



Avaya Solution & Interoperability Test Lab

Application Notes for OpenText Qfiniti 20.4 with Avaya Session Border Controller for Enterprise 8.1.2 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 Session Border Controller for Enterprise 8.1.2 and Avaya Aura® Application Enablement Services 8.1.3. OpenText 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, and used the SIP-based Media Recording interface from Avaya Session Border Controller for Enterprise to capture media for calls between the monitored agents and the PSTN.

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 Session Border Controller for Enterprise (SBCE) 8.1.2 and Avaya Aura® Application Enablement Services 8.1.3. 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, and used the SIP-based Media Recording (SIPREC) interface from SBCE to capture media for calls between the monitored agents and the PSTN.

When there is an active call at the agent station, Qfiniti is informed of the call via TSAPI events and starts the call recording with captured media from the SIPREC interface. The TSAPI events are also used to determine when to stop the call recording.

The compliance testing covered inbound ACD calls that were delivered to agents and a couple of basic outbound calls manually dialed by agent to the PSTN. The compliance testing scope did not include outbound ACD calls as part of any outbound application.

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.

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 agent telephones 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 interfaces between Qfiniti and Avaya products did not include use of any specific encryption features as requested by OpenText.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Qfiniti:

- Handling of TSAPI messages in areas of event notification and value queries.
- Use of SIPREC to obtain media from SBCE for call recording.
- Proper recording, logging, and playback of calls for scenarios involving agent drop, customer drop, hold, reconnect, simultaneous calls, long duration, multiple agents, and manual call 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, the held interval was included in the recordings and contained audio from the PSTN caller.
- By design, the recording entry associated with the transfer-from agent for all transfer and conference scenarios reported two DNIS numbers. One number being the number dialed by the PSTN caller and the other being the number dialed by the transfer-from/conference-from agent.
- By design, the recording entry associated with the transfer-from/conference-from agent for all supervised transfer and conference scenarios reported two ANI numbers. One number being the PSTN caller number and the other being the transfer-from/conference-from agent station extension.
- By design, for conference scenarios involving two agents and the PSTN, the three-way conversation can only be associated with one agent and therefore only contained in the recording associated with the conference-to agent.
- In the unsupervised conference scenario involving two agents and the PSTN, the remaining conversation between the conference-to agent and PSTN was captured in the recording entry associated with the conference-from agent instead of the conference-to 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, Application Enablement Services, Session Manager, SBCE, and call center devices are not the focus of these Application Notes and will not be described.

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

Device Type	Extension
Skill Group	61001, 61002
Supervisor	65000
Agent Station	65001 (H.323), 66002 (SIP)
Agent ID	65881, 65882

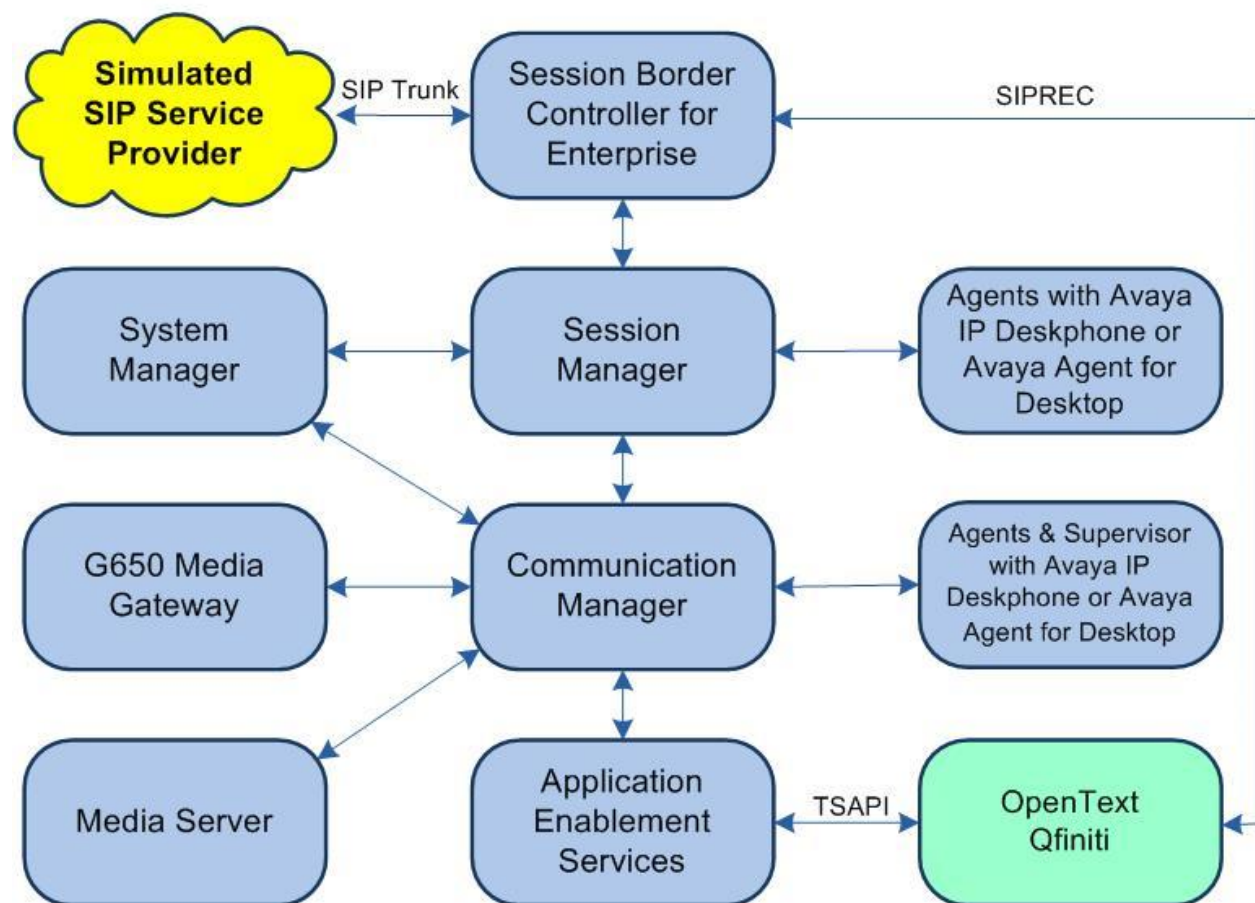


Figure 1: Compliance Testing Configuration

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 (8.1.3.0.1.890.26685)
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	8.1.2 (8.1.2.0-31-19809)
Avaya Agent for Desktop (H.323 & SIP)	2.0.6.0.10
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">Microsoft SQL Server 2019Avaya TSAPI Windows Client (csta32.dll)	20.4.0 Standard 15.0.4034.2 8.0.0.38

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 system parameters features
- Administer SIP trunk group

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. Note that the CTI link number and extension number may vary. Enter “ADJ-IP” in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

add cti-link 1		Page	1 of 3
CTI LINK			
CTI Link: 1			
Extension: 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 by the agent stations. For **Audio Codec**, make certain that variants of G711 and/or G729 codec are configured, as shown below. Note that Qfiniti supports the G711 and G729 codec variants.

```
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 System Parameters Features

Log into the System Access Terminal. Use the “change system-parameters features” command to enable **Create Universal Call ID (UCID)**, which is located on **Page 5**. For **UCID Network Node ID**, enter an available node ID.

```
change system-parameters features                                     Page 5 of 19
                           FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:                               Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
  Switch Name:
  Emergency Extension Forwarding (min): 10
  Enable Inter-Gateway Alternate Routing? n
  Enable Dial Plan Transparency in Survivable Mode? n
  COR to Use for DPT: station
  EC500 Routing in Survivable Mode: dpt-then-ec500

MALICIOUS CALL TRACE PARAMETERS
  Apply MCT Warning Tone? n      MCT Voice Recorder Trunk Group:
  Delay Sending RELease (seconds): 0

SEND ALL CALLS OPTIONS
  Send All Calls Applies to: station      Auto Inspect on Send All Calls? n
  Preserve previous AUX Work button states after deactivation? n

UNIVERSAL CALL ID
  Create Universal Call ID (UCID)? y      UCID Network Node ID: 27
```

Navigate to **Page 13** and enable **Send UCID to ASAI**. This parameter allows for the universal call ID to be sent to Qfiniti.

```
change system-parameters features                                     Page 13 of 19
                           FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER MISCELLANEOUS
  Callr-info Display Timer (sec): 10
  Clear Callr-info: next-call
  Allow Ringer-off with Auto-Answer? n

  Reporting for PC Non-Predictive Calls? n

  Agent/Caller Disconnect Tones? N
  Interruptible Aux Notification Timer (sec): 3
  Zip Tone Burst for Callmaster Endpoints: double

ASAI
  Copy ASAI UI During Conference/Transfer? n
  Call Classification After Answer Supervision? y
  Send UCID to ASAI? y
  For ASAI Send DTMF Tone to Call Originator? y
  Send Connect Event to ASAI For Announcement Answer? n
  Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```

5.5. Administer SIP Trunk Group

Use the “change trunk-group n” command, where “n” is the trunk group number used by Communication Manager with Session Manager for outbound calls to the PSTN. Enter the following values for the specified fields and retain the default values for the remaining fields.

In this case, the pertinent trunk group number is “212”. Navigate to **Page 3**. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **UI Treatment:** “shared”
- **Send UCID:** “y”

```
add trunk-group 212                                     Page 3 of 5
TRUNK FEATURES
    ACA Assignment? n                                   Measured: none
                                                    Maintenance Tests? y

    Suppress # Outpulsing? n   Numbering Format: public
                                UI Treatment: shared
                                Maximum Size of UUI Contents: 128
                                Replace Restricted Numbers? n
                                Replace Unavailable Numbers? n

                                Modify Tandem Calling Number: tandem-cpn-form
                                Send UCID? y

    Show ANSWERED BY on Display? 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 Qfiniti user
- Administer security database
- Restart service
- Obtain Tlink name

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" and "Management Console" is displayed. A red horizontal bar spans the width of the page, with a "Help" link on the right. In the center, there is a login box with the text "Please login here:" followed by a "Username" label 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 shows 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 displays user information: "Welcome: User", "Last login: Tue Mar 2 09:26:04 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: Thu Mar 04 09:22:55 EST 2021", and "HA Status: Not Configured". The left sidebar contains a menu with options: 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 contains a paragraph explaining the OAM Web's purpose and a bulleted list of administrative domains: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. A note at the bottom states: "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" menu item selected in the left sidebar. The main content area is titled "Licensing" and contains three sections of instructions: "If you are setting up and maintaining the WebLM, you need to use the following:" with a bullet point for "WebLM Server Address"; "If you are importing, setting up and maintaining the license, you need to use the following:" with a bullet point for "WebLM Server Access"; and "If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:" with a bullet point for "Reserved Licenses". The left sidebar menu is expanded to show "WebLM Server Address", "WebLM Server Access", and "Reserved Licenses" under the "Licensing" category.

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

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

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

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

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

The main table shows the license capacity for various features:

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 navigation pane shows the hierarchy: AE Services > TSAPI > TSAPI Links. The main content area displays the "TSAPI Links" screen with a table header containing "Link", "Switch Connection", "Switch CTI Link #", "ASAI Link Version", and "Security". Below the header are buttons for "Add Link", "Edit Link", and "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, the existing switch connection "cm7" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.

The screenshot shows the "Add TSAPI Links" screen in the Avaya Management Console. The left navigation pane is the same as the previous screenshot. The main content area displays the "Add TSAPI Links" form with the following fields: "Link" (dropdown menu with value 1), "Switch Connection" (dropdown menu with value cm7), "Switch CTI Link Number" (dropdown menu with value 1), "ASAI Link Version" (dropdown menu with value 12), and "Security" (dropdown menu with value Unencrypted). At the bottom of the form are buttons for "Apply Changes" and "Cancel Changes".

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: Tue Mar 2 09:26:04 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: Thu Mar 04 09:22:55 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". On the right, a welcome message for the user "User" is shown, along with login details: "Last login: Tue Mar 2 09:26:04 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: Thu Mar 04 09:22:55 EST 2021", 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 is a dark grey menu with the following items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security" (expanded), "Account Management", "Audit", "Certificate Management", "Enterprise Directory", "Host AA", "PAM", "Security Database" (expanded), and "Control" (selected).

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.

6.6. Restart Service

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

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Mar 2 09:26:04 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: Thu Mar 04 09:22:55 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 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

6.7. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring Qfiniti.

In this case, the associated Tlink name is “AVAYA#CM7#CSTA#AES7”. Note the use of the switch connection “CM7” from **Section 6.3** as part of the Tlink name. Also note the host name of Application Enablement Services as part of the Tlink name, in this case “AES7”.

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 for the user is shown in the top right corner, including login details and system status. The main navigation pane on the left lists various services, with "Security" expanded to show "Security Database" and "Tlinks" selected. The main content area displays the "Tlinks" page, which shows a single Tlink named "AVAYA#CM7#CSTA#AES7" with a "Delete Tlink" button.

Welcome: User
Last login: Tue Mar 2 09:26:04 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: Thu Mar 04 09:22:55 EST 2021
HA Status: Not Configured

Security | Security Database | Tlinks

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
CTI Users
Devices
Device Groups
Tlinks

Tlinks

Tlink Name
AVAYA#CM7#CSTA#AES7
Delete Tlink

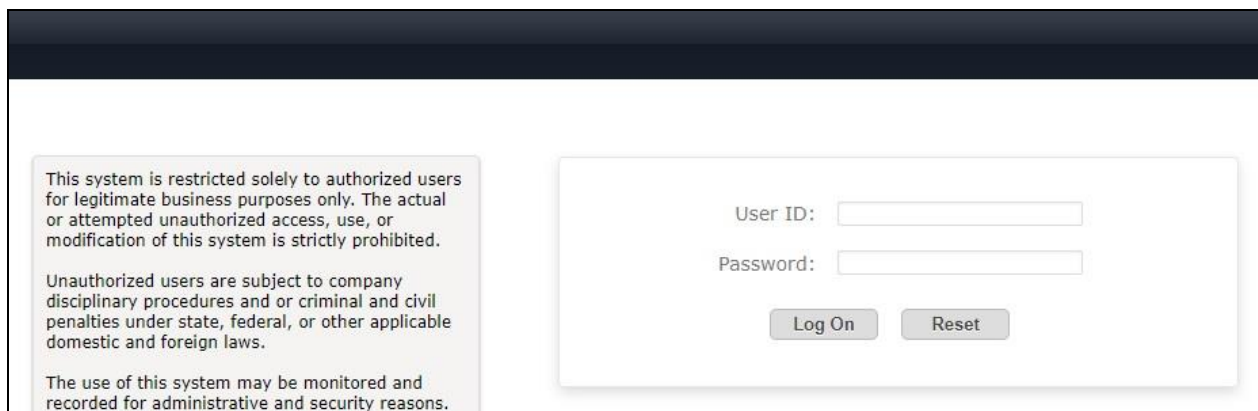
7. Configure Avaya Aura® Session Manager

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

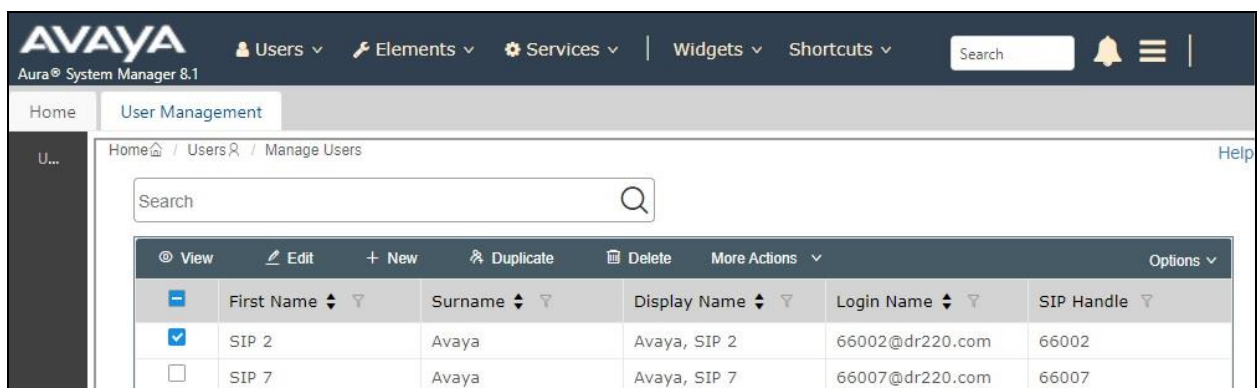
7.1. Launch System Manager

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 fields for System (DR-CM), Profile Type (Endpoint), Extension (66002), Set Type (J169CC), Port (S000068), and Preferred Handle (Select). A blue Editor icon is visible next to the Extension field, highlighted with a red box. Other fields include Use Existing Endpoints, Template, Security Code, Voice Mail Number, and Calculate Route Pattern.

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

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

The screenshot shows the 'Edit Endpoint' configuration page in the Avaya Aura System Manager 8.1 interface. The page 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
 - Extension: 66002
 - Template: Select (dropdown)
 - Set Type: J169CC
 - Port: S000068
 - Security Code: (empty)
 - Name: Avaya, SIP 2
- Configuration 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) *:**
 - Class of Restriction (COR): 1
 - Emergency Location Ext: 66002
 - Tenant Number: 1
 - SIP Trunk: Qaar
 - Coverage Path 1: 1
 - Lock Message: ☐
 - Multibyte Language: Not Applicable (dropdown)
 - SIP URI: (empty)
 - Class Of Service (COS): 1
 - Message Lamp Ext.: 66002
 - Type of 3PCC Enabled: Avaya (dropdown, highlighted with a red box)**
 - Coverage Path 2: (empty)
 - Localized Display Name: Avaya, SIP 2
 - Enable Reachability for Station Domain Control: system (dropdown)

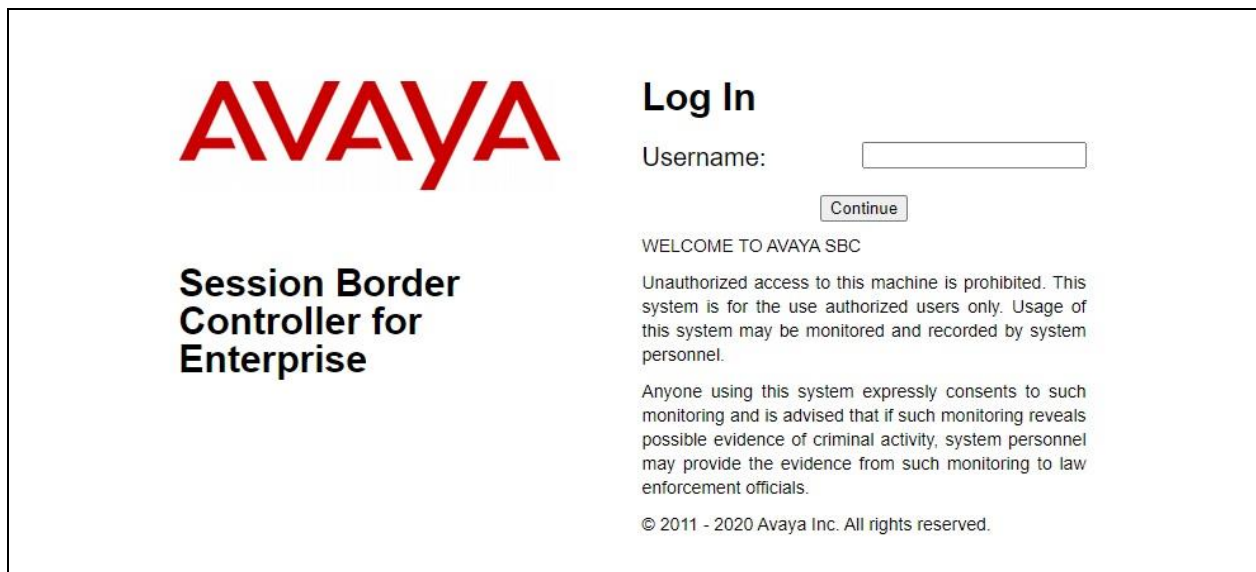
8. Configure Avaya Session Border Controller for Enterprise

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

- Launch web interface
- Administer SIP servers
- Administer routing
- Administer application rules
- Administer media rules
- Administer signaling rules
- Administer end point policy groups
- Administer recording profile
- Administer session policies
- Administer session flows
- Administer end point flows

8.1. Launch Web Interface

Access the SBCE web interface by using the URL “https://ip-address/sbc” in an Internet browser window, where “ip-address” is the IP address of the SBCE management interface. The screen below is displayed. Log in using the appropriate credentials.



The image shows the login page of the Avaya Session Border Controller for Enterprise (SBCE). On the left, the Avaya logo is displayed in red, with the text "Session Border Controller for Enterprise" below it. On the right, there is a "Log In" section. It includes a "Username:" label followed by a text input field. Below the input field is a "Continue" button. Underneath the button, the text "WELCOME TO AVAYA SBC" is displayed. Below that, a disclaimer states: "Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel." Further down, another disclaimer states: "Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials." At the bottom, the copyright notice "© 2011 - 2020 Avaya Inc. All rights reserved." is shown.

8.2. Administer SIP Servers

In the subsequent screen, select **Device** → **SBCE** from the top menu, followed by **Backup/Restore** → **Services** → **SIP Servers** from the left pane to display existing SIP server profiles. Click **Add** to add a SIP server profile for Qfiniti.

The screenshot shows the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes 'Device: SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main title is 'Session Border Controller for Enterprise' with the Avaya logo. The left sidebar contains a menu with 'EMS Dashboard', 'Software Management', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'SIP Servers' (highlighted), 'LDAP', 'RADIUS', 'Domain Policies', and 'TLS Management'. The main content area is titled 'SIP Servers: EXT-Server' and features an 'Add' button (highlighted with a red box), 'Rename', 'Clone', and 'Delete' buttons. Below the 'Add' button is a 'Server Profiles' list with 'EXT-Server', 'SM-Server', and 'IPO-Server'. The 'EXT-Server' profile is selected, showing configuration details in a tabbed interface with tabs for 'General', 'Authentication', 'Heartbeat', 'Registration', 'Ping', and 'Advanced'. The 'General' tab is active, displaying 'Server Type' as 'Trunk Server', 'DNS Query Type' as 'NONE/A', and a table for 'IP Address / FQDN', 'Port', and 'Transport' with the following data:

IP Address / FQDN	Port	Transport
10.64.102.224	5060	UDP

An 'Edit' button is located below the table.

The **Add Server Configuration Profile** pop-up screen is displayed. Enter a desired **Profile Name** as shown below.

The screenshot shows the 'Add Server Configuration Profile' pop-up screen. The title bar of the pop-up is 'Add Server Configuration Profile' with a close button (X). The main content area has a 'Profile Name' label and a text input field containing 'Qfiniti-Server'. Below the input field is a 'Next' button. The background shows the SBCE web interface with the 'SIP Servers' page visible.

The **Edit SIP Server Profile – General** pop-up screen is displayed. Click **Add** to add an entry and enter the following values for the specified fields and retain the default values for the remaining fields.

- **Server Type:** “Recording Server”
- **IP Address / FQDN:** IP address of the Qfiniti server.
- **Port:** “5060”
- **Transport:** “TCP”

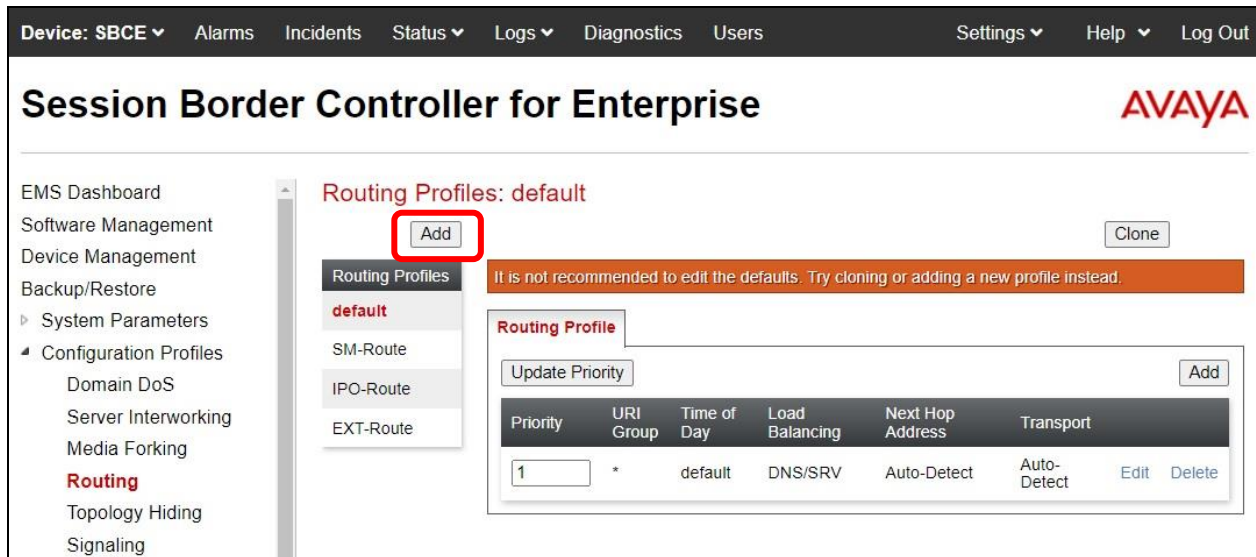
The screenshot shows the 'Edit SIP Server Profile - General' pop-up window. The 'Server Type' is set to 'Recording Server'. The 'SIP Domain' field is empty. 'DNS Query Type' is set to 'NONE/A' and 'TLS Client Profile' is set to 'None'. Below these fields is a table with three columns: 'IP Address / FQDN', 'Port', and 'Transport'. The table contains one row with the values '10.64.101.202', '5060', and 'TCP'. There are 'Add', 'Back', 'Next', and 'Edit' buttons.

Navigate to the **Add SIP Server Profile - Advanced** screen. Retain the check in **Enable Grooming** and the default values in the remaining fields.

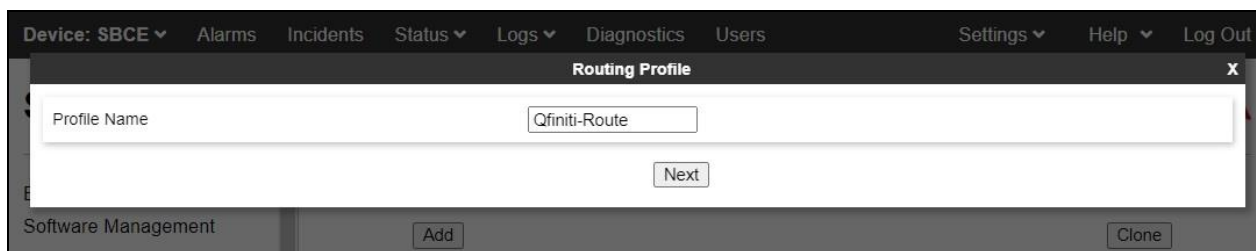
The screenshot shows the 'Add SIP Server Profile - Advanced' pop-up window. 'Enable Grooming' is checked. 'Interworking Profile' and 'Signaling Manipulation Script' are both set to 'None'. 'Securable' and 'Enable FGDN' are unchecked. 'TCP Failover Port' is 5060 and 'TLS Failover Port' is 5061. 'Tolerant' is unchecked. 'URI Group' is set to 'None' and 'NG911 Support' is unchecked. There are 'Back' and 'Finish' buttons.

8.3. Administer Routing

Select **Backup/Restore** → **Configuration Profiles** → **Routing** from the left pane to display existing routing profiles. Click **Add** to add routing profile for Qfiniti.



The **Routing Profile** pop-up screen is displayed. Enter a desired **Profile Name** as shown below.



The **Routing Profile** pop-up screen is updated. Click **Add** to add a next hop entry. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Priority / Weight:** The highest priority of “1”.
- **SIP Server Profile:** Select the Qfiniti SIP server profile from **Section 8.2**.
- **Next Hop Address:** Retain the auto populated value.

The screenshot shows the 'Routing Profile' configuration window. The top navigation bar includes 'Device: SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The 'Routing Profile' window has a close button 'X' in the top right corner.

The configuration fields are as follows:

- URI Group: *
- Time of Day: default
- Load Balancing: Priority
- NAPTR: ☐
- Transport: None
- LDAP Routing: ☐
- LDAP Server Profile: None
- LDAP Base DN (Search): None
- Matched Attribute Priority: ☒
- Alternate Routing: ☒
- Next Hop Priority: ☒
- Next Hop In-Dialog: ☐
- Ignore Route Header: ☐
- ENUM: ☐
- ENUM Suffix:

An 'Add' button is located at the bottom right of the configuration fields.

Below the configuration fields is a table for adding next hop entries:

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				Qfiniti-Server	10.64.101.202:5060 (TCP)	None	Delete

At the bottom of the table are 'Back' and 'Finish' buttons.

8.4. Administer Application Rules

Select **Backup/Restore** → **Domain Policies** → **Application Rules** from the left pane to display existing application rules. Click **Add** to add an application rule for Qfiniti.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header displays 'Session Border Controller for Enterprise' and the 'AVAYA' logo. The left sidebar contains a menu with 'EMS Dashboard', 'Software Management', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', and 'Domain Policies'. Under 'Domain Policies', 'Application Rules' is highlighted. The main content area is titled 'Application Rules: default' and features an 'Add' button (circled in red) and a 'Clone' button. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below this, an 'Application Rule' pop-up is shown with a table of existing rules:

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200	5
Video	<input type="checkbox"/>	<input type="checkbox"/>		

The **Application Rule** pop-up screen is displayed. Enter a desired **Rule Name** as shown below.

The screenshot shows the 'Application Rule' pop-up screen. The background is the same web interface as the previous screenshot. The pop-up has a title bar 'Application Rule' with a close button 'X'. It contains a 'Rule Name' input field with the text 'Qfiniti-Application' and a 'Next' button.

The **Application Rule** pop-up screen is updated. Check **Audio In** and **Audio Out**, and enter desired values for **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint**, as shown below. Retain the default values in the remaining fields.

The screenshot shows the 'Application Rule' configuration window. The 'Application Type' section has 'Audio' selected with 'In' and 'Out' checkboxes checked, and 'Maximum Concurrent Sessions' set to 100 and 'Maximum Sessions Per Endpoint' set to 10. The 'Video' section is unselected. The 'Miscellaneous' section includes 'CDR Support' (Off), 'RADIUS Profile' (None), 'Media Statistics Support' (unchecked), 'Call Duration' (Setup), and 'RTCP Keep-Alive' (unchecked). 'Back' and 'Finish' buttons are at the bottom.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	100	10
Video	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous

- CDR Support: ☒ Off, ☐ RADIUS, ☐ CDR Adjunct
- RADIUS Profile: None
- Media Statistics Support: ☐
- Call Duration: ☒ Setup, ☐ Connect
- RTCP Keep-Alive: ☐

Buttons: Back, Finish

8.5. Administer Media Rules

Select **Backup/Restore** → **Domain Policies** → **Media Rules** from the left pane to display existing media rules. Click **Add** to add a media rule for Qfiniti.

The screenshot shows the 'Media Rules' configuration page. The left pane shows the navigation menu with 'Media Rules' selected. The main area shows the 'default-low-med' rule. The 'Add' button is highlighted with a red box. The 'Encryption' tab is active, showing 'Audio Encryption' settings: 'Preferred Formats' (RTP), 'Interworking' (checked), 'Symmetric Context Reset' (checked), and 'Key Change in New Offer' (unchecked).

Media Rules: default-low-med

Buttons: Add, Clone

Warning: It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Tabs: Encryption, Codec Prioritization, Advanced, QoS

Audio Encryption

Preferred Formats	RTP
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

The **Media Rule** pop-up screen is displayed. Enter a desired **Rule Name** as shown below.

The screenshot shows the 'Media Rule' pop-up screen. At the top, there is a navigation bar with 'Device: SBCE' and various menu items. The main area has a 'Rule Name' input field containing 'Qfiniti-Media' and a 'Next' button. At the bottom, there are 'Add' and 'Clone' buttons.

The **Media Rule** pop-up screen is updated. Navigate to the **Audio Codec** page. Move the relevant G711 and G729 codec variants from the **Available** column to the **Selected** column, as shown below. Retain the default values in all remaining fields and pages.

The screenshot shows the 'Media Rule' pop-up screen with the 'Audio Codec' tab selected. The 'Codec Prioritization' checkbox is checked. The 'Transcode' checkbox is unchecked. The 'P-Time (Optional)' dropdown is set to 20. The 'Available' column lists various codecs, including G729AB (18) [T] and G726-32 [DT]. The 'Selected' column lists PCMU (0) [T] and G729 (18) [T]. The 'Video Codec' section is also visible below.

8.6. Administer Signaling Rules

Select **Backup/Restore** → **Domain Policies** → **Signaling Rules** (not shown) from the left pane to display existing signaling rules.

8.6.1. Qfiniti Signaling Rule

Click **Add** to add a signaling rule for Qfiniti.



The **Signaling Rule** pop-up screen is displayed. Enter a desired **Rule Name** as shown below.



The **Signaling Rule** pop-up screen is updated. Navigate to the **UCID** page. Check **Enabled**. For **Node ID**, enter a unique number across the customer system, in this case “15”. Retain the default value in the remaining field.



8.6.2. Session Manager Signaling Rule

Select the existing signaling rule for Session Manager, in this case **SM-Signaling**. Select the **UCID** tab. Make certain that **UCID** is checked, and that **Node ID** is configured with a unique number across the customer system, as shown below.

The screenshot shows the 'Session Border Controller for Enterprise' interface. The left sidebar contains a navigation menu with 'Signaling Rules' highlighted. The main content area is titled 'Signaling Rules: SM-Signaling'. It features an 'Add' button and buttons for 'Rename', 'Clone', and 'Delete'. Below these is a tabbed interface with tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', and 'Signaling'. The 'Signaling' tab is active, showing a 'UCID' checkbox which is checked, and a 'Node ID' field set to '11'. There is also a 'Protocol Discriminator' field set to '0x00' and an 'Edit' button.

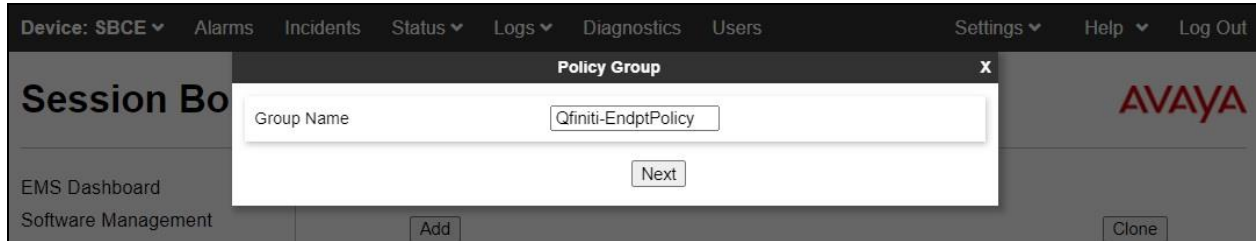
8.7. Administer End Point Policy Groups

Select **Backup/Restore** → **Domain Policies** → **End Point Policy Groups** from the left pane to display the existing policy groups. Click **Add** to add a policy group for Qfiniti.

The screenshot shows the 'Session Border Controller for Enterprise' interface. The left sidebar contains a navigation menu with 'End Point Policy Groups' highlighted. The main content area is titled 'Policy Groups: default-low'. It features an 'Add' button (highlighted with a red box) and a 'Clone' button. Below these is a table of policy groups. The table has columns: Order, Application, Border, Media, Security, Signaling, Charging, and RTP Mon Gen. The first row shows a policy group with Order 1, Application 'default', Border 'default', Media 'default-low-med', Security 'default-low', Signaling 'default', Charging 'None', and RTP Mon Gen 'Off'. There is an 'Edit' button for this row. A 'Summary' button is also present.

Order	Application	Border	Media	Security	Signaling	Charging	RTP Mon Gen
1	default	default	default-low-med	default-low	default	None	Off

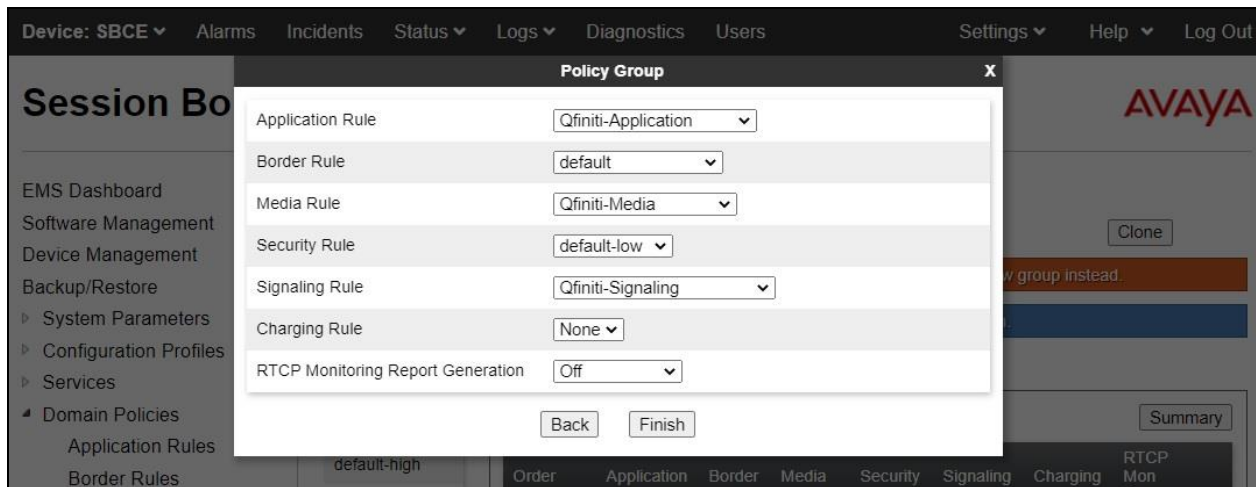
The **Policy Group** pop-up screen is displayed. Enter a desired **Group Name** as shown below.



The screenshot shows the Avaya EMS Dashboard with a 'Policy Group' pop-up window. The 'Group Name' field is populated with 'Qfiniti-EndptPolicy'. The 'Next' button is visible. The background shows the 'Session Board' and 'Software Management' sections.

The **Policy Group** pop-up screen is updated. Enter the following values for the specified fields and retain the default values for the remaining fields.

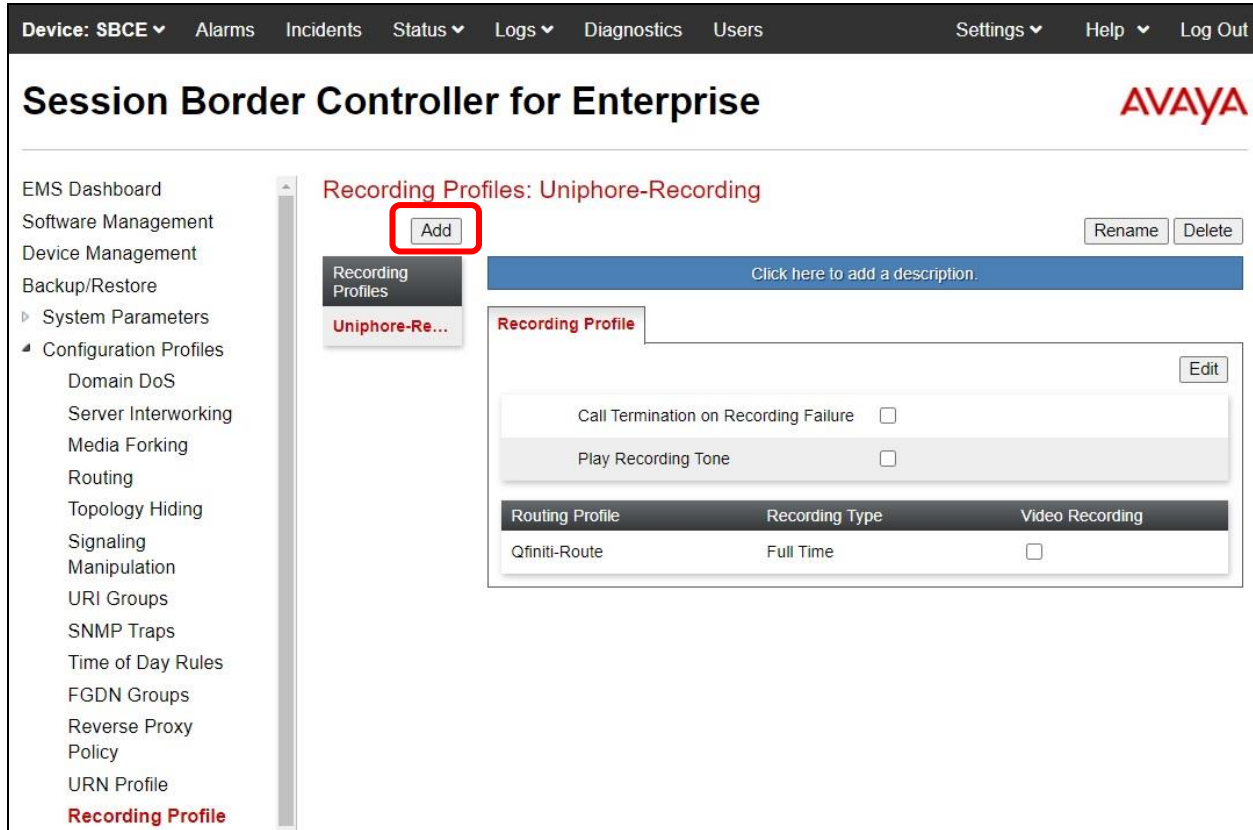
- **Application Rule:** Select the Qfiniti application rule from **Section 8.4**.
- **Media Rule:** Select the Qfiniti media rule from **Section 8.5**.
- **Signaling Rule:** Select the Qfiniti signaling rule from **Section 8.6.1**.



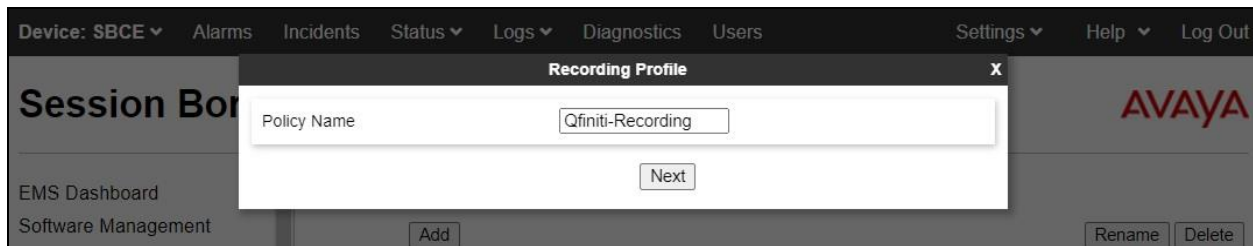
The screenshot shows the 'Policy Group' pop-up window with the following settings: Application Rule (Qfiniti-Application), Border Rule (default), Media Rule (Qfiniti-Media), Security Rule (default-low), Signaling Rule (Qfiniti-Signaling), Charging Rule (None), and RTCP Monitoring Report Generation (Off). The 'Back' and 'Finish' buttons are at the bottom. The background shows the 'Session Board' and 'Software Management' sections.

8.8. Administer Recording Profile

Select **Backup/Restore** → **Configuration Profiles** → **Recording Profile** from the left pane to display the existing profiles. Click **Add** to add a recording profile for Qfiniti.



The **Recording Profile** pop-up screen is displayed. Enter a desired **Policy Name** as shown below.



The **Recording Profile** pop-up screen is updated. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Play Recording Tone:** Check this field is customer desires recording tone to be played.
- **Routing Profile:** Select the Qfiniti routing profile from **Section 8.3**.
- **Recording Type:** “Full Time”

The screenshot shows the 'Recording Profile' pop-up window. It contains the following fields and controls:

- Call Termination on Recording Failure:** ☐
- Play Recording Tone:** ☐
- Add:** Button
- Routing Profile:** Dropdown menu showing 'Qfiniti-Route'
- Recording Type:** Dropdown menu showing 'Full Time'
- Video Recording:** ☐
- Delete:** Button
- Back:** Button
- Finish:** Button

8.9. Administer Session Policies

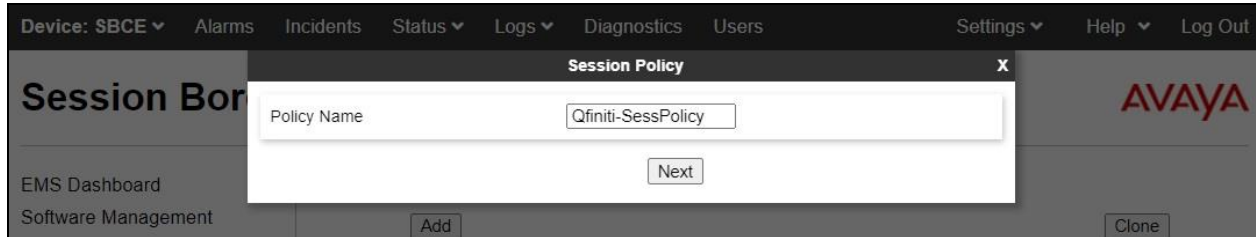
Select **Backup/Restore** → **Domain Policies** → **Session Policies** from the left pane to display the existing session policies. Click **Add** to add a session policy for Qfiniti.

The screenshot shows the 'Session Policies' configuration page. The left pane shows the navigation menu with 'Session Policies' selected. The main area displays the 'default' session policy. The 'Add' button is highlighted with a red box. The 'Media' tab is selected, showing the following settings:

Media	URN Profile
Media Anchoring	<input checked="" type="checkbox"/>
Media Forking Profile	None
Converged Conferencing	<input type="checkbox"/>
Recording Server	<input type="checkbox"/>
Media Server	<input type="checkbox"/>

The 'Edit' button is located at the bottom right of the settings table.

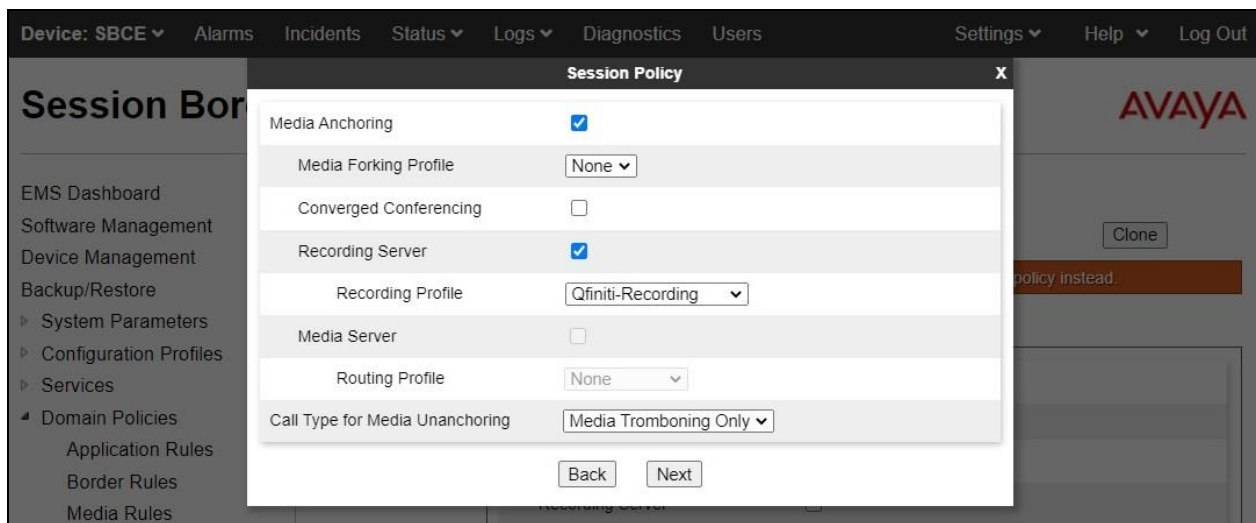
The **Session Policy** pop-up screen is displayed. Enter a desired **Policy Name** as shown below.



The screenshot shows the 'Session Policy' pop-up window. The 'Policy Name' field is populated with 'Qfiniti-SessPolicy'. A 'Next' button is visible at the bottom right of the form. The background shows the 'Session Board' interface with a sidebar menu and a top navigation bar.

The **Session Policy** pop-up screen is updated. Enter the following values for the specified fields and retain the default values for the remaining fields.

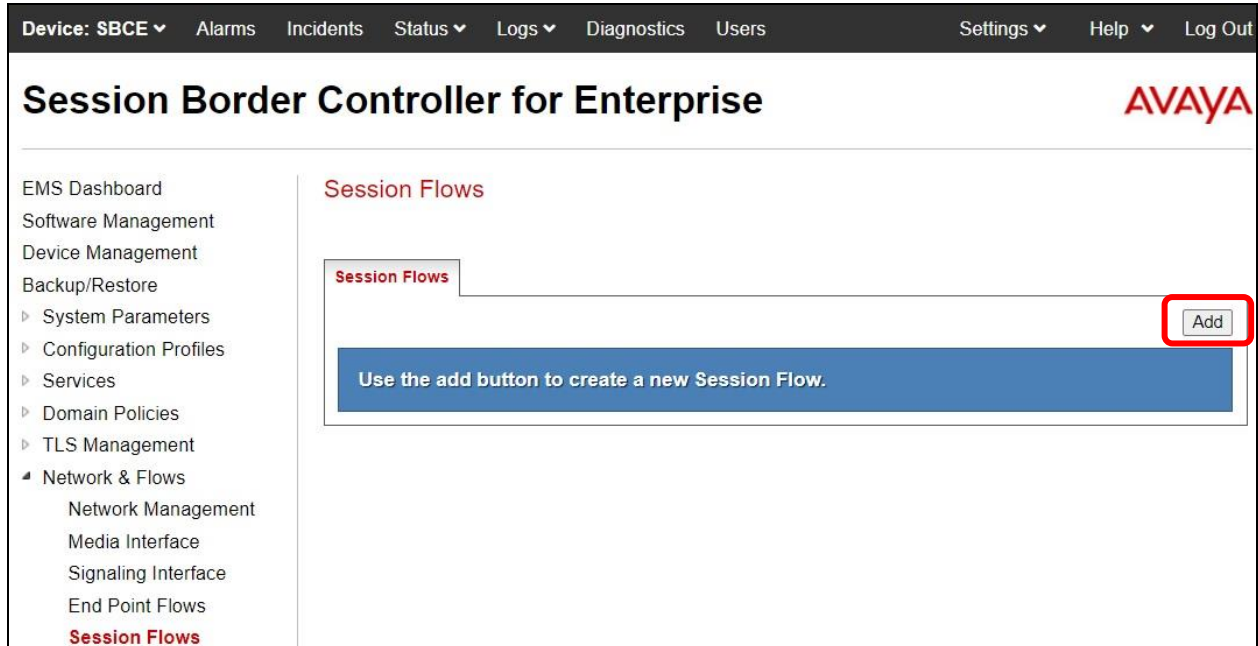
- **Media Anchoring:** Check this field.
- **Recording Server:** Check this field.
- **Recording Profile:** Select the Qfiniti recording profile from **Section 8.8**.



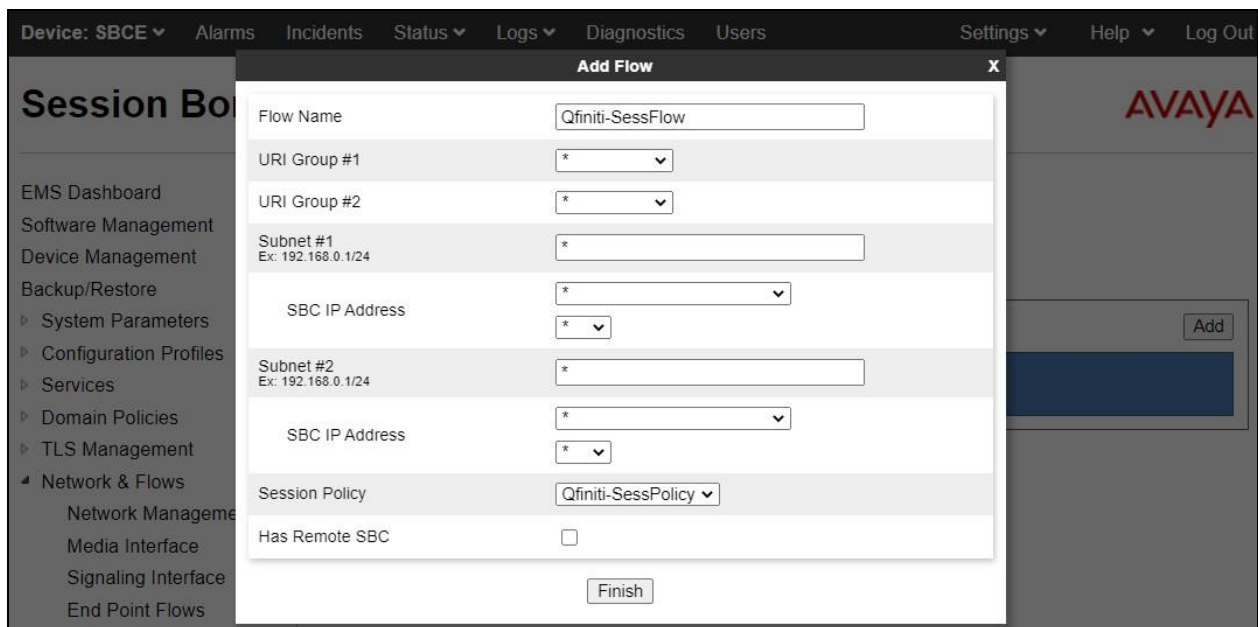
The screenshot shows the 'Session Policy' pop-up window with the following settings: 'Media Anchoring' is checked, 'Media Forking Profile' is set to 'None', 'Converged Conferencing' is unchecked, 'Recording Server' is checked, 'Recording Profile' is set to 'Qfiniti-Recording', 'Media Server' is unchecked, 'Routing Profile' is set to 'None', and 'Call Type for Media Unanchoring' is set to 'Media Tromboning Only'. 'Back' and 'Next' buttons are at the bottom. The background shows the 'Session Board' interface with a sidebar menu and a top navigation bar.

8.10. Administer Session Flows

Select **Backup/Restore** → **Network & Flows** → **Session Flows** from the left pane to display the existing session flows. Click **Add** to add a session flow for Qfiniti.



The **Add Flow** pop-up screen is displayed. For **Flow Name**, enter a desired name. For **Session Policy**, select the Qfiniti session policy from **Section 8.9**. Retain the default values in the remaining fields.



8.11. Administer End Point Flows

Select **Backup/Restore** → **Network & Flows** → **End Point Flows** from the left pane. Select the **Server Flows** tab and click **Add** to add a server flow for Qfiniti.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Device: SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. The left sidebar contains a navigation menu with options like EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, and Network & Flows. Under Network & Flows, the End Point Flows option is highlighted. The main content area is titled 'End Point Flows' and features two tabs: 'Subscriber Flows' and 'Server Flows'. The 'Server Flows' tab is active, and an 'Add' button is highlighted with a red box. Below the tabs, a message states: 'Modifications made to a Server Flow will only take effect on new sessions.' A blue bar indicates 'Hover over a row to see its description.' The interface shows two sections for SIP Servers: 'EXT-Server' and 'SM-Server'. Each section contains a table with columns for Priority, Flow Name, URI Group, Received Interface, Signaling Interface, End Point Policy Group, and Routing Profile. The 'EXT-Server' table has one row with Priority 1, Flow Name 'EXT-Flow', URI Group '*', Received Interface 'Private-Signaling', Signaling Interface 'Public-Signaling', End Point Policy Group 'default-low', and Routing Profile 'SM-Route'. The 'SM-Server' table has one row with Priority 1, Flow Name 'SM-Flow', URI Group '*', Received Interface 'Public-Signaling', Signaling Interface 'Private-Signaling', End Point Policy Group 'SM-EndptPolicy', and Routing Profile 'EXT-Route'. Each row has 'View', 'Clone', 'Edit', and 'Delete' buttons.

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	EXT-Flow	*	Private-Signaling	Public-Signaling	default-low	SM-Route	View Clone Edit Delete

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SM-Flow	*	Public-Signaling	Private-Signaling	SM-EndptPolicy	EXT-Route	View Clone Edit Delete

The **Add Flow** pop-up screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Flow Name:** A descriptive name.
- **SIP Server Profile:** The Qfiniti SIP server profile from **Section 8.2**.
- **Received Interface:** The external signaling interface in this case “Public-Signaling”.
- **Signaling Interface:** The internal signaling interface in this case “Private-Signaling”.
- **Media Interface:** The internal media interface in this case “Private-Media”.
- **End Point Policy Group:** The Qfiniti end point policy group from **Section 8.7**.

The screenshot shows the 'Add Flow' pop-up screen in the Avaya EMS Dashboard. The form contains the following fields and values:

Field	Value
Flow Name	Qfiniti-Flow
SIP Server Profile	Qfiniti-Server
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public-Signaling
Signaling Interface	Private-Signaling
Media Interface	Private-Media
Secondary Media Interface	None
End Point Policy Group	Qfiniti-EndptPolicy
Routing Profile	default
Topology Hiding Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>

A 'Finish' button is located at the bottom of the form.

9. Configure OpenText Qfiniti

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

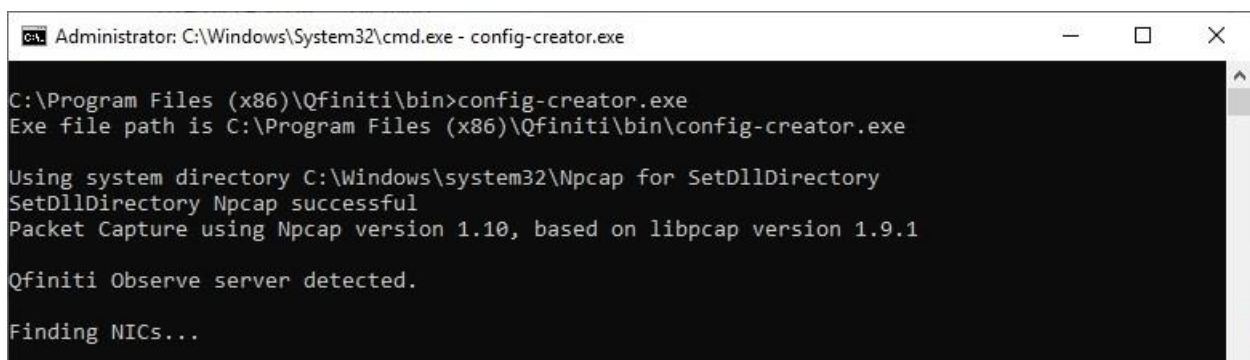
- Obtain network card data
- Launch SysConfig web interface
- Administer switches
- Administer CTI server
- Administer board configuration
- Administer general
- Administer machines
- Administer components
- Administer CTI sources
- Administer phone interface
- Administer logging data – phone class of 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. Obtain Network Card Data

From the Qfiniti server, open a Command Prompt window and navigate to the **C:\Program Files (x86)\Qfiniti\bin** directory.

Run the command **config-creator.exe** as shown below, which will create the **NICs.txt** file.



```
Administrator: C:\Windows\System32\cmd.exe - config-creator.exe

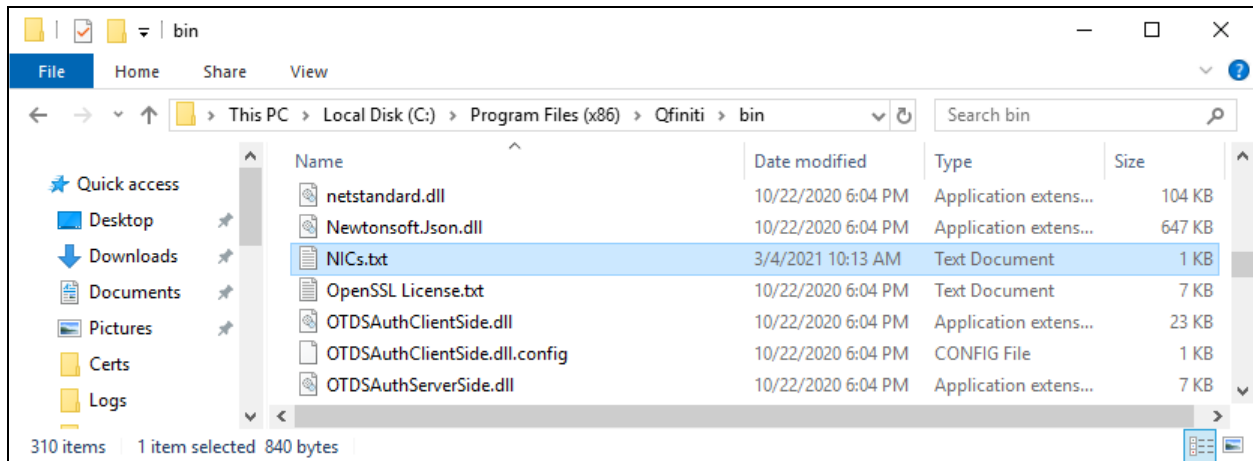
C:\Program Files (x86)\Qfiniti\bin>config-creator.exe
Exe file path is C:\Program Files (x86)\Qfiniti\bin\config-creator.exe

Using system directory C:\Windows\system32\Npcap for SetDllDirectory
SetDllDirectory Npcap successful
Packet Capture using Npcap version 1.10, based on libpcap version 1.9.1

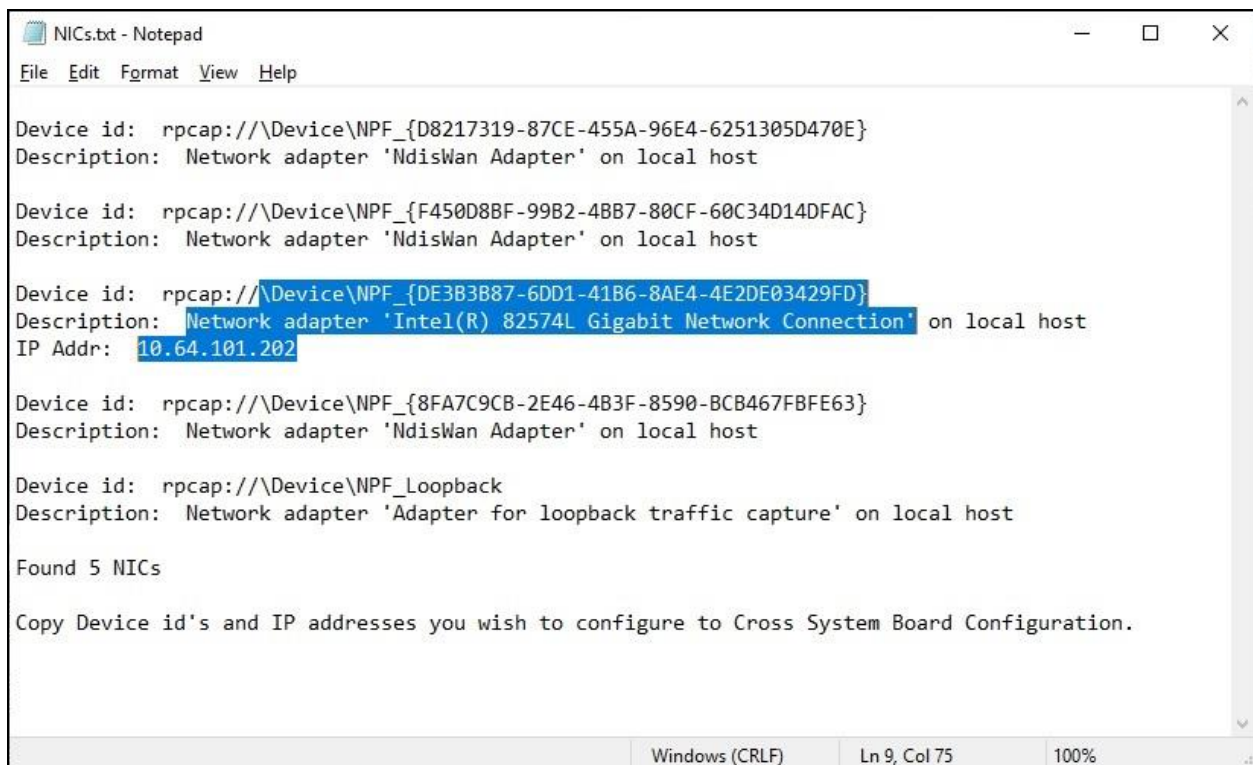
Qfiniti Observe server detected.

Finding NICs...
```


From the **C:\Program Files (x86)\Qfiniti\bin** directory, open the newly created **NICs.txt** file with a text editor application such as NotePad.



Locate the device with connection to the local network, in this case the device with an **IP Addr** of **10.64.101.202**. Make a note of the **Device id**, **Description**, and **IP Addr** values, which will be used later for board configuration.



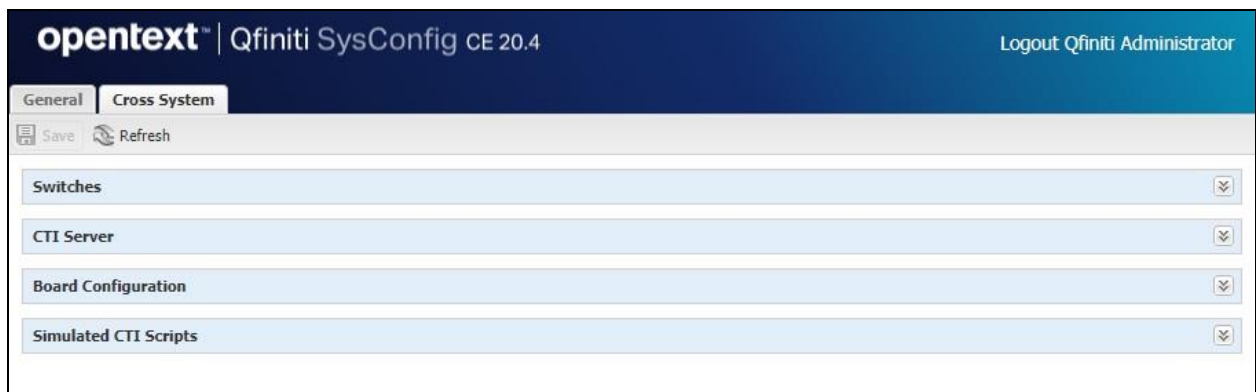
9.2. Launch SysConfig Web Interface

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 interface. It features a dark blue background with the 'opentext' logo in white. Below the logo, the text 'Sign in to continue to qfiniti-system-configuration' is displayed. There are two white input fields: the top one is labeled 'User name' and the bottom one 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. The top header bar is dark blue with the 'opentext' logo and 'Qfiniti SysConfig CE 20.4' on the left, and 'Logout Qfiniti Administrator' on the right. Below the header, there are two tabs: 'General' and 'Cross System', with 'Cross System' being the active tab. Under the 'Cross System' tab, there are two buttons: 'Save' and 'Refresh'. Below these buttons, there are four expandable sections, each with a blue header bar and a dropdown arrow on the right: 'Switches', 'CTI Server', 'Board Configuration', and 'Simulated CTI Scripts'.

9.3. Administer Switches

Expand the **Switches** sub-section and click the **New Item** icon to add a new entry for Session Border Controller for Enterprise for SIPREC integration. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name, in this case “AvayaSIPREC”.
- **Switch Model:** “SIP”
- **Observe Mode:** “By Extension”
- **Interface Type:** “Network Tap”
- **SIP Identifier:** “session_id”
- **Transport:** The Qfiniti SIP server transport from **Section 8.2**.
- **SIP Recording Type:** “Dynamic Registration”
- **SBC Recording Type:** “SIPREC”
- **SIP Id CTI Location:** “EventData.ConnID”

The screenshot shows the OpenText Qfiniti Administrator interface. The 'Switches' section is expanded, and a new switch is being added. The configuration fields are filled with the values specified in the list above. A red circle highlights the '+ Add' button in the right sidebar.

Field	Value
Name	AvayaSIPREC
Switch Model	SIP
Vendor	
Post Release Delay	0
Observe Mode	By Extension
Observe String	
Interface Type	Network Tap
Use CTI Source for Alias	<input type="checkbox"/>
Vlan Support	False
Trigger Type	Signaling
RTP Segmentation Rate (0-100)	20
Ring Timer (0-600)	5
Digit Collection (0-600)	5
Drop Duplicates	Do not drop duplicates
SIP Identifier	session_id
Transport	TCP
SIP Recording Type	Dynamic Registration
SBC Recording Type	SIPREC
IP fragmentation	False
Extension IP Address Mapping	Default
SIP Id CTI Location	EventData.ConnID
Switch IP Address 1	

9.4. Administer CTI Server

Expand the **CTI Server** sub-section and click the **New Item** icon to add a new entry for Application Enablement Services for TSAPI integration. 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 9.3**.
- **ServerName:** Host name portion of the Tlink name from **Section 6.7**.
- **User Name:** The Qfiniti user credentials from **Section 6.4**.
- **Password:** The Qfiniti user credentials from **Section 6.4**.
- **Vendor:** “AVAYA”
- **Driver:** Switch connection portion of the Tlink name from **Section 6.7**.
- **Service:** “CSTA”
- **ConnID Location:** “UCID”

The screenshot displays the Qfiniti SysConfig CE 20.4 web interface. The main window has a header with the 'opentext' logo and 'Qfiniti SysConfig CE 20.4'. On the right, there is a 'Logout Qfiniti Administrator' link. The left sidebar contains a navigation menu with 'General' and 'Cross System' tabs, and a list of items including 'Switches', 'CTI Server', 'Name', 'Dialer4DMCC', 'Board Configuration', and 'Simulated CTI Scripts'. The 'CTI Server' item is selected. A modal dialog box titled 'CTI Server' is open in the center. It contains the following fields: 'Name' (text input with 'AvayaTSAPI'), 'Type' (dropdown menu with 'Avaya TSAPI'), 'Available Switch' (dropdown menu with 'AvayaSIPREC'), 'ServerName' (text input with 'AES7'), 'User Name' (text input with 'qfiniti'), 'Password' (password field with masked characters), 'Vendor' (text input with 'AVAYA'), 'Driver' (text input with 'CM7'), 'Service' (text input with 'CSTA'), 'BackUp ServerName' (text input), 'BackUp User Name' (text input), 'BackUp Password' (password field), 'BackUp Vendor' (text input), 'BackUp Driver' (text input), 'BackUp Service' (text input), 'ConnID Location' (dropdown menu with 'UCID'), 'UCID prefix' (text input), and 'Query VDN/Split name' (dropdown menu with 'No'). At the bottom of the dialog are 'Add', 'Ok', and 'Cancel' buttons. On the right side of the main window, a red circle highlights a '+' icon, which is the 'New Item' button mentioned in the text.

9.5. Administer Board Configuration

Expand the **Board Configuration** sub-section and click the **New Item** icon. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name, in this case “SIPRECNIC”.
- **Model:** “Network Interface Card (NIC)”
- **Network Card Identifier 1:** The network device ID value from **Section 9.1**.
- **Network Card Description 1:** The network device description value from **Section 9.1**.
- **Network Card IP Address 1:** The network device IP address value from **Section 9.1**.

The screenshot displays the 'Board Configuration' dialog box within the 'opentext | Qfiniti SysConfig CE 20.4' application. The dialog is titled 'Board Configuration' and has a close button (X) in the top right corner. It contains a list of configuration fields for network cards. The first card is configured with the following values:

- Name: SIPRECNIC
- Model: Network Interface Card (NIC)
- Active 1: True
- Network Card Identifier 1: \Device\NPF_{DE3B3B87-6DD1-41B6-8AE4-4E2C}
- Network Card Description 1: Network adapter 'Intel(R) 82574L Gigabit Netwoi
- Network Card IP Address 1: 10.64.101.202
- Network Card Port 1: 5060

The dialog also includes fields for a second, third, and fourth card, all of which are currently empty. At the bottom of the dialog are 'Add', 'Ok', and 'Cancel' buttons. In the background, the main application window is visible, showing a sidebar with 'General' and 'Cross System' tabs, and a list of items including 'Switches', 'CTI Server', 'Board Configuration', 'Name', 'DummyBd4DMCC', and 'Simulated CTI Scripts'. A red circle highlights the '+' icon in the background interface, indicating where to click to add a new item.

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 “SIPREC System”.
- **Switch:** Select the switch name from **Section 9.3**.
- **System Type:** Check **Voice Recording - Logging**.

The screenshot shows the 'opentext | Qfiniti SysConfig CE 20.4' interface. The 'General' tab is selected. In the 'Systems' section, the '+ New' button is circled in red. The 'General' sub-section is expanded, showing the following fields:

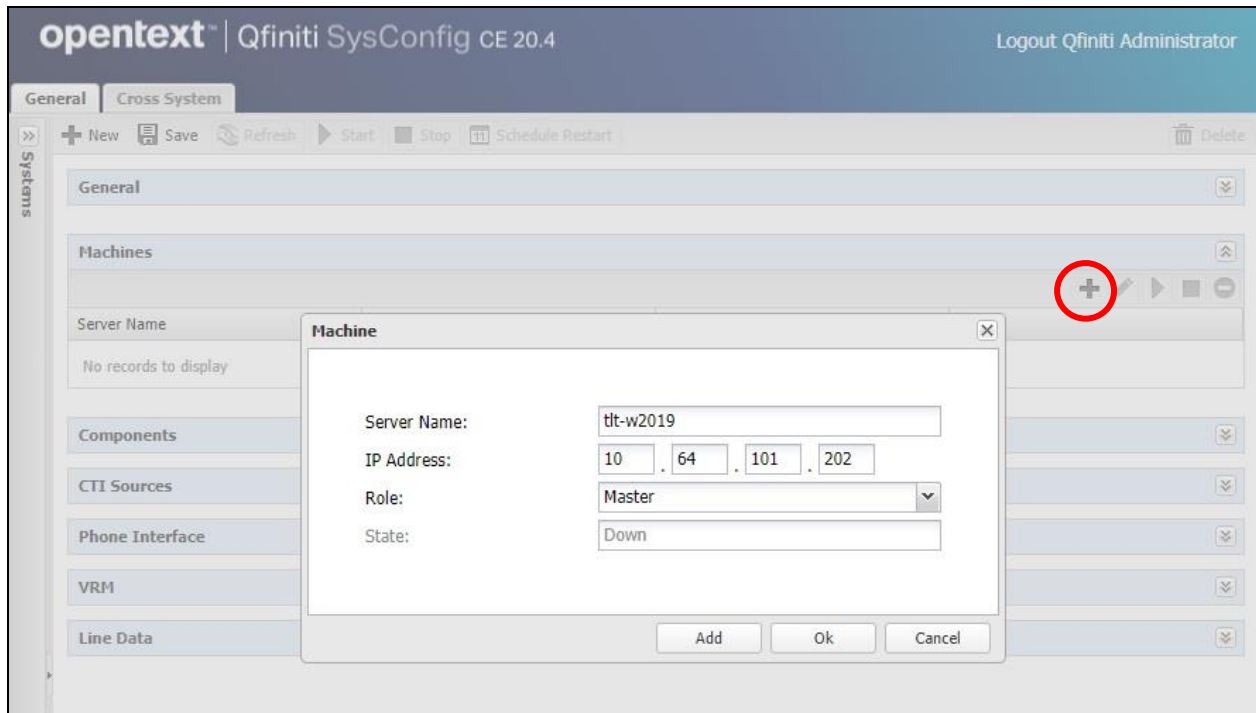
- Name:** SIPREC System
- Switch:** AvayaSIPREC
- System Type:**
 - ☒ Voice Recording - Logging
 - ☐ Voice Recording - QA
 - ☐ Screen Recording
 - ☐ Remote Screen Site
 - ☐ Explore
 - ☐ Survey
 - ☐ Backup
 - ☐ Cloud Connector
- Description:** (empty text area)
- ☒ Available for Use
- ☒ NAT Environment

The 'Machines' section is empty, showing a table with columns: Server Name, IP Address, Role, and State. The message 'No records to display' is shown below the table.

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:** “Microsoft GSM”
- **PCM Acquisition:** “Service Observe”
- **VoIP Transcoding:** “Transcode”

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

The screenshot displays the 'opentext | Qfiniti SysConfig CE 20.4' web interface. The top navigation bar includes a 'Logout Qfiniti Administrator' link. The main interface is divided into three sections: 'General', 'Cross System', and 'Systems'. The 'Systems' section is active, showing a list of components on the left and a list of assigned components on the right. The 'Assigned Components' list includes 'Logger Voice Recording Manager', which is highlighted. Below this, the 'Component Data' section is visible, containing various configuration fields and their values.

Component Data	
Post Service Observe dial string:	
Optimal Recording CODEC:	Microsoft GSM
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:	Transcode

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**.
- **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 application. The main window has a sidebar with 'Systems' and 'CTI Sources' sections. The 'CTI Sources' section is expanded, showing a list of machines, including 'tit-w2019'. A dialog box titled 'CTI Source' is open in the foreground. The dialog box contains the following fields and values:

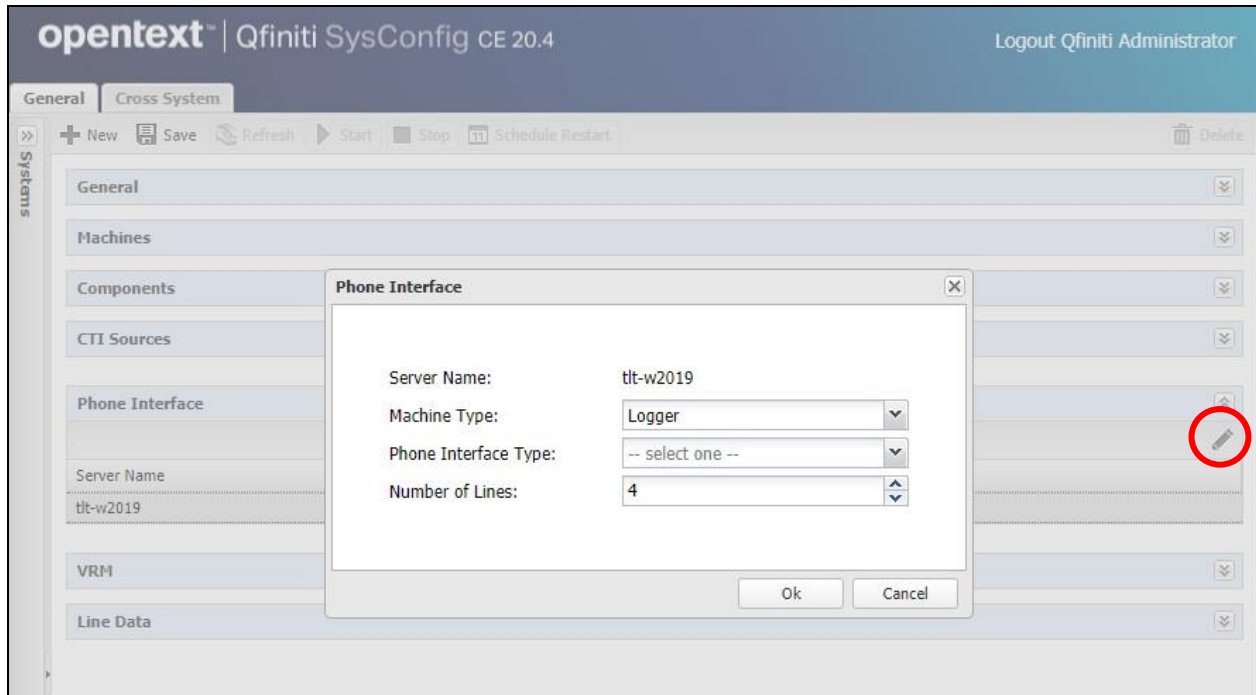
- CTI Server:** AvayaTSAPI
- PreInitExtensions:** Yes
- Queue:** 61001-61002
- Agent Extensions:** 65001, 66002
- UUdata script name:** CTI_UUdataScripts_AVAYA_TSAPI.ini
- Auto Login Extensions:** (empty)

The 'Queue' and 'Agent Extensions' fields have 'Or Drop files here' and 'Single Export' options. The 'Auto Login Extensions' field has two 'Enter Value' input boxes. The background interface shows the 'CTI Sources' section with a list of machines, including 'tit-w2019'. A red circle highlights the '+' icon in the top right corner of the 'CTI Sources' list, indicating the 'Add CTI Source' action.

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.

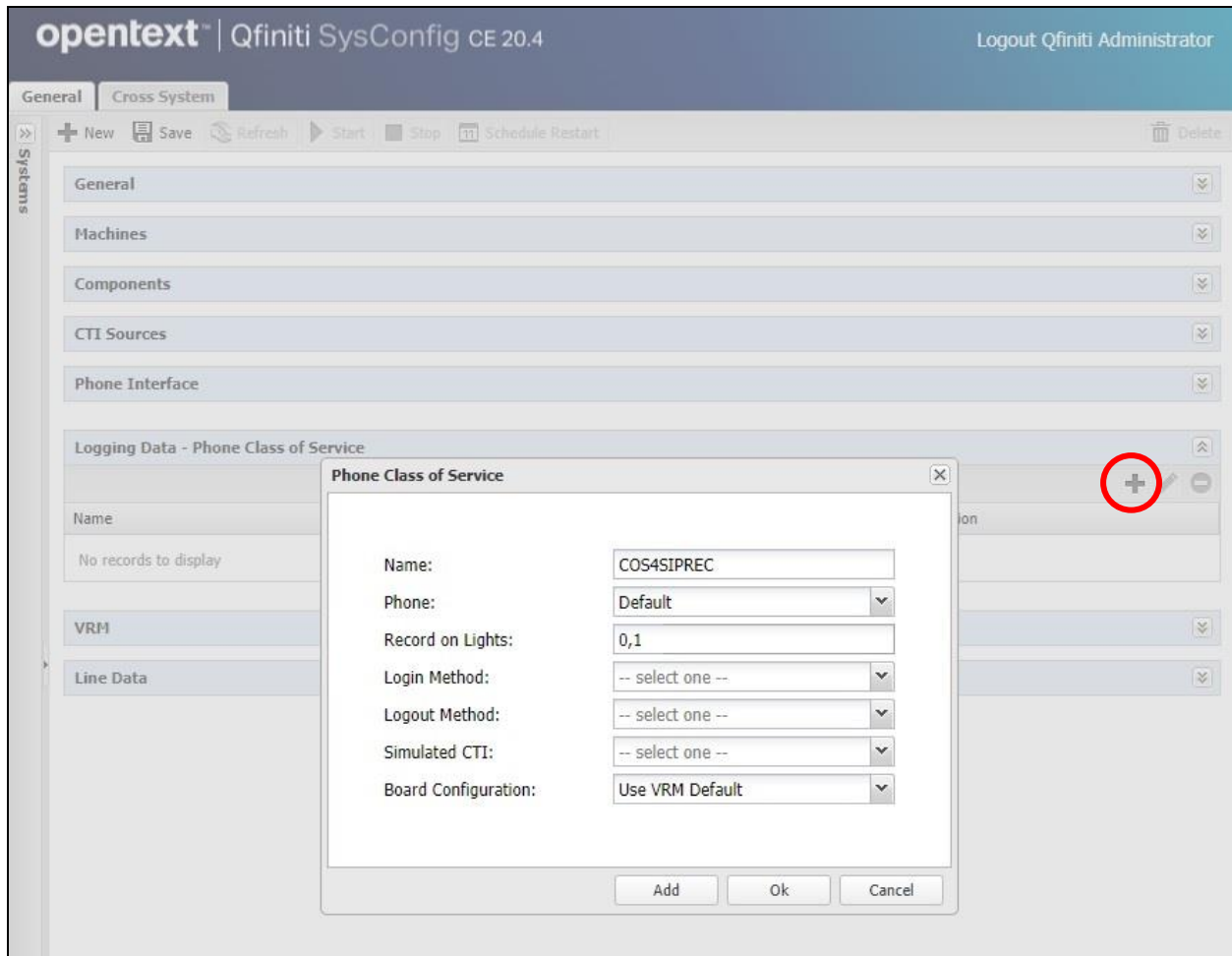
- **Machine Type:** “Logger”
- **Number of Lines:** Select twice the number of agents from **Section 3**.



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 “COS4SIPREC”.
- **Phone:** “Default”
- **Record on lights:** “0,1”



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 “VRM4SIPREC”.
- **VRM Type:** “Logging”
- **Interface Type:** “Dynamic Registration VoIP Recording”
- **Line From and Line To:** Range of lines from **Section 9.10**, in this case “1” to “4”.
- **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. A modal dialog box titled "VRM" is open, allowing for the configuration of a new VRM. The dialog contains the following fields and options:

- VRM Name:** Text input field containing "VRM4SIPREC".
- VRM Type:** Dropdown menu set to "Logging".
- Mirror from VRM:** Dropdown menu set to "-- select one --".
- Interface Type:** Dropdown menu set to "Dynamic Registration VoIP Recording".
- Use Range:** A checkbox labeled "(1-5, 6-100)" is checked, with a file upload icon and the text "Or Drop files here" to its right.
- Line From:** Text input field containing "1".
- Line To:** Text input field containing "4".
- Allow Extension Duplication:** A checkbox is present and unchecked.
- Default Class of Service:** Dropdown menu set to "COS4SIPREC".
- Default Board Config:** Dropdown menu set to "SIPRECNIC".

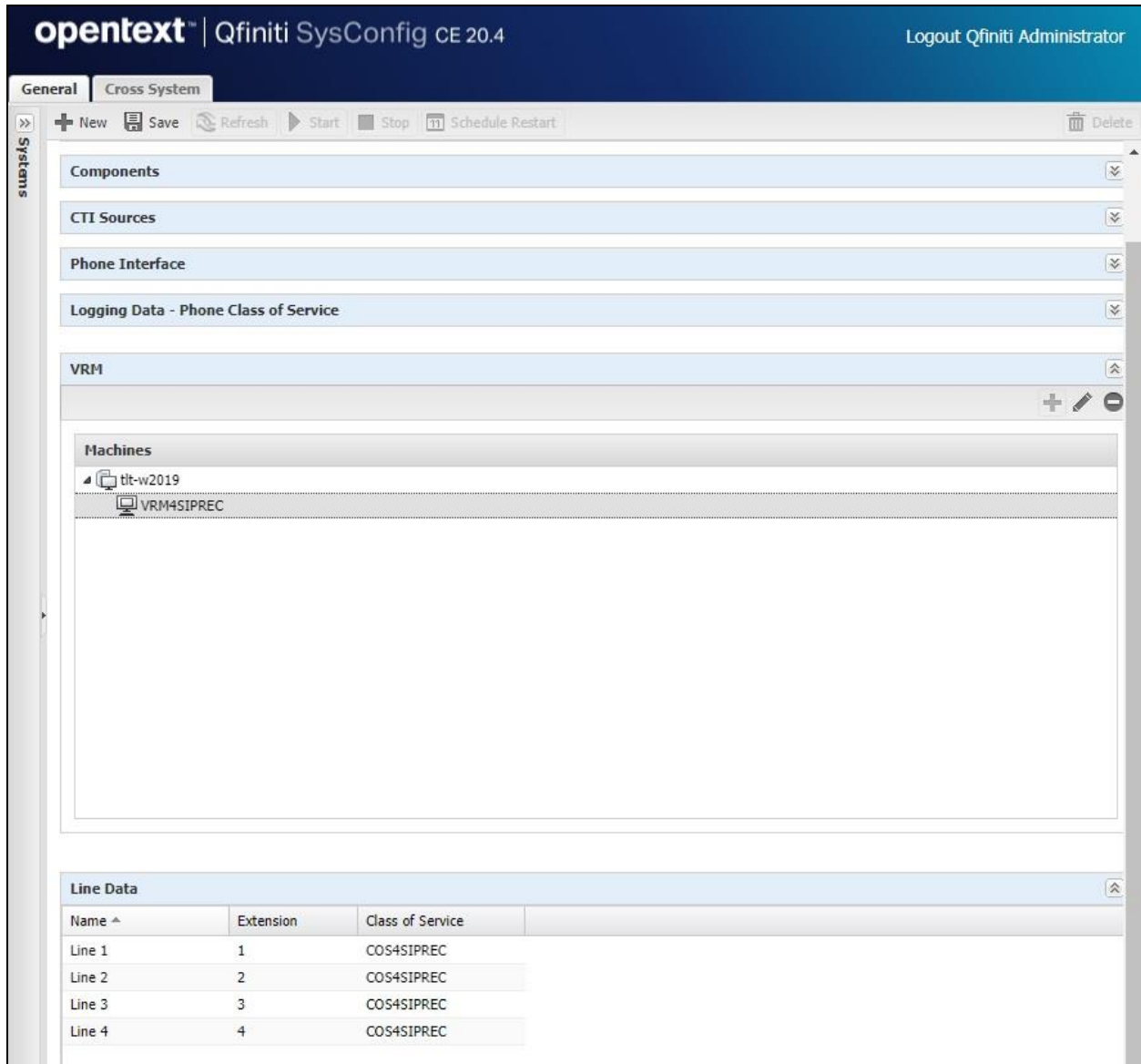
At the bottom of the dialog are "Ok" and "Cancel" buttons. In the background, the main interface shows a sidebar with a "VRM" section expanded, and a red circle highlights a "+" icon in the right-hand pane, indicating the "Add VRM" action.

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 line number. For **Class of Service**, select the phone class of service from **Section 9.11**.

Repeat this section to administer all lines as shown below.



The screenshot shows the opentext Qfiniti SysConfig CE 20.4 interface. The 'General' tab is selected, and the 'Cross System' section is active. The 'VRM' section is expanded, showing a list of machines. The 'Line Data' section is also expanded, displaying a table with four lines, each with an extension and a class of service.

Name ^	Extension	Class of Service
Line 1	1	COS4SIPREC
Line 2	2	COS4SIPREC
Line 3	3	COS4SIPREC
Line 4	4	COS4SIPREC

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' interface. The 'General' tab is selected. The 'Name' field is 'SIPREC System' and the 'Switch' is 'AvayaSIPREC'. Under 'System Type', several options are listed with checkboxes: 'Voice Recording - Logging' (checked), 'Voice Recording - QA', 'Screen Recording', 'Remote Screen Site', 'Explore', 'Survey', 'Backup', and 'Cloud Connector'. A 'Description' text area is below. At the bottom, the 'Available for Use' checkbox is checked and circled in red, with a help icon (?) next to it. The 'NAT Environment' checkbox is unchecked.

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' logo at the top. Below it are two input fields: 'User name' and 'Password', both with placeholder text. The background is a dark blue gradient.

9.16. Administer Observe Settings

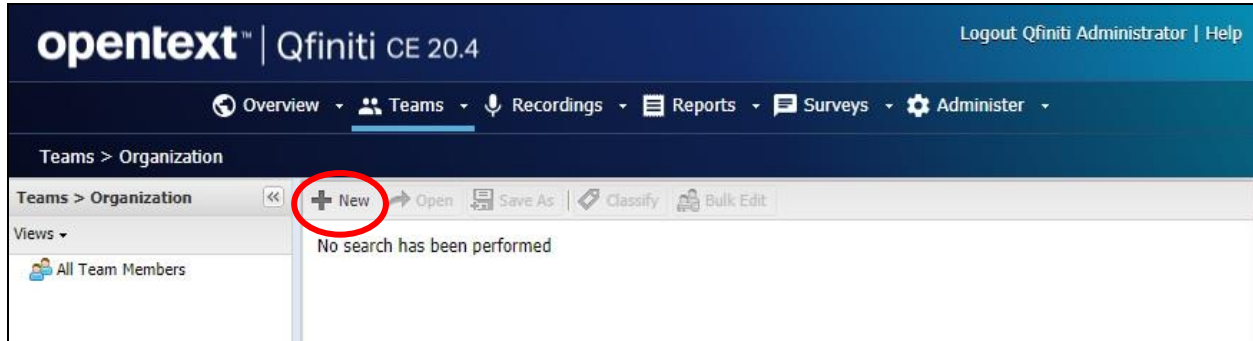
In the subsequent screen, select **Administer** → **Settings** from the top menu, followed by **Observe Settings** in the left pane.

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' interface. The top navigation bar includes 'Overview', 'Teams', 'Recordings', 'Reports', 'Surveys', and 'Administer'. The 'Administer' menu is expanded, showing 'Settings' and 'Observe Settings'. The left sidebar lists 'Alarm Settings', 'License Settings', 'Observe Settings' (selected), 'Platform Settings', 'Survey Settings', and 'Web Access Settings'. The main content area is titled 'Administer > Settings > Observe Settings' and features a 'Save' button. The 'Recording Options' section, with the instruction 'Select the option and check the boxes to activate the desired recording options.', contains an 'Option:' dropdown set to 'Continuous Record' and a 'Type:' section with four checkboxes: '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 instructs the user to 'Enter the UNC path to store the phone player prompts.' and includes a text input field for the '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 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 form is titled 'General Information' and includes fields for 'First Name', 'Middle Name', 'Last Name', 'Email Address', 'Role', 'Username', 'Password', 'Confirm Password', and 'Partition'. The 'First Name' field contains 'FNAgent1', 'Last Name' contains 'LnAgent1', 'Role' is set to 'Administrators', 'Username' is 'agent1', 'Password' and 'Confirm Password' are masked with dots, and 'Partition' is 'Qfiniti'. There are checkboxes for 'Active' and 'Enabled', and a 'View Inactive Members' link. A 'Delete' button is also visible in the top right corner.

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**

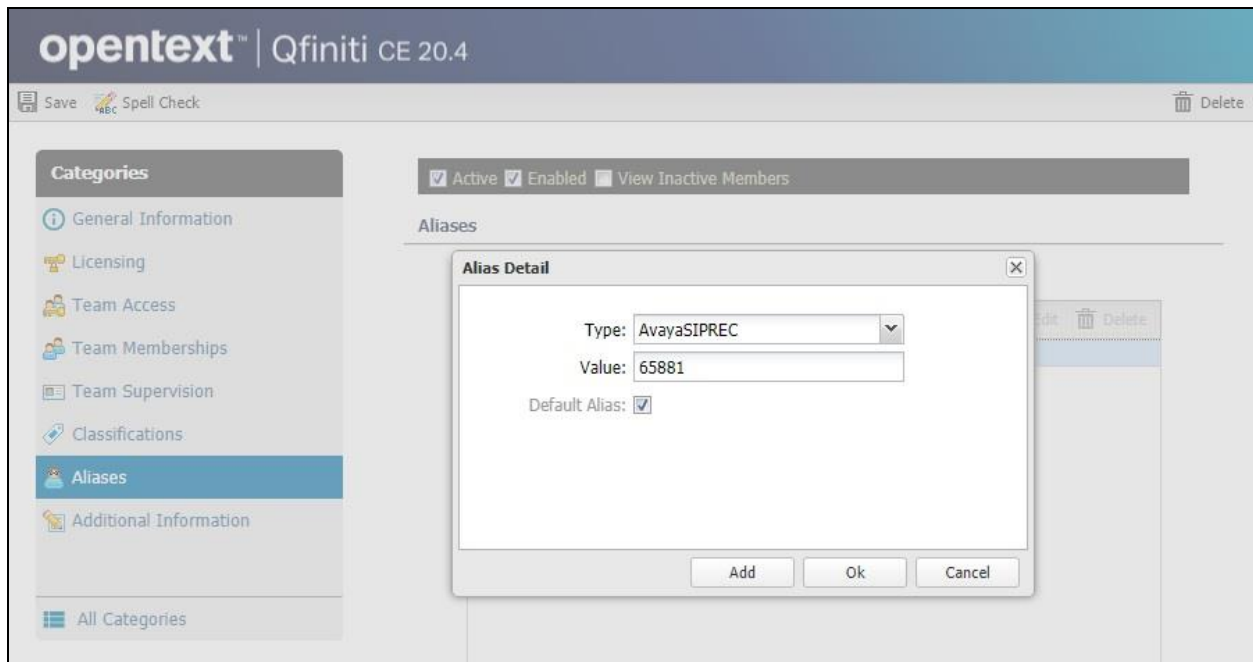
☒ Active ☒ Enabled ☐ View Inactive Members

Aliases

Define aliases for this team member.

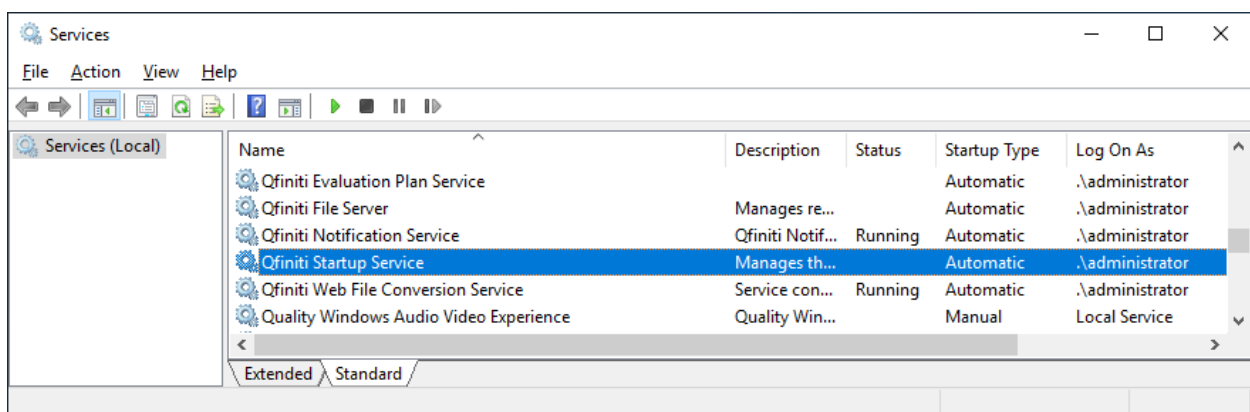
The **Alias Detail** pop-up screen is displayed. For **Type**, select the switch server name from **Section 9.3**. For **Value**, enter the agent ID for the first agent in **Section 3**, in this case “65881”. Retain the default value in the remaining field.

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

10.1. Verify TSAPI Connection

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

Verify that **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”.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Thu Mar 4 09:21:16 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: Thu Mar 04 10:59:37 EST 2021
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
<input checked="" type="radio"/>	1	cm7	1	Talking	Mon Feb 22 16:15:22 2021	Online	18	4	19	19	30

Online Offline

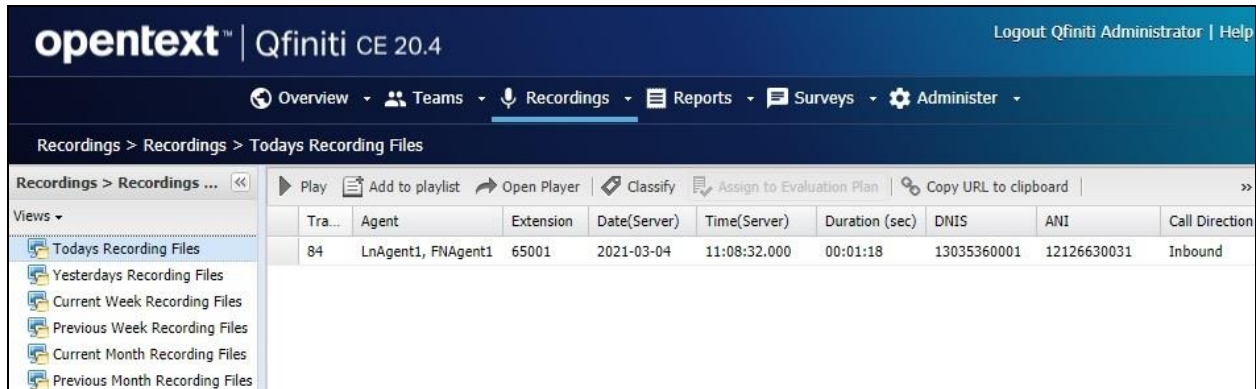
For service-wide information, choose one of the following:

TSAPI Service Status TLink Status User Status

10.2. Verify SIPREC Recording

Log an agent in to handle and complete an ACD 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

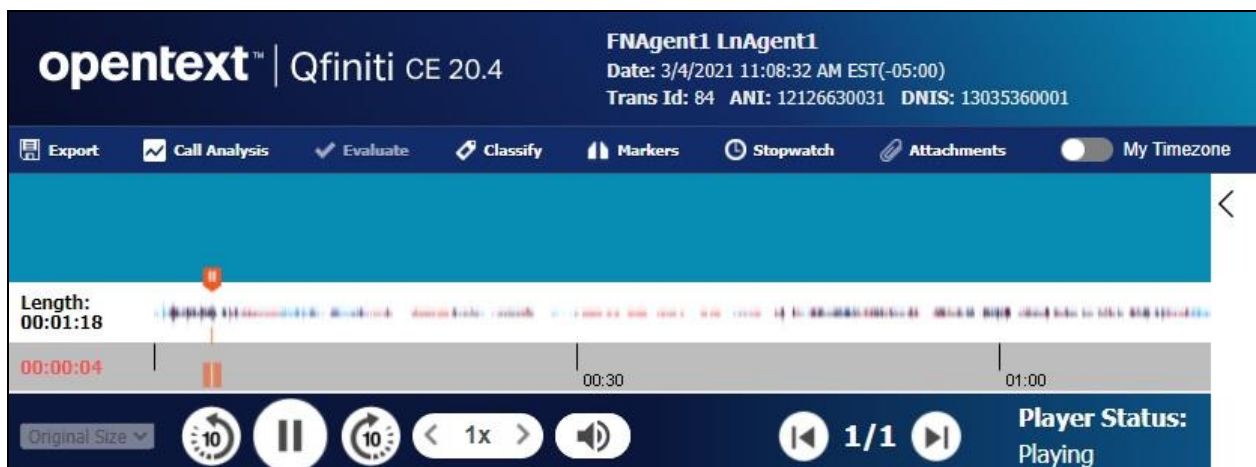
Recordings > Recordings ... << Play Add to playlist Open Player Classify Assign to Evaluation Plan Copy URL to clipboard >>

Views

- Todays Recording Files
- Yesterdays Recording Files
- Current Week Recording Files
- Previous Week Recording Files
- Current Month Recording Files
- Previous Month Recording Files

Tra...	Agent	Extension	Date(Server)	Time(Server)	Duration (sec)	DNIS	ANI	Call Direction
84	LnAgent1, FNAgent1	65001	2021-03-04	11:08:32.000	00:01:18	13035360001	12126630031	Inbound

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



opentext™ | Qfiniti CE 20.4 FNAgent1 LnAgent1

Date: 3/4/2021 11:08:32 AM EST(-05:00)

Trans Id: 84 ANI: 12126630031 DNIS: 13035360001

Export Call Analysis Evaluate Classify Markers Stopwatch Attachments My Timezone

Length: 00:01:18

00:00:04 00:30 01:00

Original Size 10 10 < 1x > 1/1 Player Status: Playing

11. Conclusion

These Application Notes describe the configuration steps required for OpenText Qfiniti 20.4 to successfully interoperate with Avaya Session Border Controller for Enterprise 8.1.2 and Avaya Aura® Application Enablement Services 8.1.3. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

12. 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 Session Border Controller for Enterprise*, Release 8.1.x, Issue 4, December 2020, 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.