



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

---

# **Application Notes for OpenText Qfiniti 20.4 with Avaya Proactive Contact 5.2 with PG230 and Avaya Aura® Application Enablement Services 8.1.3 – Issue 1.0**

## **Abstract**

These Application Notes describe the configuration steps required for OpenText Qfiniti 20.4 to interoperate with Avaya Proactive Contact 5.2 with PG230 and Avaya Aura® Application Enablement Services 8.1.3. OpenText Qfiniti is a call recording solution.

In the compliance testing, OpenText Qfiniti used the Event Services interface from Avaya Proactive Contact to obtain information on calls and agent states, and used the Service Observing feature from 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 20.4 to interoperate with Avaya Proactive Contact 5.2 with PG230 and Avaya Aura® Application Enablement Services 8.1.3. Qfiniti is a call recording solution.

In the compliance testing, Qfiniti used the Event Services interface from Proactive Contact to obtain information on calls and agent states, and used the Service Observing feature from the Application Enablement Services Device, Media, and Call Control (DMCC) XML interface to capture media associated with the monitored agent stations for call recording.

The DMCC interface is used by Qfiniti to register virtual IP softphones, and for adding softphones to active calls using the Service Observing feature to pick up the media for call recording. When there is an active call at the monitored agent station, Qfiniti is informed of the call via events from the Event Services interface and starts call recording by using Service Observing via the DMCC interface to add a virtual IP softphone to the active call to obtain the media. The Event Services events are also used to determine when to stop the call recordings.

The compliance testing covered the recording of calls that were delivered by Proactive Contact for the PG230 deployment option. The possible recording of inbound calls delivered by Communication Manager under the agent blending mode is outside the scope of this compliance test.

## 2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of Qfiniti, the application automatically established Event Services connection with Proactive Contact and DMCC connection with Application Enablement Services and registered the virtual IP softphones.

For the manual part of the testing, each call was handled manually at the agent with generation of unique audio content for recording. Necessary agent actions such as hold and reconnect were performed from the Proactive Contact Agent application running on the agent desktops to test various call scenarios.

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

The verification of tests included use of Qfiniti logs for proper message exchanges and use of Qfiniti web interfaces for proper logging and playback of call recordings.

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 Qfiniti and Proactive Contact included encrypted SSL for Event Services and non-encrypted DMCC with Application Enablement Services, 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 Event Services agent states and call events.
- Use of DMCC registration services to register the virtual IP softphones.
- Use of DMCC services to register virtual IP softphones, and to activate Service Observing via button press to obtain the media for call recording.
- Proper recording, logging, and playback of calls for scenarios involving agent drop, customer drop, hold, reconnect, simultaneous calls, conference, transfer, forward work, long duration, multiple agents, manual call, inbound call blending, outbound call blending, and outbound agent blending scenarios.

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

## 2.2. Test Results

All test cases were executed and verified. The following were observations on Qfiniti from the compliance testing.

- By design, all call recordings contained audio up to the agent finished work action.
- By design, the held interval was included in the recordings and contained audio from the agent.

## 2.3. Support

Technical support on Qfiniti can be obtained through the following:

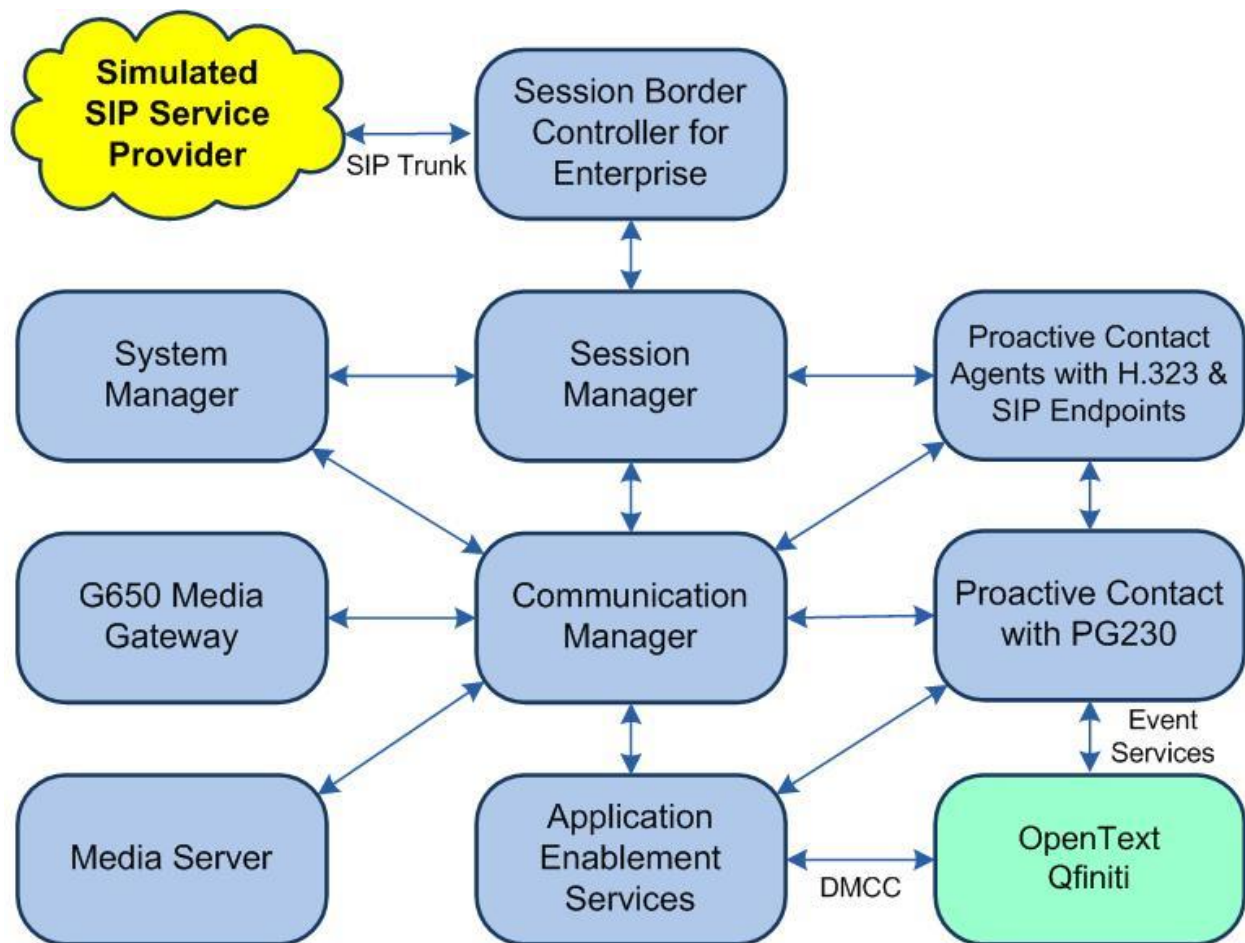
- **Phone:** (800) 540-7292
- **Web:** <http://engage.opentext.com/products/qfiniti>

### 3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The detailed administration of basic connectivity between Communication Manager and Proactive Contact, between Communication Manager and Application Enablement Services, and of call center devices are not the focus of these Application Notes and will not be described.

The agent station extensions used in the compliance testing are shown in the table below.

Extension	Type
65001	H.323
66002	SIP



**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 (8.1.3.0.1.890.26685)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	8.0.2.138
Avaya Aura® Application Enablement Services in Virtual Environment	8.1.3 (8.1.3.0.0.25-0)
Avaya Aura® Session Manager in Virtual Environment	8.1.3 (8.1.3.0.813014)
Avaya Aura® System Manager in Virtual Environment	8.1.3 (8.1.3.0.1012091)
Avaya Session Border Controller for Enterprise in Virtual Environment	8.1.1 (8.1.1.0-19390)
Avaya Proactive Contact	5.2.0.2
Avaya Proactive Contact Agent	5.2.0.2
Avaya 9611G & J179 IP Deskphone (H.323)	6.8502
Avaya J169 IP Deskphone (SIP)	4.0.7.1.5
OpenText Qfiniti on Microsoft Windows Server 2019 <ul style="list-style-type: none"><li>Avaya Event Service SDK</li><li>OpenSSL Shared Library</li><li>Microsoft SQL Server 2019</li><li>Avaya DMCC XML</li></ul>	20.4.0 with QF-16308 Standard 5.2 1.0.2o 15.0.4034.2 7.0.0.38

## 5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer IP codec set
- Administer system parameters features
- Administer class of restriction
- Administer agent stations
- Administer virtual IP softphones

### 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 **Service Observing (Basic)** customer option is set to “y” on **Page 7**. 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 7 of 12
CALL CENTER OPTIONAL FEATURES

Call Center Release: 8.0

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
Expert Agent Selection (EAS)? y      Vectoring (G3V4 Enhanced)? y
EAS-PHD? y                          Vectoring (3.0 Enhanced)? y
Forced ACD Calls? n                 Vectoring (ANI/II-Digits Routing)? y
Least Occupied Agent? n              Vectoring (G3V4 Advanced Routing)? y
Lookahead Interflow (LAI)? y         Vectoring (CINFO)? y
Multiple Call Handling (On Request)? y Vectoring (Best Service Routing)? y
Multiple Call Handling (Forced)? y    Vectoring (Holidays)? y
PASTE (Display PBX Data on Phone)? y Vectoring (Variables)? y
(NOTE: You must logoff & login to effect the permission changes.)
```

## 5.2. 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 networks 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 with 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.711MU          n           2          20
2: G.729
3:
4:
5:
6:
7:

Media Encryption                                Encrypted SRTP: best-effort
1: 1-srtp-aescm128-hmac80
2: aes
3: none
4:
5:
```



### 5.3. 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          Coach on SSC? n
```

## 5.4. 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 43
CLASS OF RESTRICTION	
COR Number: 2	
COR Description: Service Observing	
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

## 5.5. Administer Agent Stations

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 5.4**.

Repeat this section to administer all H.323 agent stations from **Section 3**. In the compliance testing, one agent station was administered as shown below.

change station 65001	Page 1 of 5	
STATION		
Extension: 65001	Lock Messages? n	BCC: 0
Type: 9611	Security Code: *	TN: 1
Port: S00104	Coverage Path 1: 1	<b>COR: 2</b>
Name: CM Station 1	Coverage Path 2:	COS: 1
Unicode Name? n	Hunt-to Station:	Tests? Y

## 5.6. 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 5.4**.
- **IP SoftPhone:** “y”

add station 65991		Page 1 of 5
STATION		
<b>Extension:</b> 65991	Lock Messages? n	BCC: 0
<b>Type:</b> 4620	<b>Security Code:</b> 123456	TN: 1
Port: IP	Coverage Path 1:	<b>COR:</b> 2
<b>Name:</b> Qfiniti DMCC 1	Coverage Path 2:	COS: 1
Unicode Name? n	Hunt-to Station:	Tests: y
STATION OPTIONS		
Location:	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 65991	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Expansion Module? n	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	<b>IP SoftPhone? y</b>	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	

Navigate to **Page 4** and add “serv-obsrv” to the 6<sup>th</sup> button as required by Qfiniti.

add station 65991		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	<b>6: serv-obsrv</b>	
3: call-appr	7:	
4:	8:	

Repeat this section to administer the desired number of virtual IP softphones. In the compliance testing, two virtual IP softphones were administered as shown below.

list station 65991 count 2										
STATIONS										
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Cable	Room/ Jack	Cv1/ Cv2	COS	COR/ TN		
65991	S000011	Qfiniti DMCC 1						2		
	4620		no					1 1		
65992	S000012	Qfiniti DMCC 2						2		
	4620		no					1 1		

## 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 H.323 gatekeeper
- Administer Qfiniti user
- Administer security database
- Administer ports
- Restart service

### 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 right side, a "Welcome: User" message provides login details: "Last login: Wed Feb 24 14:55:10 2021 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: 8.1.3.0.0.25-0", "Server Date and Time: Wed Feb 24 15:28:33 EST 2021", and "HA Status: Not Configured".

The left sidebar contains a list of navigation items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The "Licensing" item is highlighted.

The main content area, titled "Welcome to OAM", contains the following text:

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. The top header and navigation bar are identical to the previous screenshot. The left sidebar shows the "Licensing" item highlighted, with sub-items: "WebLM Server Address", "WebLM Server Access", and "Reserved Licenses".

The main content area, titled "Licensing", contains the following text:

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

- WebLM Server Address

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

- WebLM Server Access

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

- Reserved Licenses

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 **Device Media and Call Control** as shown below.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The left pane displays a navigation tree with the following items: WebLM Home, Install license, Licensed products, APPL\_ENAB, Application\_Enablement (expanded), 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, CCTR, ContactCenter, and COMMUNICATION\_MANAGER. The right pane displays the 'Application Enablement (CTI) - Release: 8 - SID: 10503000 (Enterprise license)' screen. It includes a breadcrumb trail: 'You are here: Licensed Products > Application\_Enablement > View by Feature'. Below this, it states 'License installed on: August 8, 2019 4:43:51 PM -05:00' and 'License File Host IDs: VE-83-02-2D-26-52-01'. A table lists the features and their license capacities:

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 H.323 Gatekeeper

Select **Communication Manager Interface** → **Switch Connections** from the left pane. The **Switch Connections** screen shows a listing of the existing switch connections.

Locate the connection name associated with the relevant Communication Manager, in this case “cm7”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

Welcome: User  
Last login: Wed Feb 24 14:55:10 2021 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: 8.1.3.0.0.25-0  
Server Date and Time: Wed Feb 24 15:28:33 EST 2021  
HA Status: Not Configured

Communication Manager Interface | Switch Connections [Home](#) | [Help](#) | [Logout](#)

AE Services  
Communication Manager Interface  
Switch Connections  
Dial Plan  
High Availability  
Licensing  
Maintenance  
Networking

Switch Connections

Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm7	Yes	30	1

Edit Connection Edit PE/CLAN IPs Edit H.323 Gatekeeper Delete Connection Survivability Hierarchy

The **Edit H.323 Gatekeeper** screen is displayed next. Enter the IP address of a C-LAN circuit pack or the Processor on Communication Manager to use as the H.323 gatekeeper, in this case “10.64.101.236” as shown below. Click **Add Name or IP**.

Welcome: User  
Last login: Wed Feb 24 14:55:10 2021 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: 8.1.3.0.0.25-0  
Server Date and Time: Wed Feb 24 15:28:33 EST 2021  
HA Status: Not Configured

Communication Manager Interface | Switch Connections [Home](#) | [Help](#) | [Logout](#)

AE Services  
Communication Manager Interface  
Switch Connections  
Dial Plan  
High Availability  
Licensing  
Maintenance  
Networking

Edit H.323 Gatekeeper - cm7

Add Name or IP

Name or IP Address

Delete IP Back



## 6.4. Administer Qfiniti User

Select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane (not shown).

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: Wed Feb 24 14:55:10 2021 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: 8.1.3.0.0.25-0  
Server Date and Time: Wed Feb 24 15:30:17 EST 2021  
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 Idqfiniti

\* Common Nameqfiniti

\* Surnameqfiniti

\* User Password\*\*\*\*\*

\* Confirm Password\*\*\*\*\*

Admin Note

Avaya RoleNone

Business Category

Car License

CM Home

Css Home

CT UserNo

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 **Enable SDB for DMCC Service** is unchecked, as shown below.

In the event that the security database is used by the customer with the parameter already enabled, then follow reference [2] to configure access privileges for the Qfiniti 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 welcome message and system information are shown in the top right corner. The main navigation pane on the left lists various services, with "Security" expanded to show "Security Database" and "Control" selected. The main content area displays the "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" configuration page, which includes two unchecked checkboxes for enabling SDB services and an "Apply Changes" button.

Welcome: User  
Last login: Wed Feb 24 14:55:10 2021 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: 8.1.3.0.0.25-0  
Server Date and Time: Wed Feb 24 15:28:33 EST 2021  
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. Administer Ports

Select **Networking** → **Ports** from the left pane, to display the **Ports** screen in the right pane.

In the **DMCC Server Ports** section, make certain the radio button for **Unencrypted Port** is selected under the **Enabled** column, as shown below. Retain the default values in the remaining fields.

**AVAYA** Application Enablement Services  
Management Console

Welcome: User  
Last login: Wed Feb 24 14:55:10 2021 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: 8.1.3.0.0.25-0  
Server Date and Time: Wed Feb 24 15:28:33 EST 2021  
HA Status: Not Configured

Networking | PortsHome | Help | Logout

▶ 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

Unencrypted TCP Port9999

Encrypted TCP Port9998

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Encrypted Port4722

TR/87 Port4723

Enabled Disabled

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☒ ☐

## 6.7. Restart Service

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

**AVAYA** **Application Enablement Services**  
Management Console

Welcome: User  
Last login: Wed Feb 24 14:55:10 2021 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: 8.1.3.0.0.25-0  
Server Date and Time: Wed Feb 24 15:28:33 EST 2021  
HA Status: Not Configured

Maintenance | Service ControllerHome | Help | Logout

▶ 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 checked="" 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](#)

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart Web Server

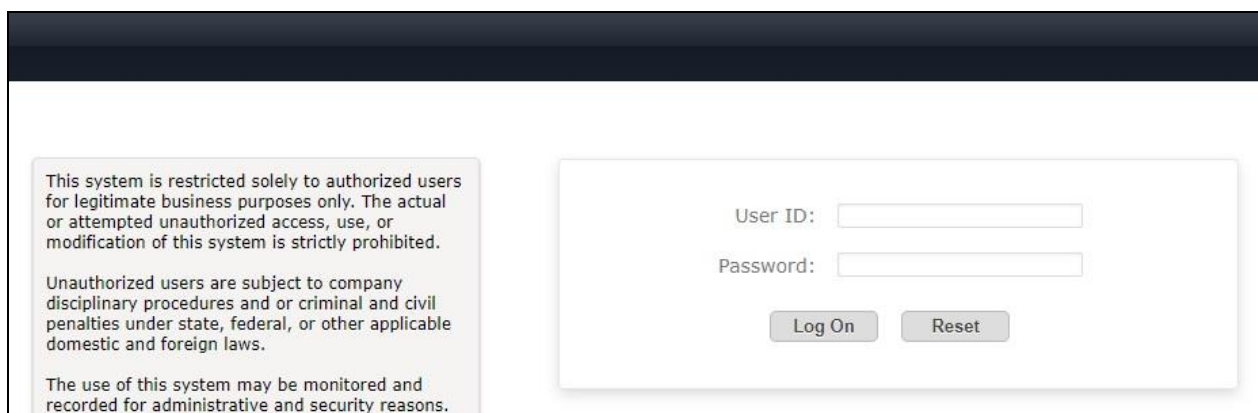
## 7. Configure Avaya Aura® Session Manager

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 users

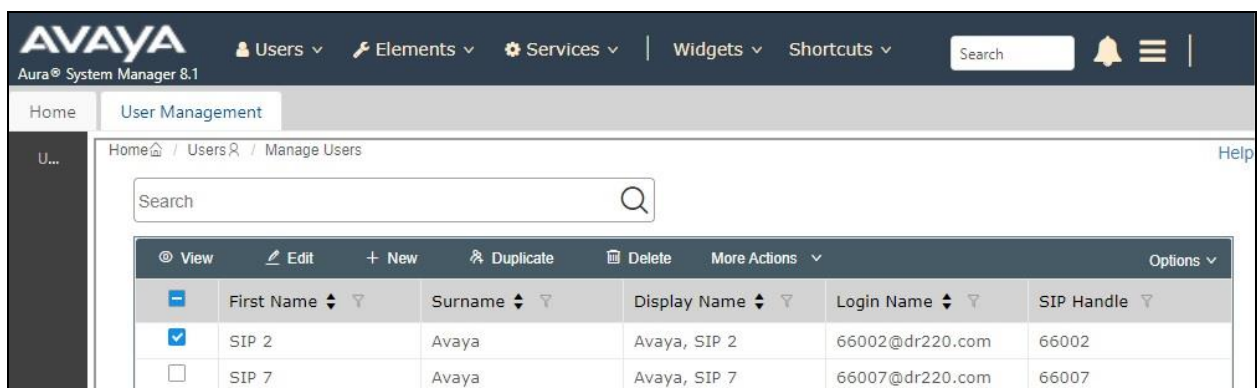
### 7.1. Launch System Manager

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 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 “66002”, and click **Edit**.



View	Edit	New	Duplicate	Delete	More Actions	Options
<input checked="" type="checkbox"/>						

First Name	Surname	Display Name	Login Name	SIP Handle
SIP 2	Avaya	Avaya, SIP 2	66002@dr220.com	66002
SIP 7	Avaya	Avaya, SIP 7	66007@dr220.com	66007

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 menu items for Users, Elements, Services, Widgets, and Shortcuts. The breadcrumb trail indicates the path: Home > Users > Manage Users. The main title is "User Profile | Edit | 66002@dr220.com". Below the title are tabs for Identity, Communication Profile, Membership, and Contacts. The Communication Profile tab is active. On the left, under "PROFILES", the "CM Endpoint Profile" is selected with a toggle switch. The main form area contains various fields for configuring the profile:

- \* System:** DR-CM
- \* Profile Type:** Endpoint
- \* Extension:** 66002 (The Editor icon next to this field is highlighted with a red box)
- \* Set Type:** J169CC
- Port:** S000068
- Preferred Handle:** Select
- Sip Trunk:** aar
- Use Existing Endpoints:** ☐
- Template:** Start typing...
- Security Code:** Enter Security Code
- Voice Mail Number:**
- Calculate Route Pattern:** ☐

Buttons at the top right include "Commit & Continue", "Commit", and "Cancel".

The **Edit Endpoint** pop-up screen is displayed. For **Class of Restriction (COR)**, enter the COR number from **Section 5.4** as shown below.

Repeat this section for all SIP agent extensions from **Section 3**. In the compliance testing, one SIP agent extension 66002 was configured.

The screenshot shows the 'Edit Endpoint' configuration screen in the Avaya Aura System Manager 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The main content area is titled 'Edit Endpoint' and includes a 'Done' button and a '[Save As Template]' link. The configuration is organized into several sections:

- System Information:**
  - System: DR-CM
  - Template: Select (dropdown)
  - Port: S000068
  - Name: Avaya, SIP 2
- Extension Information:**
  - Extension: 66002
  - Set Type: J169CC
  - Security Code: (empty)
- Configuration Tabs:**
  - General Options (G) \* (selected)
  - Feature Options (F)
  - Site Data (S)
  - Abbreviated Call Dialing (A)
  - Enhanced Call Fwd (E)
  - Button Assignment (B)
  - Profile Settings (P)
  - Group Membership (M)
- General Options (G) \* Fields:**
  - Class of Restriction (COR):** 2 (highlighted with a red box)
  - Emergency Location Ext: 66002
  - Tenant Number: 1
  - SIP Trunk: Qaar
  - Coverage Path 1: 1
  - Lock Message: ☐
  - Multibyte Language: Not Applicable (dropdown)
  - SIP URI: (empty)
- Other Fields:**
  - Class Of Service (COS): 1
  - Message Lamp Ext.: 66002
  - Type of 3PCC Enabled: None (dropdown)
  - Coverage Path 2: (empty)
  - Localized Display Name: Avaya, SIP 2
  - Enable Reachability for Station Domain Control: system (dropdown)

## 8. Configure Avaya Proactive Contact

This section provides the procedures for obtaining the host name of Proactive Contact.

Log in to the Linux shell of Proactive Contact. Use the “uname -a” command to obtain the host name, which will be used later to configure Qfiniti.

In the compliance testing, the host name of Proactive Contact is “lzpds4b”, as shown below.

```
$ uname -a  
Linux lzpds4b 2.6.32-754.28.1.el6.i686 #1 SMP Fri Jan 31 06:05:46 EST 2020 i686  
i686 i386 GNU/Linux  
LZPDS4B(xxx)@/opt/avaya/pds [431]  
$
```



## 9. Configure OpenText Qfiniti

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

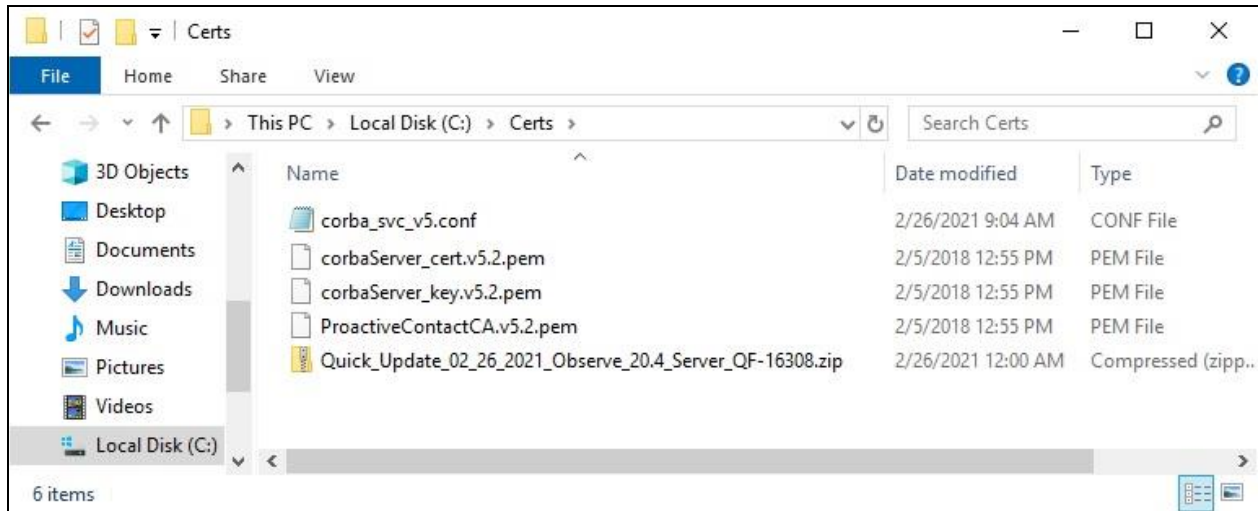
- Administer certificates
- Launch SysConfig web interface
- Administer switches
- Administer CTI server
- Administer board configuration
- Administer general
- Administer machines
- Administer components
- Administer CTI sources
- Administer phone interface
- Administer logging data – phone class of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

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

## 9.1. Administer Certificates

From the Qfiniti server, create a folder under the **C:** directory along with a desired name, in this case **Certs**. Note that Qfiniti requires the directory name to not contain spaces.

Copy one configuration and three certificate files shown below that were provided by OpenText to the newly created folder. In the compliance testing, the four files were unzipped from the Qfiniti Quick Update QF-16308 package shown below.



Open the **corba\_svc\_v5.conf** configuration file with an editor application and update the three **PEM** parameters with complete path and name of the pertinent certificate file, as shown below.

```
dynamic SSLIOP_Factory Service_Object * TAO_SSLIOP:
_make_TAO_SSLIOP_Protocol_Factory() "-SSLAuthenticate
SERVER_AND_CLIENT -SSLPrivateKey PEM:C:\Certs
\corbaServer_key.v5.2.pem -SSLCertificate PEM:C:\Certs
\corbaServer_cert.v5.2.pem -SSLCAfile PEM:C:\Certs
\ProactiveContactCA.v5.2.pem"
static Resource_Factory "-ORBProtocolFactory SSLIOP_Factory"
```

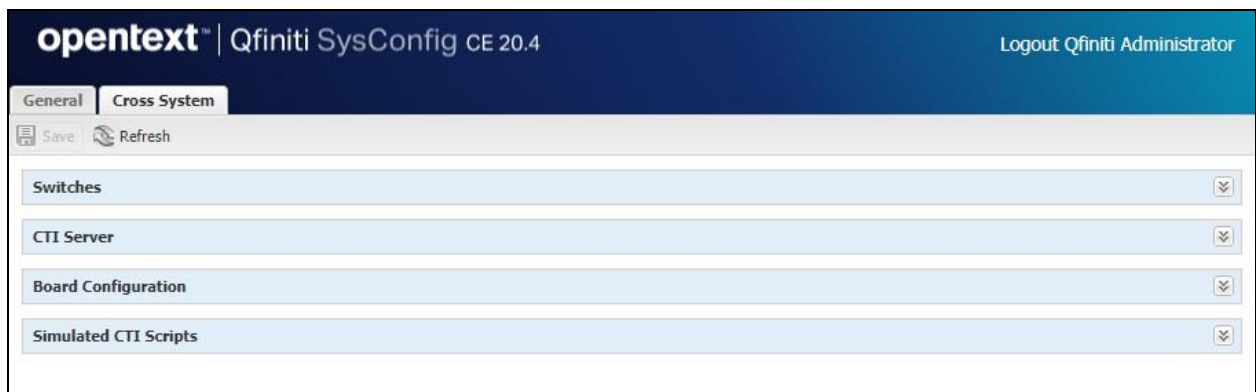
## 9.2. Launch SysConfig Web Interface

Access the SysConfig web interface by using the URL “http://hostname/sysconfig” 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.

The image shows the Opentext login screen. It has a dark blue background with the 'opentext' logo in white. Below the logo, it says 'Sign in to continue to qfiniti-system-configuration'. There are two white input fields: the first is labeled 'User name' and the second is labeled 'Password'.

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

The image shows the Opentext SysConfig CE 20.4 interface. At the top, it says 'opentext | Qfiniti SysConfig CE 20.4' and 'Logout Qfiniti Administrator'. Below this, there are two tabs: 'General' and 'Cross System'. The 'Cross System' tab is selected. Below the tabs, there are four sections: 'Switches', 'CTI Server', 'Board Configuration', and 'Simulated CTI Scripts'. Each section has a dropdown arrow on the right.

### 9.3. Administer Switches

Expand the **Switches** sub-section and 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 “AES4DMCC”.
- **Switch Model:** “Avaya AES/CM”
- **Observe Mode:** “By Extension”
- **Interface Type:** “DMCC / TAPI / DRLink”
- **Use CTI Source for Alias:** Check this field.
- **Avaya CM Hostname:** The relevant switch connection name from **Section 6.3**.
- **AES IP Address:** The IP address of Application Enablement Services server.
- **User Name:** The Qfiniti user credentials from **Section 6.4**.
- **Password:** The Qfiniti user credentials from **Section 6.4**.

The screenshot shows the OpenText Qfiniti Switch configuration window. The window is titled "Switch" and contains various fields for configuring a switch. The "Name" field is set to "AES4DMCC", "Switch Model" is "Avaya AES/CM", "Observe Mode" is "By Extension", "Interface Type" is "DMCC / TAPI / DRLink", and "Use CTI Source for Alias" is checked. Other fields include "APC Dialer in use?", "Avaya CM Hostname", "Port", "1st Line Appearance", "AES IP Address", "Service Observe Button", "User Name", "Password", "AES Connection Alarm Trigger", "Wait Before Dial", "Busy Repeat Max", "Survey Excluded Extensions", and "Alt. AES IP Address". The "Add", "Ok", and "Cancel" buttons are at the bottom.

## 9.4. Administer CTI Server

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

- **Name:** A descriptive name, in this case “Dialer4DMCC”.
- **Type:** “Avaya Dialer”
- **Available Switch:** Select the switch name from **Section 9.3**.
- **User Name:** The Proactive Contact Event Service client credentials.
- **Password:** The Proactive Contact Event Service client credentials.
- **NameServe Value 1:** “NameService=corbaloc:ssliop:lzpds4b:23201/NameService”, where **lzpds4b** is the Proactive Contact hostname from **Section 8**.
- **NameServe Flag 2:** “-ORBSvcConf”
- **NameServe Value 2:** Complete path of the **corba\_svc\_v5.conf** file from **Section 9.1**.
- **NameServe Value 3:** “10”
- **Event Service P2:** The Proactive Contact host name from **Section 8**.
- **Dialer Version:** “PACv5.X”
- **NameServe Value 4:** Complete path of the **corbalog.log** file from **Section 9.1**.

The screenshot shows the 'opentext | Qfiniti' interface for 'CTI Server' management. The left sidebar has tabs for 'General', 'Cross System', 'Switches', 'CTI Server', 'Board Configuration', and 'Simulated CTI Scripts'. The 'CTI Server' tab is selected, showing a list of servers with columns for Name and Type. The main area displays the configuration form for a new CTI Server. The form includes fields for Name (Dialer4DMCC), Type (Avaya Dialer), Available Switch (AES4DMCC), User Name (client1), Password (masked), NameServe Flag 1 (-ORBInitRef), NameServe Value 1 (NameService=corbaloc:ssliop:lzpds4b:23201/Nar), NameServe Flag 2 (-ORBSvcConf), NameServe Value 2 (C:\Certs\corba\_svc\_v5.conf), NameServe Flag 3 (-ORBDebugLevel), NameServe Value 3 (10), Event Service P0 (PDS), Event Service P1 (dialers), Event Service P2 (lzpds4b), Event Service P3 (eventserver), Event Service P4 (v2\_0), Dialer Version (PACv5.X), NameServe Flag 4 (-ORBLogFile), NameServe Value 4 (C:\Certs\corbalog.log), and NameServe Flag 5. A red circle highlights the '+' icon in the right sidebar, indicating the 'New Item' button.

## 9.5. Administer Board Configuration

Expand the **Board Configuration** sub-section and 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 “DummyBd4DMCC”.
- **Model:** “Network Interface Card (NIC)”

The screenshot shows the Qfiniti SysConfig CE 20.4 interface. The 'Board Configuration' dialog box is open, displaying the following fields and values:

Field	Value
Name	DummyBd4DMCC
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	
Network Card IP Address 4	
Network Card Port 4	5060

The 'Add', 'Ok', and 'Cancel' buttons are located at the bottom of the dialog box. A red circle highlights the '+' icon in the right sidebar, indicating the 'New Item' button.

## 9.6. Administer General

Select the **General** tab. Expand the **General** sub-section and click the **New Item** 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 descriptive name, in this case “DevConnect”.
- **Switch:** Select the switch name from **Section 9.3**.
- **System Type:** Check **Voice Recording - Logging**.

The screenshot displays the Opentext Qfiniti SysConfig CE 20.4 web interface. The top navigation bar includes the 'opentext' logo, the product name 'Qfiniti SysConfig CE 20.4', and a 'Logout Qfiniti Administrator' link. Below the navigation bar, there are two tabs: 'General' and 'Cross System'. The 'General' tab is active, showing a 'Systems' section with a 'Quick Find' input field and a message: 'No Systems found. Start by creating a New System.' To the right of this message is a '+ New' button, which is circled in red. Below the 'Systems' section, there is a 'General' sub-section with the following fields and options:

- Name:** A text input field containing 'DevConnect'.
- Switch:** A dropdown menu showing 'AES4DMCC'.
- System Type:** A list of checkboxes with the following options:
  - ☒ Voice Recording - Logging
  - ☐ Voice Recording - QA
  - ☐ Screen Recording
  - ☐ Remote Screen Site
  - ☐ Explore
  - ☐ Survey
  - ☐ Backup
  - ☐ Cloud Connector
- Description:** A large text area.
- ☐ Available for Use (with a help icon)
- ☐ NAT Environment

Below the 'General' sub-section, there are four expandable sections: 'Machines', 'Components', 'CTI Sources', and 'Phone Interface', each with a downward arrow icon.

## 9.7. Administer Machines

Expand the **Machines** sub-section and click the **New Item** 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”.





## 9.8. 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”

Follow reference [5] to configure **Archive Manager** and **Qfiniti File Server** components (not shown).

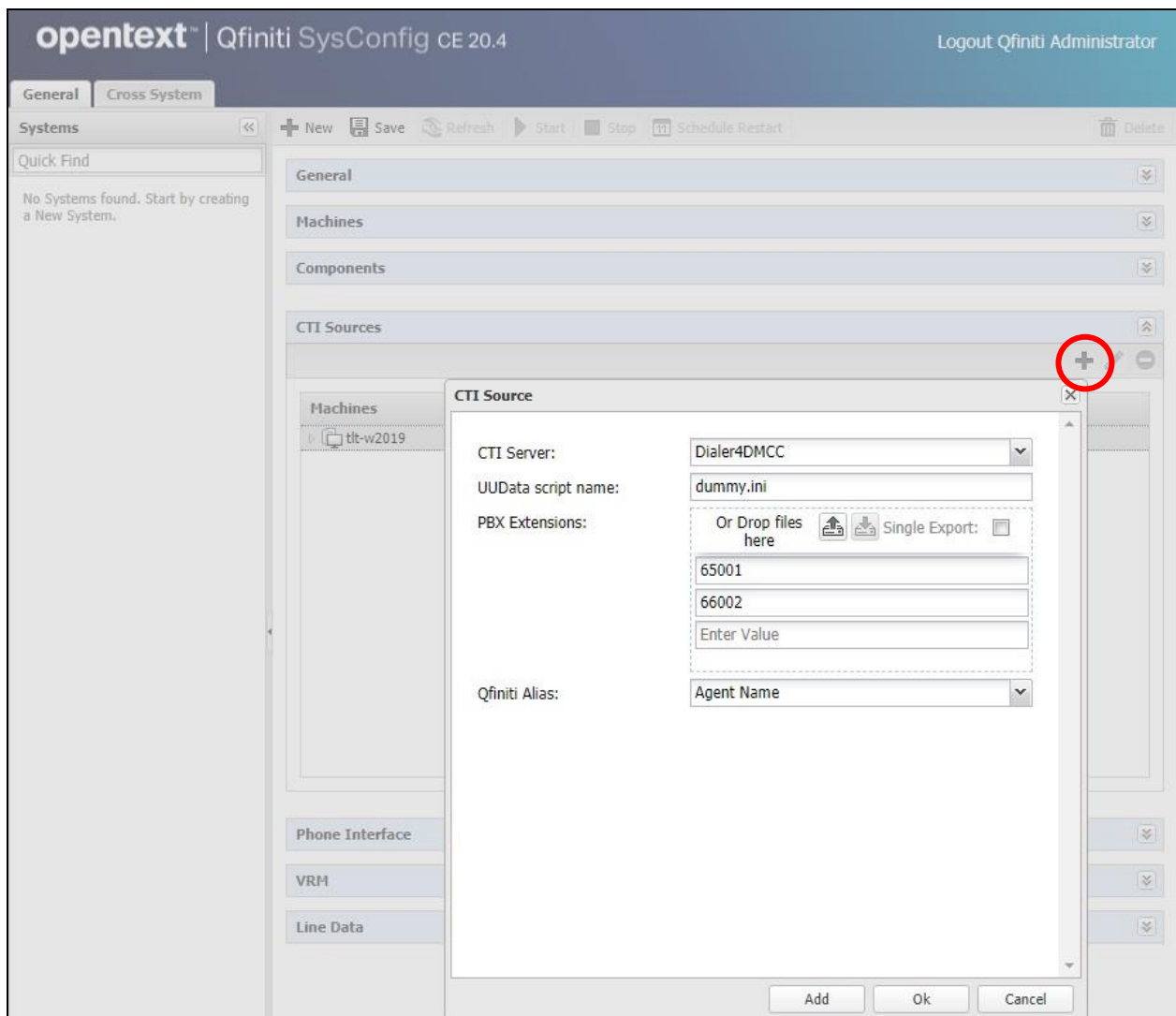
The screenshot displays the 'opentext | Qfiniti SysConfig CE 20.4' interface. The top navigation bar includes 'General' and 'Cross System' tabs. The 'Systems' section on the left shows a 'Quick Find' box and a message: 'No Systems found. Start by creating a New System.' The main 'Components' section is divided into 'Available Components' and 'Assigned Components'. The 'Assigned Components' list includes: Archive Manager, Central Messaging Server, CTI Manager, Data Import Listener, Disk Monitor, Dispatcher, Global Trigger Manager, IP Message Scheduler, **Logger Voice Recording Manager** (highlighted), Master Service, Plan Manager, Qfiniti File Server, and Session Manager. Below this, the 'Component Data' section contains the following configuration fields:

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.xml
Service Observe fail retry delay:	30
Start Recording On:	Alerting
CTI Init:	On Startup
Line Reset Threshold in Sec:	0
VoIP Transcoding:	NONE

## 9.9. Administer CTI Sources

Expand the **CTI Sources** sub-section. Select the applicable machine server name from **Section 9.7**, followed by the **Add CTI Source** icon. Enter the following values for the specified fields and retain the default values for the remaining fields.

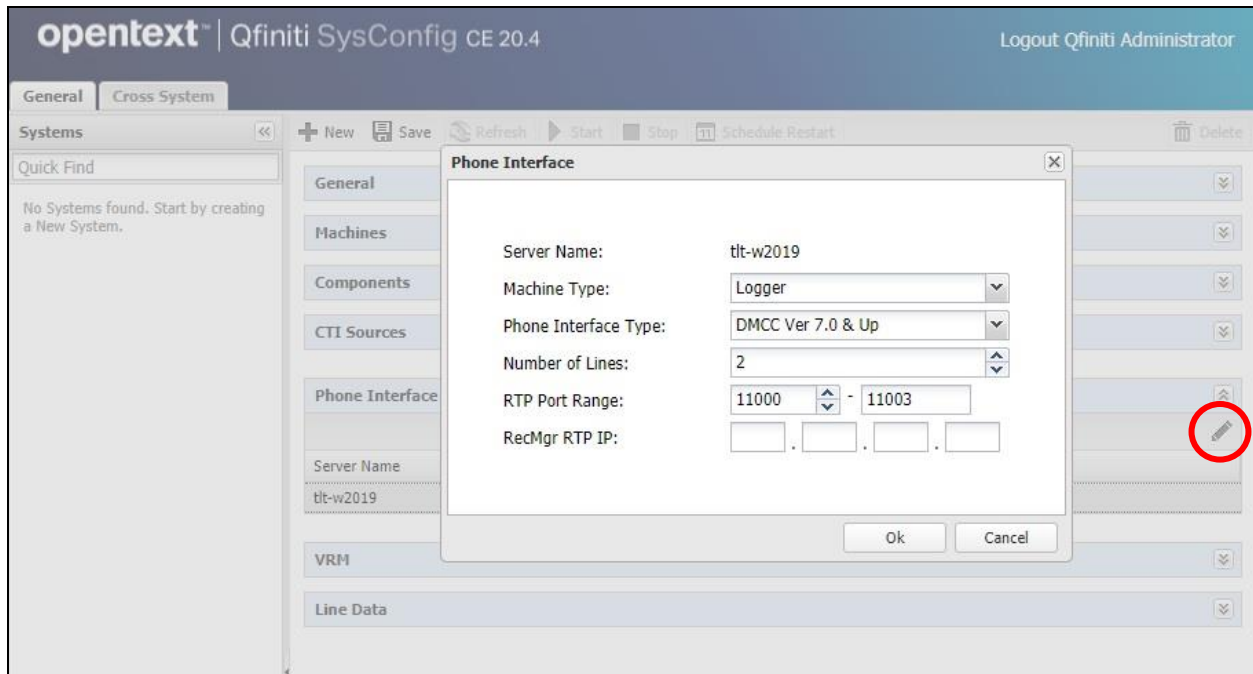
- **CTI Server:** Select the CTI server name from **Section 9.4**.
- **UUData script name:** Script is not used in the integration but required to be configured.
- **PBX Extensions:** The agent station extensions from **Section 3**.
- **Qfiniti Alias:** “Agent Name”



## 9.10. Administer Phone Interface

Expand the **Phone Interface** sub-section. Select the machine server name from **Section 9.7** 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.

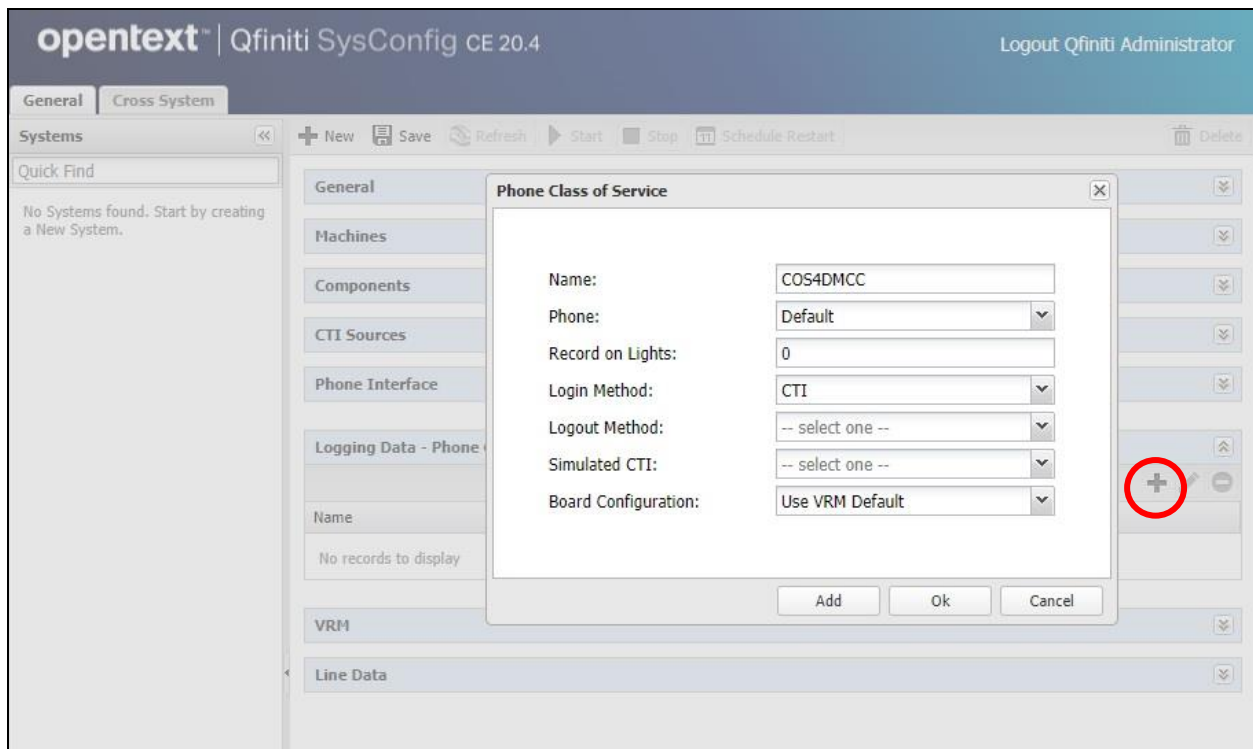
- **Machine Type:** “Logger”
- **Phone Interface Type:** “DMCC Ver 7.0 & Up”
- **Number of Lines:** Select the total number of agents from **Section 3**.



## 9.11. Administer Logging Data – Phone Class of Service

Expand the **Logging Data – Phone Class of Service** sub-section. Select 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 “COS4DMCC”.
- **Phone:** “Default”
- **Record on lights:** “0”
- **Login Method:** “CTI”.



## 9.12. Administer VRM

Expand the **VRM** sub-section. Select the machine server name from **Section 9.7**, followed by the **Add VRM** icon. Enter the following values for the specified fields.

- **VRM Name:** A desired name, in this case “VRM4DMCC”.
- **VRM Type:** “Logging”
- **Interface Type:** “Station Side DMCC”
- **Line From and Line To:** Range of agent stations, in this case two stations so “1” to “2”.
- **Default Class of Service:** Select the phone class of service name from **Section 9.11**.
- **Default Board Config:** Select the board name from **Section 9.5**.

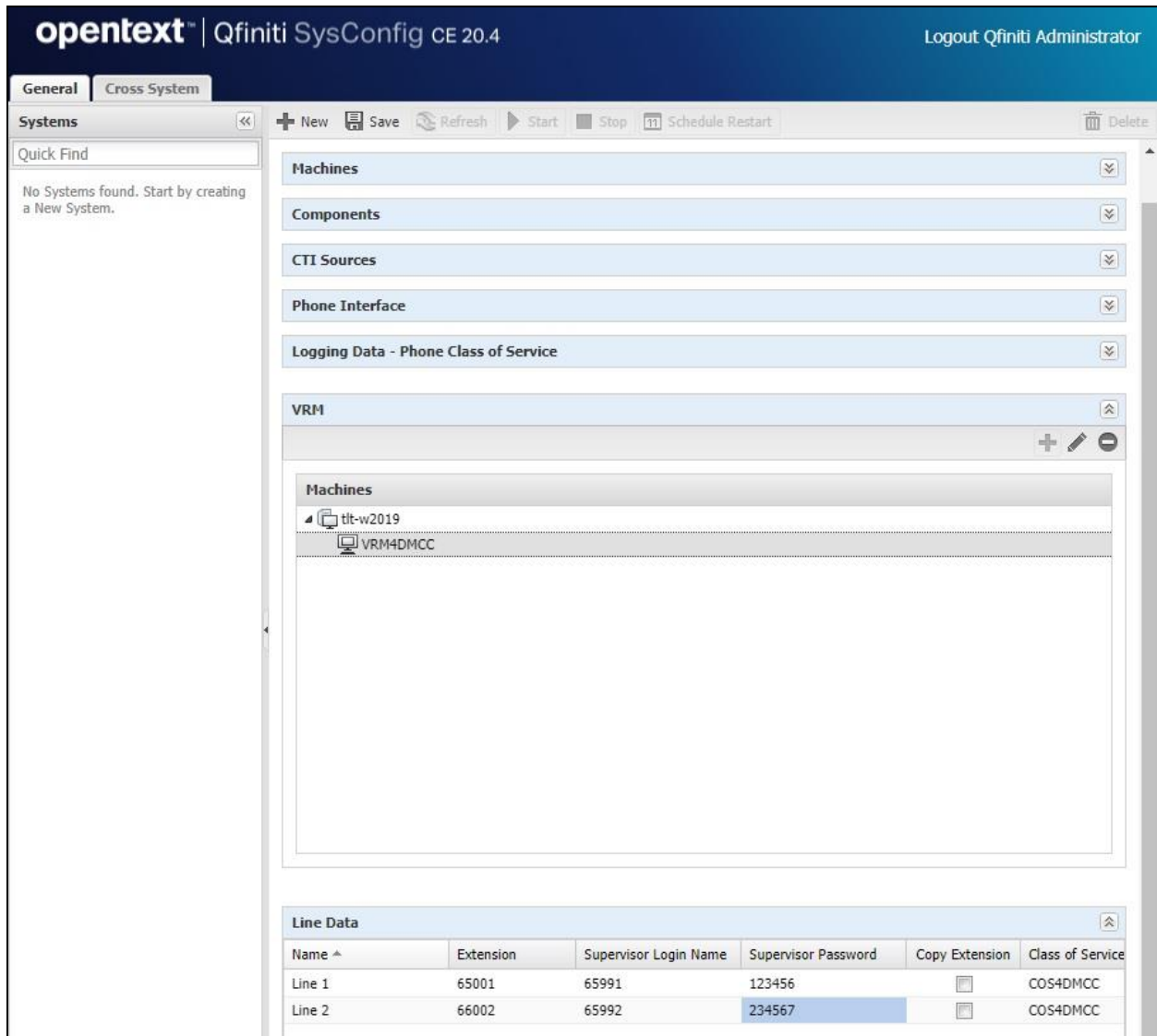
The screenshot displays the opentext Qfiniti SysConfig CE 20.4 web interface. The top navigation bar includes the opentext logo, the product name 'Qfiniti SysConfig CE 20.4', and a 'Logout Qfiniti Administrator' link. Below the navigation bar, there are tabs for 'General' and 'Cross System'. The main content area is divided into a left sidebar and a right pane. The sidebar contains a 'Systems' section with a 'Quick Find' box and a message 'No Systems found. Start by creating a New System.' The right pane shows a list of system components: General, Machines, Components, CTI Sources, Phone Interface, and Logging Data - Phone Class of Service. The 'VRM' section is expanded, and a red circle highlights the '+ New' button. Below this, a 'Machines' list shows a single entry 'tlt-w2019'. A modal window titled 'VRM' is open, displaying the configuration form for a new VRM. The form fields are as follows:

VRM Name:	VRM4DMCC
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:	2
Allow Extension Duplication:	<input type="checkbox"/>
Default Class of Service:	COS4DMCC
Default Board Config:	DummyBd4DMCC

### 9.13. Administer Line Data

Select the newly added VRM from **Section 9.12**, 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 5.6** respectively.

Repeat this section to administer all agent station extensions from **Section 3** with all virtual IP softphones from **Section 5.6**, as shown below.

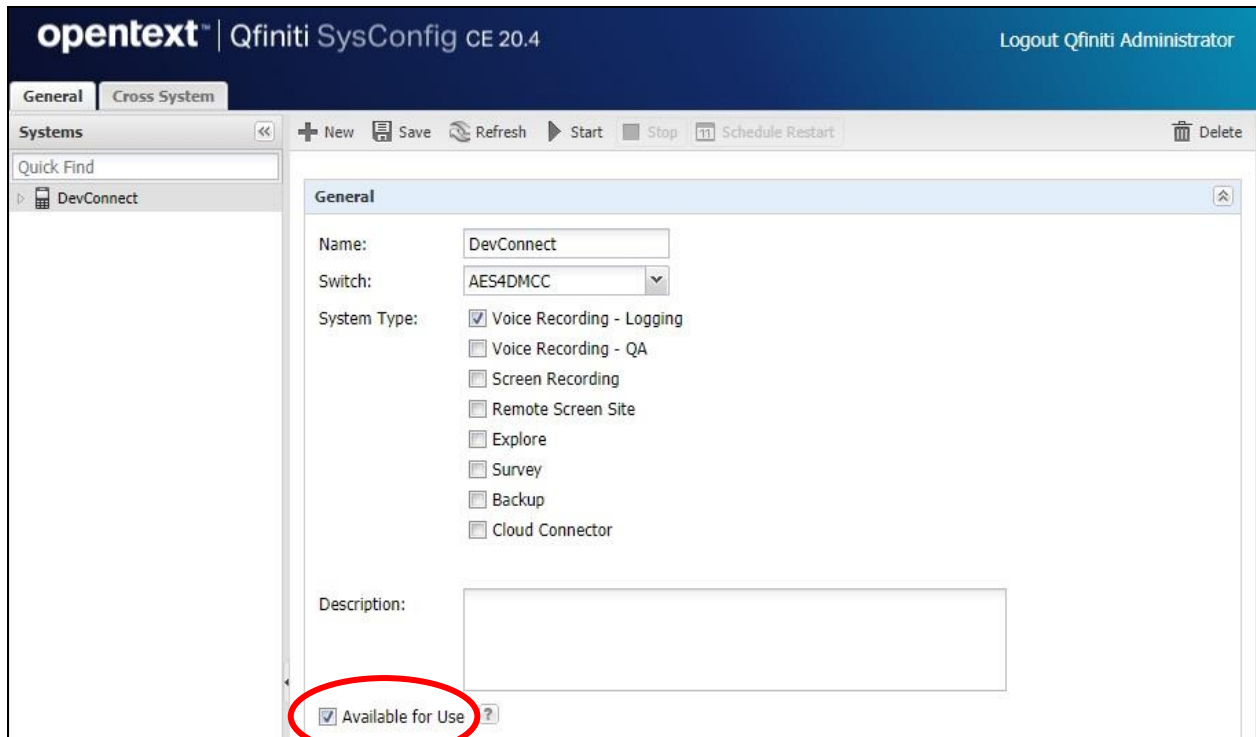


The screenshot displays the opentext Qfiniti SysConfig CE 20.4 web interface. The top navigation bar includes the 'opentext' logo, the product name 'Qfiniti SysConfig CE 20.4', and a 'Logout Qfiniti Administrator' link. Below the navigation bar, there are tabs for 'General' and 'Cross System'. The main content area is divided into a left sidebar and a right pane. The sidebar contains a 'Systems' section with a 'Quick Find' input field and a message: 'No Systems found. Start by creating a New System.' The right pane shows a hierarchical tree of system components: 'Machines', 'Components', 'CTI Sources', 'Phone Interface', 'Logging Data - Phone Class of Service', and 'VRM'. The 'VRM' component is expanded, showing a list of machines: 'tit-w2019' and 'VRM4DMCC'. Below this, the 'Line Data' table is visible, containing two rows of data.

Name ^	Extension	Supervisor Login Name	Supervisor Password	Copy Extension	Class of Service
Line 1	65001	65991	123456	<input type="checkbox"/>	COS4DMCC
Line 2	66002	65992	234567	<input type="checkbox"/>	COS4DMCC

## 9.14. Enable Use

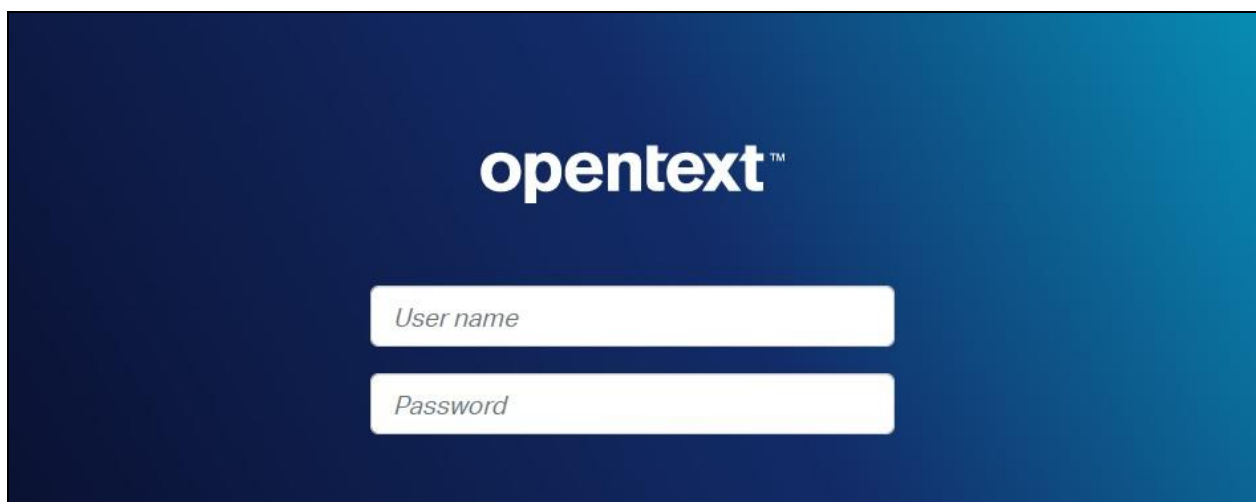
Scroll up the right pane and expand the **General** sub-section. Check **Available for Use**.



The screenshot shows the opentext Qfiniti SysConfig CE 20.4 web interface. The 'General' tab is selected, and the 'General' sub-section is expanded. The 'Name' field is 'DevConnect' and the 'Switch' is 'AES4DMCC'. Under 'System Type', several options are listed with checkboxes: 'Voice Recording - Logging' (checked), 'Voice Recording - QA' (unchecked), 'Screen Recording' (unchecked), 'Remote Screen Site' (unchecked), 'Explore' (unchecked), 'Survey' (unchecked), 'Backup' (unchecked), and 'Cloud Connector' (unchecked). At the bottom, the 'Description' field is empty. A red circle highlights the 'Available for Use' checkbox, which is checked.

## 9.15. 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.



The screenshot shows the opentext Qfiniti Web Interface login screen. It features the opentext logo at the top. Below the logo are two input fields: 'User name' and 'Password'.

## 9.16. Administer Observe Settings

In the subsequent screen, select **Administer** → **Settings** from the top menu, followed by **Observe Settings** in the left pane.

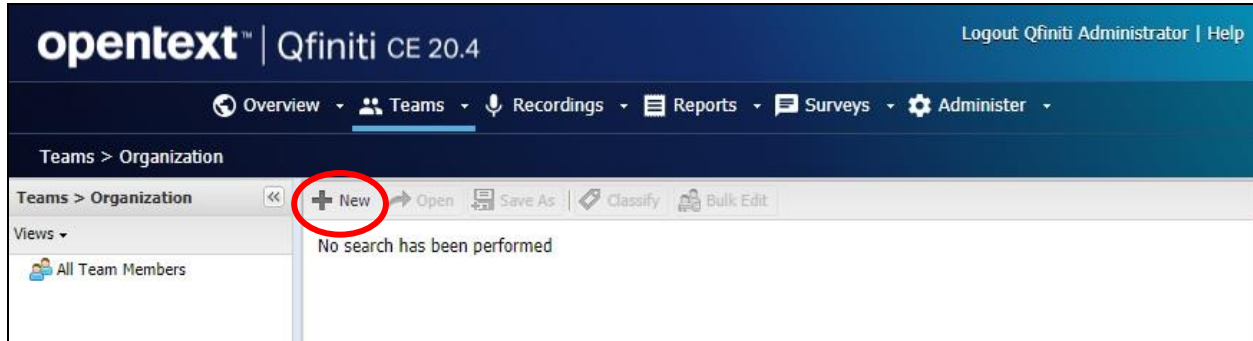
Scroll down to the **Recording Options** sub-section. For **Option**, select “Continuous Record”. For **Type**, check **Allow voice recordings**, as shown below. Retain the default values for the remaining fields.

The screenshot shows the OpenText Qfiniti CE 20.4 Administer Observe Settings page. The top navigation bar includes the OpenText logo, Qfiniti CE 20.4 version, and a Logout Qfiniti Administrator | Help link. Below the navigation bar is a menu with Overview, Teams, Recordings, Reports, Surveys, and Administer. The Administer menu is expanded, showing a breadcrumb trail: Administer > Settings > Observe Settings. The left sidebar contains a list of settings: Alarm Settings, License Settings, Observe Settings (selected), Platform Settings, Survey Settings, and Web Access Settings. The main content area is titled 'Observe Settings' and contains a 'Save' button. The 'Recording Options' section is expanded, showing a dropdown menu for 'Option' set to 'Continuous Record'. The 'Type' section has four checkboxes: 'Allow voice recordings' (checked), 'Allow screen recordings' (unchecked), 'Allow voice and screen recordings' (unchecked), and 'Allow screen recordings on transfer' (unchecked). The 'Phone Player' section is also expanded, showing a text input field for 'UNC Path'.



## 9.17. 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.

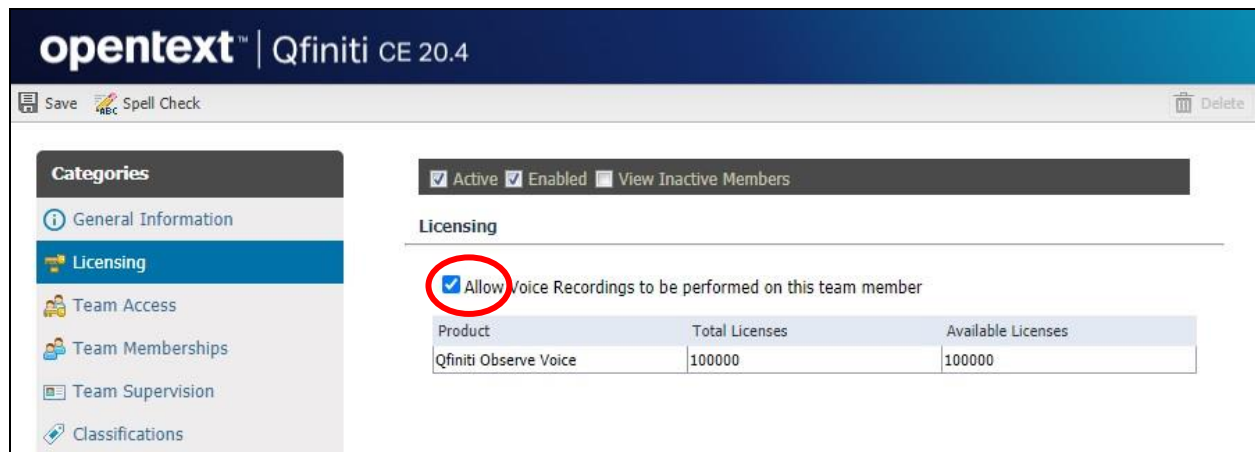


In the pop-up screen below, enter the following values for the specified fields and retain the default values for the remaining fields.

- **First Name:** A desired first name for the first agent line from **Section 9.13**.
- **Last Name:** A desired last name for the first agent line from **Section 9.13**.
- **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 'New Agent' form in the Opentext Qfiniti CE 20.4 interface. On the left is a 'Categories' sidebar with options like 'General Information', 'Licensing', 'Team Access', etc. The main area is titled 'General Information' and contains several input fields: 'First Name' (filled with 'FNAgent1'), 'Middle Name' (empty), 'Last Name' (filled with 'LnAgent1'), 'Email Address' (empty), 'Username' (filled with 'agent1'), 'Password' (masked with dots), 'Confirm Password' (masked with dots), and 'Partition' (filled with 'Qfiniti'). There are also checkboxes for 'Active' and 'Enabled', and a 'View Inactive Members' link. A 'Role' dropdown is set to 'Administrators'.

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.



opentext™ | Qfiniti CE 20.4

Save Spell Check Delete

**Categories**

- General Information
- Licensing**
- Team Access
- Team Memberships
- Team Supervision
- Classifications

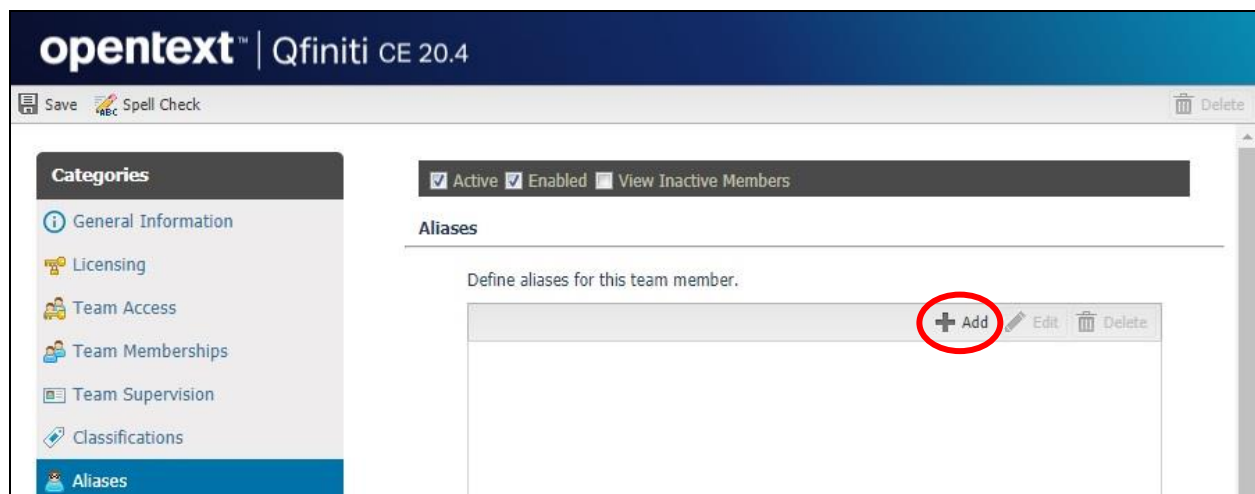
☒ Active ☒ Enabled ☐ View Inactive Members

**Licensing**

☒ Allow Voice Recordings to be performed on this team member

Product	Total Licenses	Available Licenses
Qfiniti Observe Voice	100000	100000

Follow reference [5] to configure subsequent steps for the new agent (not shown). Upon reaching the **Aliases** step, click the **Add** icon to create an alias.



opentext™ | Qfiniti CE 20.4

Save Spell Check Delete

**Categories**

- General Information
- Licensing
- Team Access
- Team Memberships
- Team Supervision
- Classifications
- Aliases**

☒ Active ☒ Enabled ☐ View Inactive Members

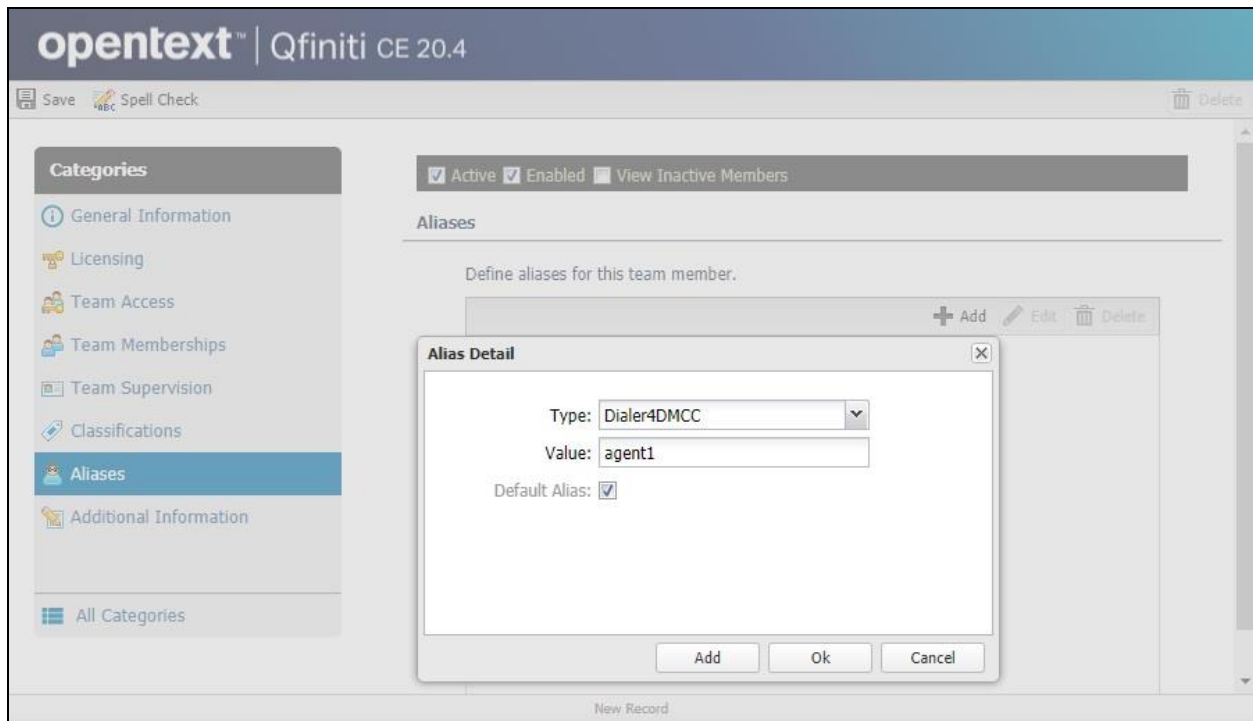
**Aliases**

Define aliases for this team member.

	<b>+ Add</b>	Edit	Delete
--	--------------	------	--------

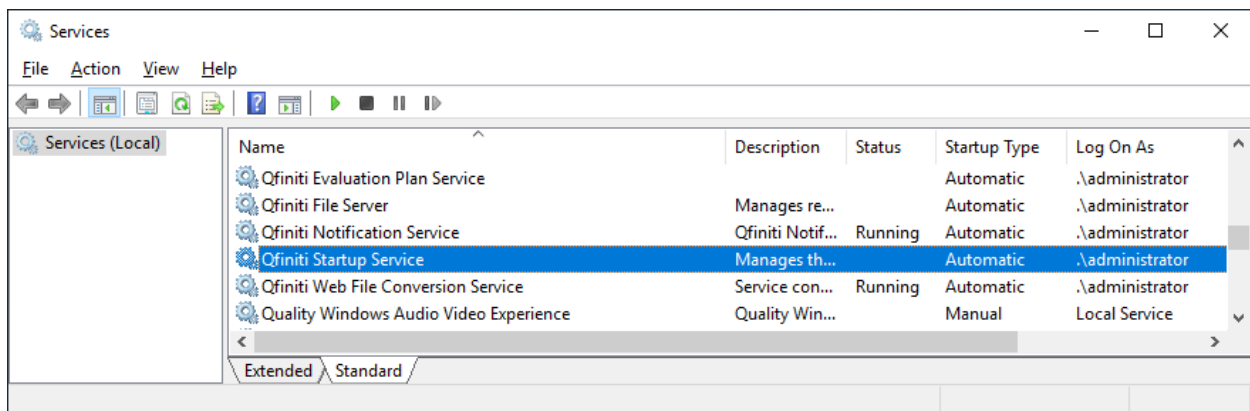
The **Alias Detail** pop-up screen is displayed. For **Type**, select the CTI server name from **Section 9.4**. For **Value**, enter the agent ID for the first line in **Section 9.13** that the agent uses to log into Proactive Contact Agent, in this case “agent1”. Retain the default value in the remaining field.

Repeat this section to add a team member for each line from **Section 9.13**. In the compliance testing, two team members with alias values “agent1” and “agent2” were configured.



## 9.18. Start Service

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



## 10. Verification Steps

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

### 10.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify registration status of the virtual IP softphones by using the “list registered-ip-stations” command. Verify that all virtual IP softphones from **Section 5.6** are displayed along with the IP address of the Application Enablement Services server, as shown below.

```
list registered-ip-stations
```

REGISTERED IP STATIONS			
Station Ext or Orig Port Socket	Set Type/ Net Rgn	Prod ID/ Release	Station IP Address/ Gatekeeper IP Address
65000	9611	IP_Phone	192.168.200.219
tls	1	6.8502	10.64.101.236
65001	9611	IP_Phone	192.168.200.125
tls	1	6.8502	10.64.101.236
<b>65991</b>	<b>4620</b>	<b>IP_API_A</b>	<b>10.64.101.239</b>
<b>tcp</b>	<b>1</b>	<b>6.8502</b>	<b>10.64.101.236</b>
<b>65992</b>	<b>4620</b>	<b>IP_API_A</b>	<b>10.64.101.239</b>
<b>tcp</b>	<b>1</b>	<b>6.8502</b>	<b>10.64.101.236</b>

## 10.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, 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 a session with the Qfiniti user from **Section 6.4**, and that the **# of Associated Devices** reflects the number of lines from **Section 9.13**, as shown below.

**Application Enablement Services**  
**Management Console**

Welcome: User  
 Last login: Wed Feb 24 15:27:41 2021 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: 8.1.3.0.0.25-0  
 Server Date and Time: Fri Feb 26 10:12:40 EST 2021  
 HA Status: Not Configured

Status | Status and Control | **DMCC Service Summary**
Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▼ **Status**
  - Alarm Viewer
  - ▶ Logs
  - ▶ Log Manager
  - ▼ **Status and Control**
    - CVLAN Service Summary
    - DLG Services Summary
    - **DMCC Service Summary**

### DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
Generated on Fri Feb 26 10:12:19 EST 2021

Service Uptime:
3 days, 17 hours 55 minutes

Number of Active Sessions:
1

Number of Sessions Created Since Service Boot:
2

Number of Existing Devices:
2

Number of Devices Created Since Service Boot:
4

■	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	7FB4E7FED8524A62D E004D0F52DBFC43-158	qfiniti	Qfiniti	10.64.101.202	XML Unencrypted	2

Terminate Sessions
Show Terminated Sessions

Item 1-1 of 1  
1 Go

## 10.3. Verify Avaya Proactive Contact

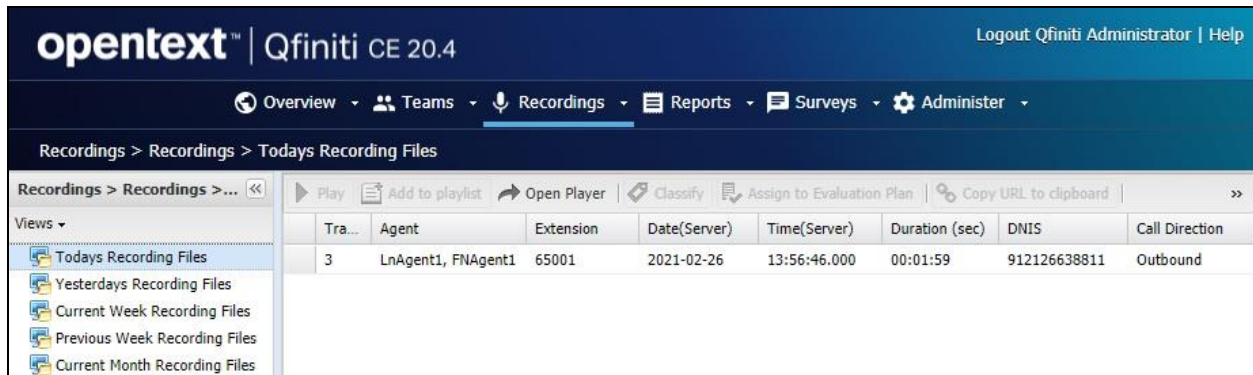
Log in to the Linux shell of Proactive Contact and issue the “netstat | grep ensERVER” command. Verify that there is an entry showing an **ESTABLISHED** connection with IP address of the Qfiniti server, as shown below.

tcp	0	0	lzpds4b:enserver_ssl	10.64.101.202:54304	ESTABLISHED
tcp	0	0	lzpds4b:enserver_ssl	lzpds4b:33464	ESTABLISHED
tcp	0	0	lzpds4b:33464	lzpds4b:enserver_ssl	ESTABLISHED

## 10.4. Verify OpenText Qfiniti

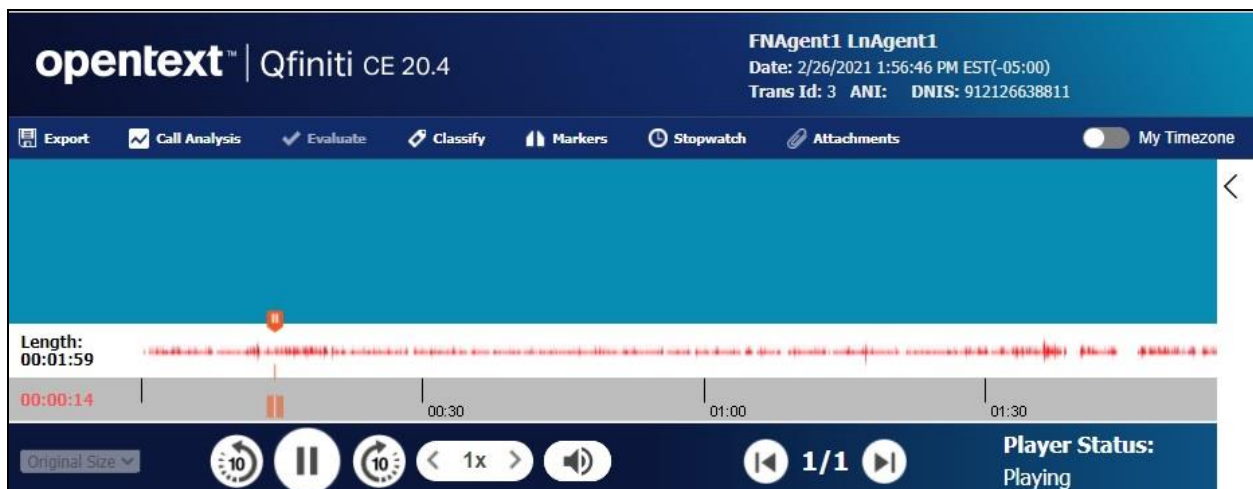
Start a job on Proactive Contact and log an agent in to handle and complete an outbound call. Follow the procedure in **Section 9.15** to launch the Qfiniti web interface, and log in using the appropriate user credentials.

Select **Recordings** → **Recordings** from the top menu, followed by **Todays Recording Files** from the left pane, to display a list of recordings for today. Verify that there is an entry reflecting the last call, with proper values in the relevant fields.



opentext™   Qfiniti CE 20.4		Logout Qfiniti Administrator   Help						
Overview Teams Recordings Reports Surveys Administer								
Recordings > Recordings > Todays Recording Files								
Recordings > Recordings >... <<								
Views >								
Todays Recording Files								
Yesterdays Recording Files								
Current Week Recording Files								
Previous Week Recording Files								
Current Month Recording Files								
Play Add to playlist Open Player Classify Assign to Evaluation Plan Copy URL to clipboard >>								
Tra...	Agent	Extension	Date(Server)	Time(Server)	Duration (sec)	DNIS	Call Direction	
3	LnAgent1, FNAgent1	65001	2021-02-26	13:56:46.000	00:01:59	912126638811	Outbound	

Double click on the entry and verify that the recording can be played back.



## 10.5. Conclusion

These Application Notes describe the configuration steps required for OpenText Qfiniti 20.4 to successfully interoperate with Avaya Proactive Contact 5.2 with PG230 and Avaya Aura® Application Enablement Services 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 8, November 2020, available at <http://support.avaya.com>.
2. *Administering Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 8, December 2020, available at <http://support.avaya.com>.
3. *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 8, February 2021, available at <http://support.avaya.com>.
4. *Administering Avaya Proactive Contact*, Release 5.2, Issue 1, July 2018, available at <http://support.avaya.com>.
5. *OpenText Qfiniti User Guide*, Version 20.4, Rev. 2020-Oct-28, available to existing customers at <https://knowledge.opentext.com/knowledge>.

---

**©2021 Avaya Inc. All Rights Reserved.**

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

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