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

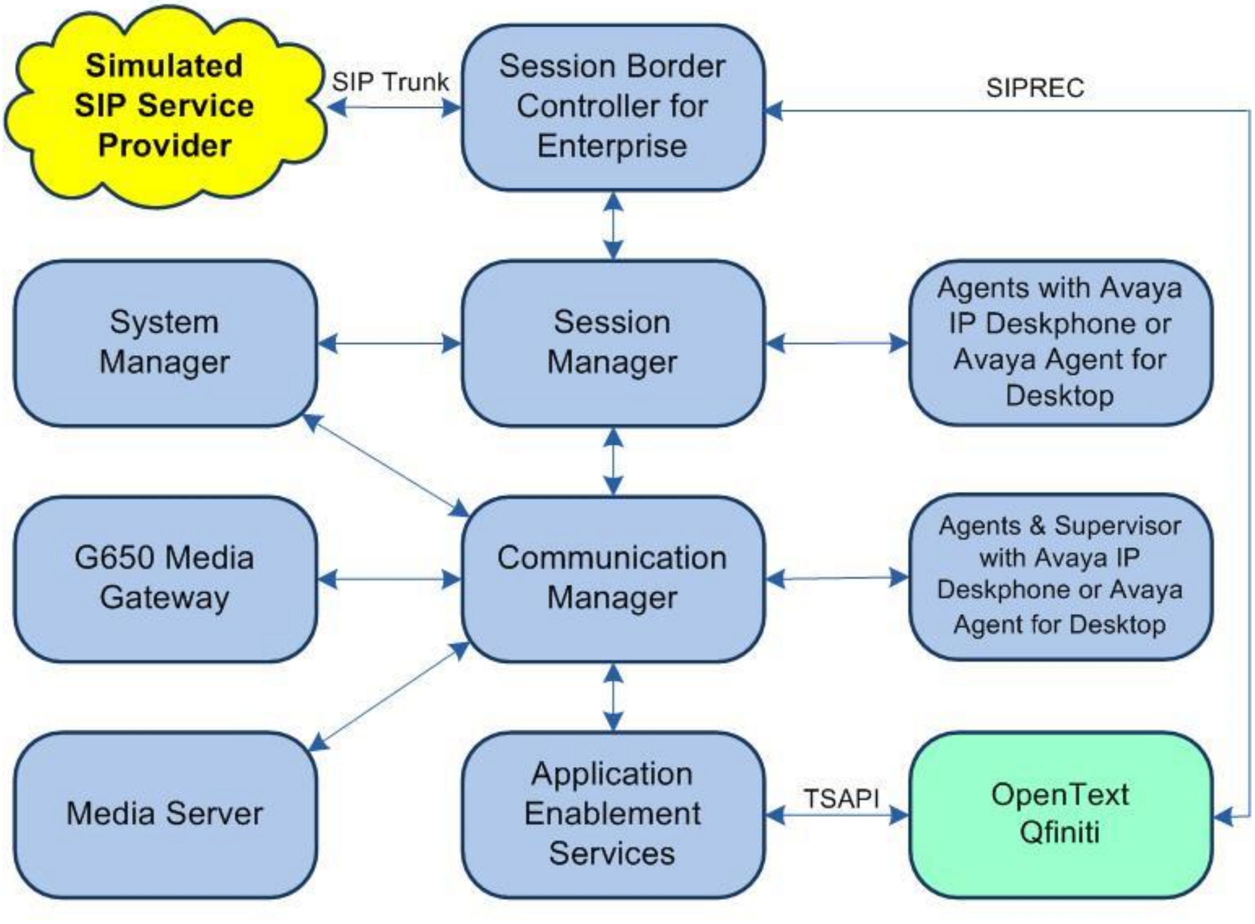

Simulated SIP Service Provider
SIP Trunk
Session Border Controller for Enterprise
SIPREC
System Manager
Session Manager
Agents with Avaya IP Deskphone or Avaya Agent for Desktop
G650 Media Gateway
Communication Manager
Agents & Supervisor with Avaya IP Deskphone or Avaya Agent for Desktop
Media Server
Application Enablement Services
TSAPI
OpenText Qfiniti

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 • Microsoft SQL Server 2019 • Avaya 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
```

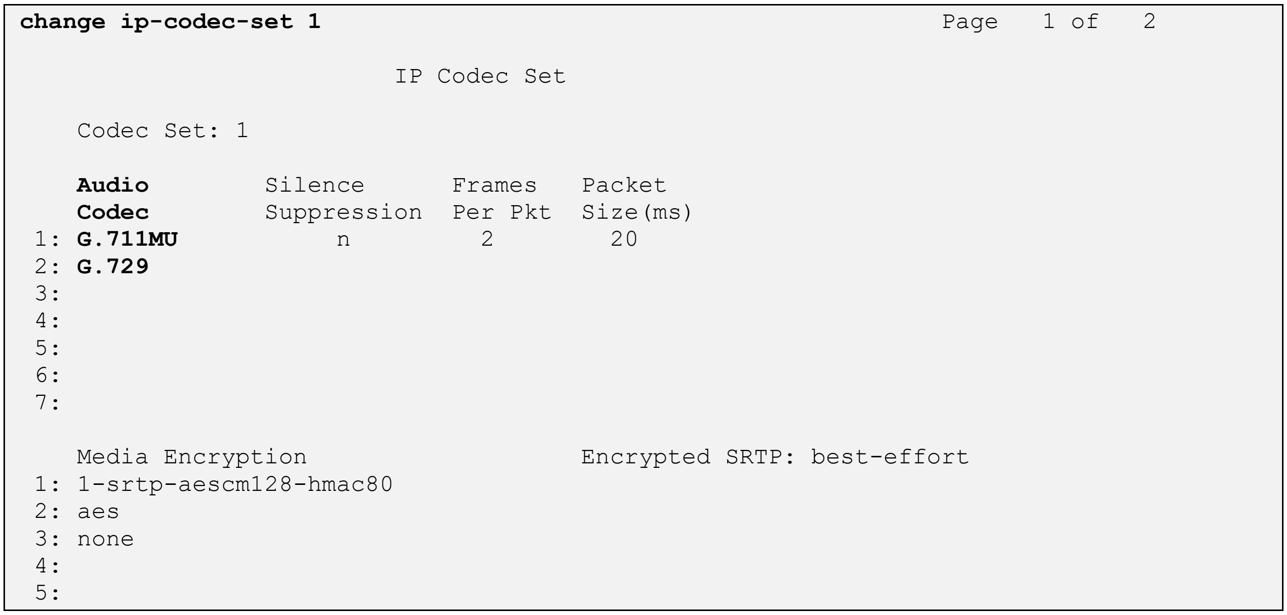
5.2. Administer CTI Link

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 UUI 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.

- **UUI 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
                                                UUI 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

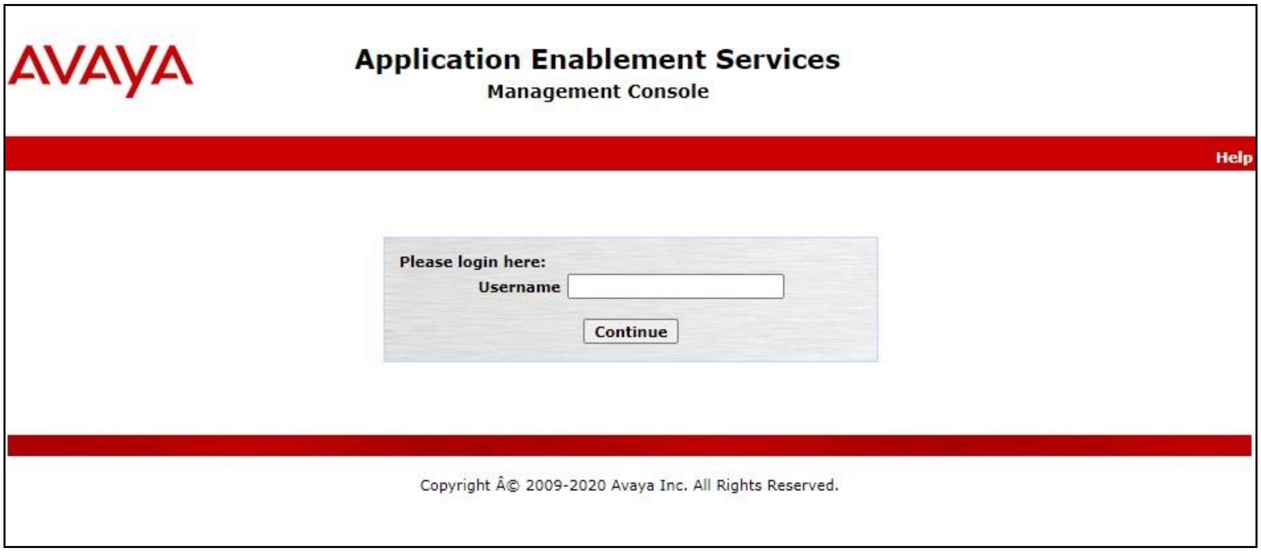
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer Qfiniti user
- Administer security database
- Restart service
- Obtain Tlink name

6.1. Launch OAM Interface

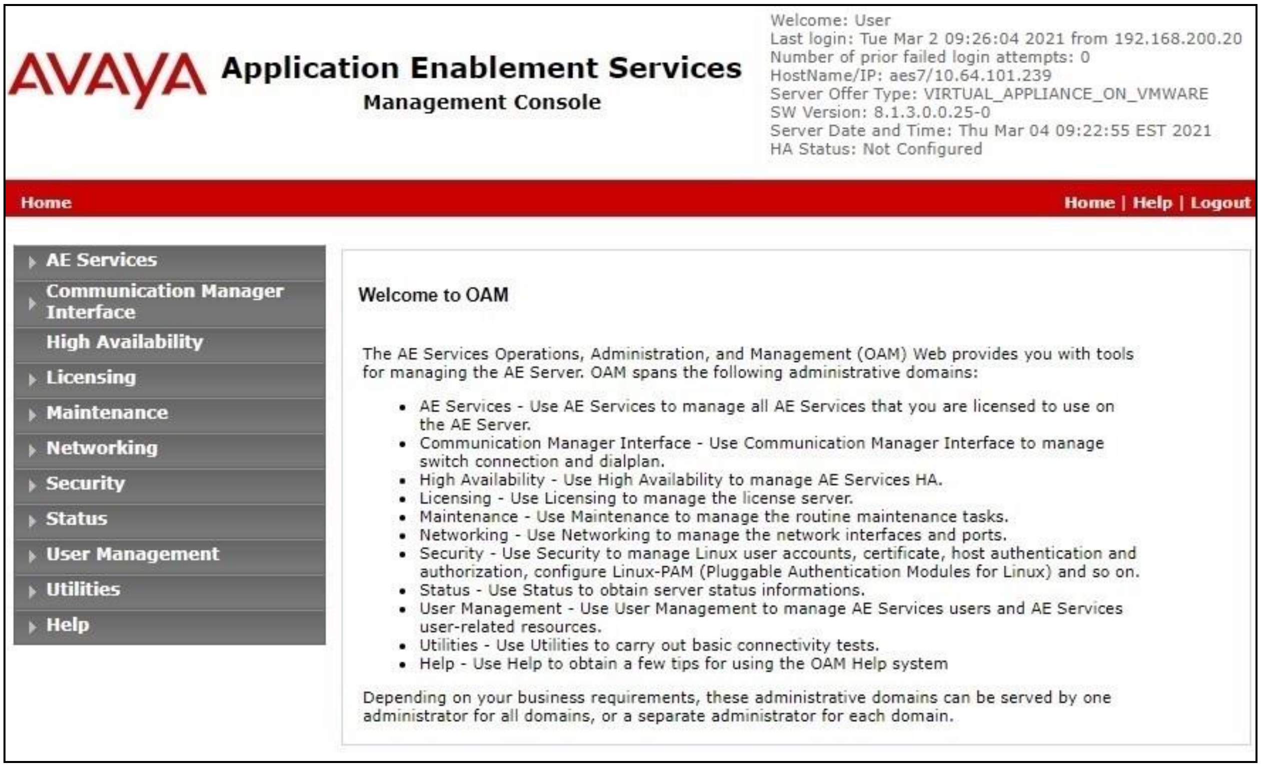
Access the OAM web-based interface by using the URL "https://ip-address" in an Internet browser window, where "ip-address" is the IP address of the Application Enablement Services server.

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



Copyright Â© 2009-2020 Avaya Inc. All Rights Reserved.

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



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

Welcome to OAM

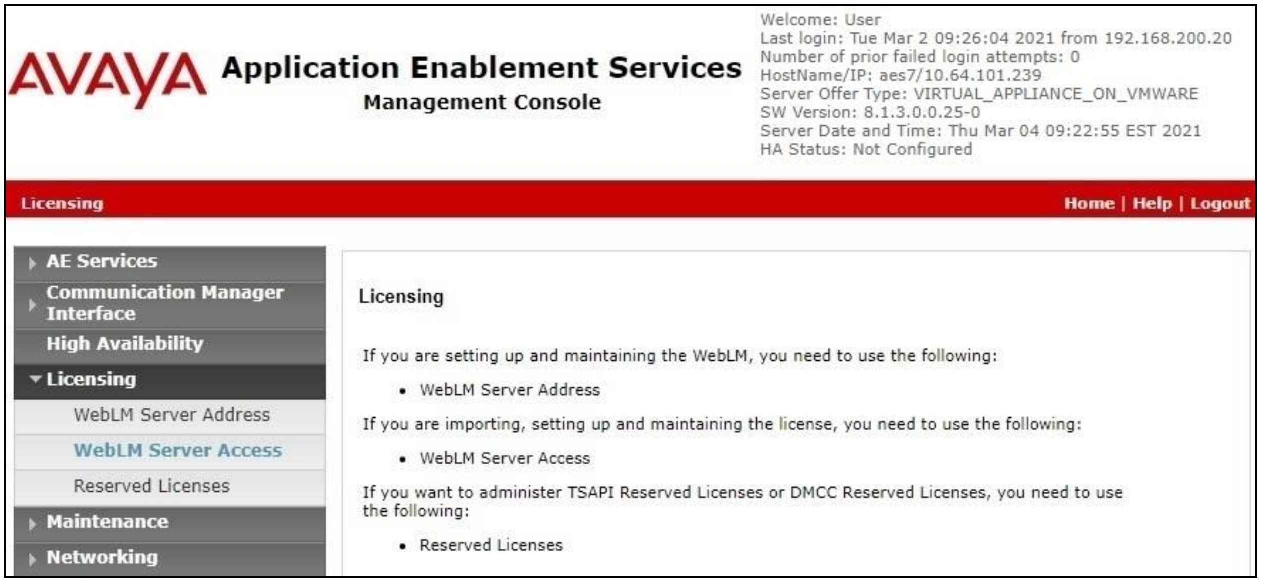
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- 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).



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

Licensing

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

- WebLM Server Address

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

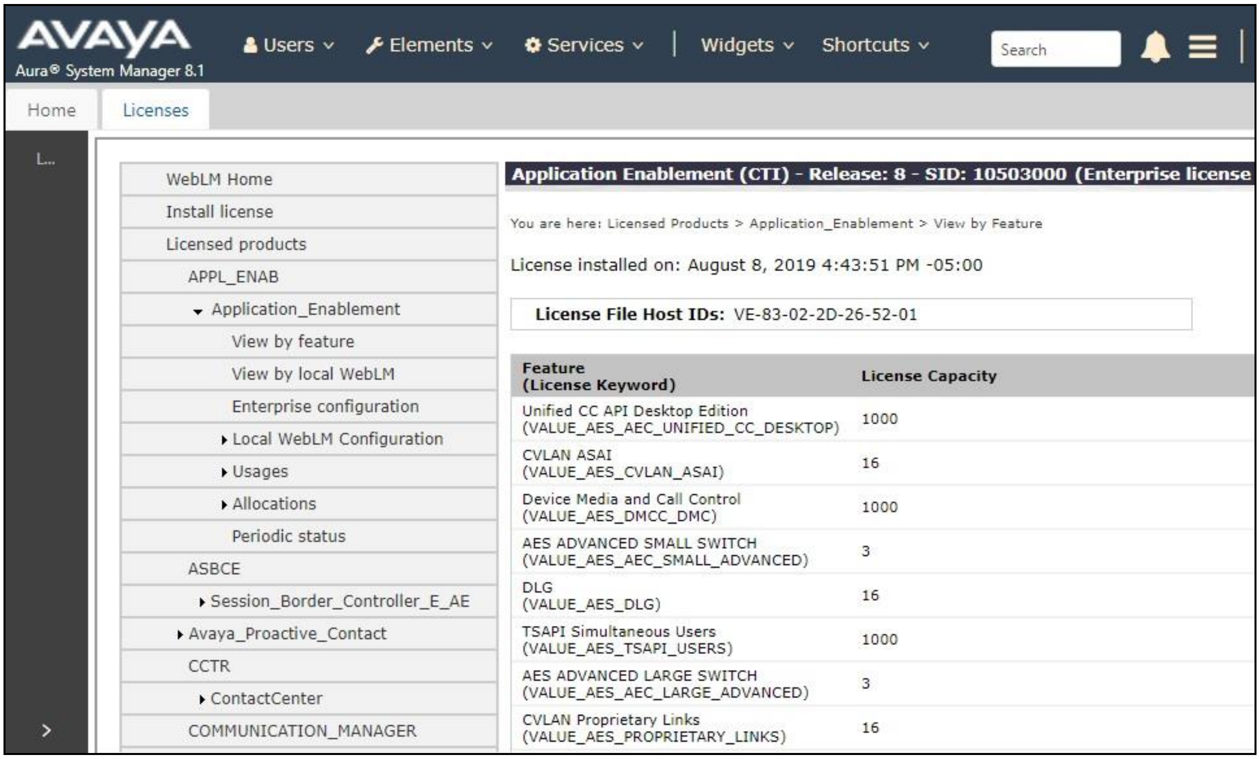
- WebLM Server Access

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

- Reserved Licenses

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

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



Application Enablement (CTI) - Release: 8 - SID: 10503000 (Enterprise license

You are here: Licensed Products > Application_Enablement > View by Feature

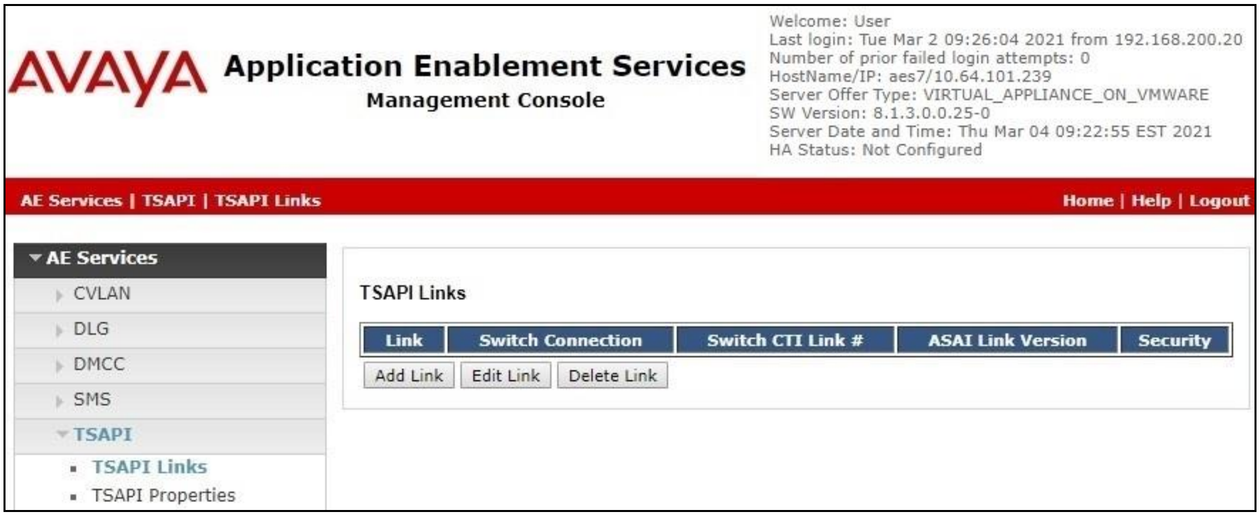
License installed on: August 8, 2019 4:43:51 PM -05:00

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**.



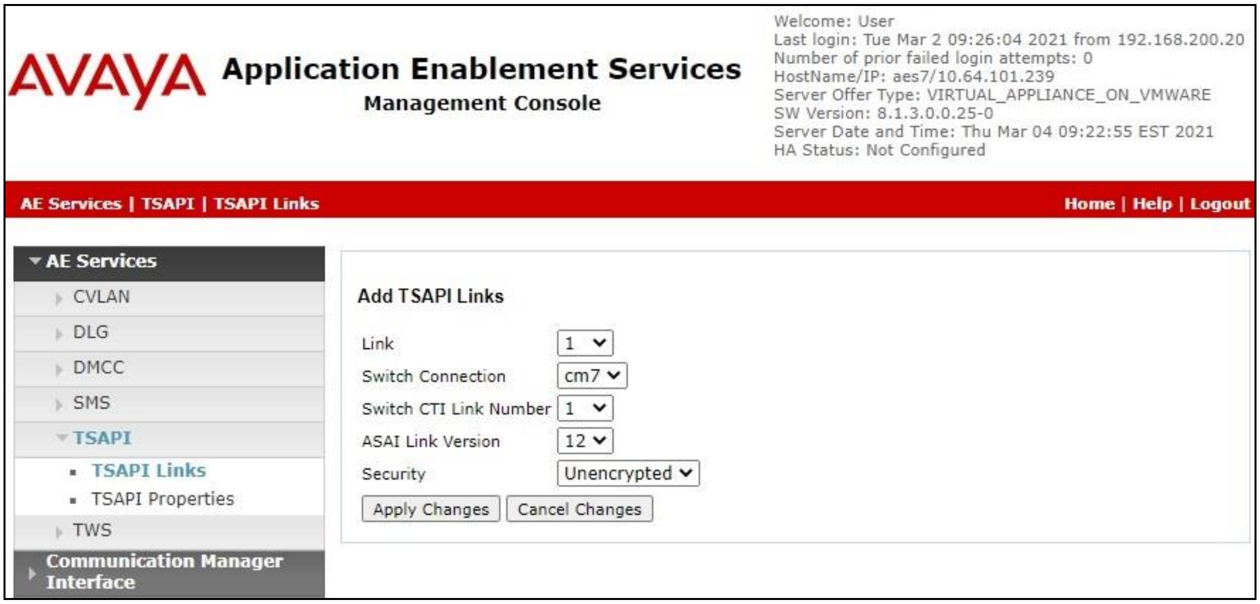
Welcome: User
Last login: Tue Mar 2 09:26:04 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Thu Mar 04 09:22:55 EST 2021
HA Status: Not Configured

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security

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.



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

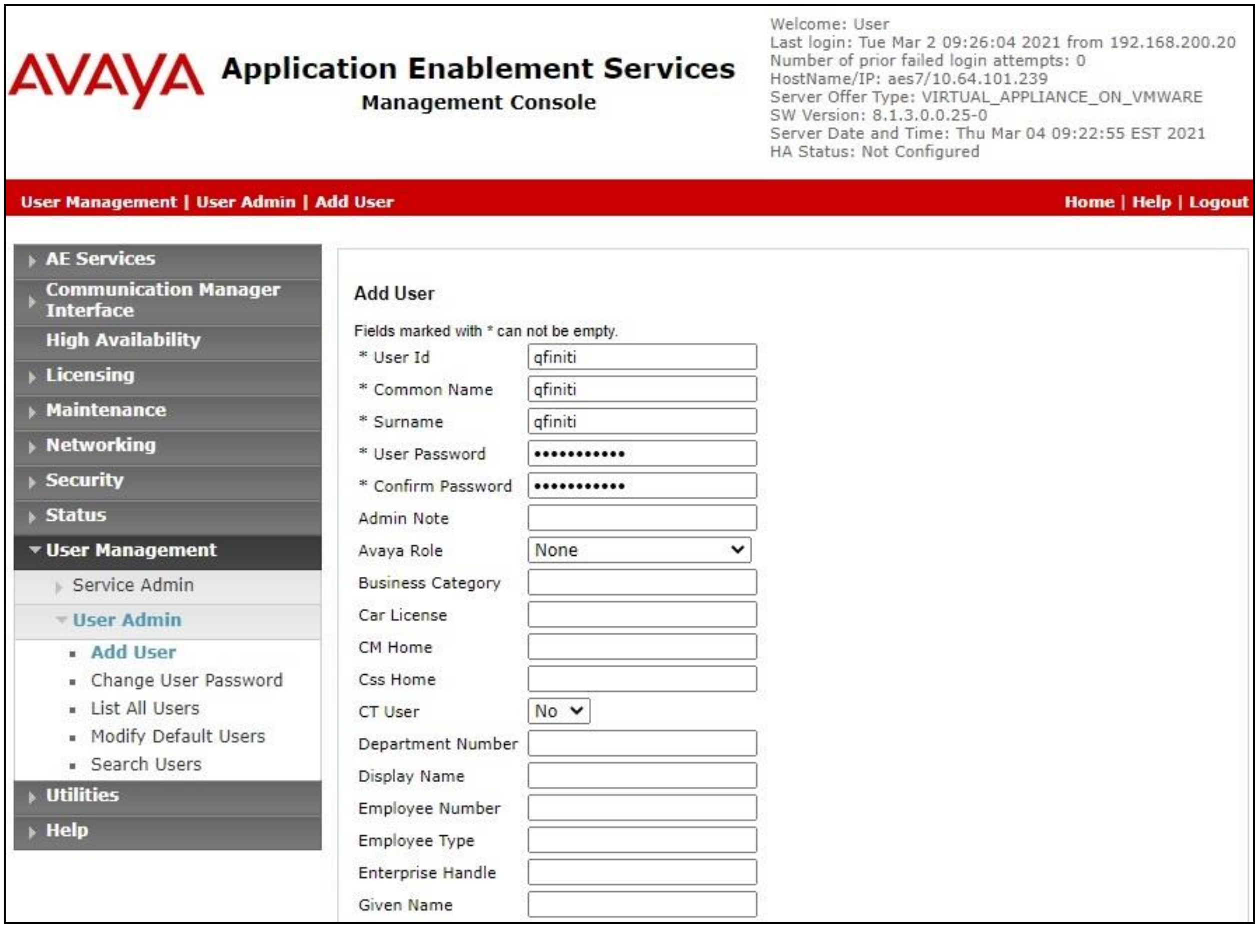
Add TSAPI Links

Link	1
Switch Connection	cm7
Switch CTI Link Number	1
ASAI Link Version	12
Security	Unencrypted

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.



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

Add User

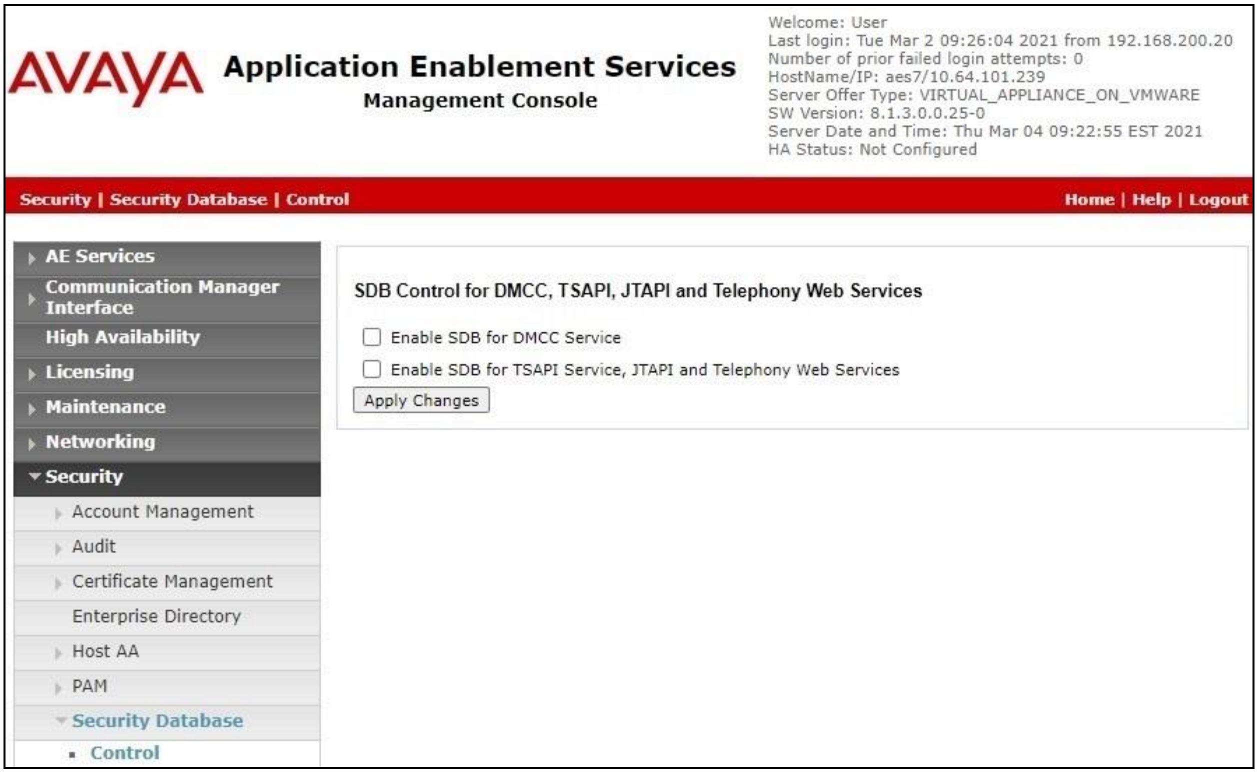
Fields marked with * can not be empty.

* User Id	qfiniti
* Common Name	qfiniti
* Surname	qfiniti
* User Password	•••••••••••
* Confirm Password	•••••••••••
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	No
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**.



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

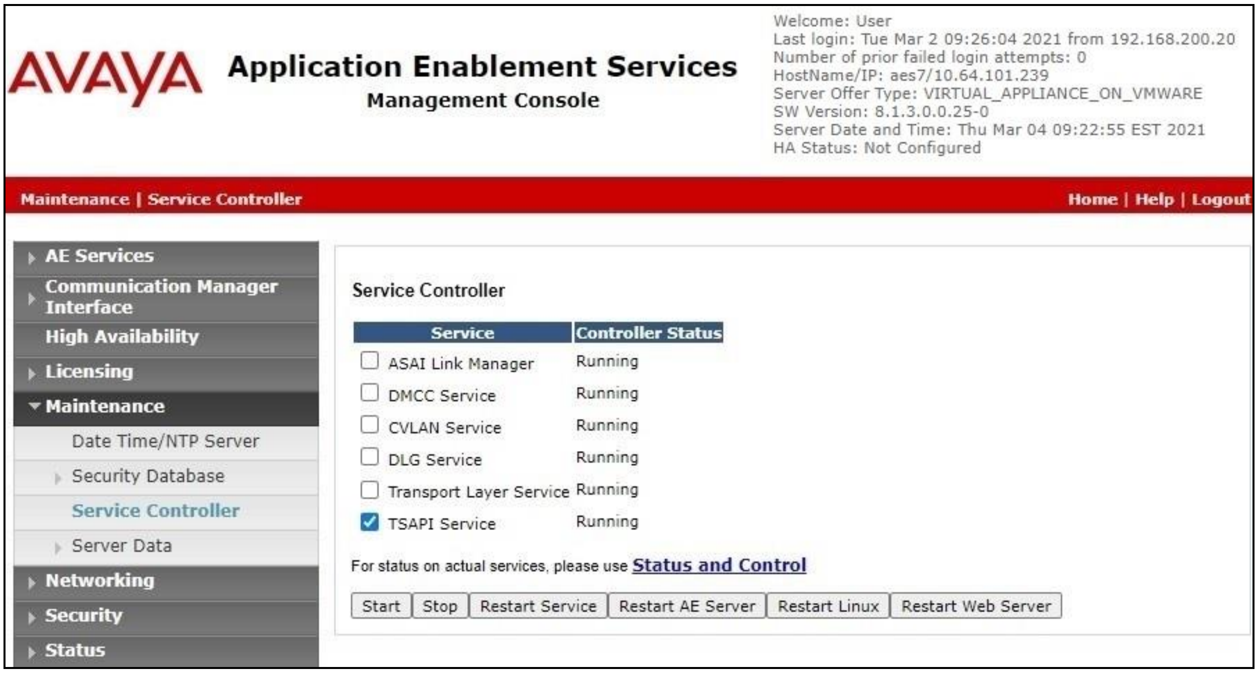
SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

□ Enable SDB for DMCC Service

□ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

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**.



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

Service Controller

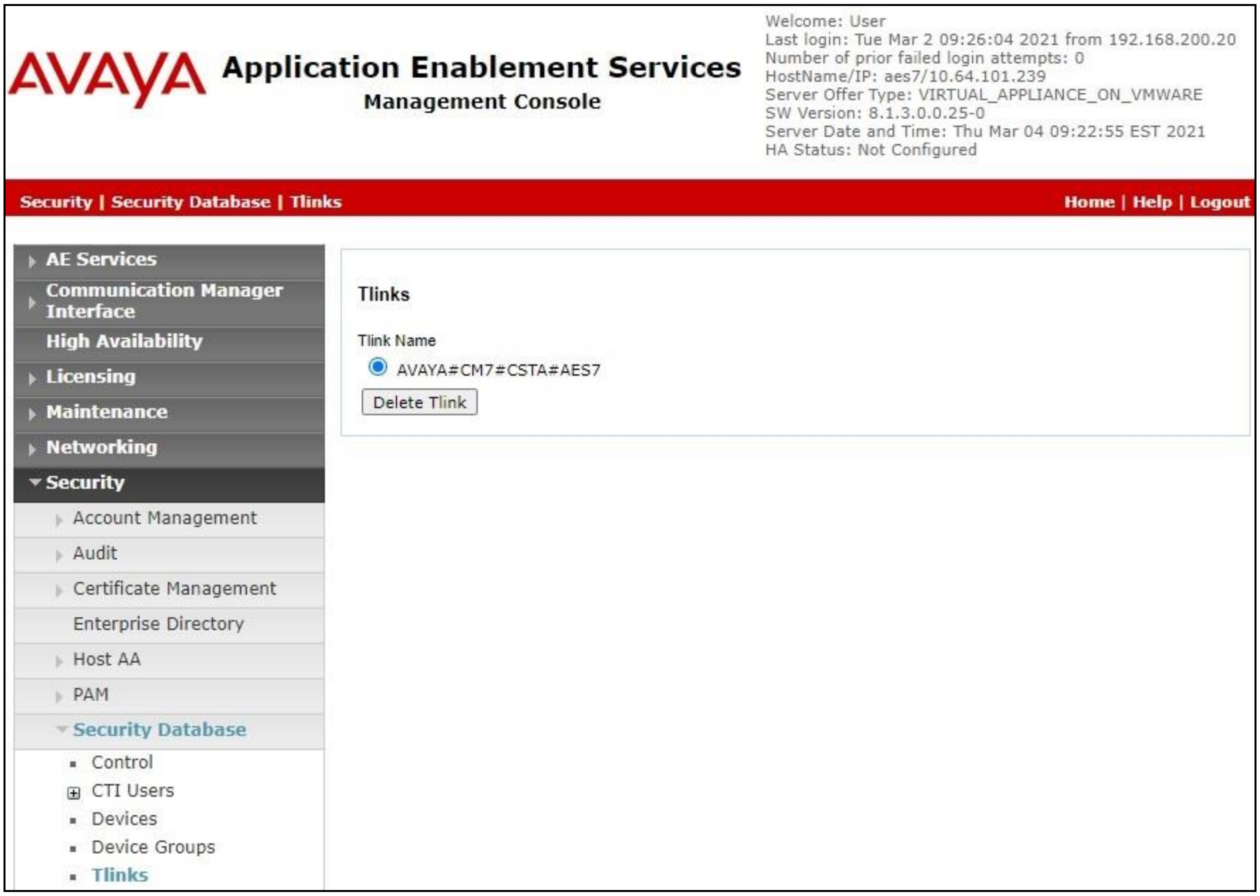
Service	Controller Status
□ ASAI Link Manager	Running
□ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
☑ TSAPI Service	Running

For status on actual services, please use Status and Control

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".



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

Tlinks

Tlink Name

● AVAYA#CM7#CSTA#AES7

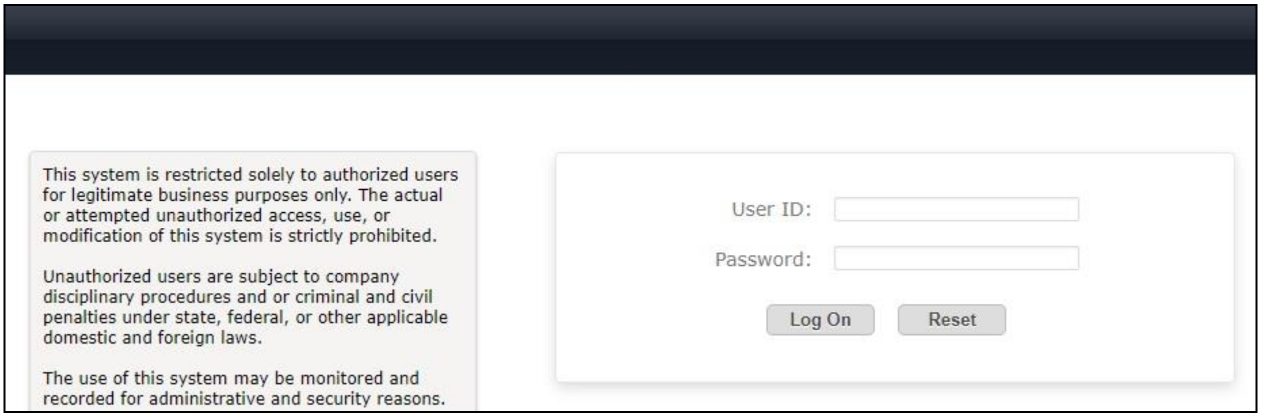
7. Configure Avaya Aura® Session Manager

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.



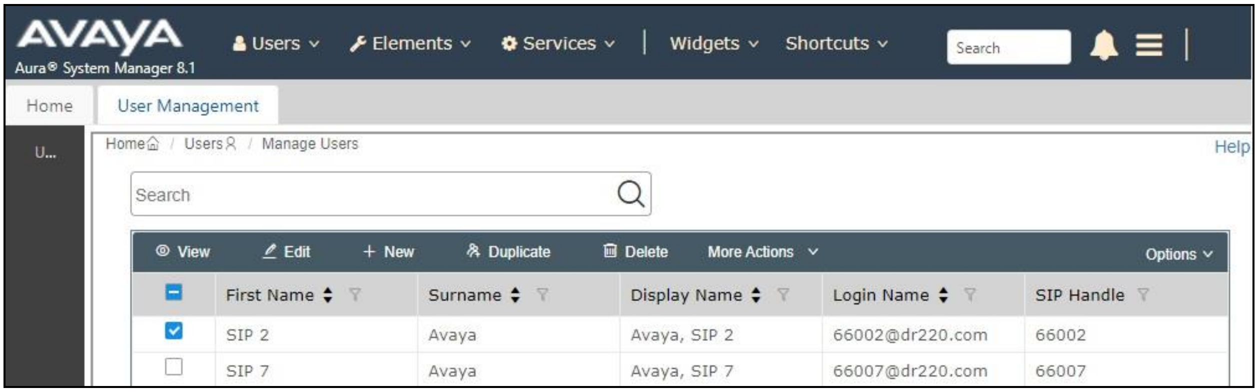
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons.

7.2. Administer Users

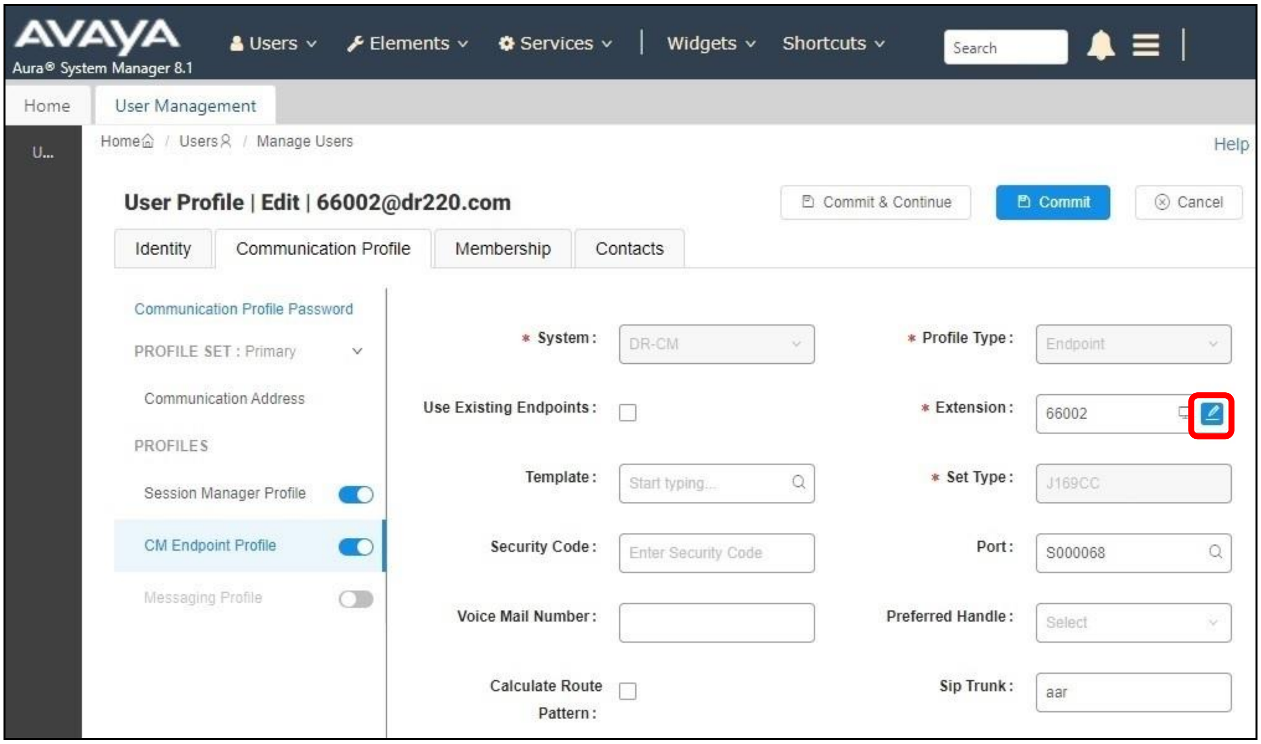
In the subsequent screen (not shown), select **Users → User Management** from the top menu. Select **User Management → Manage Users** (not shown) from the left pane to display the screen below. Select the entry associated with the first SIP agent station from **Section 3**, in this case "66002", and click **Edit**.



☐	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.

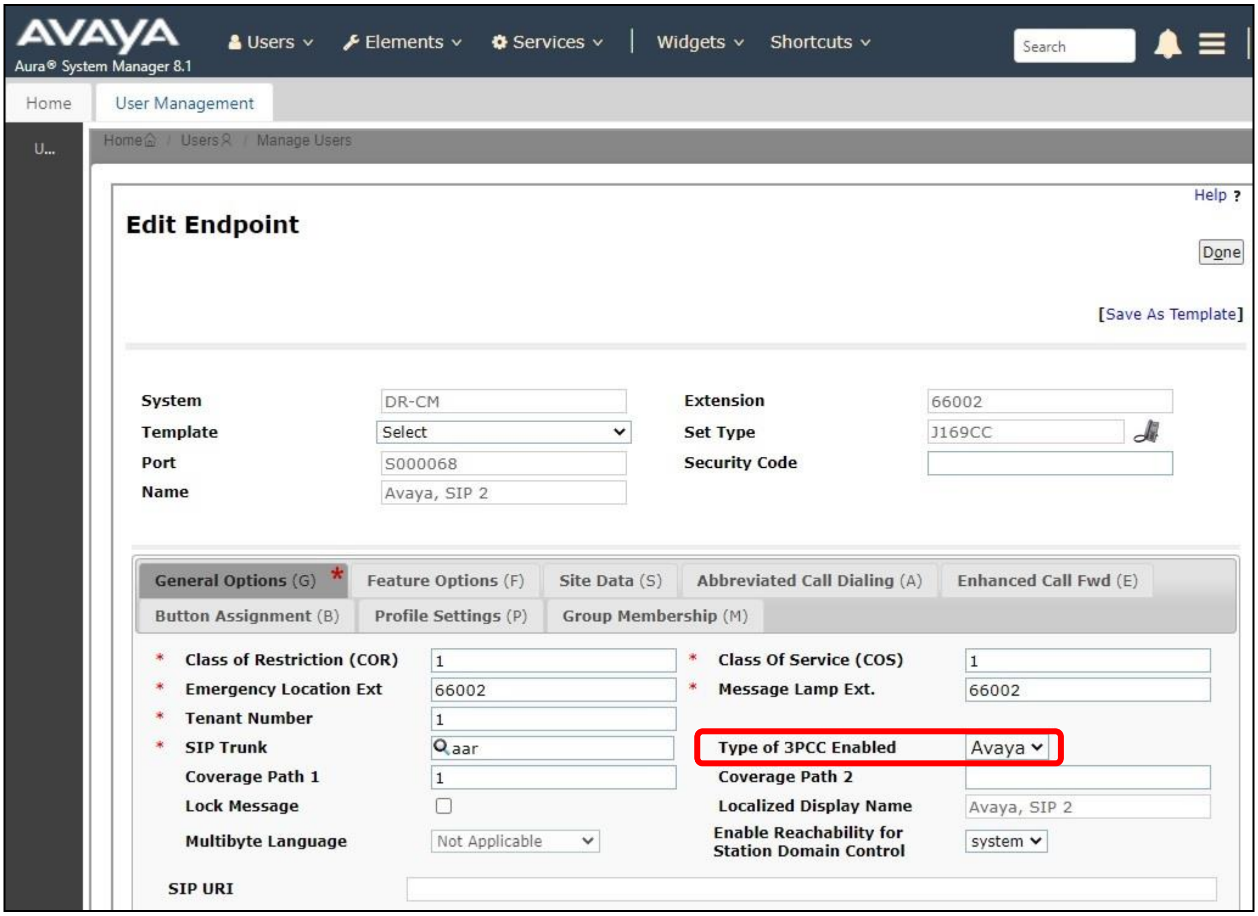


User Profile | Edit | 66002@dr220.com

* System :	DR-CM	* Profile Type :	Endpoint
Use Existing Endpoints :	□	* Extension :	66002
Template :	Start typing...	* Set Type :	J169CC
Security Code :	Enter Security Code	Port :	S000068
Voice Mail Number :		Preferred Handle :	Select
Calculate Route Pattern :	□	Sip Trunk :	aar

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.



Edit Endpoint

System	DR-CM	Extension	66002
Template	Select	Set Type	J169CC
Port	S000068	Security Code	
Name	Avaya, SIP 2		

* Class of Restriction (COR)	1	* Class Of Service (COS)	1
* Emergency Location Ext	66002	* Message Lamp Ext.	66002
* Tenant Number	1		
* SIP Trunk	aar	Type of 3PCC Enabled	Avaya
Coverage Path 1	1	Coverage Path 2	
Lock Message	□	Localized Display Name	Avaya, SIP 2
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system
SIP URI			

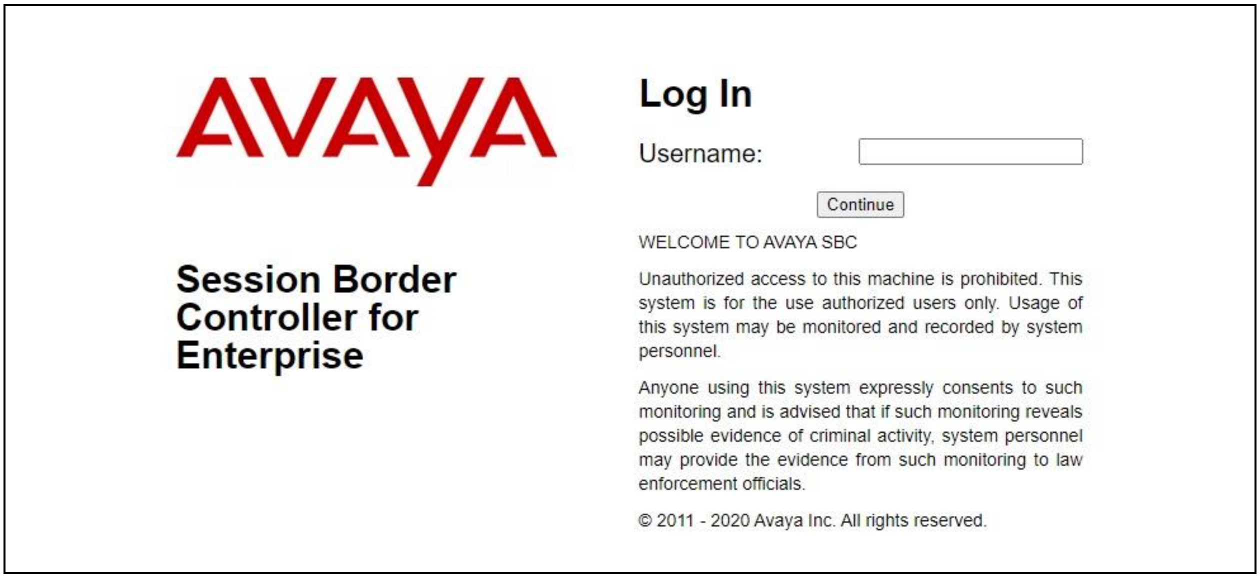
8. Configure Avaya Session Border Controller for Enterprise

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.



WELCOME TO AVAYA SBC

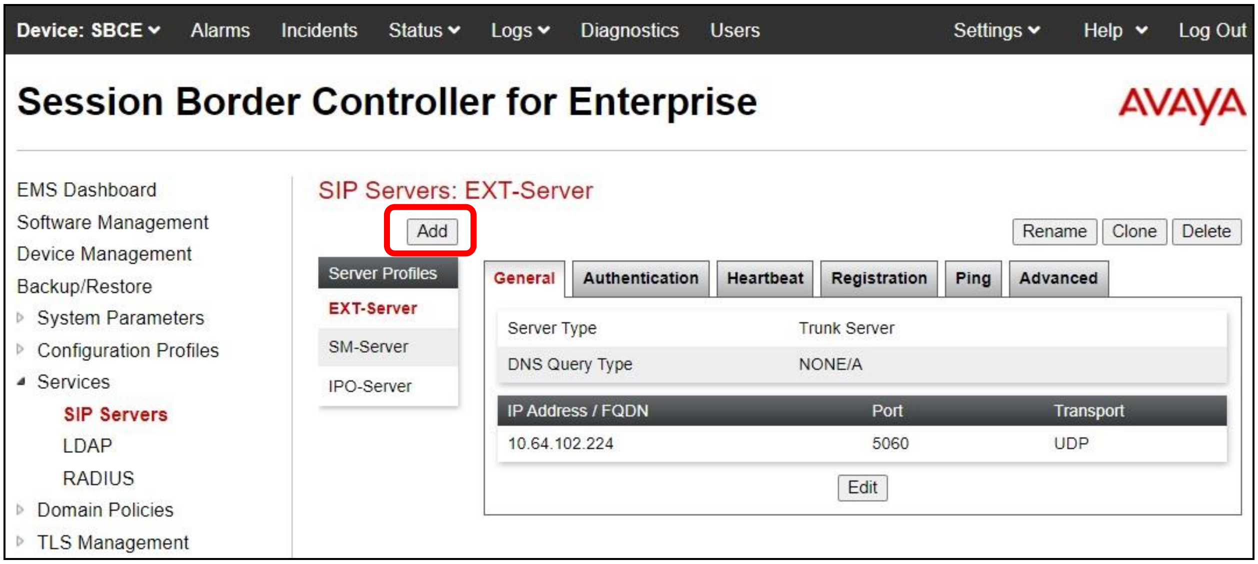
Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

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.

© 2011 - 2020 Avaya Inc. All rights reserved.

8.2. Administer SIP Servers

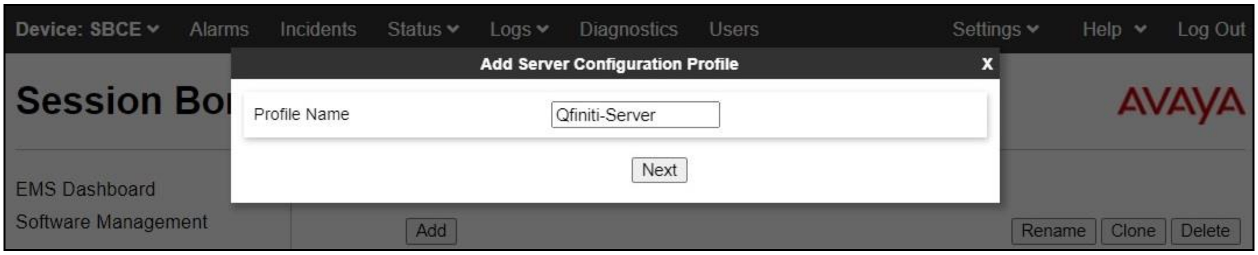
In the subsequent screen, select **Device → SBCE** from the top menu, followed by **Backup/Restore → Services → SIP Servers** from the left pane to display existing SIP server profiles. Click **Add** to add a SIP server profile for Qfiniti.



Server Type	Trunk Server
DNS Query Type	NONE/A

IP Address / FQDN	Port	Transport
10.64.102.224	5060	UDP

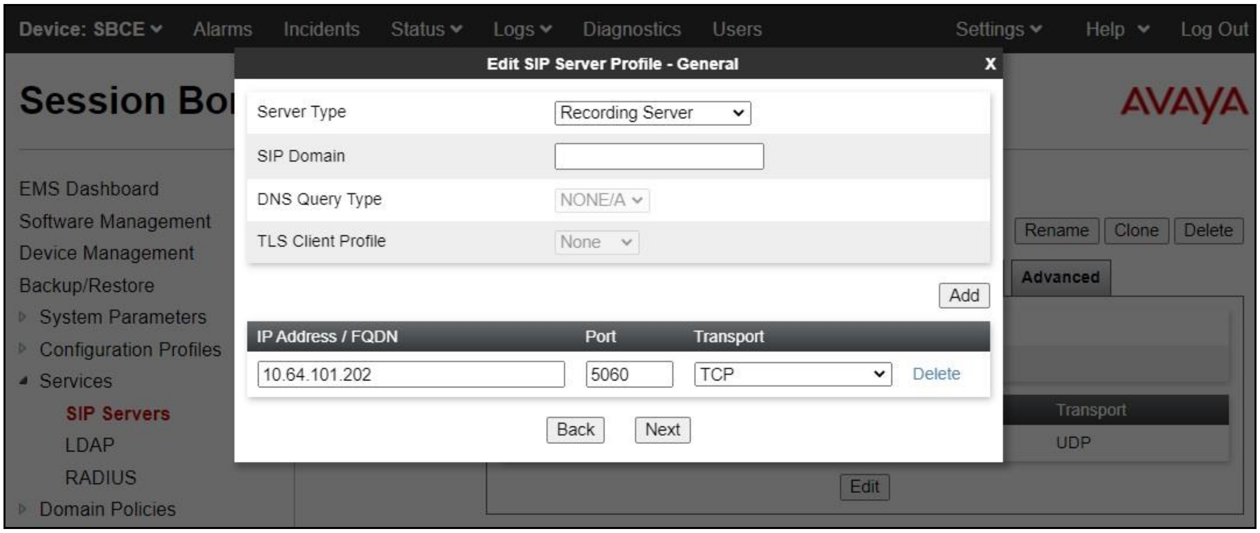
The **Add Server Configuration Profile** pop-up screen is displayed. Enter a desired **Profile Name** as shown below.



Profile Name	Qfiniti-Server

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"

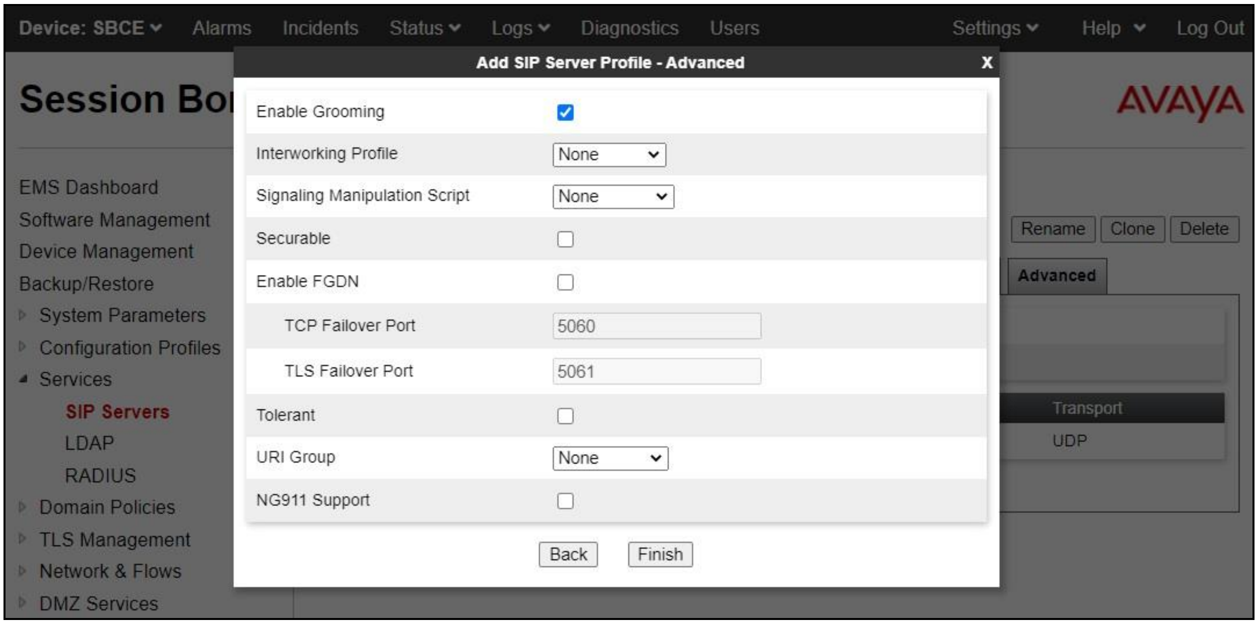


Edit SIP Server Profile - General

Server Type	Recording Server
SIP Domain	
DNS Query Type	NONE/A
TLS Client Profile	None

IP Address / FQDN	Port	Transport
10.64.101.202	5060	TCP

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

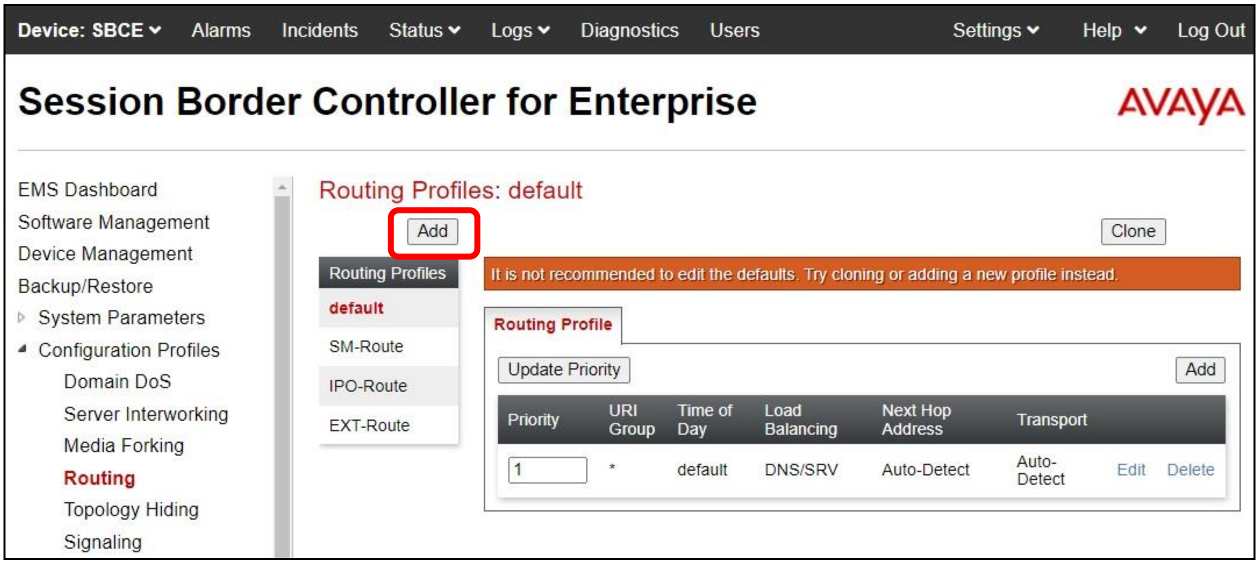


Add SIP Server Profile - Advanced

Enable Grooming	☑
Interworking Profile	None
Signaling Manipulation Script	None
Securable	☐
Enable FGDN	☐
TCP Failover Port	5060
TLS Failover Port	5061
Tolerant	☐
URI Group	None
NG911 Support	☐

8.3. Administer Routing

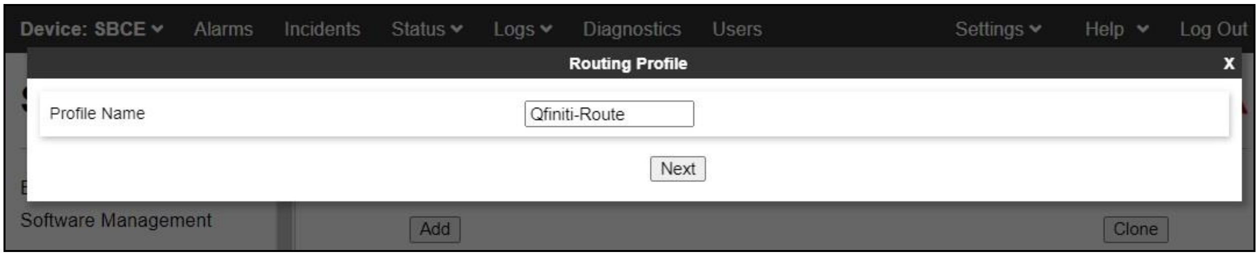
Select **Backup/Restore → Configuration Profiles → Routing** from the left pane to display existing routing profiles. Click **Add** to add routing profile for Qfiniti.



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

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport		
1	*	default	DNS/SRV	Auto-Detect	Auto-Detect	Edit	Delete

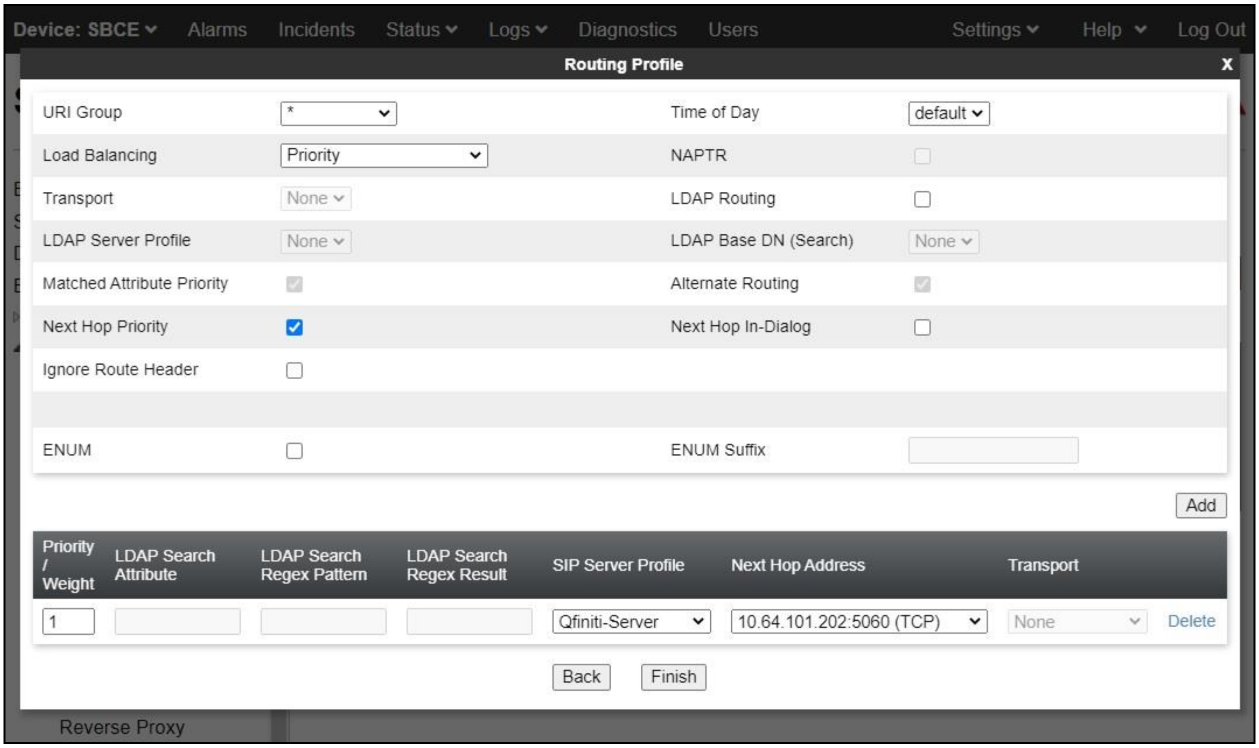
The **Routing Profile** pop-up screen is displayed. Enter a desired **Profile Name** as shown below.



Profile Name	Qfiniti-Route

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.



Routing Profile

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	

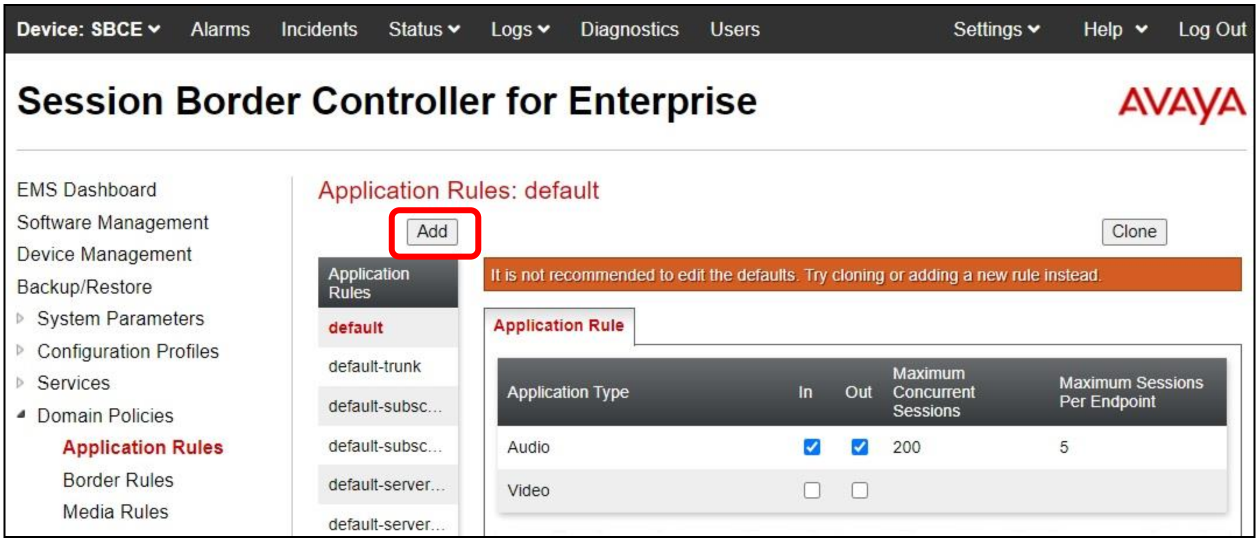
Add

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

Back Finish

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.

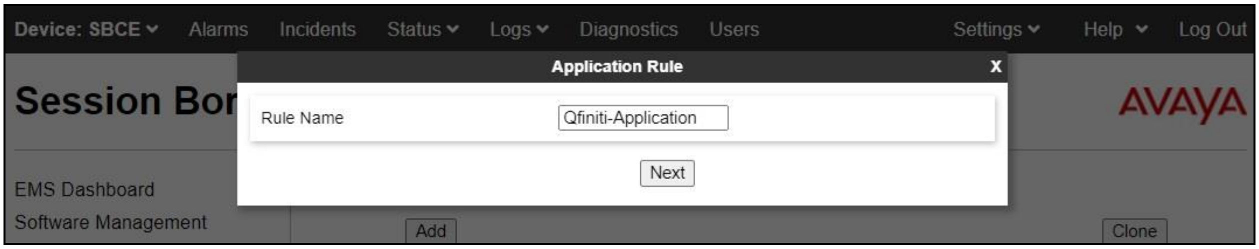


Application Rules: default

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

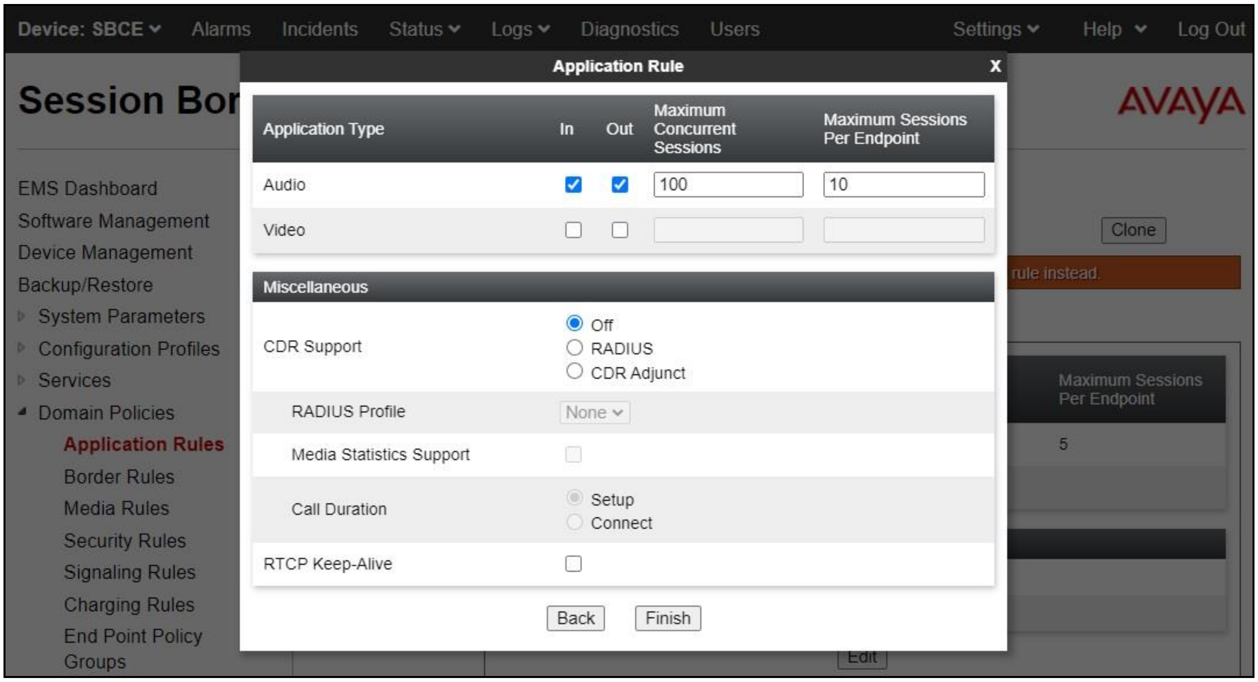
Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	☑	☑	200	5
Video	□	□		

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



Rule Name: Qfiniti-Application

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.



Application Rule

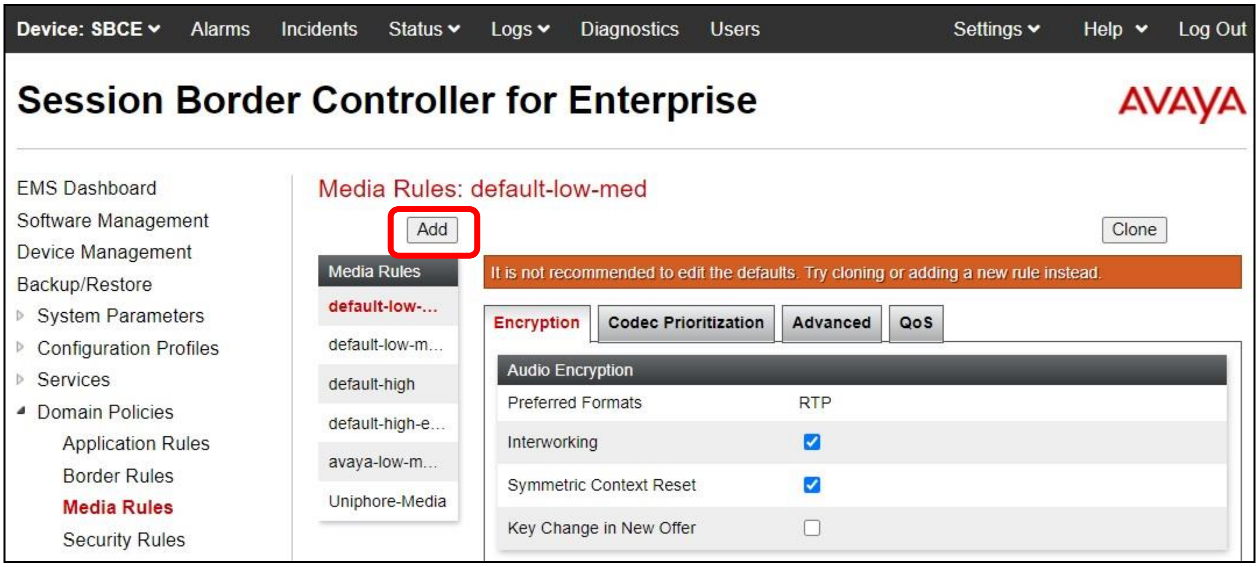
Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	☑	☑	100	10
Video	☐	☐		

Miscellaneous

CDR Support	● Off ○ RADIUS ○ CDR Adjunct
RADIUS Profile	None
Media Statistics Support	☐
Call Duration	○ Setup ○ Connect
RTCP Keep-Alive	☐

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.



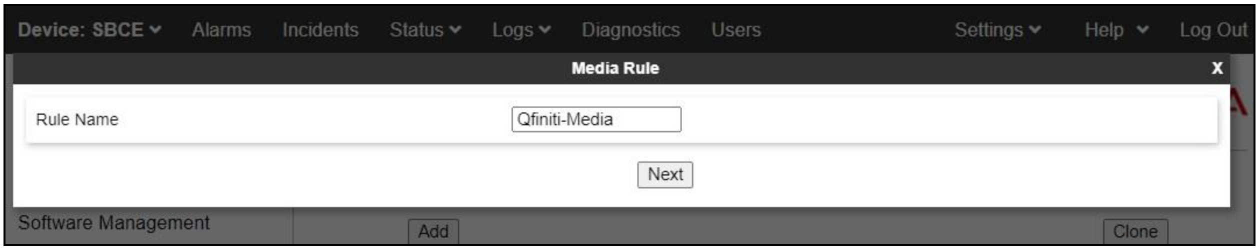
Media Rules: default-low-med

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

Audio Encryption

Preferred Formats	RTP
Interworking	☑
Symmetric Context Reset	☑
Key Change in New Offer	☐

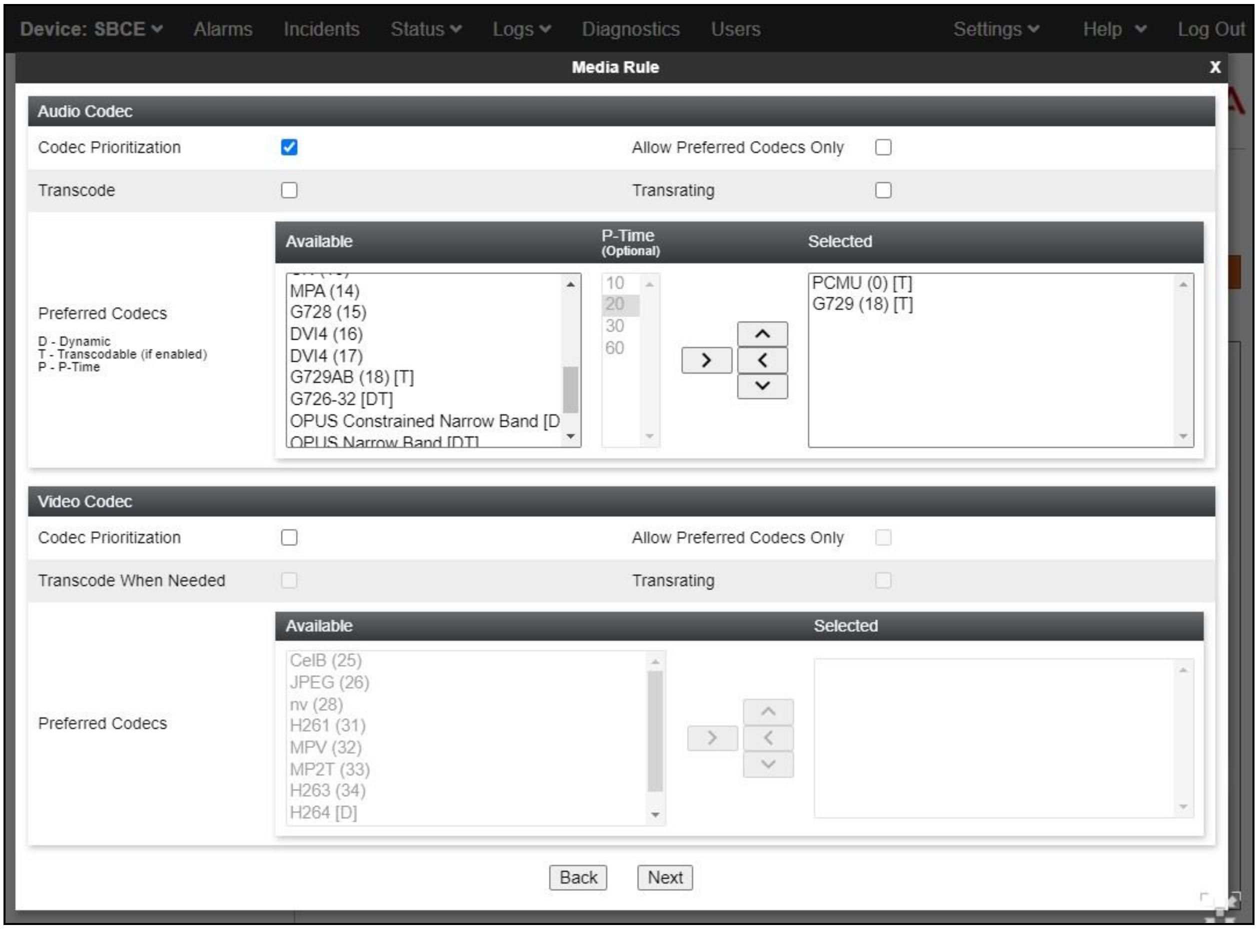
The **Media Rule** pop-up screen is displayed. Enter a desired **Rule Name** as shown below.



Media Rule

Rule Name: Qfiniti-Media

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.



Media Rule

Audio Codec

Codec Prioritization	☑	Allow Preferred Codecs Only	□
Transcode	□	Transrating	□

Preferred Codecs

D - Dynamic
T - Transcodable (if enabled)
P - P-Time

Available	P-Time (Optional)	Selected
MPA (14) G728 (15) DVI4 (16) DVI4 (17) G729AB (18) [T] G726-32 [DT] OPUS Constrained Narrow Band [D OPUS Narrow Band [DT]	10 20 30 60	PCMU (0) [T] G729 (18) [T]

Video Codec

Codec Prioritization	□	Allow Preferred Codecs Only	□
Transcode When Needed	□	Transrating	□

Preferred Codecs

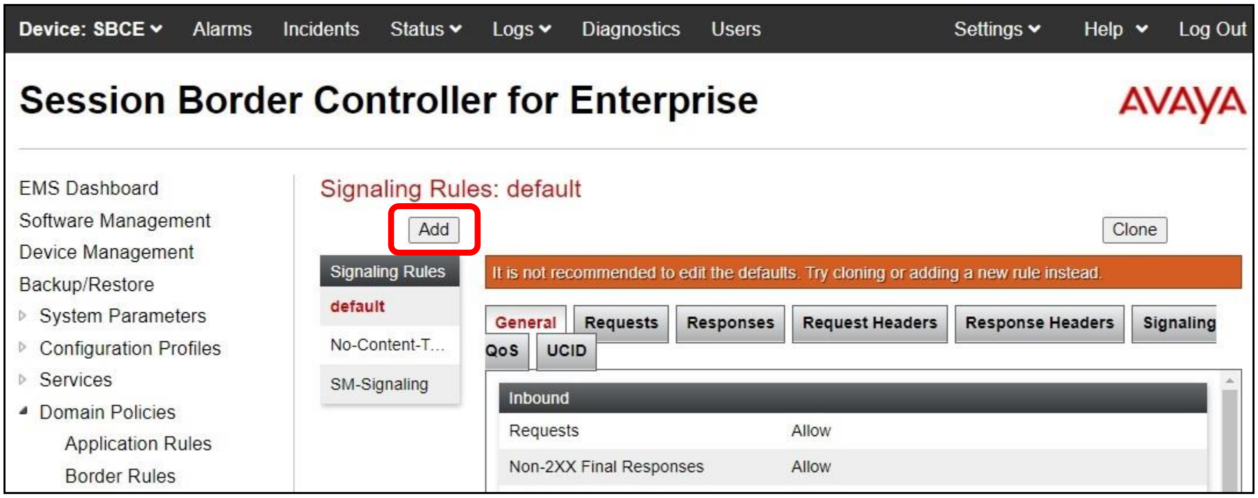
Available	Selected
CelB (25) JPEG (26) nv (28) H261 (31) MPV (32) MP2T (33) H263 (34) H264 [D]	

8.6. Administer Signaling Rules

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

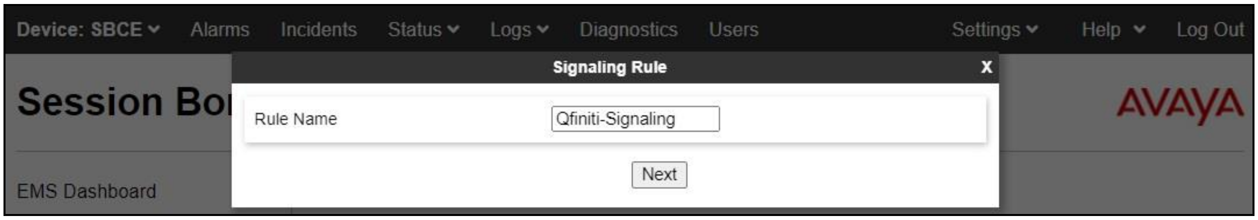
8.6.1. Qfiniti Signaling Rule

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



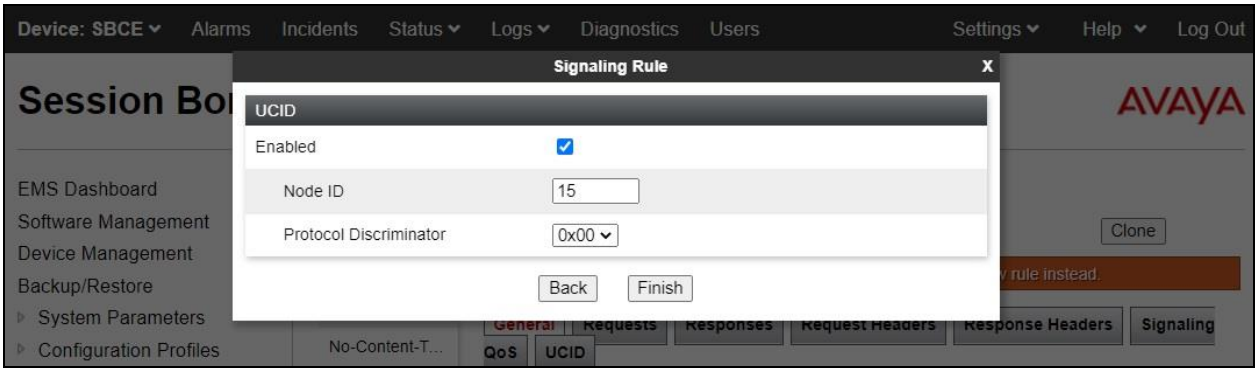
Inbound	
Requests	Allow
Non-2XX Final Responses	Allow

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



Rule Name: Qfiniti-Signaling

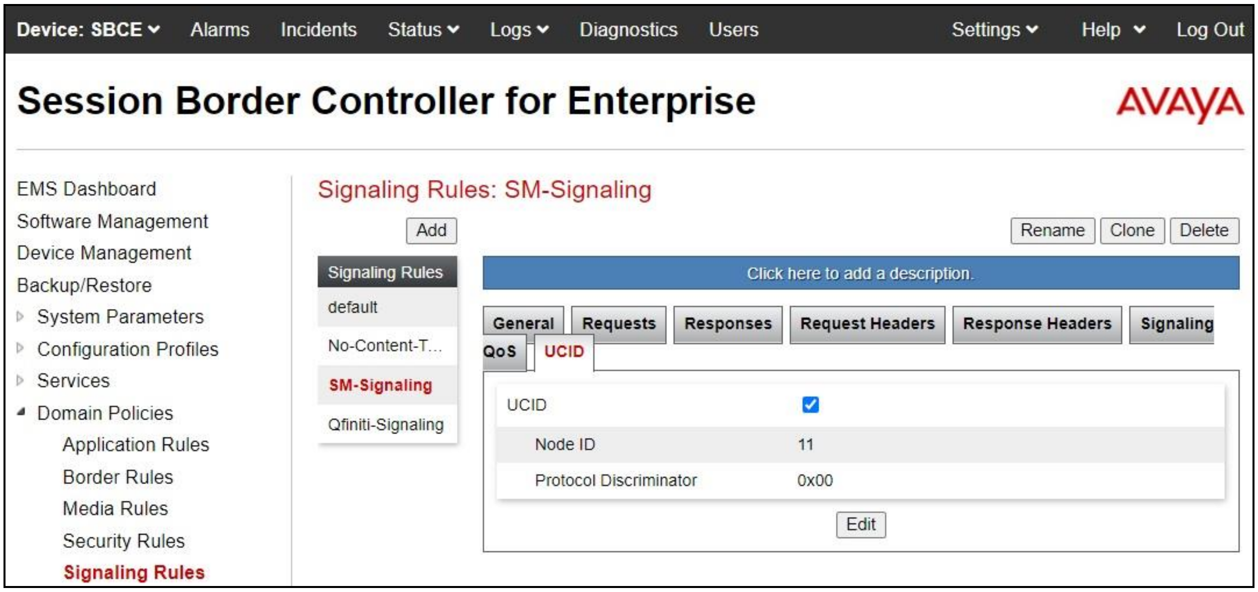
The **Signaling Rule** pop-up screen is updated. Navigate to the **UCID** page. Check **Enabled**. For **Node ID**, enter a unique number across the customer system, in this case “15”. Retain the default value in the remaining field.



UCID	
Enabled	☑
Node ID	15
Protocol Discriminator	0x00

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.

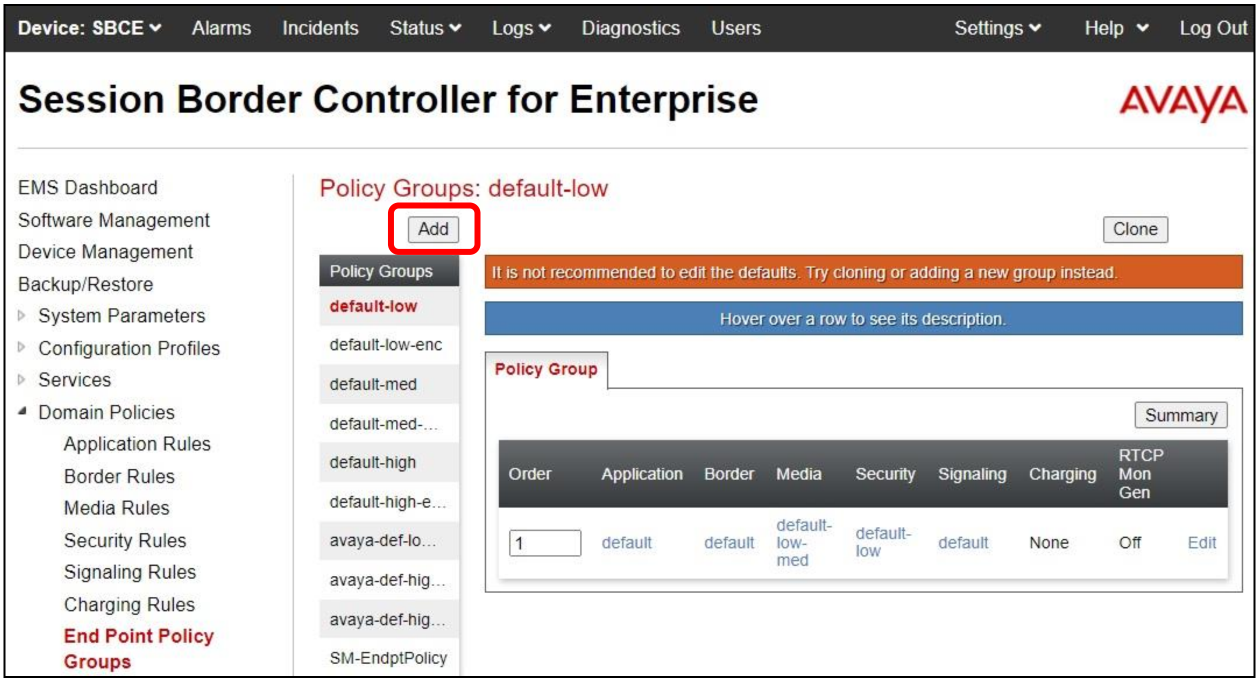


Signaling Rules: SM-Signaling

UCID	☑
Node ID	11
Protocol Discriminator	0x00

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.



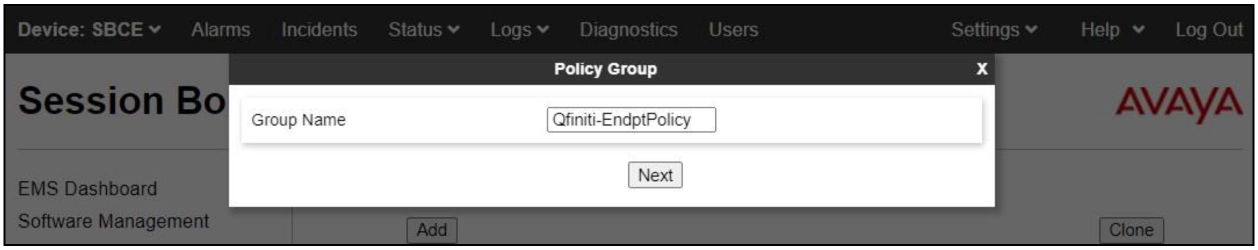
Policy Groups: default-low

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

Hover over a row to see its description.

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

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

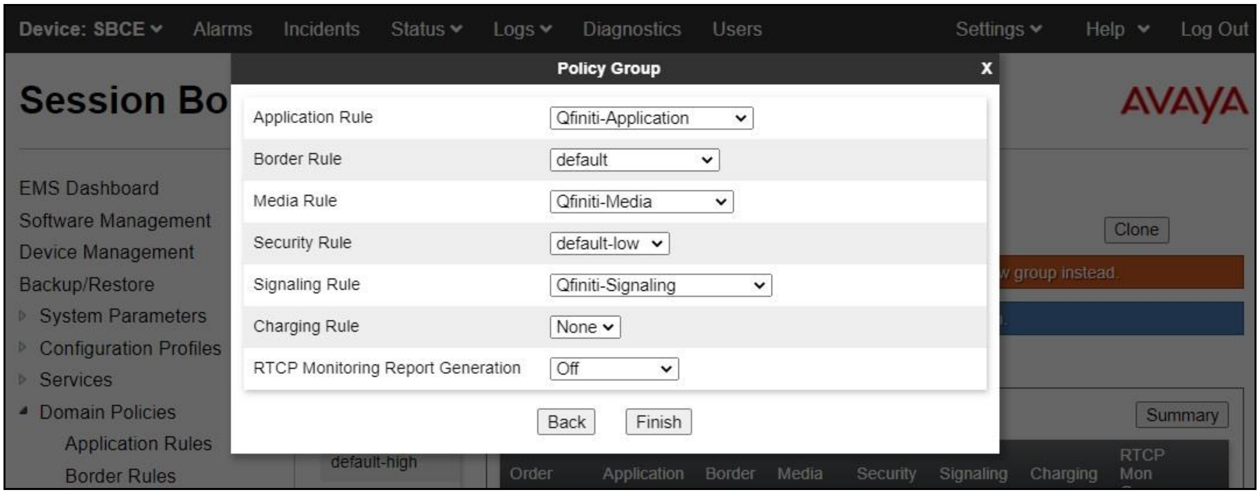


Policy Group

Group Name: Qfiniti-EndptPolicy

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**.

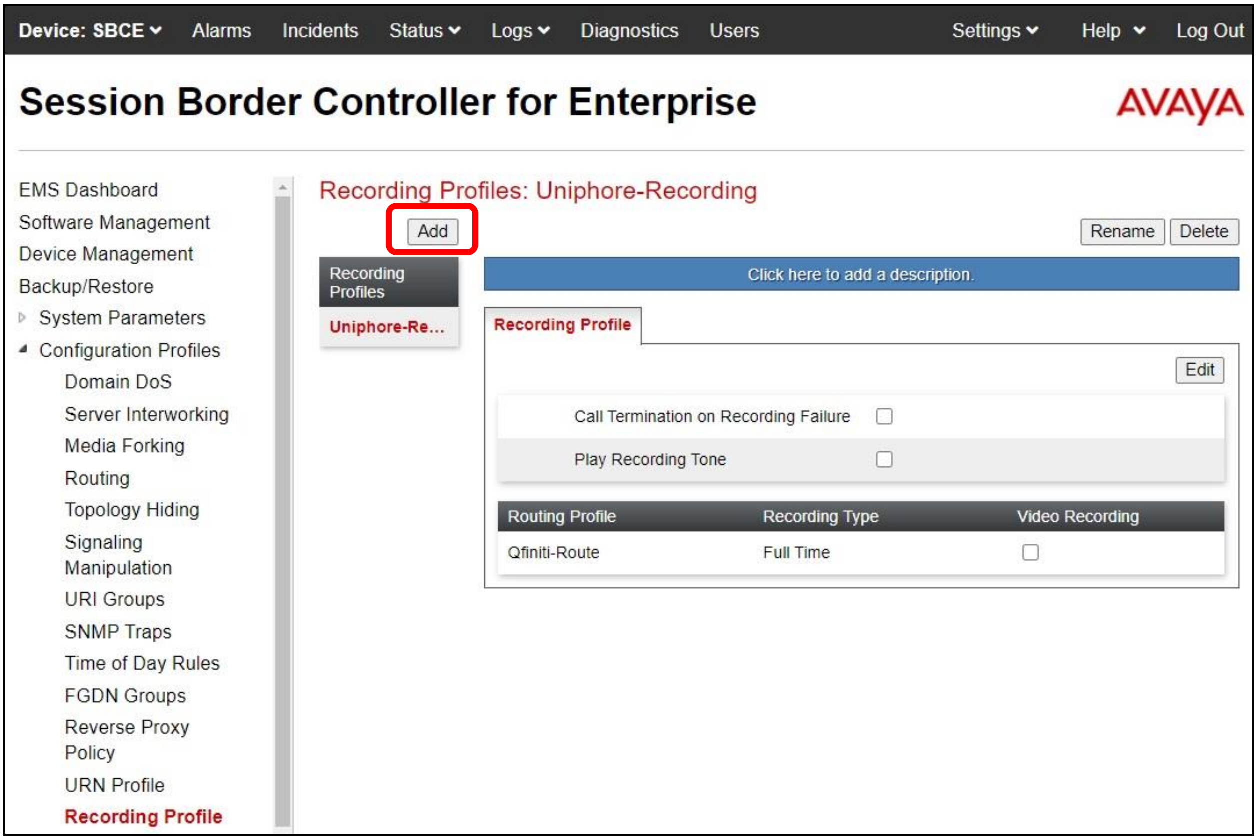


Policy Group

Application Rule	Qfiniti-Application
Border Rule	default
Media Rule	Qfiniti-Media
Security Rule	default-low
Signaling Rule	Qfiniti-Signaling
Charging Rule	None
RTCP Monitoring Report Generation	Off

8.8. Administer Recording Profile

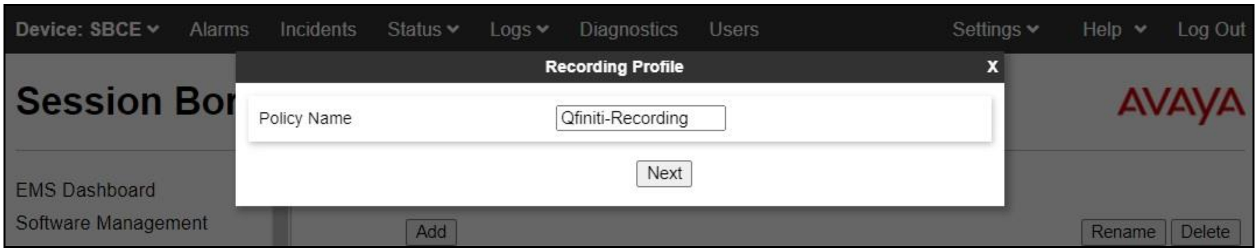
Select **Backup/Restore → Configuration Profiles → Recording Profile** from the left pane to display the existing profiles. Click **Add** to add a recording profile for Qfiniti.



Call Termination on Recording Failure	☐
Play Recording Tone	☐

Routing Profile	Recording Type	Video Recording
Qfiniti-Route	Full Time	☐

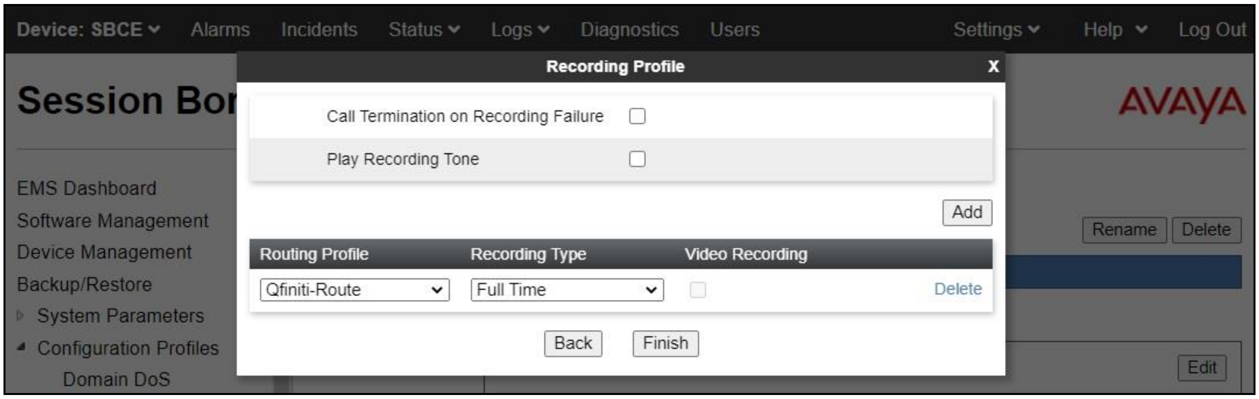
The **Recording Profile** pop-up screen is displayed. Enter a desired **Policy Name** as shown below.



Policy Name: Qfiniti-Recording

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"



Recording Profile

Call Termination on Recording Failure	☐
Play Recording Tone	☐

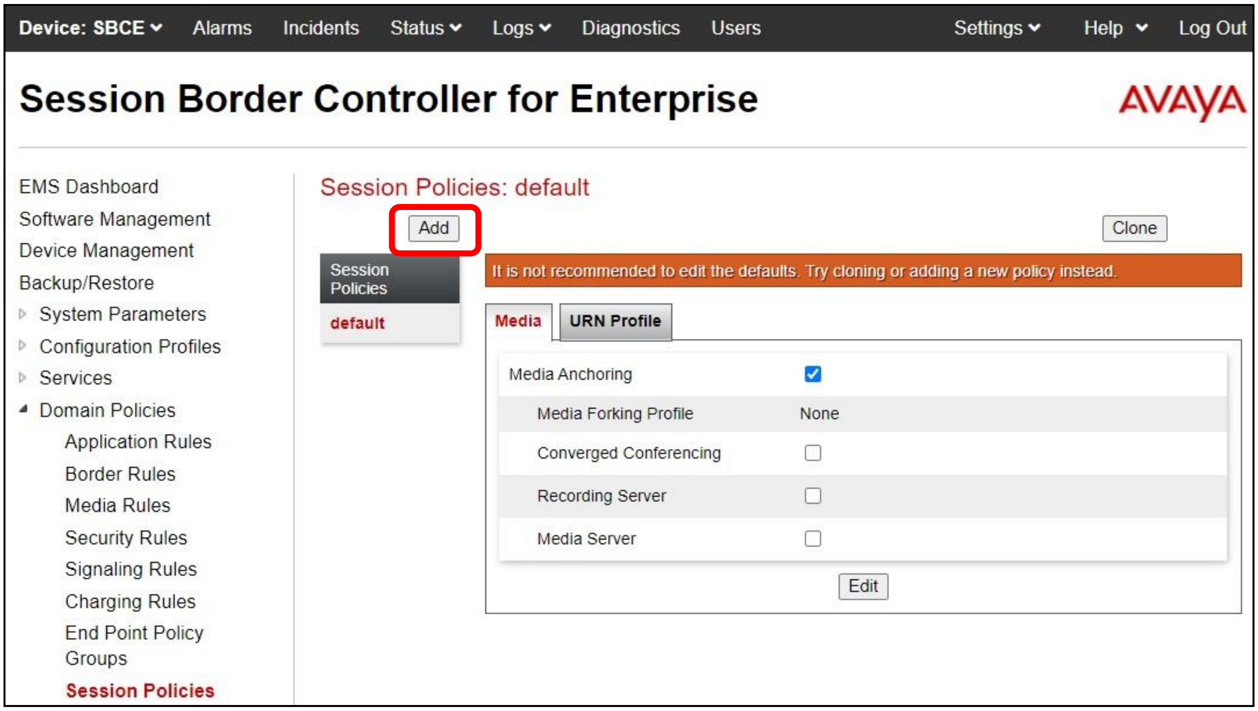
Add

Routing Profile	Recording Type	Video Recording	
Qfiniti-Route	Full Time	☐	Delete

Back Finish

8.9. Administer Session Policies

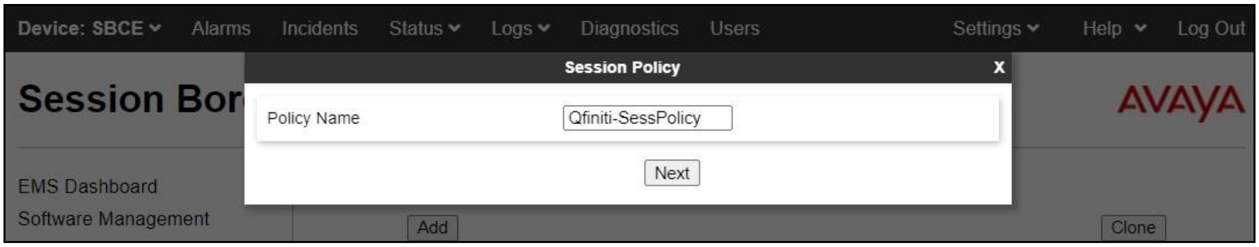
Select **Backup/Restore → Domain Policies → Session Policies** from the left pane to display the existing session policies. Click **Add** to add a session policy for Qfiniti.



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

Media Anchoring	☑
Media Forking Profile	None
Converged Conferencing	☐
Recording Server	☐
Media Server	☐

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

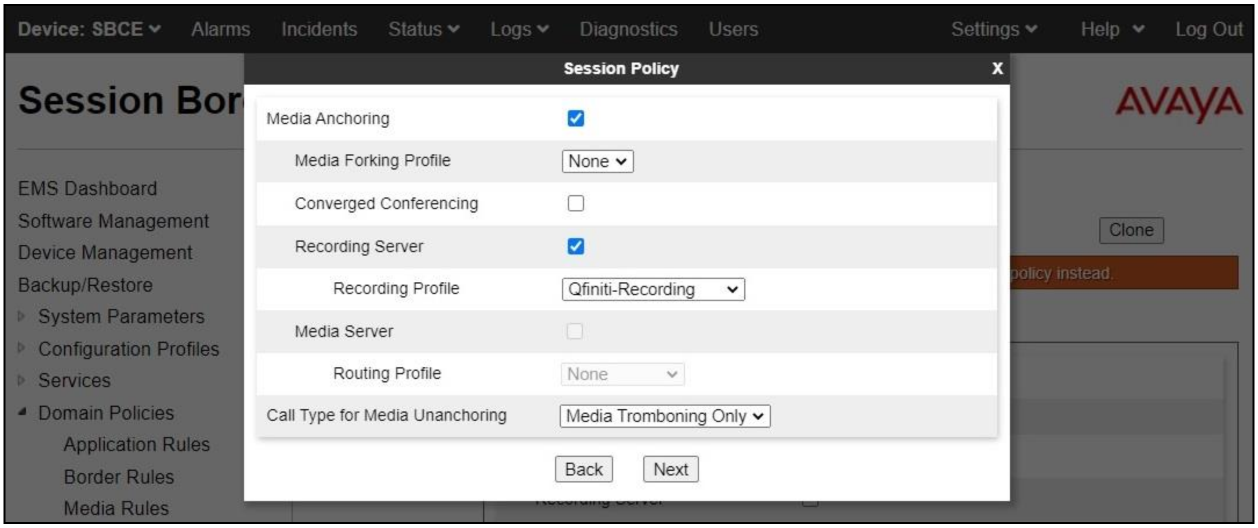


Session Policy

Policy Name: Qfiniti-SessPolicy

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**.

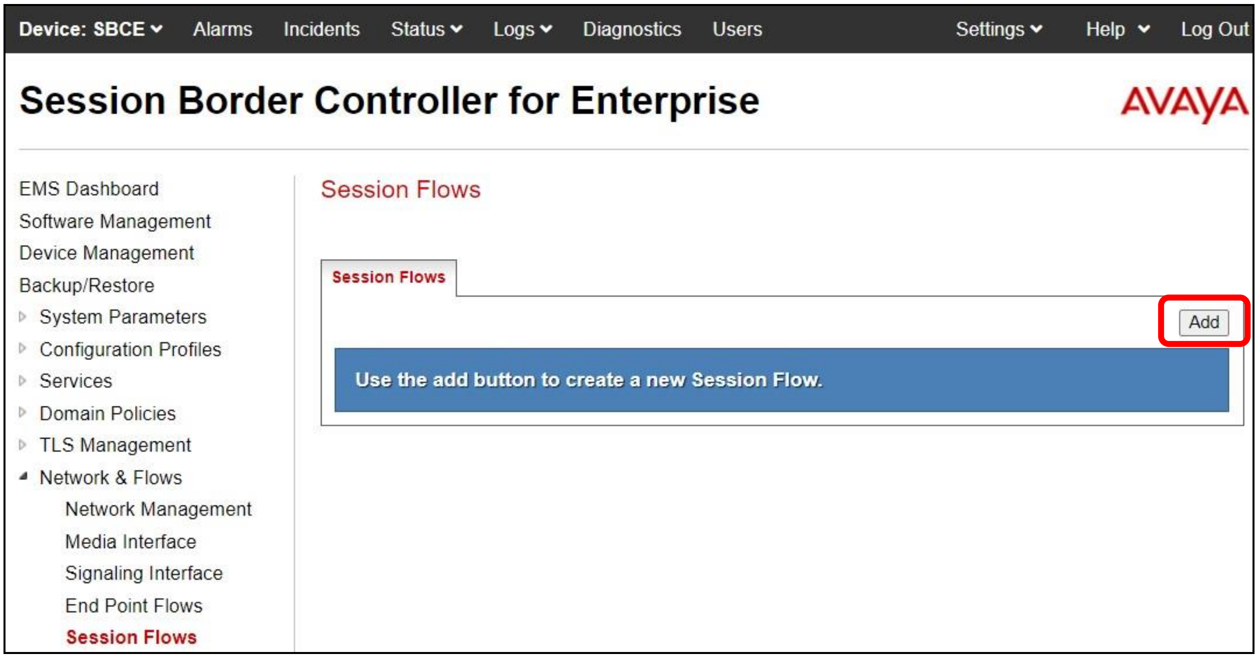


Session Policy

Media Anchoring	☑
Media Forking Profile	None
Converged Conferencing	□
Recording Server	☑
Recording Profile	Qfiniti-Recording
Media Server	□
Routing Profile	None
Call Type for Media Unanchoring	Media Tromboning Only

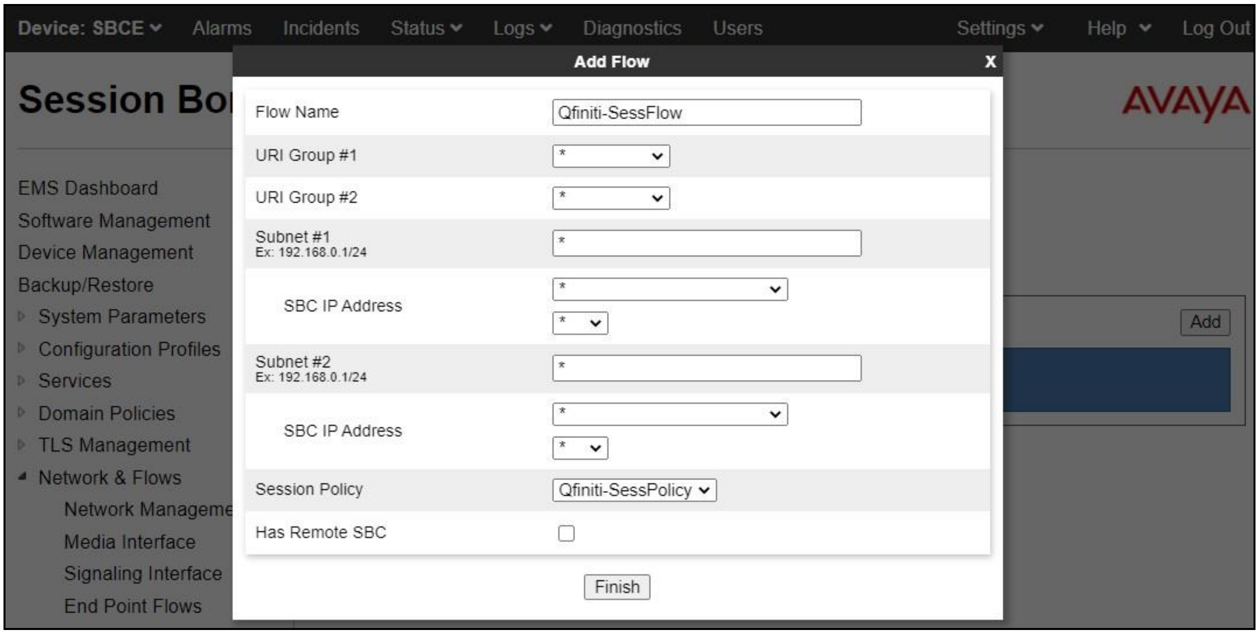
8.10. Administer Session Flows

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.



Use the add button to create a new Session Flow.

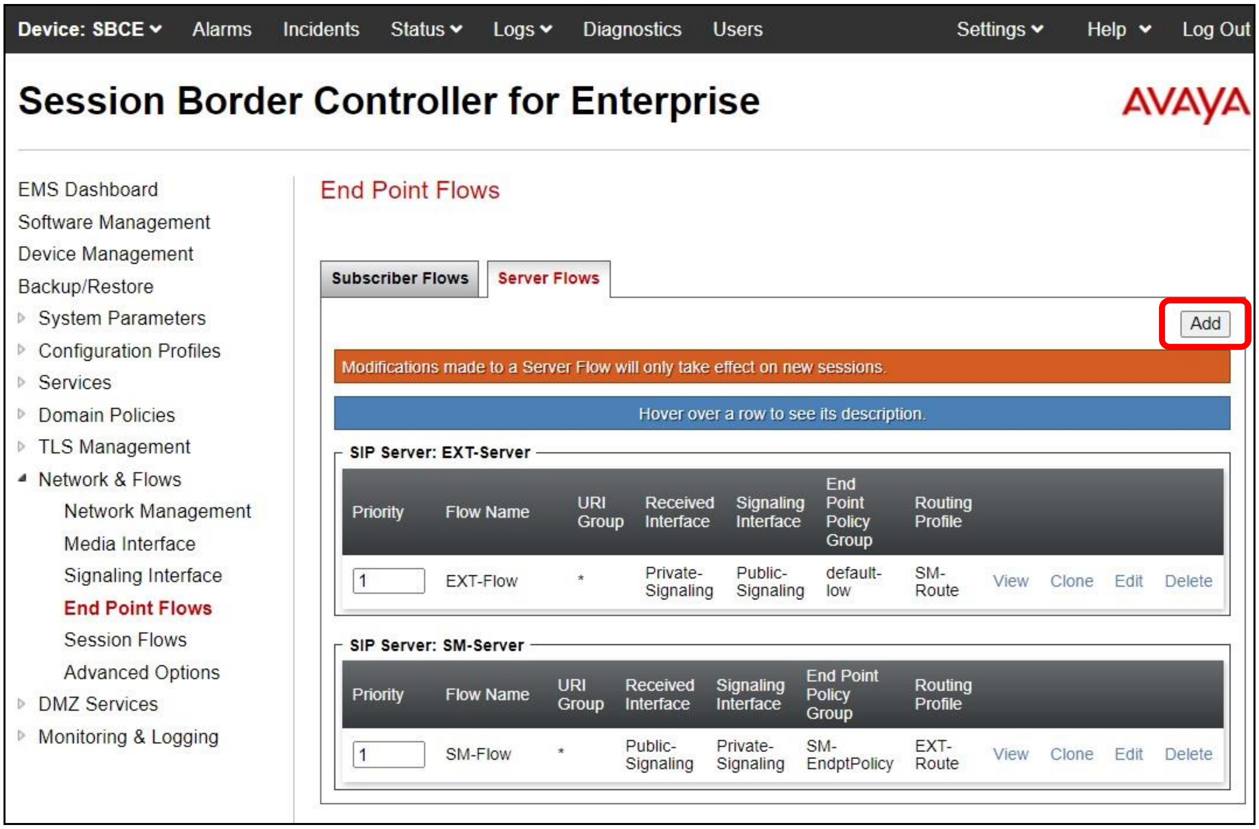
The **Add Flow** pop-up screen is displayed. For **Flow Name**, enter a desired name. For **Session Policy**, select the Qfiniti session policy from **Section 8.9**. Retain the default values in the remaining fields.



Flow Name	Qfiniti-SessFlow
URI Group #1	*
URI Group #2	*
Subnet #1 Ex: 192.168.0.1/24	*
SBC IP Address	* *
Subnet #2 Ex: 192.168.0.1/24	*
SBC IP Address	* *
Session Policy	Qfiniti-SessPolicy
Has Remote SBC	□

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.



Modifications made to a Server Flow will only take effect on new sessions.

Hover over a row to see its description.

SIP Server: EXT-Server

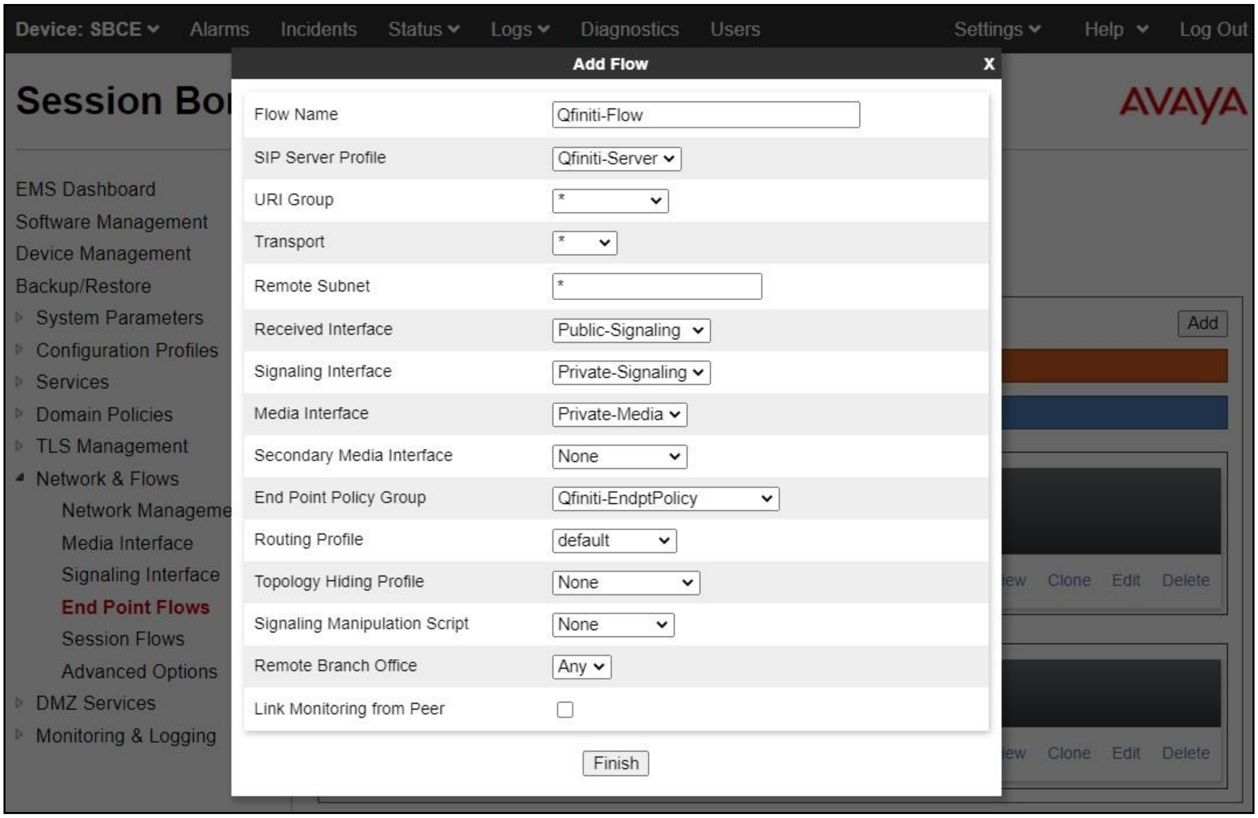
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	EXT-Flow	*	Private-Signaling	Public-Signaling	default-low	SM-Route	View	Clone	Edit	Delete

SIP Server: SM-Server

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**.



Add Flow

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	□

9. Configure OpenText Qfiniti

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

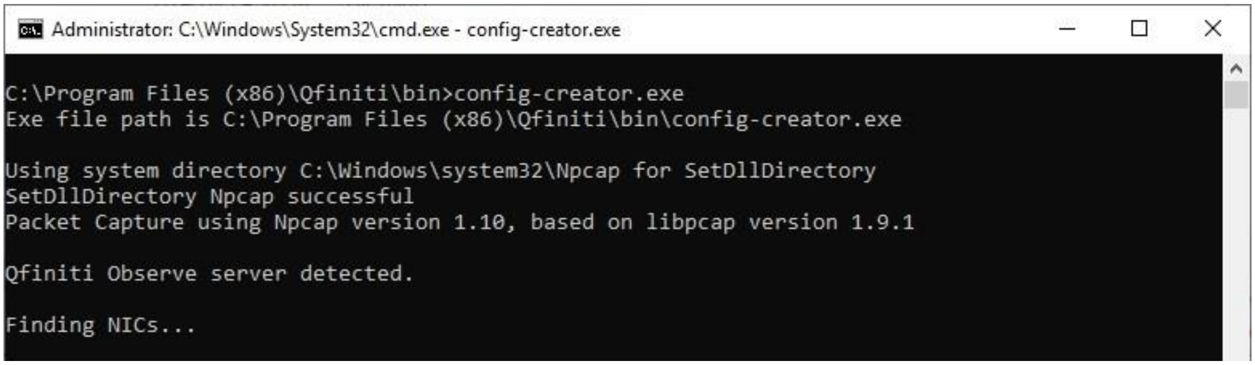
- Obtain network card data
- Launch SysConfig web interface
- Administer switches
- Administer CTI server
- Administer board configuration
- Administer general
- Administer machines
- Administer components
- Administer CTI sources
- Administer phone interface
- Administer logging data – phone class of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

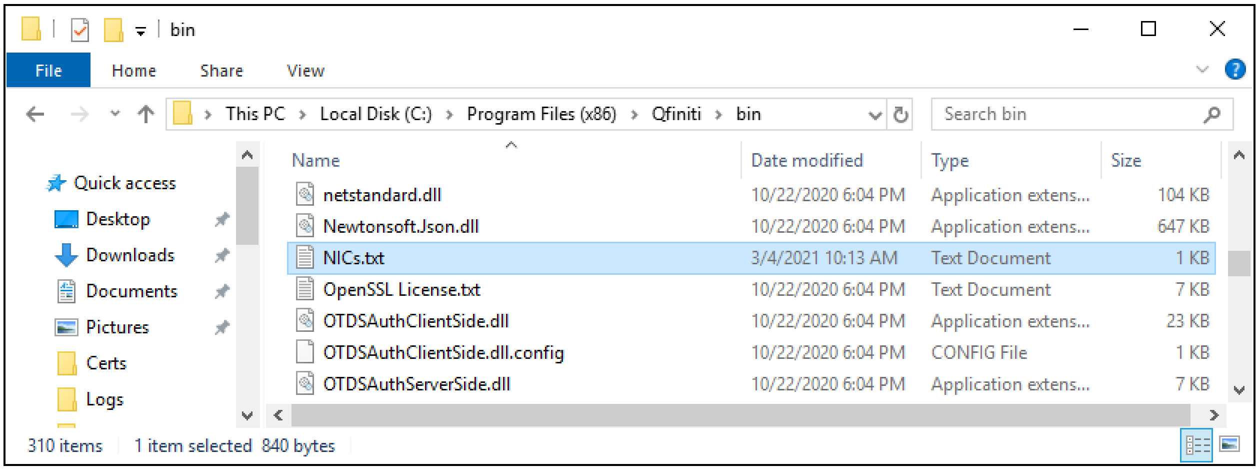
Run the command **config-creator.exe** as shown below, which will create the **NICs.txt** file.



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

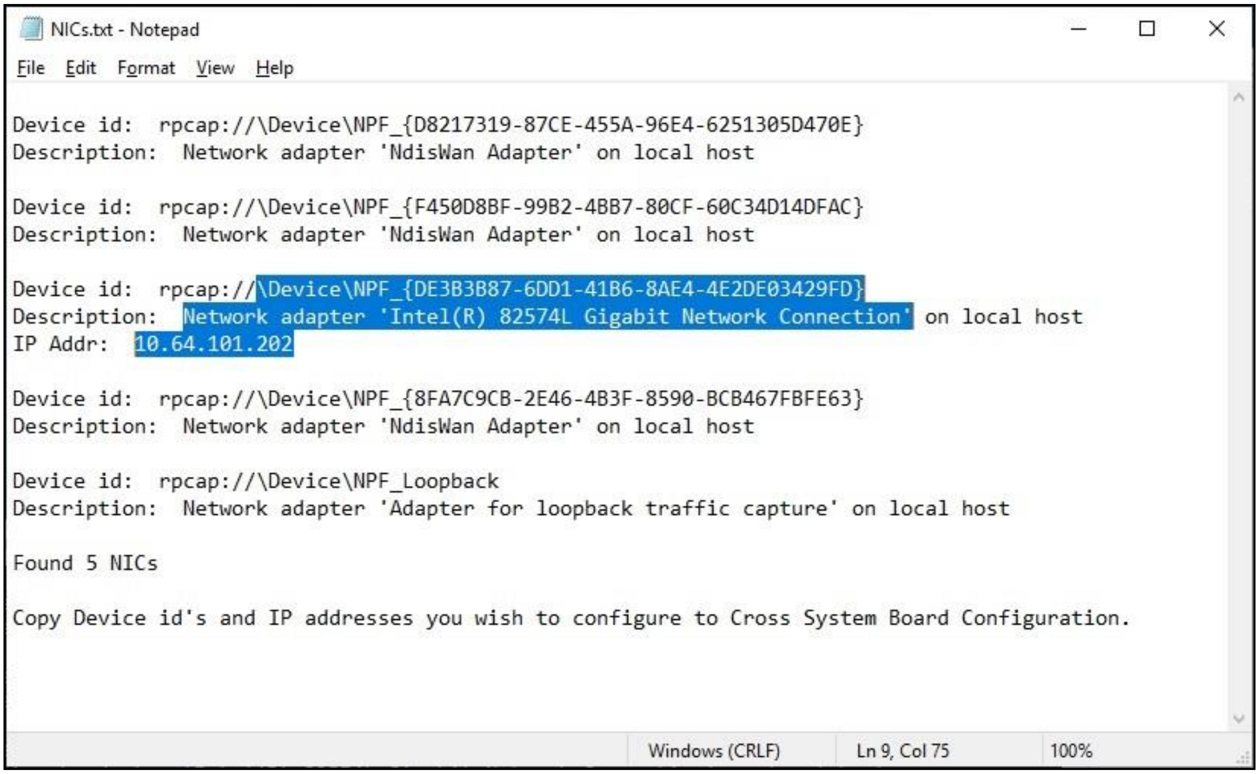
```
C:\Program Files (x86)\Qfiniti\bin>config-creator.exe
Exe file path is C:\Program Files (x86)\Qfiniti\bin\config-creator.exe

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.



Name	Date modified	Type	Size
netstandard.dll	10/22/2020 6:04 PM	Application extens...	104 KB
Newtonsoft.Json.dll	10/22/2020 6:04 PM	Application extens...	647 KB
NICs.txt	3/4/2021 10:13 AM	Text Document	1 KB
OpenSSL License.txt	10/22/2020 6:04 PM	Text Document	7 KB
OTDSAuthClientSide.dll	10/22/2020 6:04 PM	Application extens...	23 KB
OTDSAuthClientSide.dll.config	10/22/2020 6:04 PM	CONFIG File	1 KB
OTDSAuthServerSide.dll	10/22/2020 6:04 PM	Application extens...	7 KB

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.

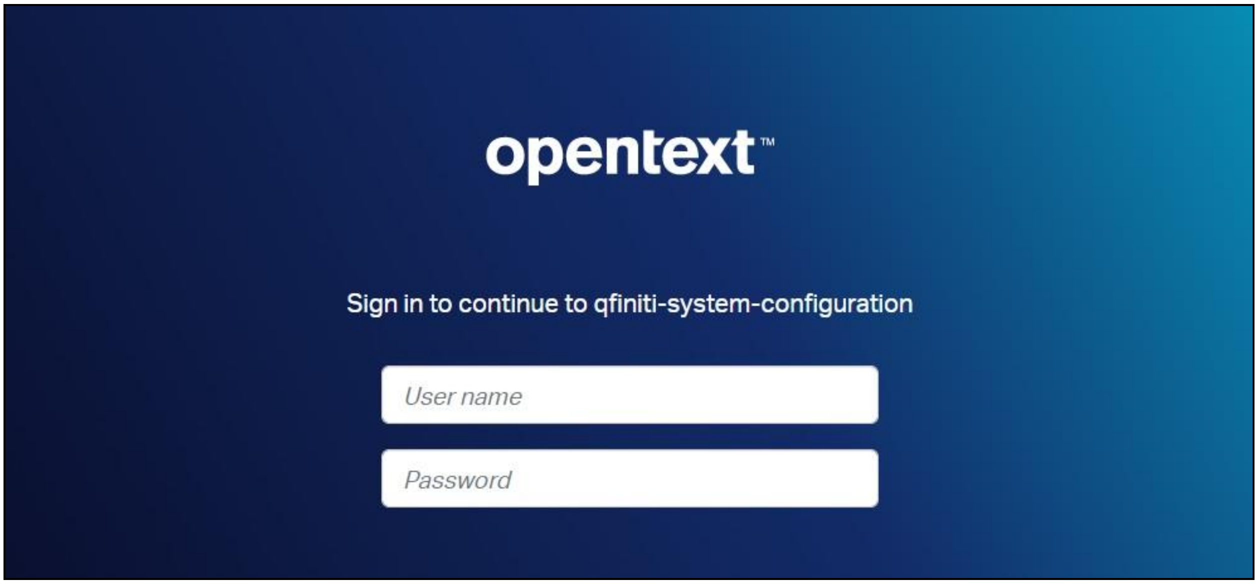


```
Device id:  rpcap://\Device\NPF_{D8217319-87CE-455A-96E4-6251305D470E}
Description:  Network adapter 'NdisWan Adapter' on local host

Device id:  rpcap://\Device\NPF_{F450D8BF-99B2-4BB7-80CF-60C34D14DFAC}
Description:  Network adapter 'NdisWan Adapter' on local host

Device id:  rpcap://\Device\NPF_{DE3B3B87-6DD1-41B6-8AE4-4E2DE03429FD}
Description:  Network adapter 'Intel(R) 82574L Gigabit Network Connection' on local host
IP Addr:  10.64.101.202

Device id:  rpcap://\Device\NPF_{8FA7C9CB-2E46-4B3F-8590-BCB467FBFE63}
Description:  Network adapter 'NdisWan Adapter' on local host

Device id:  rpcap://\Device\NPF_Loopback
Description:  Network adapter 'Adapter for loopback traffic capture' on local host

Found 5 NICs

Copy Device id's and IP addresses you wish to configure to Cross System Board Configuration.
```

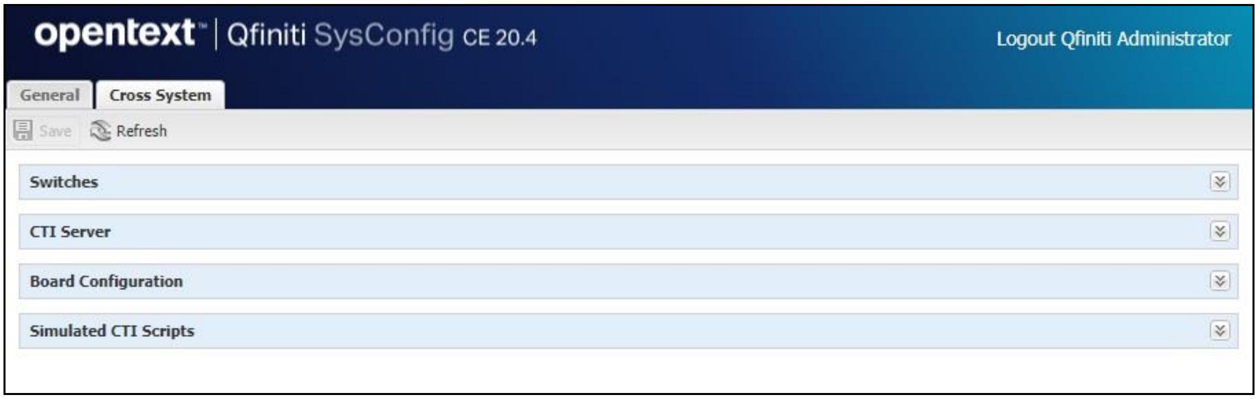
9.2. Launch SysConfig Web Interface

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.



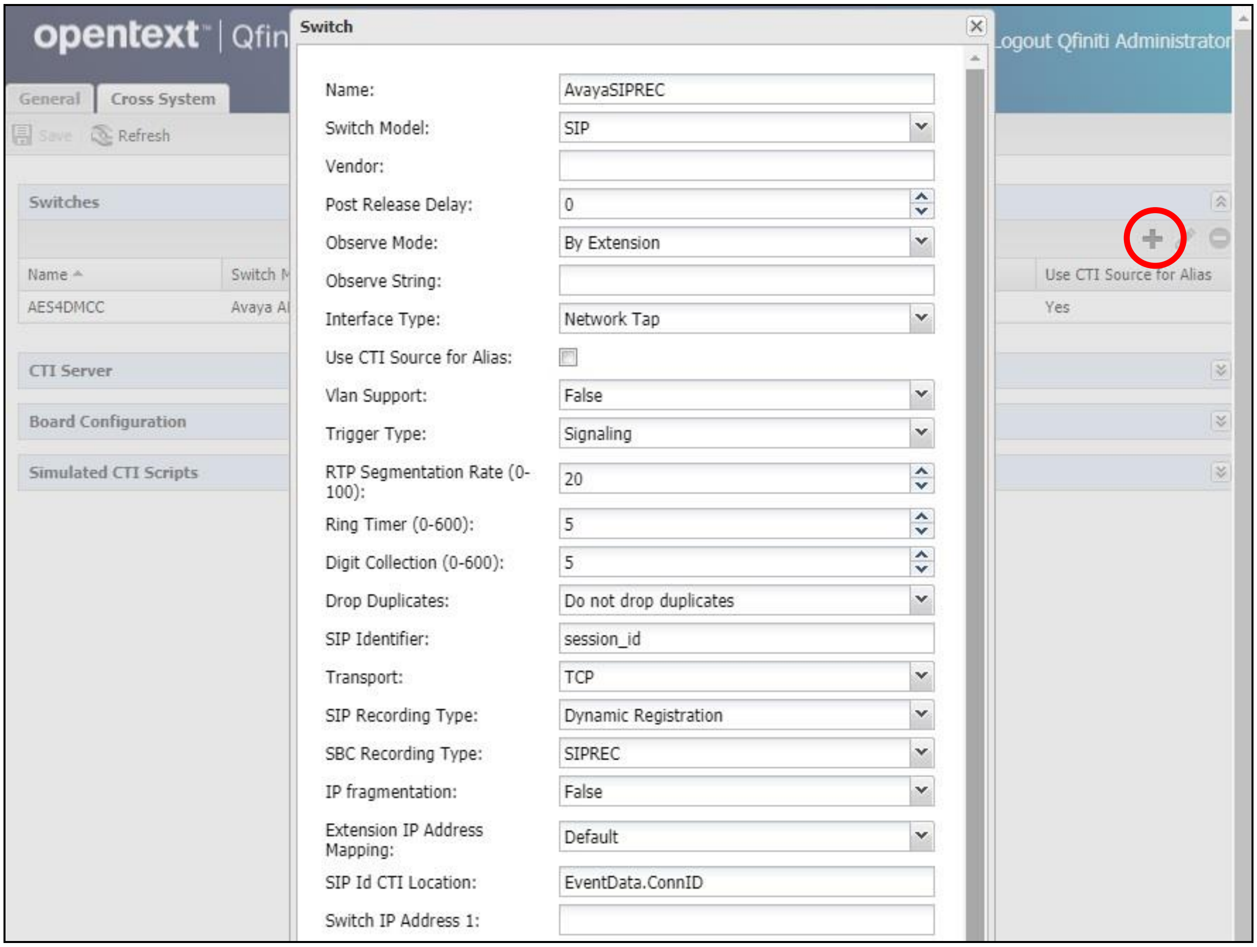
In the subsequent screen, select the **Cross System** tab to display the screen below.



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"



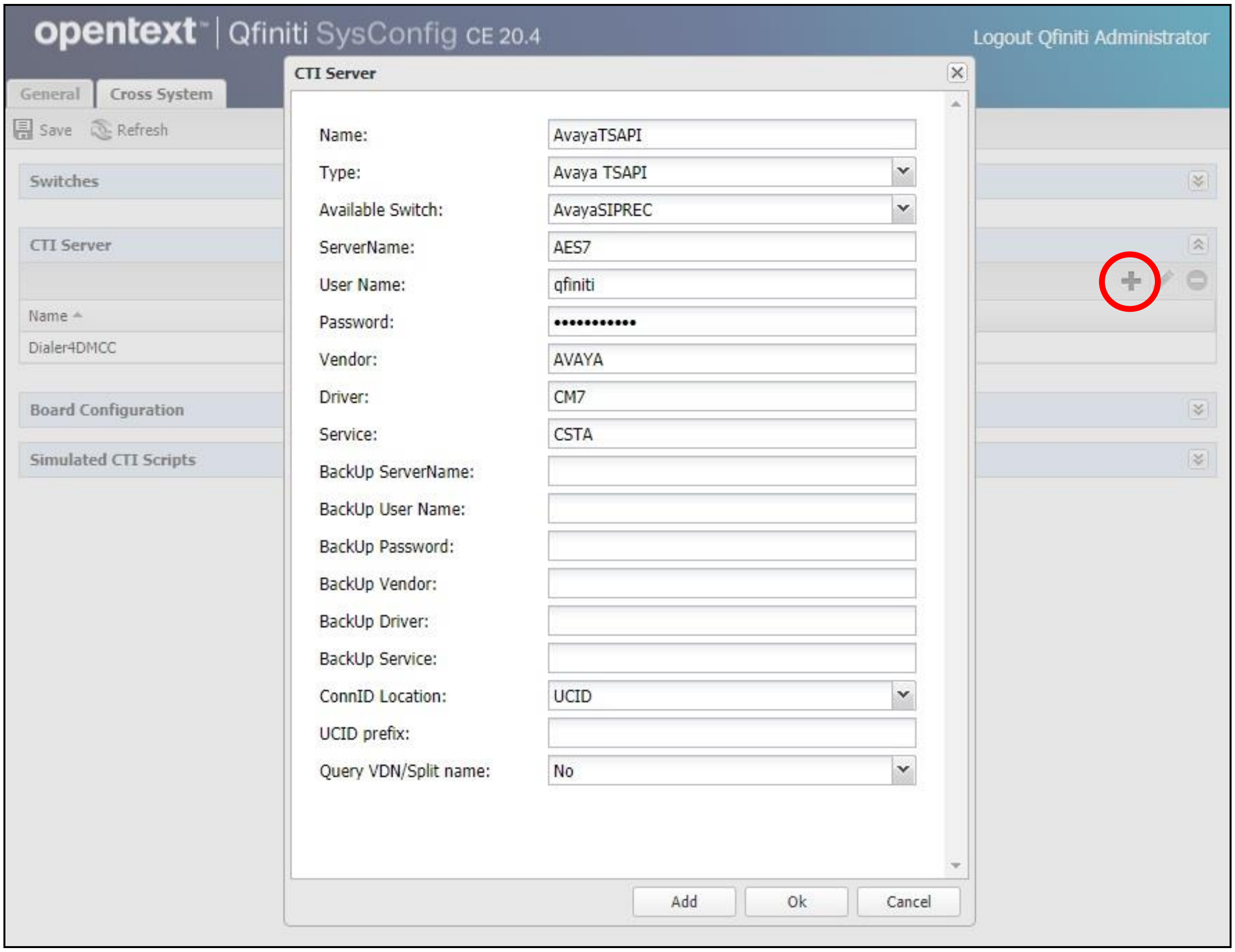
Switch

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: □
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"

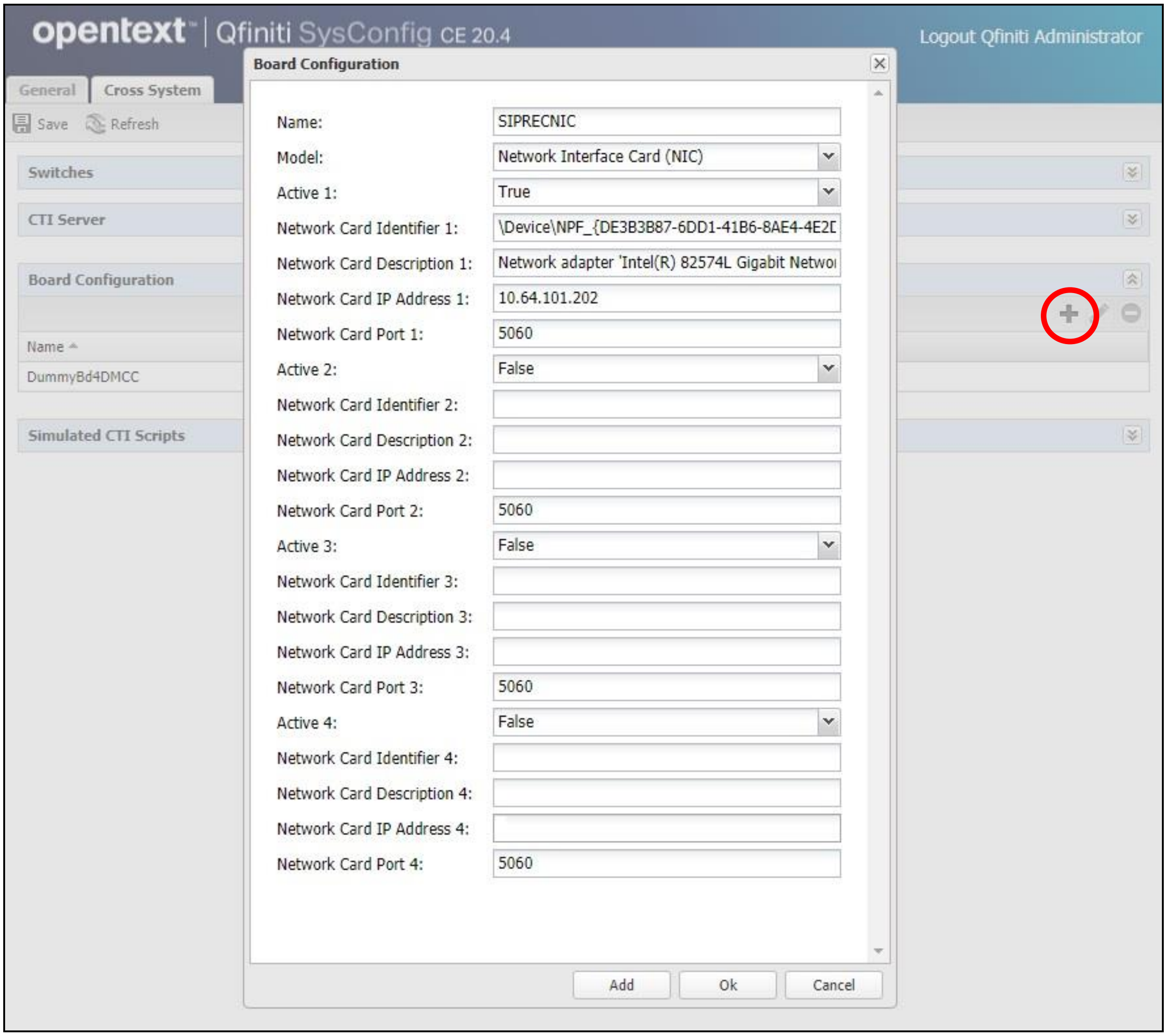


Name: AvayaTSAPI
Type: Avaya TSAPI
Available Switch: AvayaSIPREC
ServerName: AES7
User Name: qfiniti
Password: ••••••••••••
Vendor: AVAYA
Driver: CM7
Service: CSTA
BackUp ServerName:
BackUp User Name:
BackUp Password:
BackUp Vendor:
BackUp Driver:
BackUp Service:
ConnID Location: UCID
UCID prefix:
Query VDN/Split name: No

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 Identifer 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**.



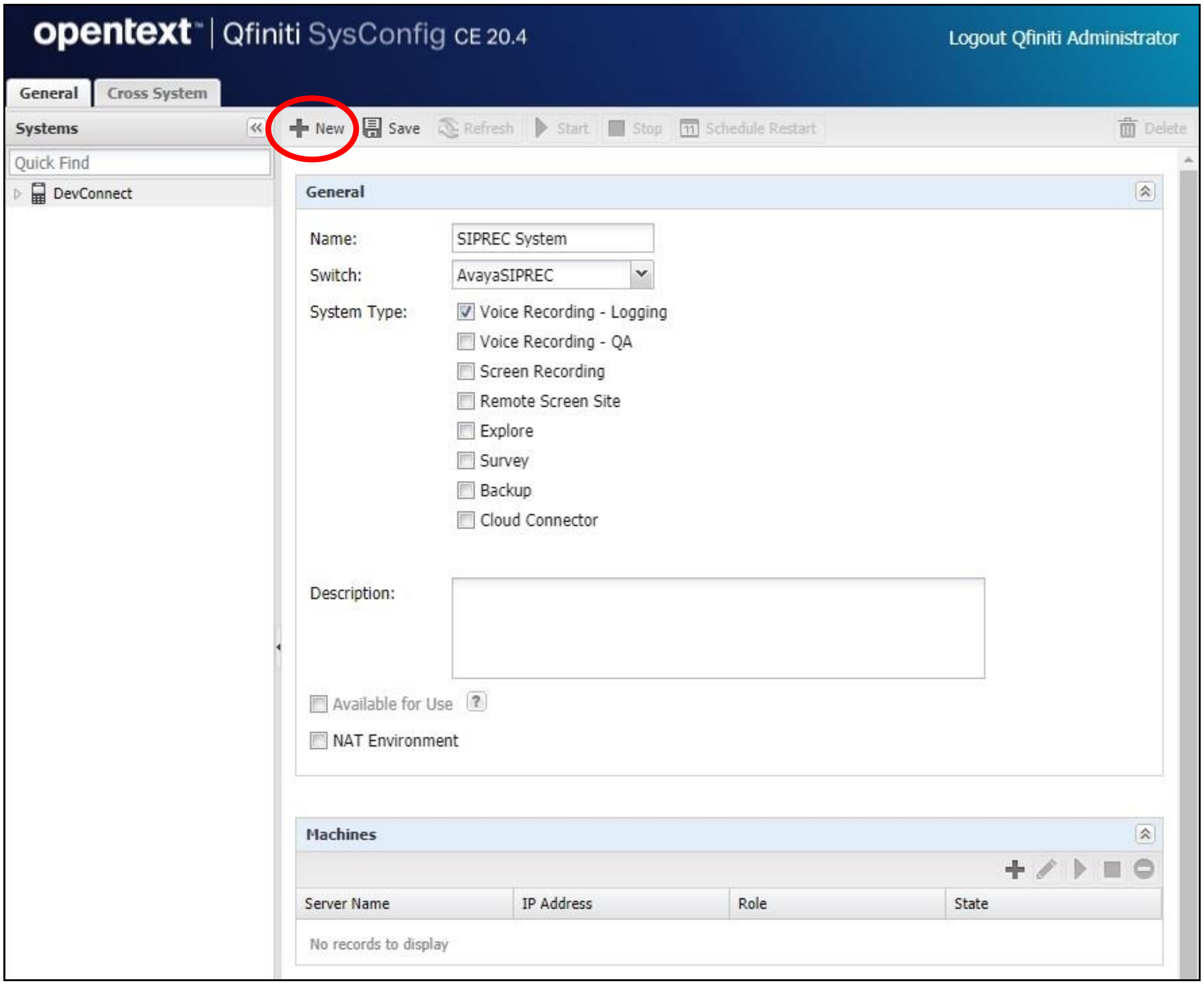
Board Configuration

Name:	SIPRECNIC
Model:	Network Interface Card (NIC)
Active 1:	True
Network Card Identifier 1:	\Device\NPF_{DE3B3B87-6DD1-41B6-8AE4-4E2D
Network Card Description 1:	Network adapter 'Intel(R) 82574L Gigabit Netwo
Network Card IP Address 1:	10.64.101.202
Network Card Port 1:	5060
Active 2:	False
Network Card Identifier 2:	
Network Card Description 2:	
Network Card IP Address 2:	
Network Card Port 2:	5060
Active 3:	False
Network Card Identifier 3:	
Network Card Description 3:	
Network Card IP Address 3:	
Network Card Port 3:	5060
Active 4:	False
Network Card Identifier 4:	
Network Card Description 4:	
Network Card IP Address 4:	
Network Card Port 4:	5060

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**.



General

Name: SIPREC System

Switch: AvayaSIPREC

System Type:
☑ Voice Recording - Logging
☐ Voice Recording - QA
☐ Screen Recording
☐ Remote Screen Site
☐ Explore
☐ Survey
☐ Backup
☐ Cloud Connector

Description:

☐ Available for Use ?

☐ NAT Environment

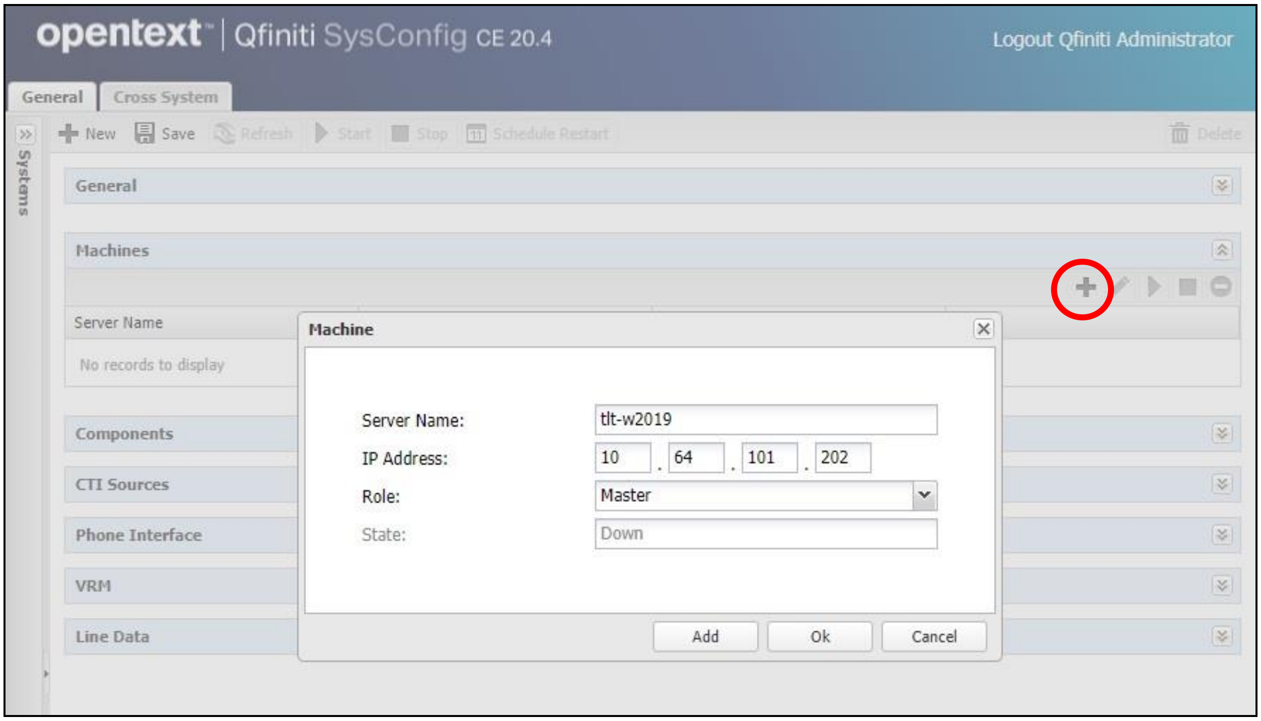
Machines

Server Name	IP Address	Role	State
No records to display			

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".



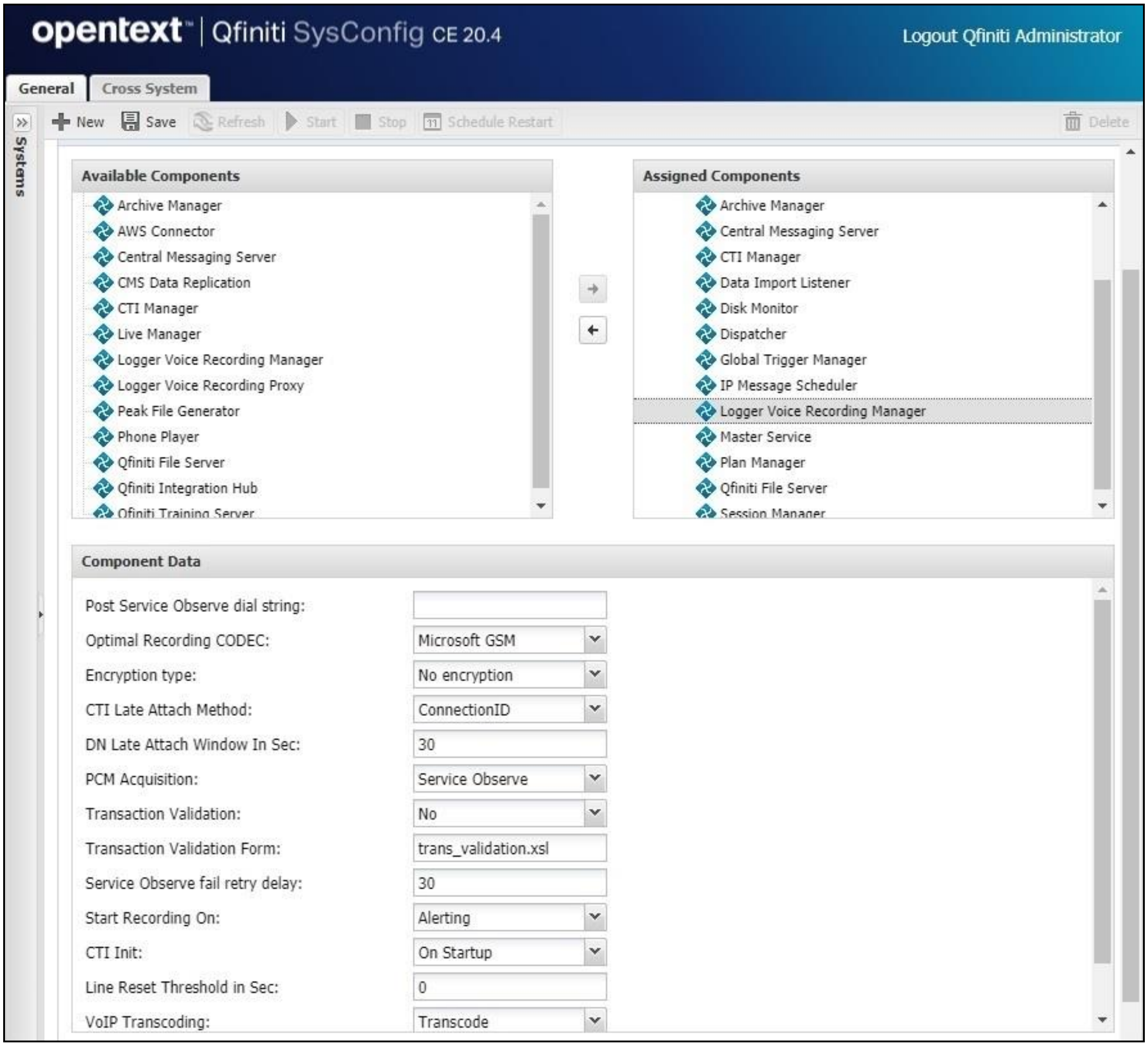
Server Name: tlt-w2019
IP Address: 10 . 64 . 101 . 202
Role: Master
State: Down

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).



Available Components
- Archive Manager
- AWS Connector
- Central Messaging Server
- CMS Data Replication
- CTI Manager
- Live Manager
- Logger Voice Recording Manager
- Logger Voice Recording Proxy
- Peak File Generator
- Phone Player
- Qfiniti File Server
- Qfiniti Integration Hub
- Qfiniti Training Server

Assigned Components
- Archive Manager
- Central Messaging Server
- CTI Manager
- Data Import Listener
- Disk Monitor
- Dispatcher
- Global Trigger Manager
- IP Message Scheduler
- Logger Voice Recording Manager
- Master Service
- Plan Manager
- Qfiniti File Server
- Session Manager

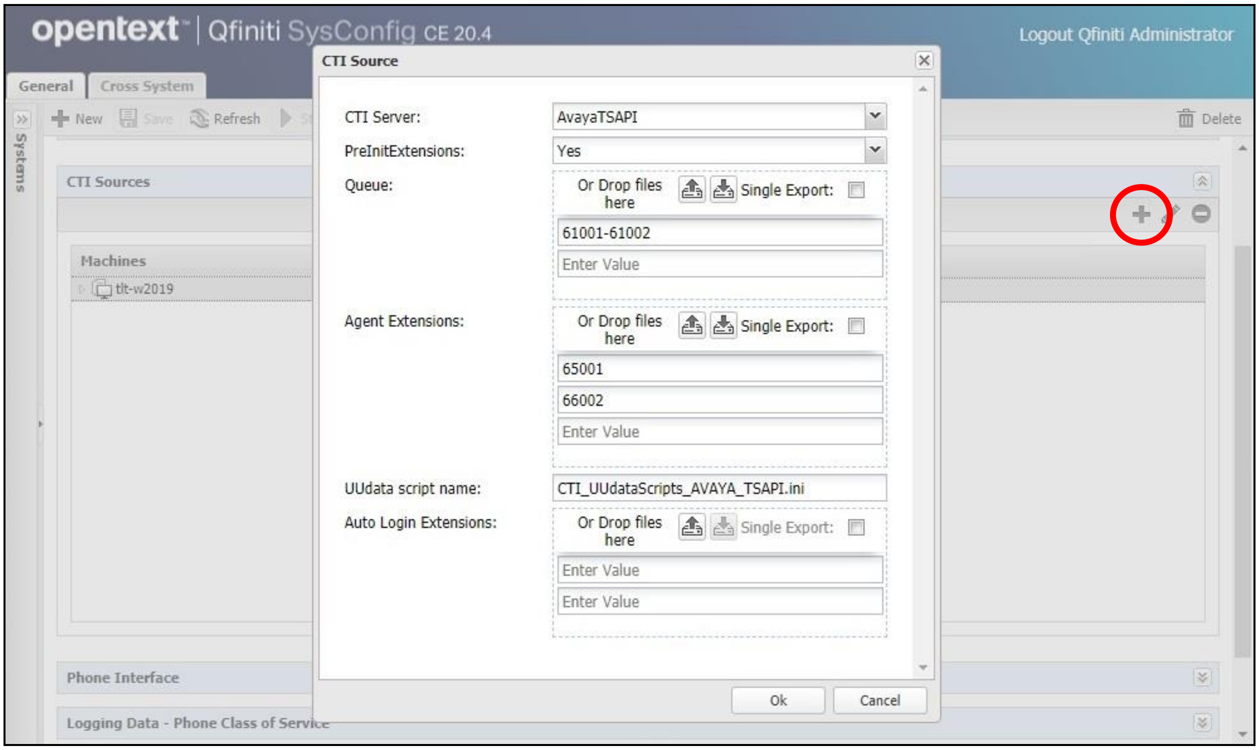
Component Data

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.xsl
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**.



CTI Server: AvayaTSAPI

PreInitExtensions: Yes

Queue: 61001-61002

Agent Extensions: 65001, 66002

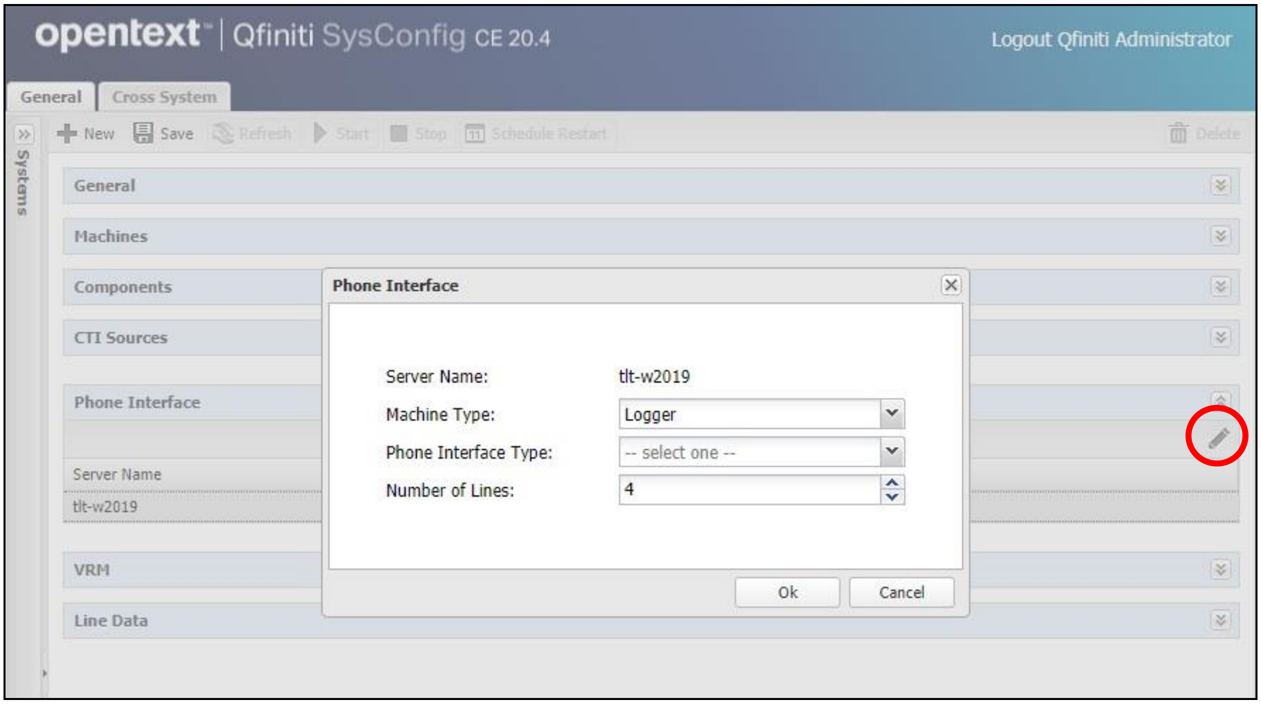
UUdata script name: CTI_UUdataScripts_AVAYA_TSAPI.ini

Auto Login Extensions: Enter Value

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**.



Phone Interface

Server Name: tlt-w2019

Machine Type: Logger

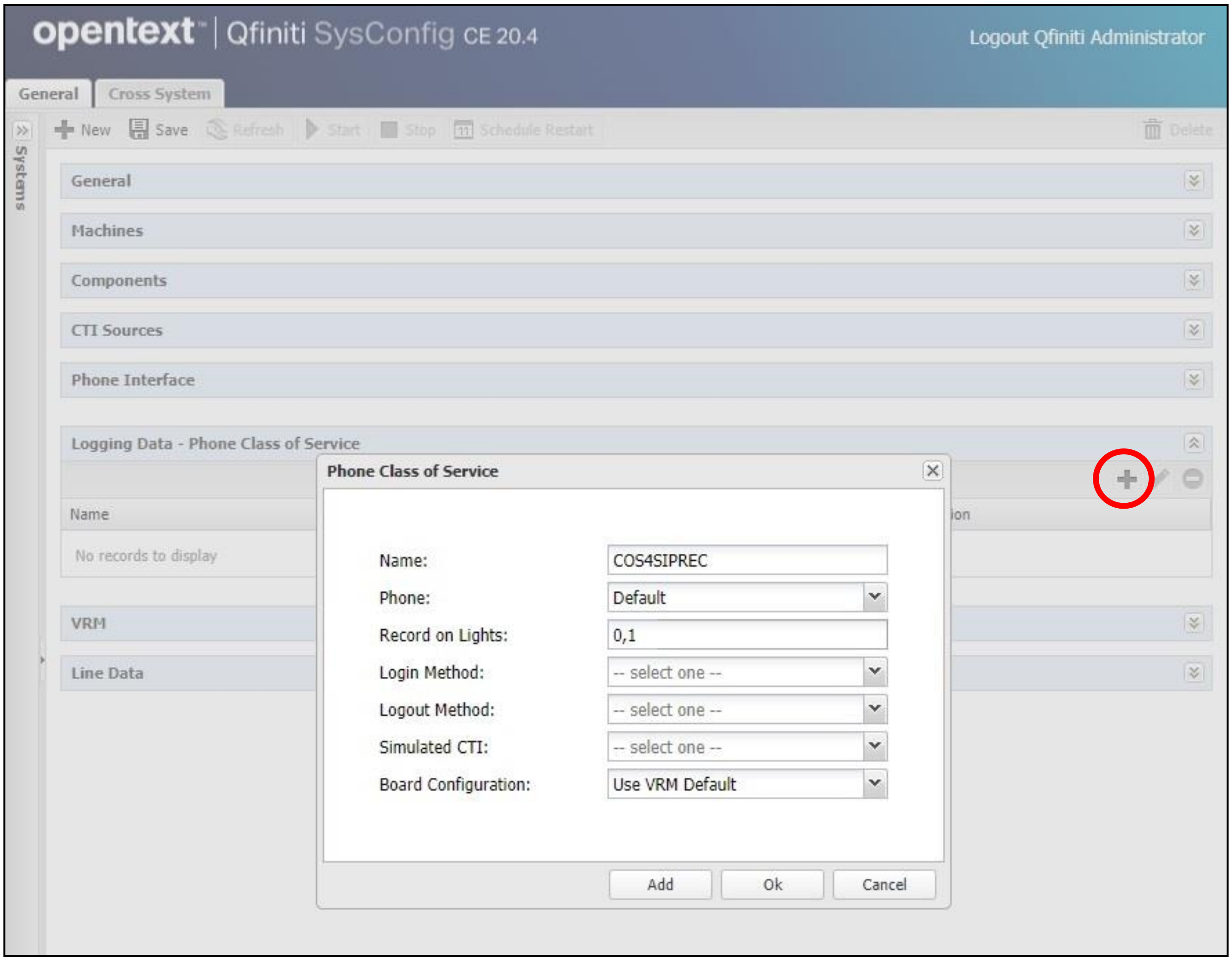
Phone Interface Type: -- select one --

Number of Lines: 4

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"

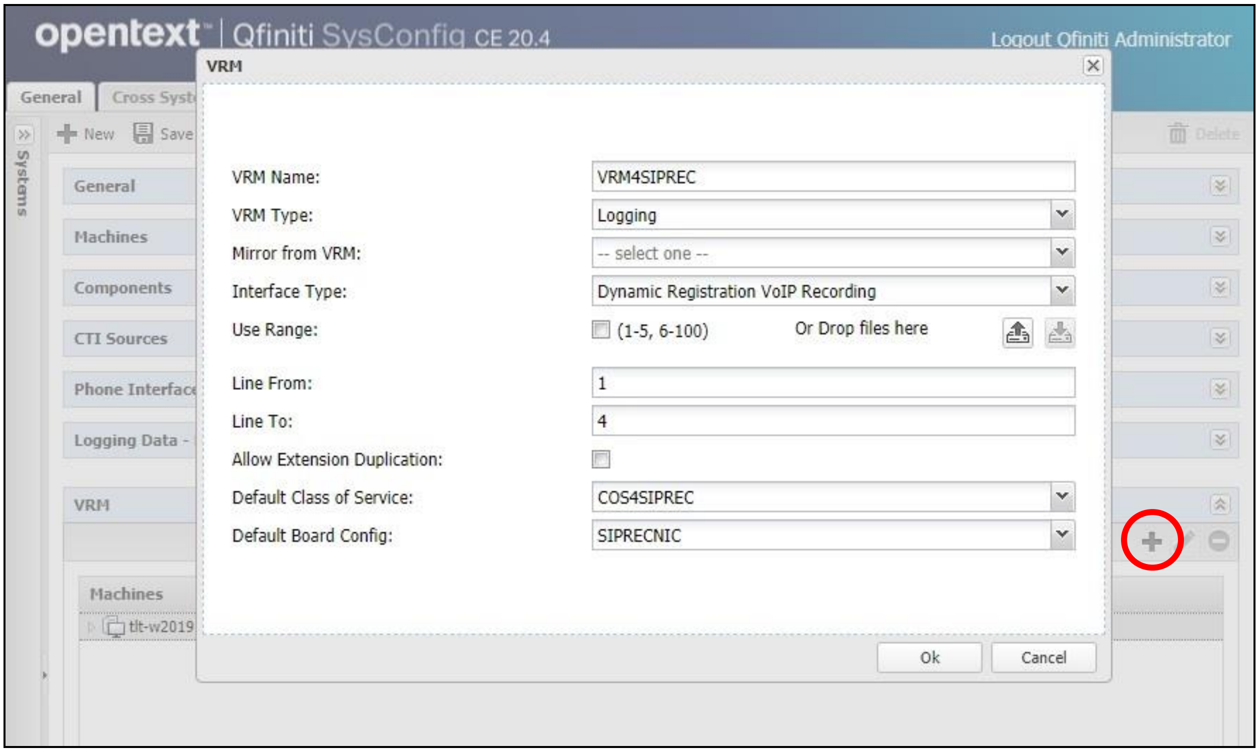


Name:	COS4SIPREC
Phone:	Default
Record on Lights:	0,1
Login Method:	-- select one --
Logout Method:	-- select one --
Simulated CTI:	-- select one --
Board Configuration:	Use VRM Default

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**.



VRM Name: VRM4SIPREC

VRM Type: Logging

Mirror from VRM: -- select one --

Interface Type: Dynamic Registration VoIP Recording

Use Range: □ (1-5, 6-100)

Line From: 1

Line To: 4

Allow Extension Duplication: □

Default Class of Service: COS4SIPREC

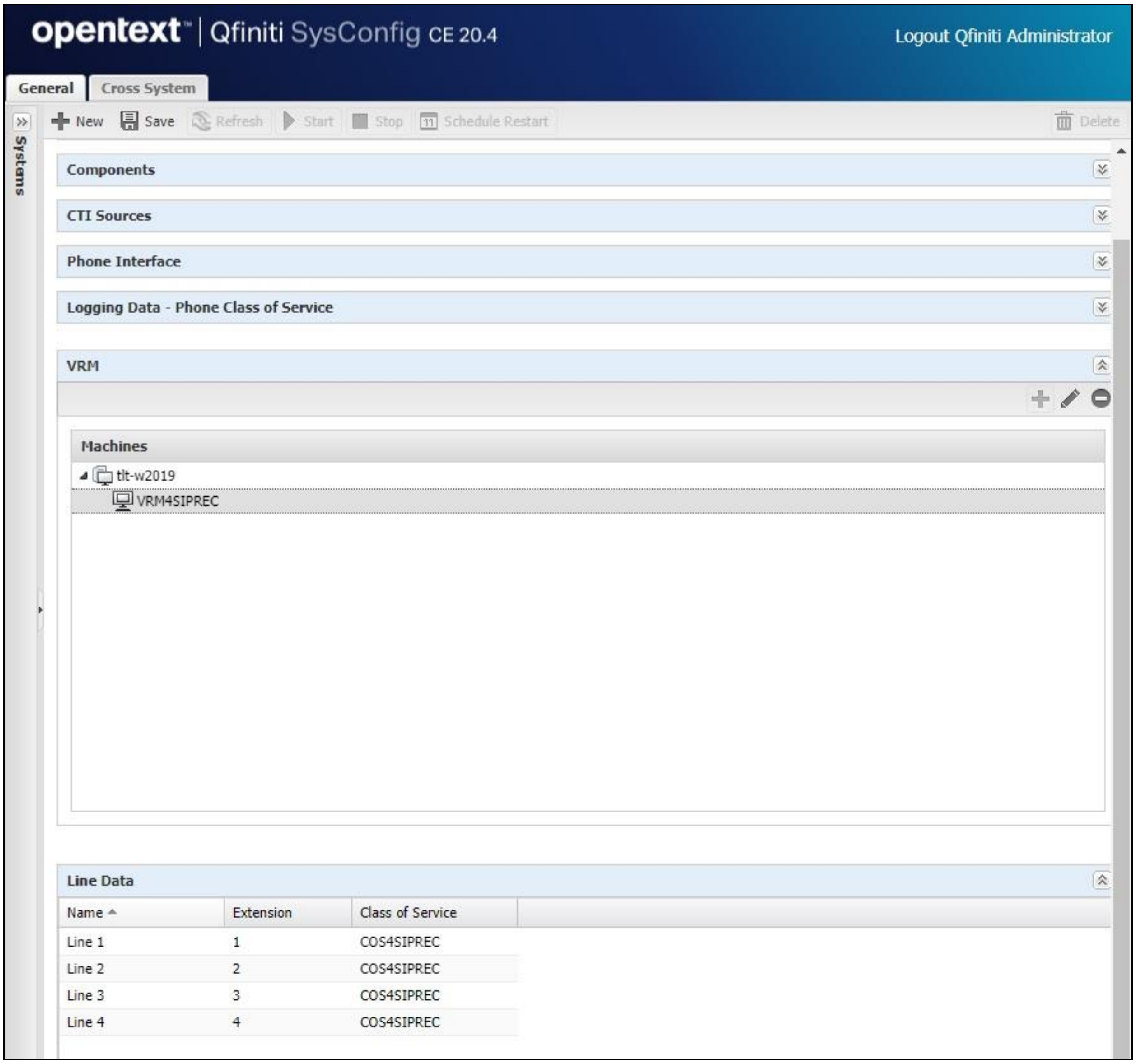
Default Board Config: SIPRECNIC

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**.

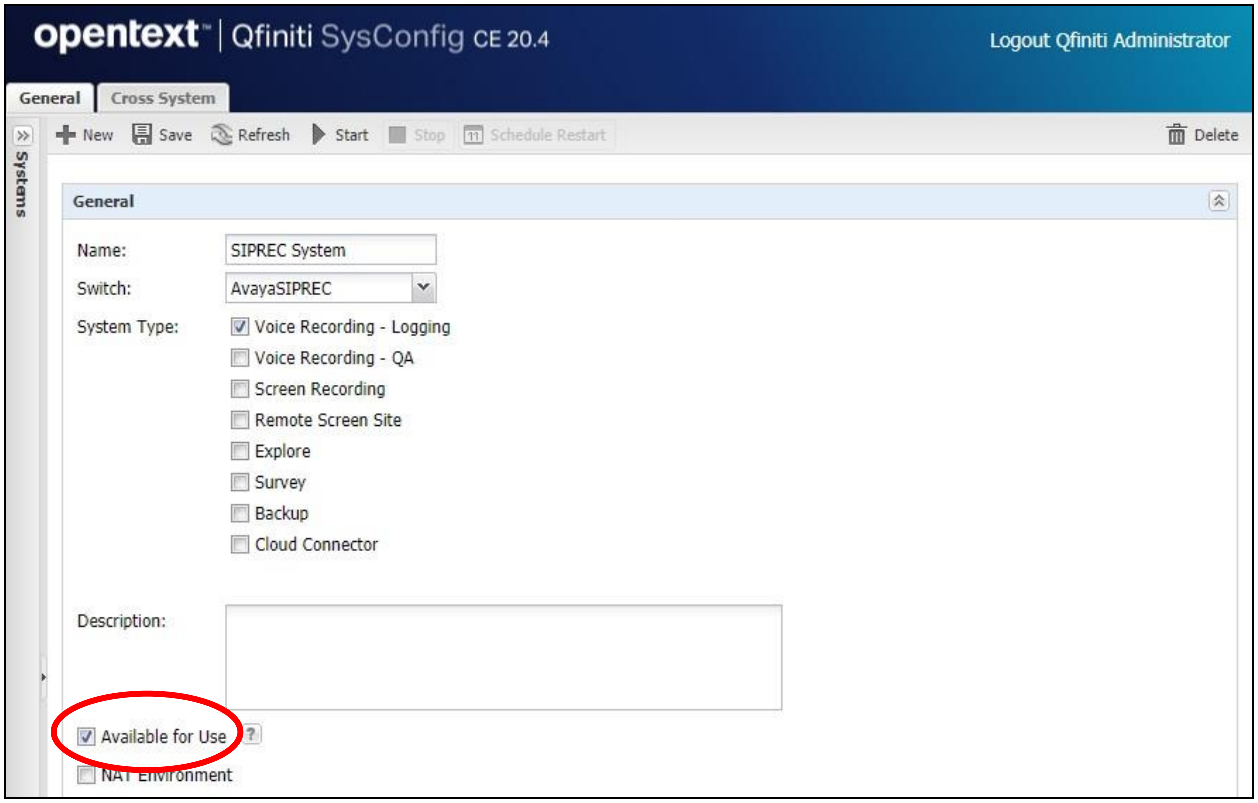
Repeat this section to administer all lines as shown below.



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**.



General

Name: SIPREC System

Switch: AvayaSIPREC

System Type:
☑ Voice Recording - Logging
□ Voice Recording - QA
□ Screen Recording
□ Remote Screen Site
□ Explore
□ Survey
□ Backup
□ Cloud Connector

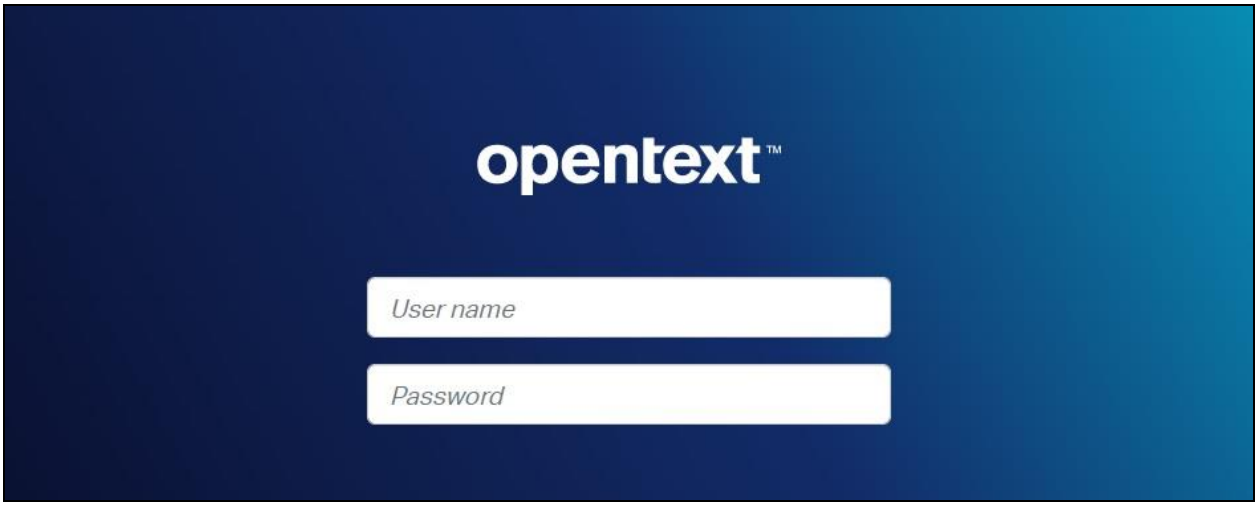
Description:

☑ Available for Use

□ NAT Environment

9.15. Launch Qfiniti Web Interface

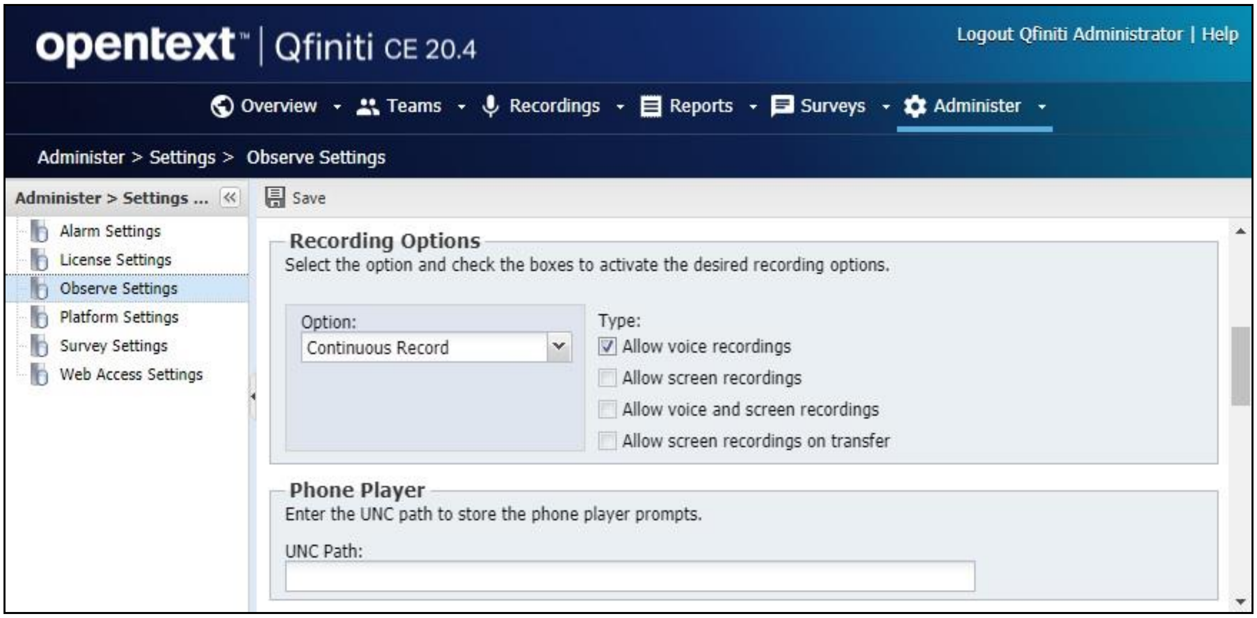
Access the Qfiniti web interface by using the URL "http://hostname/qwa" in an Internet browser window, where "hostname" is the hostname of the Qfiniti server. The screen below is displayed. Log in using the appropriate credentials.



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.



Recording Options

Select the option and check the boxes to activate the desired recording options.

Option: Continuous Record

Type:

☑ Allow voice recordings

□ Allow screen recordings

□ Allow voice and screen recordings

□ Allow screen recordings on transfer

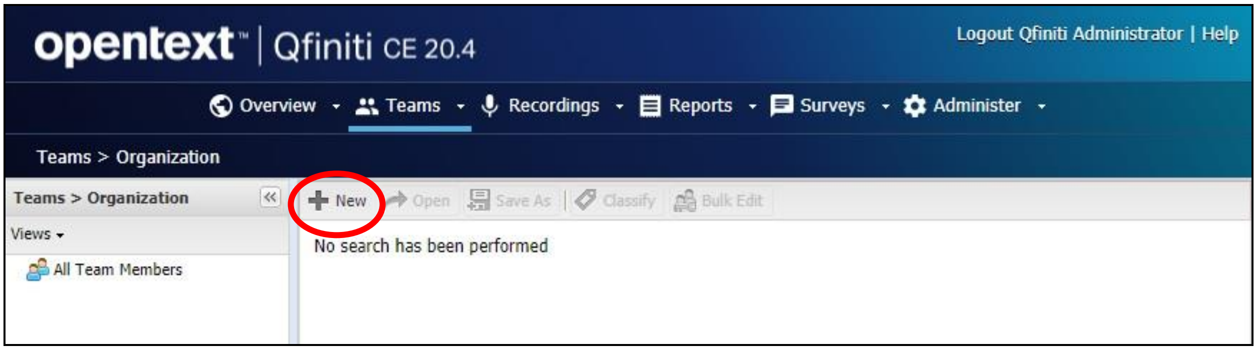
Phone Player

Enter the UNC path to store the phone player prompts.

UNC Path:

9.17. Administer Agents

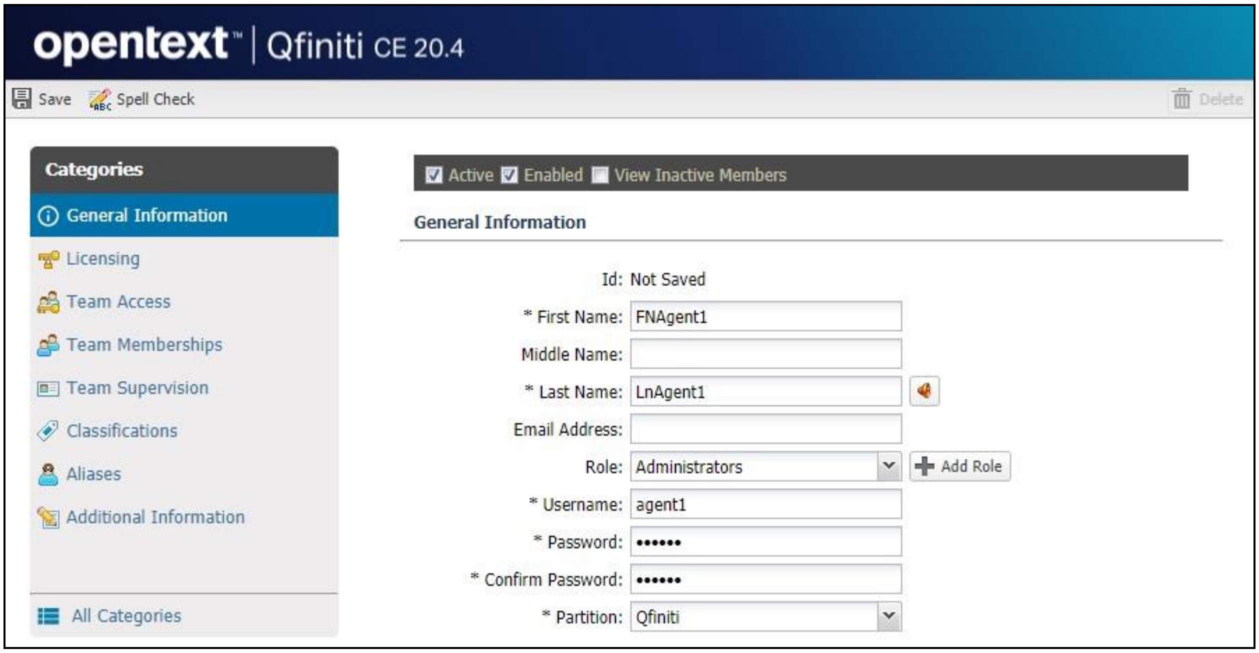
Select **Teams → Organization** from the top menu, to display the screen below. Select the **New** icon in the right pane to add an agent.



No search has been performed

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"

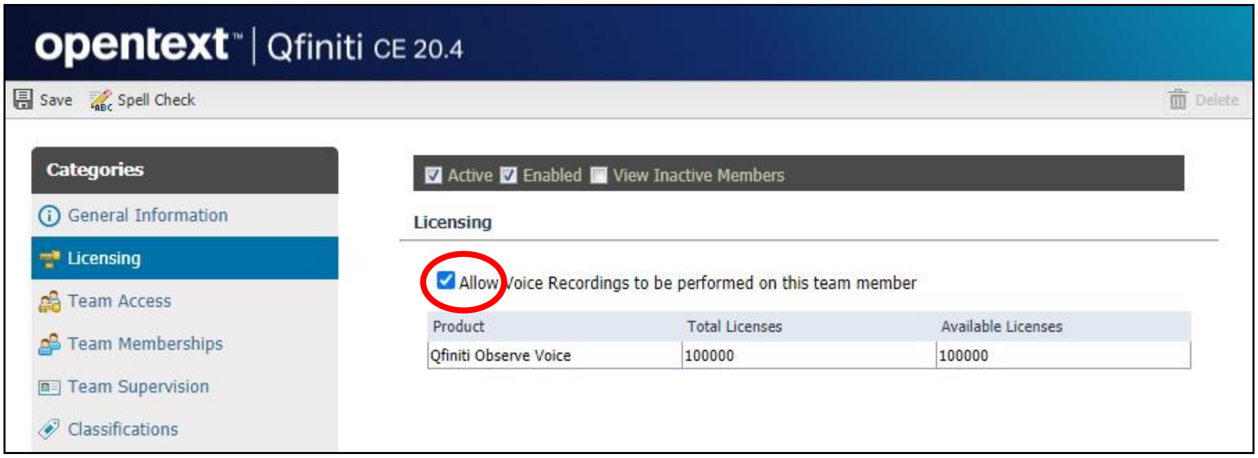


☑ Active ☑ Enabled □ View Inactive Members

General Information

Id:	Not Saved
* First Name:	FNAgent1
Middle Name:	
* Last Name:	LnAgent1
Email Address:	
Role:	Administrators
* Username:	agent1
* Password:	••••••
* Confirm Password:	••••••
* Partition:	Qfiniti

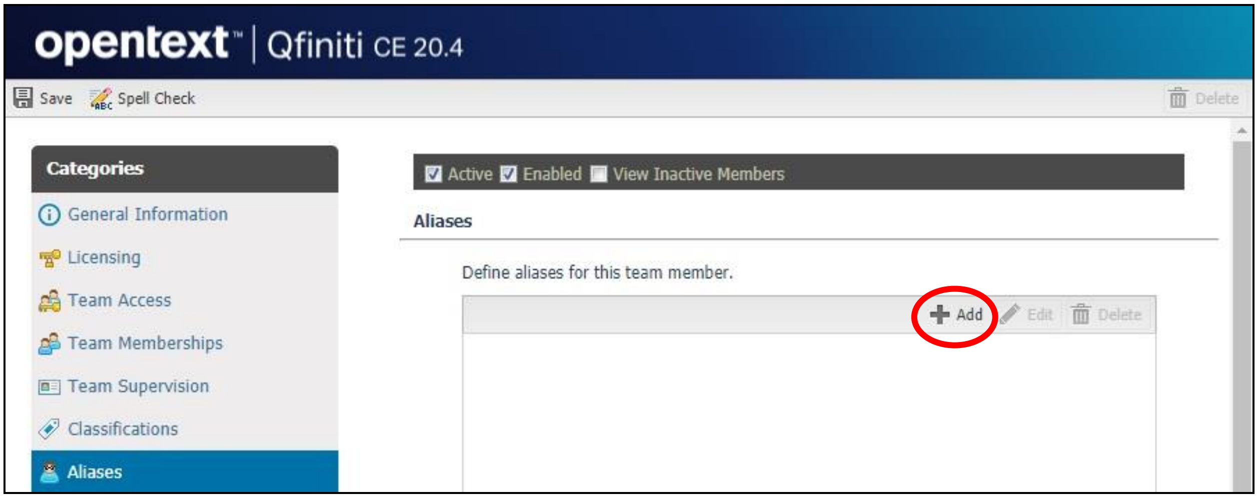
Select **Licensing** from the left pane to display the **Licensing** screen. Check **Allow Voice Recordings to be performed on this team member**, as shown below.



☑ Allow Voice Recordings to be performed on this team member

Product	Total Licenses	Available Licenses
Qfiniti Observe Voice	100000	100000

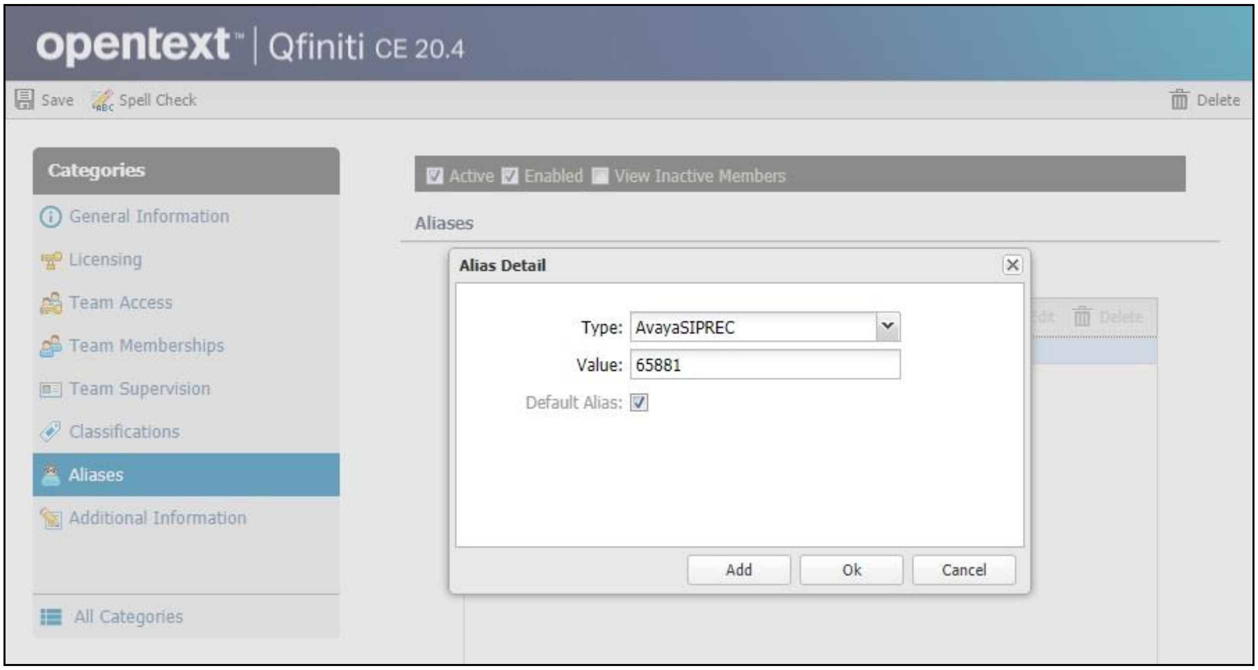
Follow reference **[5]** to configure subsequent steps for the new agent (not shown). Upon reaching the **Aliases** step, click the **Add** icon to create an alias.



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.



Alias Detail

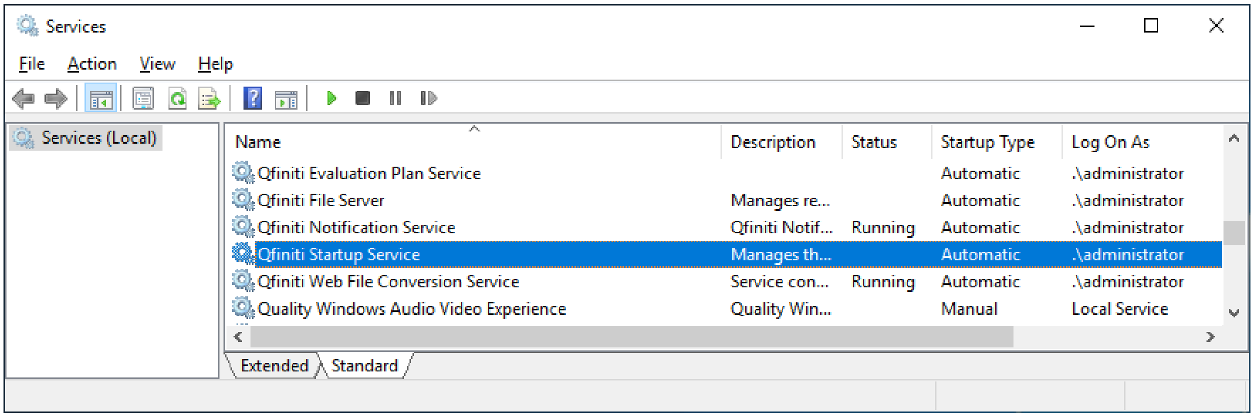
Type: AvayaSIPREC

Value: 65881

Default Alias: ☑

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



Name	Description	Status	Startup Type	Log On As
Qfiniti Evaluation Plan Service			Automatic	.\administrator
Qfiniti File Server	Manages re...		Automatic	.\administrator
Qfiniti Notification Service	Qfiniti Notif...	Running	Automatic	.\administrator
Qfiniti Startup Service	Manages th...		Automatic	.\administrator
Qfiniti Web File Conversion Service	Service con...	Running	Automatic	.\administrator
Quality Windows Audio Video Experience	Quality Win...		Manual	Local Service

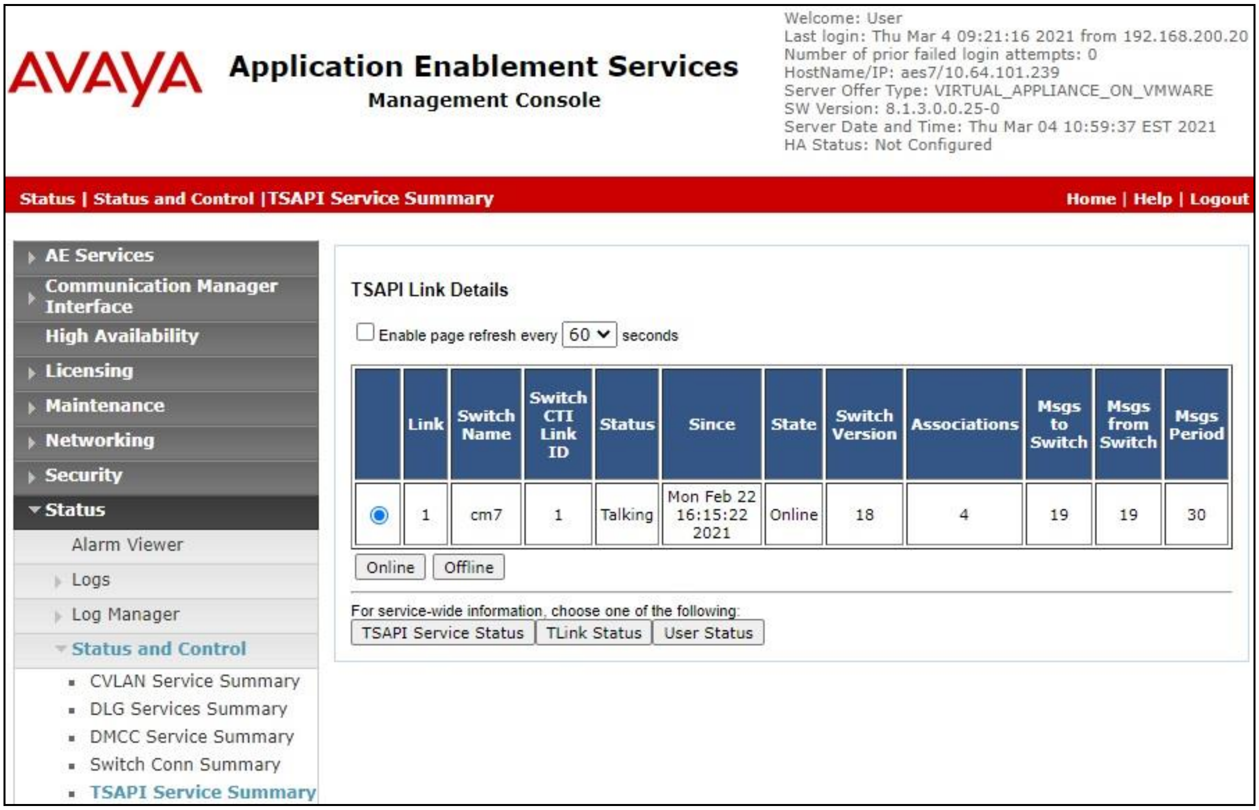
10. Verification Steps

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".



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

TSAPI Link Details

☐ Enable page refresh every 60 seconds

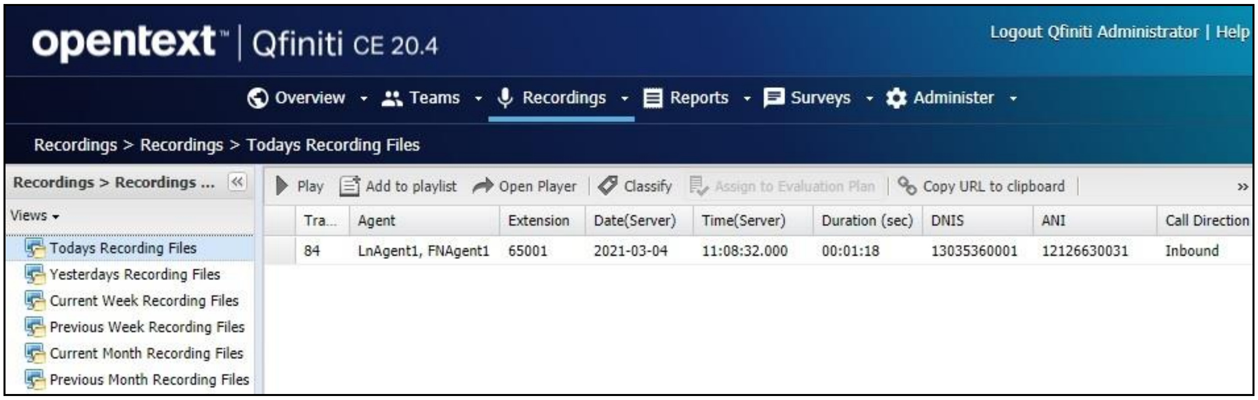
	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	cm7	1	Talking	Mon Feb 22 16:15:22 2021	Online	18	4	19	19	30

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

10.2. Verify SIPREC Recording

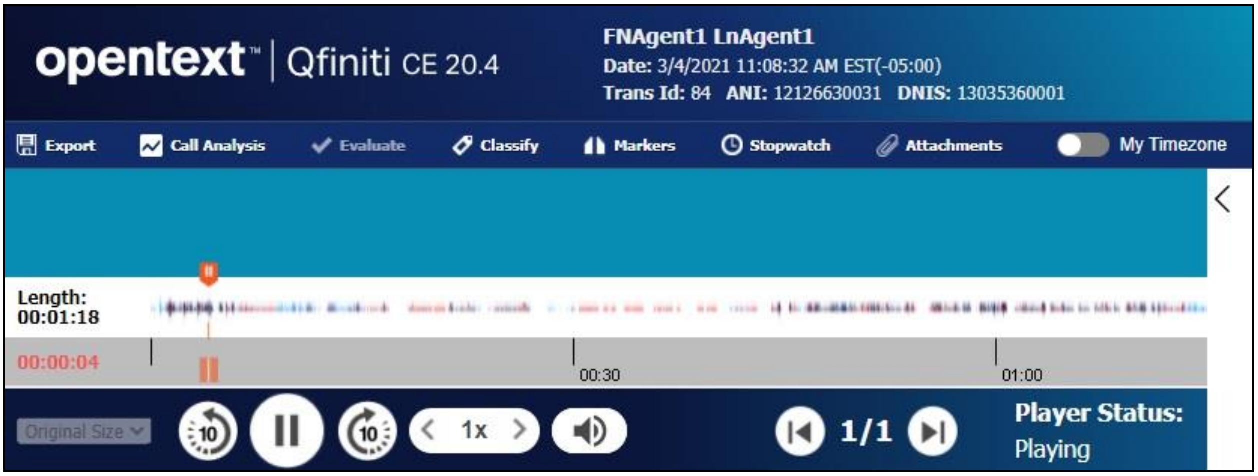
Log an agent in to handle and complete an ACD call. Follow the procedure in **Section 9.15** to launch the Qfiniti web interface, and log in using the appropriate user credentials.

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 ...
Views
Todays Recording Files
Yesterdays Recording Files
Current Week Recording Files
Previous Week Recording Files
Current Month Recording Files
Previous Month Recording Files
Play
Add to playlist
Open Player
Classify
Assign to Evaluation Plan
Copy URL to clipboard

Tra...	Agent	Extension	Date(Server)	Time(Server)	Duration (sec)	DNIS	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.



FNAgent1 LnAgent1
Date: 3/4/2021 11:08:32 AM EST(-05:00)
Trans Id: 84 **ANI:** 12126630031 **DNIS:** 13035360001

Length: 00:01:18

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.

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.