



Avaya Solution & Interoperability Test Lab

Application Notes for OpenText Qfiniti Survey 20.4 with Avaya Aura® Application Enablement Services 8.1.3 and Avaya Aura® Session Manager 8.1.3 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for OpenText Qfiniti Survey 20.4 to interoperate with Avaya Aura® Application Enablement Services 8.1.3, Avaya Aura® Session Manager 8.1.3, and Avaya Aura® Communication Manager 8.1.3. OpenText Qfiniti Survey is an inbound IVR-based survey system that is part of the OpenText Qfiniti product suite.

In the compliance testing, OpenText Qfiniti Survey used the Telephony Services Application Programming Interface from Avaya Aura® Application Enablement Services and SIP users with Avaya Aura® Session Manager to provide automated survey to inbound ACD callers.

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 Survey (Survey) 20.4 to interoperate with Avaya Aura® Application Enablement Services 8.1.3, Avaya Aura® Session Manager 8.1.3, and Avaya Aura® Communication Manager 8.1.3. Survey is an inbound IVR-based survey system that is part of the Qfiniti product suite.

In the compliance testing, Survey used the Telephony Services Application Programming Interface (TSAPI) from Application Enablement Services and SIP users with Session Manager to provide automated survey to inbound ACD callers.

The TSAPI interface is used by Survey to monitor skill groups, agent stations, and virtual SIP users. The SIP user interface is used by Survey to register virtual SIP users with Session Manager for connecting inbound ACD callers to Survey. The virtual SIP users are configured as members of a hunt group on Communication Manager.

Survey supports various modes, and the compliance testing used the agent transfer mode with agent verbally offering survey to PSTN callers toward end of inbound ACD call and performs unsupervised transfer of agreed callers to the Survey hunt group.

Upon connection of PSTN caller with Survey caller via an available virtual SIP user, Survey plays pertinent survey questions and collects responses via DTMF selections. Survey can also record PSTN caller voice responses for open-ended questions such as additional comments and performs immediate transfer of PSTN caller to supervisor via SIP REFER upon meeting specific criteria.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Survey application, the application automatically used SIP to register the virtual SIP users, and TSAPI to request monitoring of skill groups, agent stations, and virtual SIP users.

For the manual part of testing, survey calls were manually transferred by agents to the Survey hunt group. DTMF and voice input were provided as responses to pertinent survey questions.

The verification of tests included use of Qfiniti web interface for proper logging of survey results and playback of voice responses.

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 Note, the interfaces between Avaya systems and Survey 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 Survey:

- Handling of TSAPI messages in areas of event notification and value queries.
- Handling of SIP messages in areas of registration, G.711, media shuffling, codec negotiation, session refresh, REFER, and inbound DTMF.
- Proper handling of survey results for scenarios involving agent transfer, abandon, no response, partial response, complete response, voice response recording and playback, immediate transfer to supervisor, and multiple agents.

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

2.2. Test Results

All test cases were executed, and the following were observations on Survey:

- By design, Survey does not log the PSTN calling number as part of survey results. If required by customer, this can be accomplished via scripting changes on Survey.
- Survey does not support SRTP nor SDP capability negotiation. As such, the compliance testing used a separate set of network region and codec set in Communication Manager for integration with Survey.

2.3. Support

Technical support on Survey can be obtained through the following:

- **Phone:** (800) 540-7292
- **Web:** <http://engage.opentext.com/products/qfiniti>

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**, with “**dr220.com**” being the domain name. The configuration of Session Manager is performed via the web interface of System Manager. The detailed administration of basic connectivity between Communication Manager, Application Enablement Services, System Manager, Session Manager, and of call center devices are not the focus of these Application Notes and will not be described.

In the compliance testing, Survey monitored the skill groups and agent station extensions shown in the table below.

Device Type	Extension
Skill Group	61001, 61002
Agent Station	65001 (H.323), 66006 (SIP)
Agent ID	65881, 65882
Supervisor Station	65000

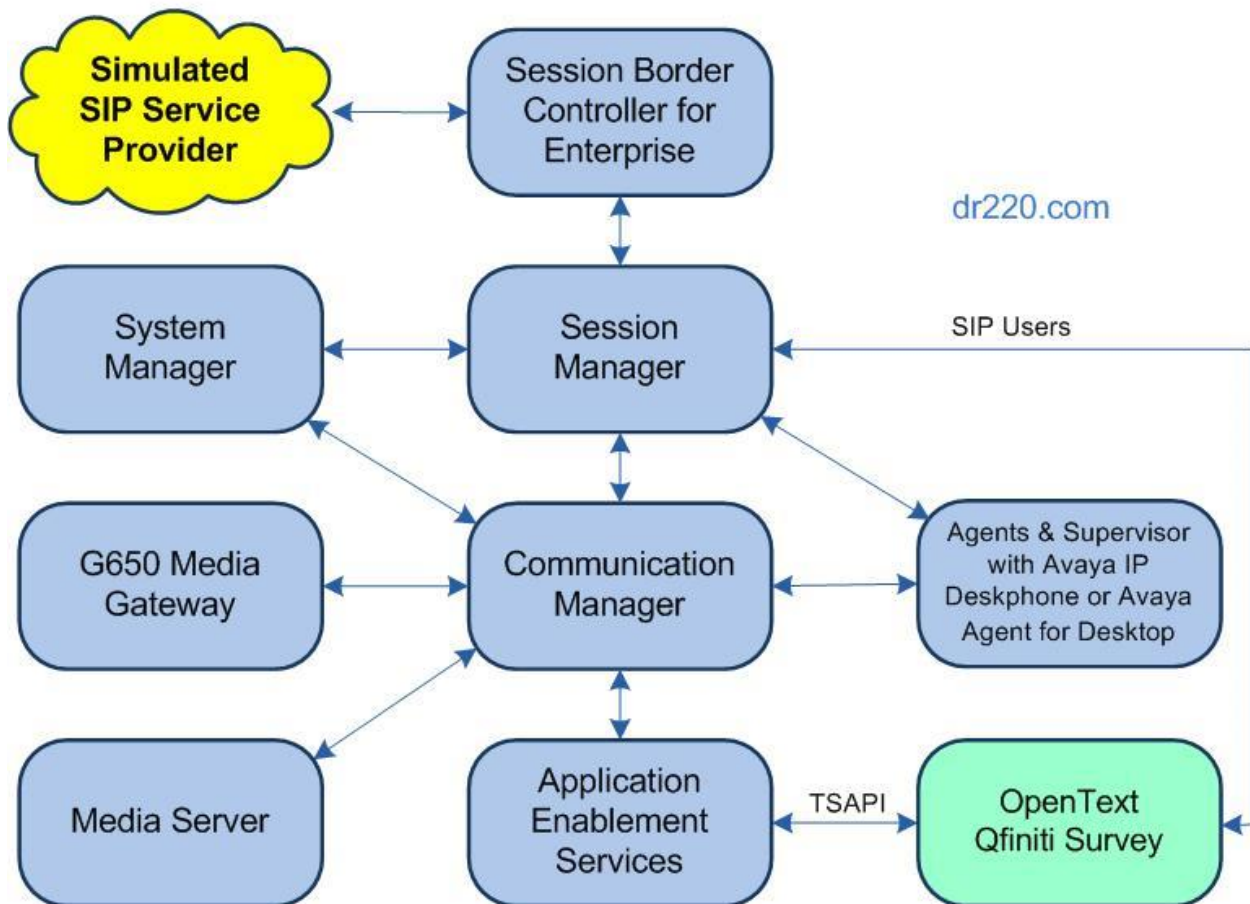


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	8.1.3 (8.1.3.3.1.890.27168)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	8.0.2.200
Avaya Aura® Application Enablement Services in Virtual Environment	8.1.3.3.0.4-0
Avaya Aura® Session Manager in Virtual Environment	8.1.3 (8.1.3.3.813310)
Avaya Aura® System Manager in Virtual Environment	8.1.3 (8.1.3.3.1013878)
Avaya Session Border Controller for Enterprise in Virtual Environment	8.1.2 (8.1.2.0-31-19809)
Avaya Agent for Desktop (H.323 & SIP)	2.0.6.17.3006
Avaya J179 & 9611G IP Deskphone (H.323)	6.8511
Avaya J169 IP Deskphone (SIP)	4.0.10.3.2
OpenText Qfiniti on Microsoft Windows Server 2019 <ul style="list-style-type: none">Avaya TSAPI Windows Client (csta32.dll)	20.4.0 with QF-18193 & QF-18501 Standard 8.1.3.25

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.

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: 60111	
Type: ADJ-IP	
COR: 1	
Name: AES CTI Link	
Unicode Name? n	

5.3. Administer Hunt Group

After the virtual SIP users have been created in **Section 7.3**, add a hunt group with virtual SIP users as members to route calls to Survey. Use the “**add hunt-group n**” command, where “**n**” is an available hunt group number. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Group Number:** The available group number.
- **Group Name:** A descriptive name.
- **Group Extension:** An available extension number.

add hunt-group 3	Page 1 of 60
HUNT GROUP	
Group Number: 3	ACD? n
Group Name: Survey Agent Transfer	Queue? n
Group Extension: 61003	Vector? n
Group Type: ucd-mia	Coverage Path:
TN: 1	Night Service Destination:
COR: 1	MM Early Answer? n
Security Code:	Local Agent Preference? n
ISDN/SIP Caller Display:	

Navigate to **Page 3** and enter extensions of all virtual SIP users from **Section 7.3** as members.

add hunt-group 3	Page 3 of 60		
HUNT GROUP			
Group Number: 3	Group Extension: 61003	Group Type: ucd-mia	
Member Range Allowed: 1 - 1500	Administered Members (min/max): 0 /0		
Total Administered Members: 0			
GROUP MEMBER ASSIGNMENTS			
Ext	Name(16 characters)	Ext	Name(16 characters)
1: 66991		14:	
2: 66992		15:	
3:		16:	

5.4. Administer Codec Set

Administer a codec set for integration with Survey. Use the “**change ip-codec-set n**” command, where “**n**” is an existing codec set number to use for interoperability.

For **Audio Codec**, enter the pertinent G.711 variant as shown below. Note that G.711 is the only codec type supported by Survey. For **Media Encryption** and **Encrypted SRTCP**, enter “**none**” and “**enforce-unenc-srtcp**” as shown below. Retain the default values for the remaining fields.

change ip-codec-set 3				Page	1 of	2
IP MEDIA PARAMETERS						
Codec Set: 3						
	Audio	Silence	Frames	Packet		
	Codec	Suppression	Per Pkt	Size(ms)		
1:	G.711MU	n	2	20		
2:						
3:						
4:						
5:						
6:						
7:						
Media Encryption				Encrypted SRTCP: enforce-unenc-srtcp		
1:	none					

5.5. Administer Network Region

Administer a network region for integration with Survey. Use the “**change ip-network-region n**” command, where “**n**” is an existing network region number to use for interoperability.

Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Authoritative Domain:** The SIP domain from **Section 3**.
- **Name:** A descriptive name.
- **Codec Set:** The codec set number from **Section 5.4**.

Enter “**no**” for **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio**.

change ip-network-region 3		Page	1 of	20
IP NETWORK REGION				
Region: 3	NR Group: 3			
Location:	Authoritative Domain: dr220.com			
Name: Survey	Stub Network Region: n			
MEDIA PARAMETERS	Intra-region IP-IP Direct Audio: no			
Codec Set: 3	Inter-region IP-IP Direct Audio: no			
UDP Port Min: 2048	IP Audio Hairpinning? n			
UDP Port Max: 3329				
DIFFSERV/TOS PARAMETERS				
Call Control PHB Value: 46				

Navigate to **page 4**, locate the entry associated with the network region assigned to the agent stations, in this case “1”. For **codec set**, enter the codec set value from above as shown below, to enable the Survey codec set to be used for calls with agent stations.

change ip-network-region 3									
Page 4 of 20									
Source Region: 3 Inter Network Region Connection Management									
I M									
G A t									
dst	codec	direct	WAN-BW-limits	Video	Intervening	Dyn	A	G	c
rgn	set	WAN	Units	Total Norm	Prio Shr	Regions	CAC	R	L
1	3	y	NoLimit					n	t
2									
3	3							all	
4									
5									
6									

5.6. Administer Network Region Map

Use the “**change ip-network-map**” command to map virtual SIP users to the network region configured for integration with Survey.

For **IP Address**, enter IP address of the Survey server. For **Network Reg**, enter the network region number from **Section 5.5**.

change ip-network-map									
Page 1 of 63									
IP ADDRESS MAPPING									
Subnet Network Emergency									
IP Address Bits Reg VLAN Location Ext									

FROM: 10.64.101.202	/	3	n						
TO: 10.64.101.202									
FROM:	/		n						
TO:									

6. Configure Avaya Aura® Application Enablement Services

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

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer Survey user
- Administer security database
- Restart services

6.1. Launch OAM Interface

Access the OAM web-based interface by using the URL “**https://ip-address**” in an Internet browser window, where “**ip-address**” is the IP address of the Application Enablement Services server.

The **Please login here** screen is displayed. Log in using the appropriate credentials.



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" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A red horizontal bar spans the width of the page, with the word "Help" in white text on the right side. In the center of the page is a light gray rectangular box containing the text "Please login here:" followed by a label "Username" and a text input field. Below the input field is a "Continue" button. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2020 Avaya Inc. All Rights Reserved." is displayed.

The **Welcome to OAM** screen is displayed next.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A red navigation bar at the top contains "Home", "Help", and "Logout" links. On the left, a sidebar lists various services: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled "Welcome to OAM" and provides an overview of the OAM web interface, listing the administrative domains it manages: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. It also mentions that these domains can be managed by a single administrator or separate administrators.

Welcome: User
Last login: Tue Jan 18 15:44:45 2022 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.3.0.4-0
Server Date and Time: Tue Jan 18 16:50:09 EST 2022
HA Status: Not Configured

Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

6.2. Verify License

Select **Licensing** → **WebLM Server Access** in the left pane, to display the applicable WebLM server log in screen (not shown). Log in using the appropriate credentials and navigate to display installed licenses (not shown).

The screenshot displays the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the left sidebar. The main content area is titled "Licensing" and provides instructions on how to set up and maintain the WebLM, including the need to use the following: WebLM Server Address, WebLM Server Access, and Reserved Licenses. It also mentions that if you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following: Reserved Licenses.

Welcome: User
Last login: Tue Jan 18 15:44:45 2022 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.3.0.4-0
Server Date and Time: Tue Jan 18 16:50:09 EST 2022
HA Status: Not Configured

Licensing | Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
WebLM Server Address
WebLM Server Access
Reserved Licenses
Maintenance
Networking

Licensing

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

- WebLM Server Address

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

- WebLM Server Access

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

- Reserved Licenses

Select **Licensed products** → **APPL_ENAB** → **Application_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users**, as shown below.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The left pane displays a navigation tree with the following structure:

- Home
- Licenses
 - WebLM Home
 - Install license
 - Licensed products
 - APPL_ENAB
 - Application_Enablement
 - View by feature
 - View by local WebLM
 - Enterprise configuration
 - Local WebLM Configuration
 - Usages
 - Allocations
 - Periodic status
 - ASBCE
 - Session_Border_Controller_E_AE
 - Avaya_Proactive_Contact
 - ContactCenter
 - CCTR
 - ContactCenter
 - COMMUNICATION_MANAGER

The right pane displays the **Application Enablement (CTI) - Release: 8 - SID: 10503000 (Enterprise license)** screen. The breadcrumb trail is: **You are here: Licensed Products > Application_Enablement > View by Feature**. The license was installed on **August 8, 2019 4:43:51 PM -05:00**. The **License File Host IDs** are **VE-83-02-2D-26-52-01**.

Feature (License Keyword)	License Capacity
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	1000
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	16
Device Media and Call Control (VALUE_AES_DMCC_DMC)	1000
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	3
DLG (VALUE_AES_DLG)	16
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	1000
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	3
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	16

6.3. Administer TSAPI Link

Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.

The screenshot shows the Avaya Management Console interface. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left sidebar shows a navigation tree with "AE Services" expanded, and "TSAPI Links" selected. The main content area displays the "TSAPI Links" screen, which includes a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
------	-------------------	-------------------	-------------------	----------

Buttons: Add Link, Edit Link, Delete Link

The **Add TSAPI Links** screen is displayed next. The **Link** field is only local to the Application Enablement Services server and may be set to any available number.

For **Switch Connection**, select the relevant switch connection from the drop-down list, in this case "cm7". For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**.

Retain the default value for **ASAI Link Version** and set **Security** to the desired value, in this case "Both" to allow for both encrypted and non-encrypted connections.

The screenshot shows the "Add TSAPI Links" screen in the Avaya Management Console. The left sidebar is the same as the previous screenshot. The main content area displays the "Add TSAPI Links" form, which includes fields for Link, Switch Connection, Switch CTI Link Number, ASAI Link Version, and Security. The values entered are: Link (1), Switch Connection (cm7), Switch CTI Link Number (1), ASAI Link Version (12), and Security (Both). Below the form are buttons for "Apply Changes", "Cancel Changes", and "Advanced Settings".

Form fields and values:

- Link: 1
- Switch Connection: cm7
- Switch CTI Link Number: 1
- ASAI Link Version: 12
- Security: Both

Buttons: Apply Changes, Cancel Changes, Advanced Settings

6.4. Administer Survey User

Select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane.

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select “Yes” from the drop-down list. Retain the default value in the remaining fields.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Jan 18 15:44:45 2022 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.3.0.4-0
Server Date and Time: Tue Jan 18 16:50:09 EST 2022
HA Status: Not Configured

User Management | User Admin | Add UserHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

■ Add User

■ Change User Password

■ List All Users

■ Modify Default Users

■ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Id

* Common Name

* Surname

* User Password

* Confirm Password

Admin Note

Avaya Role

Business Category

Car License

CM Home

Css Home

CT User

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

6.5. Administer Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Make certain that both parameters are unchecked, as shown below.

In the case that the security database is used by the customer with parameters already enabled, then follow reference [2] to configure access privileges for the Survey user from **Section 6.4**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A user welcome message is visible in the top right corner, indicating the user is logged in from 192.168.200.20. The main navigation pane on the left lists various services, with "Security" expanded to show "Security Database" and "Control". The right pane displays the "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" configuration page. This page contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is located below the checkboxes.

Welcome: User
Last login: Tue Jan 18 15:44:45 2022 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.3.0.4-0
Server Date and Time: Tue Jan 18 16:50:09 EST 2022
HA Status: Not Configured

Security | Security Database | Control

Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control

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

☐ Enable SDB for DMCC Service
☐ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services
Apply Changes

6.6. Restart Service

Select **Maintenance** → **Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check **TSAPI Service** and click **Restart Service**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows a tree structure with "Maintenance" expanded, and "Service Controller" selected. The main content area shows a table of services with their status. The "TSAPI Service" is checked, and the "Restart Service" button is highlighted.

Welcome: User
Last login: Tue Jan 18 15:44:45 2022 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.3.0.4-0
Server Date and Time: Tue Jan 18 16:50:09 EST 2022
HA Status: Not Configured

Maintenance | Service Controller Home | Help | Logout

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 checked="" 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

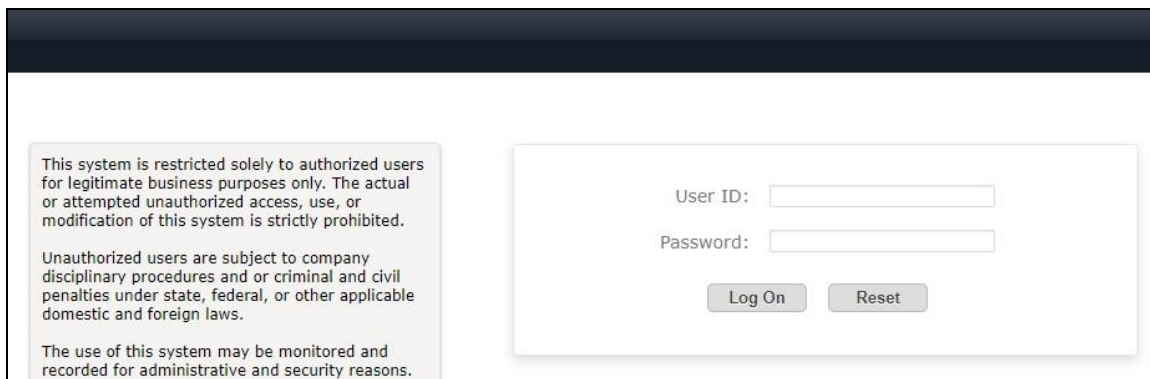
7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via the web interface of System Manager. The procedures include the following areas:

- Launch System Manager
- Administer SIP agent users
- Administer virtual SIP users
- Administer SIP entities

7.1. Launch System Manager

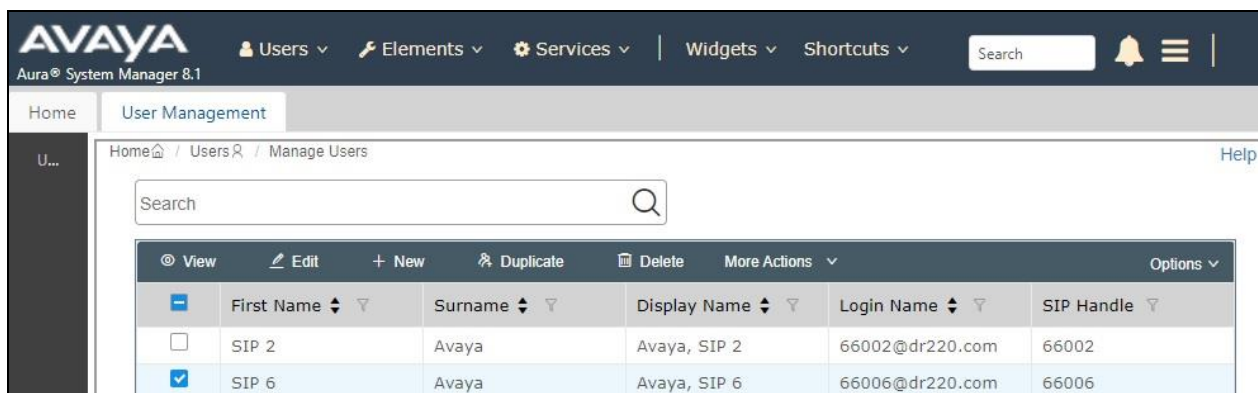
Access the System Manager web interface by using the URL “**https://ip-address**” in an Internet browser window, where “**ip-address**” is the IP address of System Manager. Log in using the appropriate credentials.



7.2. Administer SIP Agent Users

In the subsequent screen (not shown), select **Users → User Management** from the top menu. Select **User Management → Manage Users** (not shown) from the left pane to display the screen below.

Select the entry associated with the first SIP agent station from **Section 3**, in this case “**66006**”, and click **Edit**.



	First Name	Surname	Display Name	Login Name	SIP Handle
<input type="checkbox"/>	SIP 2	Avaya	Avaya, SIP 2	66002@dr220.com	66002
<input checked="" type="checkbox"/>	SIP 6	Avaya	Avaya, SIP 6	66006@dr220.com	66006

The **User Profile | Edit** screen is displayed. Select the **Communication Profile** tab, followed by **CM Endpoint Profile** to display the screen below.

Click on the **Editor** icon shown below.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, a search bar, and tabs for Users, Elements, Services, Widgets, and Shortcuts. The main content area is titled "User Profile | Edit | 66006@dr220.com" and features tabs for Identity, Communication Profile, Membership, and Contacts. The Communication Profile tab is active, and the left sidebar shows the "CM Endpoint Profile" selected. The main form contains various fields for user configuration, including System (DR-CM), Profile Type (Endpoint), Extension (66006), Set Type (J169CC), Port (S000115), and Voice Mail Number (admin). The "Extension" field has a blue "Editor" icon (a square with a pencil) next to it, which is highlighted with a red box.

The **Edit Endpoint** pop-up screen is displayed. For **Type of 3PCC Enabled**, select “Avaya” as shown below.

Repeat this section for all SIP agent stations from **Section 3**. In the compliance testing, one SIP agent station was configured.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and notification bell are also present. The main content area is titled 'Edit Endpoint' and includes a 'Done' button and a '[Save As Template]' link. The configuration fields are organized into two columns:

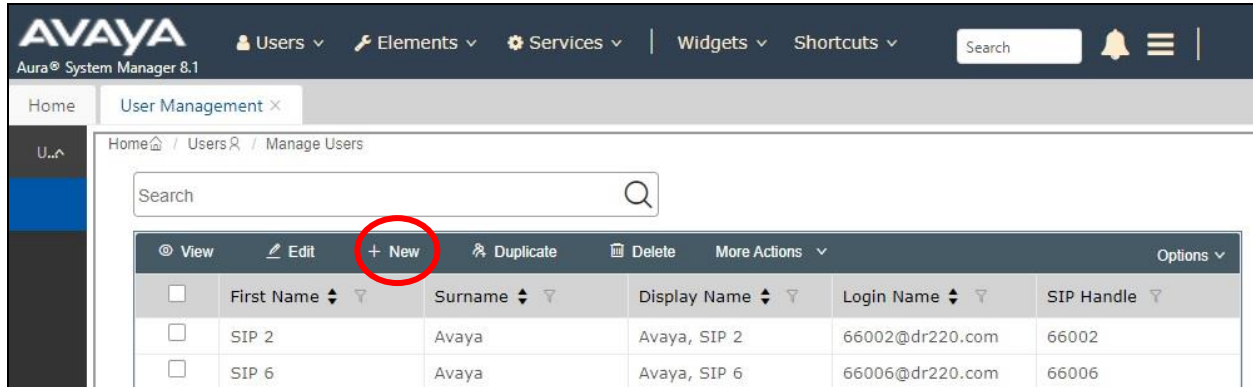
Field	Value	Field	Value
System	DR-CM	Extension	66006
Template	Select	Set Type	J169CC
Port	S000115	Security Code	
Name	Avaya, SIP 6		

Below these fields are several tabs: General Options (G), Feature Options (F), Site Data (S), Abbreviated Call Dialing (A), Enhanced Call Fwd (E), Button Assignment (B), Profile Settings (P), and Group Membership (M). The 'General Options (G)' tab is active, showing various settings:

Field	Value	Field	Value
* Class of Restriction (COR)	1	* Class Of Service (COS)	1
* Emergency Location Ext	66006	* Message Lamp Ext.	66006
* Tenant Number	1		
* SIP Trunk	Qaar	Type of 3PCC Enabled	Avaya
Coverage Path 1		Coverage Path 2	
Lock Message	<input type="checkbox"/>	Localized Display Name	Avaya, SIP 6
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system
SIP URI			

7.3. Administer Virtual SIP Users

From the left pane, select **User Management** → **Manage Users** (not shown) to display the **Managed Users** screen again. Click **New** to add a user.



7.3.1. Identity

The **User Profile | Add** screen is displayed. Enter desired **Last Name** and **First Name**.

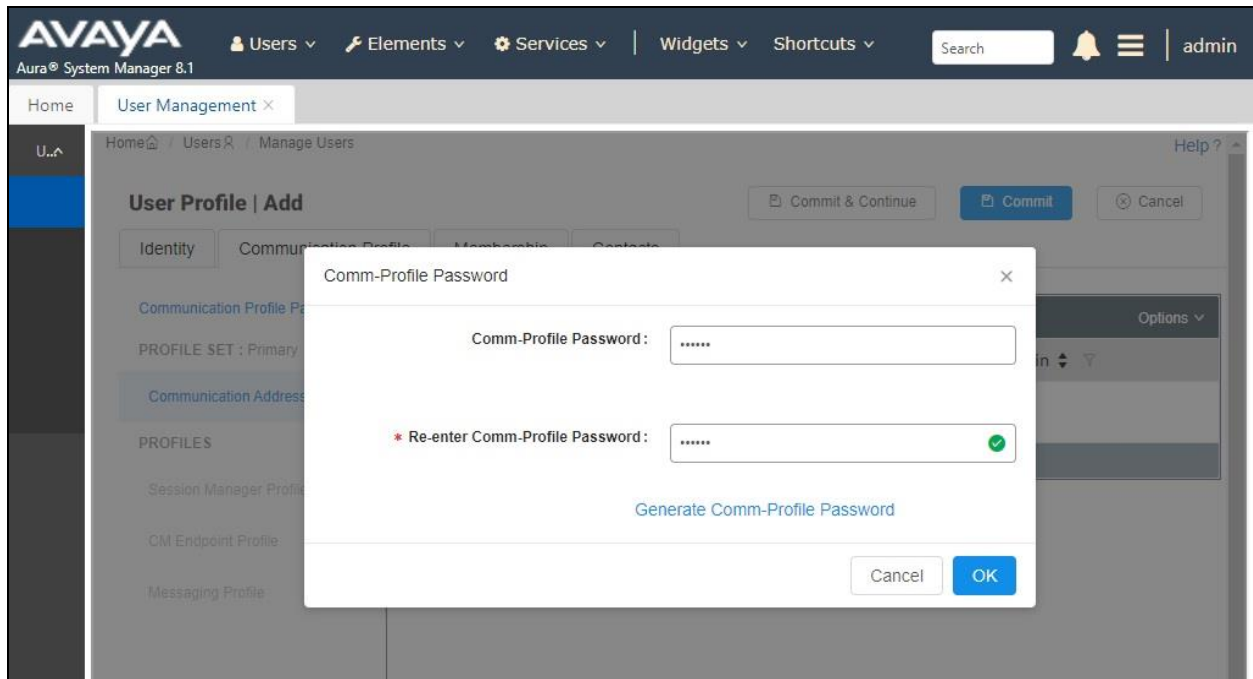
For **Login Name**, enter “**x@y**”, where “**x**” is an available user extension and “**y**” is the applicable domain name from **Section 3**. Retain the default values in the remaining fields.

The screenshot shows the 'User Profile | Add' screen. The 'Identity' tab is selected. The 'Basic Info' section is active. Fields include: User Provisioning Rule (dropdown), Last Name (Survey), First Name (SIP1), Login Name (66991@dr220.com), Description (Description Of User), Last Name (in Latin alphabet characters) (Survey), First Name (in Latin alphabet characters) (SIP1), Middle Name (Middle Name Of User), and Email Address (Email Address Of User). Buttons for 'Commit & Continue', 'Commit', and 'Cancel' are at the top right.

7.3.2. Communication Profile

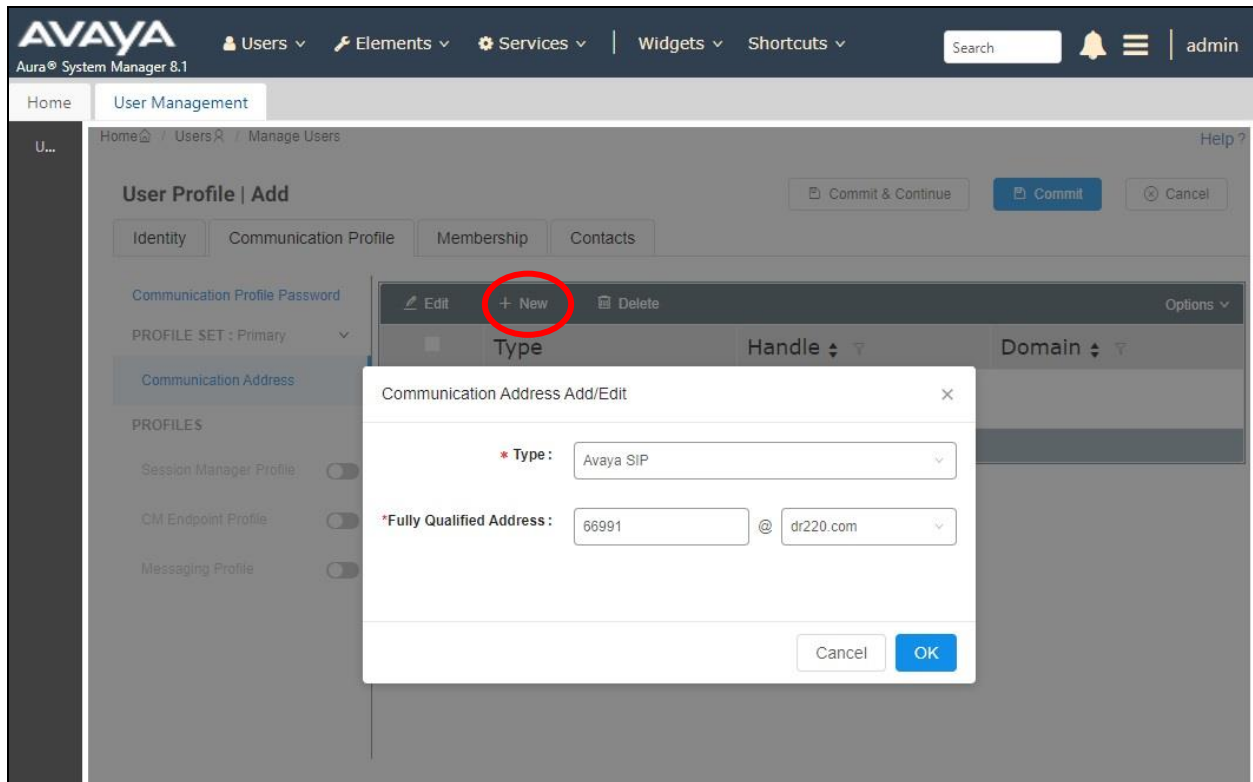
Select the **Communication Profile** tab, followed by **Communication Profile Password** to display the **Comm-Profile Password** pop-up box.

For **Communication-Profile Password** and **Re-enter Comm-Profile Password**, enter the desired password for the virtual SIP user to use for registration.



Select **Communication Address** from the left pane, followed by **New** to display the **Communication Address Add/Edit** pop-up box.

For **Type**, select “**Avaya SIP**”. For **Fully Qualified Address**, enter and select the SIP user extension and domain name to match the login name from **Section 7.3.1**.



Select **Session Manager Profile**. For **Primary Session Manager**, **Origination Sequence**, **Termination Sequence**, and **Home Location** (not shown), select values that correspond to applicable Session Manager and Communication Manager as shown below. Retain the default values in the remaining fields.

The screenshot displays the Avaya Aura System Manager 8.1 interface for adding a new user profile. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and tabs for Users, Elements, Services, Widgets, and Shortcuts. The main content area is titled 'User Profile | Add' and features four tabs: Identity, Communication Profile, Membership, and Contacts. The 'Communication Profile' tab is selected, showing a 'Communication Profile Password' section with a dropdown for 'PROFILE SET : Primary' and a 'Communication Address' field. Below this is a 'PROFILES' section with three toggles: 'Session Manager Profile' (checked), 'CM Endpoint Profile' (unchecked), and 'Messaging Profile' (unchecked). The 'SIP Registration' section contains fields for 'Primary Session Manager' (set to DR-SM), 'Secondary Session Manager' (Start typing...), 'Survivability Server' (Start typing...), and 'Max. Simultaneous Devices' (Select). A checkbox for 'Block New Registration When Maximum Registrations Active?' is also present. The 'Application Sequences' section shows 'Origination Sequence' and 'Termination Sequence' both set to DR220-CM-APP-Sequence. The left sidebar shows the 'Session Manager Profile' toggle is turned on.

Select **CM Endpoint Profile** from the left pane. For **System**, select value that corresponds to applicable Communication Manager. For **Template**, select “9641SIP_DEFAULT_CM_8_1”. For **Extension**, enter the SIP user extension from **Section 7.3.1**. Retain the default values in the remaining fields.

Click on the **Editor** icon shown below.

The screenshot shows the 'User Profile | Add' form in the Avaya Aura System Manager 8.1 interface. The form is divided into several sections: Identity, Communication Profile, Membership, and Contacts. The 'Communication Profile' section is active, showing fields for System (DR-CM), Profile Type (Endpoint), Extension (66991), Set Type (9641SIP), Security Code, Port (IP), Voice Mail Number, Preferred Handle, SIP URI, and Sip Trunk (aar). The 'Extension' field is highlighted with a red circle, and an editor icon (a blue square with a white pencil) is visible next to it. The 'System' field is set to 'DR-CM', 'Profile Type' is 'Endpoint', 'Set Type' is '9641SIP', 'Port' is 'IP', 'Sip Trunk' is 'aar', 'SIP URI' is 'Select', 'Calculate Route Pattern' is checked, 'Delete on Unassign from User or on Delete User' is checked, 'Allow H.323 and SIP Endpoint Dual Registration' is unchecked, 'Enhanced Callr-Info Display for 1-line phones' is unchecked, and 'Override Endpoint Name and Localized Name' is checked. The left pane shows the 'User Management' section with 'CM Endpoint Profile' selected. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'.

In the pop-up screen, locate the **Type of 3PCC Enabled** parameter, and select “**Avaya**” from the drop-down list as shown below. Retain the existing values in the remaining fields.

The screenshot shows the 'User Profile | Add' dialog box in the Avaya Aura System Manager. The 'General Options (G)' tab is active. The 'Type of 3PCC Enabled' dropdown is highlighted with a red box and set to 'Avaya'. Other fields include Class of Restriction (COR) set to 1, Emergency Location Ext. set to 66991, Tenant Number set to 1, SIP Trunk set to Qaar, and Class of Service (COS) set to 1.

Repeat **Section 7.3** to add the desired number of virtual SIP users. In the compliance testing, two SIP users with extensions “**66991**” and “**66992**” were created for two simultaneous connections to Survey.

The screenshot shows the 'User Management' page in the Avaya Aura System Manager. A table lists the created users. The last two rows, SIP1 and SIP2, are highlighted with a red box.

View	Edit	New	Duplicate	Delete	More Actions	Options
	First Name	Surname	Display Name	Login Name	SIP Handle	
<input type="checkbox"/>	SIP 2	Avaya	Avaya, SIP 2	66002@dr220.com	66002	
<input type="checkbox"/>	SIP 6	Avaya	Avaya, SIP 6	66006@dr220.com	66006	
<input type="checkbox"/>	SIP1	Survey	Survey, SIP1	66991@dr220.com	66991	
<input type="checkbox"/>	SIP2	Survey	Survey, SIP2	66992@dr220.com	66992	

7.4. Administer Session Manager Entity

Select **Elements** → **Routing** → **SIP Entities** from the top menu to display the **Routing** tab, followed by the applicable SIP entity for Session Manager from the left pane (not shown), in this case “**DR-SM**”. The **SIP Entity Details** screen is displayed.

The screenshot shows the AVAYA Aura System Manager 8.1 interface. The top navigation bar includes the AVAYA logo, "Aura® System Manager 8.1", and menu items: Users, Elements, Services, Widgets, and Shortcuts. A search bar and a notification bell are on the right. The left sidebar shows a tree view with "Routing" selected. The main content area is titled "SIP Entity Details" and includes "Commit" and "Cancel" buttons. The "General" sub-section contains the following fields:

- Name:** DR-SM
- IP Address:** 10.64.101.238
- SIP FQDN:** (empty)
- Type:** Session Manager (dropdown)
- Notes:** TLT DR SM
- Location:** DR-Loc (dropdown)
- Outbound Proxy:** (empty dropdown)
- Time Zone:** America/New_York (dropdown)
- Minimum TLS Version:** Use Global Setting (dropdown)
- Credential name:** (empty)

Scroll down to **Listen Ports** sub-section and verify that the transport protocol to be used by Survey is specified in the list, in this case “**UDP**”. Also verify that the corresponding **Endpoint** column is checked, as shown below.

The screenshot shows the AVAYA Aura System Manager 8.1 interface, specifically the "Listen Ports" sub-section. It includes "Add" and "Remove" buttons and a "3 Items" indicator. The table below lists the configured listen ports:

<input type="checkbox"/>	Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/>	5060	TCP	dr220.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5060	UDP	dr220.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5061	TLS	dr220.com	<input checked="" type="checkbox"/>	

Below the table, there is a "Select : All, None" option.

8. Configure OpenText Qfiniti Survey

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

- Launch SysConfig web interface
- Administer switches
- Administer CTI server
- Administer board configuration
- Administer general
- Administer machines
- Administer components
- Administer CTI sources
- Administer phone interface
- Administer VRM
- Administer line data
- Enable use
- Launch Qfiniti web interface
- Administer agents
- Administer triggers
- Administer alerts
- 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.

Prior to configuration, the pertinent Survey forms and questions are assumed to be pre-configured and ready for use.

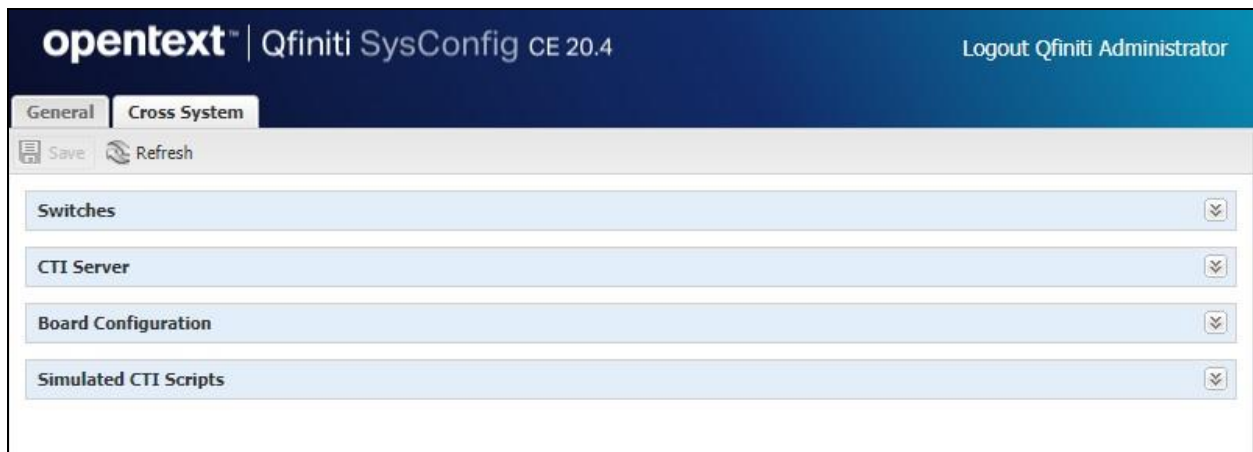
8.1. Launch SysConfig Web Interface

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 Qfiniti.

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

The image shows the login page of the Opentext SysConfig web interface. The background is a dark blue gradient. At the top center, the 'opentext' logo is displayed in white. Below the logo, the text 'Sign in to continue to qfiniti-system-configuration' is centered. There are two white input fields: the first is labeled 'User name' and the second is labeled 'Password'. Both labels are in a light gray font and positioned above their respective input fields.

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

The image shows the 'Cross System' tab of the Opentext SysConfig CE 20.4 web interface. The top header bar is dark blue with the 'opentext' logo on the left, 'Qfiniti SysConfig CE 20.4' in the center, and 'Logout Qfiniti Administrator' on the right. Below the header, there are two tabs: 'General' and 'Cross System', with 'Cross System' being the active tab. Under the tabs, there are two buttons: 'Save' and 'Refresh'. The main content area contains four expandable sections, each with a light blue header and a downward arrow icon on the right: 'Switches', 'CTI Server', 'Board Configuration', and 'Simulated CTI Scripts'.

8.2. Administer Switches

Expand the **Switches** sub-section and click the **New Item** icon to add a new entry for connection with Session Manager. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name, in this case “AvayaSM”.
- **Switch Model:** “SIP”
- **Interface Type:** “Network Tap”

The screenshot displays the OpenText Qfiniti SysConfig CE 20.4 web interface. The left sidebar shows the navigation menu with 'Switches' selected. The main content area is titled 'Switch' and contains a form for configuring a new switch. The form fields are as follows:

Field	Value
Name	AvayaSM
Switch Model	SIP
Vendor	
Post Release Delay	0
Observe Mode	-- select one --
Observe String	
Interface Type	Network Tap
Use CTI Source for Alias	<input type="checkbox"/>
Vlan Support	False
Trigger Type	Signaling
RTP Segmentation Rate (0-100)	20
Ring Timer (0-600)	5
Digit Collection (0-600)	5
Drop Duplicates	Do not drop duplicates
SIP Identifier	Call-ID
Transport	UDP
SIP Recording Type	None
SBC Recording Type	None
IP fragmentation	False
Extension IP Address Mapping	Default

On the right side of the interface, there is a pane with a '+ Add' button circled in red, indicating where to click to add a new switch entry.

8.3. Administer CTI Server

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

- **Name:** A descriptive name, in this case “AvayaTSAPI”.
- **Type:** “Avaya TSAPI”
- **Available Switch:** Select the switch name from **Section 8.2**.
- **ServerName:** The host name of Application Enablement Services.
- **User Name:** The Survey user credentials from **Section 6.4**.
- **Password:** The Survey user credentials from **Section 6.4**.
- **Vendor:** “AVAYA”
- **Driver:** The relevant switch connection name from **Section 6.3**.
- **Service:** “CSTA”

The screenshot displays the 'opentext | Qfiniti SysConfig CE 20.4' application window. The 'General' tab is selected, and the 'CTI Server' section is expanded in the left sidebar. A 'CTI Server' configuration dialog box is open, showing the following fields and values:

Field	Value
Name	AvayaTSAPI
Type	Avaya TSAPI
Available Switch	AvayaSM
ServerName	AES7
User Name	qfiniti
Password	*****
Vendor	AVAYA
Driver	CM7
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

The dialog box has 'Ok' and 'Cancel' buttons at the bottom. In the background, the main interface shows a list of CTI Servers with a red circle highlighting the '+' icon for adding a new entry.

8.4. Administer Board Configuration

Expand the **Board Configuration** sub-section and click the **New Item** icon. 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)”
- **Active 1:** “True”
- **Network Card Identifier 1:** A desired value for identifier.
- **Network Card Description 1:** A desired description.
- **Network Card IP Address 1:** IP address of the Survey server.

The screenshot displays the Qfiniti SysConfig CE 20.4 application window. The 'Board Configuration' dialog box is open, showing a list of configuration fields. The 'Name' field is set to 'NIC', 'Model' is 'Network Interface Card (NIC)', 'Active 1' is 'True', 'Network Card Identifier 1' is 'Card 1', 'Network Card Description 1' is 'Card 1', 'Network Card IP Address 1' is '10.64.101.202', 'Network Card Port 1' is '5060', 'Active 2' is 'False', 'Network Card Identifier 2' is empty, 'Network Card Description 2' is empty, 'Network Card IP Address 2' is empty, 'Network Card Port 2' is '5060', 'Active 3' is 'False', 'Network Card Identifier 3' is empty, 'Network Card Description 3' is empty, 'Network Card IP Address 3' is empty, 'Network Card Port 3' is '5060', and 'Active 4' is 'False'. The 'Add' button is highlighted with a red circle. The background shows the 'General' tab selected in the left sidebar, with 'Board Configuration' highlighted under 'Cross System'.

Field	Value
Name	NIC
Model	Network Interface Card (NIC)
Active 1	True
Network Card Identifier 1	Card 1
Network Card Description 1	Card 1
Network Card IP Address 1	10.64.101.202
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

8.5. Administer General

Select the **General** tab. Expand the **General** sub-section and 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 “Survey System”.
- **Switch:** Select the switch name from **Section 8.2**.
- **System Type:** Check **Survey**.

The screenshot displays the OpenText Qfiniti SysConfig CE 20.4 web interface. The top navigation bar includes the 'General' and 'Cross System' tabs. The 'Systems' section on the left contains a 'Quick Find' search bar and a list of systems, including 'DMCC Logger'. The main content area is titled 'General' and contains the following fields and options:

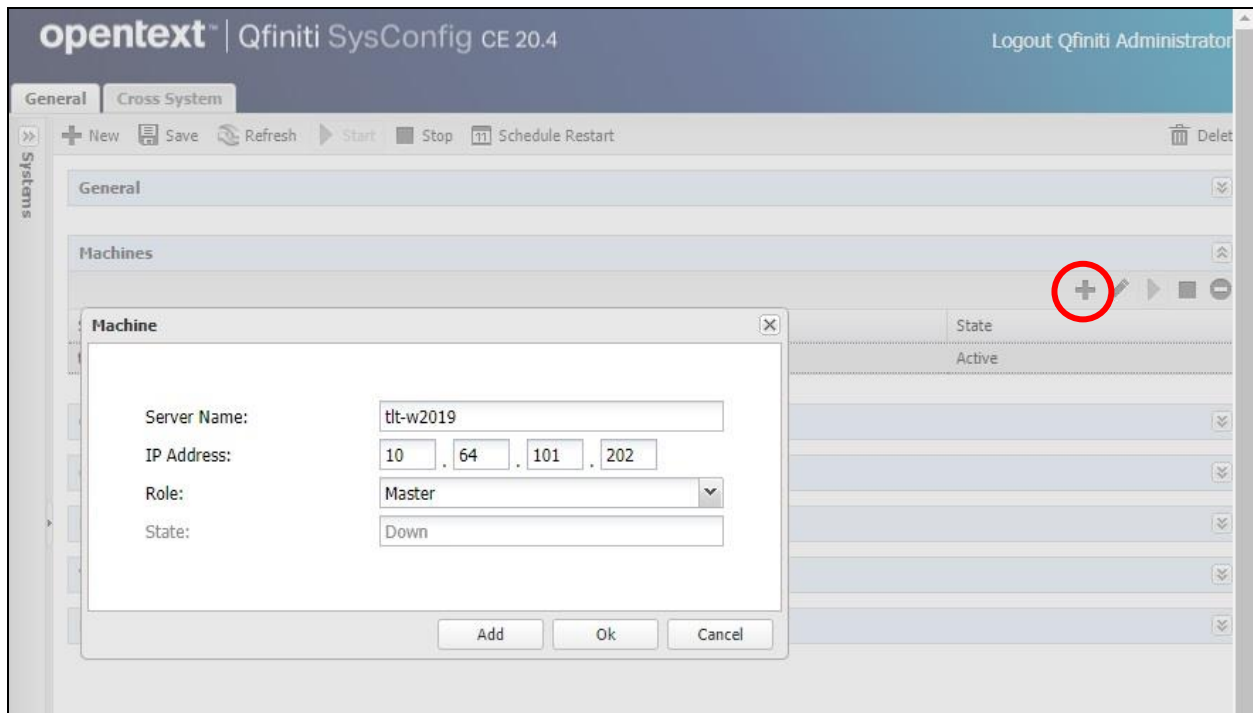
- Name:** A text input field containing 'Survey System'.
- Switch:** A dropdown menu with 'AvayaSM' selected.
- System Type:** A list of checkboxes with 'Survey' checked. Other options include 'Voice Recording - Logging', 'Voice Recording - QA', 'Screen Recording', 'Remote Screen Site', 'Explore', 'Backup', and 'Cloud Connector'.
- Description:** A large text area.
- Available for Use:** A checkbox with a help icon.
- NAT Environment:** A checkbox.

Below the 'General' section are expandable sections for 'Machines', 'Components', 'CTI Sources', 'Phone Interface', 'VRM', and 'Line Data'.

8.6. Administer Machines

Expand the **Machines** sub-section 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 Survey server.
- **IP Address:** The IP address of the Survey server.
- **Role:** “Master”.



8.7. Administer Components

Expand the **Components** sub-section and follow reference [4] to assign and configure the required components, including **Archive Manager**, **Qfiniti File Server**, and **Survey**.

For the **Survey** component under **Assigned Components**, scroll the section as necessary to enter the following values for the specified fields (not all are shown below) and retain the default values for the remaining fields. In the compliance testing, the **Default Route** was set to the first skill group extension in **Section 3**.

- **Survey Switch Type:** “Lucent Definity G3”
- **Default Route:** A desired route destination when there is no match on DNIS.
- **Dial String:** Blank out the default value.
- **Recording Path:** The pertinent directory path on Survey server for recordings.
- **Voice Message Path:** The pertinent directory path on Survey server for voice messages.
- **Front End Condition:** Set to “Disabled” when there is no separate front end IVR system.
- **SIP Registration Proxy:** IP address of Session Manager signaling interface.
- **SIP URI Address:** The SIP domain name from **Section 3**.

The screenshot displays the 'opentext | Qfiniti SysConfig CE 20.4' web interface. The top navigation bar includes 'General' and 'Cross System' tabs. The 'Systems' section on the left lists 'DMCC Logger', 'Survey System', and 'tlt-w2019'. The 'Survey' component is selected, showing its configuration details in the 'Component Data' section. The configuration fields are as follows:

Component Data	
Front End Condition:	Disabled
Enable Recordings:	Enabled
Call Handling:	Default Route
Default Trigger:	
CTI Init:	Individual
Inter Digit Delay:	3
SIP Registration Proxy:	10.64.101.238
SIP URI Address:	dr220.com
Starting RTP Port:	17384
Default Username:	
Default Password:	
Default Contact:	
Prompt Folder:	

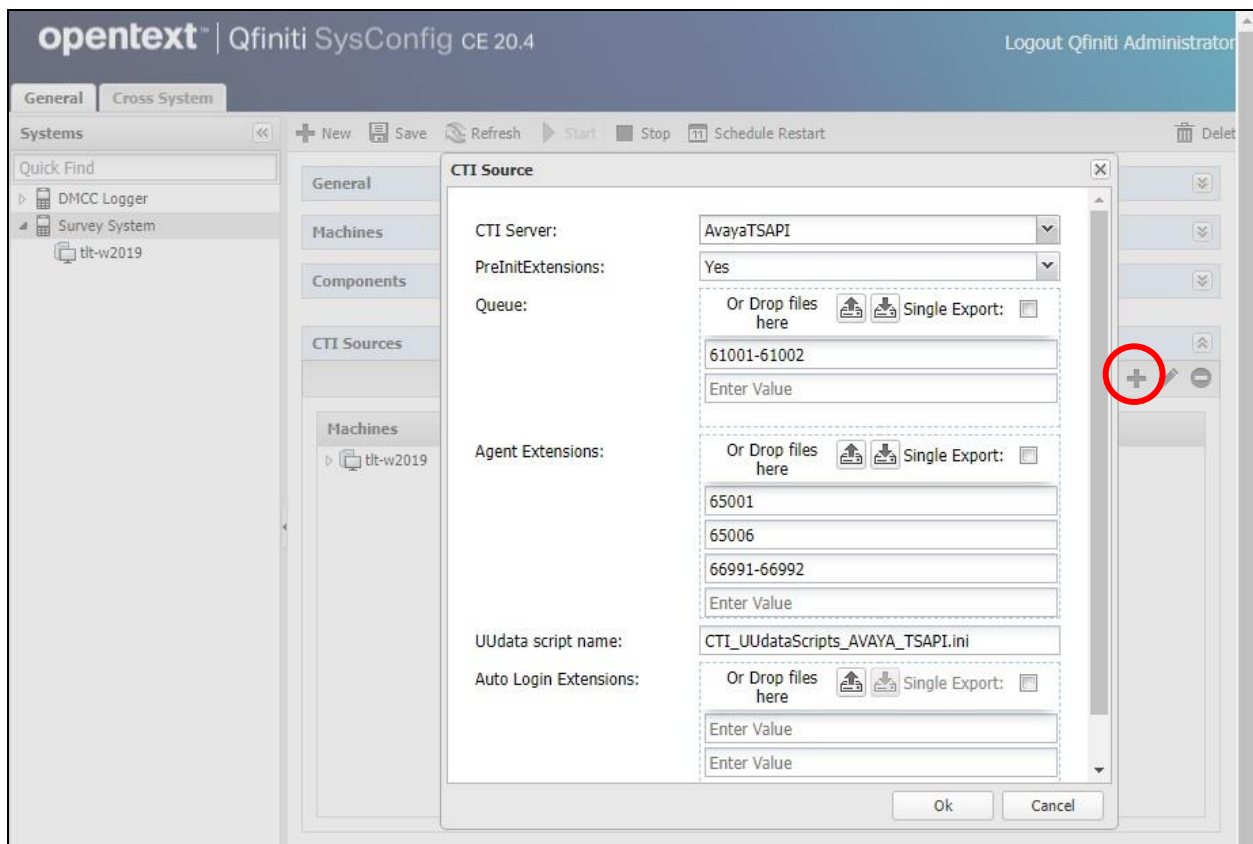
At the bottom, there is a 'CTI Sources' section with a dropdown arrow.

8.8. Administer CTI Sources

Expand the **CTI Sources** sub-section. Select the applicable machine server name from **Section 8.6**, 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 CTI server name from **Section 8.3**.
- **Queue:** The skill group extensions from **Section 3**.

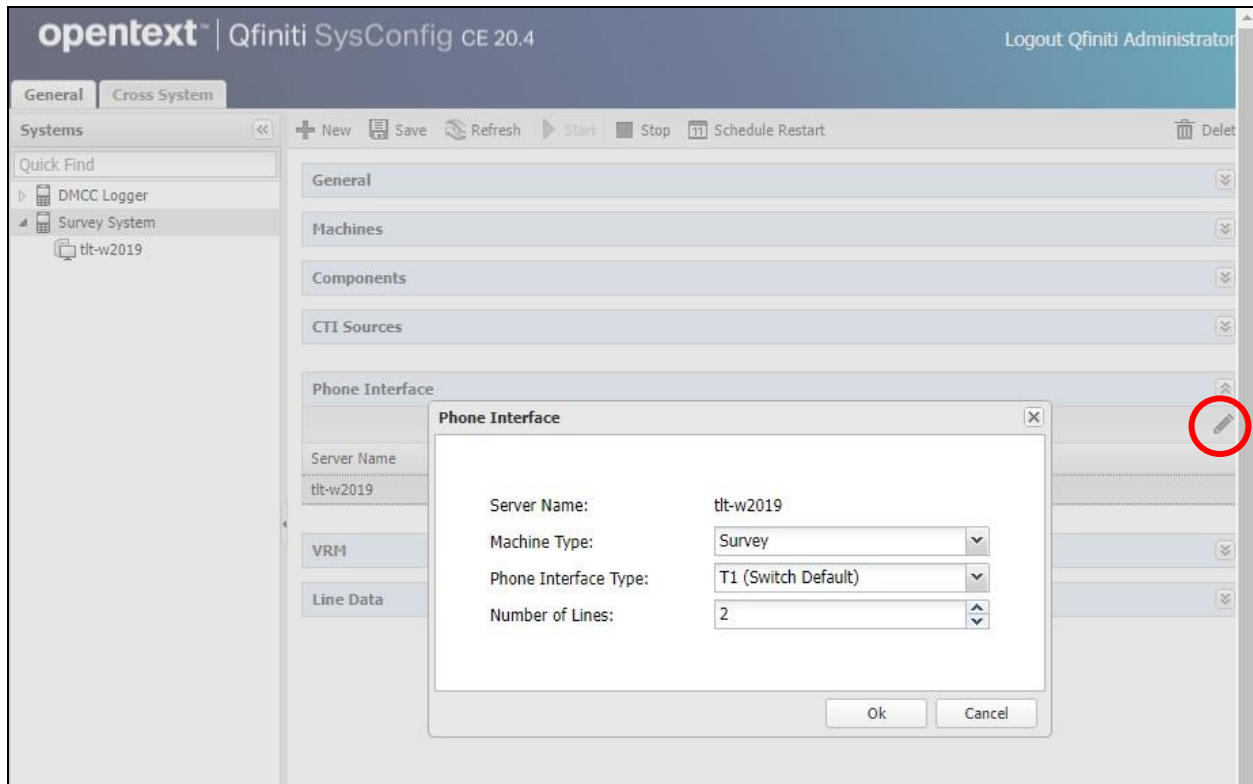
For **Agent Extensions**, enter the agent station extensions from **Section 3** and the virtual SIP user extensions from **Section 7.3**, as shown below.



8.9. Administer Phone Interface

Expand the **Phone Interface** sub-section (not shown). Select the machine server name from **Section 8.6**, 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.

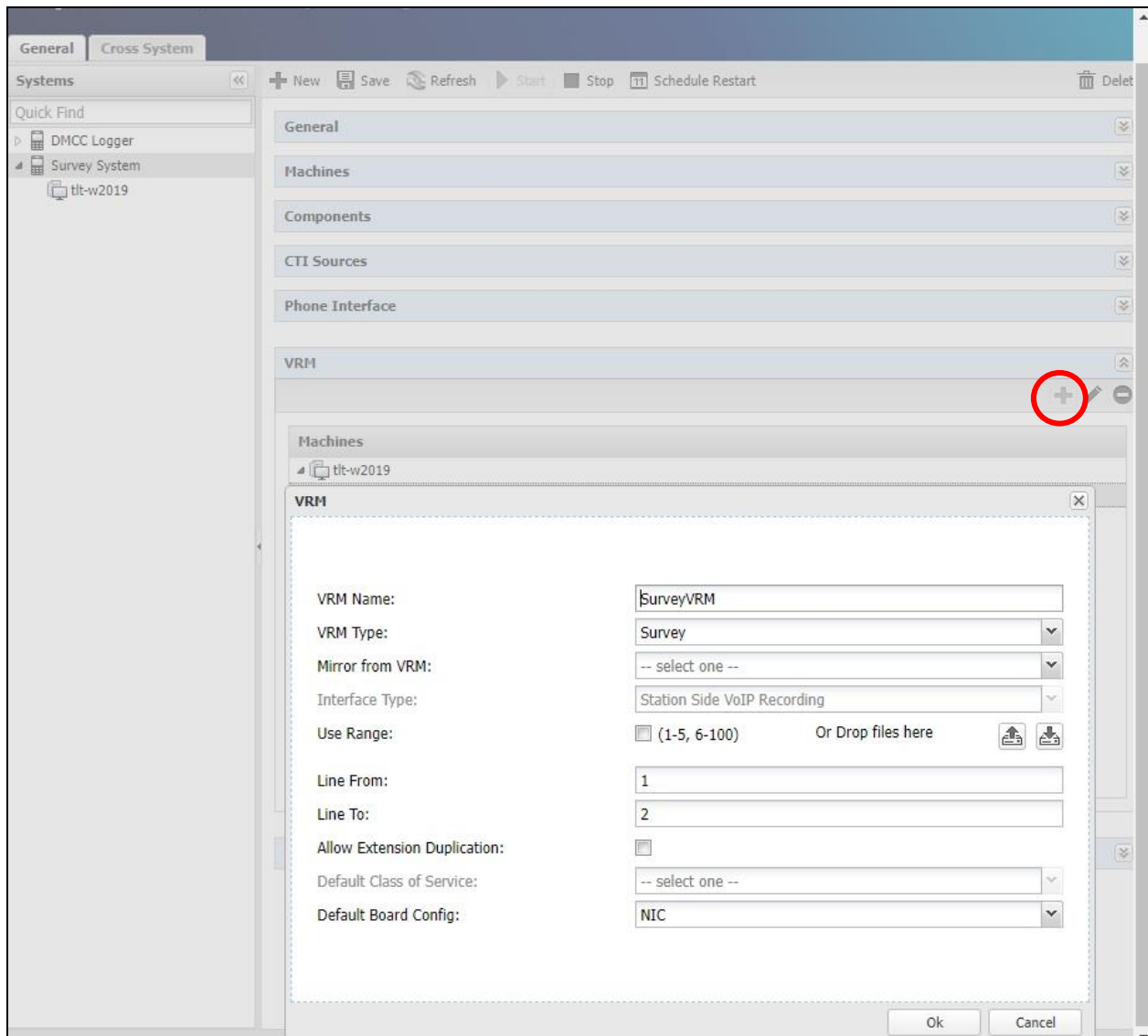
- **Machine Type:** “Survey”
- **Phone Interface Type:** “T1 (Switch Default)”
- **Number of Lines:** The total number of virtual SIP users from **Section 7.3**.



8.10. Administer VRM

Expand the **VRM** sub-section. Select the machine server name from **Section 8.6**, followed by the **Add VRM** icon. Enter the following values for the specified fields.

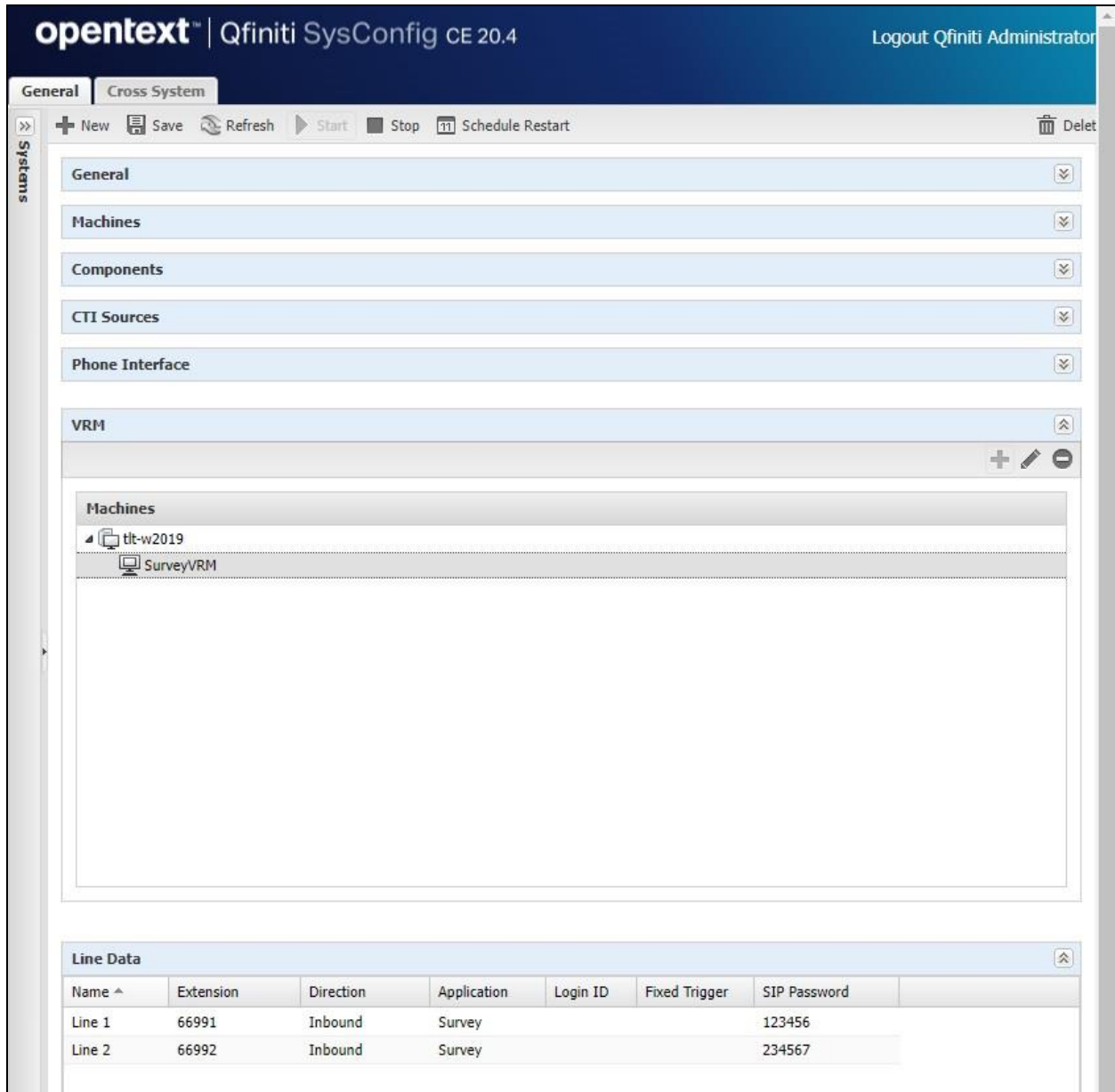
- **VRM Name:** A desired name, in this case “SurveyVRM”.
- **VRM Type:** “Survey”
- **Line From and Line To:** Range of virtual SIP users, in this case two users so “1” to “2”.
- **Default Board Config:** Select the board name from **Section 8.4**.



8.11. Administer Line Data

Select the newly added VRM from **Section 8.10**, and expand the **Line Data** sub-section. Select the first line. For **Extension** and **SIP Password**, enter the first virtual SIP user extension and the associated communication profile password from **Section 7.3** respectively. Retain the default values in the remaining fields.

Repeat this section to administer all virtual SIP users from **Section 7.3**, as shown below.



The screenshot shows the opentext Qfiniti SysConfig CE 20.4 interface. The 'General' tab is selected. The 'VRM' section is expanded, showing a list of machines. The 'Line Data' section is also expanded, displaying a table with two lines of data.

Name ^	Extension	Direction	Application	Login ID	Fixed Trigger	SIP Password
Line 1	66991	Inbound	Survey			123456
Line 2	66992	Inbound	Survey			234567

8.12. Enable Use

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

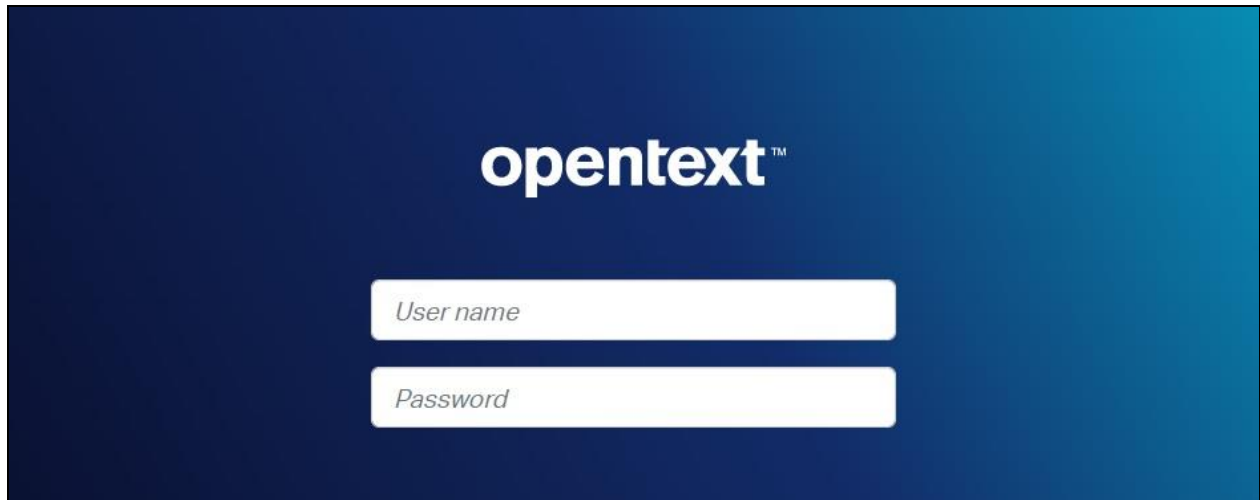
The screenshot displays the 'opentext | Qfiniti SysConfig CE 20.4' web interface. The top navigation bar includes a 'Logout Qfiniti Administrator' link. Below the header, there are tabs for 'General' and 'Cross System'. The left sidebar, titled 'Systems', shows a tree view with 'DMCC Logger' and 'Survey System' (expanded), with a sub-item 'tlt-w2019'. The main content area is titled 'General' and contains the following fields and options:

- Name:** Survey System
- Switch:** AvayaSM
- System Type:**
 - ☐ Voice Recording - Logging
 - ☐ Voice Recording - QA
 - ☐ Screen Recording
 - ☐ Remote Screen Site
 - ☐ Explore
 - ☒ Survey
 - ☐ Backup
 - ☐ Cloud Connector
- Description:** (empty text box)
- ☒ Available for Use (highlighted with a red box)
- ☐ NAT Environment

At the top of the main content area, there is a toolbar with buttons: New, Save, Refresh, Start, Stop, Schedule Restart, and Delete.

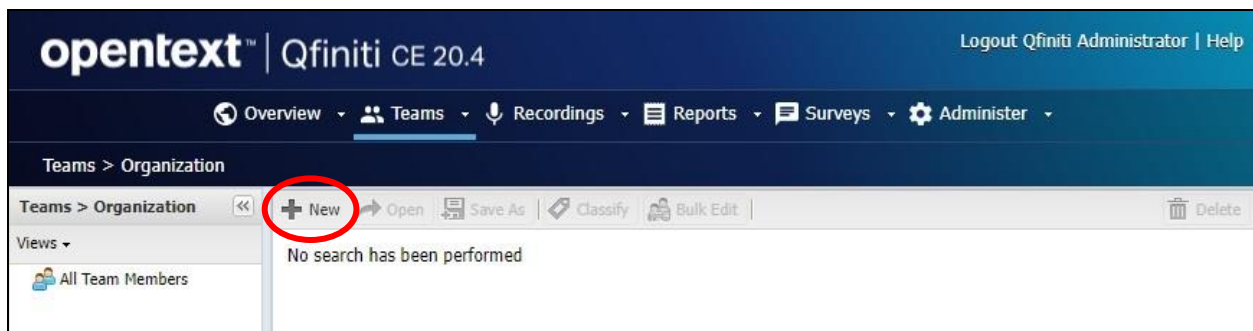
8.13. Launch Qfiniti Web Interface

Access the Qfiniti web interface by using the URL “**http://hostname/qwa**” in an Internet browser window, where “**hostname**” is the hostname of the Qfiniti server. The screen below is displayed. Log in using the appropriate credentials.



8.14. 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.



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

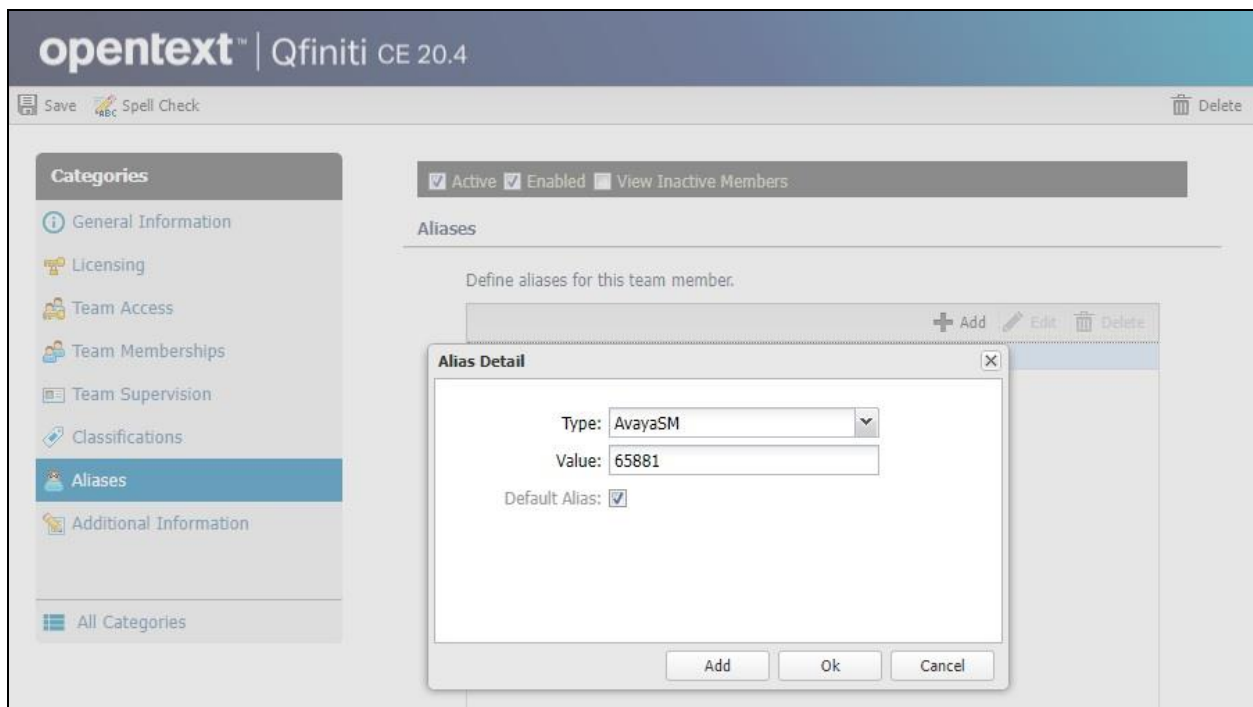
- **First Name:** A desired first name for the first agent from **Section 3**.
- **Last Name:** A desired last name for the first agent from **Section 3**.
- **Role:** Select a desired and existing role.
- **Username:** The desired login credentials for the agent.
- **Password:** The desired login credentials for the agent.
- **Confirm Password:** The same desired login credential for the agent.
- **Partition:** “Qfiniti”

The screenshot shows the OpenText Qfiniti CE 20.4 user management interface. The left sidebar contains a 'Categories' menu with options: General Information (selected), Licensing, Team Access, Team Memberships, Team Supervision, Classifications, Aliases, and Additional Information. The main content area is titled 'General Information' and includes a header with checkboxes for 'Active', 'Enabled', and 'View Inactive Members'. Below this, the 'Id' is 4. The form fields are: * First Name (Agent1), Middle Name (empty), * Last Name (Avaya), Email Address (empty), Role (Administrators), * Username (agent1), Password (masked), Confirm Password (masked), and * Partition (Qfiniti). There is an 'Add Role' button next to the Role dropdown.

Follow reference [4] to configure subsequent steps for the new agent (not shown). Upon reaching the **Aliases** step, click the **Add** icon to create an alias.

The screenshot shows the OpenText Qfiniti CE 20.4 user management interface, specifically the 'Aliases' tab. The left sidebar is the same as the previous screenshot, but 'Aliases' is now selected. The main content area is titled 'Aliases' and includes a header with checkboxes for 'Active', 'Enabled', and 'View Inactive Members'. Below this, the text 'Define aliases for this team member.' is displayed. A table is shown with a single row containing an 'Add' button (circled in red), an 'Edit' button, and a 'Delete' button.

The **Alias Detail** pop-up screen is displayed. For **Type**, select the switch server name from **Section 8.2**. For **Value**, enter the agent ID for the first agent in **Section 3**, in this case “**65881**”. Retain the default value in the remaining field.



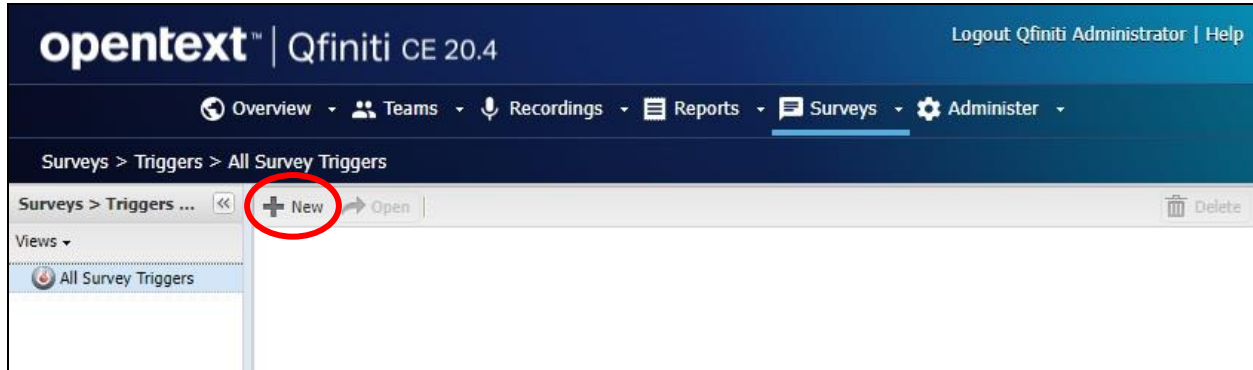
Repeat this section to add a team member for each agent from **Section 3**. In the compliance testing, two team members with alias values “**65881**” and “**65882**” were configured.

The screenshot shows the OpenText Qfiniti CE 20.4 interface with the 'Teams > Organization > All Team Members' view. The table below lists the team members:

First Name	Middle Name	Last Name	Login ID	Status	Account Disabled
Qfiniti		Administrator	administrator	Active	No
Agent1		Avaya	agent1	Active	No
Agent2		Avaya	agent2	Active	No

8.15. Administer Triggers

Select **Surveys** → **Triggers** from the top menu to display the screen below. Select the **New** icon in the right pane to add a trigger.



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

- **Name:** A descriptive trigger name, in this case “AgentTransferTrigger”.
- **DNIS:** The hunt group extension from **Section 5.3**.
- **Switch:** The switch name from **Section 8.2**.
- **Survey Form:** Select an existing survey form.

The screenshot shows the 'General Information' form for a new trigger in the Opentext Qfiniti CE 20.4 interface. The form is titled 'General Information' and has a 'Categories' sidebar on the left. The sidebar includes 'General Information' (selected), 'Trigger Type' (checked), and 'All Categories'. The main form area contains the following fields: '* Name: AgentTransferTrigger', '* DNIS: 61003', '* Switch: AvayaSM', '* Survey Form: Demo Form', and 'Survey Language: English'. There is a 'View Survey Form' button next to the 'Survey Form' field. At the bottom, there are two checkboxes: 'Play message 1988 "Survey Not Available" when this trigger is inactive' (unchecked) and 'Active' (checked). The top of the form has 'Save' and 'Spell Check' buttons.

Select **Trigger Type** from the left pane to display the **Trigger Type** screen. For **Type**, select “**Mode 2: Agent transfers caller to Survey**” as shown below. Retain the default values in the remaining fields.

opentext™ | Qfiniti CE 20.4

Save Spell Check

Categories

- General Information
- Trigger Type**
- All Categories

Trigger Type

Type: Mode 2: Agent transfers caller to Survey

Outbound Extension:

ANI Limit:

If call is Transferred: Do not offer a survey

Dial Mode: Standard Dial

☐ Record the call when this trigger activates a survey

☐ Limit the number of Completed Surveys generated

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
Max Per Day	0	0	0	0	0	0	0
Max Per Hour	0	0	0	0	0	0	0

8.16. Administer Alerts

Select **Surveys** → **Questions** from the top menu to display the list of pre-configured survey questions. Select the desired entry to set the criteria for immediate transfer to supervisor.

opentext™ | Qfiniti CE 20.4 Logout Qfiniti Administrator | Help

Overview Teams Recordings Reports Surveys Administer

Surveys > Questions > All Survey Questions

Surveys > Questio... << + New Open Save As Delete

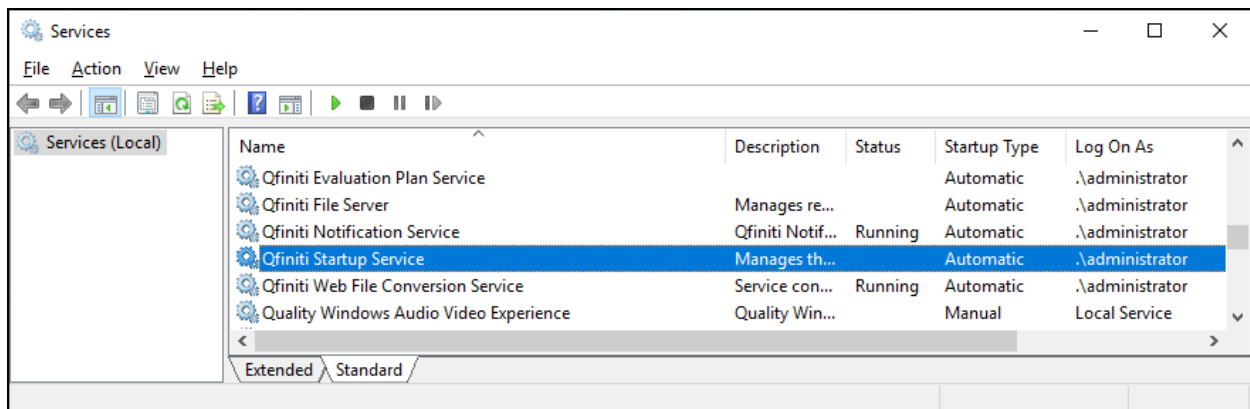
Question Name	Voice Question ...	Type	Prompt	Alert Type	Alert Data	Version
Press 1 to 5	Pres 1 2 3 4 or 5	Quantitative	2011	Transfer		2
Voice Message	Would you like t...	Comment	2012	Transfer		1
Yes or no	Yes or no	Yes/No	2010	Transfer		1

The screen below is displayed. Select **Inbound Alerts** in the left pane. For **Send an Alert if**, set the desired criteria. For **Alert Method**, set **Transfer Number** to the supervisor extension from **Section 3**.

The screenshot shows the 'opentext | Qfiniti CE 20.4' interface. On the left, a 'Categories' sidebar lists 'General Information', 'Web Question', 'Voice Question', 'Answer Choices', 'Inbound Alerts' (selected), and 'All Categories'. The main area is titled 'Inbound Alerts' with a 'Version: 2' indicator. It contains a 'Send an Alert if' section with a dropdown set to 'Greater Than Or Equal (>=)' and a numeric input set to '5'. Below this is an 'Alert Method' section with two radio buttons: 'Transfer Call' (selected) and 'Send email'. A text field labeled '* Transfer Number:' contains the value '65000'.

8.17. Start Services

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



9. Verification Steps

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

9.1. 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	aes7	established	31	29

9.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify status of the TSAPI service by selecting **Status** → **Status and Control** → **TSAPI Service Summary** (not shown) from the left pane. The **TSAPI Link Details** screen is displayed.

Verify that the **Status** is “**Talking**” for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the total number of monitored skill groups and agent stations from **Section 3** plus the total number of virtual SIP users from **Section 7.3**, in this case “**6**”.

**Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Feb 1 10:37:13 2022 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.3.0.4-0
Server Date and Time: Tue Feb 01 11:57:26 EST 2022
HA Status: Not Configured

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

TSAPI Link Details

☐ Enable page refresh every 60 seconds

Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
1	cm7	1	Talking	Mon Jan 31 13:52:13 2022	Online	18	6	29	31	30

OnlineOffline

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

TSAPI Service StatusTLink StatusUser Status

9.3. Verify Avaya Aura® Session Manager

From the System Manager Web interface, select **Elements → Session Manager → System Status → User Registrations** to display the **User Registrations** screen.

Verify that all virtual SIP users from **Section 7.3** are registered, as shown below with a checkmark in the **Registered Prim** column.

Help ?

User Registrations

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

View ▾

Default

Export

Force Unregister

AST Device Notifications:

Reboot

Reload ▾

Fallback

As of 10:35 AM

Advanced Search ▾

Customize ▾

7 Items

Show ▾

Filter: Enable

<input type="checkbox"/>	Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered			
											Prim	Sec	Surv	Visiting
<input type="checkbox"/>	▶ Show	66006@dr220.com	SIP 6	Avaya	DR-Loc	192.168.200.169	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	▶ Show	66991@dr220.com	SIP1	Survey	DR-Loc	10.64.101.202	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	▶ Show	66992@dr220.com	SIP2	Survey	DR-Loc	10.64.101.202	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

9.4. Verify OpenText Qfiniti Survey

Establish an ACD call from PSTN with an available agent. At end of ACD call, agent uses the phone to perform unsupervised transfer of PSTN caller to the Survey hunt group. Verify that PSTN caller hears the first Survey question and can use DTMF to respond to quantitative questions and leave voice messages for open-ended questions to complete the survey.

From the Qfiniti web interface, select **Surveys → Survey Results**, followed by **Todays Completed Surveys** (not shown) in the left pane to display the screen below. Verify that there is an entry corresponding to last survey with proper values in the pertinent fields. Double click on the entry.



Sur...	Survey Date	DNIS	Inbo...	ANI	Login...	First ...	Last ...	Mode	Voice ...	Status
	02/01/2022 1:25:00 PM	61003	66991	65001	65881	Agent1	Avaya	Call Transfer	Yes	Survey Completed

Verify that a pop-up screen is displayed with proper captured response for each survey question as shown below. Click on the **Play** option associated with **Voice Message**.

opentext™ | Qfiniti CE 20.4

Save Play Classify Delete

Name	Survey Type	Date:	Team Member Name:	DNIS:
Demo Form (Version:2)	Inbound	2/1/2022 1:25:31 PM	Avaya, Agent1	61003

- 1: Press 1 to 5
Pres 1 2 3 4 or 5 3
- 2: Yes or no
Yes or no Yes
- 3: Voice Message
Would you like to leave a voice message?

Delete Transcript **Play**

Verify that the voice response left by the PSTN caller can be played back.



10. Conclusion

These Application Notes describe the configuration steps required for OpenText Qfiniti Survey 20.4 to successfully interoperate with Avaya Aura® Communication Application Enablement Services 8.1.3 and Avaya Aura® Session Manager 8.1.3. All feature and serviceability test cases were completed with observations 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 8.1.x, Issue 12, July 2021, available at <http://support.avaya.com>.
2. *Administering Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 12, October 2021, available at <http://support.avaya.com>.
3. *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 10, September 2021, available at <http://support.avaya.com>.
4. *OpenText Qfiniti Survey Configuration Guide*, Rev. 2019-Nov-14, available to existing customers at <https://knowledge.opentext.com/knowledge/llisapi.dll>.

©2022 Avaya Inc. All Rights Reserved.

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

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