privileges for the Qfiniti user.

7.6.2. Associate Devices with CTI User

Navigate to **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the CTI user added in **Section 7.5** and click on **Edit**.

▶ 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

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

Edit

List 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**.

7.7. 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

8. Configure OpenText Qfiniti

This section provides the procedures for configuring Qfiniti. The procedures include the following areas.

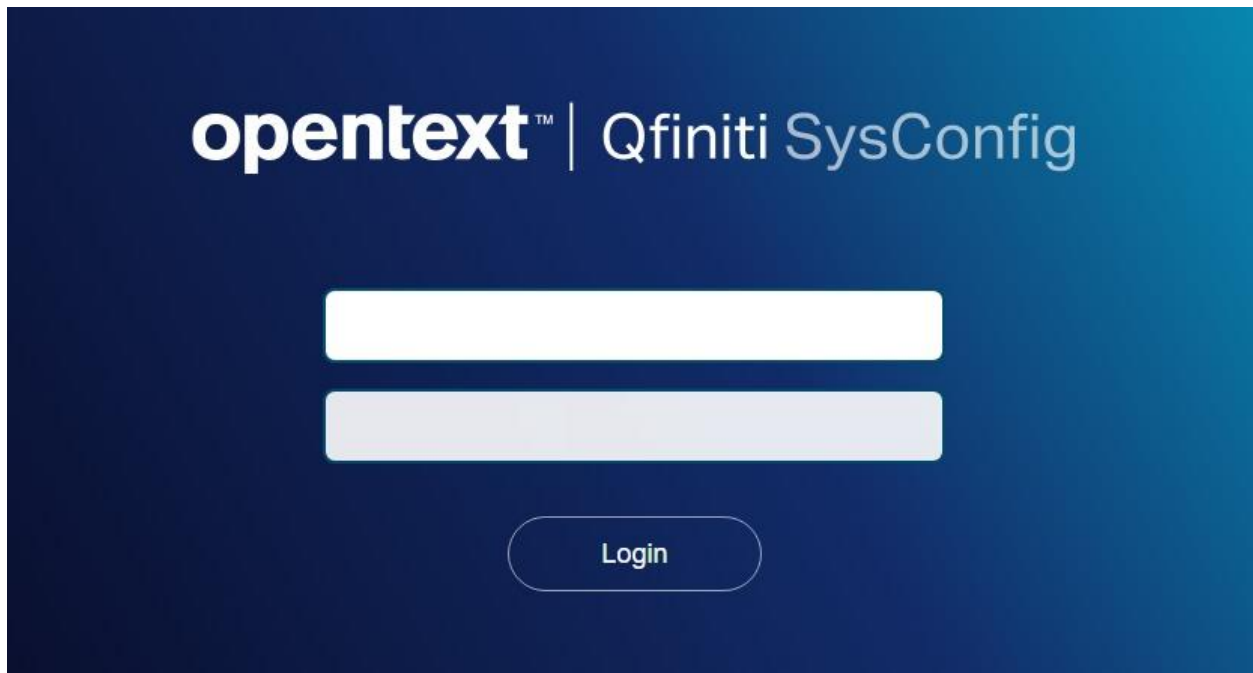
- Launch SysConfig web interface
- Administer switches
- Administer POM CTI server
- Administer AES CTI server
- Administer board configuration
- Administer general
- Administer machines
- Administer components
- Administer POM CTI sources
- Administer TSAPI CTI sources
- Administer phone interface
- Administer logging data – phone class of service
- Administer VRM
- Administer line data
- Enable use
- Launch Qfiniti web interface
- Administer observe settings
- Administer agents
- Start services

The configuration of Qfiniti is performed by OpenText field service engineers. The procedural steps are presented in these Application Notes for informational purposes.

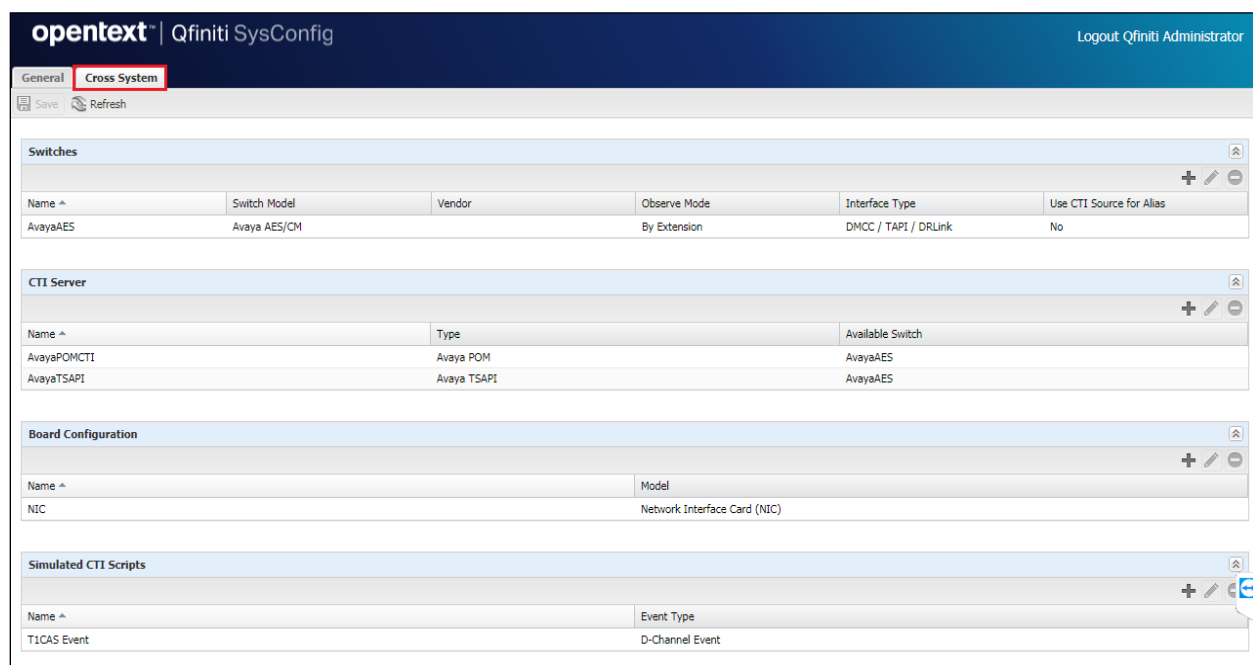
8.1. Launch SysConfig Web Interface

Access the SysConfig web interface by using the URL “http://ip-address/sysconfig” in an Internet browser window, where “ip-address” is the IP address of the Qfiniti server.

The screen below is displayed. Log in using the appropriate credentials.



In the subsequent screen, select the **Cross System** tab to display the screen below.



8.2. Administer Switches

Expand the **Switches** sub-section (shown on the previous page) and select the switch connection already configured or click the **New Item** icon to add a new entry for Application Enablement Services. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name, in this case **AvayaAES**.
- **Switch Model:** **Avaya AES/CM**.
- **Post Release Delay:** Desired wait interval in seconds for registration response (2 seconds is recommended).
- **Observe Mode:** **By Extension**.
- **Interface Type:** **DMCC / TAPI / DRLink**.
- **Avaya CM Hostname:** The relevant switch connection name from **Section 7.2**.
- **AES IP Address:** The IP address of Application Enablement Services server.
- **User Name:** The Qfiniti user credentials from **Section 7.5**.
- **Password:** The Qfiniti user credentials from **Section 7.5**.

The screenshot displays the Qfiniti SysConfig web interface. On the left, a sidebar contains navigation tabs: **General**, **Cross System**, **Switches**, **CTI Server**, **Board Configuration**, and **Simulated CTI Scripts**. The **Switches** tab is active, showing a table with one entry: **AvayaAES** with **Avaya AES/CM** as the **Switch Model**. The main area on the right is titled **Switch** and contains a form for configuring the selected switch. The form fields and their values are as follows:

Field	Value
Name	AvayaAES
Switch Model	Avaya AES/CM
Vendor	
Post Release Delay	2
Observe Mode	By Extension
Observe String	
Interface Type	DMCC / TAPI / DRLink
Use CTI Source for Alias	<input type="checkbox"/>
APC Dialer in use?	No
Avaya CM Hostname	cm101x
Port	4721
1st Line Appearance	263
AES IP Address	10.10.40.16
Service Observe Button	268
User Name	devconnect
Password	*****
AES Connection Alarm Trigger	Never
Wait Before Dial	500
Busy Repeat Max	6
Survey Excluded Extensions	Enter Value

8.3. Administer POM CTI Server

Expand the **CTI Server** sub-section and click on the configured POM CTI connection as shown below or click the **New Item** icon to add a new connection to POM. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name, in this case **AvayaPOM**.
- **Type:** **Avaya POM**.
- **Available Switch:** Select the switch name from **Section 8.2**.
- **POM IP Address:** Set this to the IP address of the POM server.
- **POM Port:** This was the default port, as per **Section 6.1**.
- **Admin User Name:** The Qfiniti user credentials from **Section 6.2**.
- **Admin Password:** The Qfiniti user credentials from **Section 6.2**.
- **Use Secure Communication:** This was left as **No**.

The screenshot shows a software interface with a sidebar on the left and a main configuration area on the right. The sidebar has tabs for 'General' and 'Cross System'. Under 'Cross System', there are sections for 'Switches', 'CTI Server', 'Board Configuration', and 'Simulated CTI Scripts'. The 'CTI Server' section is expanded, showing a list of servers: 'AvayaPOM' and 'AvayaTSAPI'. The main configuration area is titled 'CTI Server' and contains the following fields:

Name:	AvayaPOM
Type:	Avaya POM
Available Switch:	AvayaAES
Use Secure Communication?:	No
POM IP Address:	10.10.40.25
POM Port:	7999
Admin User Name:	opentextpom
Admin Password:	••••••••

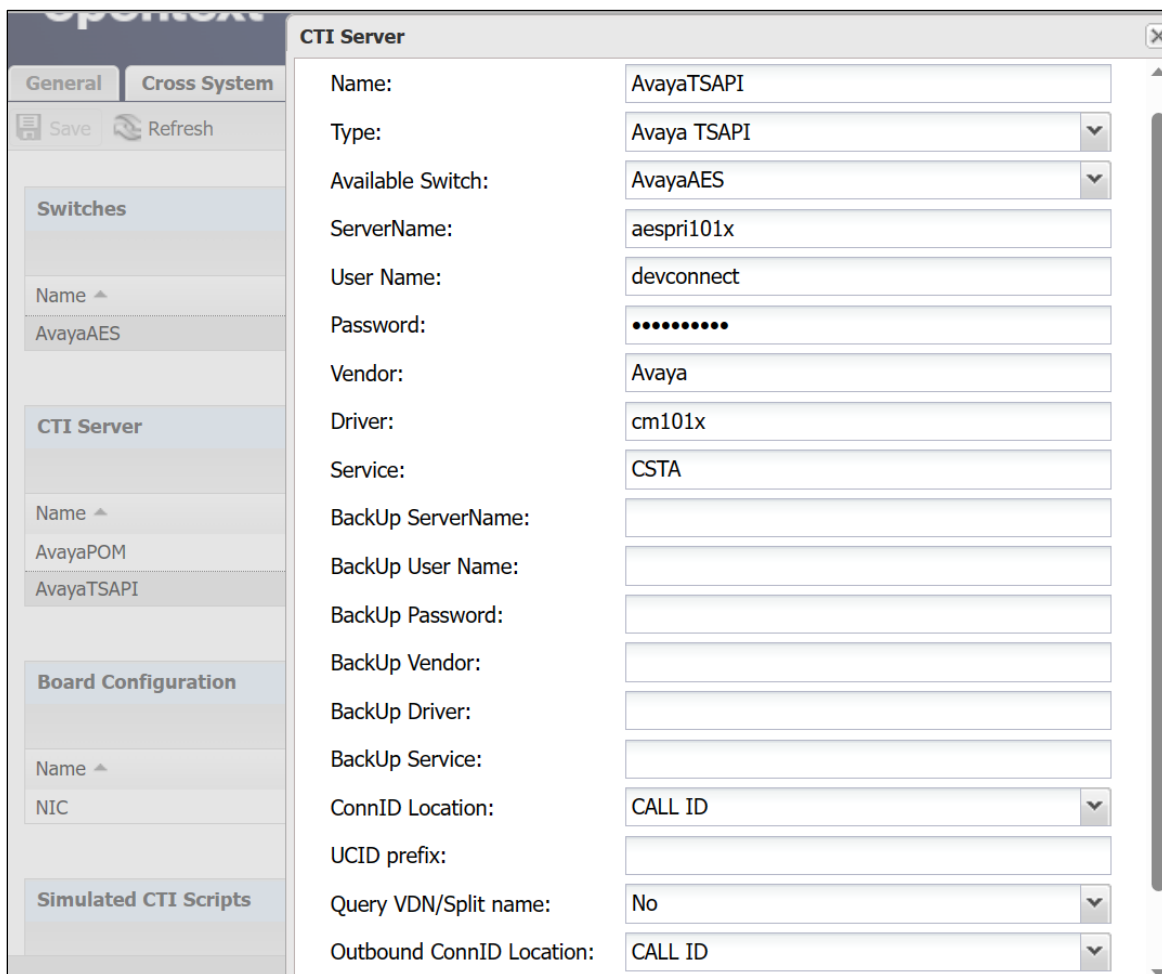
At the bottom right of the window are 'Ok' and 'Cancel' buttons.

8.4. Administer AES CTI Server

Expand the **CTI Server** sub-section and click on the configured AES CTI connection as shown below or the **New Item** icon to add a new entry for a TSAPI connection. Enter the following values for the specified fields and retain the default values for the remaining fields.

Note: The information for some of the fields below such as Vendor, Driver and Service can be obtained directly from the Tlink information in **Section 7.3**.

- **Name:** A descriptive name, in this case **AvayaTSAPI**.
- **Type:** **Avaya TSAPI**.
- **Available Switch:** Select the switch name from **Section 8.2**.
- **ServerName:** This is the name of the AES as per **Section 7.3**.
- **User Name:** The Qfiniti user credentials from **Section 7.5**.
- **Password:** The Qfiniti user credentials from **Section 7.5**.
- **Vendor:** **Avaya**.
- **Driver:** The relevant switch connection name from **Section 7.3**.
- **Service:** **CSTA**.



CTI Server

General Cross System

Save Refresh

Switches

Name ▲

AvayaAES

CTI Server

Name ▲

AvayaPOM

AvayaTSAPI

Board Configuration

Name ▲

NIC

Simulated CTI Scripts

Name: AvayaTSAPI

Type: Avaya TSAPI

Available Switch: AvayaAES

ServerName: aespri101x

User Name: devconnect

Password:

Vendor: Avaya

Driver: cm101x

Service: CSTA

BackUp ServerName:

BackUp User Name:

BackUp Password:

BackUp Vendor:

BackUp Driver:

BackUp Service:

ConnID Location: CALL ID

UCID prefix:

Query VDN/Split name: No

Outbound ConnID Location: CALL ID

8.5. Administer Board Configuration

Expand the **Board Configuration** sub-section and select the NIC configured (as shown below) or click the **New Item** icon. Note that board is not used in the integration but required to be configured. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name, in this case **NIC**.
- **Model** **Network Interface Card (NIC)**.

The screenshot displays the 'opentext | Qfiniti SysConfig' application. The left sidebar contains a navigation menu with sections: 'General' (with 'Save' and 'Refresh' buttons), 'Cross System', 'Switches' (containing a table with 'AvayaAES' and 'Avaya AES/CM'), 'CTI Server' (containing a table with 'AvayaPOMCTI' and 'AvayaTSAPI'), 'Board Configuration' (highlighted), and 'Simulated CTI Scripts'. The 'Board Configuration' section is expanded, showing a table with one entry: 'NIC'. The right pane, titled 'Board Configuration', shows the configuration details for the selected 'NIC' item. The fields are: Name (NIC), Model (Network Interface Card (NIC)), Active 1 (False), Network Card Identifier 1, Network Card Description 1, Network Card IP Address 1, Network Card Port 1 (5060), Active 2 (False), Network Card Identifier 2, Network Card Description 2, Network Card IP Address 2, Network Card Port 2 (5060), Active 3 (False), Network Card Identifier 3, Network Card Description 3, Network Card IP Address 3, Network Card Port 3 (5060), Active 4 (False), Network Card Identifier 4, Network Card Description 4, and Network Card IP Address 4.

Name	Switch Model
AvayaAES	Avaya AES/CM

Name
AvayaPOMCTI
AvayaTSAPI

Name
NIC

Name

Name

Name

8.6. Administer General

Select the **General** tab. Expand the **General** sub-section and select the configured connection or click the **New** icon to add a new system. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A desired name, in this case **POM Certification**.
- **Switch:** Select the switch name from **Section 8.2**.
- **System Type:** Check **Voice Recording – Logging**.

The screenshot shows the OpenText Qfiniti SysConfig CE 22.4 interface. The top navigation bar includes the OpenText logo and the text "Qfiniti SysConfig CE 22.4". Below this, there are tabs for "General" and "Cross System". The "General" tab is active, and the "Systems" section is expanded, showing a list of systems: "POM Certification" and "QFINITIWIN2019". The "POM Certification" system is selected, and its configuration details are displayed in the main area.

General

Name: POM Certification

Switch: AvayaAES

System Type:

- ☒ Voice Recording - Logging
- ☐ Voice Recording - QA
- ☐ Screen Recording
- ☐ Remote Screen Site
- ☐ Explore
- ☐ Survey
- ☐ Backup
- ☐ Cloud Connector

Description:

☒ Available for Use ?

☐ NAT Environment

Machines

Server Name	IP Address	Role
QFINITIWIN2019	10.10.40.120	Master

8.7. Administer Machines

Expand the **Machines** sub-section (see bottom of previous page) and click the **New Item** icon to add a new machine. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Server Name:** The host name of the Qfiniti server.
- **IP Address:** The IP address of the Qfiniti server.
- **Role:** **Master.**

The screenshot shows a software interface with a sidebar on the left containing sections: 'Available for Use' (with a checked checkbox), 'NAT Environment' (with an unchecked checkbox), 'Machines' (highlighted), 'Components', and 'CTI Sources'. The 'Machines' section contains a table with one entry: 'QFINITIWIN2019'. A modal dialog box titled 'Machine - Master Startup Machine' is open in the foreground. It contains the following fields: 'Server Name' with the value 'QFINITIWIN2019', 'IP Address' with the value '10.10.40.120' (displayed in four separate input boxes), 'Role' with a dropdown menu showing 'Master', and 'State' with a dropdown menu showing 'Down'. At the bottom of the dialog are 'Ok' and 'Cancel' buttons.

8.8. Administer Components

Expand the **Components** sub-section and follow reference [5] to assign and configure the required components. Under **Assigned Components**, select **Logger Voice Recording Manager**. Under **Component Data**, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Optimal Recording CODEC:** **PCM G.711.**
- **PCM Acquisition:** **Service Observe.**
- **Start Recording On:** **Call Active.**

Available Components	
<ul style="list-style-type: none">Archive ManagerAWS ConnectorCentral Messaging ServerCMS Data ReplicationCTI ManagerLive ManagerLogger Voice Recording ManagerLogger Voice Recording ProxyPeak File GeneratorPhone PlayerQfiniti File ServerQfiniti Integration HubQfiniti Training Server	

Assigned Components	
<ul style="list-style-type: none">Central Site<ul style="list-style-type: none">QFINITIWIN2019<ul style="list-style-type: none">Agent MonitorAlarm Manager ServerArchive ManagerCentral Messaging ServerCTI ManagerData Import ListenerDisk MonitorDispatcherGlobal Trigger ManagerIP Message SchedulerLogger Voice Recording Manager	

Component Data	
Post Service Observe dial string:	<input type="text"/>
Optimal Recording CODEC:	PCM G.711
Encryption type:	No encryption
CTI Late Attach Method:	ConnectionID
DN Late Attach Window In Sec:	30
PCM Acquisition:	Service Observe
Transaction Validation:	No
Transaction Validation Form:	trans_validation.xsl
Service Observe fail retry delay:	30
Start Recording On:	Call Active
CTI Init:	On Startup
Line Reset Threshold in Sec:	0
VoIP Transcoding:	NONE

8.9. Administer POM CTI Sources

Expand the **CTI Sources** sub-section. Select the applicable machine server name from **Section 0**, followed by the **Add CTI Source** icon. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **CTI Server:** Select the POM CTI server name from **Section 8.3**.
- **Zones:** This was set to **ALL**.
- **Agent Extensions:** The agent station extensions from **Section 3**.

The screenshot shows the 'CTI Sources' configuration window. On the left, a tree view under 'Machines' shows 'QFINITIWIN2019' expanded, with 'AvayaPOM' and 'AvayaTSAPI' listed. The main area is titled 'CTI Source' and contains the following fields:

- CTI Server:** A dropdown menu with 'AvayaPOM' selected.
- Zones:** A text field with 'ALL' entered.
- Udata script name:** A text field with 'CTI_UUdataScripts_POM.ini' entered.
- Agent Extensions:** A section with a dashed border containing the text 'Or Drop files here' with upload and download icons, a 'Single Export' checkbox, and a list box with the following extensions: 3001, 3063, 3101, and 3111.

At the bottom right of the 'CTI Source' window are 'Ok' and 'Cancel' buttons.

8.10. Administer TSAPI CTI Sources

Expand the **CTI Sources** sub-section. Select the applicable machine server name from **Section 0**, followed by the **Add CTI Source** icon. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **CTI Server:** Select the TSAPI CTI server name from **Section 8.4**.
- **Queue:** The skill group extensions from **Section 3**.
- **Agent Extensions:** The agent station extensions from **Section 3**.

Note: For compliance testing extensions **3063** and **3111** were monitored for incoming calls as well as outgoing POM calls and therefore only these two extensions were added below.

The screenshot displays the 'CTI Sources' configuration window. On the left, a tree view shows 'Machines' expanded, with 'QFINITIWIN2019' selected, containing 'AvayaPOM' and 'AvayaTSAPI'. Below this are sections for 'Phone Interface', 'Logging Data - Phone Class of Serv', 'VRM', and 'Line Data'. The main area shows the 'CTI Source' configuration for 'AvayaTSAPI'. Fields include: 'CTI Server' (AvayaTSAPI), 'PreInitExtensions' (Yes), 'Queue' (81-82), 'Agent Extensions' (3063, 3111), 'UUdata script name' (CTI_UUdataScripts_AVAYA_TSAPI.ini), and 'Auto Login Extensions' (empty). Each extension field has a 'Single Export' checkbox. The 'Queue' and 'Agent Extensions' fields have a dashed border and a 'Drop files here' icon. The 'Auto Login Extensions' field has a dashed border and a 'Drop files here' icon. The 'Enter Value' text is present below each extension field.

Field	Value
CTI Server	AvayaTSAPI
PreInitExtensions	Yes
Queue	81-82
Agent Extensions	3063, 3111
UUdata script name	CTI_UUdataScripts_AVAYA_TSAPI.ini
Auto Login Extensions	

8.11. Administer Phone Interface

Expand the **Phone Interface** sub-section. Select the machine server name from **Section 0**, and click on the **Edit** icon to edit the entry. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Machine Type:** **Logger.**
- **Phone Interface Type:** **DMCC Ver 7.0 & Up.**
- **Number of Lines:** The total number of agent stations from **Section 3**, in this case **4**.

The screenshot shows a configuration window titled "Phone Interface" with a close button (X) in the top right corner. The window contains the following fields and values:

Field	Value
Server Name:	QFINITIWIN2019
Machine Type:	Logger
Phone Interface Type:	DMCC Ver 7.0 & Up
Number of Lines:	4
RTP Port Range:	11000 - 11007
RecMgr RTP IP:	0 . 0 . 0 . 0

At the bottom right of the window are "Ok" and "Cancel" buttons. In the background, a table is partially visible with the following structure:

Phone Interface
Server Name
QFINITIWIN2019
Logging Data - Phone Class
Name
POMCOS
VRM

8.12. Administer Logging Data – Phone Class of Service

Expand the **Logging Data – Phone Class of Service** sub-section. Select the configured Phone Class of Service (as shown below) or click on the **New Item** icon. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A desired name, in this case **POMCOS**.
- **Phone:** This can be set to “Default” or **Avaya 8410D** as shown below.
- **Record on lights:** **0**.
- **Login Method:** **CTI**.

The screenshot displays a configuration window titled "Phone Class of Service". The window contains the following fields and values:

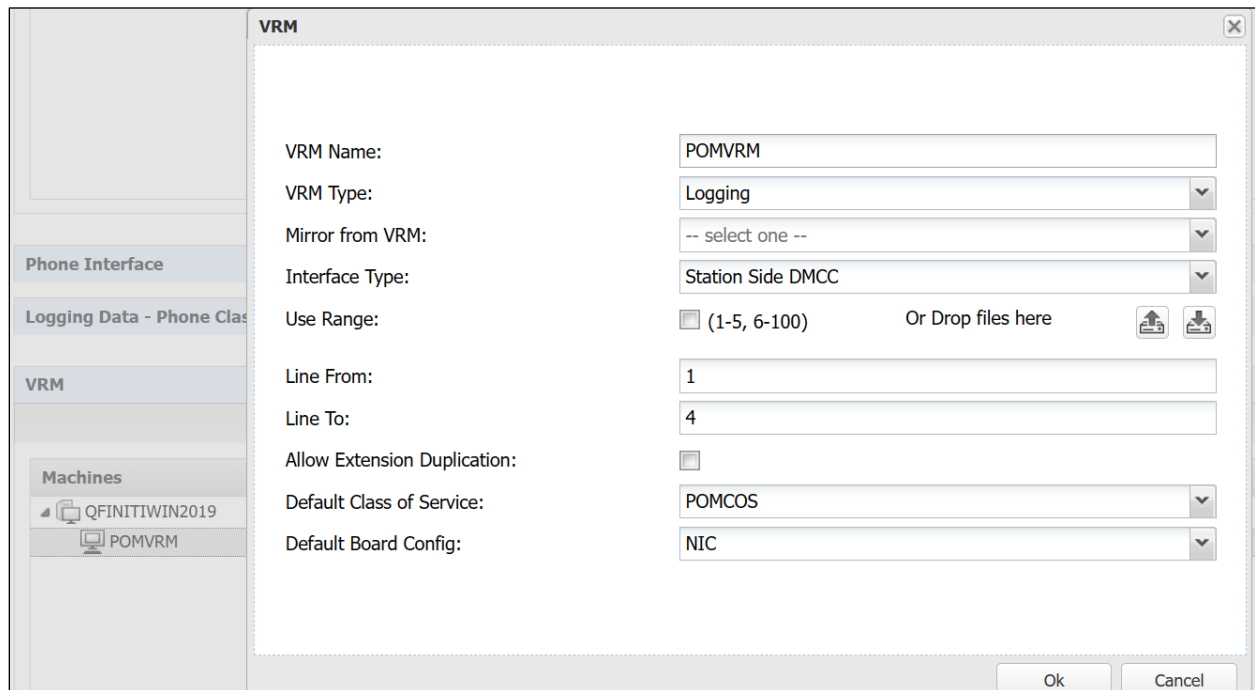
Field	Value
Name:	POMCOS
Phone:	Avaya 8410D
Record on Lights:	0
Login Method:	CTI
Logout Method:	-- select one --
Simulated CTI:	-- select one --
Board Configuration:	Use VRM Default

At the bottom of the window are "Ok" and "Cancel" buttons. The background interface shows a sidebar with sections: "Phone Interface", "Logging Data - Phone Class of Service" (which is expanded), "VRM", and "Machines". Under "Logging Data - Phone Class of Service", the "Name" field is set to "POMCOS".



8.13. Administer VRM

Expand the **VRM** sub-section. Select the machine server name from **Section 0**, followed by the **Add VRM** icon. Enter the following values for the specified fields.

- **VRM Name:** A desired name, in this case **POMVRM**.
- **VRM Type:** **Logging**.
- **Interface Type:** **Station Side DMCC**.
- **Line From** and **Line To:** Range of agent stations, in this case three stations so **1** to **4**.
- **Default Class of Service:** Select the phone class of service name from **Section 8.12**.
- **Default Board Config:** Select the board name from **Section 8.5**.



The screenshot shows a software interface with a sidebar on the left and a main configuration area on the right. The sidebar contains a tree view with the following items: Phone Interface, Logging Data - Phone Clas, VRM, and Machines. The 'Machines' item is expanded, showing two entries: QFINITIWIN2019 and POMVRM. The 'VRM' item is selected in the sidebar. The main configuration area is titled 'VRM' and contains the following fields:

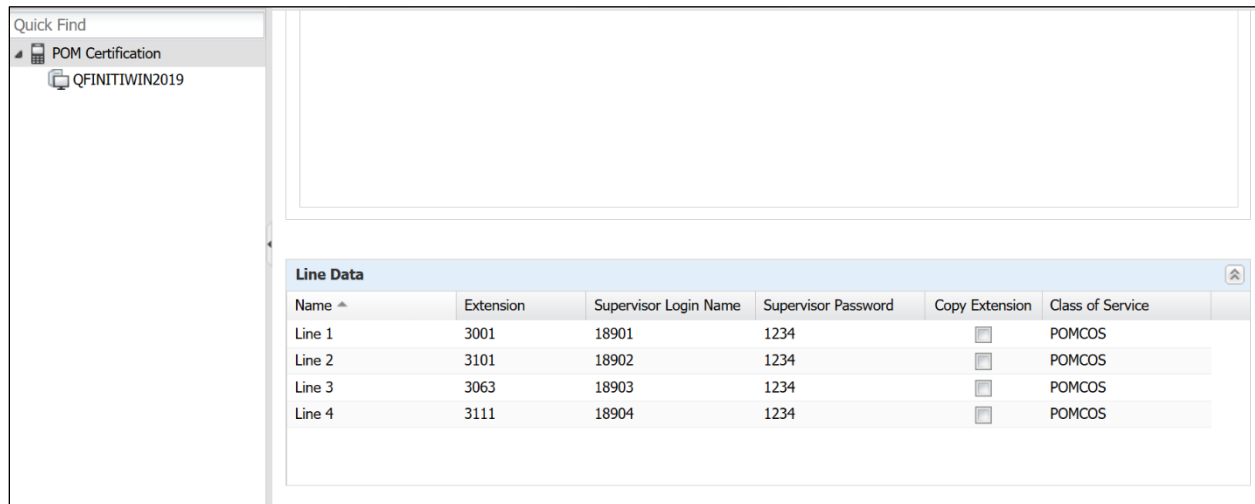
VRM Name:	POMVRM
VRM Type:	Logging
Mirror from VRM:	-- select one --
Interface Type:	Station Side DMCC
Use Range:	<input type="checkbox"/> (1-5, 6-100) Or Drop files here  
Line From:	1
Line To:	4
Allow Extension Duplication:	<input type="checkbox"/>
Default Class of Service:	POMCOS
Default Board Config:	NIC

At the bottom right of the window are 'Ok' and 'Cancel' buttons.

8.14. Administer Line Data

Select the newly added VRM from **Section 8.13** and expand the **Line Data** sub-section. Select the first line. For **Extension**, enter the first agent station extension from **Section 3**. For **Supervisor Login Name** and **Supervisor Password**, enter the first virtual IP softphone extension and associated security code from **Section 5.7** respectively.

Repeat this section to administer all virtual IP softphones from **Section 5.7**, as shown below.



Name	Extension	Supervisor Login Name	Supervisor Password	Copy Extension	Class of Service
Line 1	3001	18901	1234	<input type="checkbox"/>	POMCOS
Line 2	3101	18902	1234	<input type="checkbox"/>	POMCOS
Line 3	3063	18903	1234	<input type="checkbox"/>	POMCOS
Line 4	3111	18904	1234	<input type="checkbox"/>	POMCOS

8.15. Enable Use

Scroll up the right pane and expand the **General** sub-section. Check **Available for Use**.

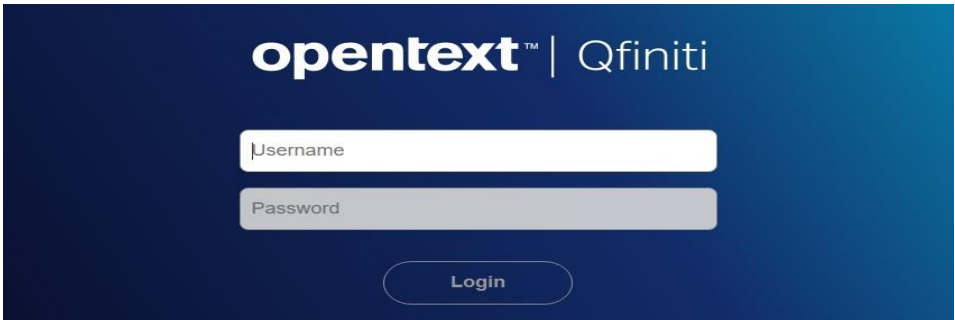
The screenshot displays the 'opentext | Qfiniti SysConfig' web interface. The 'General' tab is selected in the top navigation bar. On the left, the 'Systems' pane shows a list with 'POM Certification' selected. The main configuration area on the right is titled 'General' and contains the following fields:

- Name:** POM Certification
- Switch:** AvayaAES
- System Type:** A list of checkboxes where 'Voice Recording - Logging' is checked, and 'Voice Recording - QA', 'Screen Recording', 'Remote Screen Site', 'Explore', 'Survey', 'Backup', and 'Cloud Connector' are unchecked.
- Description:** An empty text area.
- Available for Use:** A checkbox that is checked and highlighted with a red rectangle.
- NAT Environment:** An unchecked checkbox.

At the top of the configuration area, there is a toolbar with buttons for '+ New', 'Save', 'Refresh', 'Start', 'Stop', and 'Schedule Restart'.

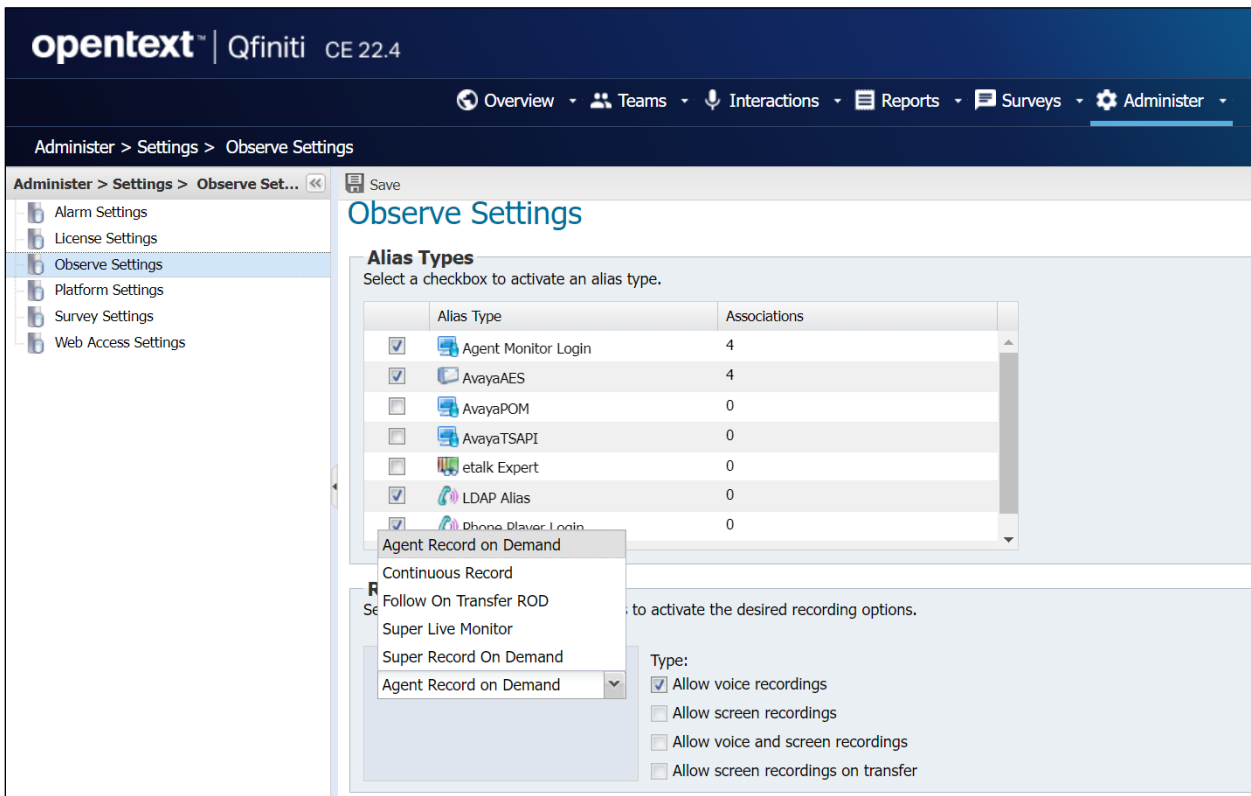
8.16. Launch Qfiniti Web Interface

Access the Qfiniti web interface (Qfiniti Web Access) by using the URL “http://ip-address/QWA/Login.aspx” in an Internet browser window, where “ip-address” is the IP address of the Qfiniti server. The screen below is displayed. Log in using the appropriate credentials.



8.17. Administer Observe Settings

In the subsequent screen, select **Administer** → **Settings** from the top menu, followed by **Observe Settings** in the left pane. Scroll down to the **Recording Options** sub-section. Note the various options that are available for call recording, for compliance testing **Agent Record on Demand** was chosen. For **Type**, check **Allow voice recordings**, as shown below. Retain the default values for the remaining fields.



8.18. Administer Agents

Select **Teams** → **Organization** from the top menu to display the screen below. Select the **New** icon in the right pane to add an agent or click on any of the configured agents shown below, for example **Agent One**.

opentext™ | Qfiniti CE 22.4

Overview Teams Interactions Reports

Teams > Organization > All Team Members

Teams > Organization > All Team Members

+ New Open Save As Classify Bulk Edit

Views

All Team Members

First Name	Middle Name	Last Name	Login ID	Status
Business		Admin	businessadmin	Active
Qfiniti		Administrator	administrator	Active
Agent	eTAC	Four	AFour	Active
Agent	eTAC	One	AOne	Active
Agent	eTAC	Three	AThree	Active
Agent	eTAC	Two	ATwo	Active

Organization

Quick find

My Organization

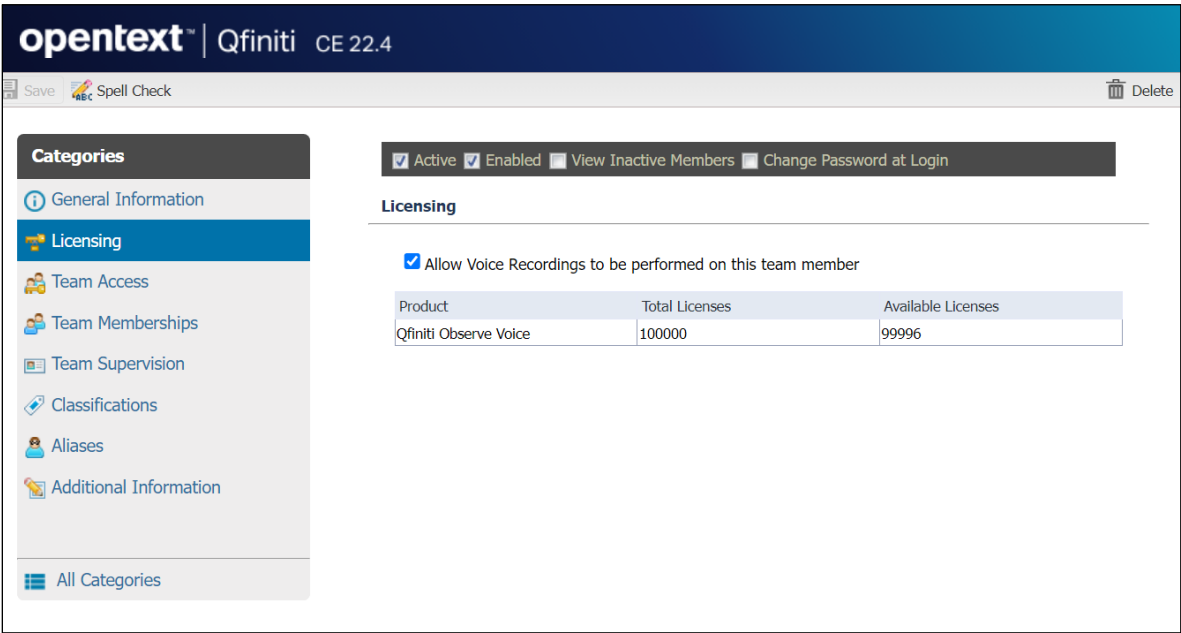
- Agents
- Unassigned Members
- Admin, Business
- Administrator, Qfiniti

In the pop-up screen below, enter the following values for the specified fields, and retain the default values for the remaining fields.

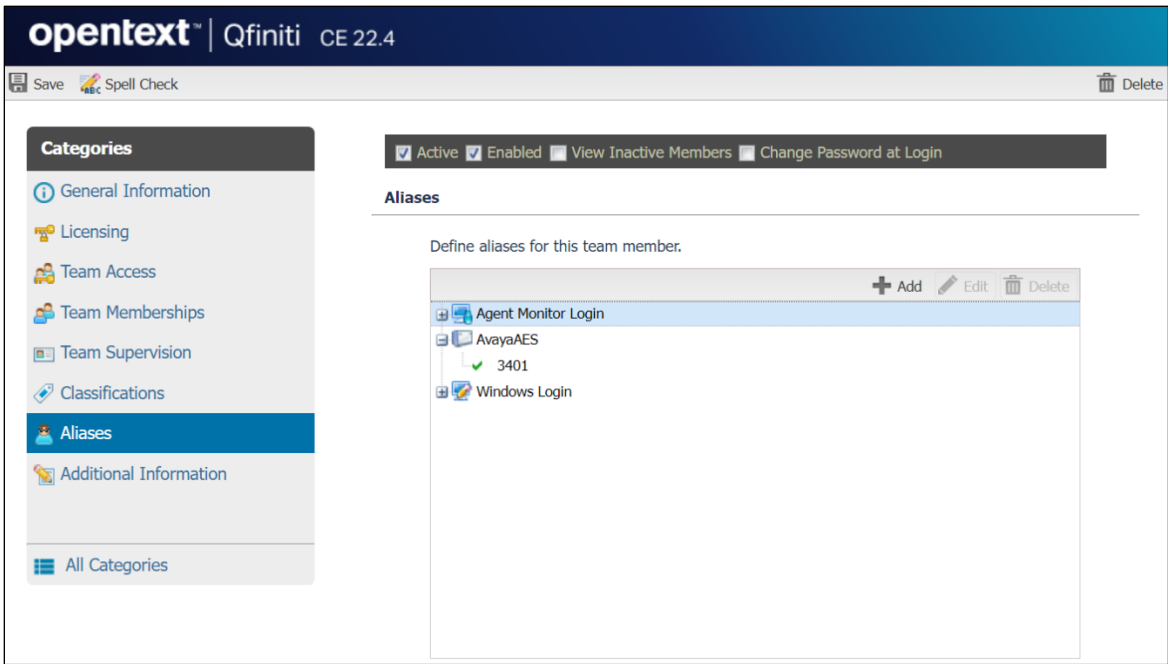
- **First Name:** A desired first name for the first agent line from **Section 8.14**.
- **Last Name:** A desired last name for the first agent line from **Section 8.14**.
- **Role:** Select a desired and existing role.
- **Username:** The desired login credentials for the agent.
- **Password:** The desired login credentials for the agent.
- **Confirm Password:** The same desired login credential for the agent.

The screenshot shows a web browser window titled "Teams - Organization - Google Chrome". The address bar displays a URL starting with "qfinitiwin2019/QWA/Pages/Detail.aspx?". The page header includes the "opentext" logo and "Qfiniti CE 22.4". Below the header, there are buttons for "Save" and "Spell Check", and a "Delete" button. The main content area is divided into a left sidebar and a right panel. The sidebar, titled "Categories", lists various options: "General Information" (selected), "Licensing", "Team Access", "Team Memberships", "Team Supervision", "Classifications", "Aliases", "Additional Information", and "All Categories". The right panel, titled "General Information", contains a form for editing a team member. At the top of this panel, there are checkboxes for "Active" and "Enabled", and buttons for "View Inactive Members" and "Change Password at Login". The form fields include: "Id: 5", "* First Name: Agent", "Middle Name: eTAC", "* Last Name: One", "Email Address:", "Role: Administrators" (with a dropdown arrow and an "Add Role" button), "* Username: AOne", "Password: *****", "Confirm Password: *****", and "* Partition: --Select one--".

Select **Licensing** from the left pane to display the **Licensing** screen. Check **Allow Voice Recordings to be performed on this team member**, as shown below.

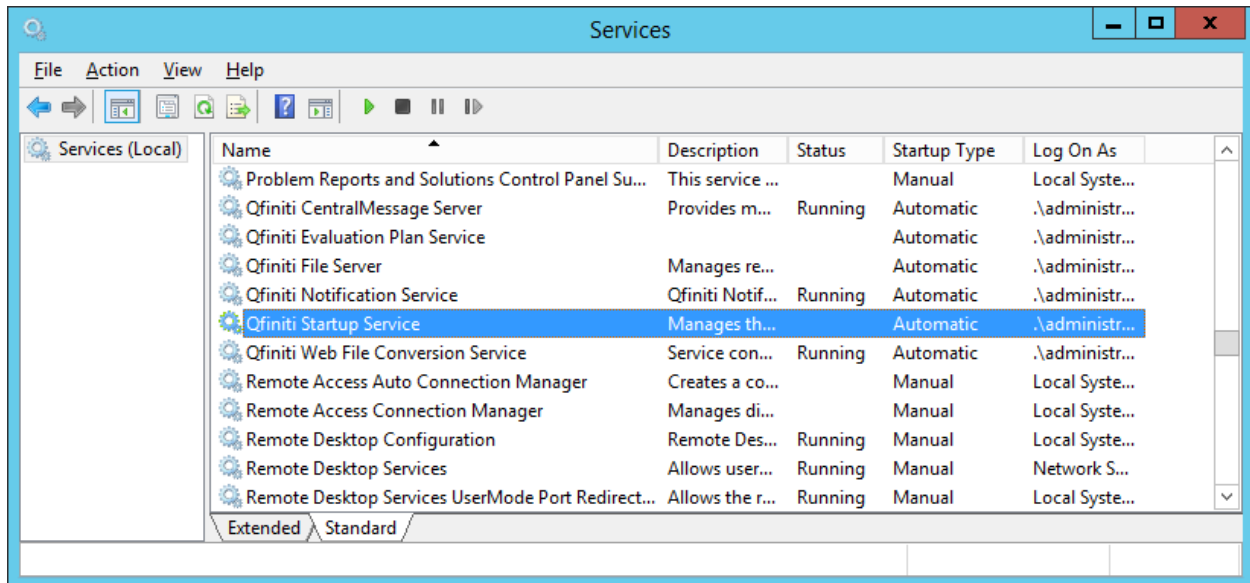


Click on **Aliases** in the left window. A new alias can be added here by clicking on the **Add** icon. For **Type**, select the switch server name from **Section 8.2**. For **Value**, enter the agent ID from **Section 3** that is used by the first agent in **Section 8.14** in this case “3401”. Retain the default value in the remaining field. The screen shot below shows the configured alias already assigned to **First Agent**.



8.19. Start Services

From the Qfiniti server, select **Windows → Control Panel → Administrative Tools → Services** to display the **Services** screen. Start the **Qfiniti Startup Service** as shown below.



9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, and Qfiniti.

9.1. 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. These are some of the key checks that can be performed.

- Verify CTI Service State on Communication Manager.
- Verify TSAPI link and user on Application Enablement Services.
- Verify Avaya Experience Portal is running.
- Verify Avaya Proactive Outreach Manager is running.

9.1.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify status of the administered CTI link by using the **status aesvcs cti-link** command. Verify that the **Service State** is **established** for the CTI link number administered in **Section 5.2** as shown below.

status aesvcs cti-link						
AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	12	no	aespri101x	established	42	26

9.1.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify the **Status** is **Talking** for the TSAPI link administered in **Section 7.2**. Clicking on **User Status** will show the TSAPI users that are currently connected.

Status | Status and Control | TSAPI Service SummaryHome | 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

▶ User Management

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 Mar 9 09:15:53 2023	Online	20	10	1120	1123	30

OnlineOffline

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

TSAPI Service StatusTLink StatusUser Status

The TSAPI user **devconnect** is connected as shown and so the TSAPI events should be passed to this user.

CTI User Status

☐ Enable page refresh every 60 seconds

CTI UsersAll UsersSubmit

Open Streams 3

Closed Streams 0

Open Streams

Name	Time Opened	Time Closed	Tlink Name
devconnect	Fri 28 Apr 2023 06:00:10 PM IST		AVAYA#CM101X#CSTA#AESPRI101X
DMCCLCSUserDoNotModify	Wed 19 Apr 2023 01:07:05 PM IST		AVAYA#CM101X#CSTA#AESPRI101X
DMCCLCSUserDoNotModify	Wed 19 Apr 2023 01:07:05 PM IST		AVAYA#CM101X#CSTA#AESPRI101X

Show Closed StreamsClose All Opened StreamsBack

Verify status of the DMCC link by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

Verify the **User** column shows an active session with the Qfiniti user name from **Section 7.5** and that the **# of Associated Devices** column reflects the number of virtual IP softphones from **Section 5.7** in this case **4**, as shown below.

DMCC Service Summary - Session Summary

Please do not use back button

☒ Enable page refresh every seconds

Session Summary [Device Summary](#)
Generated on Fri Apr 28 18:07:42 IST 2023

Service Uptime: 9 days, 5 hours 0 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 83

Number of Existing Devices: 4

Number of Devices Created Since Service Boot: 4

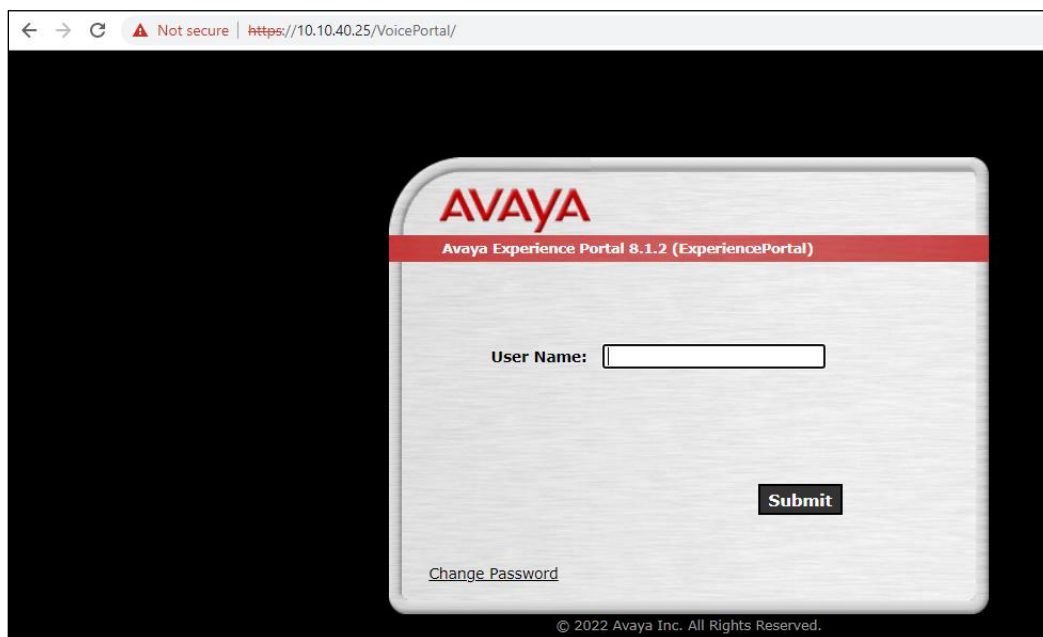
	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	3E8894CF863EFA239 DE7E307C104C54F-82	devconnect	Qfiniti	10.10.40.120	XML Unencrypted	4

[Terminate Sessions](#) [Show Terminated Sessions](#)

Item 1-1 of 1
 Go

9.1.3. Verify Avaya Experience Portal is running

Before checking on Proactive Outreach Manager, check that Experience Portal and Media Processing are running. Log into Experience Portal by opening a browser session to the Experience Portal servers IP address as shown.



Once logged in, navigate to **System Management** → **EPM Manager** in the left window, and check that the server **Mode** is **Online** and **State** is **Running**, as shown below.

Avaya Experience Portal 8.1.2 (ExperiencePortal)

Expand All

Collapse All

User Management

Roles

Users

Login Options

Real-time Monitoring

System Monitor

Active Calls

Port Distribution

System Maintenance

Audit Log Viewer

Trace Viewer

Log Viewer

Alarm Manager

System Management

Application Server

EPM Manager

MPP Manager

Software Upgrade

System Backup

System Configuration

Applications

EPM Servers

MPP Servers

SNMP

Speech Servers

VoIP Connections

Zones

Security

Certificates

Licensing

Reports

You are here: [Home](#) > System Management > EPM Manager

EPM Manager (Mar 9, 2023 5:01:02 PM GMT)

Refresh

This page displays the current state of each EPM in the Experience Portal system. To enable the state and mode commands, select one or more EPMs. To enable the mode commands, the selected EPMs must also be stopped.

Last Poll: Mar 9, 2023 5:00:57 PM GMT

Server Name	Type	Mode	State	Config
<input type="checkbox"/> EPM		Primary	Online	Running OK

State Commands

Start Stop Restart Reboot Halt

Mode Commands

Offline Online

Help

Navigate to **MPP Manager** in the left window and again ensure that **Mode** is **Online**, and **State** is **Running**.

Avaya Experience Portal 8.1.2 (ExperiencePortal)

Expand All

Collapse All

User Management

Roles

Users

Login Options

Real-time Monitoring

System Monitor

Active Calls

Port Distribution

System Maintenance

Audit Log Viewer

Trace Viewer

Log Viewer

Alarm Manager

System Management

Application Server

EPM Manager

MPP Manager

Software Upgrade

System Backup

System Configuration

Applications

EPM Servers

MPP Servers

SNMP

Speech Servers

VoIP Connections

Zones

Security

Certificates

Licensing

Reports

You are here: [Home](#) > System Management > MPP Manager

MPP Manager (Mar 9, 2023 5:01:23 PM GMT)

Refresh

This page displays the current state of each MPP in the Experience Portal system. To enable the state and mode commands, select one or more MPPs. To enable the mode commands, the selected MPPs must also be stopped.

Last Poll: Mar 9, 2023 5:01:19 PM GMT

Server Name	Mode	State	Config	Auto Restart	Restart Schedule	Active Calls		
					Today	Recurring	In	Out
<input type="checkbox"/> mpp810.devconnect.local	Online	Running	OK	Yes	No	None	0	0

State Commands

Start Stop Restart Reboot Halt Cancel

Mode Commands

Offline Test Online

Restart/Reboot Options

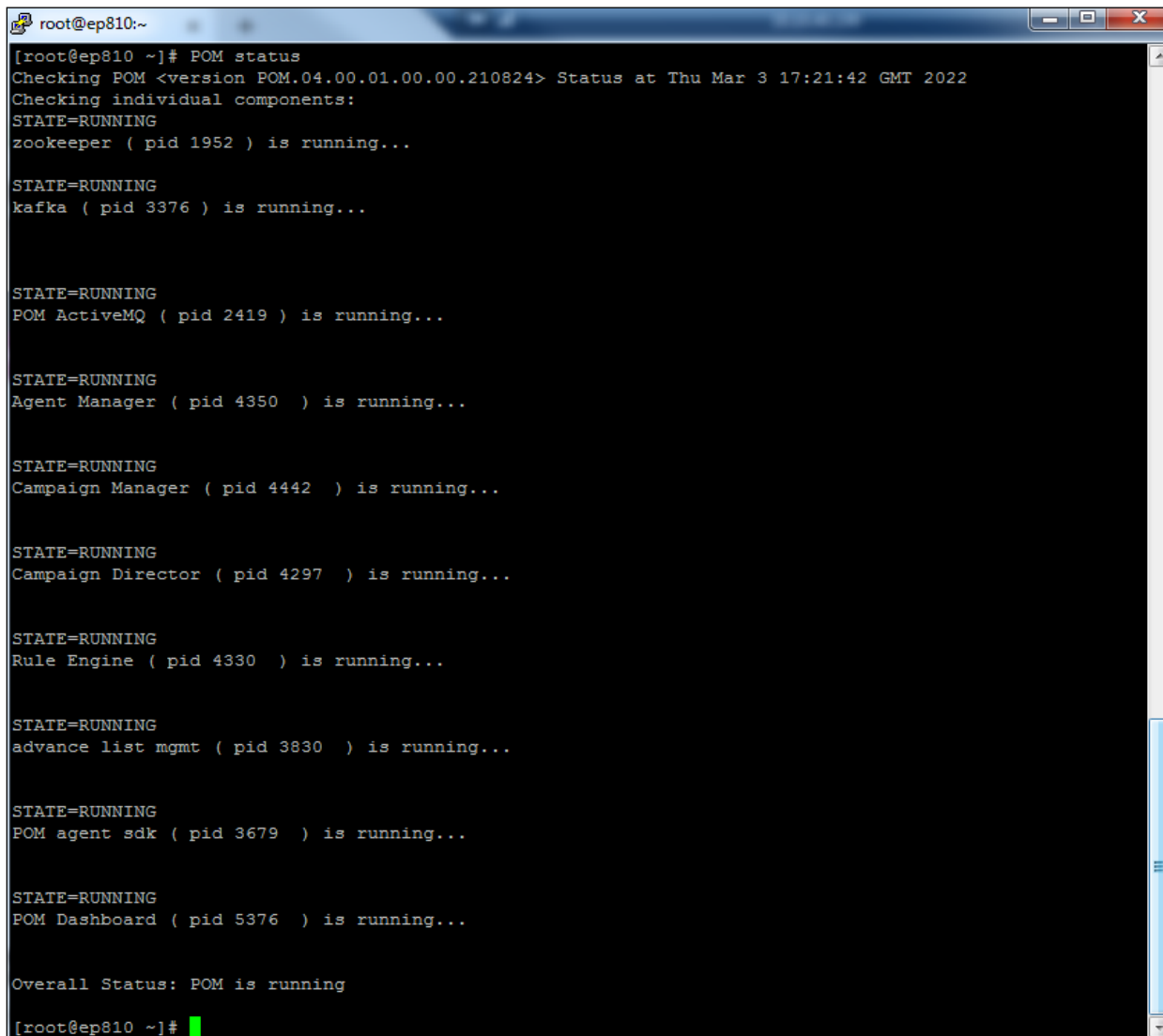
☒ One server at a time

☐ All servers

Help

9.1.4. Verify Avaya Proactive Outreach Manager is running

The status of the POM server can be checked from an SSH session to the POM server using something like PuTTY. Open a connection to Experience Portal/POM server and then ensure that the user “root” is used by typing **su – root** (not shown). Type **POM status** and verify that all POM services are **RUNNING**, as shown below.



```
[root@ep810 ~]# POM status
Checking POM <version POM.04.00.01.00.00.210824> Status at Thu Mar 3 17:21:42 GMT 2022
Checking individual components:
STATE=RUNNING
zookeeper ( pid 1952 ) is running...

STATE=RUNNING
kafka ( pid 3376 ) is running...

STATE=RUNNING
POM ActiveMQ ( pid 2419 ) is running...

STATE=RUNNING
Agent Manager ( pid 4350 ) is running...

STATE=RUNNING
Campaign Manager ( pid 4442 ) is running...

STATE=RUNNING
Campaign Director ( pid 4297 ) is running...

STATE=RUNNING
Rule Engine ( pid 4330 ) is running...

STATE=RUNNING
advance list mgmt ( pid 3830 ) is running...

STATE=RUNNING
POM agent sdk ( pid 3679 ) is running...

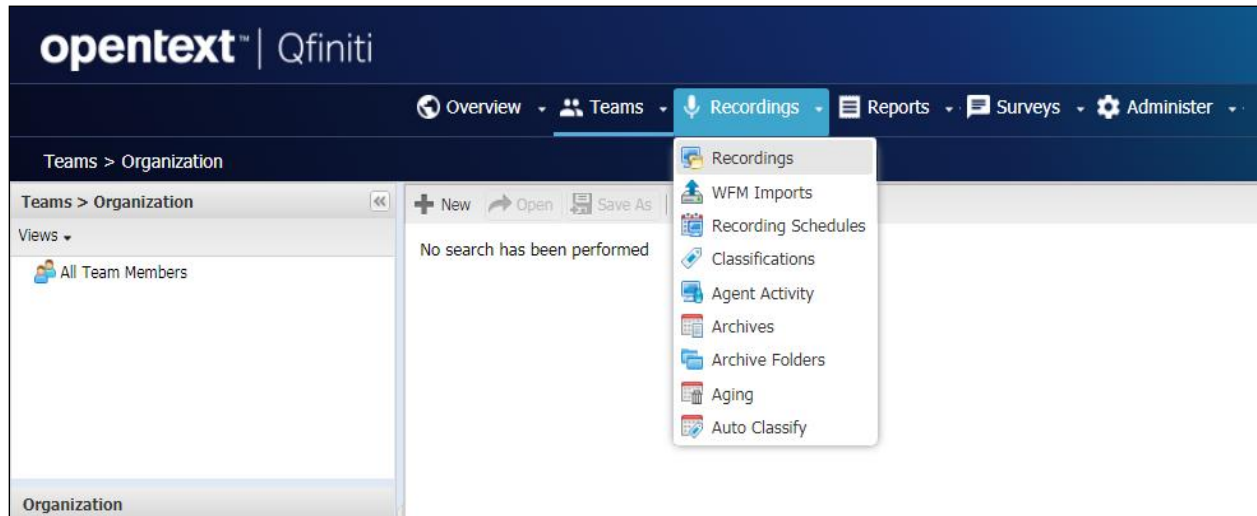
STATE=RUNNING
POM Dashboard ( pid 5376 ) is running...

Overall Status: POM is running
[root@ep810 ~]#
```


9.2. Verify OpenText Qfiniti

Log an agent in to handle and complete an outbound POM call. Follow the procedure in **Section 8.16** to launch the Qfiniti web interface and log in using the appropriate user credentials.

Select **Recordings** → **Recordings** from the top menu.

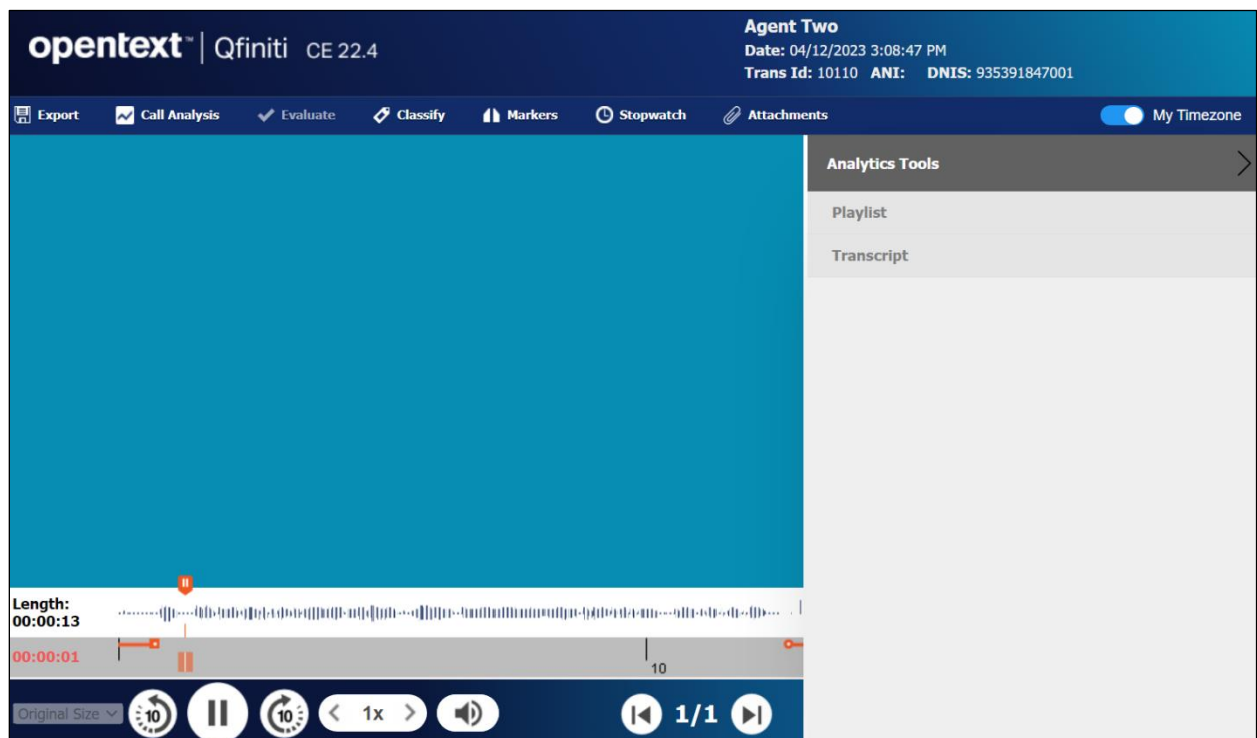


Click on the list of recordings that are to be viewed in the left window. For example, **Current Month Recording Files** is selected below, showing all the recordings present for the current month. Verify that there is an entry reflecting the last call, with proper values in the relevant fields.

The screenshot shows the opentext Qfiniti CE 22.4 interface. The left sidebar has a 'Views' menu with options like 'Today's Recording Files', 'Yesterday's Recording Files', 'Current Week Recording Files', 'Previous Week Recording Files', 'Current Month Recording Files' (selected), 'Previous Month Recording Files', 'Current Year Recording Files', 'Prev 12 Calendar Mos Recording F', 'Previous Year Recording Files', and 'Unknown Agent Recording Files'. The main area displays a table of recordings.

Transaction ID	Agent	Recording Type	Date(Server)	Time(Server)	Duration (sec)	Call Direction	Extension	DNIS	ANI
10114	Two, Agent eTAC	Voice	2023-04-12	15:25:21.000	00:00:21	Outbound	3101	935391847001	
10113	Two, Agent eTAC	Voice	2023-04-12	15:19:45.000	00:01:15	Outbound	3101	935391847001	
10112	Two, Agent eTAC	Voice	2023-04-12	15:14:48.000	00:00:18	Outbound	3101	935391847001	
10111	Two, Agent eTAC	Voice	2023-04-12	15:09:47.000	00:01:36	Outbound	3101	935391847001	
10110	Two, Agent eTAC	Voice	2023-04-12	15:08:47.000	00:00:13	Outbound	3101	935391847001	
10108	Two, Agent eTAC	Voice	2023-04-12	14:46:38.000	00:01:32	Outbound	3101	935391847001	
10107	Two, Agent eTAC	Voice	2023-04-07	14:35:29.000	00:02:52	Outbound	3101	935391847001	
10106	Two, Agent eTAC	Voice	2023-04-06	18:43:39.000	00:00:27	Outbound	3101	935391847001	
10105	Two, Agent eTAC	Voice	2023-04-06	18:14:05.000	00:00:13	Unknown	3101		
10104	Two, Agent eTAC	Voice	2023-04-06	18:12:19.000	00:01:15	Outbound	3101	935391847001	
10103	Two, Agent eTAC	Voice	2023-04-06	18:00:47.000	00:00:09	Outbound	3101	935391847001	
10102	Two, Agent eTAC	Voice	2023-04-06	17:38:47.000	00:00:17	Outbound	3101	935391847001	
10101	Two, Agent eTAC	Voice	2023-04-06	17:36:10.000	00:00:32	Outbound	3101	935391847001	
10100	Two, Agent eTAC	Voice	2023-04-06	17:30:10.000	00:00:20	Outbound	3101	935391847001	
10099	One, Agent eTAC	Voice	2023-04-06	17:21:14.000	00:01:20	Outbound	3001	935391847001	
10098	Two, Agent eTAC	Voice	2023-04-06	17:12:27.000	00:00:13	Outbound	3101	935391847001	
10097	Two, Agent eTAC	Voice	2023-04-06	17:10:21.000	00:01:16	Outbound	3101	935391847001	
10096	One, Agent eTAC	Voice	2023-04-06	17:08:08.000	00:02:55	Outbound	3001	935391847001	
10095	Two, Agent eTAC	Voice	2023-04-06	16:43:41.000	00:01:19	Outbound	3101	935391847001	

Double click on the entry and verify that the recording can be played back. Note that the device playing back the audio will need an audio device available and enabled.



10. Conclusion

These Application Notes describe the configuration steps required for Qfiniti to successfully interoperate with Avaya Proactive Outreach Manager, Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using Service Observing. All feature and serviceability test cases were completed with an observation noted in **Section 2.2**.

11. Additional References

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

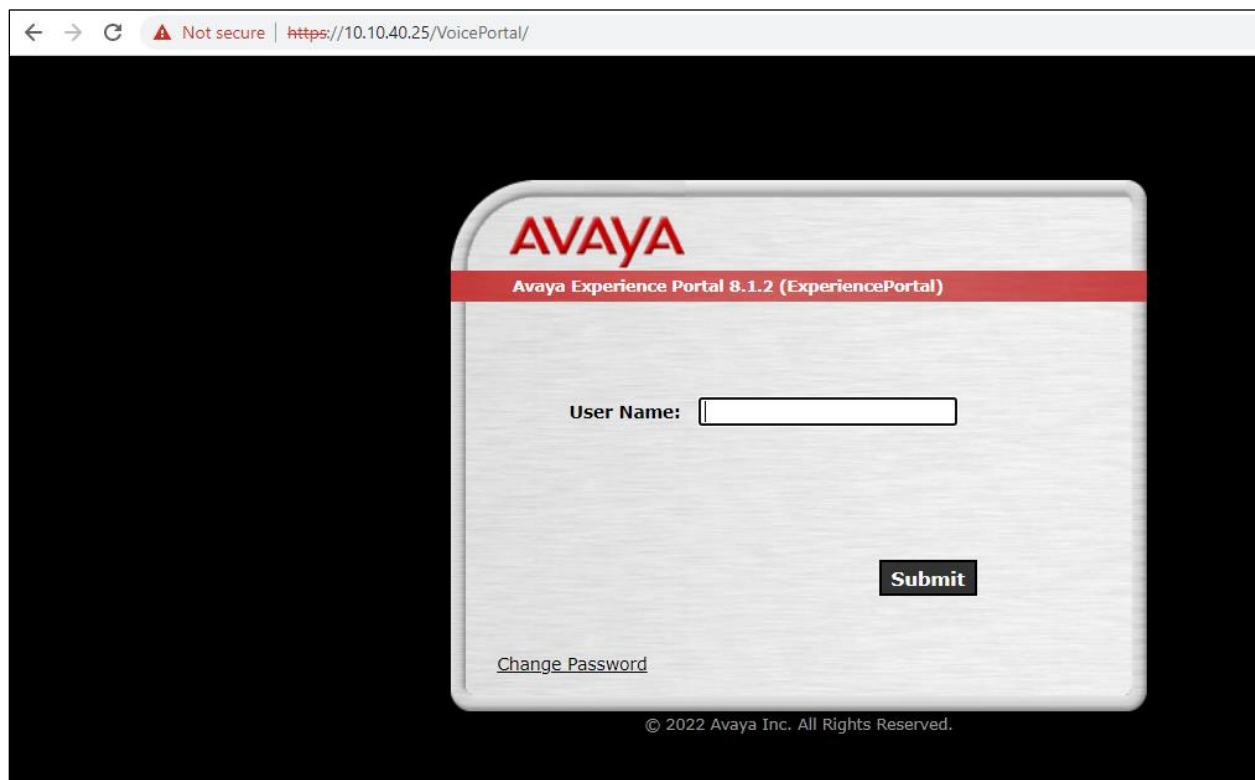
1. *Administering Avaya Aura® Communication Manager*, Release 10.1.x, available at <http://support.avaya.com>.
2. *Administering Aura® Application Enablement Services*, Release 10.1.x, available at <http://support.avaya.com>.
3. *Avaya Proactive Outreach Manager Integration*, Release 4.0.2, available at <http://support.avaya.com>.
4. *Implementing Avaya Proactive Outreach Manager*, Release 4.0.2, available at <http://support.avaya.com>.
5. *OpenText Qfiniti User Guide*, Version 22.4, November 2022, available to existing customers at [WFO Software Home Page - Extended ECM CE 23.2 \(opentext.com\)](https://www.opentext.com/Products/Software/Avaya/Avaya-Software-Home-Page-Extended-ECM-CE-23.2).

12. Appendix

There are many configurations that are required for various campaigns to operate, the screen shots displayed here are to serve to display the setup used for compliance testing. This configuration shows the preview campaign that was used, the contact list and strategy associated with that outbound preview campaign.

It is assumed that both POM and Experience Portal are already installed with the connections made to both Session Manager and AES. The setup and configuration of these connections are therefore outside the scope of these Application Notes. **The procedural steps that are presented in this Appendix for informational purposes only.**

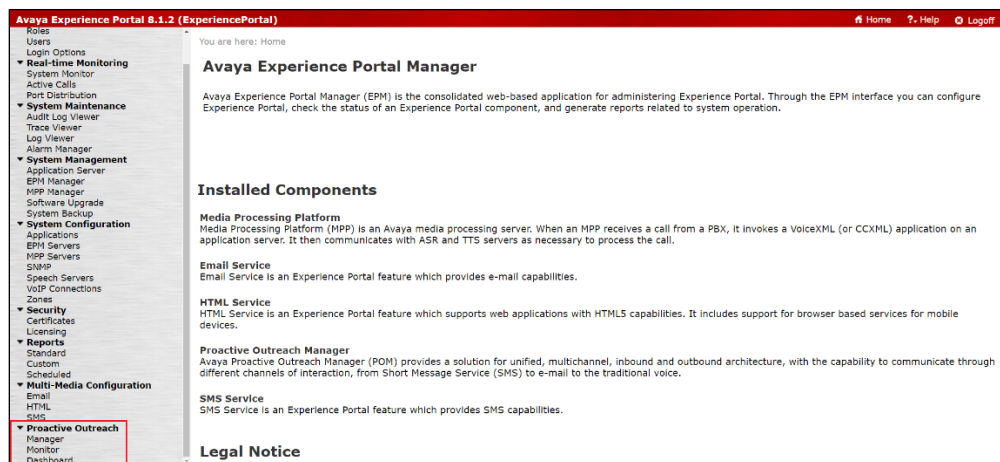
Experience Portal is configured via the Experience Portal Manager (EPM) web interface. To access the web interface, enter **https://[IP-Address]/VoicePortal** as the URL in an internet browser, where IP-Address is the IP address of the EPM. Log in using the Administrator user role. The screen shown below is displayed.



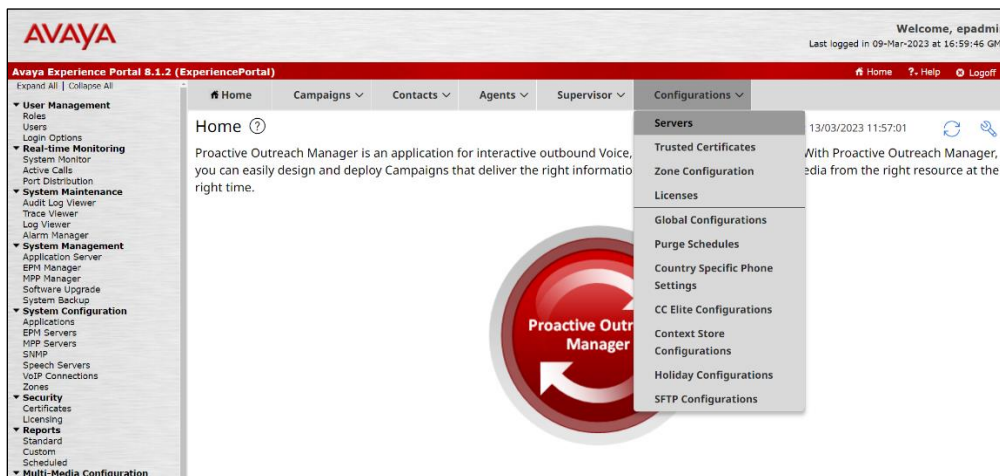
Note: The following sections aim to display the configuration on POM that was used during compliance testing and to help the reader understand the setup of POM that was used. They do not serve as a setup and configuration guide for POM or Experience Portal.

12.2. Display configuration of POM Server

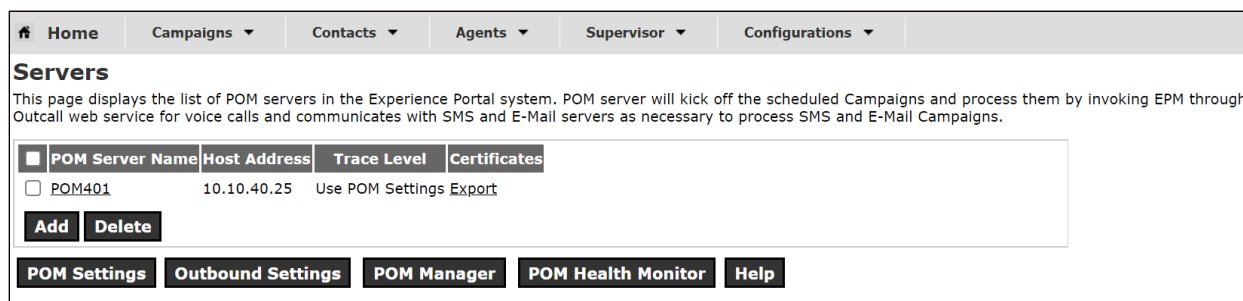
Information on the POM server can be found by navigating to **Proactive Outreach → Manager** in the left window, as shown.



From the main window, select **Configurations → Servers**.

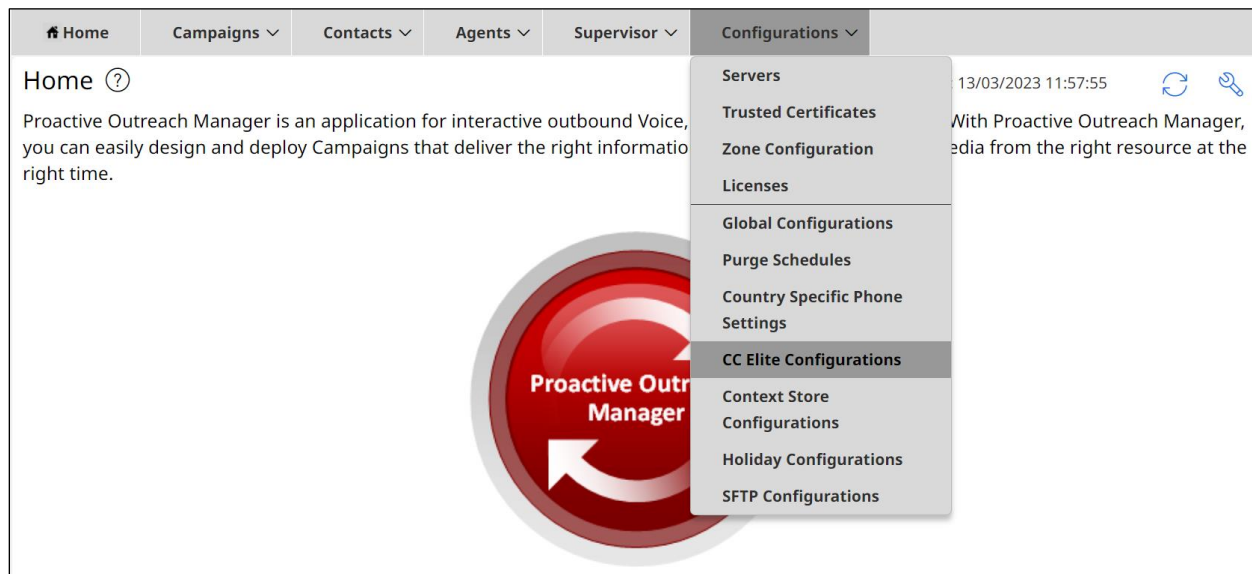


Information on the POM server can be found by either selecting the **POM Server Name** or the various buttons underneath that.



12.3. Display configuration of the CTI connection

Select **Configuration** → **CC Elite Configurations** from the main window.



Both the **Aura81** and **Aura 10.1** CTI groups were already in place for compliance testing, clicking on the **Aura 10.1** group will open the connection to show the details.

CC Elite Configurations

This page allows editing of CTI server setup details, CMS server setup details and skills in POM database associated with CC Elite skills.

Last poll: 13/03/2023 11:57:51

CTI Configuration

CTI Group Name	CM IP Address	CM Login	AES IP Address	AES Secure Connection	CTI Group Role	Action
Aura81	10.10.40.37	pomout	10.10.40.38	false	Select	
Aura10.1	10.10.40.13	pomout	10.10.40.16	false	Active	

Add CTI Detail **Help**

CMS Configuration

Server IP Port	CMS Secure Connection	Server Role↑	Agent Thrashing Interval (seconds)	Action
----------------	-----------------------	--------------	------------------------------------	--------

Add CMS Configuration **Help**

Information such as the IP Address of Communication Manager and the AES are stored here as well as a Communication Manager user that needs to be created.

Edit CTI Detail

This page allows editing of existing CTI details.

Edit CTI Configuration

* CTI group name Aura10.1
* CM IP address 10.10.40.13
* CM login pomout
* CM password
* AES IP address 10.10.40.16
AES Secure Connection ☐
CTI group role Active

Save Cancel Help

From the **Configure CTI setup details, CMS setup and POM Skills** page, the outbound skill must be added. Again, this was already in place but can be added by clicking on **Add Skill**. The skill below matches the outbound hunt group that must be setup.

Aura81	10.10.40.37	pomout	10.10.40.38	false	Select	
Aura10.1	10.10.40.13	pomout	10.10.40.16	false	Active	

Add CTI Detail Help

CMS Configuration

Server IP Port	CMS Secure Connection	Server Role	Agent Thrashing Interval (seconds)	Action
----------------	-----------------------	-------------	------------------------------------	--------

Add CMS Configuration Help

Skillset name All
Skillset type All Skills All

Show Refresh Skills

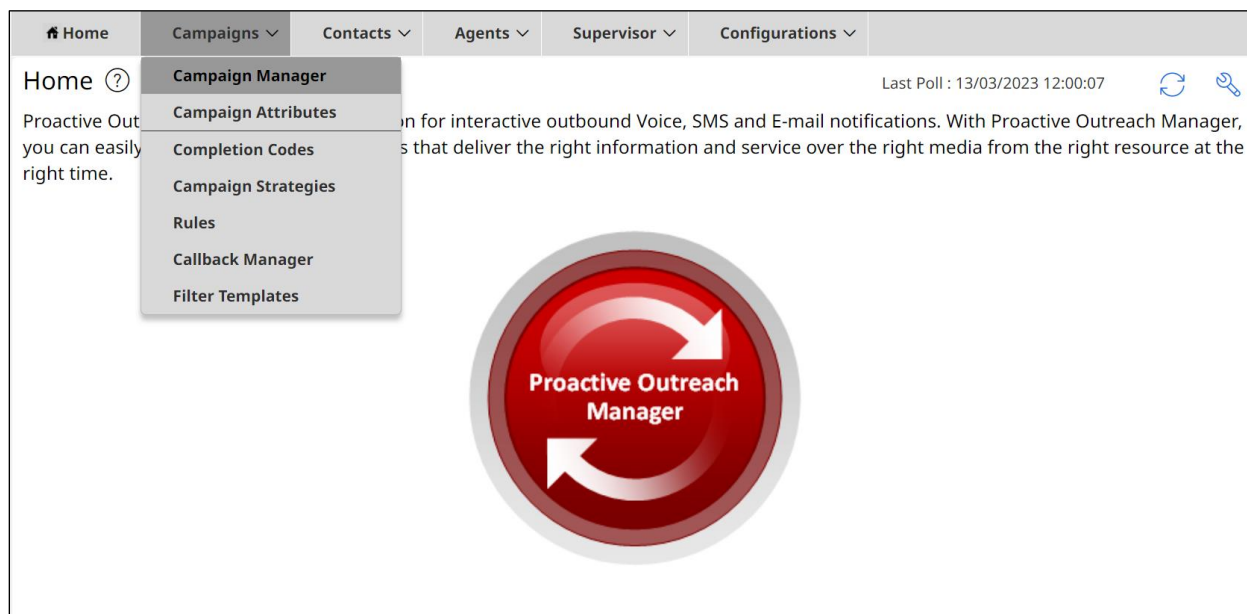
CC Elite Skill Number	POM Skill Name	Skill Type	Parameter to Monitor for Blending	EWT levels	Agent Acquire Threshold	Agent Release Thresh
10	Outbound	Outbound	-	-	0	0

Add Skill Help

12.4. Display POM Campaigns

It is assumed that the POM campaigns are already setup and running prior to the connection from Desktop Connect. The setup and configuration of the POM Campaign including the Strategies and Contact Lists are outside the scope of these Application Notes. However, an example of the Preview Strategy and Contact List are included in this **Appendix**.

Navigate to **Campaigns → Campaign Manager** from the main window, as shown.



The following two campaigns were setup for compliance testing.

- **Preview** – this campaign allows the agent to make the outbound call by presenting the call information to the agent desktop and allowing the agent click on “preview dial”.
- **Progressive** – this campaign makes the call first and then presents the call information to the agent desktop, this effectively forces the call to the agent.

The screenshot shows the 'Campaign Manager' interface. It includes a 'New Campaign' button, a search bar labeled 'Search Campaign', and a table of campaigns. The table has columns for Name, Contact List - Filter Template, Type, Campaign Strategy, Last Executed, and Waiting ...

Name	Contact List - Filter Template	Type	Campaign Strategy	Last Executed	Waiting ...
Preview	OnetoPSTN - None	Finite	Preview	09/03/2023 10:30:09	0
Progressive	OnetoPSTN - None	Finite	Progressive	09/03/2023 10:31:09	0

12.5. Display Campaign Components

The following section shows the configuration of the various components that contribute to the overall campaign.

12.5.1. Completion Codes

Navigate to **Campaigns → Completion Codes** as shown below.



There are three Completion Codes already present on this POM and each of these can be assigned to the Campaign Strategy. If a new code was to be added, click on **Add** shown below.

The screenshot shows the "Completion Codes" configuration page. It includes a header with navigation tabs and a sub-header "Completion Codes" with a help icon. Below the header, there is a description: "Depending on your user role, this page allows you to create, modify, delete custom Completion Codes." There are two buttons: "New Completion Code" (blue) and "Delete" (orange). A search bar labeled "Search Completion Code" is also present. The main content is a table with the following columns: ID, Completion Code, RPC, Success, Closure, AMA, and Description.

ID	Completion Code	RPC	Success	Closure	AMA	Description
74	Success	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Successful Sale
75	Callback	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Wants call back
76	NoAnswer	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Not answered

The example below shows the **Success** Completion Code which is assigned to the Preview Strategy that is to be displayed below.

Completion Codes / Success ?

This page allows you to modify Completion Codes.

Name

Success

Description

Successful Sale

Right Party Connect

Success

Closure

Answer Machine by Agent


12.5.2. Campaign Strategies

Navigate to **Campaigns** → **Campaign Strategies** as shown below.





The Campaign Strategies are shown where a new strategy can be added by clicking on **Add** or existing strategies can be viewed by clicking on the **Name** of the strategy displayed.

Campaign Strategies

[Refresh](#)



This page allows the user to manage Campaign Strategies, depending on the user role.

 [Advanced](#)



Show













50

 | Page: 1/1



Go



Name	State	Task Types	Action
Preview	Completed	 	   
Progressive	Completed	 	   

Add

Import

Help

Clicking on the **Preview** strategy from the screen above will show the **Campaign Strategy** called **Preview** that was created for compliance testing.

Campaign Strategy Editor - Google Chrome

Not secure | https://10.10.40.25/VP_POM/faces/admin/ContactStrategy.xhtml

SHOW TOOL BOXSHOW SOURCESAVE SAVE DRAFTCOPYPASTEDELETEHELP

Campaign Strategy: Preview

Campaign Strategy

Handler (initial)

Preview

Address

Result Processors

Result (Call Answered)

Agent

Property	Value
Name	Preview
Description	Preview
Sender's Display Name	Preview
Sender's Address	sip:98765@greanep.sil6.avaya.com
Timeout (sec)	
Restrict On No Suitable Address	Yes
Guard Times	Disable
Skipover To Next Phone	Disable
Min Contact Time	hh:mm:ss
Max Contact Time	hh:mm:ss
Re-check Interval (min)	

Scrolling down from the screen on the previous page shows the settings that were used for compliance testing.

The screenshot shows the 'Campaign Strategy: Preview' interface. On the left, a tree view shows the hierarchy: Campaign Strategy → Handler (initial) → Preview → Address → Result Processors → Result (Call Answered) → Agent. The 'Preview' node is selected. On the right, the 'PACING PARAMETERS' section is visible, containing the following settings:

PACING PARAMETERS	
Call Pacing Type	Preview
Runtime Change Pacing Type	OFF
Timed Preview	No
Preview Time (Sec)	
Can Cancel Preview	Enable
Min. Agents*	1
Max. Agents*	5
Agent Outbound Skill*	Outbound
ACW Time (Sec)*	30
# of ACW extensions	2
Default Completion code*	Success

12.5.3. Contact List

To add or view the Contact Lists, navigate to **Contacts** → **Contact Lists** as shown below.



There is a Contact List already configured for the Preview Campaign called **OnetoPSTN**. Details of this Contact List can be viewed by clicking on the **Contact List Name** icon. A new Contact List can be added by clicking on **Add** and uploading the contacts from a file.

Contact Lists ?

This page displays all the Contact Lists. Depending on the user role, you can add, change, delete and empty Contact List. You can see Contacts in a Contact List. If organizations are enabled, you can associate Contact List with organization.

New Contact List
Filter Refresh Down

Contact List Na...	Zone ...	Total ...	Availa...	Excluded...	Last Updated	Allowed O...
⋮ OnetoPSTN	Default	1	1	0	02/03/2023 14:5...	

The Contact List shown has just one entry, with some of the details displayed. Clicking on that entry will show further details.

Contact List / OnetoPSTN ?

Details
Data Source
Attributes
Contacts
Excluded Contacts

Cancel
Save

New Contact
Filter Refresh Down

System Con...	ID	First Name	Last Name	Phone 1	Phone 1 Co...
⋮ 1	1	Paul	Greaney	9353915101	1

Contact information, such as name and address are shown, and scrolling down will reveal more.

Contact List / Contacts / 1 ?

Cancel
Save

Contact List Name

OnetoPSTN

Predefined Attributes

ID
1

First Name
Paul

Last Name
Greaney

E-Mail
paul@gmail.com

Country Predefined
UK

Zipcode Predefined
H91 XXXX

Zipcode Time Zone Predefined

Zipcode State Predefined

Address Line 5 Predefined
Galway

Address Line 4 Predefined
Oranmore

Title Predefined
Mr.

The **Phone 1** and **Phone 2** information is most important for the outbound calls to take place successfully.

Contact List / Contacts / 1 ?

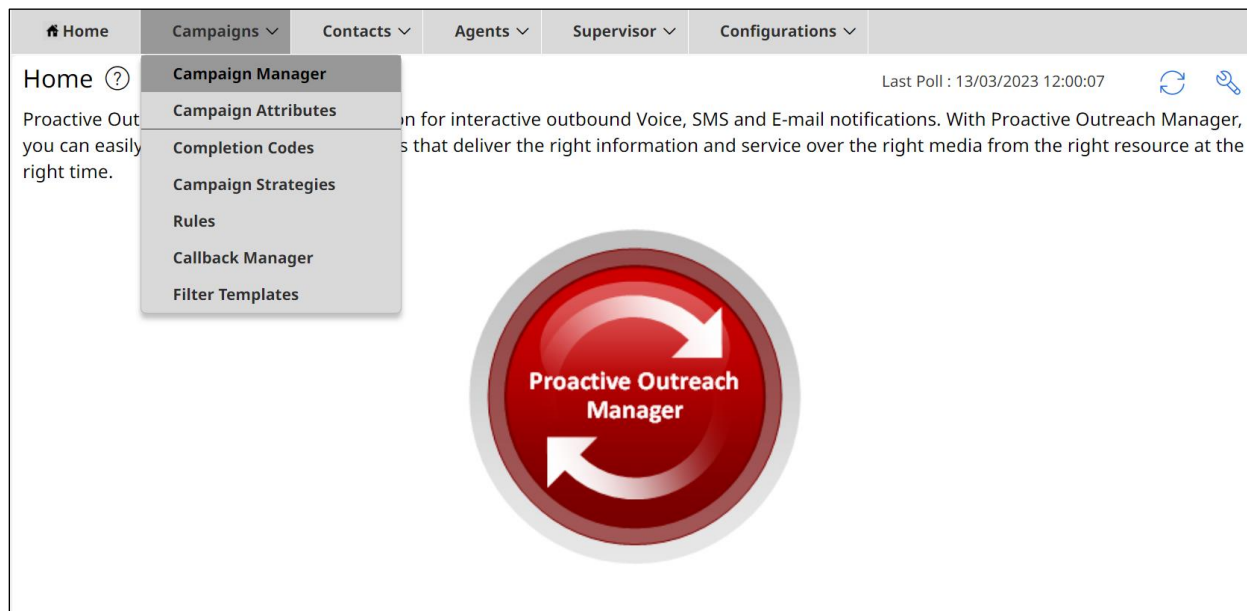
Cancel Save

Phone Attributes

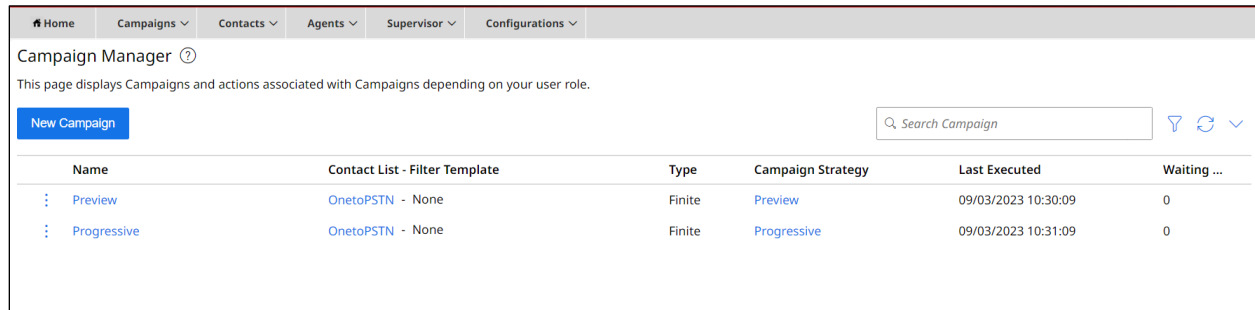
Phone 1 9353915101	Phone 1 Country Code 1	Time Zone Europe/Dublin
Phone 1 State	Phone 1 Wireless	Phone 2 9353915101
Phone 2 Country Code 1	Phone 2 Time Zone Europe/Dublin	Phone 2 State
Phone 2 Wireless	Phone 1 Allowed Time	Phone 1 Disallowed Time
Phone 2 Allowed Time	Phone 2 Disallowed Time	

12.5.4. Display Preview Campaign

Navigate to **Campaigns** → **Campaign Manager** as shown below.



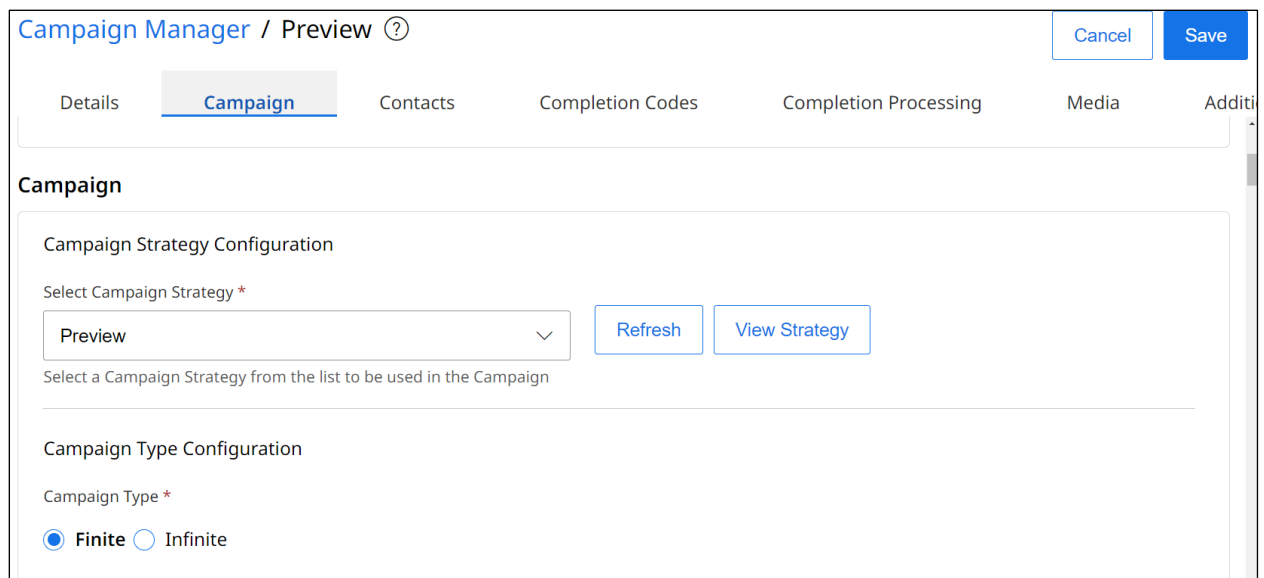
Clicking on **Preview** below to open the campaign and display the various components.



The screenshot shows the 'Campaign Manager' interface. At the top, there is a navigation bar with tabs: Home, Campaigns (selected), Contacts, Agents, Supervisor, and Configurations. Below the navigation bar, the title 'Campaign Manager' is followed by a help icon. A subtitle states: 'This page displays Campaigns and actions associated with Campaigns depending on your user role.' There is a 'New Campaign' button on the left and a search bar on the right. The main content is a table with the following columns: Name, Contact List - Filter Template, Type, Campaign Strategy, Last Executed, and Waiting ...

Name	Contact List - Filter Template	Type	Campaign Strategy	Last Executed	Waiting ...
Preview	OnetoPSTN - None	Finite	Preview	09/03/2023 10:30:09	0
Progressive	OnetoPSTN - None	Finite	Progressive	09/03/2023 10:31:09	0

The **Campaign Strategy** that was shown previously is entered in the **Campaign** tab.



The screenshot shows the 'Campaign Manager / Preview' interface. At the top, there is a navigation bar with tabs: Details, Campaign (selected), Contacts, Completion Codes, Completion Processing, Media, and Additions. There are 'Cancel' and 'Save' buttons on the right. The main content is the 'Campaign' tab, which contains two sections: 'Campaign Strategy Configuration' and 'Campaign Type Configuration'. In the 'Campaign Strategy Configuration' section, there is a dropdown menu for 'Select Campaign Strategy *' with 'Preview' selected, and 'Refresh' and 'View Strategy' buttons. Below the dropdown, there is a text prompt: 'Select a Campaign Strategy from the list to be used in the Campaign'. In the 'Campaign Type Configuration' section, there is a dropdown menu for 'Campaign Type *' with 'Finite' selected and 'Infinite' as an option.

Campaign Strategy Configuration

Select Campaign Strategy *

Preview Refresh View Strategy

Select a Campaign Strategy from the list to be used in the Campaign

Campaign Type Configuration

Campaign Type *

☒ Finite ☐ Infinite

The **Contact List** displayed previously is associated with this campaign under the **Contacts** tab.

The screenshot displays the 'Campaign Manager / Preview' interface. At the top, there are tabs for 'Details', 'Campaign', 'Contacts' (which is selected and underlined), 'Completion Codes', 'Completion Processing', 'Media', and 'Additions'. To the right of the tabs are 'Cancel' and 'Save' buttons. Below the tabs, the 'Contacts' section is titled. Under this title, there is a 'Contact List Configuration' area. This area includes a 'Contact List and Filter Template Association *' section. Within this section, there are three main fields: 'Contact List *' with a dropdown menu showing 'OnetoPSTN', 'Filter Template' with a dropdown menu showing 'Select', and 'Dialing Allocation Percentage' with a text input field containing '100'. To the right of these fields are three icons: an eye, a pencil, and a trash can. Below these fields are two buttons: '+ Add New' and 'Save All'. At the bottom of the configuration area, there are two checkboxes: 'Apply same filter' and 'No Dialing Allocation'. At the very bottom of the 'Contacts' section is a 'View Contacts' button.

The **Completion Codes** that were displayed previously are added under the **Completion Codes** tab.

©2023 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.