Avaya Solution & Interoperability Test Lab

Application Notes for OpenText Qfiniti 20.4 with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 Using Service Observing No Talk – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for OpenText Qfiniti 20.4 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 using Service Observing No Talk. Qfiniti is a call recording solution.

In the compliance testing, OpenText Qfiniti used the Telephony Services Application Programming Interface from Avaya Aura® Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager, and the Service Observing feature via Avaya Aura® Application Enablement Services Device, Media, and Call Control interface to capture media associated with the monitored agent stations for call recording.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required for OpenText Qfiniti 20.4 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 using Service Observing No Talk. Qfiniti is a call recording solution.

In the compliance testing, Qfiniti used the Telephony Services Application Programming Interface (TSAPI) from Application Enablement Services to monitor skill groups and agent stations on Communication Manager, and the Service Observing feature in the No Talk mode via Application Enablement Services Device, Media, and Call Control (DMCC) XML interface to capture media associated with the monitored agent stations for call recording.

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

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of Qfiniti, the application automatically used TSAPI to perform device queries and requested monitoring of skill groups and agent stations, and DMCC to register virtual IP softphones and activate Service Observing of agent stations via dialing of the Service Observing No Talk feature access code.

For the manual part of testing, each call was handled manually on the agent phone with generation of unique audio content for recordings. Necessary user actions such as hold and resume were performed from the agent phones to test various call scenarios.

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

The verification of tests included use of Application Enablement Services and Qfiniti logs for proper message exchanges and use of Qfiniti web interface for proper logging and playback of calls.

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

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

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

For the testing associated with this Application Note, the interfaces between Avaya systems and Qfiniti used non-encrypted connections for TSAPI and DMCC messaging, and encrypted SRTP for DMCC media, as requested by OpenText.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Qfiniti:

- Handling of TSAPI messages in areas of event notification and value queries.

- Use of DMCC services to register virtual IP softphones and activate Service Observing via dialing of feature access code to obtain media for call recording.

- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, resume, G.711, G.729, forwarding, service observing, long duration, multiple calls, multiple agents, transfer, and conference.

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

2.2. Test Results

All test cases were executed and verified.

2.3. Support

Technical support on Qfiniti can be obtained through the following:

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

3. Reference Configuration

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

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

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

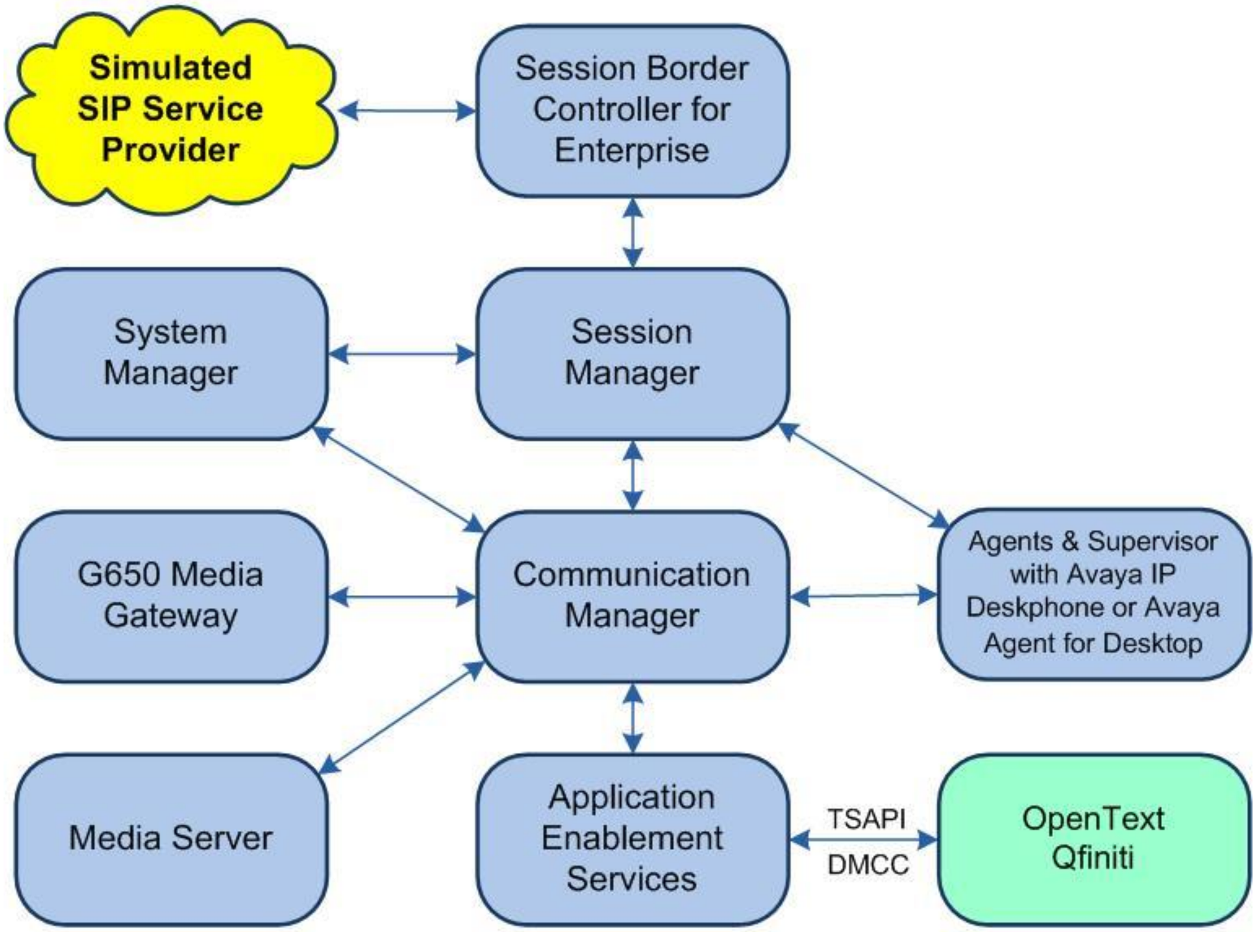

Simulated SIP Service Provider
Session Border Controller for Enterprise
System Manager
Session Manager
G650 Media Gateway
Communication Manager
Agents & Supervisor with Avaya IP Deskphone or Avaya Agent for Desktop
Media Server
Application Enablement Services
TSAPI
DMCC
OpenText Qfiniti

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 (8.1.3.3.1.890.27168)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	8.0.2.200
Avaya Aura® Application Enablement Services in Virtual Environment	8.1.3.3.0.4-0
Avaya Aura® Session Manager in Virtual Environment	8.1.3 (8.1.3.3.813310)
Avaya Aura® System Manager in Virtual Environment	8.1.3 (8.1.3.3.1013878)
Avaya Session Border Controller for Enterprise in Virtual Environment	8.1.2 (8.1.2.0-31-19809)
Avaya Agent for Desktop (H.323 & SIP)	2.0.6.17.3006
Avaya J179 & 9611G IP Deskphone (H.323)	6.8511
Avaya J169 IP Deskphone (SIP)	4.0.10.3.2
OpenText Qfiniti on Microsoft Windows Server 2019 • Avaya TSAPI Windows Client (csta32.dll) • Avaya DMCC XML	20.4.0 with QF-18193 & QF-18501 Standard 8.1.3.25 7.0.0.38

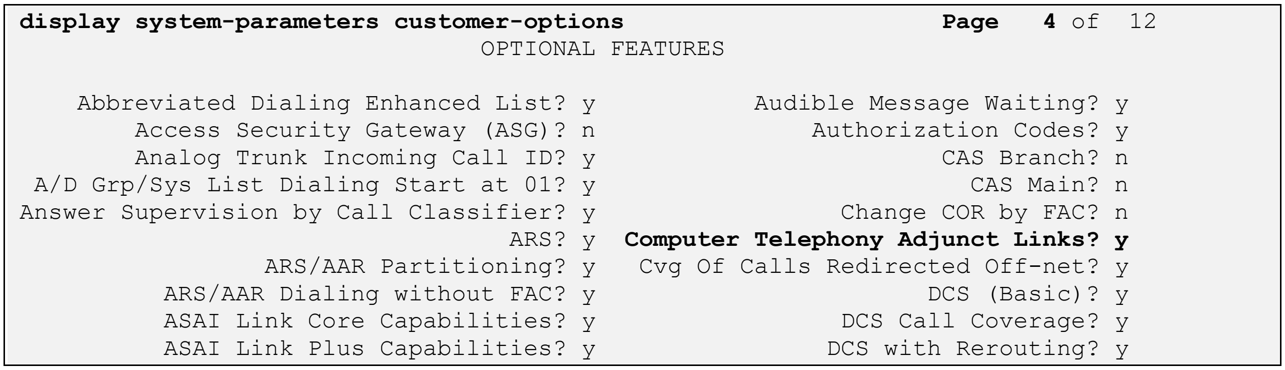
5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer IP codec set
- Administer system parameters features
- Administer feature access codes
- Administer class of restriction
- Administer agent stations
- Administer virtual IP softphones

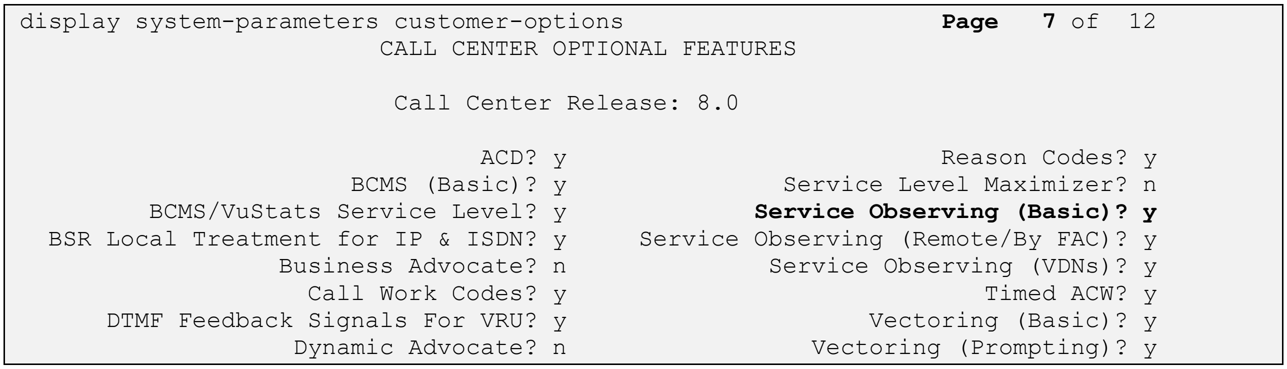
5.1. Verify License

Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the "**display system-parameters customer-options**" command to verify that the **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
```

Navigate to **Page 7** and verify that the **Service Observing (Basic)** customer option is set to "**y**".

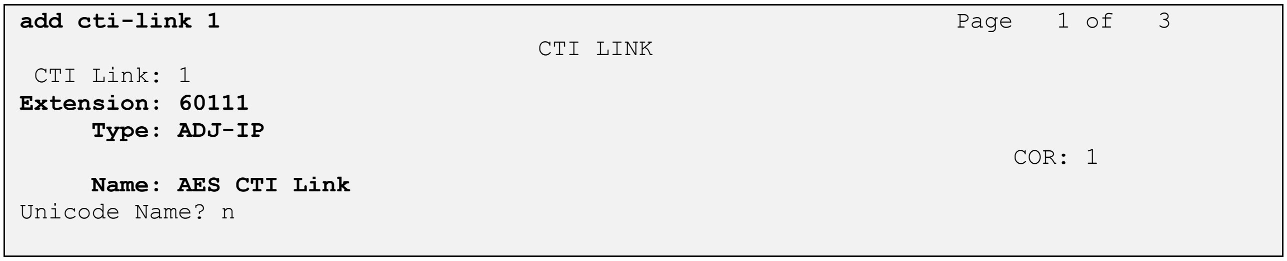


```
display system-parameters customer-options                      Page   7 of  12
                         CALL CENTER OPTIONAL FEATURES

                          Call Center Release: 8.0

                                ACD? y                          Reason Codes? y
                       BCMS (Basic)? y             Service Level Maximizer? n
         BCMS/VuStats Service Level? y          Service Observing (Basic)? y
  BSR Local Treatment for IP & ISDN? y     Service Observing (Remote/By FAC)? y
                  Business Advocate? n             Service Observing (VDNs)? y
                    Call Work Codes? y                            Timed ACW? y
      DTMF Feedback Signals For VRU? y                    Vectoring (Basic)? y
                  Dynamic Advocate? n                 Vectoring (Prompting)? y
```

5.2. Administer CTI Link

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

Enter "**ADJ-IP**" in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.



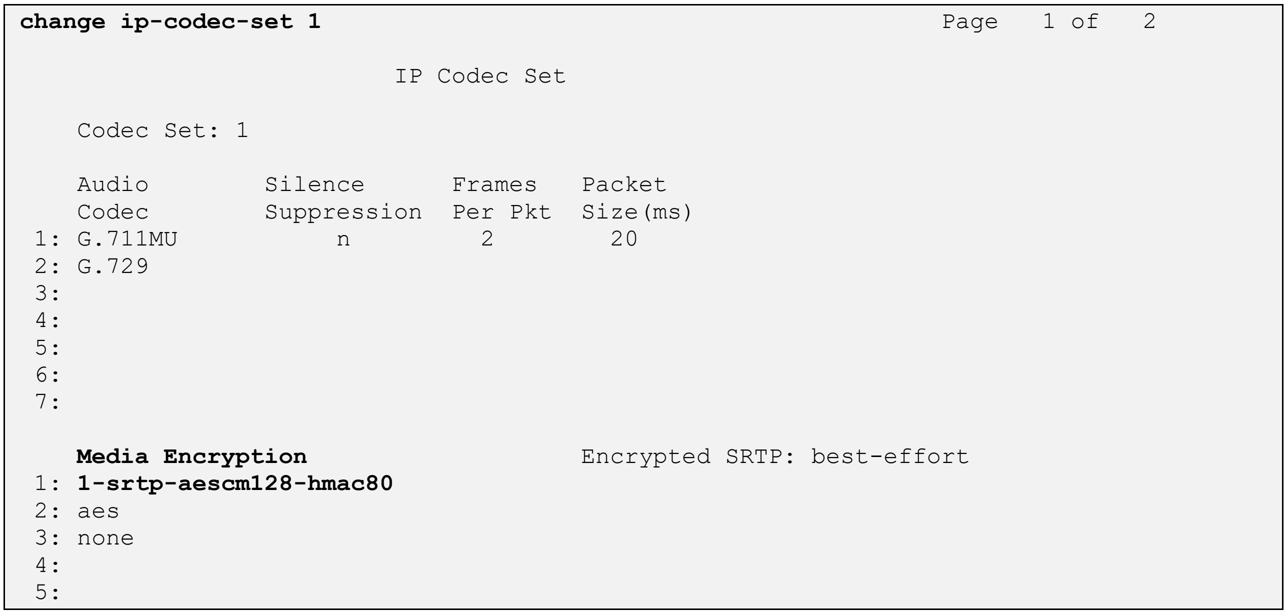
```
add cti-link 1                                                  Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 60111
     Type: ADJ-IP
                                                                    COR: 1
     Name: AES CTI Link
Unicode Name? n
```

5.3. Administer IP Codec Set

Enter the "**change ip-codec-set n**" command, where "**n**" is an existing codec set number used for integration with Qfiniti.

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

In the compliance testing, this IP codec set was assigned to the agent stations and to the virtual IP softphones used by Qfiniti.



```
change ip-codec-set 1                                          Page   1 of   2

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2: G.729
 3:
 4:
 5:
 6:
 7:

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

5.4. Administer System Parameters Features

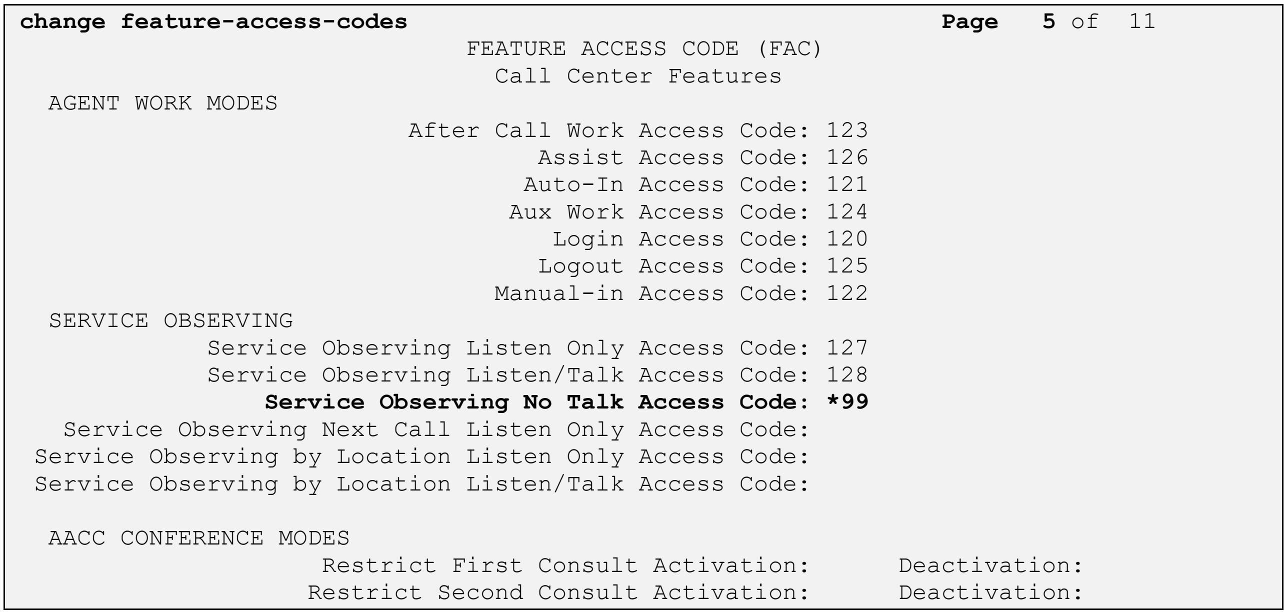
Enter the "**change system-parameters features**" command and navigate to **Page 11**. Set **Service Observing: Warning Tone** to the needed setting per customer requirement, and enable **Allow Two Observers in Same Call**, as shown below.

```
change system-parameters features                               Page  11 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
  EAS
         Expert Agent Selection (EAS) Enabled? y
        Minimum Agent-LoginID Password Length:
          Direct Agent Announcement Extension:                    Delay:
    Message Waiting Lamp Indicates Status For: station
                           Work Mode On Login: aux
  VECTORING
                    Converse First Data Delay: 0      Second Data Delay: 2
                Converse Signaling Tone(msec): 100         Pause (msec): 70
                      Prompting Timeout(secs): 10
                  Interflow-qpos EWT Threshod: 2
    Reverse Star/Pound Digit For Collect Step? n
          Available Agent Adjustments for BSR? n
                             BSR Tie Strategy: 1st-found
   Store VDN Name in Station's Local Call Log? n
  SERVICE OBSERVING
              Service Observing: Warning Tone? n     or Conference Tone? n
    Allowed with Exclusion: Service Observing? n                    SSC? n
             Allow Two Observers in Same Call? y
```

5.5. Administer Feature Access Codes

Enter the "**change system-parameters features**" command and navigate to **Page 5**. Set **Service Observing No Talk Access Code** to an available code. This code will be dialed by the virtual IP softphones for activation of Service Observing.

Note that the benefit of using the No Talk mode for Service Observing is in elimination to reserve talk path time slots for the virtual IP softphones as observers.



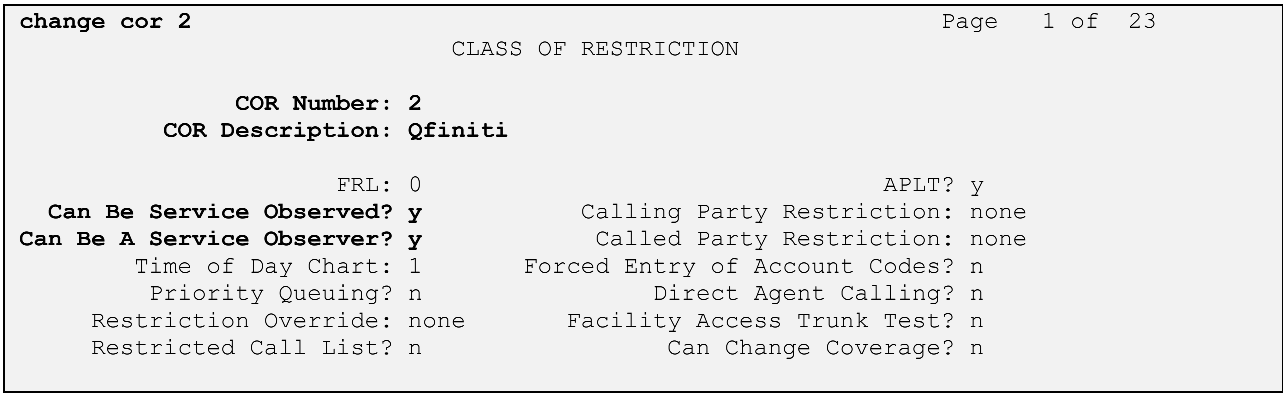
```
change feature-access-codes                                         Page   5 of  11
                               FEATURE ACCESS CODE (FAC)
                                 Call Center Features
  AGENT WORK MODES
                           After Call Work Access Code: 123
                                    Assist Access Code: 126
                                   Auto-In Access Code: 121
                                  Aux Work Access Code: 124
                                     Login Access Code: 120
                                    Logout Access Code: 125
                                 Manual-in Access Code: 122
  SERVICE OBSERVING
             Service Observing Listen Only Access Code: 127
             Service Observing Listen/Talk Access Code: 128
                 Service Observing No Talk Access Code: *99
   Service Observing Next Call Listen Only Access Code:
 Service Observing by Location Listen Only Access Code:
 Service Observing by Location Listen/Talk Access Code:

  AACC CONFERENCE MODES
                     Restrict First Consult Activation:      Deactivation:
                    Restrict Second Consult Activation:      Deactivation:
```

5.6. Administer Class of Restriction

Enter the “**change cor n**” command, where “**n**” is the class of restriction (COR) number used for integration with Qfiniti.

For **COR Description**, enter a desired description. Set the **Can Be Service Observed** and **Can Be A Service Observer** fields to “**y**”, as shown below. In the compliance testing, this COR was assigned to the agent stations and virtual IP softphones.

If desired, separate COR can be used for enablement of each parameter. The COR with **Can Be Service Observed** enabled needs to be assigned to the agent stations, and the COR with **Can Be A Service Observer** enabled needs to be assigned to the virtual IP softphones.



```
change cor 2                                                    Page   1 of  23
                              CLASS OF RESTRICTION

               COR Number: 2
          COR Description: Qfiniti

                      FRL: 0                                APLT? y
  Can Be Service Observed? y           Calling Party Restriction: none
Can Be A Service Observer? y            Called Party Restriction: none
        Time of Day Chart: 1       Forced Entry of Account Codes? n
         Priority Queuing? n                Direct Agent Calling? n
     Restriction Override: none       Facility Access Trunk Test? n
     Restricted Call List? n                 Can Change Coverage? n
```

5.7. Administer Agent Stations

Enter the "**change station n**" command, where "**n**" is the first H.323 agent station extension from **Section 3**. For **COR**, enter the COR number from **Section 5.6**.

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

```
change station 65001                                            Page   1 of   5
                                     STATION

Extension: 65001                         Lock Messages? n               BCC: 0
     Type: 9611                          Security Code: *                TN: 1
     Port: S000106                     Coverage Path 1: 1              COR: 2
     Name: CM Station 1                Coverage Path 2:                 COS: 1
Unicode Name? n                     Hunt-to Station:                  Tests? y
```

5.8. Administer Virtual IP Softphones

Add a virtual IP softphone using the "**add station n**" command, where "**n**" is an available extension number. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Extension:** The available extension number.
- **Type:** Any IP telephone type, such as "4620".
- **Name:** A descriptive name.
- **Security Code:** A desired code.
- **COR:** The COR number from **Section 5.6**.
- **IP SoftPhone:** "y"

```
add station 65991                                               Page   1 of   5
                                     STATION

Extension: 65991                         Lock Messages? n               BCC: 0
     Type: 4620                          Security Code: 234567           TN: 1
     Port: IP                          Coverage Path 1:                COR: 2
     Name: Qfiniti DMCC 1              Coverage Path 2:                 COS: 1
Unicode Name? n                     Hunt-to Station:                  Tests? y
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                             Message Lamp Ext: 65991
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                  Button Modules? 0
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? y

                                               IP Video Softphone? n
                              Short/Prefixed Registration Allowed: default
```

Navigate to **Page 4** and add "**serv-obsrv**" to the 6th button. Note that this button is required by Qfiniti for purpose of monitoring the Service Observing activation status.

```
add station 65991                                               Page   4 of   5
                                     STATION
 SITE DATA
       Room:                                            Headset? n
       Jack:                                            Speaker? n
      Cable:                                           Mounting: d
      Floor:                                        Cord Length: 0
   Building:                                          Set Color:

ABBREVIATED DIALING
     List1:                    List2:                    List3:




BUTTON ASSIGNMENTS
 1: call-appr                            5:
 2: call-appr                            6: serv-obsrv
 3: call-appr                            7:
 4:                                      8:
```

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

```
list station 65991 count 2

                                  STATIONS

Ext/          Port/   Name/                          Room/      Cv1/  COR/
 Hunt-to       Type      Surv GK NN      Move  Cable   Jack   Cv2  COS  TN

65991            S000134 Qfiniti DMCC 1                               2
               4620                        no                        1  1
65992            S000135 Qfiniti DMCC 2                               2
               4620                        no                        1  1
```

6. Configure Avaya Aura® Application Enablement Services

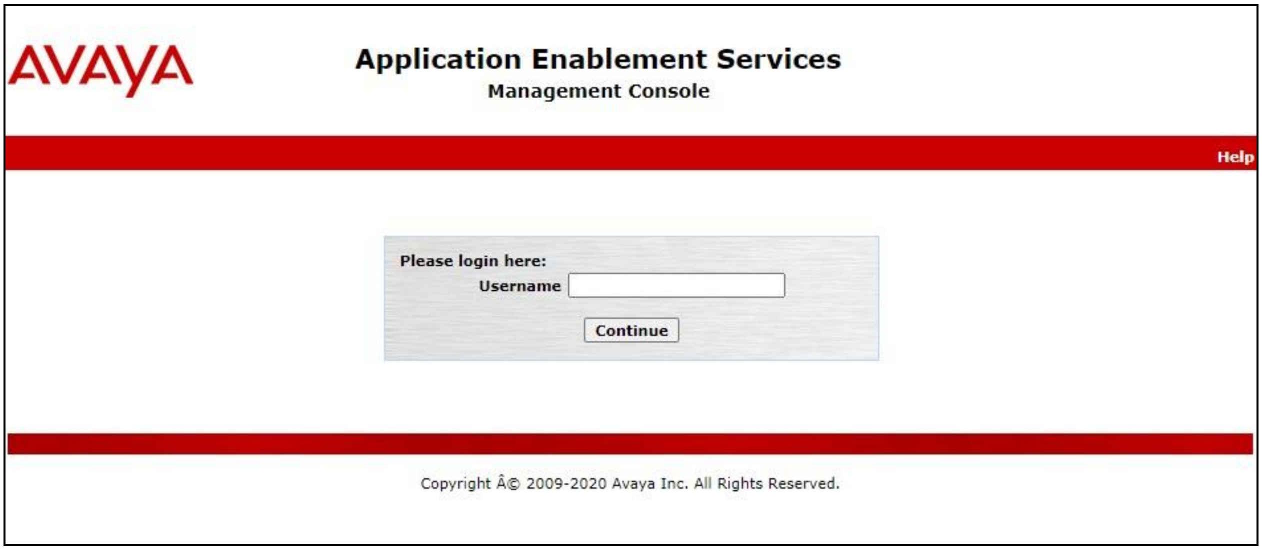
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- Administer Qfiniti user
- Administer security database
- Administer ports
- Restart services

6.1. Launch OAM Interface

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

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

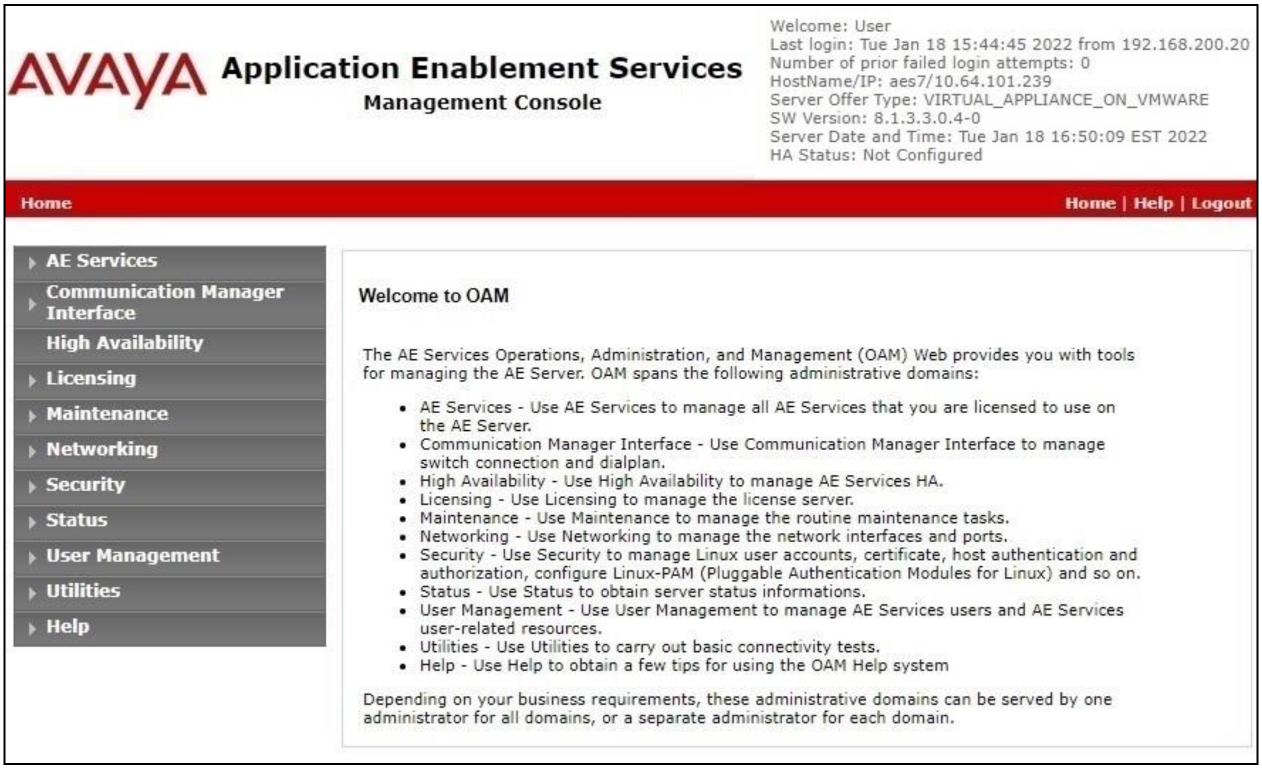


Application Enablement Services
Management Console

Please login here:
Username

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

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



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

Welcome to OAM

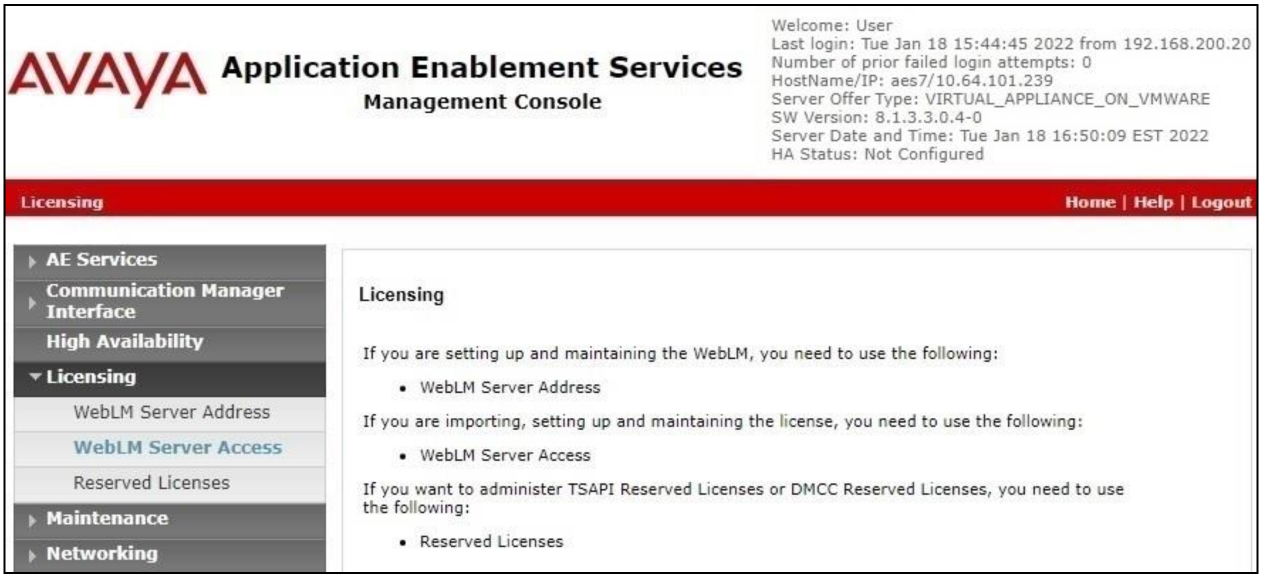
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

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

Licensing

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

- WebLM Server Address

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

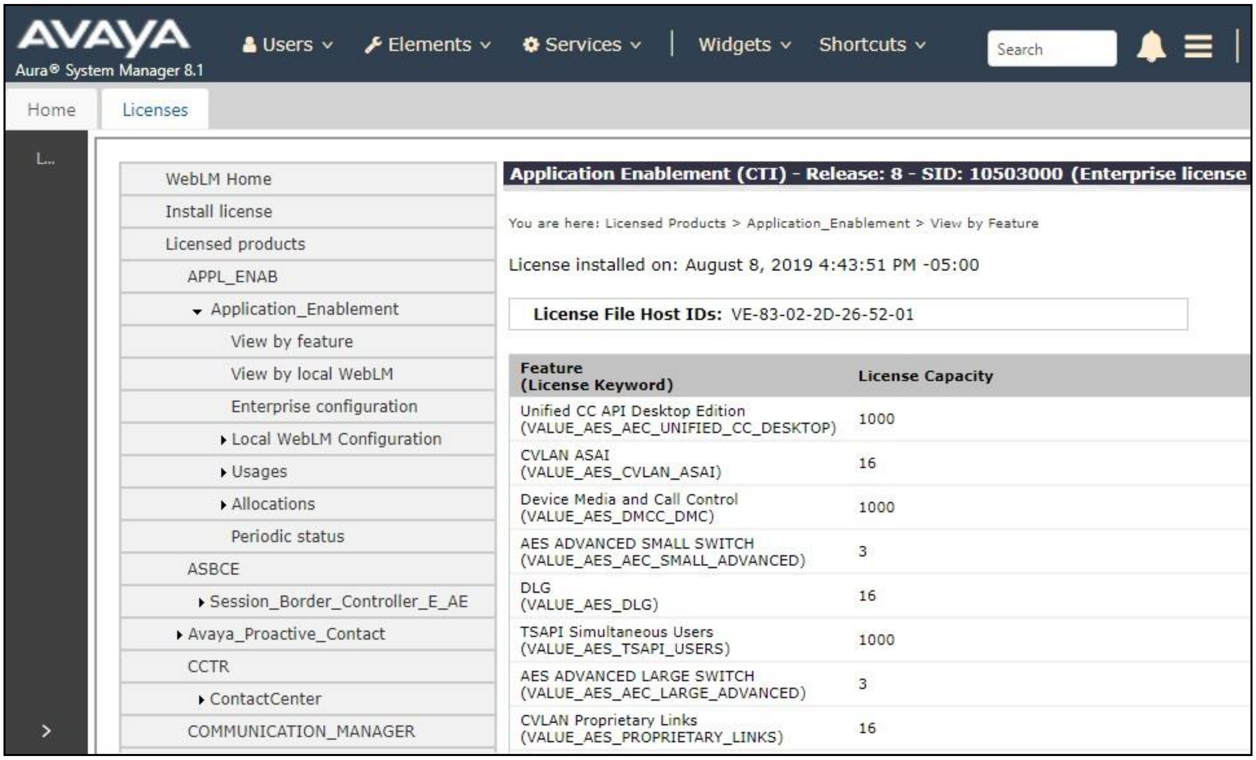
- WebLM Server Access

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

- Reserved Licenses

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

Verify that there are sufficient licenses for **Device Media and Call Control** and **TSAPI Simultaneous Users**, as shown below. The DMCC license is used for the virtual IP softphones, and the TSAPI license is used for device monitoring.



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

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

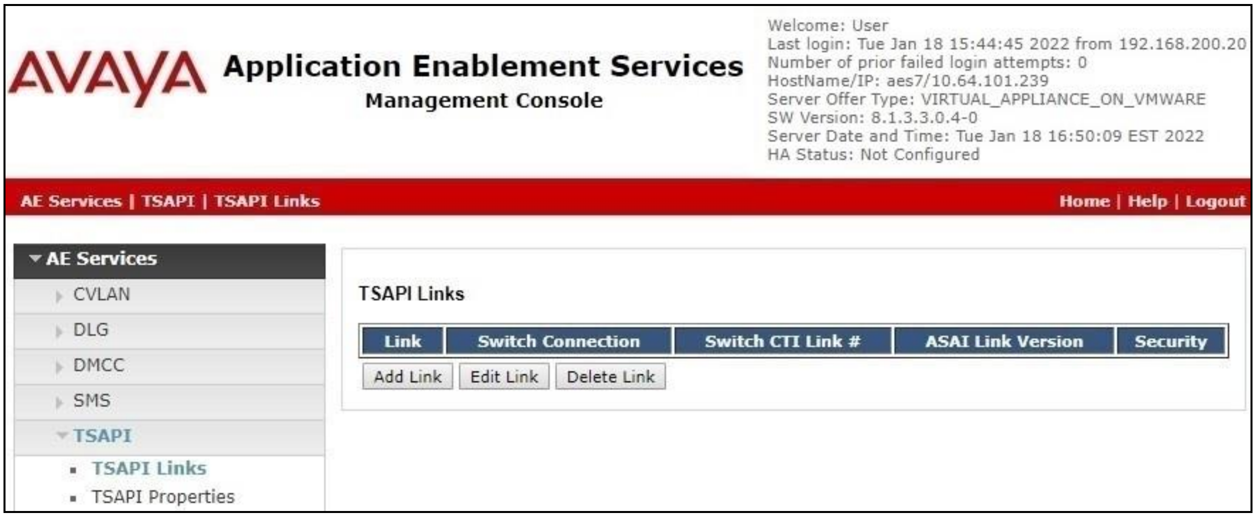
License installed on: August 8, 2019 4:43:51 PM -05:00

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

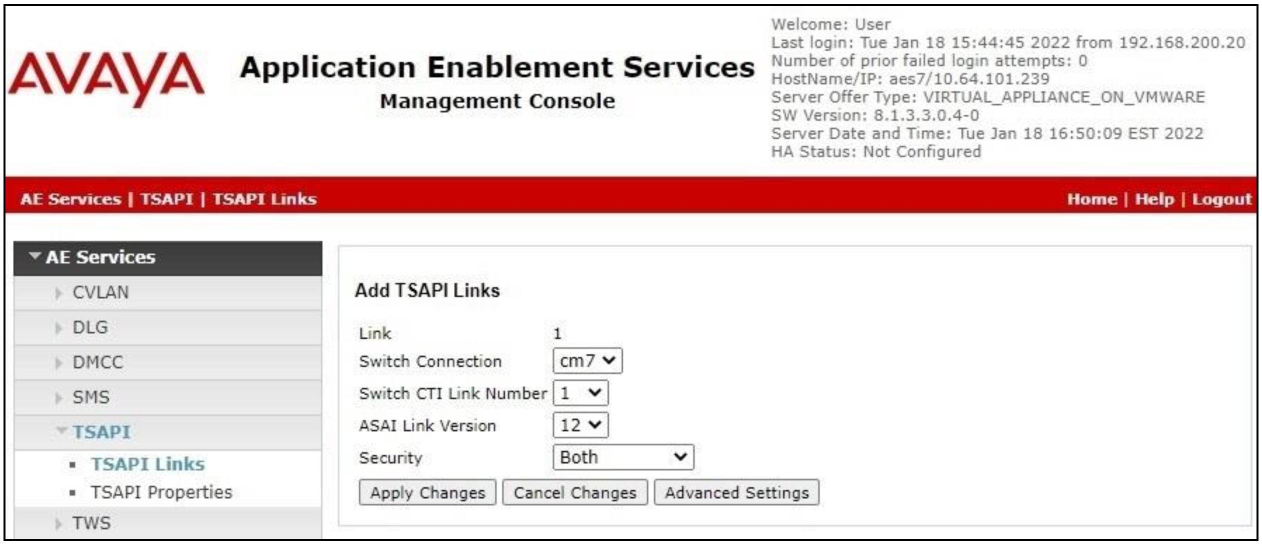
TSAPI Links

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 "**cm7**". For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**.

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



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

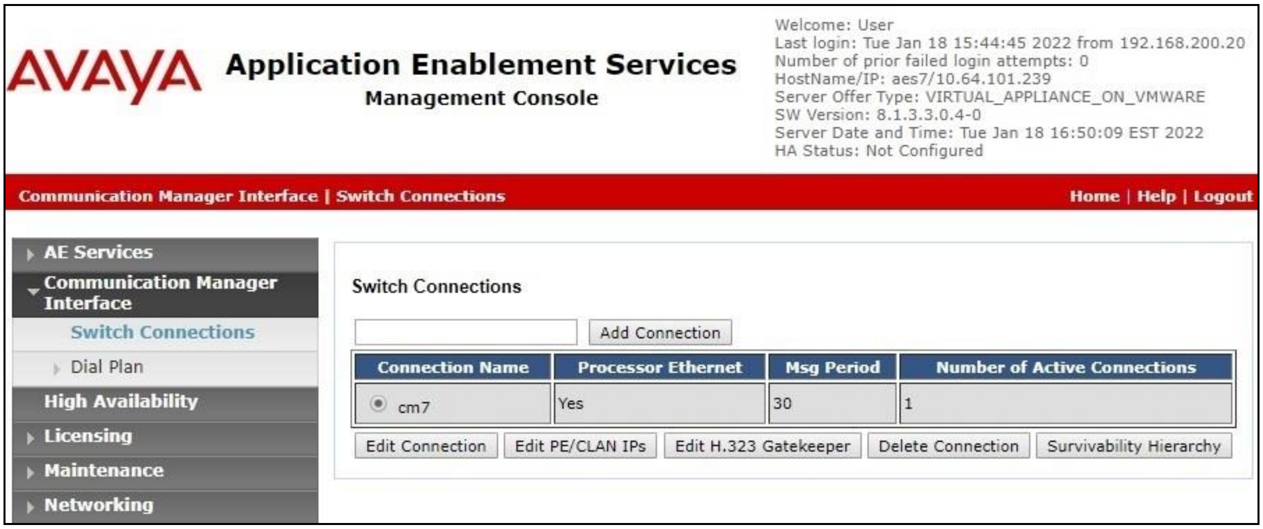
Add TSAPI Links

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

6.4. Administer H.323 Gatekeeper

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

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

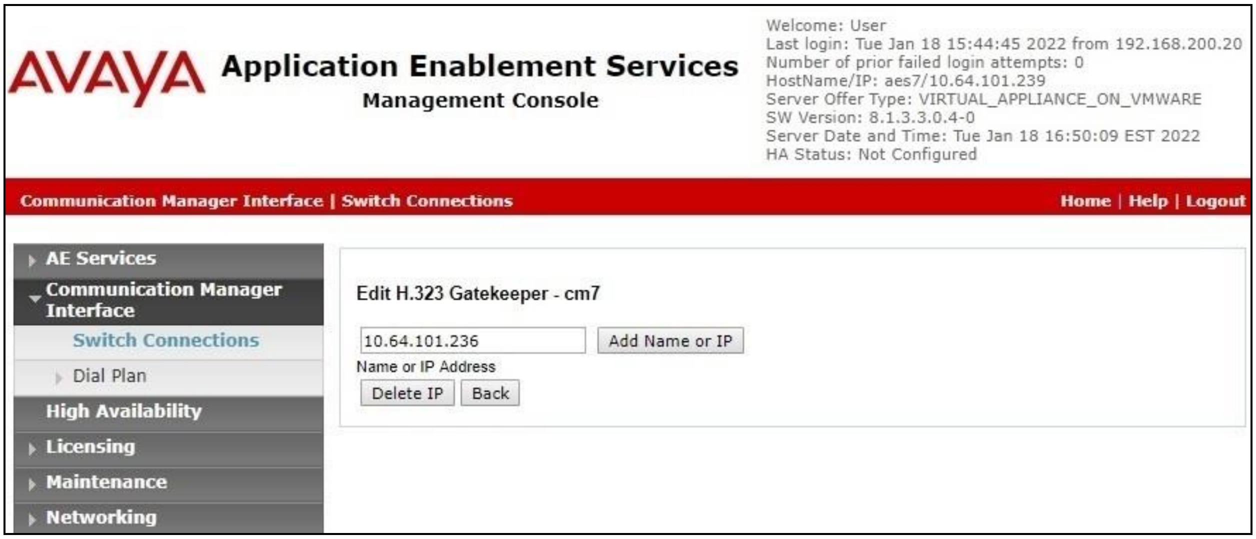


Welcome: User
Last login: Tue Jan 18 15:44:45 2022 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.3.0.4-0
Server Date and Time: Tue Jan 18 16:50:09 EST 2022
HA Status: Not Configured

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● cm7	Yes	30	1

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



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

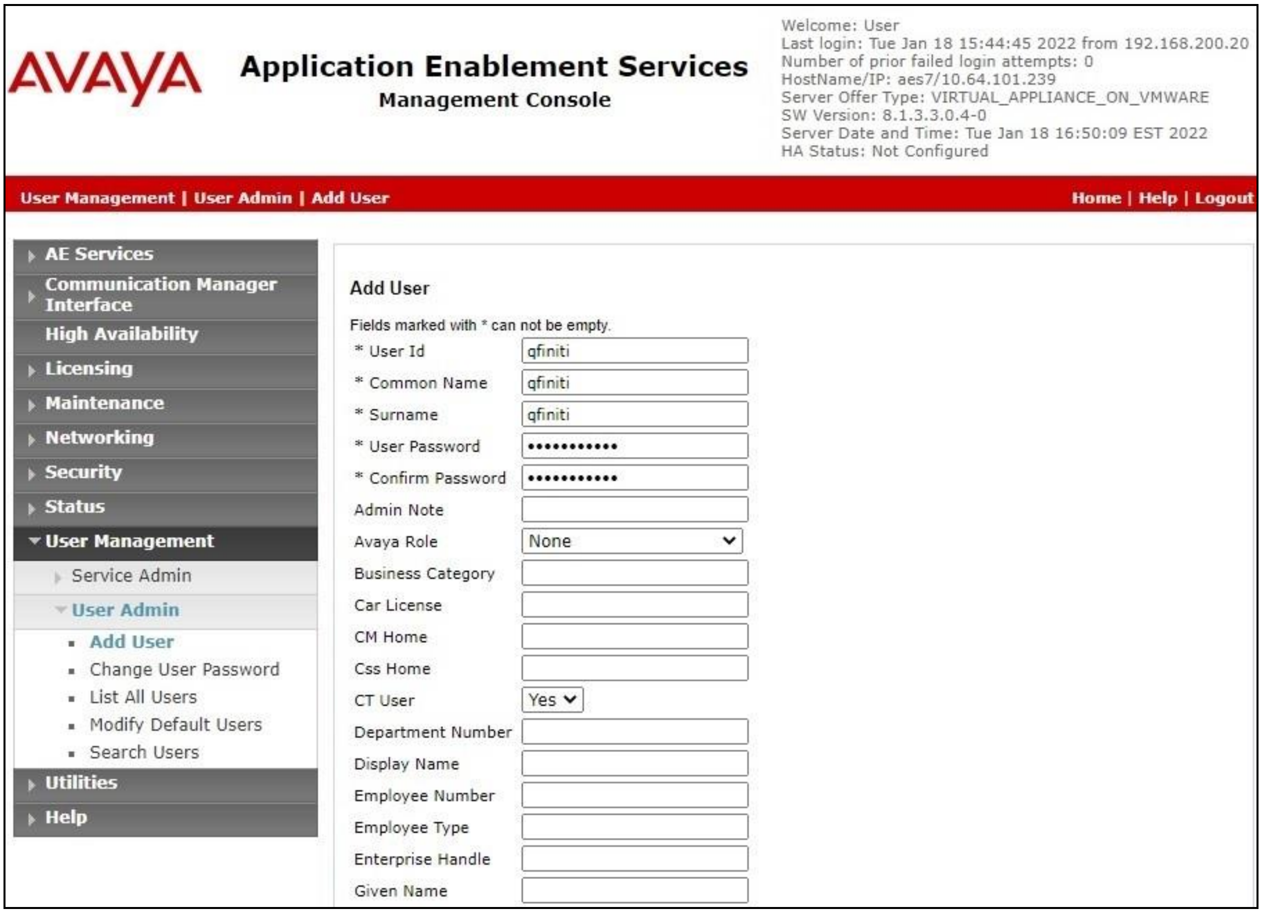
Edit H.323 Gatekeeper - cm7

Name or IP Address: 10.64.101.236

6.5. Administer Qfiniti User

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

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



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

Add User

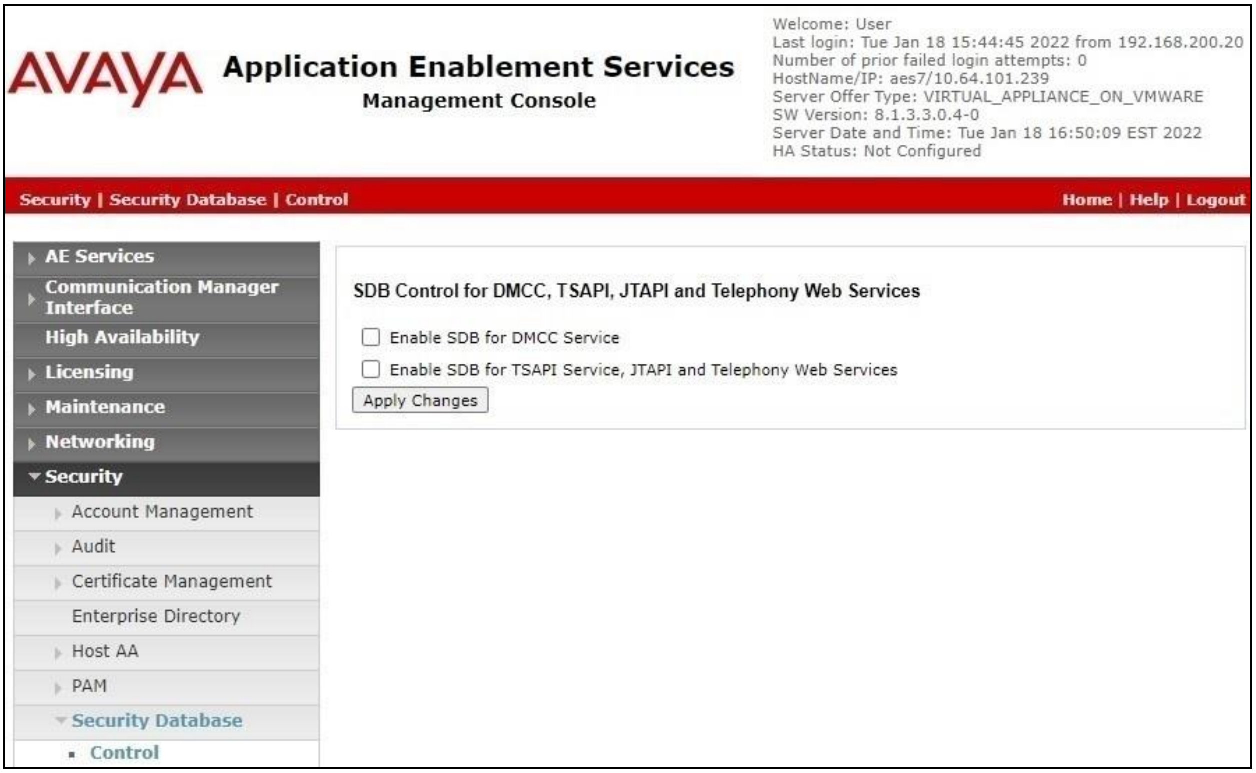
Fields marked with * can not be empty.

* 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	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	
Enterprise Handle	
Given Name	

6.6. Administer Security Database

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

In the case that the security database is used by the customer with parameters already enabled, then follow reference [**2**] to configure access privileges for the Qfiniti user from **Section 6.5**.



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

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

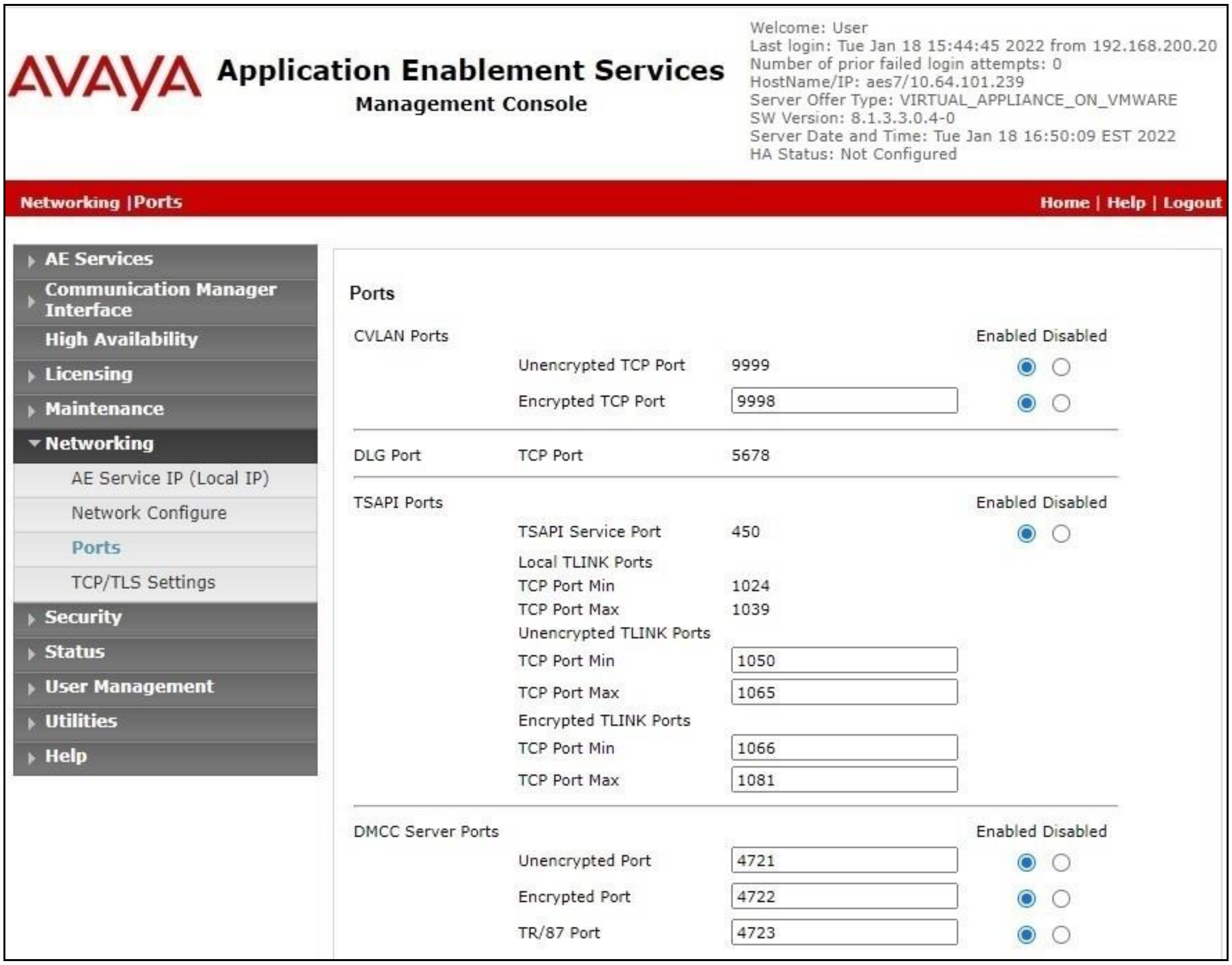
☐ Enable SDB for DMCC Service

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

6.7. Administer Ports

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

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



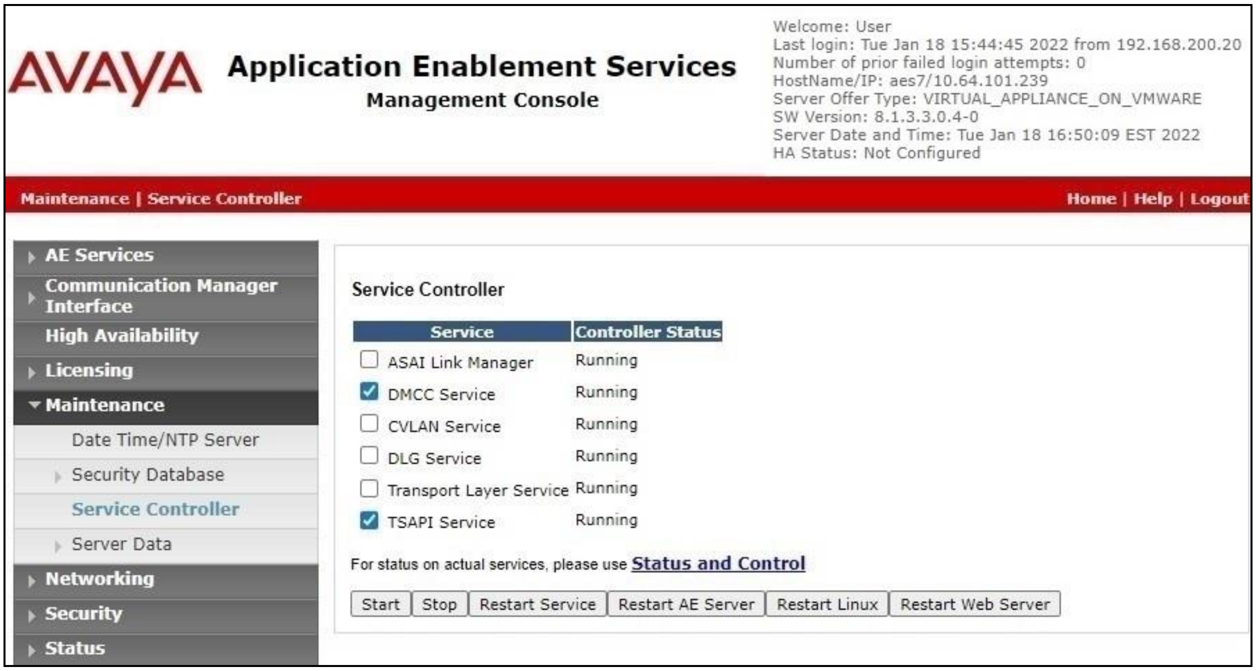
Welcome: User
Last login: Tue Jan 18 15:44:45 2022 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.3.0.4-0
Server Date and Time: Tue Jan 18 16:50:09 EST 2022
HA Status: Not Configured

Ports

			Enabled	Disabled
CVLAN Ports				
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports				
	TSAPI Service Port	450	●	○
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	1050		
	TCP Port Max	1065		
	Encrypted TLINK Ports			
	TCP Port Min	1066		
	TCP Port Max	1081		
DMCC Server Ports				
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	●	○

6.8. Restart Services

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



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

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

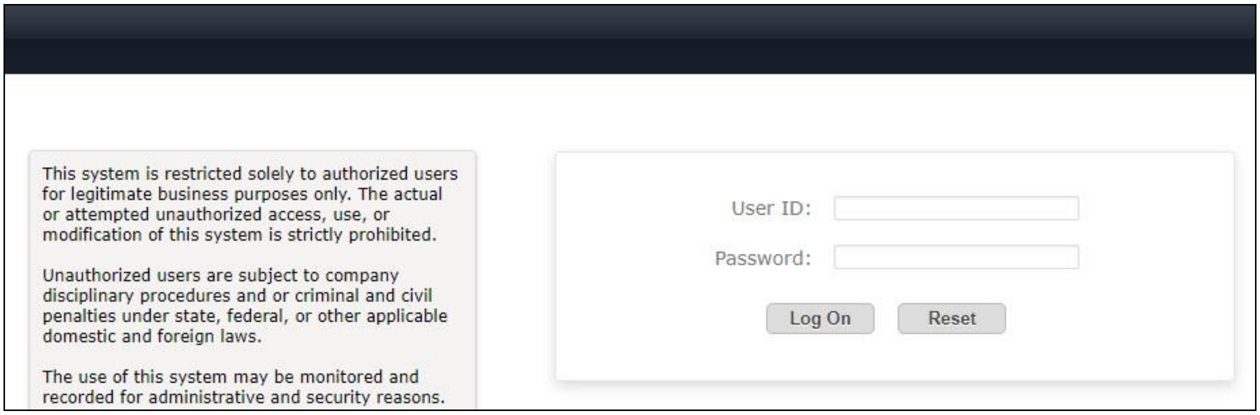
7. Configure Avaya Aura® Session Manager

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.

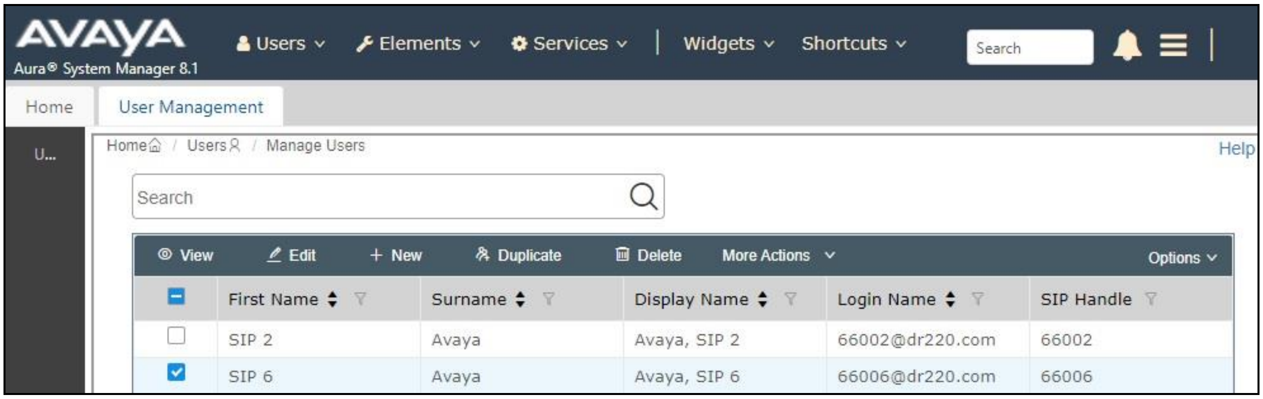
Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

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.

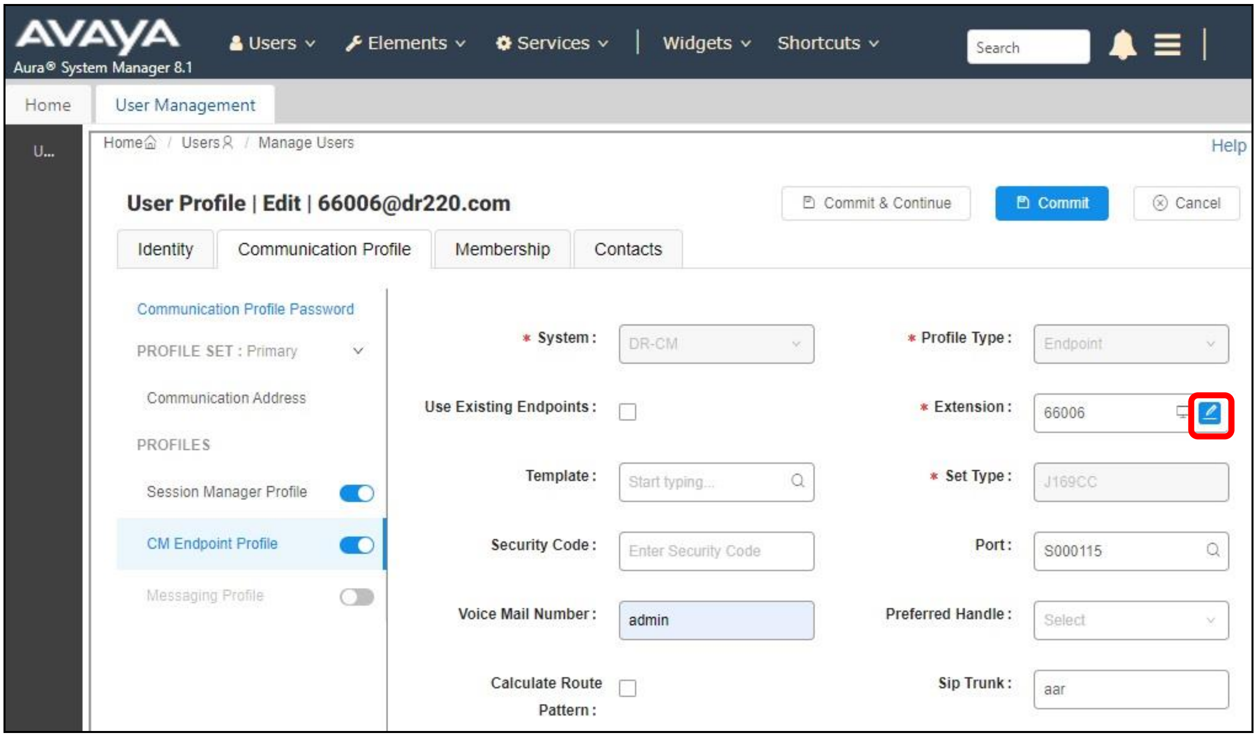
Select the entry associated with the first SIP agent station from **Section 3**, in this case "**66006**", and click **Edit**.



	First Name	Surname	Display Name	Login Name	SIP Handle
☐	SIP 2	Avaya	Avaya, SIP 2	66002@dr220.com	66002
☑	SIP 6	Avaya	Avaya, SIP 6	66006@dr220.com	66006

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

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



User Profile | Edit | 66006@dr220.com

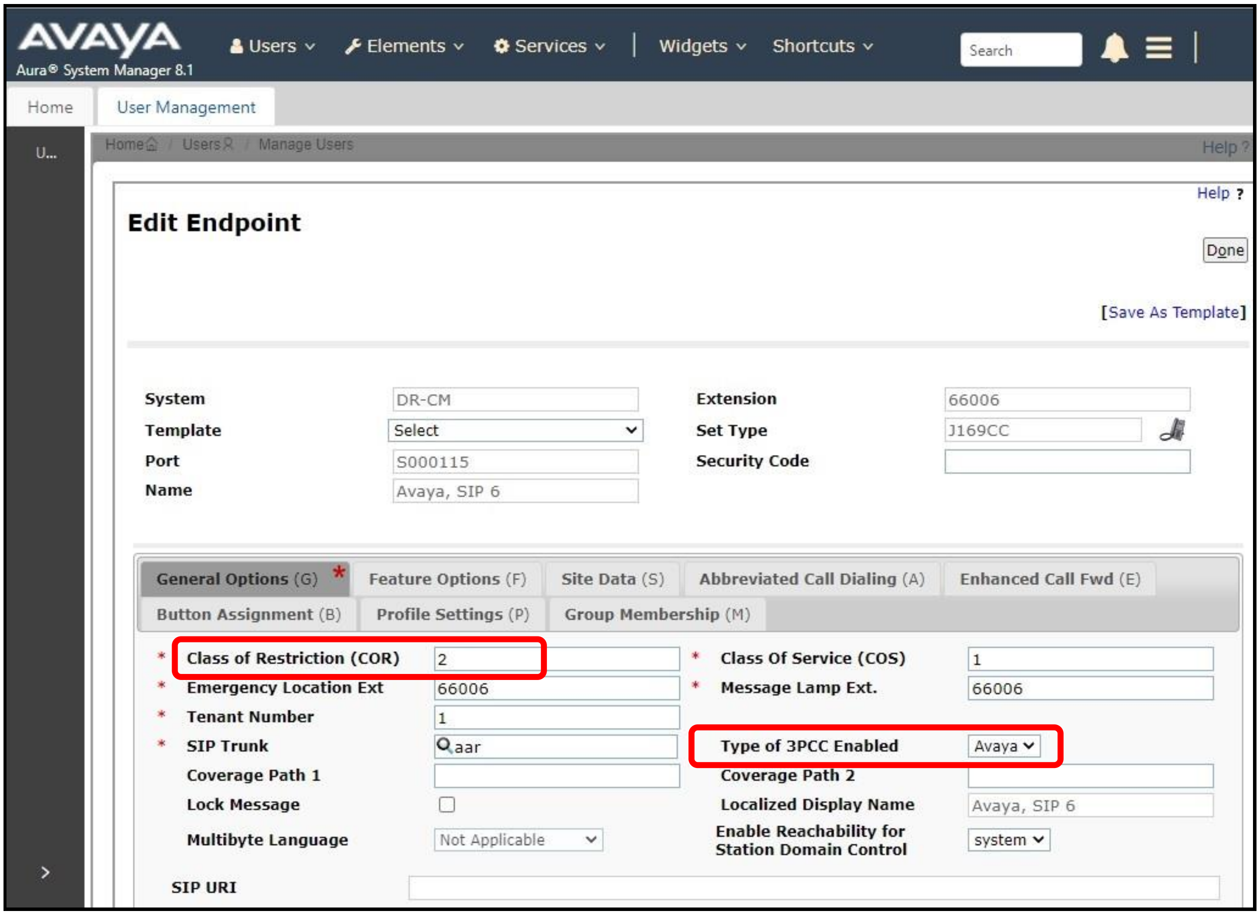
Identity | Communication Profile | Membership | Contacts

* System :	DR-CM	* Profile Type :	Endpoint
Use Existing Endpoints :	□	* Extension :	66006
Template :	Start typing...	* Set Type :	J169CC
Security Code :	Enter Security Code	Port :	S000115
Voice Mail Number :	admin	Preferred Handle :	Select
Calculate Route Pattern :	□	Sip Trunk :	aar

The **Edit Endpoint** pop-up screen is displayed. For **Class of Restriction (COR)**, enter the COR number from **Section 5.6**.

For **Type of 3PCC Enabled**, select "**Avaya**" as shown below.

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



Edit Endpoint

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

* Class of Restriction (COR)	2	* Class Of Service (COS)	1
* Emergency Location Ext	66006	* Message Lamp Ext.	66006
* Tenant Number	1		
* SIP Trunk	aar	Type of 3PCC Enabled	Avaya
Coverage Path 1		Coverage Path 2	
Lock Message	□	Localized Display Name	Avaya, SIP 6
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system
SIP URI			

8. Configure OpenText Qfiniti

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

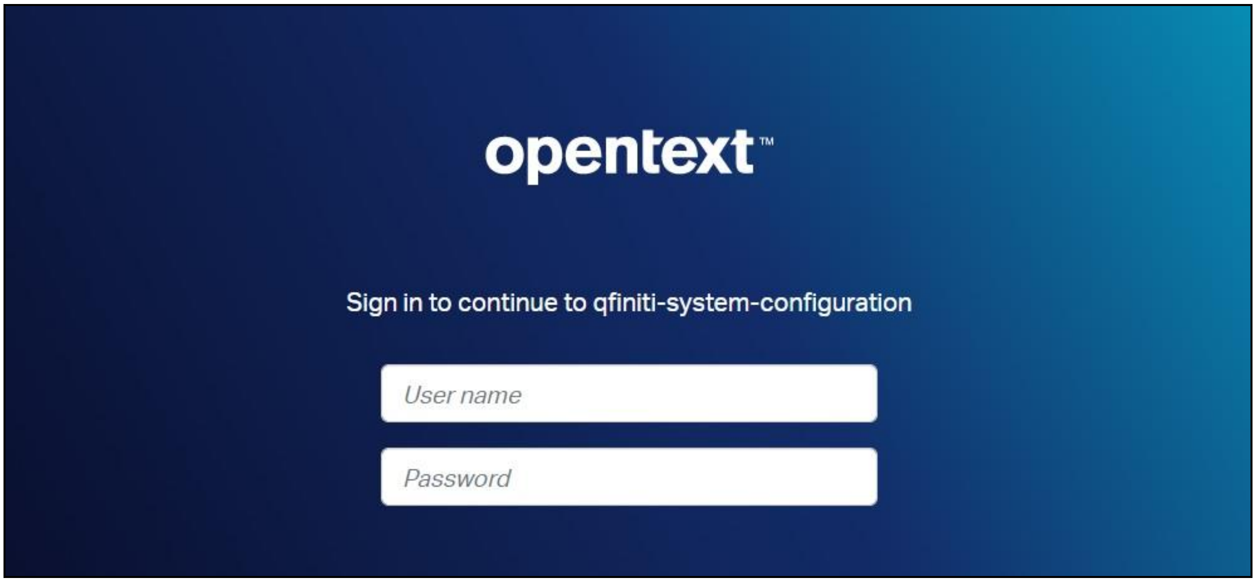
- Launch SysConfig web interface
- Administer switches
- Administer CTI server
- Administer board configuration
- Administer general
- Administer machines
- Administer components
- Administer CTI sources
- Administer phone interface
- Administer logging data – phone class of service
- Administer VRM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

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

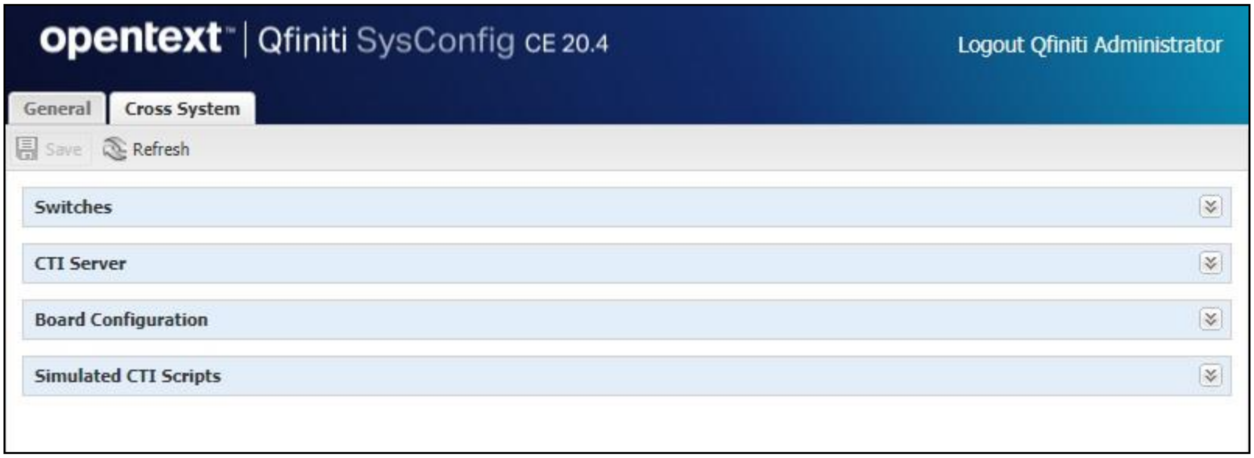
8.1. Launch SysConfig Web Interface

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

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



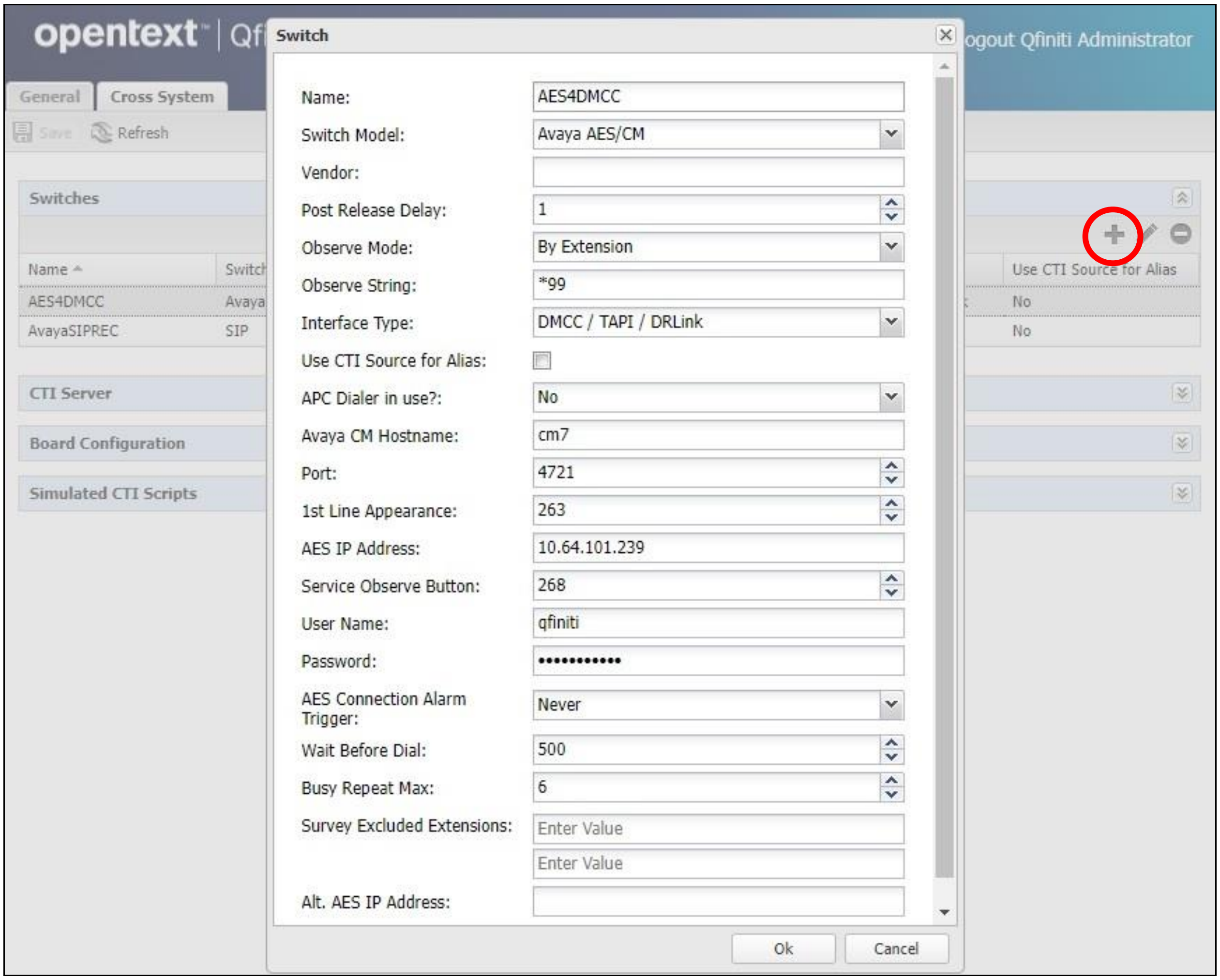
In the subsequent screen, select the **Cross System** tab to display the screen below.



8.2. Administer Switches

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

- **Name:** A descriptive name, in this case "AES4DMCC".
- **Switch Model:** "Avaya AES/CM"
- **Post Release Delay:** Desired wait interval in seconds for registration response.
- **Observe Mode:** "By Extension"
- **Observe String:** The pertinent feature access code from **Section 5.5**.
- **Interface Type:** "DMCC / TAPI / DRLink"
- **Avaya CM Hostname:** The relevant switch connection name from **Section 6.3**.
- **AES IP Address:** The IP address of Application Enablement Services server.
- **User Name:** The Qfiniti user credentials from **Section 6.5**.
- **Password:** The Qfiniti user credentials from **Section 6.5**.



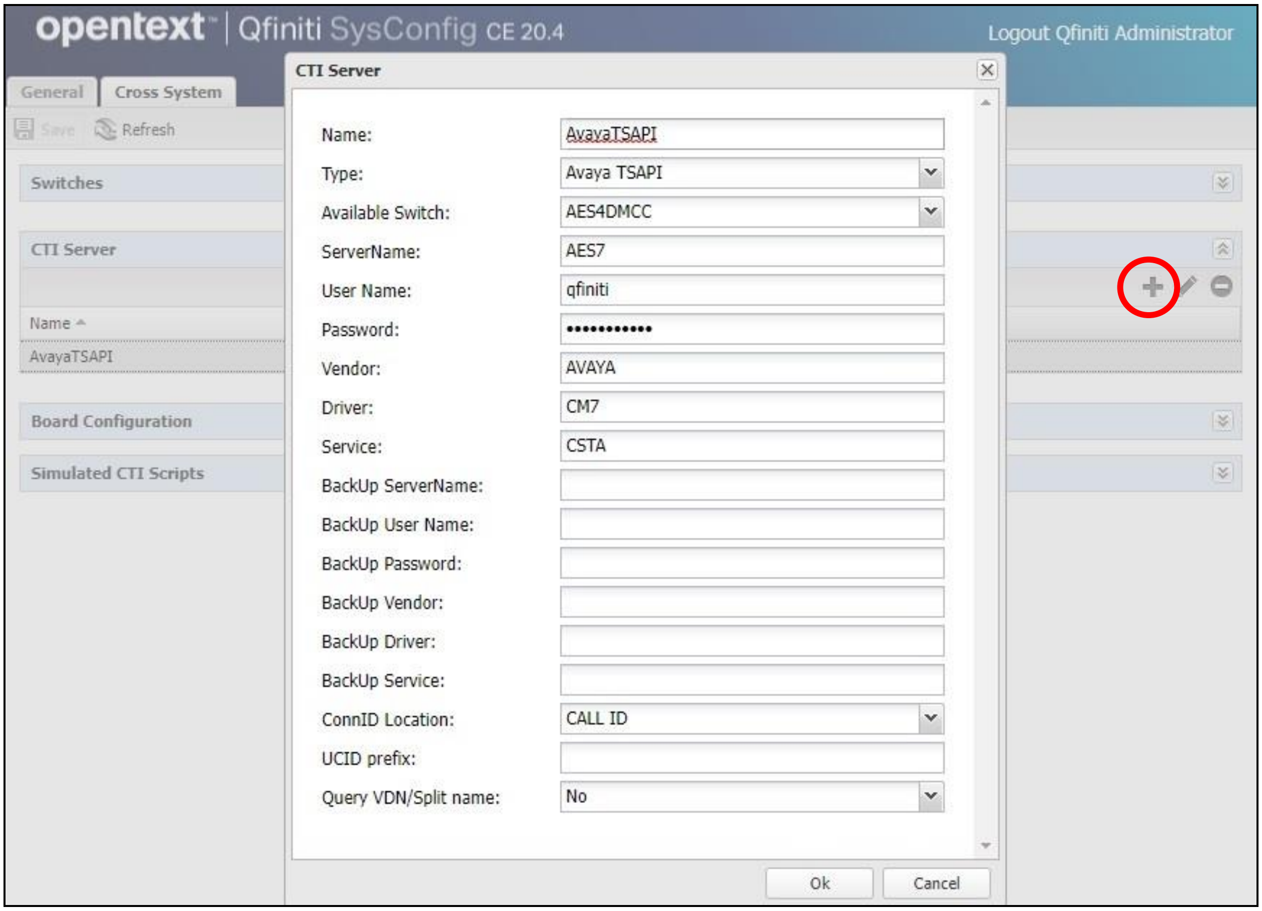
Switch

Name:	AES4DMCC
Switch Model:	Avaya AES/CM
Vendor:	
Post Release Delay:	1
Observe Mode:	By Extension
Observe String:	*99
Interface Type:	DMCC / TAPI / DRLink
Use CTI Source for Alias:	□
APC Dialer in use?:	No
Avaya CM Hostname:	cm7
Port:	4721
1st Line Appearance:	263
AES IP Address:	10.64.101.239
Service Observe Button:	268
User Name:	qfiniti
Password:	●●●●●●●●●●●
AES Connection Alarm Trigger:	Never
Wait Before Dial:	500
Busy Repeat Max:	6
Survey Excluded Extensions:	Enter Value Enter Value
Alt. AES IP Address:	

8.3. Administer CTI Server

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

- **Name:** A descriptive name, in this case "AvayaTSAPI".
- **Type:** "Avaya TSAPI"
- **Available Switch:** Select the switch name from **Section 8.2**.
- **ServerName:** The host name of Application Enablement Services.
- **User Name:** The Qfiniti user credentials from **Section 6.5**.
- **Password:** The Qfiniti user credentials from **Section 6.5**.
- **Vendor:** "AVAYA"
- **Driver:** The relevant switch connection name from **Section 6.3**.
- **Service:** "CSTA"



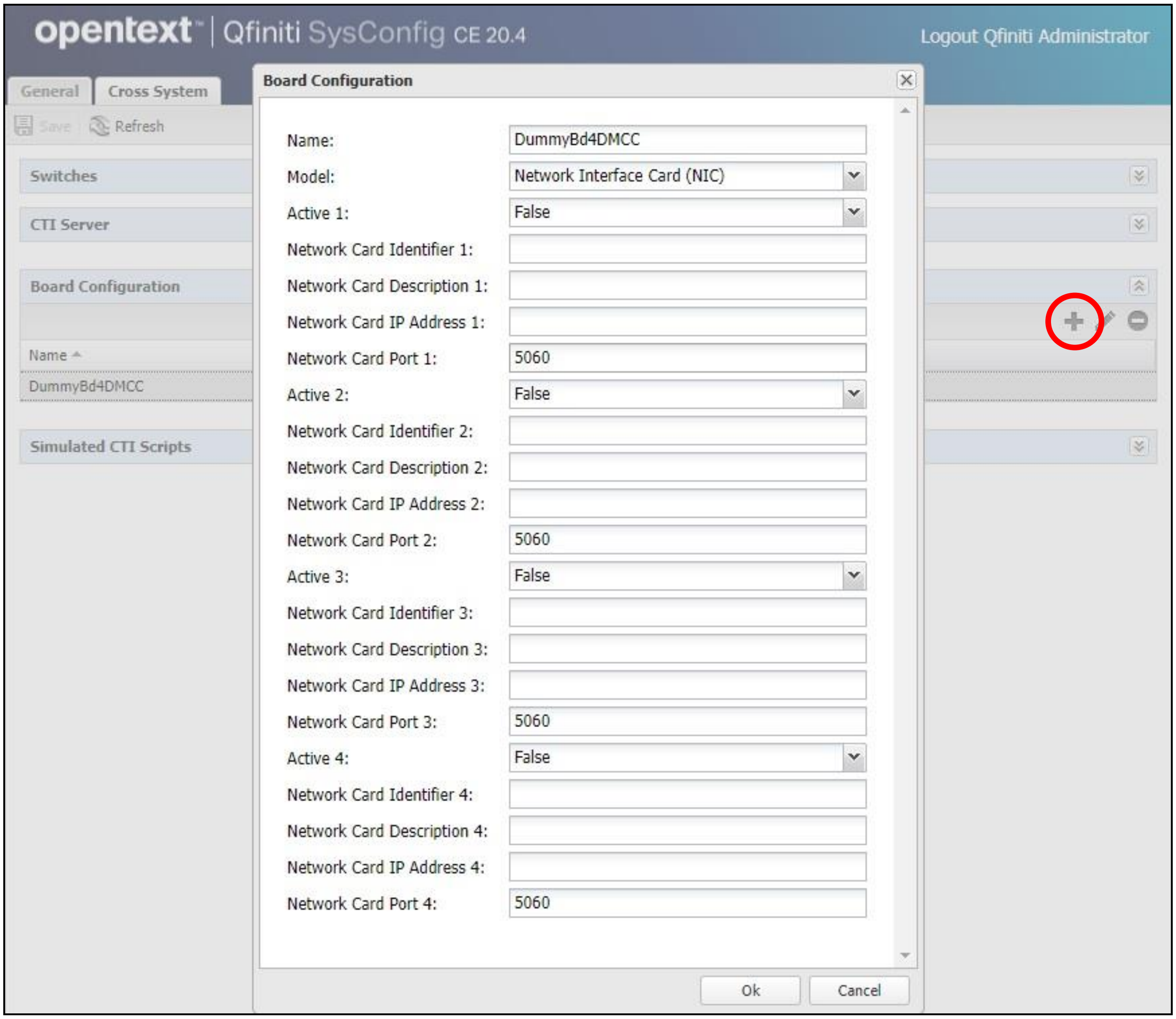
CTI Server

Name:	AvayaTSAPI
Type:	Avaya TSAPI
Available Switch:	AES4DMCC
ServerName:	AES7
User Name:	qfiniti
Password:	•••••••••••
Vendor:	AVAYA
Driver:	CM7
Service:	CSTA
BackUp ServerName:	
BackUp User Name:	
BackUp Password:	
BackUp Vendor:	
BackUp Driver:	
BackUp Service:	
ConnID Location:	CALL ID
UCID prefix:	
Query VDN/Split name:	No

8.4. Administer Board Configuration

Expand the **Board Configuration** sub-section and click the **New Item** icon. Note that board is not used in the integration but required to be configured. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name, in this case "DummyBd4DMCC".
- **Model:** "Network Interface Card (NIC)"



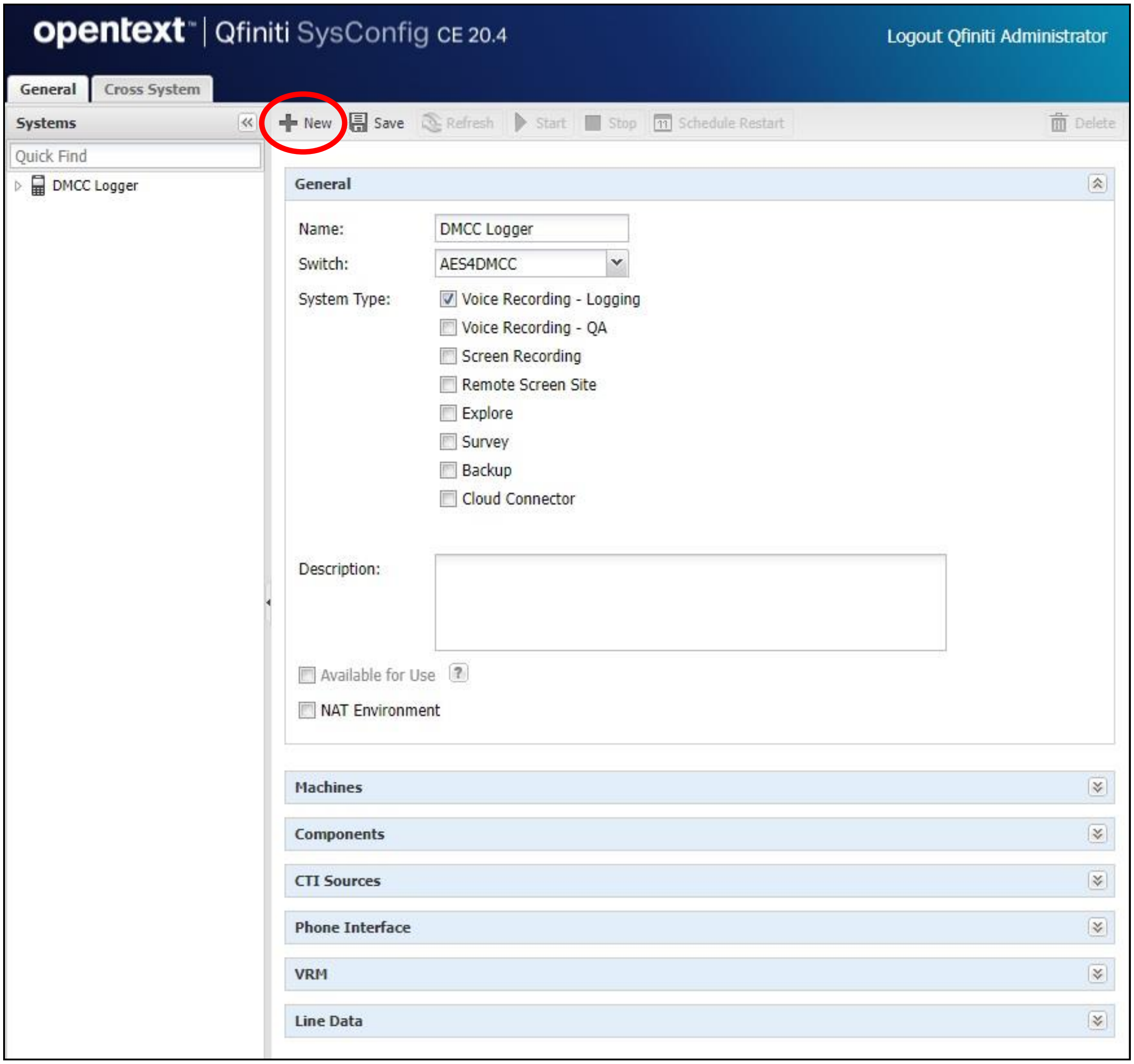
Board Configuration

Name:	DummyBd4DMCC
Model:	Network Interface Card (NIC)
Active 1:	False
Network Card Identifier 1:	
Network Card Description 1:	
Network Card IP Address 1:	
Network Card Port 1:	5060
Active 2:	False
Network Card Identifier 2:	
Network Card Description 2:	
Network Card IP Address 2:	
Network Card Port 2:	5060
Active 3:	False
Network Card Identifier 3:	
Network Card Description 3:	
Network Card IP Address 3:	
Network Card Port 3:	5060
Active 4:	False
Network Card Identifier 4:	
Network Card Description 4:	
Network Card IP Address 4:	
Network Card Port 4:	5060

8.5. Administer General

Select the **General** tab. Expand the **General** sub-section and click the **New** icon to add a new system. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A desired name, in this case "DMCC Logger".
- **Switch:** Select the switch name from **Section 8.2**.
- **System Type:** Check **Voice Recording - Logging**.

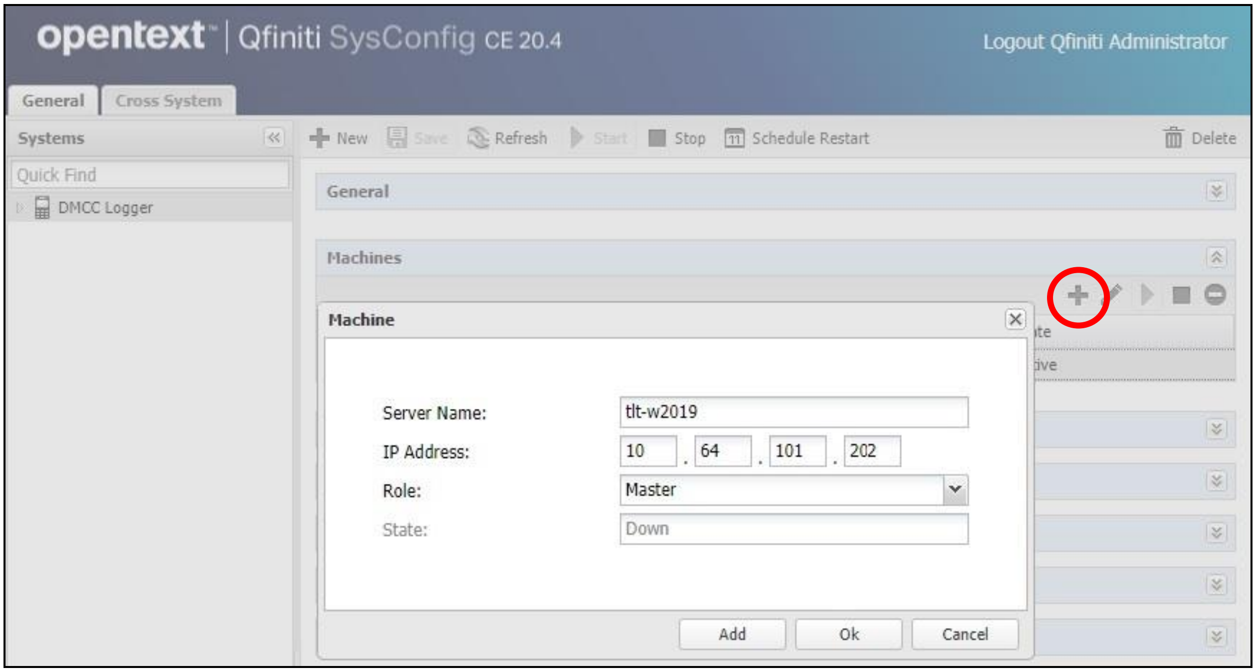


Name: DMCC Logger
Switch: AES4DMCC
System Type:
☑ Voice Recording - Logging
☐ Voice Recording - QA
☐ Screen Recording
☐ Remote Screen Site
☐ Explore
☐ Survey
☐ Backup
☐ Cloud Connector
Description:
☐ Available for Use
☐ NAT Environment

8.6. Administer Machines

Expand the **Machines** sub-section and click the **New Item** icon to add a new machine. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Server Name:** The host name of the Qfiniti server.
- **IP Address:** The IP address of the Qfiniti server.
- **Role:** "Master".

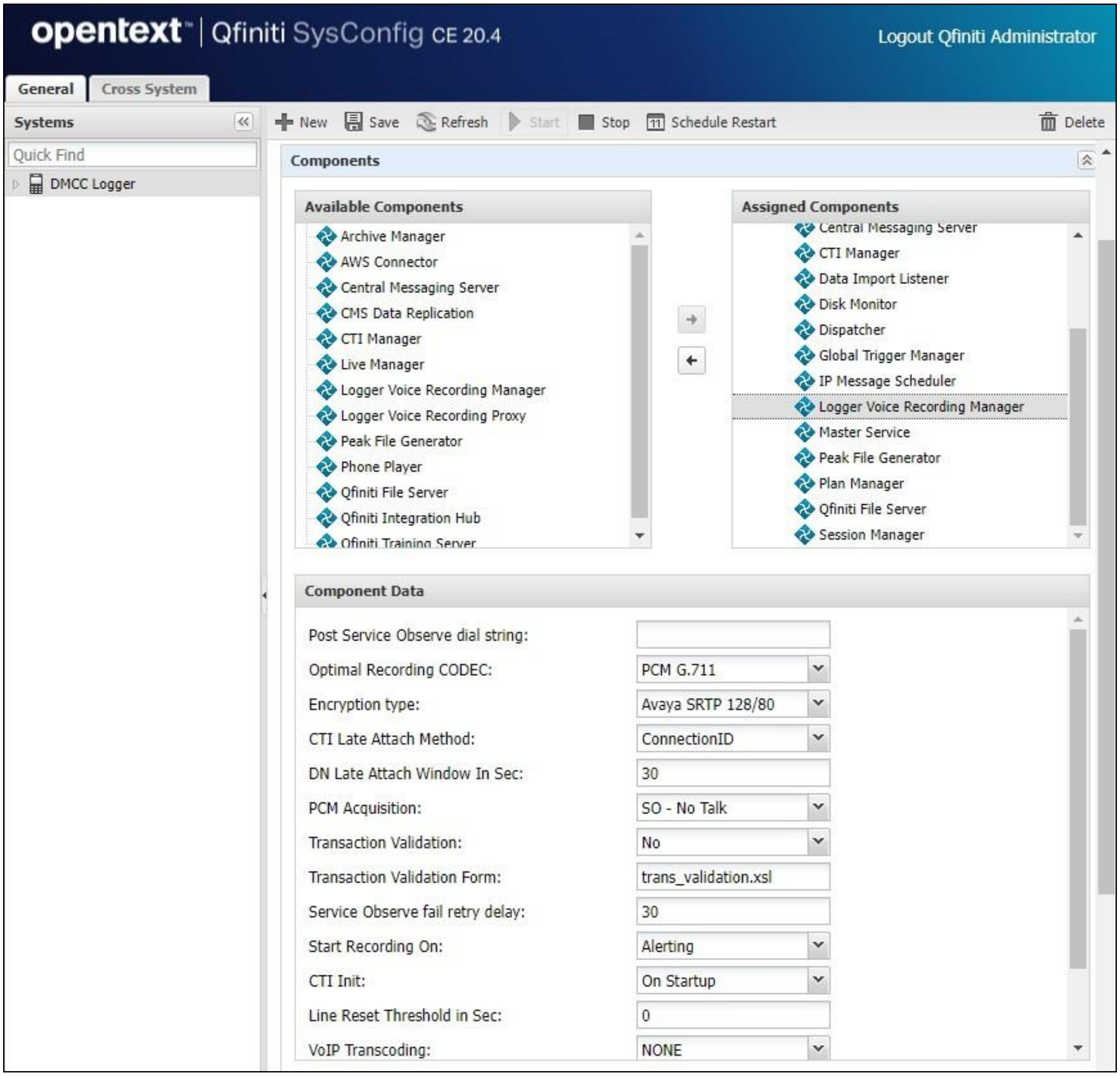


Server Name: tlt-w2019
IP Address: 10 . 64 . 101 . 202
Role: Master
State: Down

8.7. Administer Components

Expand the **Components** sub-section and follow reference [**4**] to assign and configure the required components. Under **Assigned Components**, select **Logger Voice Recording Manager**. Under **Component Data**, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Optimal Recording CODEC:** Select the pertinent codec, in this case "PCM G.711".
- **Encryption type:** "Avaya SRTP 128/80"
- **PCM Acquisition:** "SO – No Talk"

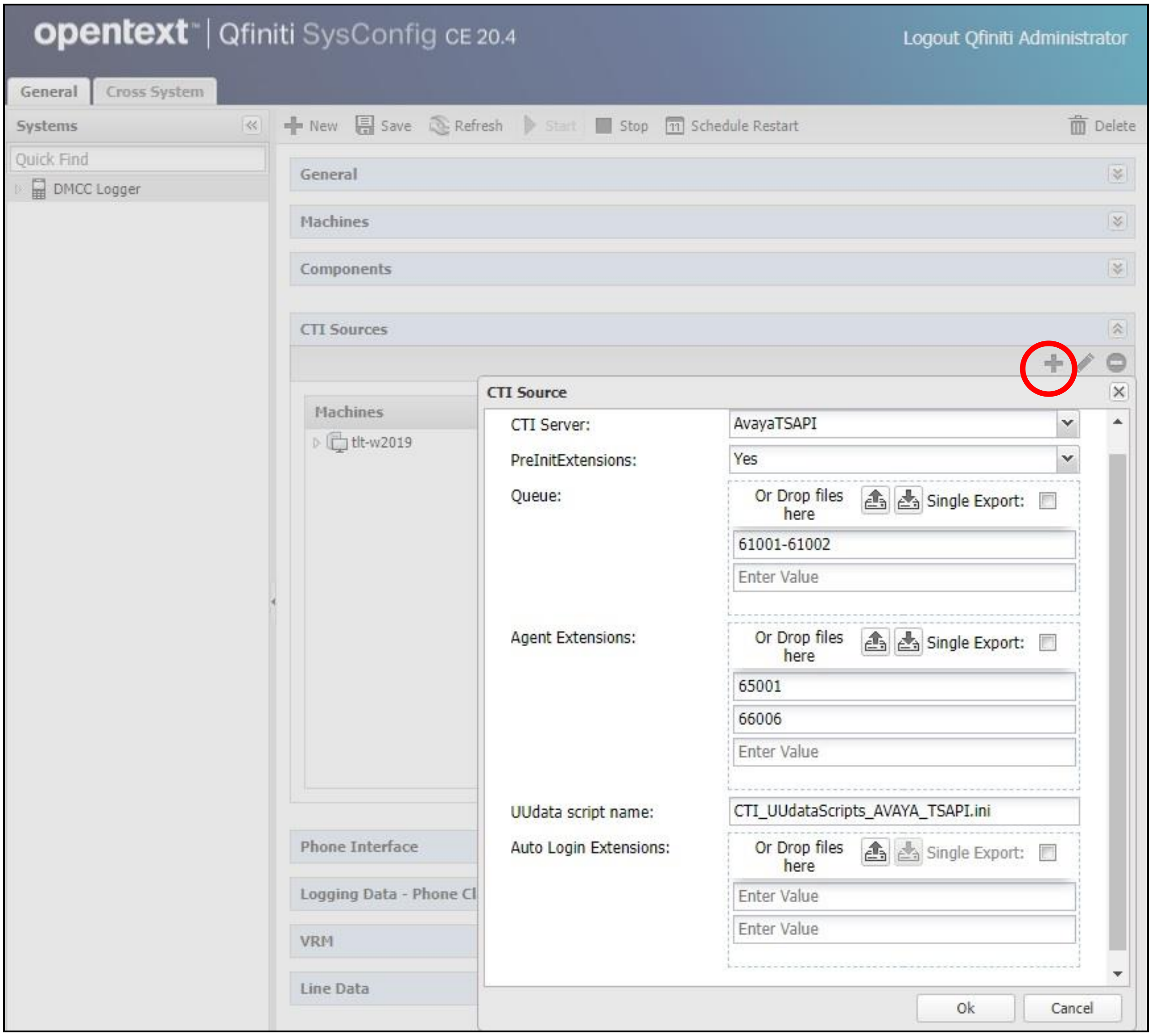


Post Service Observe dial string:	
Optimal Recording CODEC:	PCM G.711
Encryption type:	Avaya SRTP 128/80
CTI Late Attach Method:	ConnectionID
DN Late Attach Window In Sec:	30
PCM Acquisition:	SO - No Talk
Transaction Validation:	No
Transaction Validation Form:	trans_validation.xsl
Service Observe fail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

8.8. Administer CTI Sources

Expand the **CTI Sources** sub-section. Select the applicable machine server name from **Section 8.6**, followed by the **Add CTI Source** icon. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **CTI Server:** Select the CTI server name from **Section 8.3**.
- **Queue:** The skill group extensions from **Section 3**.
- **Agent Extensions:** The agent station extensions from **Section 3**.



CTI Server: AvayaTSAPI

PreInitExtensions: Yes

Queue: 61001-61002

Agent Extensions: 65001, 66006

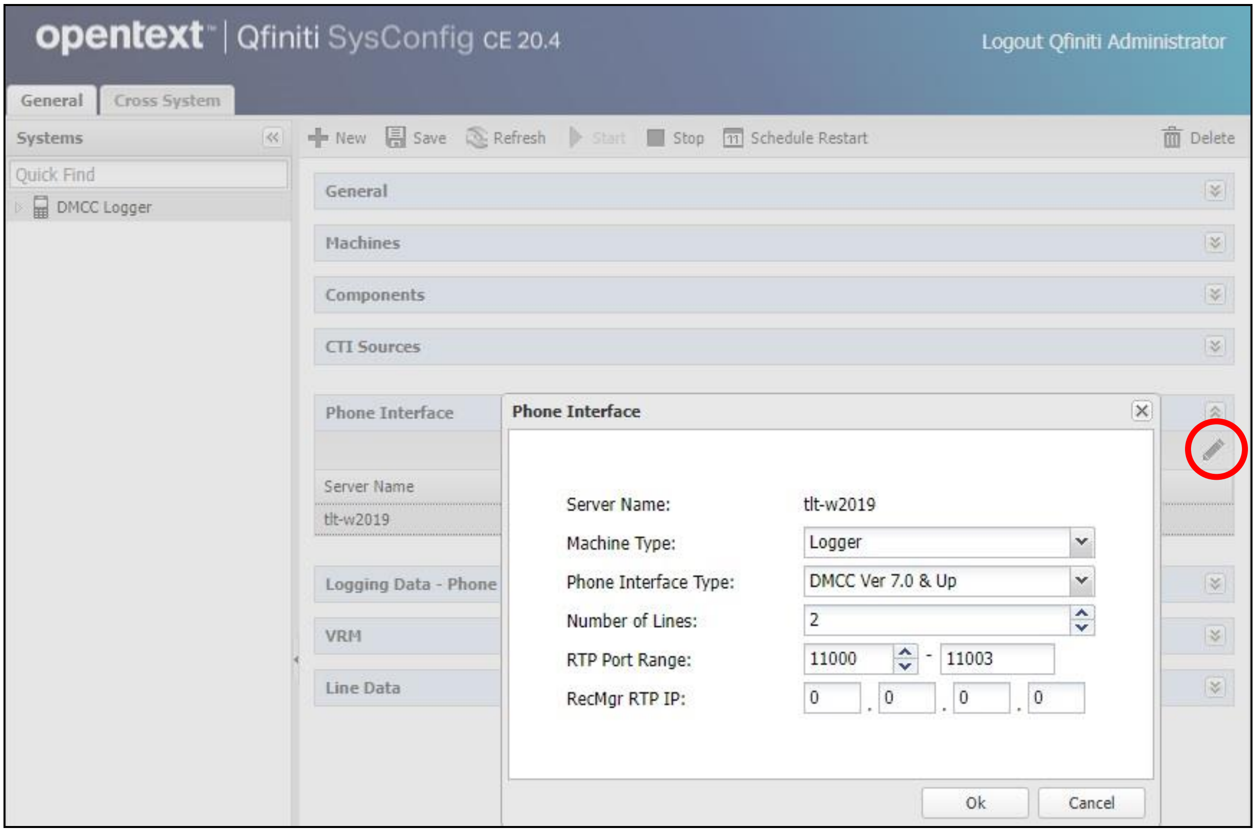
UUdata script name: CTI_UUdataScripts_AVAYA_TSAPI.ini

Auto Login Extensions:

8.9. Administer Phone Interface

Expand the **Phone Interface** sub-section (not shown). Select the machine server name from **Section 8.6**, and click on the **Edit** icon to edit the entry. Enter the following values for the specified fields and retain the default values for the remaining fields.

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



Phone Interface

Server Name
tlt-w2019

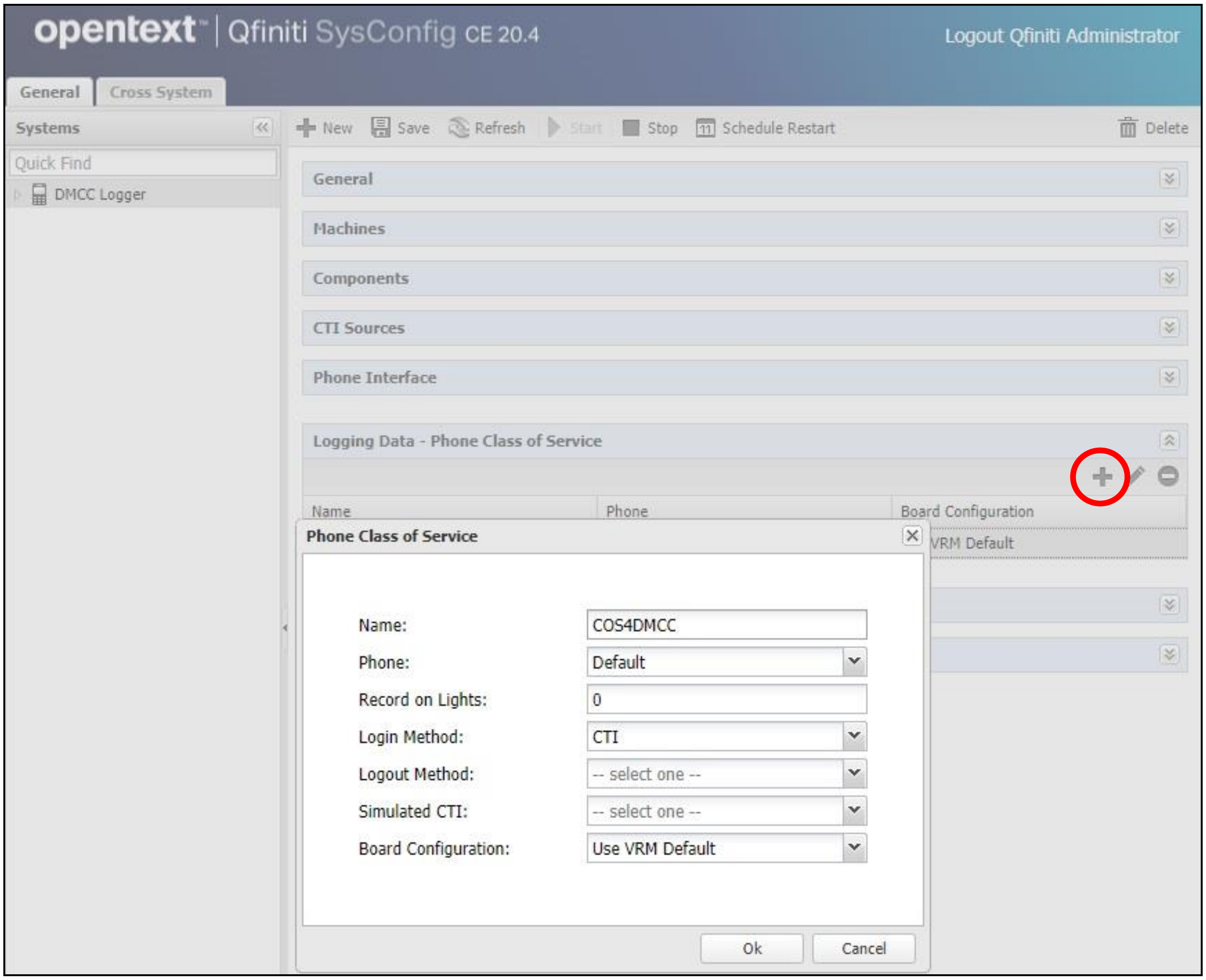
Phone Interface

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

8.10. Administer Logging Data – Phone Class of Service

Expand the **Logging Data** – **Phone Class of Service** sub-section. Select the **New Item** icon. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A desired name, in this case "COS4DMCC".
- **Phone:** "Default"
- **Record on lights:** "0"
- **Login Method:** "CTI".



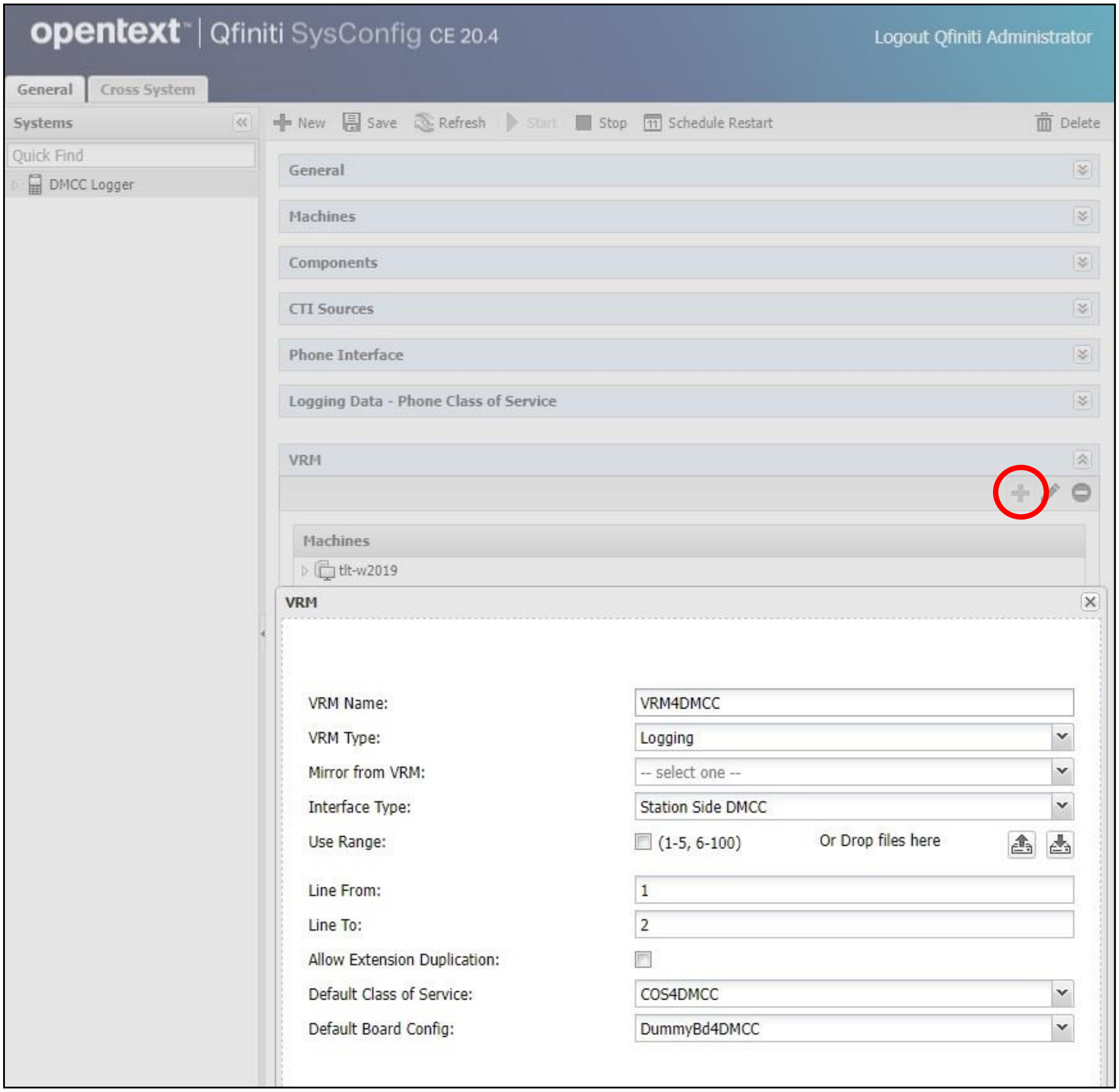
Phone Class of Service

Name:	COS4DMCC
Phone:	Default
Record on Lights:	0
Login Method:	CTI
Logout Method:	-- select one --
Simulated CTI:	-- select one --
Board Configuration:	Use VRM Default

8.11. Administer VRM

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

- **VRM Name:** A desired name, in this case “VRM4DMCC”.
- **VRM Type:** “Logging”
- **Interface Type:** “Station Side DMCC”
- **Line From** and **Line To:** Range of agent stations, in this case two stations so “1” to “2”.
- **Default Class of Service:** Select the phone class of service name from **Section 8.10**.
- **Default Board Config:** Select the board name from **Section 8.4**.

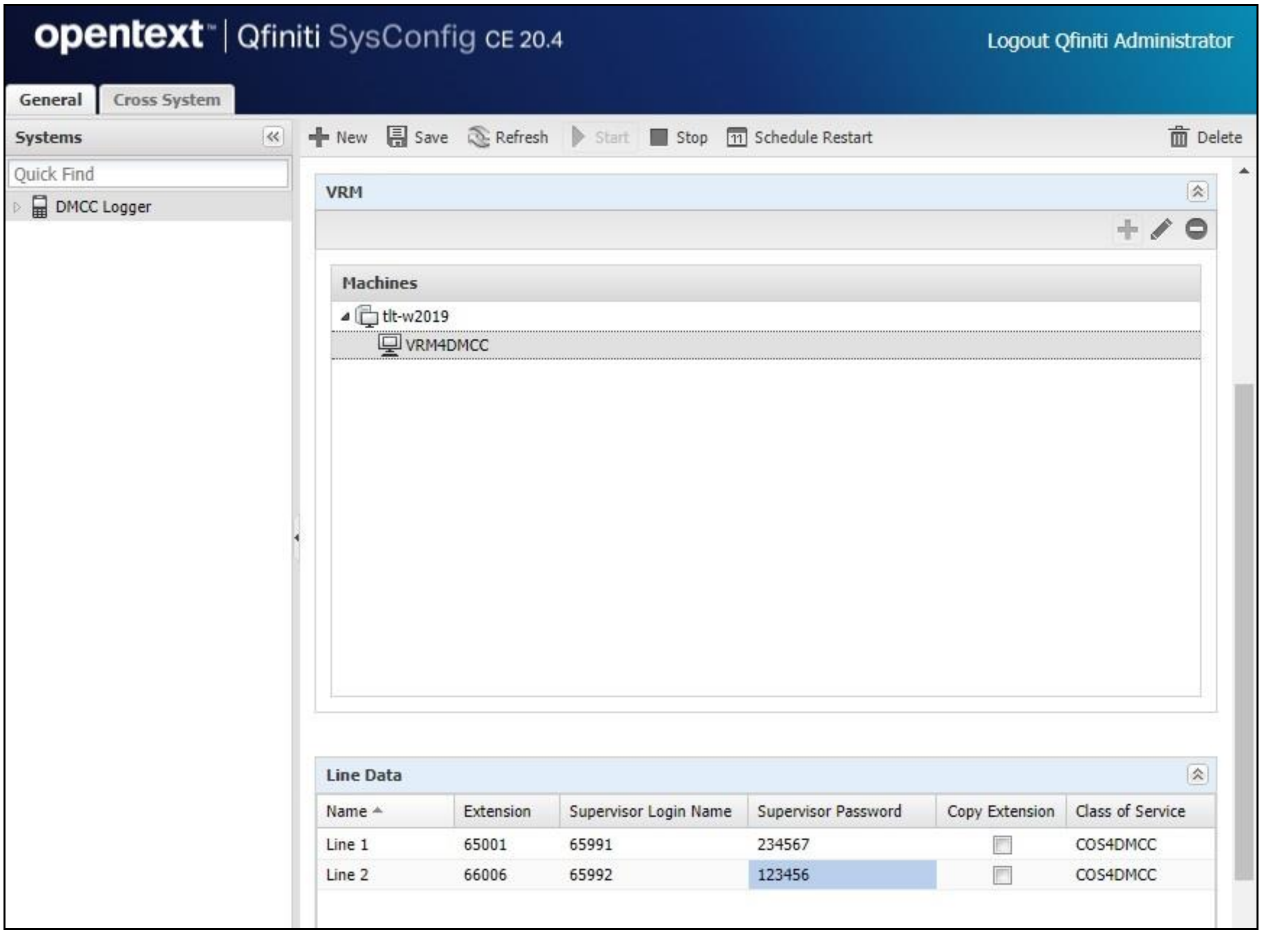


VRM Name: VRM4DMCC
VRM Type: Logging
Mirror from VRM: -- select one --
Interface Type: Station Side DMCC
Use Range: □ (1-5, 6-100) Or Drop files here
Line From: 1
Line To: 2
Allow Extension Duplication: □
Default Class of Service: COS4DMCC
Default Board Config: DummyBd4DMCC

8.12. Administer Line Data

Select the newly added VRM from **Section 8.11**, and expand the **Line Data** sub-section. Select the first line. For **Extension**, enter the first agent station extension from **Section 3**. For **Supervisor Login Name** and **Supervisor Password**, enter the first virtual IP softphone extension and associated security code from **Section 5.8** respectively.

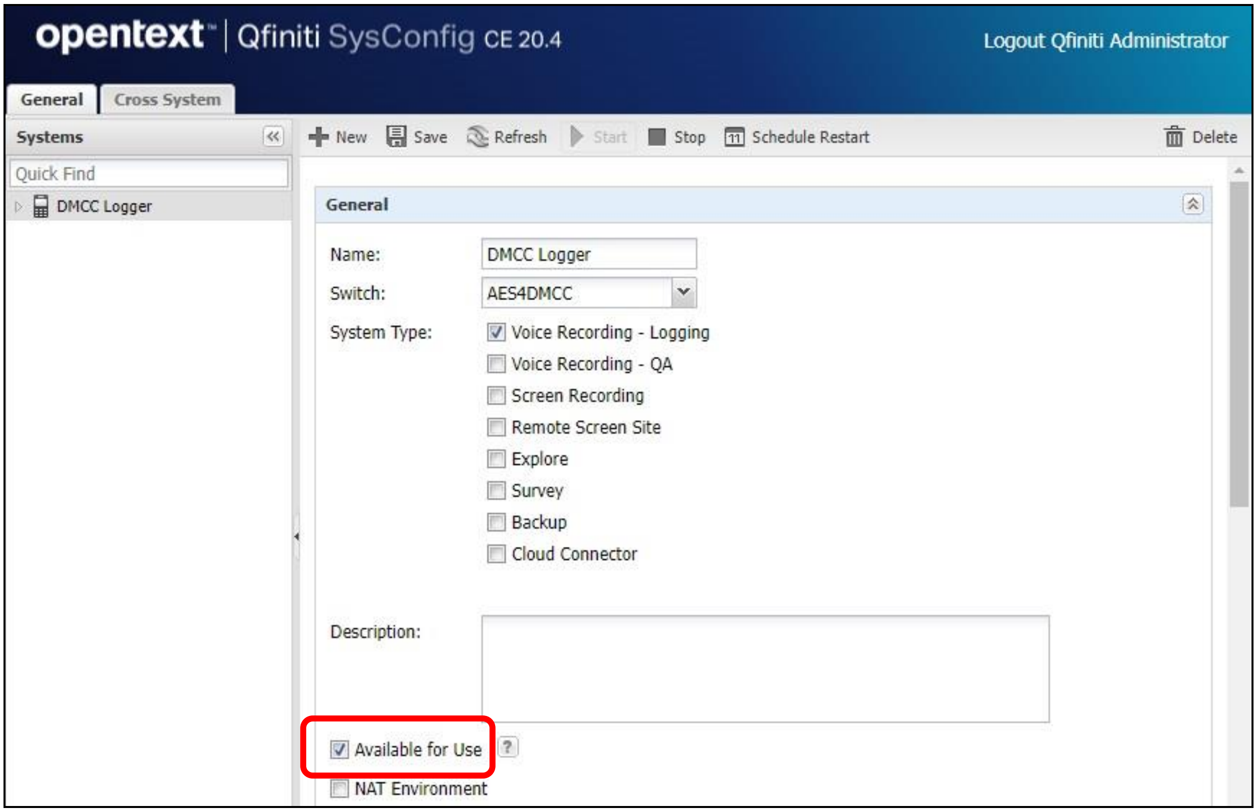
Repeat this section to administer all lines, as shown below.



Name	Extension	Supervisor Login Name	Supervisor Password	Copy Extension	Class of Service
Line 1	65001	65991	234567	□	COS4DMCC
Line 2	66006	65992	123456	□	COS4DMCC

8.13. Enable Use

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



Name: DMCC Logger

Switch: AES4DMCC

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

Description:

☑ Available for Use
□ NAT Environment

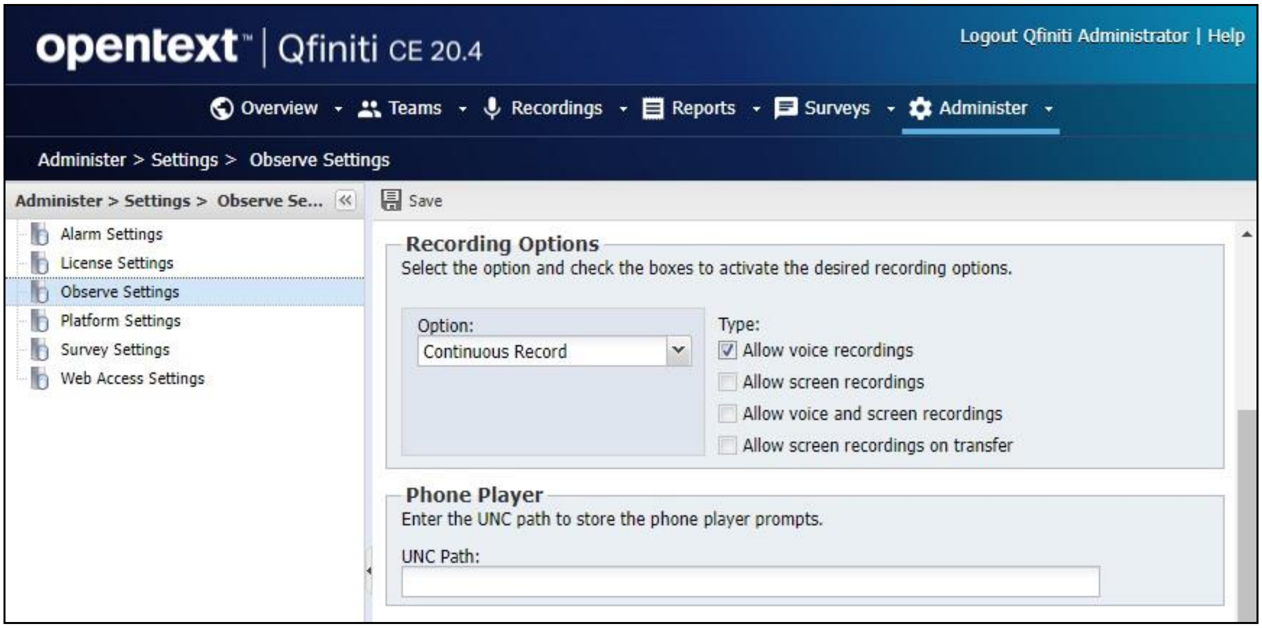
8.14. Launch Qfiniti Web Interface

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

8.15. Administer Observe Settings

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

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



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

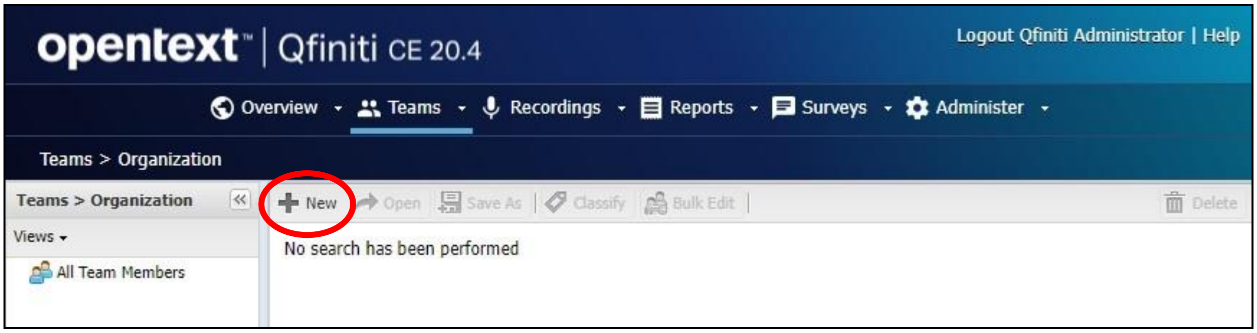
Phone Player

Enter the UNC path to store the phone player prompts.

UNC Path:

8.16. Administer Agents

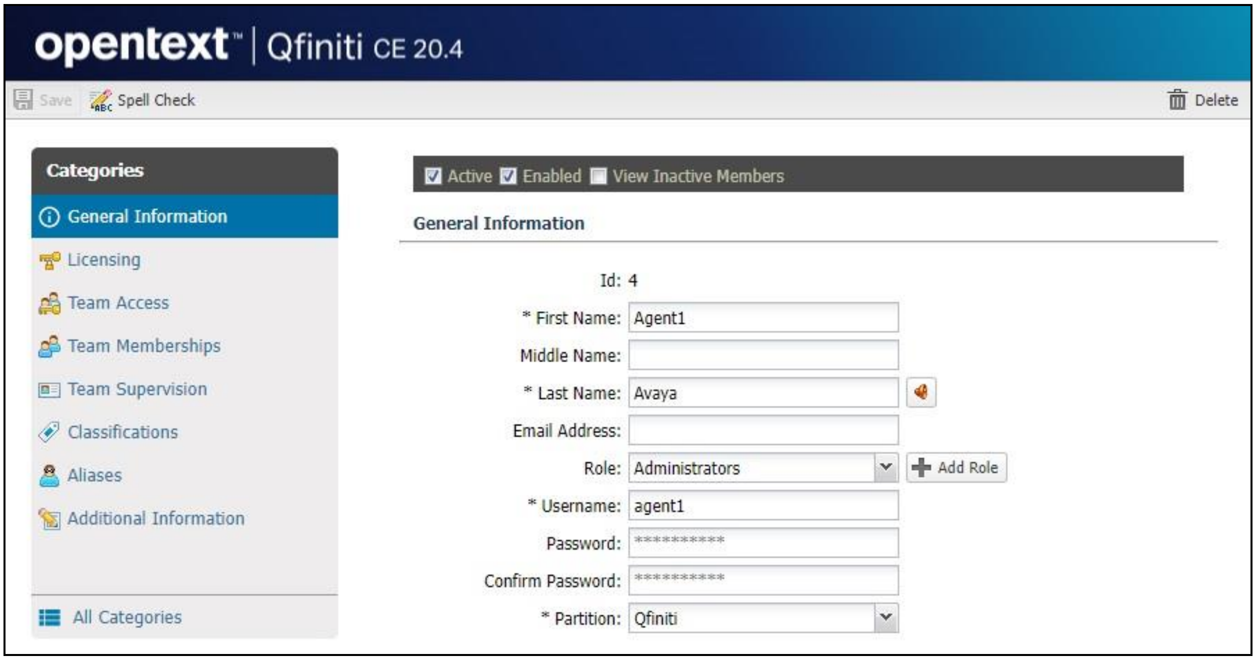
Select **Teams → Organization** from the top menu to display the screen below. Select the **New** icon in the right pane to add an agent.



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"

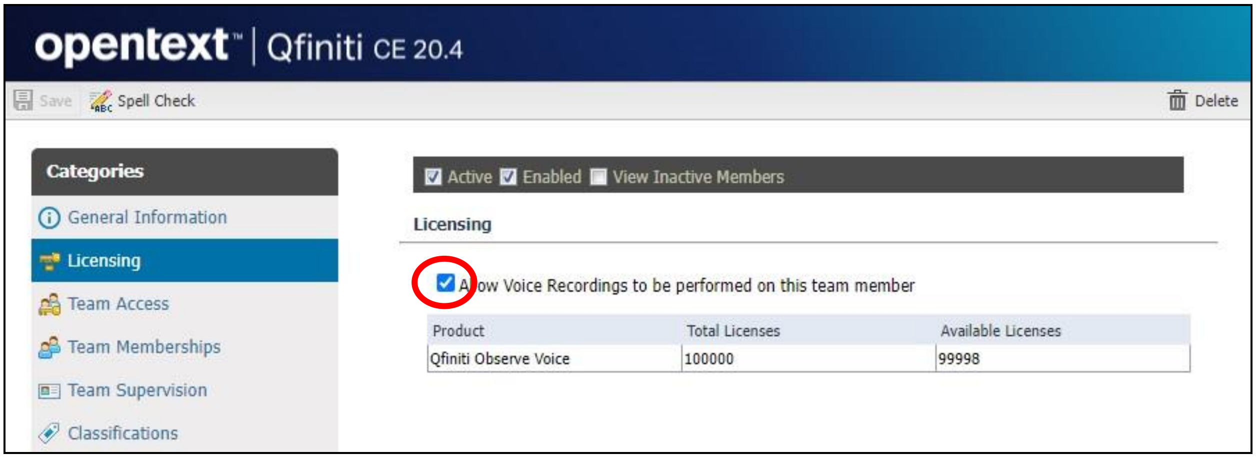


☑ Active ☑ Enabled □ View Inactive Members

General Information

Id:	4
* First Name:	Agent1
Middle Name:	
* Last Name:	Avaya
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.



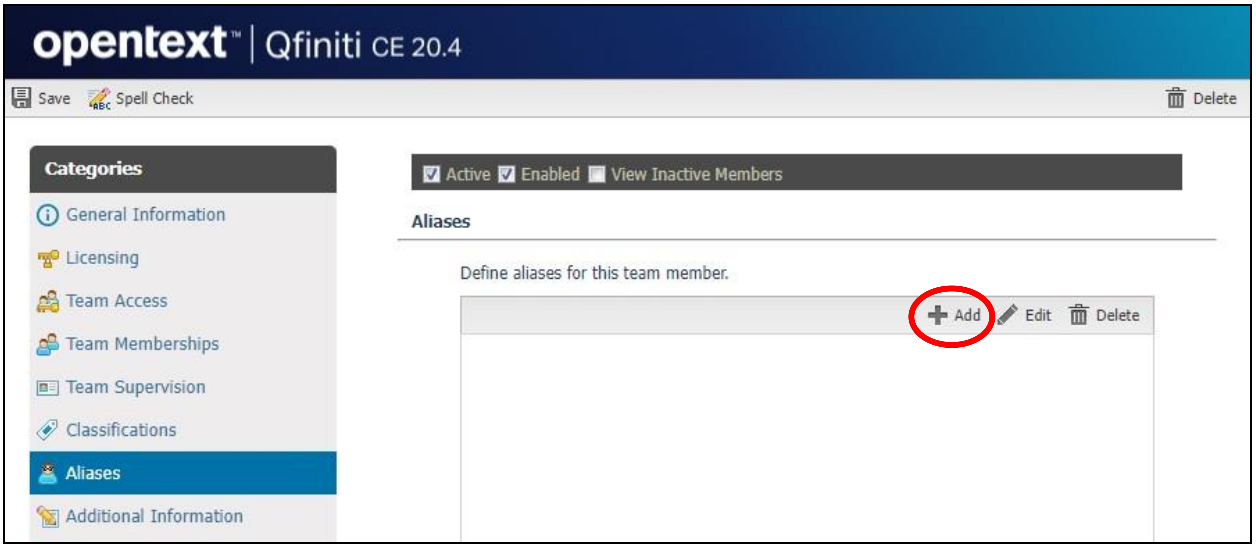
☑ Active ☑ Enabled □ View Inactive Members

Licensing

☑ Allow Voice Recordings to be performed on this team member

Product	Total Licenses	Available Licenses
Qfiniti Observe Voice	100000	99998

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

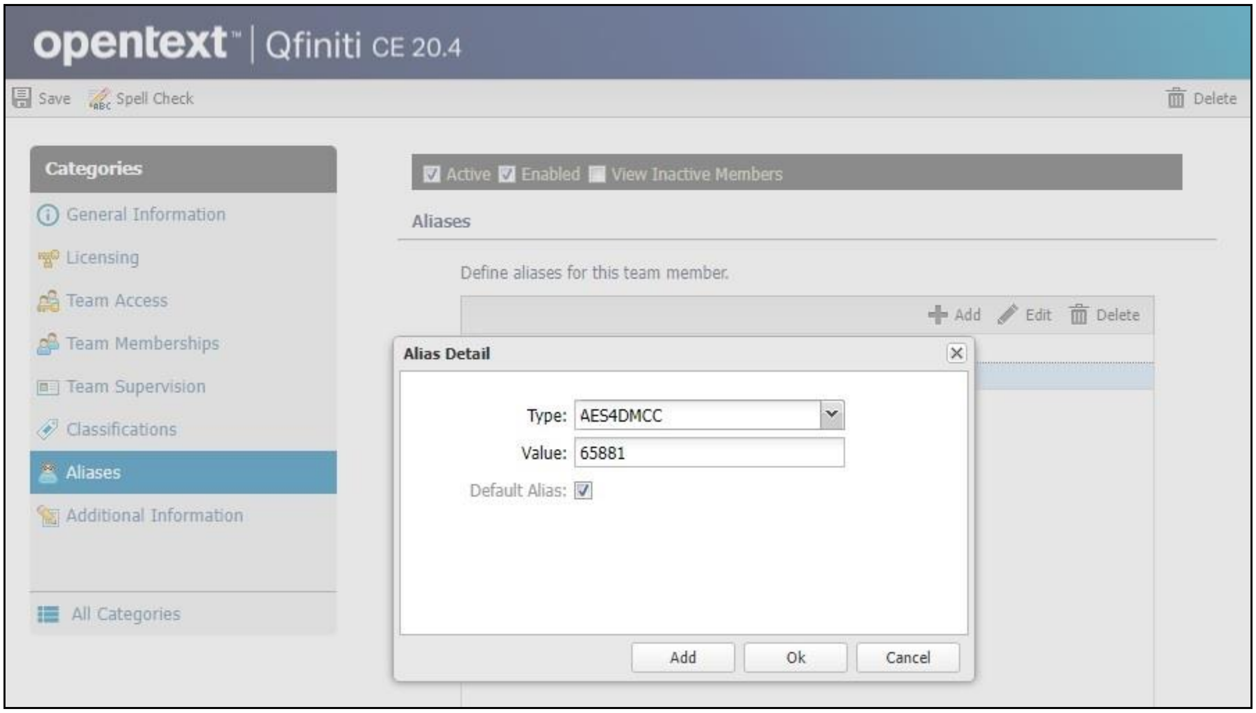


☑ Active ☑ Enabled □ View Inactive Members

Aliases

Define aliases for this team member.

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

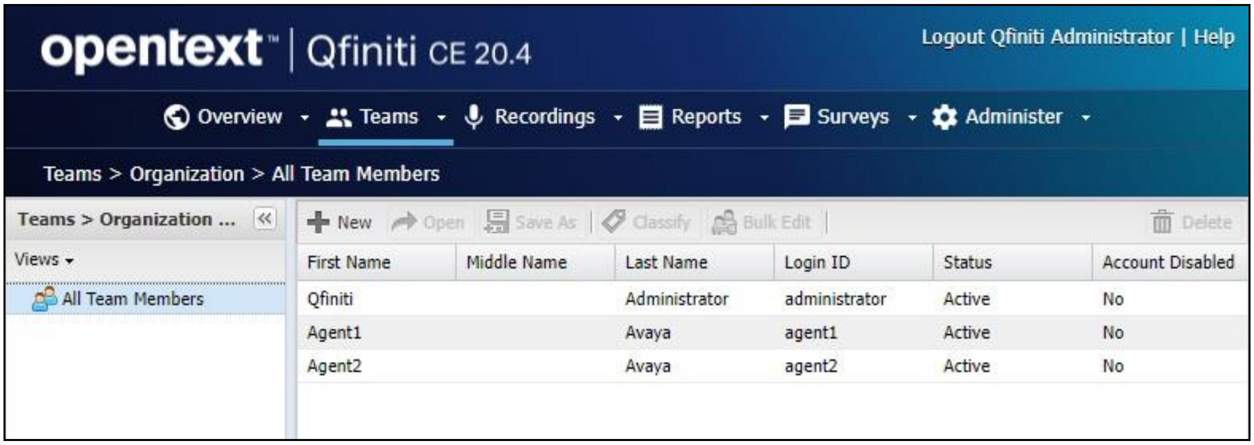


Type: AES4DMCC

Value: 65881

Default Alias: ☑

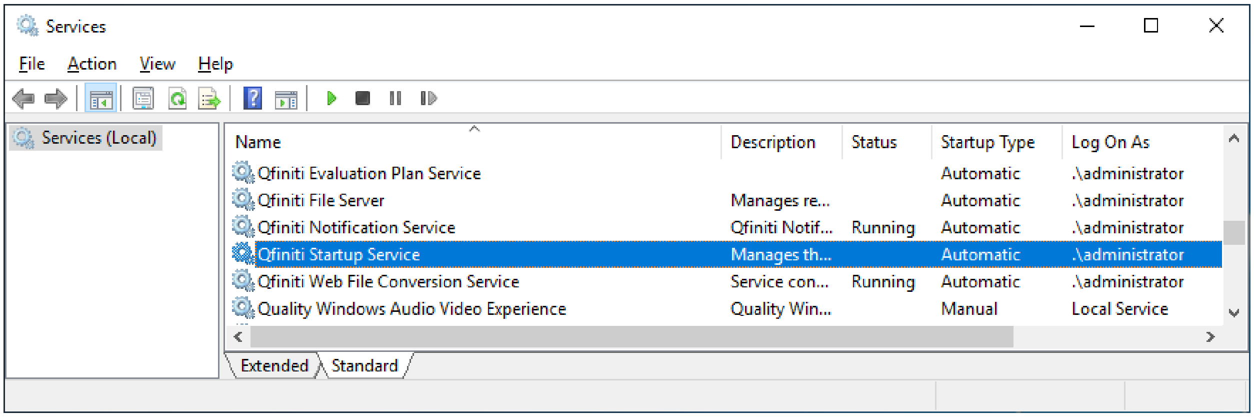
Repeat this section to add a team member for each agent from **Section 3**. In the compliance testing, two team members with alias values "**65881**" and "**65882**" were configured.



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

8.17. Start Services

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



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

9. Verification Steps

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

9.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify status of the administered CTI link by using the "**status aesvcs cti-link**" command. Verify that the **Service State** is "**established**" for the CTI link number administered in **Section 5.2**, as shown below.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

CTI   Version  Mnt   AE Services      Service       Msgs     Msgs
Link           Busy  Server           State         Sent     Rcvd

1     12       no    aes7             established   25       25
```

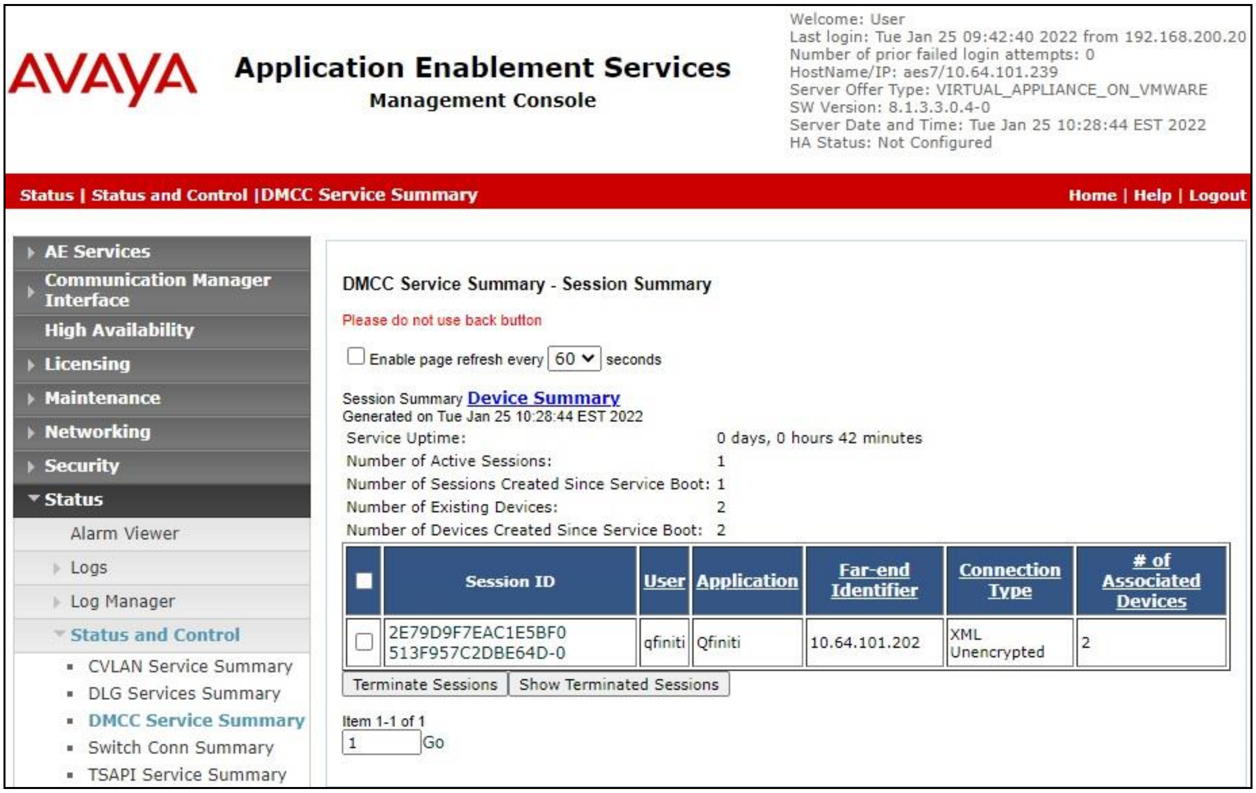
Verify registration status of the virtual IP softphones by using the "**list registered-ip-stations**" command. Verify that all virtual IP softphones from **Section 5.8** are displayed along with the IP address of the Application Enablement Services server, as shown below.

```
list registered-ip-stations

                            REGISTERED IP STATIONS

Station Ext       Set Type/ Prod ID/    Station IP Address/
or Orig Port      Net Rgn   Release     Gatekeeper IP Address
  Socket
65000             9611      IP_Phone    192.168.200.179
  tls             1         6.8502      10.64.101.236
65001             9611      IP_Phone    192.168.200.212
  tls             1         6.8502      10.64.101.236
65991             4620      IP_API_A    10.64.101.239
  tcp             1         3.2040      10.64.101.236
65992             4620      IP_API_A    10.64.101.239
  tcp             1         3.2040      10.64.101.236
```

9.2. Verify Avaya Aura® Application Enablement Services

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

Verify the **User** column shows an active session with the Qfiniti user name from **Section 6.5**, and that the **# of Associated Devices** column reflects the number of virtual IP softphones from **Section 5.8**, in this case "**2**", as shown below.



Welcome: User
Last login: Tue Jan 25 09:42:40 2022 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.3.0.4-0
Server Date and Time: Tue Jan 25 10:28:44 EST 2022
HA Status: Not Configured

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary Device Summary
Generated on Tue Jan 25 10:28:44 EST 2022

Service Uptime:	0 days, 0 hours 42 minutes
Number of Active Sessions:	1
Number of Sessions Created Since Service Boot:	1
Number of Existing Devices:	2
Number of Devices Created Since Service Boot:	2

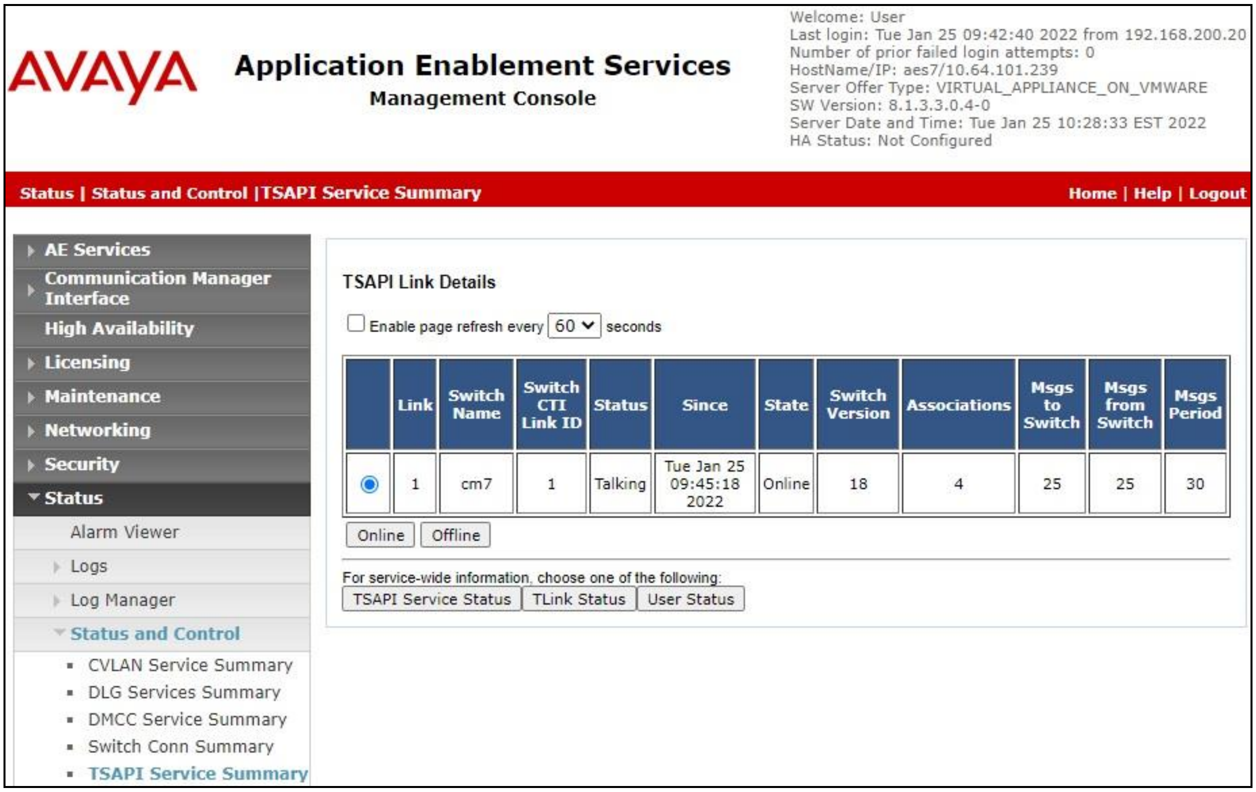
☐	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
☐	2E79D9F7EAC1E5BF0 513F957C2DBE64D-0	qfiniti	Qfiniti	10.64.101.202	XML Unencrypted	2

Terminate Sessions | Show Terminated Sessions

Item 1-1 of 1
1 Go

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

Verify that the **Status** is "**Talking**" for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the total number of monitored skill groups and agent stations from **Section 3**, in this case "**4**".



Welcome: User
Last login: Tue Jan 25 09:42:40 2022 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.3.0.4-0
Server Date and Time: Tue Jan 25 10:28:33 EST 2022
HA Status: Not Configured

TSAPI Link Details

☐ Enable page refresh every 60 seconds

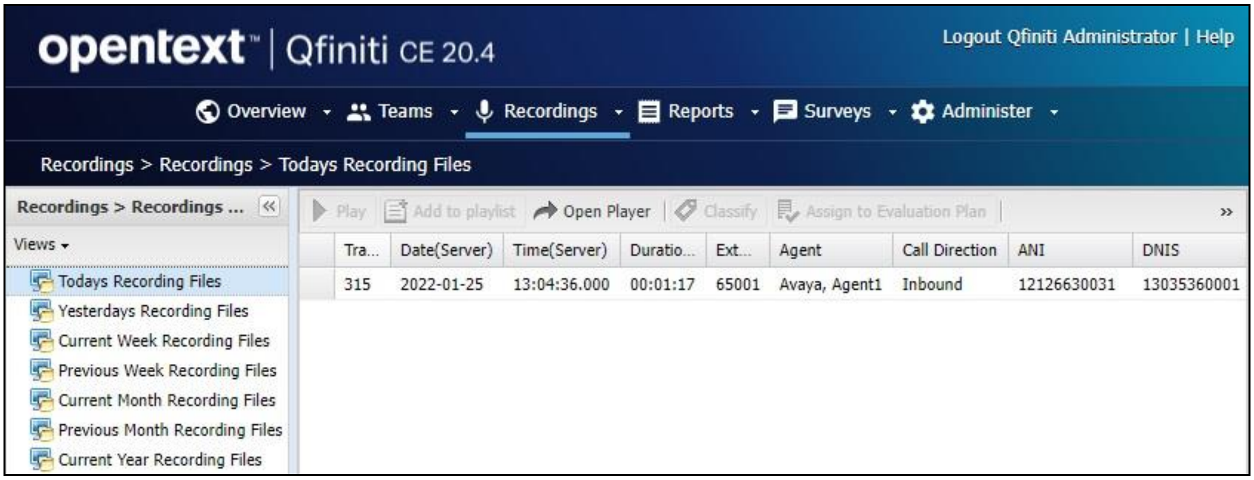
	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	cm7	1	Talking	Tue Jan 25 09:45:18 2022	Online	18	4	25	25	30

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

9.3. Verify OpenText Qfiniti

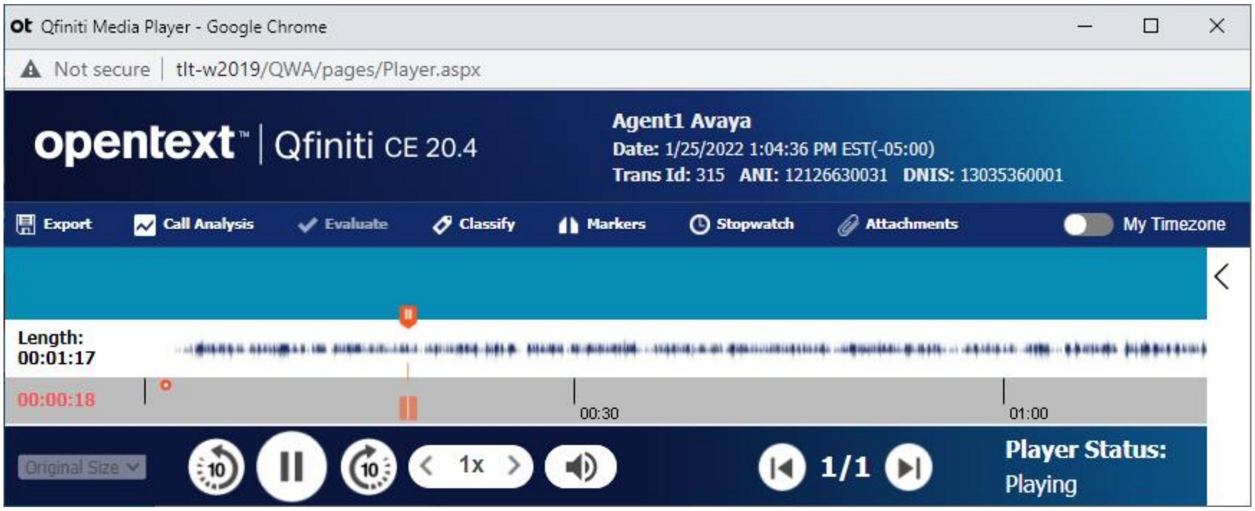
Log an agent in to handle and complete an ACD call. Follow the procedure in **Section 8.14** to launch the Qfiniti web interface, and log in using the appropriate user credentials.

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


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
Current Year Recording Files
Play
Add to playlist
Open Player
Classify
Assign to Evaluation Plan

Tra...	Date(Server)	Time(Server)	Duratio...	Ext...	Agent	Call Direction	ANI	DNIS
315	2022-01-25	13:04:36.000	00:01:17	65001	Avaya, Agent1	Inbound	12126630031	13035360001

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



Agent1 Avaya
Date: 1/25/2022 1:04:36 PM EST(-05:00)
Trans Id: 315 **ANI:** 12126630031 **DNIS:** 13035360001

Length: 00:01:17

Player Status: Playing

10. Conclusion

These Application Notes describe the configuration steps required for OpenText Qfiniti 20.4 to successfully interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 using Service Observing No Talk. All feature and serviceability test cases were completed successfully.

11. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 12, July 2021, available at http://support.avaya.com.

2. *Administering Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 12, October 2021, available at http://support.avaya.com.

3. *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 10, September 2021, available at http://support.avaya.com.

4. *OpenText Qfiniti User Guide*, Version 20.4, Rev. 2020-Oct-28, available to existing customers at https://knowledge.opentext.com/knowledge/llisapi.dll.

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.