



Avaya Solution & Interoperability Test Lab

Application Notes for OpenText Qfiniti 20.4 with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 Using Multiple Registration – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for OpenText Qfiniti 20.4 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 using Multiple Registration. Qfiniti is a call recording solution.

In the compliance testing, OpenText Qfiniti used the Telephony Services Application Programming Interface from Avaya Aura® Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager, and the Multiple Registration feature via 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 Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 using Multiple Registration. Qfiniti is a call recording solution.

In the compliance testing, Qfiniti used the Telephony Services Application Programming Interface (TSAPI) from Application Enablement Services to monitor skill groups and agent stations on Communication Manager, and the Multiple Registration feature via Application Enablement Services Device, Media, and Call Control (DMCC) XML interface to capture media associated with the monitored agent stations for call recording.

The TSAPI interface is used by Qfiniti to monitor skill groups and agent stations on Communication Manager. The DMCC interface is used by Qfiniti to register a virtual IP softphone against each monitored agent station to pick up the media for call recording.

When there is an active call at a monitored agent station, Qfiniti is informed of the call via event reports from the TSAPI interface and starts the call recording using media from the associated virtual IP softphone. The event reports are also used to determine when to stop the call recordings.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of Qfiniti, the application automatically performed device queries and requested monitoring of skill groups and agent stations using TSAPI and registered virtual IP softphones against the agent stations using DMCC.

For the manual part of testing, each call was handled manually on the agent phone with generation of unique audio content for recordings. Necessary user actions such as hold and resume were performed from the agent phones 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 Application Enablement Services and Qfiniti logs for proper message exchanges and use of Qfiniti web interface for proper logging and playback of calls.

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

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

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interfaces between Avaya systems and Qfiniti used non-encrypted connections for TSAPI and DMCC messaging, and encrypted SRTP for DMCC media, 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 TSAPI messages in areas of event notification and value queries.
- Use of DMCC services to register virtual IP softphones against agent stations and obtain media for call recording.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, resume, G.711, G.729, forwarding, service observing, long duration, multiple calls, multiple agents, transfer, and conference.

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

2.2. Test Results

All test cases were executed and verified.

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 Application Enablement Services, and of call center devices are not the focus of these Application Notes and will not be described.

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

| Device Type | Extension |
|-----------------------------|--------------------------------|
| Skill Group | 61001, 61002 |
| Agent Station | 65001 (H.323), 66006 (SIP) |
| Agent Station Security Code | 234567 (65001), 123456 (66006) |
| Agent ID | 65881, 65882 |

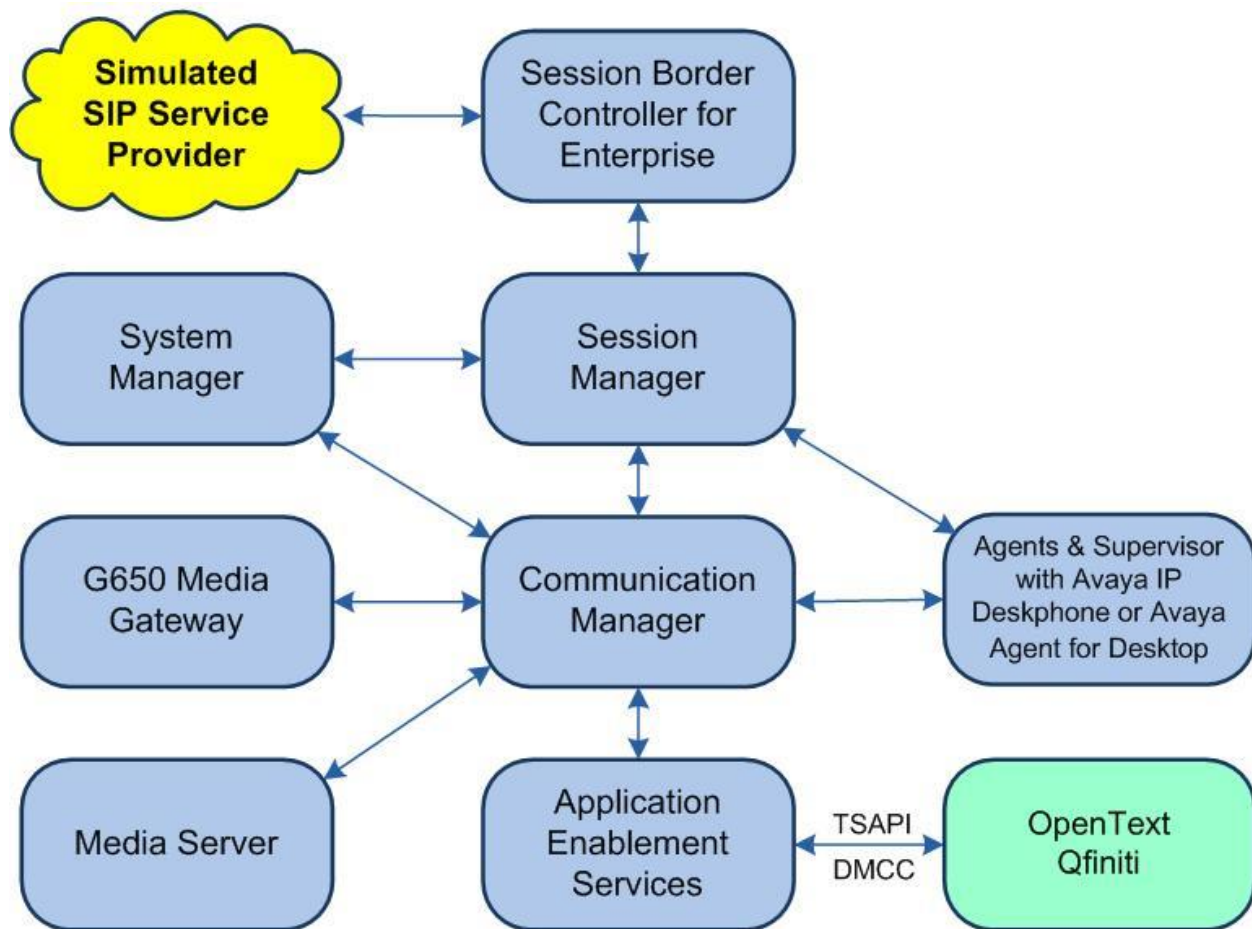


Figure 1: Compliance Testing Configuration

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)Avaya DMCC XML | 20.4.0 with QF-18193 & QF-18501 Standard 8.1.3.25 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 CTI link
- Administer IP codec set
- Administer agent stations

5.1. Verify License

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

| | | |
|---|--|--------------|
| display system-parameters customer-options | | Page 4 of 12 |
| OPTIONAL FEATURES | | |
| Abbreviated Dialing Enhanced List? y | Audible Message Waiting? y | |
| Access Security Gateway (ASG)? n | Authorization Codes? y | |
| Analog Trunk Incoming Call ID? y | CAS Branch? n | |
| A/D Grp/Sys List Dialing Start at 01? y | CAS Main? n | |
| Answer Supervision by Call Classifier? y | Change COR by FAC? n | |
| ARS? y | Computer Telephony Adjunct Links? y | |
| ARS/AAR Partitioning? y | Cvg Of Calls Redirected Off-net? y | |
| ARS/AAR Dialing without FAC? y | DCS (Basic)? y | |
| ASAI Link Core Capabilities? y | DCS Call Coverage? y | |
| ASAI Link Plus Capabilities? y | DCS with Rerouting? y | |

5.2. Administer CTI Link

Add a CTI link using the “**add cti-link n**” command, where “n” is an available CTI link number. Enter an available extension number in the **Extension** field.

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 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 **Media Encryption**, make certain that “**1-srtp-aescm128-hmac80**” is included, which will be the media encryption method used with Qfiniti.

In the compliance testing, this IP codec set was assigned to the agent stations.

```
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:
```

5.4. Administer Agent Stations

Use the “**change station n**” command, where “**n**” is the first H.323 agent station extension from **Section 3**. Enable **IP SoftPhone**, to allow a virtual IP softphone to be registered against the station.

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 4 |
| STATION | | |
| Extension: 65001 | Lock Messages? n | BCC: 0 |
| Type: 9611 | Security Code: * | TN: 1 |
| Port: S000106 | Coverage Path 1: 1 | COR: 1 |
| Name: CM Station 1 | Coverage Path 2: | COS: 1 |
| Unicode Name? n | Hunt-to Station: | Tests? y |
| STATION OPTIONS | | |
| Time of Day Lock Table: | | |
| Loss Group: 19 | Personalized Ringing Pattern: 1 | |
| | Message Lamp Ext: 65001 | |
| Speakerphone: 2-way | Mute Button Enabled? y | |
| Display Language: English | Button Modules: 0 | |
| Survivable GK Node Name: | | |
| Survivable COR: internal | Media Complex Ext: | |
| Survivable Trunk Dest? y | IP SoftPhone? y | |
| | IP Video Softphone? n | |
| | Short/Prefixed Registration Allowed: default | |
| | Customizable Labels? y | |

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 H.323 gatekeeper
- Administer Qfiniti user
- Administer security database
- Administer ports
- 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, there 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, another 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 shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title 'Application Enablement Services Management Console'. On the right, a welcome message for 'User' is displayed, including login details and system information. A red navigation bar at the top contains 'Home', 'Help', and 'Logout' links. A left sidebar lists various service categories: 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 notes 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 shows the Avaya Application Enablement Services Management Console with the 'Licensing' section selected. The top header and welcome message are the same as in the previous screenshot. The red navigation bar now shows 'Licensing' as the active page. The left sidebar highlights 'Licensing' and shows sub-options: WebLM Server Address, WebLM Server Access, and Reserved Licenses. The main content area is titled 'Licensing' and provides instructions for setting up and maintaining the WebLM, including the need to use WebLM Server Address, WebLM Server Access, and 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 **Device Media and Call Control** and **TSAPI Simultaneous Users**, as shown below. The DMCC license is used for the virtual IP softphones, and the TSAPI license is used for device monitoring.

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

- 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
 - CCTR
 - ContactCenter
 - COMMUNICATION_MANAGER

The right pane displays the **Application Enablement (CTI) - Release: 8 - SID: 10503000 (Enterprise license)** screen. It includes the following information:

- You are here: Licensed Products > Application_Enablement > View by Feature
- License installed on: August 8, 2019 4:43:51 PM -05:00
- License File Host IDs: 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" 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 H.323 Gatekeeper

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

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top right corner displays user information: 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. The main header is "Communication Manager Interface | Switch Connections" with links for Home, Help, and Logout. The left sidebar shows a navigation menu with "Communication Manager Interface" expanded, and "Switch Connections" selected. The main content area is titled "Switch Connections" and contains a table with the following data:

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

Below the table are buttons: Edit Connection, Edit PE/CLAN IPs, Edit H.323 Gatekeeper, Delete Connection, and Survivability Hierarchy.


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

The screenshot shows the Avaya Application Enablement Services Management Console with the "Edit H.323 Gatekeeper - cm7" screen. The top right corner displays the same user information as the previous screenshot. The main header is "Communication Manager Interface | Switch Connections" with links for Home, Help, and Logout. The left sidebar shows the same navigation menu. The main content area is titled "Edit H.323 Gatekeeper - cm7" and contains a text input field with the value "10.64.101.236" and a button "Add Name or IP". Below the input field are buttons "Delete IP" and "Back".

6.5. Administer Qfiniti 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.

**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 User

Home | 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

6.6. 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 Qfiniti user from **Section 6.5**.

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 in the top right corner states: "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", and "HA Status: Not Configured".

The main navigation bar is red and contains the breadcrumb "Security | Security Database | Control" and links for "Home | Help | Logout". The left sidebar shows a tree view of the application's structure, with "Security" expanded and "Control" selected under "Security Database".

The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services". It contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". Below these checkboxes is an "Apply Changes" button.

6.7. Administer Ports

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

In the **DMCC Server Ports** section, select the radio button for **Unencrypted Port** 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: 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

Networking | Ports

Home | 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

Enabled Disabled

Encrypted TCP Port9998

Enabled Disabled

DLG Port

TCP Port5678

TSAPI Ports

TSAPI Service Port450

Enabled Disabled

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

Enabled Disabled

Encrypted Port4722

Enabled Disabled

TR/87 Port4723

Enabled Disabled

6.8. Restart Services

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

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

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 checked="" type="checkbox"/> TSAPI Service | Running |

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

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart Web Server

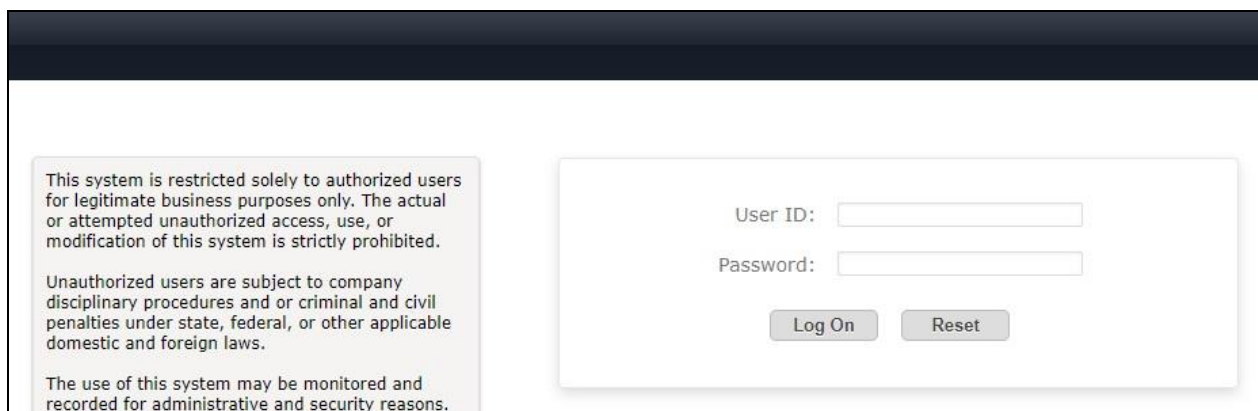
7. Configure Avaya Aura® Session Manager

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

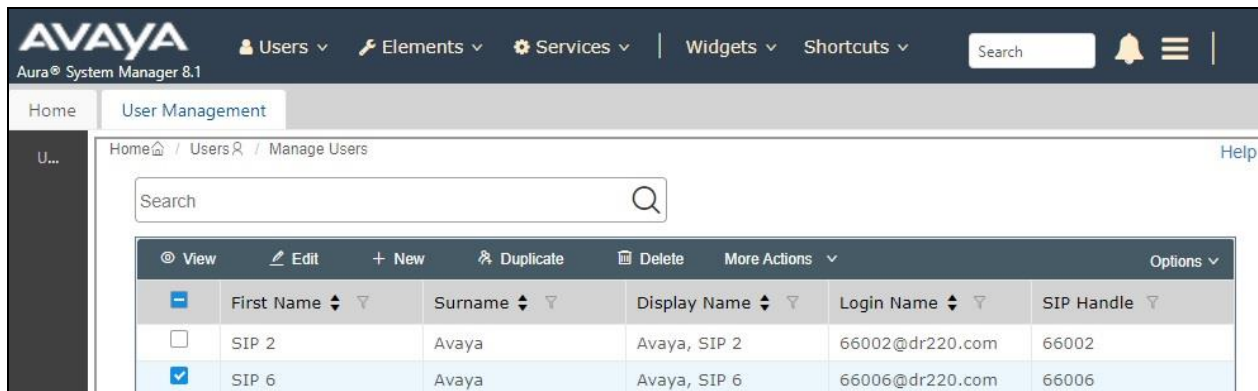
Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.



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 “**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 menu items 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 configuring the user profile, including System (DR-CM), Profile Type (Endpoint), Extension (66006), Set Type (J169CC), Port (S000115), and Voice Mail Number (admin). A blue Editor icon is visible next to the Extension field, highlighted with a red box.

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

The screenshot shows the 'Edit Endpoint' configuration page in the Avaya Aura System Manager 8.1 interface. The page is divided into several sections for configuring endpoint settings.

Top Navigation: AVAYA Aura® System Manager 8.1. Menu items include Users, Elements, Services, Widgets, and Shortcuts. A search bar and notification bell are also present.

Breadcrumbs: Home / Users / Manage Users

Page Title: Edit Endpoint

Buttons: Done, [Save As Template]

Form Fields:

- System:** DR-CM
- Extension:** 66006
- Template:** Select (dropdown)
- Set Type:** J169CC
- Port:** S000115
- Security Code:** (empty)
- Name:** Avaya, SIP 6

Tabs: General Options (G) *, Feature Options (F), Site Data (S), Abbreviated Call Dialing (A), Enhanced Call Fwd (E), Button Assignment (B), Profile Settings (P), Group Membership (M)

General Options (G) * Fields:

- * Class of Restriction (COR): 1
- * Emergency Location Ext: 66006
- * Tenant Number: 1
- * SIP Trunk: Qaar
- Coverage Path 1: (empty)
- Lock Message: ☐
- Multibyte Language: Not Applicable (dropdown)
- SIP URI: (empty)

Other Fields:

- * Class Of Service (COS): 1
- * Message Lamp Ext.: 66006
- Type of 3PCC Enabled:** Avaya (dropdown, highlighted with a red box)
- Coverage Path 2: (empty)
- Localized Display Name: Avaya, SIP 6
- Enable Reachability for Station Domain Control: system (dropdown)

Select the **Feature Options** tab in the right pane. Scroll the screen as necessary and check **IP Softphone** as shown below. Retain the existing values in the remaining fields.

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

The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and various menu items: Users, Elements, Services, Widgets, and Shortcuts. A search bar and notification bell are also present. The main content area is titled 'User Management' and shows a list of users on the left. The right pane is open to the 'Feature Options (F)' tab for a selected user. This tab contains several configuration sections: 'General Options (G)', 'Site Data (S)', 'Abbreviated Call Dialing (A)', 'Enhanced Call Fwd (E)', 'Button Assignment (B)', 'Profile Settings (P)', and 'Group Membership (M)'. The 'Profile Settings (P)' section is active and contains two columns of settings. The left column includes 'Active Station Ringing' (set to 'single'), 'MWI Served User Type' (set to 'None'), 'Per Station CPN - Send Calling Number' (set to 'None'), 'IP Phone Group ID' (empty), 'Remote Soft Phone Emergency Calls' (set to 'as-on-local'), 'LWC Reception' (set to 'spe'), 'AUDIX Name' (set to 'None'), 'EC500 State' (set to 'enabled'), 'Voice Mail Number' (empty), and 'Music Source' (empty). The right column includes 'Auto Answer' (set to 'none'), 'Coverage After Forwarding' (set to 'system'), 'Display Language' (set to 'english'), 'Hunt-to Station' (empty), 'Loss Group' (set to '19'), 'Survivable COR' (set to 'internal'), 'Time of Day Lock Table' (set to 'None'), and 'Bridging Tone for This Extension' (set to 'no'). Below these sections is a 'Features' section with a list of checkboxes. The 'IP SoftPhone' checkbox is checked and highlighted with a red box. Other checked features include 'Coverage Message Retrieval' and 'Direct IP-IP Audio Connections'. Other unchecked features include 'Always Use', 'IP Audio Hairpinning', 'Bridged Call Alerting', 'Bridged Idle Line Preference', 'Idle Appearance Preference', 'LWC Activation', and 'CDR Privacy'.

8. Configure OpenText Qfiniti

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


- Launch SysConfig web interface
- Administer switches
- Administer 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 services

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

8.1. Launch SysConfig Web Interface

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

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

The image shows the Opentext login interface. 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 web interface. At the top, there's a header with the 'opentext' logo, 'Qfiniti SysConfig CE 20.4', and a 'Logout Qfiniti Administrator' link. Below the header, there are two tabs: 'General' and 'Cross System', with 'Cross System' being the active tab. Under the 'Cross System' tab, there are two buttons: 'Save' and 'Refresh'. Below these buttons, there are four expandable sections: 'Switches', 'CTI Server', 'Board Configuration', and 'Simulated CTI Scripts'. Each section has a dropdown arrow on the right side.

8.2. Administer Switches

Expand the **Switches** sub-section and click the **New Item** icon to add a new entry for DMCC 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 “AES4DMCC”.
- **Switch Model:** “Avaya AES/CM”
- **Post Release Delay:** Desired wait interval in seconds for registration response.
- **Observe Mode:** “By Extension”
- **Interface Type:** “DMCC / TAPI / DRLink”
- **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 6.5**.
- **Password:** The Qfiniti user credentials from **Section 6.5**.

The screenshot shows the OpenText Qfiniti Administrator interface. The 'Switch' configuration window is open, displaying various fields for configuring a switch connection. The fields are as follows:

| Field | Value |
|------------------------------|--------------------------|
| Name | AES4DMCC |
| Switch Model | Avaya AES/CM |
| Vendor | |
| Post Release Delay | 1 |
| Observe Mode | By Extension |
| Observe String | |
| Interface Type | DMCC / TAPI / DRLink |
| Use CTI Source for Alias | <input type="checkbox"/> |
| APC Dialer in use? | No |
| Avaya CM Hostname | cm7 |
| Port | 4721 |
| 1st Line Appearance | 263 |
| AES IP Address | 10.64.101.239 |
| Service Observe Button | 268 |
| User Name | qfiniti |
| Password | ***** |
| AES Connection Alarm Trigger | Never |
| Wait Before Dial | 500 |
| Busy Repeat Max | 6 |
| Survey Excluded Extensions | Enter Value |
| Alt. AES IP Address | |

The 'Ok' and 'Cancel' buttons are at the bottom right of the window. In the background, the 'Switches' table is visible with columns 'Name' and 'Switch', showing entries 'AES4DMCC' and 'AvayaSIPREC'. A red circle highlights the '+' icon in the 'Switches' table header.

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 Qfiniti user credentials from **Section 6.5**.
- **Password:** The Qfiniti user credentials from **Section 6.5**.
- **Vendor:** “AVAYA”
- **Driver:** The relevant switch connection name from **Section 6.3**.
- **Service:** “CSTA”

The screenshot displays the Qfiniti SysConfig CE 20.4 application. The main window has a sidebar on the left with tabs for 'General' and 'Cross System'. Under 'Cross System', there are sections for 'Switches', 'CTI Server', 'Board Configuration', and 'Simulated CTI Scripts'. The 'CTI Server' section is expanded, showing a list of servers with 'AvayaTSAPI' selected. A 'CTI Server' configuration dialog box is open in the center, containing the following fields and values:

| Field | Value |
|----------------------|-------------|
| Name | AvayaTSAPI |
| Type | Avaya TSAPI |
| Available Switch | AES4DMCC |
| 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 |

At the bottom of the dialog are 'Ok' and 'Cancel' buttons. On the right side of the main window, a red circle highlights a '+' icon, indicating the 'New Item' button.

8.4. 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 displays the Qfiniti SysConfig CE 20.4 interface. The 'Board Configuration' dialog box is open, showing the following fields:

- 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 background interface shows the 'Board Configuration' section expanded, with a red circle highlighting the '+' icon for adding a new item.

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 “DMCC Logger”.
- **Switch:** Select the switch name from **Section 8.2**.
- **System Type:** Check **Voice Recording - Logging**.

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 shows a list of systems, with 'DMCC Logger' selected. The main area is titled 'General' and contains the following fields and options:

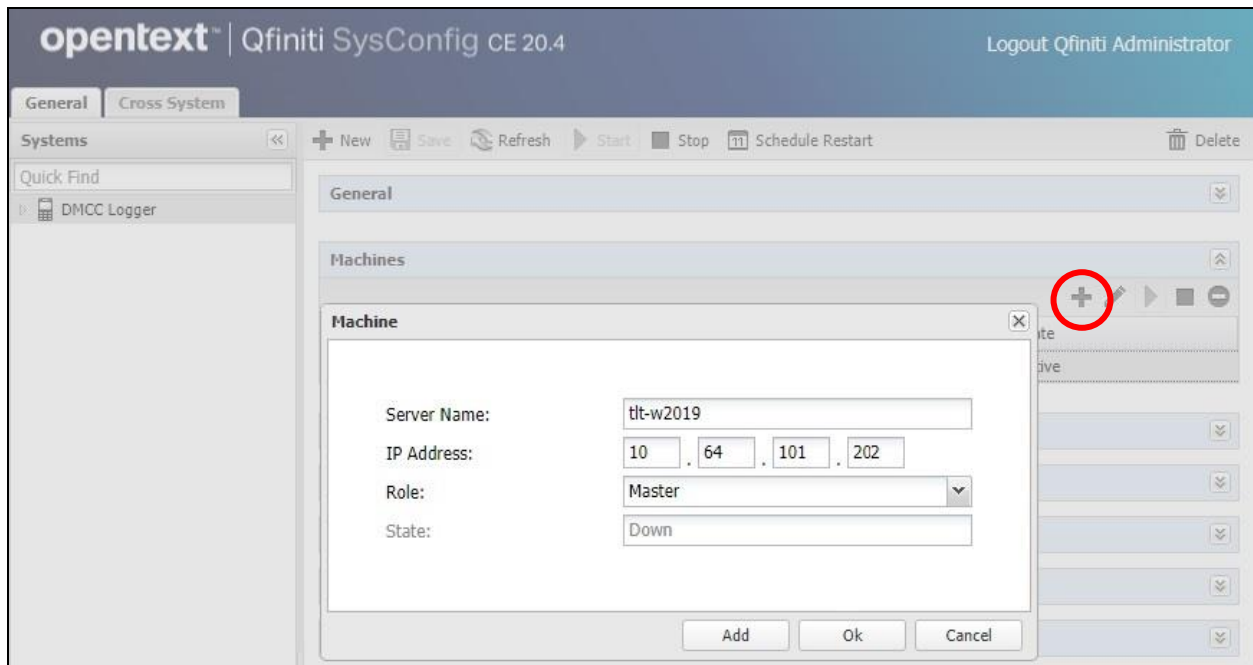
- Name:** DMCC Logger
- Switch:** AES4DMCC
- System Type:**
 - ☒ Voice Recording - Logging
 - ☐ Voice Recording - QA
 - ☐ Screen Recording
 - ☐ Remote Screen Site
 - ☐ Explore
 - ☐ Survey
 - ☐ Backup
 - ☐ Cloud Connector
- Description:** (Empty text box)
- ☐ Available for Use
- ☐ NAT Environment

Below the 'General' section, there 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 Qfiniti server.
- **IP Address:** The IP address of the Qfiniti server.
- **Role:** “Master”.



8.7. Administer Components

Expand the **Components** sub-section and follow reference [4] 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:** Select the pertinent codec, in this case “PCM G.711”.
- **Encryption type:** “Avaya SRTP 128/80”
- **PCM Acquisition:** “Media Streaming”

The screenshot displays the 'opentext | Qfiniti SysConfig CE 20.4' interface. The top navigation bar includes 'General' and 'Cross System' tabs, and a 'Logout Qfiniti Administrator' link. The main area is divided into three sections: 'Systems', 'Components', and 'Component Data'.

Systems: A sidebar with a 'Quick Find' search bar and a list containing 'DMCC Logger'.

Components: A central panel with two columns. The 'Available Components' column lists various services, including 'Logger Voice Recording Manager'. The 'Assigned Components' column lists assigned services, with 'Logger Voice Recording Manager' highlighted. Arrows between the columns allow for moving components.

Component Data: A form for configuring the selected component. The fields and their values are as follows:

| Field | Value |
|-----------------------------------|----------------------|
| Post Service Observe dial string: | |
| Optimal Recording CODEC: | PCM G.711 |
| Encryption type: | Avaya SRTP 128/80 |
| CTI Late Attach Method: | ConnectionID |
| DN Late Attach Window In Sec: | 30 |
| PCM Acquisition: | Media Streaming |
| Transaction Validation: | No |
| Transaction Validation Form: | trans_validation.xsl |
| Service Observe fail retry delay: | 30 |
| Start Recording On: | Alerting |
| CTI Init: | On Startup |
| Line Reset Threshold in Sec: | 0 |
| VoIP Transcoding: | NONE |

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**.
- **Agent Extensions:** The agent station extensions from **Section 3**.

The screenshot displays the Qfiniti SysConfig CE 20.4 interface. The top navigation bar includes the 'opentext' logo, 'Qfiniti SysConfig CE 20.4', and a 'Logout Qfiniti Administrator' link. The main interface is divided into a left sidebar and a central content area. The sidebar contains a 'Systems' section with a 'Quick Find' bar and a 'DMCC Logger' icon. The central content area has a 'General' tab selected, showing a list of 'Machines' and 'Components'. A 'CTI Sources' section is expanded, revealing a list of machines, including 'tlt-w2019'. A red circle highlights the '+' icon in the top right corner of the 'CTI Sources' list, indicating the 'Add CTI Source' action. A modal window titled 'CTI Source' is open, showing the following fields and values:

| Field | Value |
|------------------------|-----------------------------------|
| CTI Server: | AvayaTSAPI |
| PreInitExtensions: | Yes |
| Queue: | 61001-61002 |
| Agent Extensions: | 65001, 66006 |
| UUdata script name: | CTI_UUdataScripts_AVAYA_TSAPI.ini |
| Auto Login Extensions: | Enter Value |

The modal window also includes 'Ok' and 'Cancel' buttons at the bottom right.

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:** “Logger”
- **Phone Interface Type:** “DMCC Ver 7.0 & Up”
- **Number of Lines:** The total number of agent stations from **Section 3**, in this case “2”.

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 'Systems' section on the left contains a 'Quick Find' bar and a list of systems, including 'DMCC Logger'. The main content area shows a list of system components: 'General', 'Machines', 'Components', 'CTI Sources', and 'Phone Interface'. The 'Phone Interface' component is selected, and a configuration dialog box is open. The dialog box contains the following fields and values:

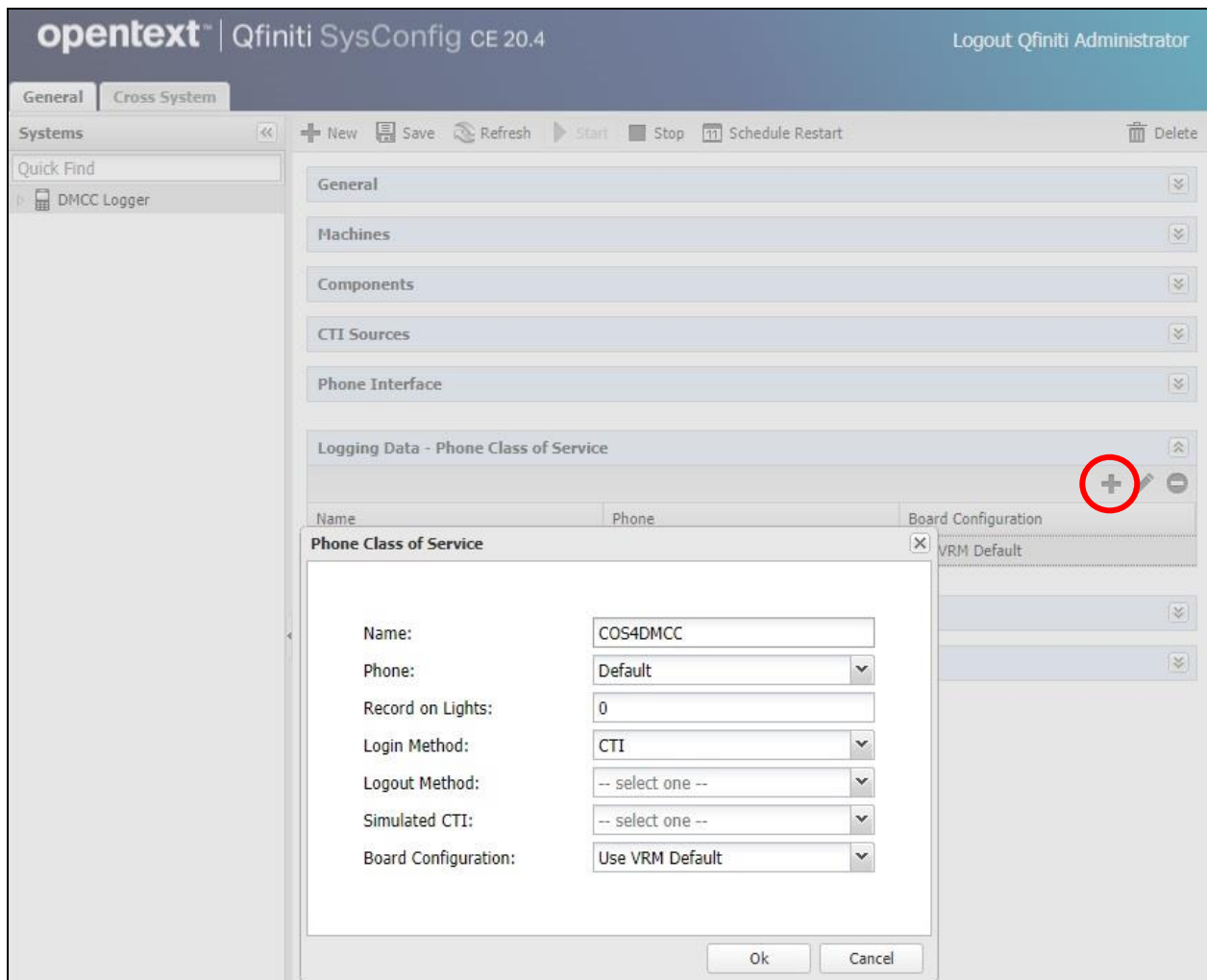
| Field | Value |
|----------------------|-------------------|
| Server Name | tlt-w2019 |
| Machine Type | Logger |
| Phone Interface Type | DMCC Ver 7.0 & Up |
| Number of Lines | 2 |
| RTP Port Range | 11000 - 11003 |
| RecMgr RTP IP | 0 . 0 . 0 . 0 |

The dialog box has 'Ok' and 'Cancel' buttons at the bottom. A red circle highlights the 'Edit' icon (a pencil) in the top right corner of the 'Phone Interface' list item.

8.10. 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”.



8.11. 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 “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 8.10**.
- **Default Board Config:** Select the board name from **Section 8.4**.

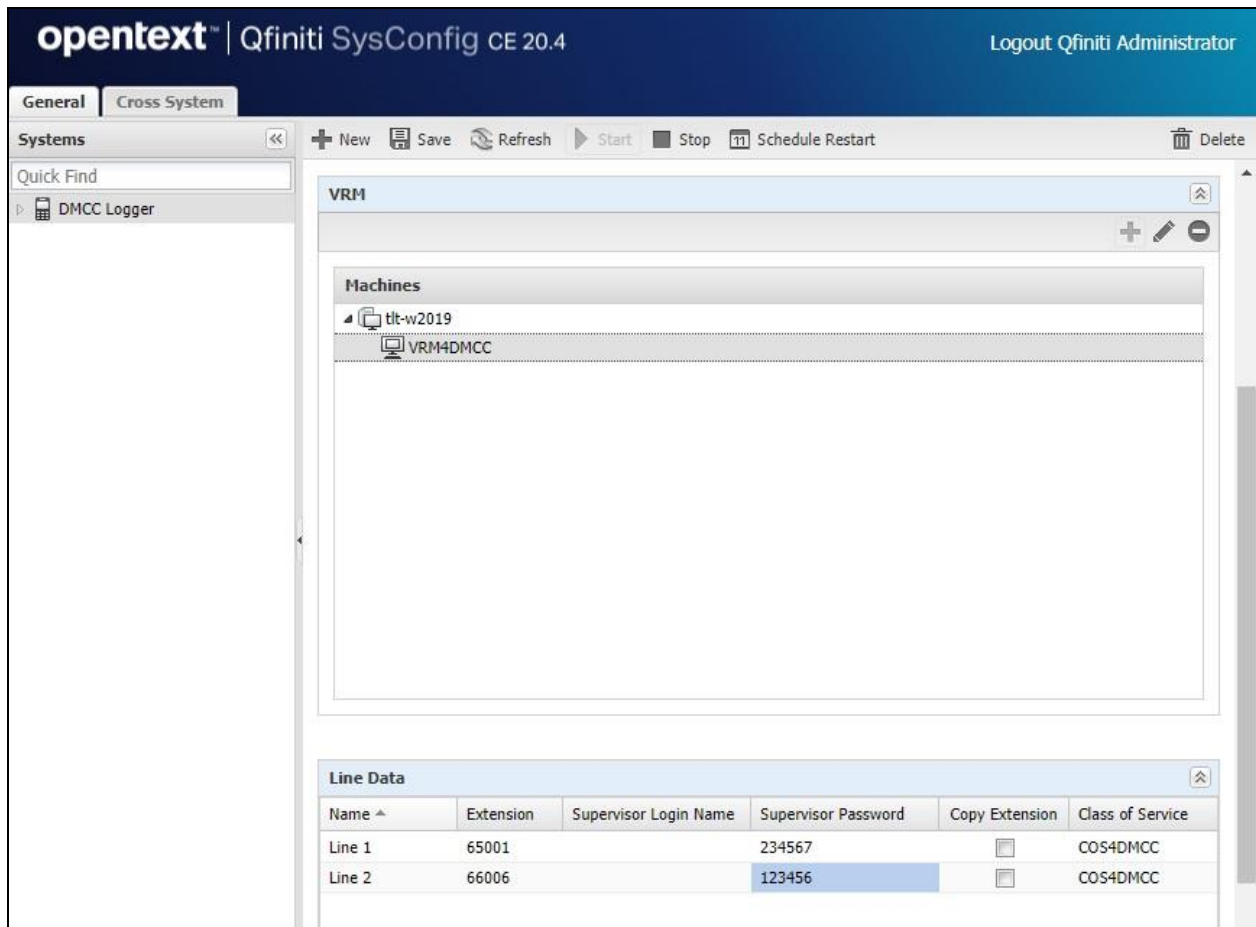
The screenshot displays the opentext Qfiniti SysConfig CE 20.4 web interface. The top navigation bar includes the opentext logo, the product name, and a 'Logout Qfiniti Administrator' link. Below the navigation bar, there are tabs for 'General' and 'Cross System'. The main area is divided into a left sidebar with a 'Quick Find' search bar and a list of system components, and a central pane showing a tree view of system components. The 'VRM' component is selected and expanded, revealing a list of machines. A red circle highlights the '+ Add' button next to the machine list. A modal window titled 'VRM' is open, showing the configuration fields for a new VRM entry. The fields are as follows:

| Field | Value |
|------------------------------|---|
| VRM Name: | VRM4DMCC |
| VRM Type: | Logging |
| Mirror from VRM: | -- select one -- |
| Interface Type: | Station Side DMCC |
| Use Range: | <input checked="" 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 |

8.12. Administer Line Data

Select the newly added VRM from **Section 8.11**, and expand the **Line Data** sub-section. Select the first line. For **Extension** and **Supervisor Password**, enter the first agent station extension and the associated security code from **Section 3** respectively.

Repeat this section to administer all agent station extensions from **Section 3**, as shown below.

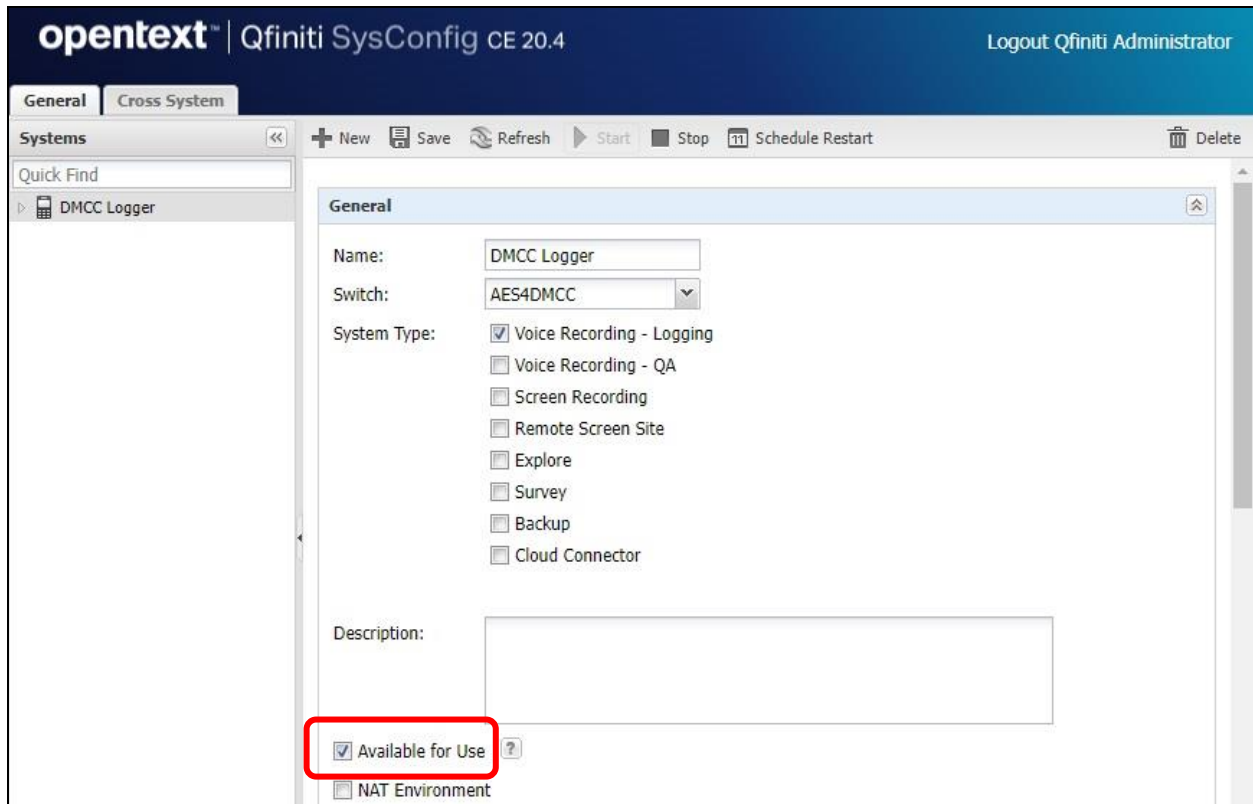


The screenshot displays the opentext Qfiniti SysConfig CE 20.4 interface. The top navigation bar includes the opentext logo, the product name, and a 'Logout Qfiniti Administrator' link. Below the navigation bar, there are tabs for 'General' and 'Cross System'. The 'Systems' section is active, showing a list of systems with a 'Quick Find' search bar. The 'DMCC Logger' system is selected. The main content area shows the 'VRM' configuration page. Under the 'Machines' section, the 'VRM4DMCC' machine is listed. The 'Line Data' table is visible at the bottom, showing two lines with their respective extensions and supervisor passwords.

| Name ^ | Extension | Supervisor Login Name | Supervisor Password | Copy Extension | Class of Service |
|--------|-----------|-----------------------|---------------------|--------------------------|------------------|
| Line 1 | 65001 | | 234567 | <input type="checkbox"/> | COS4DMCC |
| Line 2 | 66006 | | 123456 | <input type="checkbox"/> | COS4DMCC |

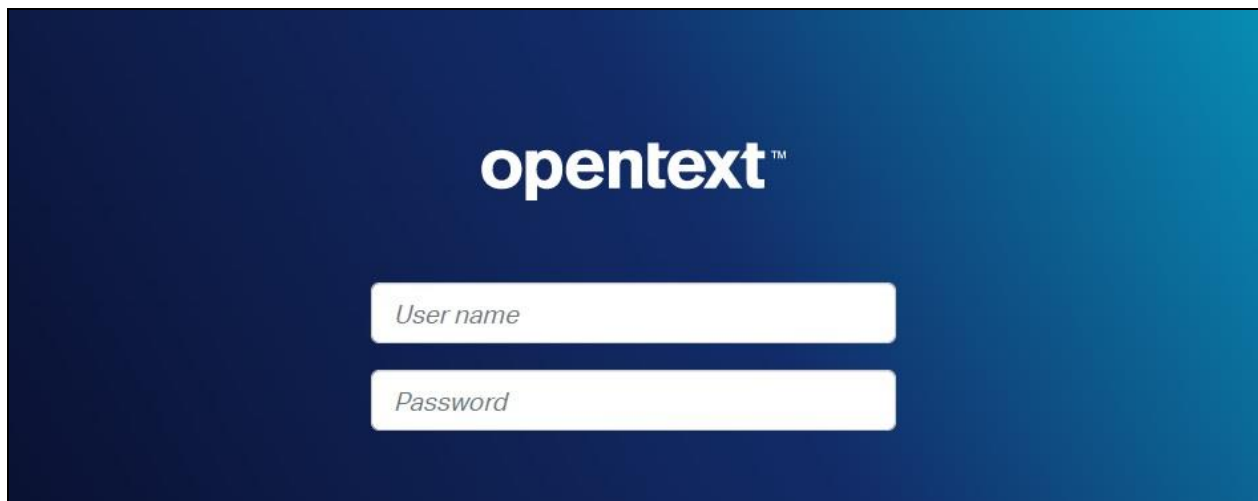
8.13. Enable Use

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



8.14. 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.



8.15. Administer Observe Settings

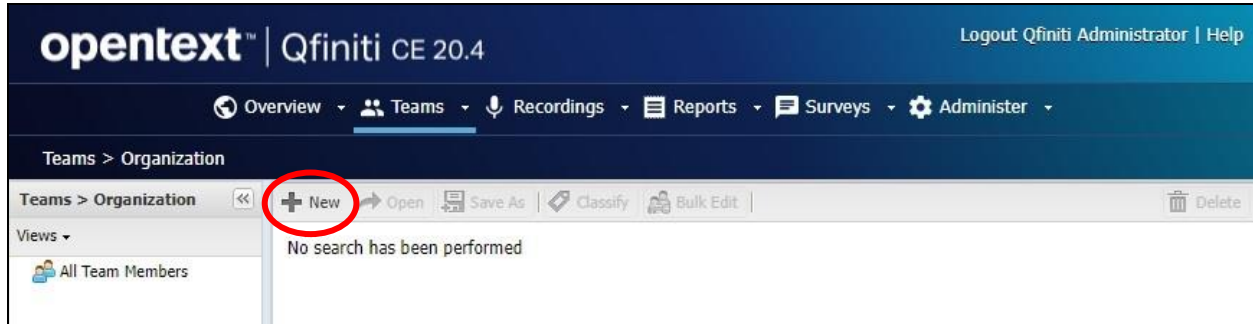
In the subsequent screen (not shown), select **Administer** → **Settings** from the top menu, followed by **Observe Settings** in the left pane.

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 displays the OpenText Qfiniti CE 20.4 interface. The top navigation bar includes 'Overview', 'Teams', 'Recordings', 'Reports', 'Surveys', and 'Administer'. The left sidebar shows a tree view with 'Observe Settings' selected. The main content area is titled 'Administer > Settings > Observe Settings' and contains a 'Save' button. The 'Recording Options' section instructs the user to 'Select the option and check the boxes to activate the desired recording options.' It features a dropdown menu for 'Option' set to 'Continuous Record' and four checkboxes under 'Type': 'Allow voice recordings' (checked), 'Allow screen recordings', 'Allow voice and screen recordings', and 'Allow screen recordings on transfer'. Below this is the 'Phone Player' section, which prompts the user to 'Enter the UNC path to store the phone player prompts.' and includes a text input field for the 'UNC Path'.

8.16. 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 'New Agent' form in the OpenText Qfiniti CE 20.4 interface. The left sidebar lists categories: General Information, Licensing, Team Access, Team Memberships, Team Supervision, Classifications, Aliases, and Additional Information. The main form area has a 'General Information' section with the following fields: Id (4), First Name (Agent1), Middle Name, Last Name (Avaya), Email Address, Role (Administrators), Username (agent1), Password, Confirm Password, and Partition (Qfiniti). There are checkboxes for 'Active' and 'Enabled', and a 'View Inactive Members' link. An 'Add Role' button is also present.

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 | 99998 |

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.

opentext™ | Qfiniti CE 20.4

Save Spell Check Delete

Categories

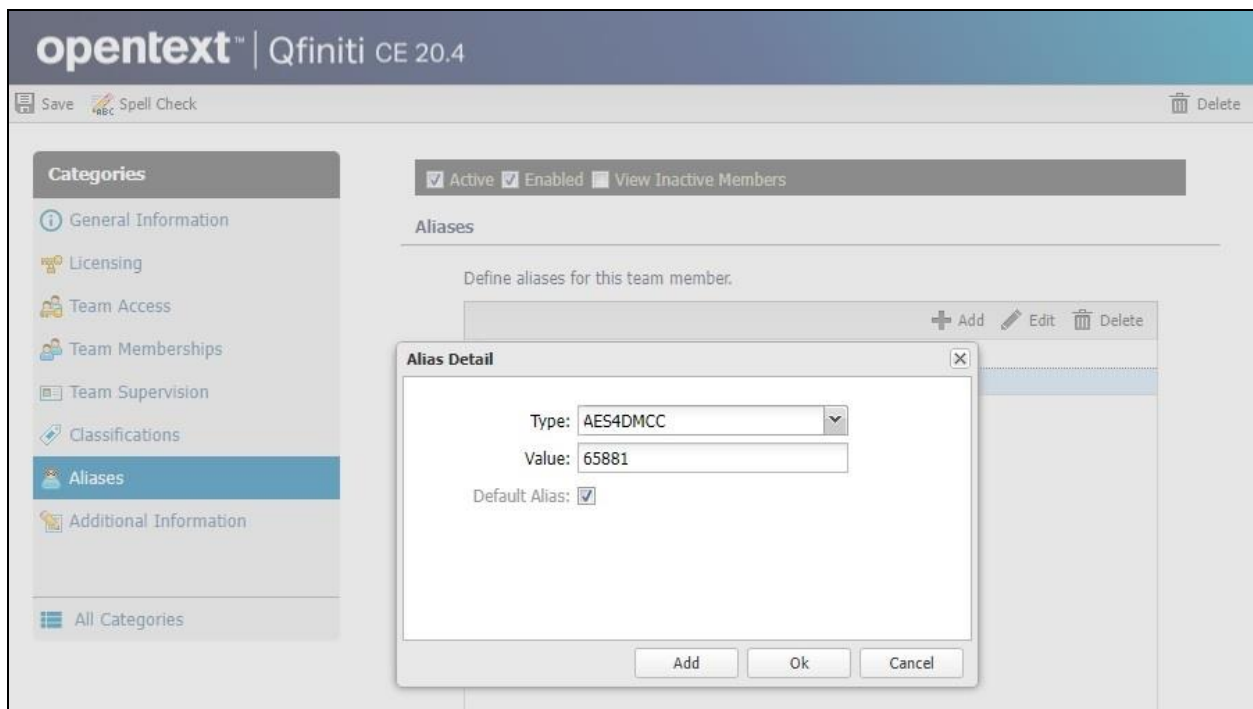
- General Information
- Licensing
- Team Access
- Team Memberships
- Team Supervision
- Classifications
- Aliases**
- Additional Information

☒ Active ☒ Enabled ☐ View Inactive Members

Aliases

Define aliases for this team member.

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.



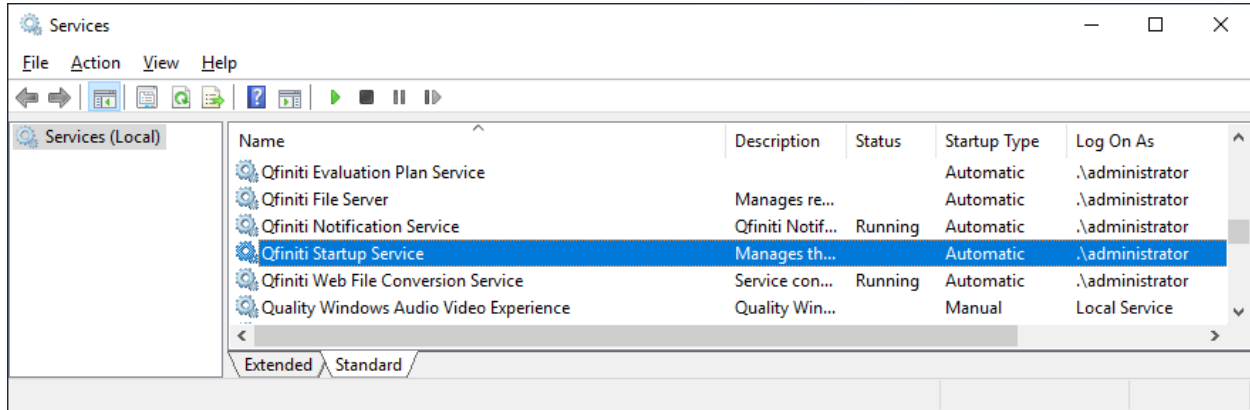
Repeat this section to add a team member for each agent from **Section 3**. In the compliance testing, two team members with alias values “**65881**” and “**65882**” were configured.

The screenshot shows the OpenText Qfiniti CE 20.4 interface with the 'Teams > Organization > All Team Members' view. The table lists team members with columns for First Name, Middle Name, Last Name, Login ID, Status, and Account Disabled. The table includes three rows: Qfiniti Administrator, Agent1, and Agent2.

| 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 |

8.17. 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, and Qfiniti.

9.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify status of 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 | 25 | 25 |

Verify registration status of virtual IP softphones by using the “**list registered-ip-stations**” command. Verify that all monitored agent stations from **Section 3** 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 | 192.168.200.179 |
| tls | 1 | 6.8502 | 10.64.101.236 |
| 65001 | 9611 | IP_Phone | 192.168.200.212 |
| tls | 1 | 6.8502 | 10.64.101.236 |
| 65001 | 9611 | IP_API_A | 10.64.101.239 |
| tcp | 1 | 3.2040 | 10.64.101.236 |
| 66006 | J169CC | IP_API_A | 10.64.101.239 |
| tcp | 1 | 3.2040 | 10.64.101.236 |

9.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify status of the DMCC service by selecting **Status** → **Status and Control** → **DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

Verify the **User** column shows an active session with the Qfiniti user name from **Section 6.5**, and that the **# of Associated Devices** column reflects the number of monitored agent stations from **Section 3**, in this case “2”, as shown below.

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

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

Switch Conn Summary

TSAPI 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 Tue Jan 18 16:50:09 EST 2022

Service Uptime: 0 days, 0 hours 3 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 1

Number of Existing Devices: 2


Number of Devices Created Since Service Boot: 2

| | Session ID | User | Application | Far-end Identifier | Connection Type | # of Associated Devices |
|--------------------------|--|---------|-------------|--------------------|--------------------|-------------------------|
| <input type="checkbox"/> | 564DE090AA285FAF6 DBD3A6BCB202F02-0 | qfiniti | Qfiniti | 10.64.101.202 | XML Unencrypted | 2 |

Terminate Sessions Show Terminated Sessions

Item 1-1 of 1
1 Go

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**, in this case “**4**”.



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 16:51:31 EST 2022

HA Status: Not Configured

Status | Status and Control | TSAPI Service Summary

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▶ Log Manager

▼ Status and Control

■ CVLAN Service Summary

■ DLG Services Summary

■ DMCC Service Summary

■ Switch Conn Summary


■ TSAPI Service Summary

TSAPI Link Details

☐ Enable page refresh every

60

 seconds

| | Link | Switch Name | Switch CTI Link ID | Status | Since | State | Switch Version | Associations | Msgs to Switch | Msgs from Switch | Msgs Period |
|---|------|-------------|--------------------|---------|--------------------------|--------|----------------|--------------|----------------|------------------|-------------|
|  | 1 | cm7 | 1 | Talking | Tue Jan 18 16:45:13 2022 | Online | 18 | 4 | 20 | 22 | 30 |

Online

Offline

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

TSAPI Service Status

TLINK Status

User Status

9.3. Verify OpenText Qfiniti

Log an agent in to handle and complete an ACD call. Follow the procedure in **Section 8.14** 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.

| Tra... | Date(Server) | Time(Server) | Duratio... | Ext... | Agent | Call Direction | ANI | DNIS |
|--------|--------------|--------------|------------|--------|---------------|----------------|-------------|-------------|
| 222 | 2022-01-19 | 09:04:33.000 | 00:01:20 | 65001 | Avaya, Agent1 | Inbound | 12126630031 | 13035360001 |

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

Length: 00:01:20

00:00:17

00:30 01:00

Original Size

1x

Player Status: Playing

10. Conclusion

These Application Notes describe the configuration steps required for OpenText Qfiniti 20.4 to successfully interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 using Multiple Registration. All feature and serviceability test cases were completed successfully.

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 User Guide*, Version 20.4, Rev. 2020-Oct-28, available to existing customers at <https://knowledge.opentext.com/knowledge/lisapi.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.