



Application Notes for Eventide NexLog DX-Series 2022.5 with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 Using Multiple Registration – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Eventide NexLog DX-Series 2022.5 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 using Multiple Registration. Eventide NexLog DX-Series is a call recording solution.

In the compliance testing, Eventide NexLog DX-Series used the Device, Media, and Call Control interface from Avaya Aura® Application Enablement Services to monitor agent stations on Avaya Aura® Communication Manager, and the Multiple Registration feature 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 Eventide NexLog DX-Series (NexLog) 2022.5 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 using Multiple Registration. NexLog is a call recording solution.

In the compliance testing, NexLog used the Device, Media, and Call Control (DMCC) interface from Application Enablement Services to monitor agent stations on Communication Manager, and the Multiple Registration feature to capture media associated with the monitored agent stations for call recording.

The DMCC interface is used by NexLog to monitor agent stations on Communication Manager and register as virtual IP softphones against monitored agent stations to pick up the media for call recording.

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

2. General Test Approach and Test Results

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

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

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

The verification of tests included use of Application Enablement Services and NexLog logs for proper message exchanges and use of NexLog 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 DMCC interface between Avaya systems and NexLog used encrypted connection, as requested by Eventide.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on NexLog:

- Use of DMCC services to register virtual IP softphones against agent stations, monitor call events, and obtain media for call recording.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, resume, G.711, service observing, long duration, multiple calls, multiple agents, transfer, and conference.

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

2.2. Test Results

All test cases were executed, and the following were observations on NexLog:

- By design, the Annotation parameter for the recording entry contains information including called number and indications of hold, retrieve, transfer, and conference.
- By design, NexLog ends an active recording upon agent placing call on hold and starts a new recording upon agent resuming the call.
- Recording entries are created when a H.323 agent dials Feature Access Codes to login, logout, and change work mode, and when an incoming ACD call is abandoned by the PSTN caller while ringing at the H.323 agent.
- Dial tone and ringing are captured in the recording associated with outbound calls, including outbound calls as part of transfer and conference scenarios.
- When a non-monitored supervisor is the transfer-to or conference-to destination in an unattended transfer/conference scenario, the supervisor extension is not reported as part of the recording entry. The attended transfer/conference can be used as workaround with the non-monitored supervisor's extension reported for those cases.
- When there are multiple calls in the system, the call direction associated with an inbound ACD call can be reported as Outbound. In these cases, the reported value in the Calling Party and Annotation parameters can be used to decipher the actual call direction.
- After a busy out and release of CTI link on Communication Manager, active device monitoring is removed on Communication Manager and not re-established by NexLog. The workaround is for the administrator to manually restart NexLog.
- For the conference scenarios, the second recording entry associated with the conference-from agent may contain twenty seconds of silence after the conference complete action and before the three-way conversation. There is no other impact besides the extra silence with the entire conference audio captured.
- Occasionally, a recording can start with less than one second of static noise. Eventide shared that this has to do with encryption key processing that occurs only when the DMCC connection is encrypted and that this will be addressed in the next NexLog release.

2.3. Support

Technical support on NexLog can be obtained through the following:

- **Phone:** (201) 641-1200
- **Web:** <https://eventidecommunications.com/technical-support>

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, NexLog monitored agent stations shown in the table below.

| Device Type | Extension |
|-----------------------------|-------------------------------|
| Agent Station | 65001 (H.323), 66002 (SIP) |
| Agent Station Security Code | 65001 (65001), 66002 (123456) |
| Agent ID | 65881, 65882 |

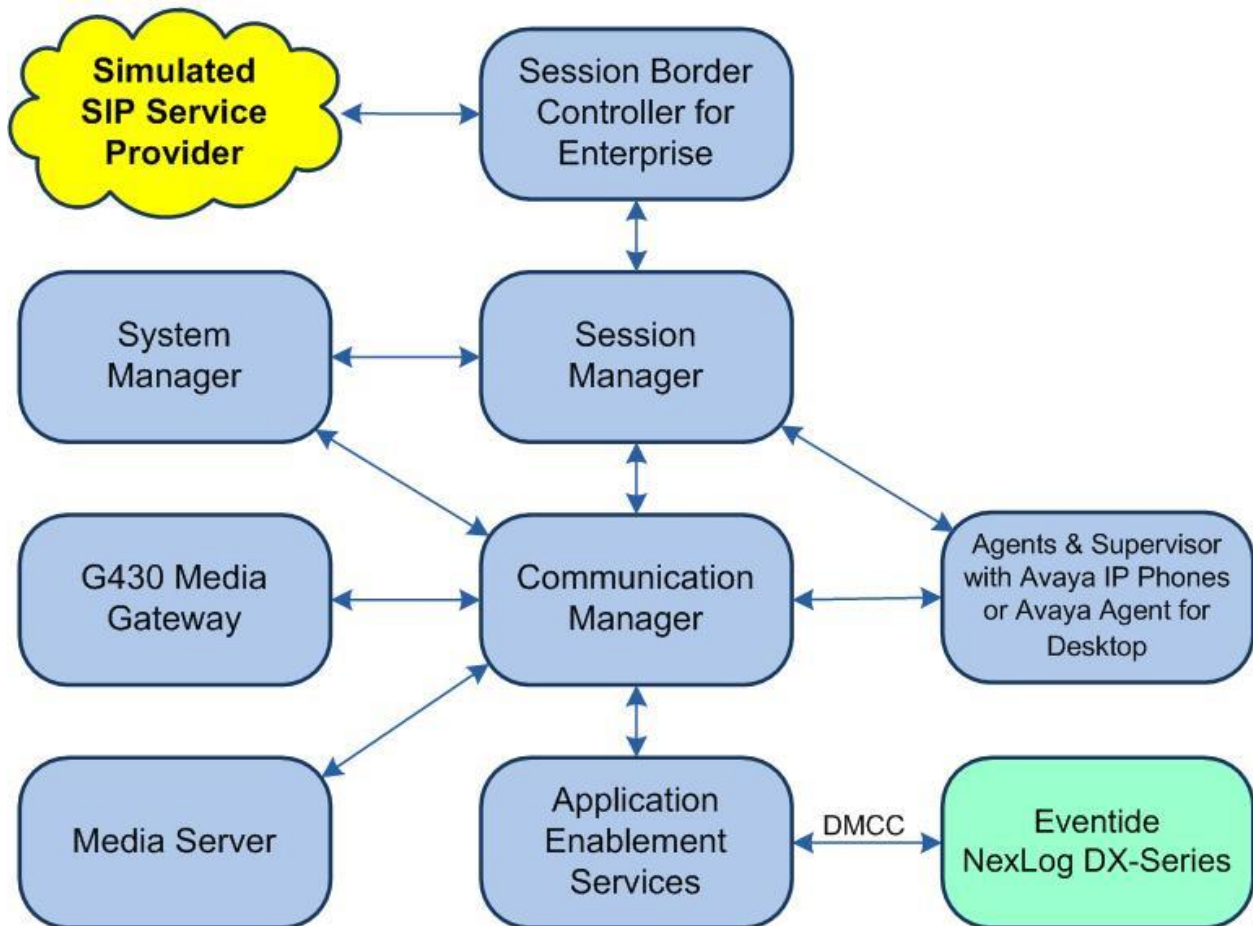


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

| Equipment/Software | Release/Version |
|---|----------------------------------|
| Avaya Aura® Communication Manager in Virtual Environment | 8.1.3.4 (8.1.3.4.0.890.27348) |
| Avaya G430 Media Gateway | 42.8.0 |
| Avaya Aura® Media Server in Virtual Environment | 8.0.2.218 |
| Avaya Aura® Application Enablement Services in Virtual Environment | 8.1.3.4.0.2-0 |
| Avaya Aura® Session Manager in Virtual Environment | 8.1.3.4 (8.1.3.4.813401) |
| Avaya Aura® System Manager in Virtual Environment | 8.1.3.4 (8.1.3.4.1014355) |
| Avaya Session Border Controller for Enterprise in Virtual Environment | 8.1.3.1 (8.1.3.1-38-21632) |
| Avaya Agent for Desktop (H.323 & SIP) | 2.0.6.19.3004 |
| Avaya J179 & 9611G IP Deskphone (H.323) | 6.8.5.11 |
| Avaya J169 IP Deskphone (SIP) | 4.0.11.0.3 |
| Eventide NexLog DX-Series in Virtual Environment | 2022.5 [2774] |
| • Avaya DMCC XML | 7.0.0.38 |

5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer IP codec set
- Administer agent stations

5.1. Verify License

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

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

Navigate to **Page 5** and verify that the **Media Encryption Over IP** customer option is set to **y**.

| | | |
|---|---|---------------------|
| display system-parameters customer-options | | Page 5 of 12 |
| OPTIONAL FEATURES | | |
| Emergency Access to Attendant? y | IP Stations? y | |
| Enable 'dadmin' Login? y | ISDN Feature Plus? n | |
| Enhanced Conferencing? y | ISDN/SIP Network Call Redirection? y | |
| Enhanced EC500? y | ISDN-BRI Trunks? y | |
| Enterprise Survivable Server? n | ISDN-PRI? y | |
| Enterprise Wide Licensing? n | Local Survivable Processor? n | |
| ESS Administration? y | Malicious Call Trace? y | |
| Extended Cvg/Fwd Admin? y | Media Encryption Over IP? y | |
| External Device Alarm Admin? y | Mode Code for Centralized Voice Mail? n | |
| Five Port Networks Max Per MCC? n | | |
| Flexible Billing? n | | |

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
Name: AES CTI Link                                COR: 1
Unicode Name? n
```

5.3. Administer IP Codec Set

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

For **Audio Codec**, make certain that a G.711 variant is included, which is the codec set supported by NexLog by default. Note that NexLog can also support the G.729 codec but will require a special license and was not covered in the compliance testing.

For **Media Encryption**, make certain that **1-srtp-aescm128-hmac80** is included, which is the DMCC media encryption method used with NexLog.

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

```
change ip-codec-set 1                             Page 1 of 2
IP Codec Set
Codec Set: 1
Audio      Silence   Frames   Packet
Codec      Suppression Per Pkt   Size(ms)
1: G.711MU      n         2       20
2: G.729
3:
4:
5:
6:
7:
Media Encryption                                Encrypted SRTP: best-effort
1: 1-srtp-aescm128-hmac80
2: aes
3: none
4:
5:
```


5.4. Administer Agent Stations

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

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

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

6. Configure Avaya Aura® Application Enablement Services

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

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- Administer NexLog user
- Administer security database
- Administer ports
- Restart services
- Export CA certificate

6.1. Launch OAM Interface

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

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



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. A red horizontal bar spans the width of the page, with a "Help" link on the right. Below this bar is a central login box with a light gray background. Inside the box, the text "Please login here:" is followed by a "Username" label and a text input field. Below the input field is a "Continue" button. At the bottom of the page, another red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2020 Avaya Inc. All Rights Reserved." is displayed.

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". On the right, a welcome message for the user is shown, including login details and system status. The left sidebar contains a navigation menu with options like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled "Welcome to OAM" and provides an overview of the tools available for managing the AE Server, along with a list of administrative domains and their functions.

Welcome: User
Last login: Tue Jun 21 10:27:22 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: 8.1.3.4.0.2-0
Server Date and Time: Tue Jun 21 10:37:35 EDT 2022
HA Status: Not Configured

Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Welcome to OAM

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

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

6.2. Verify License

Select **Licensing** → **WebLM Server Access** in the left pane, to display the applicable WebLM server log in screen (not shown). Log in using the appropriate credentials and navigate to display installed licenses (not shown).

This screenshot shows the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the left sidebar. The main content area is titled "Licensing" and provides instructions on how to set up and maintain the WebLM, including details on server address, access, and reserved licenses.

Welcome: User
Last login: Tue Jun 21 10:27:22 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: 8.1.3.4.0.2-0
Server Date and Time: Tue Jun 21 10:37:35 EDT 2022
HA Status: Not Configured

Licensing | Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
WebLM Server Address
WebLM Server Access
Reserved Licenses
Maintenance
Networking

Licensing

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

- WebLM Server Address

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

- WebLM Server Access

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

- Reserved Licenses

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

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

AVAYA Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search

Home Licenses

L...

- WebLM Home
- Install license
- Licensed products
- APPL_ENAB
- ▼ Application_Enablement
 - View license capacity
 - View peak usage
- APS_CMS_Connectors
 - ▶ APS_CMS_Connectors
- Configure Centralized Licensing
- ASBCE
 - ▶ Session_Border_Controller_E_AE
 - ▶ Avaya_Proactive_Contact
- CCTR
 - ▶ ContactCenter
- CMS
 - ▶ CMS
- Configure Centralized Licensing
- COMMUNICATION_MANAGER

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

You are here: Licensed Products > Application_Enablement > View License Capacity

License installed on: May 18, 2022 9:26:13 AM -04:00

License File Host IDs: VE-83-02-2D-26-52-01

Licensed Features

11 Items Show All ▾

| Feature (License Keyword) | Expiration date | Licensed capacity |
|--|-----------------|-------------------|
| Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP | May 13, 2023 | 100 |
| CVLAN ASAI VALUE_AES_CVLAN_ASAI | May 13, 2023 | 100 |
| Device Media and Call Control VALUE_AES_DMCC_DMC | May 13, 2023 | 100 |
| AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED | May 13, 2023 | 100 |
| DLG VALUE_AES_DLG | May 13, 2023 | 100 |
| TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS | May 13, 2023 | 1000 |

6.3. Administer TSAPI Link

Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left sidebar shows a navigation tree with "AE Services" expanded, and "TSAPI" selected. The main content area displays the "TSAPI Links" screen, which includes a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

| Link | Switch Connection | Switch CTI Link # | ASAI Link Version | Security |
|------|-------------------|-------------------|-------------------|----------|
|------|-------------------|-------------------|-------------------|----------|

Buttons: Add Link, Edit Link, Delete Link

The **Add TSAPI Links** screen is displayed next. The **Link** field is only local to the Application Enablement Services server and may be set to any available number.

For **Switch Connection**, select the relevant switch connection from the drop-down list, in this case **cm7**. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**.

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

The screenshot shows the "Add TSAPI Links" screen in the Avaya Application Enablement Services Management Console. The left sidebar is the same as the previous screenshot. The main content area displays the "Add TSAPI Links" form, which includes fields for Link, Switch Connection, Switch CTI Link Number, ASAI Link Version, and Security. The values entered are: Link (1), Switch Connection (cm7), Switch CTI Link Number (1), ASAI Link Version (12), and Security (Both). Below the form are buttons for "Apply Changes", "Cancel Changes", and "Advanced Settings".

Form fields and values:

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

Buttons: Apply Changes, Cancel Changes, Advanced Settings

6.4. Administer H.323 Gatekeeper

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

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

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Communication Manager Interface' and 'Switch Connections'. The main content area displays a table of switch connections. The table has four columns: Connection Name, Processor Ethernet, Msg Period, and Number of Active Connections. The first row shows 'cm7' with 'Yes' for Processor Ethernet, '30' for Msg Period, and '1' for Number of Active Connections. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'. The top right corner shows user information and system status.

| Connection Name | Processor Ethernet | Msg Period | Number of Active Connections |
|--------------------------------------|--------------------|------------|------------------------------|
| <input checked="" type="radio"/> 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 on Communication Manager to use as H.323 gatekeeper, in this case **10.64.101.236** as shown below. Click **Add Name or IP**.

The screenshot shows the 'Edit H.323 Gatekeeper - cm7' screen. The left navigation pane is the same as the previous screenshot. The main content area has a text input field containing '10.64.101.236' and an 'Add Name or IP' button. Below the input field are 'Delete IP' and 'Back' buttons. The top right corner shows user information and system status.

6.5. Administer NexLog 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.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Jun 21 10:27:22 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: 8.1.3.4.0.2-0
Server Date and Time: Tue Jun 21 10:44:37 EDT 2022
HA Status: Not Configured

User Management | User Admin | Add UserHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Id

* Common Name

* Surname

* User Password

* Confirm Password

Admin Note

Avaya Role

Business Category

Car License

CM Home

Css Home

CT User

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

6.6. Administer Security Database

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

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A welcome message in the top right corner states: "Welcome: User", "Last login: Tue Jun 21 10:27:22 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: 8.1.3.4.0.2-0", "Server Date and Time: Tue Jun 21 10:37:35 EDT 2022", and "HA Status: Not Configured".

The main navigation bar shows "Security | Security Database | Control" and "Home | Help | Logout". The left sidebar contains a tree view with the following items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security" (expanded), "Account Management", "Audit", "Certificate Management", "Enterprise Directory", "Host AA", "PAM", "Security Database" (expanded), and "Control" (selected).

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

6.7. 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 **Encrypted Port** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Jun 21 10:27:22 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: 8.1.3.4.0.2-0
Server Date and Time: Tue Jun 21 10:37:35 EDT 2022
HA Status: Not Configured

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

▶ AE Service IP (Local IP)

▶ Network Configure

▶ Ports

▶ TCP/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999

Encrypted TCP Port9998

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Encrypted Port4722

TR/87 Port4723

Enabled Disabled

☒ ☐

☒ ☐

Enabled Disabled

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☒ ☐

TLT; Reviewed:
SPOC 11/3/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

17 of 36
NexLog-AES81

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**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows a tree structure with "Maintenance" expanded, and "Service Controller" selected. The main content area shows the "Service Controller" page with a table of services and their status.

Welcome: User
Last login: Tue Jun 21 10:27:22 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: 8.1.3.4.0.2-0
Server Date and Time: Tue Jun 21 10:37:35 EDT 2022
HA Status: Not Configured

Maintenance | Service Controller Home | Help | Logout


Service Controller

| Service | Controller Status |
|---|-------------------|
| <input type="checkbox"/> ASAI Link Manager | Running |
| <input checked="" type="checkbox"/> DMCC Service | Running |
| <input type="checkbox"/> CVLAN Service | Running |
| <input type="checkbox"/> DLG Service | Running |
| <input type="checkbox"/> Transport Layer Service | Running |
| <input checked="" type="checkbox"/> TSAPI Service | Running |

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

Start Stop Restart Service Restart AE Server Restart Linux Restart Web Server

Select **Security** → **Certificate Management** → **CA Trusted Certificates** from the left pane, to display the **CA Trusted Certificates** screen. Select the pertinent CA certificate for secure connection with client applications, in this case **SystemManagerCA**, and click **Export**.



Application Enablement Services

Management Console

Welcome: User
 Last login: Tue Sep 6 10:00:56 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: 8.1.3.4.0.2-0
 Server Date and Time: Tue Sep 06 11:09:33 EDT 2022
 HA Status: Not Configured

Security | Certificate Management | CA Trusted Certificates

[Home](#) | [Help](#) | [Logout](#)

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▼ Certificate Management

■ CA Trusted Certificates

CA Trusted Certificates

View


Import

Export

Delete

| Alias | Status | Issued To | Issued By | Expiration Date |
|--|---------|-----------------------------------|-----------------------------------|-----------------|
| <input type="radio"/> serverCertDefault | expired | aes7-081738682-labUseOnly | aes7-081738682-labUseOnly | Aug 5, 2020 |
| <input type="radio"/> avayaprca | valid | Avaya Product Root CA | Avaya Product Root CA | Aug 14, 2033 |
| <input type="radio"/> avaya_sipca | valid | SIP Product Certificate Authority | SIP Product Certificate Authority | Aug 17, 2027 |
| <input checked="" type="radio"/> SystemManagerCA | valid | System Manager CA | System Manager CA | Oct 8, 2028 |

The **Trusted Certificate Export** screen is displayed next. Copy everything in the text box, including the **BEGIN CERTIFICATE** and **END CERTIFICATE** (not shown) lines.



Application Enablement Services

Management Console

Welcome: User

Last login: Tue Sep 6 10:00:56 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: 8.1.3.4.0.2-0

Server Date and Time: Tue Sep 06 11:09:33 EDT 2022

HA Status: Not Configured

Security | Certificate Management | CA Trusted Certificates

Home | Help | Logout

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Account Management

Audit

Certificate Management

CA Trusted Certificates

Server Certificates

Revocation Configuration

Enterprise Directory

Trusted Certificate Export

Issued To: System Manager CA

Issued By: System Manager CA

Expiration Date: Oct 8, 2028

Certificate PEM:

```

-----BEGIN CERTIFICATE-----
MIIDWzCCAOkGawIBAgIILbCFHr3mswDQYJKoZIhvcNAQELBQAwOzEaMBGGA1UEAwRU3lzdG
IE1hbWFnFnZXIqQ0ExDTALBgNVBAsMBE1HTVQxQDJAmbGNVBAoMBUFWQVBIbMB4XDTE4MTAxMTE4
NF0eXDTI4MTAwODE4MTU0NFowOzEaMBGGA1UEAwRU3lzdGVtIE1hbWFnFnZXIqQ0ExDTALBgNVB
BE1HTVQxQDJAmbGNVBAoMBUFWQVBIbMBIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1
blFeekVIOePXG46TDUR7LjyZ1NjKMBCp+vf/rLbyy8u+yO6YT9ZGzpaixEYJwZG0KSJrgdkvkv2
RWmi71UICM73wyTBQwpzK12HQ0oS1ZAWjEwa/VuPQmbahGdC7UXO4DHMczzzhWhEOJ34;
22W1t+1WqV7f5g/itP0sEbwuJN032Tn9U03hc/LWLqOomTKyBzT4ejFD/c8kARa0acw2a/+enMQ
SafShXKM9PaCbcMN29D3RftYbrTqUSKfOUOSiNev7I70KDMaC/pRXbc/6Wu03sykTUyCpB4Hx49
M/OMh/c8vdSCYNmN07PpZnHesck0e7MZYwIDAQABO2MwYTABBgNVHRMBAf8EBTADAQH/MB8G
IwQYAOBBAFFojv4IgJO2AzKk709pJB14Gz7RMB0GA1UdDgQWBBrA17+C1CTtgMypO9PaSQZdeBs
0TAOMBgNVHQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQAdggEBAJNkV7PFUnHmptIFXjdeGUUxwC
VCrmwCz42V6QqmmRGGBBg2HJfmdPZZ23hKghApey8Yyusmvg+A12qRNj5f5fox6p19XA9T8ttOI

```

Paste the copied content to a Notepad file and save with a desired file name using **.crt** as suffix, such as **SystemManagerCA.crt** in the compliance testing.

```
-----BEGIN CERTIFICATE-----  
MIIDWzCCAkOgAwIBAgIIL1bhCFHr3mswDQYJKoZIhvcNAQELBQAwwEaMBGGA1UEAwwRU3lzdGVt  
IE1hbmfFnZXIgQ0ExdTBALBgNVBAcMBCBE1HTVQxXjJAMBgNVBAoMBUFWQVVBMB4XDTE4MTAxMTE4MTU0  
NFoXDTE4MTAwODE4MTU0NFowOzEaMBGGA1UEAwwRU3lzdGVtIE1hbmfFnZXIgQ0ExdTBALBgNVBAcM  
BE1HTVQxXjJAMBgNVBAoMBUFWQVVBMBIIBijANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAE1Y9+  
blFeekV10ePXG46TdUR7LjyZ1NjkMBCp+vf/rLbyy8u+y06YT9ZGzpaXjEYJJwZgOKSJrgdkvvv2  
RWmi71UICM73wyTbQwpzK12HQ00oS1ZAWjEwa/VuPQmbahGdc7UXO4DHMczzhekWhEOJjJ4zkRM  
22W1T+1WqV7fi5q/itP0SEbuwJNo32Tn9U03hc/LWLqomTKyBzt4ejFD/c8KaRa0acw2a/+enMQ  
5afShXKM9PaCbcMN29D3RftJybrTqUSkfOUOSiNev7I7KDMAc/pRXbc/6Wu03sykTUyCpB4Hx49  
MjOMh/c8vdSCYNmN07PPZNhesCK0e7MZywIDAQABOMwYTAPBgNVHRMBAf8EBTADAQH/MB8GA1Ud  
IwQYMBaAFFojv4IgJOAZKk709pJB114Gz7RMB0GA1UdDgQWBBRaI7+CICTgmyp09PaSQZdeBs+  
0TAOBgNVHQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQADggEBAJNKv7PFUnHmpt1FXjdeGUUxwOJM  
VCrmwCz4z2V6QgmmRGBBg2HJfmdPZZ23hKgHApey8YyumsVG+A12qrNJb5tfox6p19XA9T8ttOHh  
o8FQ6/chUYVCJfwRKgUA7kKhODx75LK7mTGBv2DFBcGetEWLZzoVQS+gzwpAYgqF5fUpA8E2zn1  
m46HSSivL7WDdowqlAxcVr4ScWghTpeeMbdl1np9R/e1bv0HK742oBATQGvem3rw36vrkUBAIos  
NzXWnvIUxqtBTMQ8irD1zSEMx61IE0bXboht7eU60mnhQczFJjMLiwYuGB9Nm1mf2+gCZTk1019N  
FJMYfZjgZdg=-----END CERTIFICATE-----
```

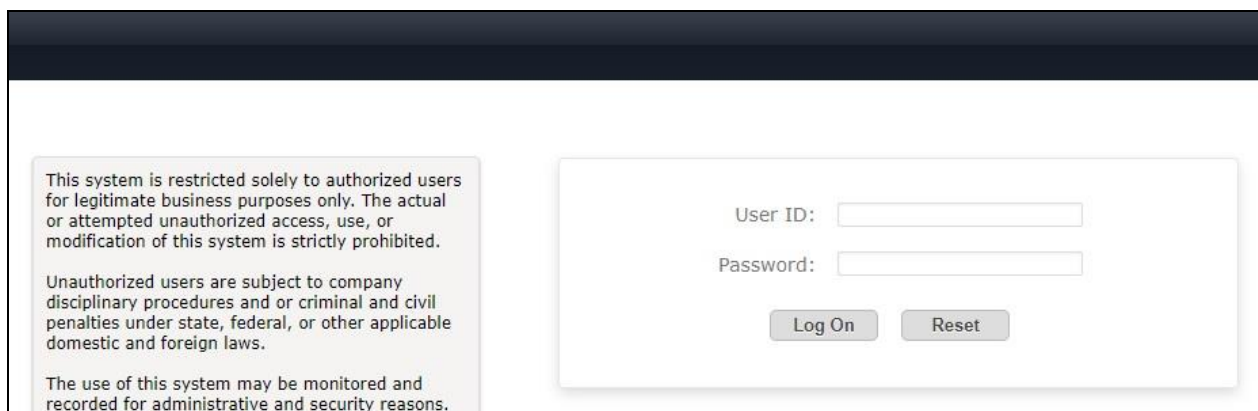
7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via the web interface of System Manager. The procedures include the following areas:

- Launch System Manager
- Administer users

7.1. Launch System Manager

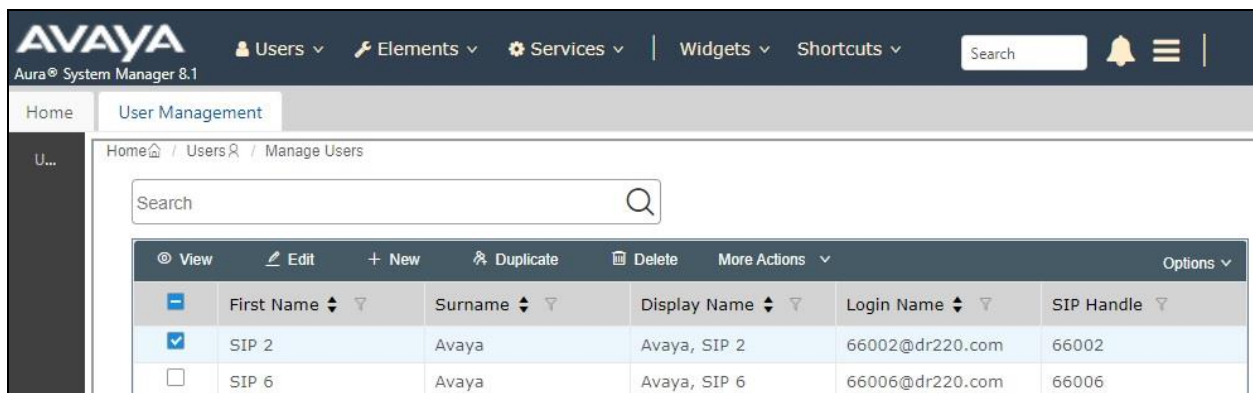
Access the System Manager web interface by using the URL **https://ip-address** in an Internet browser window, where **ip-address** is the IP address of System Manager. Log in using the appropriate credentials.



7.2. Administer Users

In the subsequent screen (not shown), select **Users → User Management** from the top menu. Select **User Management → Manage Users** (not shown) from the left pane to display the screen below.

Select the entry associated with the first SIP agent station from **Section 3**, in this case **66002**, and click **Edit**.



| View | Edit | New | Duplicate | Delete | More Actions | Options |
|-------------------------------------|-------|--------------|-----------------|--------|--------------|---------|
| <input checked="" type="checkbox"/> | | | | | | |
| SIP 2 | Avaya | Avaya, SIP 2 | 66002@dr220.com | 66002 | | |
| <input type="checkbox"/> | | | | | | |
| SIP 6 | Avaya | Avaya, SIP 6 | 66006@dr220.com | 66006 | | |

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

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

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, "Aura® System Manager 8.1", and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and notification bell are also present. The main content area is titled "User Profile | Edit | 66002@dr220.com" and includes buttons for "Commit & Continue", "Commit", and "Cancel". The "Communication Profile" tab is selected, and the "CM Endpoint Profile" is highlighted in the left sidebar. The form contains various fields for user configuration, including System (DR-CM), Profile Type (Endpoint), Extension (66002), Set Type (J169CC), and others. A red box highlights the blue Editor icon next to the Extension field.

| Field | Value |
|------------------|----------|
| System | DR-CM |
| Profile Type | Endpoint |
| Extension | 66002 |
| Set Type | J169CC |
| Port | S000068 |
| Preferred Handle | Select |
| Sip Trunk | aar |

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

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

System Information:

- System:** DR-CM
- Template:** J169CC_DEFAULT_CM_8_1
- Port:** S000068
- Name:** Avaya, SIP 2
- Extension:** 66002
- Set Type:** J169CC
- Security Code:** (empty)

Configuration Tabs:

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

General Options (G) * Configuration:

| Field | Value |
|--|--------------------------|
| * Class of Restriction (COR) | 1 |
| * Emergency Location Ext | 66002 |
| * Tenant Number | 1 |
| * SIP Trunk | Qaar |
| Coverage Path 1 | |
| Lock Message | <input type="checkbox"/> |
| Multibyte Language | Not Applicable |
| * Class Of Service (COS) | 1 |
| * Message Lamp Ext. | 66002 |
| Type of 3PCC Enabled | Avaya |
| Coverage Path 2 | |
| Localized Display Name | Avaya, SIP 2 |
| Enable Reachability for Station Domain Control | system |

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

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

The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and various menu items: Users, Elements, Services, Widgets, and Shortcuts. A search bar and notification icons are also present. The main content area is titled 'User Management' and shows a list of users on the left. The right pane is active, displaying the 'Feature Options' tab for a selected user. This tab contains various configuration fields and a 'Features' section at the bottom. In the 'Features' section, the 'IP SoftPhone' checkbox is checked and highlighted with a red rectangular box. Other features like 'Always Use', 'IP Audio Hairpinning', 'Bridged Call Alerting', 'Bridged Idle Line Preference', 'Coverage Message Retrieval', 'Direct IP-IP Audio Connections', 'Idle Appearance Preference', 'LWC Activation', and 'CDR Privacy' are also listed with their respective checkboxes.

| General Options (G) | Feature Options (F) | Site Data (S) | Abbreviated Call Dialing (A) | Enhanced Call Fwd (E) |
|--|---|----------------------|------------------------------|-----------------------|
| Button Assignment (B) | Profile Settings (P) | Group Membership (M) | | |
| Active Station Ringing : single MWI Served User Type : None Per Station CPN - Send Calling Number : None IP Phone Group ID : Remote Soft Phone Emergency Calls : as-on-local LWC Reception : spe AUDIX Name : None EC500 State : enabled Voice Mail Number : admin Music Source : | Auto Answer : none Coverage After Forwarding : system Display Language : english Hunt-to Station : Loss Group : 19 Survivable COR : internal Time of Day Lock Table : None Bridging Tone for This Extension : no | | | |
| Features <ul style="list-style-type: none"> <input type="checkbox"/> Always Use <input type="checkbox"/> IP Audio Hairpinning <input type="checkbox"/> Bridged Call Alerting <input type="checkbox"/> Bridged Idle Line Preference <input checked="" type="checkbox"/> Coverage Message Retrieval <input checked="" type="checkbox"/> Direct IP-IP Audio Connections <input type="checkbox"/> Idle Appearance Preference <input checked="" type="checkbox"/> IP SoftPhone <input checked="" type="checkbox"/> LWC Activation <input type="checkbox"/> CDR Privacy | | | | |

8. Configure Eventide NexLog DX-Series

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

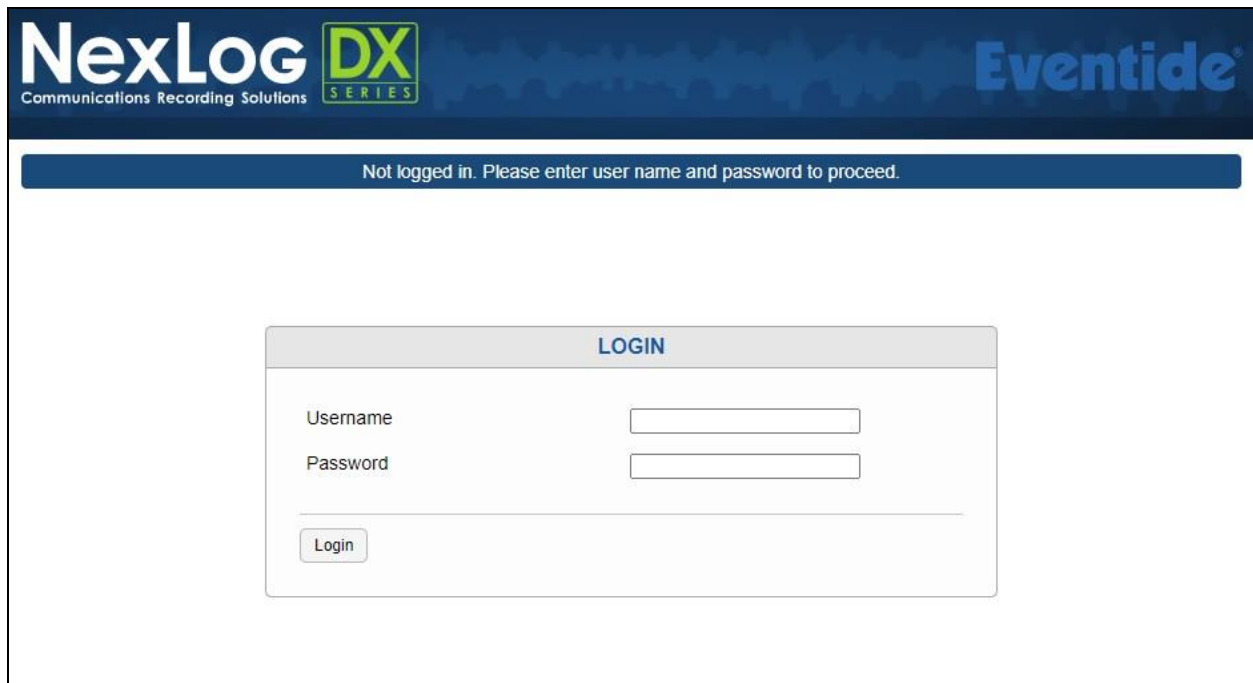
- Launch configuration web interface
- Administer SSL certificate
- Administer recording interface
- Administer channel name

The configuration of NexLog is performed by Eventide dealers. The procedural steps are presented in these Application Notes for informational purposes.

8.1. Launch Configuration Web Interface

Access the configuration web interface by using the URL **http://ip-address/admin** in an Internet browser window, where **ip-address** is the IP address of NexLog.

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



The screenshot shows the login page for NexLog DX-Series. The header features the NexLog DX-Series logo and the Eventide logo. A message at the top of the main content area states: "Not logged in. Please enter user name and password to proceed." Below this is a login form with the title "LOGIN". The form contains two input fields: "Username" and "Password". Below the password field is a "Login" button.

8.2. Administer SSL Certificate

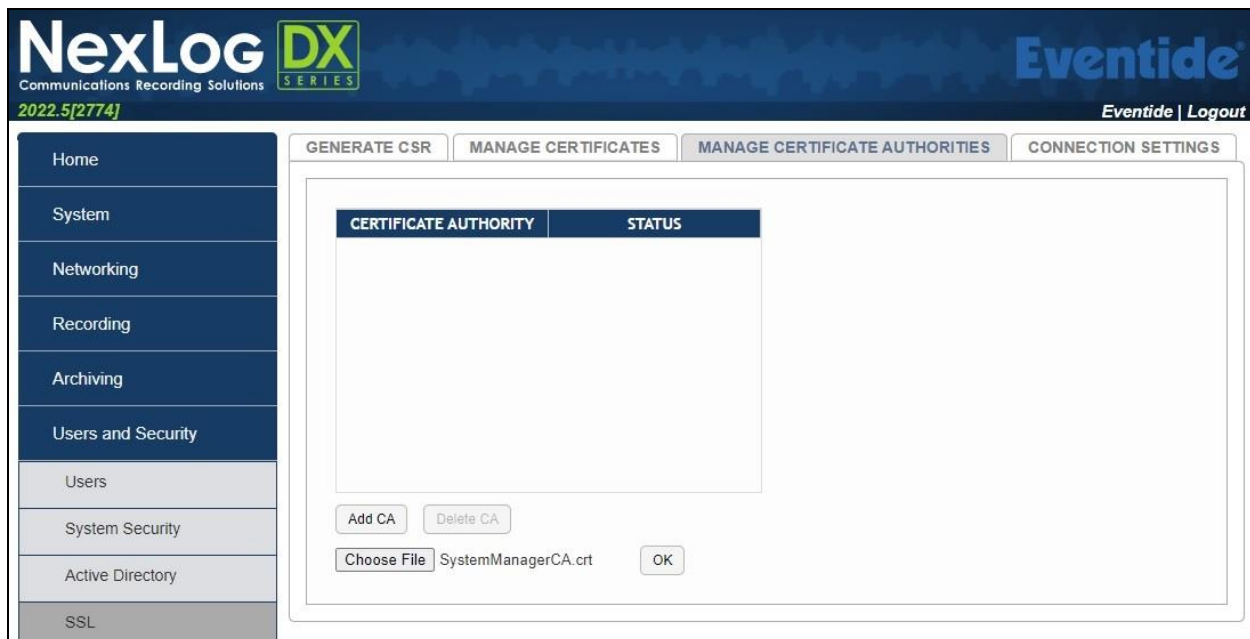
The screen below is displayed.



The screenshot shows the NexLog DX-Series Recorder status page. The left sidebar contains navigation links: Home, System, Networking, Recording, Archiving, Users and Security, and Alerts and Logs. The main content area is titled 'RECORDER' and displays system information in two columns. The footer indicates 'NexLog DX-Series Software ©2022 Eventide Inc.'.

| RECORDER | | | |
|------------------|---------------------|---------------------|---------------|
| Recorder Name | NEXLOG | Timesync | Internal |
| Facility Name | | Total Memory | 7884304 KB |
| Serial Number | 240100182 | Interface [eth0] IP | 10.64.101.207 |
| Firmware Version | 2022.4[2693] | Interface [eth1] IP | None |
| Current Time | 2022-09-06 15:48:46 | | |
| Timezone | UTC | | |
| Uptime | 1 hour, 42 minutes | | |
| Channel Count | 0 | | |

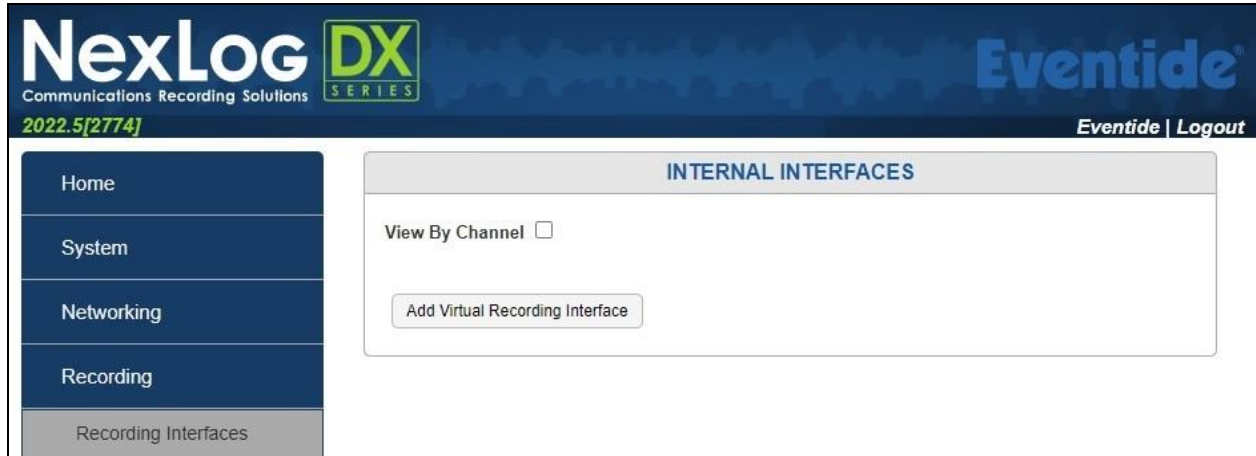
Select **Users and Security** → **SSL** followed by the **MANAGE CERTIFICATE AUTHORITIES** tab to display the screen below. Select **Add CA** followed by **Choose File** and navigate to the exported CA certificate from **Section 6.9**. Click **OK** to apply the CA certificate.



The screenshot shows the 'MANAGE CERTIFICATE AUTHORITIES' tab in the NexLog DX-Series interface. The left sidebar is expanded to show 'Users and Security' > 'SSL'. The main content area has tabs for 'GENERATE CSR', 'MANAGE CERTIFICATES', 'MANAGE CERTIFICATE AUTHORITIES', and 'CONNECTION SETTINGS'. The 'MANAGE CERTIFICATE AUTHORITIES' tab is active, displaying a table with columns 'CERTIFICATE AUTHORITY' and 'STATUS'. Below the table are buttons for 'Add CA', 'Delete CA', 'Choose File', and 'OK'. The 'Choose File' button is selected, and the file 'SystemManagerCA.crt' is shown.

8.3. Administer Recording Interface

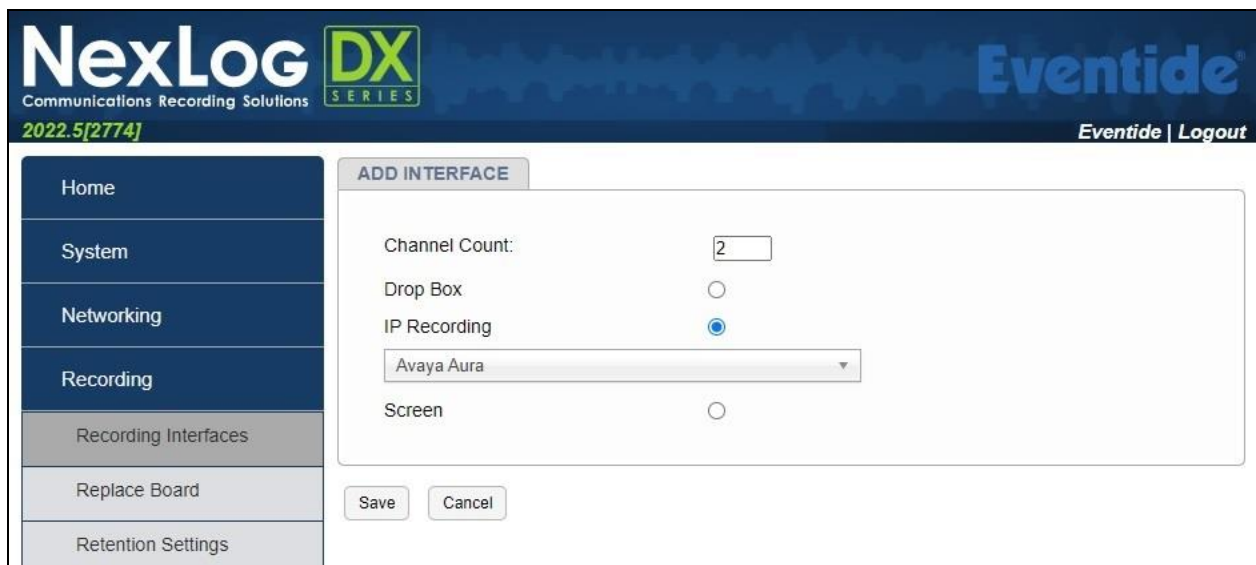
Select **Recording** → **Recording Interfaces** to display the **INTERNAL INTERFACES** screen. Click on **Add Virtual Recording Interface**.



The screen is updated with an **ADD INTERFACE** tab as shown below.

For **Channel Count**, enter the number of agent stations from **Section 3**, in this case **2**.

For **IP Recording**, select the radio button followed by **Avaya Aura** from the drop-down list as shown below.



The screen is updated with an **AVAYA AURA** tab as shown below. Enter the following values for the specified fields:

- **Username:** The NexLog user credentials from **Section 6.5**.
- **Password:** The NexLog user credentials from **Section 6.5**.
- **NexLog DX IP Address:** The IP address of NexLog server.
- **Server IP Address:** The IP address of Application Enablement Services.
- **Server Version:** The software version of Application Enablement Services.
- **Device Instance:** "0"
- **Encrypted RTP Media:** Check this field for secure signaling connection.
- **Encrypted Metadata:** Check this field.
- **Certification Name:** Name of the CA certificate from **Section 6.9** with pem suffix.
- **Name:** The relevant switch connection name from **Section 6.3**.
- **IP Address:** The IP address of the H.323 gatekeeper from **Section 6.4**.
- **Base Audio Port:** A non-reserved UDP port such as "60020".
- **Extension:** The agent station extension from **Section 3**.
- **Password:** The agent station security code from **Section 3**.

NexLog DX SERIES **Eventide**

Communications Recording Solutions **2022.5[2774]** **Eventide | Logout**

ADD INTERFACE **AVAYA AURA**

Home
System
Networking
Recording
Recording Interfaces
Replace Board
Retention Settings
Resource Groups
Call Suppression
Custom Fields
Alias Banks
Data Integrations
Geo-Location
Encryption At Rest

Username:

Password:

NexLog DX IP Address:

Application Enablement Server IP Address:

Application Enablement Server Version:

Device Instance:

Encrypted RTP Media (SRTP AES CM128 HMAC80): ☒

Encrypted Metadata: ☒

Certification Name:

Communication Manager Name:

Communication Manager IP Address:

Base Audio Port:

| | Extension | Password |
|---|------------------------------------|--|
| 1 | <input type="text" value="65001"/> | <input type="password" value="*****"/> |
| 2 | <input type="text" value="66002"/> | <input type="password" value="*****"/> |

For each phone, enter the extension of the phone to record. The must already exist on the Avaya Aura system.

8.4. Administer Channel Name

The **INTERNAL INTERFACES** screen is displayed again and updated with the newly created channels as shown below.

Update the **NAME** for each channel as desired. In the compliance testing, **Agent 65001** and **Agent 66002** were used.

NexLog DX SERIES Eventide
Communications Recording Solutions
2022.5[2774] Eventide | Logout

INTERNAL INTERFACES

View By Channel ☐

IP Recording (avaya_aura template) 2 Channels Ena

| ACTIVITY | MF ANI DETECT (SYNWAY) | NAME | ENCODING | DETECT TYPE | TDD ENABLE | VOX TRIGGER |
|----------|------------------------|-------------|------------|-------------|------------|-------------|
| 1 | Off | Agent 65001 | PASSTROUGH | VOX | Off | -32db |
| 2 | Off | Agent 66002 | PASSTROUGH | VOX | Off | -32db |

Add Virtual Recording Interface

9. Verification Steps

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

9.1. Verify Avaya Aura® Communication Manager

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

```
status aesvcs cti-link
```

| AE SERVICES CTI LINK STATUS | | | | | | |
|-----------------------------|-----------|-----------|--------------------|--------------------|-----------|-----------|
| CTI Link | Version | Mnt Busy | AE Services Server | Service State | Msgs Sent | Msgs Rcvd |
| 1 | 12 | no | aes7 | established | 41 | 19 |

Verify registration status of virtual IP softphones by using the **list registered-ip-stations** command. Verify that all monitored agent stations from **Section 3** are displayed along with the IP address of the Application Enablement Services server, as shown below.

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

| REGISTERED IP STATIONS | | | |
|---------------------------------------|----------------------|---------------------|--|
| Station Ext or Orig Port Socket | Set Type/ Net Rgn | Prod ID/ Release | Station IP Address/ Gatekeeper IP Address |
| 65000 | 9611 | IP_Phone | 192.168.200.212 |
| tls | 1 | 6.85 | 10.64.101.236 |
| 65001 | 9611 | IP_Phone | 192.168.200.179 |
| tls | 1 | 6.85 | 10.64.101.236 |
| 65001 | 9611 | IP_API_A | 10.64.101.239 |
| tcp | 1 | 3.2040 | 10.64.101.236 |
| 66002 | J169CC | IP_API_A | 10.64.101.239 |
| tcp | 1 | 3.2040 | 10.64.101.236 |

9.2. Verify Avaya Aura® Application Enablement Services

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

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

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Wed Oct 5 13:38:20 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: 8.1.3.4.0.2-0
Server Date and Time: Wed Oct 05 13:49:46 EDT 2022
HA Status: Not Configured

Status | Status and Control | DMCC Service SummaryHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▶ Log Manager

▼ Status and Control

▪ CVLAN Service Summary

▪ DLG Services Summary

▪ **DMCC Service Summary**

▪ Switch Conn Summary

▪ TSAPI Service Summary

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Wed Oct 05 13:49:31 EDT 2022

Service Uptime: 1 days, 21 hours 55 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 12

Number of Existing Devices: 2

Number of Devices Created Since Service Boot: 24


| | Session ID | User | Application | Far-end Identifier | Connection Type | # of Associated Devices |
|--------------------------|---|--------|------------------------|--------------------|-----------------|-------------------------|
| <input type="checkbox"/> | 5B8E2324D881E52A5 FC93ED57E2873B7-11 | nexlog | EventideAuraController | 10.64.101.207 | XML Encrypted | 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 number of monitored agent stations from **Section 3**, in this case **2**.



Application Enablement Services

Management Console

Welcome: User
 Last login: Wed Oct 5 13:38:20 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: 8.1.3.4.0.2-0
 Server Date and Time: Wed Oct 05 13:50:41 EDT 2022
 HA Status: Not Configured

Status | Status and Control | TSAPI Service Summary
Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▶ Log Manager

▼ Status and Control

▪ CVLAN Service Summary

▪ DLG Services Summary

▪ DMCC Service Summary

▪ Switch Conn Summary

▪ **TSAPI Service Summary**

TSAPI Link Details

☐ Enable page refresh every 60 seconds

| | Link | Switch Name | Switch CTI Link ID | Status | Since | State | Switch Version | Associations | Msgs to Switch | Msgs from Switch | Msgs Period |
|----------------------------------|------|-------------|--------------------|---------|-------------------------|--------|----------------|--------------|----------------|------------------|-------------|
| <input checked="" type="radio"/> | 1 | cm7 | 1 | Talking | Mon Oct 3 15:53:38 2022 | Online | 18 | 2 | 19 | 41 | 30 |

Online
Offline

For service-wide information, choose one of the following:
 TSAPI Service Status
TLink Status
User Status

9.3. Verify Eventide NexLog DX-Series

Access the MediaWorks web interface by using the URL **http://ip-address/client/mediaworks** in an Internet browser window, where **ip-address** is the IP address of NexLog.

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



The screenshot shows the login interface for NexLog DX-Series MediaWorks 2022.5. The interface has a dark blue background with the NexLog DX-Series logo at the top. Below the logo, the text 'MediaWorks 2022.5' is displayed. A recorder ID '10.64.101.207' is shown. The login form includes fields for 'Username' and 'Password', a 'Remember Me' checkbox, and 'Cancel' and 'Login' buttons. The Eventide logo is in the bottom left, and a gear icon is in the bottom right.

Verify the screen below is displayed with a listing of channels from **Section 8.4**.

| File | Edit | Tools | Playback | View | Help | Eventide |
|--------------|--------|--------------|----------------|-------------|-----------|----------|
| Channels | Browse | Search | Evaluations | 2 Resources | NexLog DX | |
| Channel Name | Cha... | Live Monitor | Channel Status | | | |
| Agent 65001 | 001 | | Idle | | | |
| Agent 66002 | 002 | | Idle | | | |

Log an agent in and answer an incoming ACD call. Verify that the channel entry associated with the answering agent is updated with **Channel Status** of **Recording**, as shown below.

| File | Edit | Tools | Playback | View | Help | Eventide |
|--------------|--------|--------------|----------------|-------------|-----------|----------|
| Channels | Browse | Search | Evaluations | 2 Resources | NexLog DX | |
| Channel Name | Cha... | Live Monitor | Channel Status | | | |
| Agent 65001 | 001 | | Recording | | | |
| Agent 66002 | 002 | | Idle | | | |

Complete the ACD call. Select the **2 Resources** tab 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.

| Avaya Aura Call Id | Channel Name | Start Time | Duration | Calling Party | Called Party | Call Direction... | Annotations |
|--------------------|--------------|------------|----------|---------------|--------------|-------------------|-----------------------------|
| 338 | Agent 65001 | 08:42:51 | 01:17 | 12126630031 | | Inbound | "13035360001 has answered." |
| 337 | Agent 65001 | 08:42:11 | 00:03 | | | Outbound | |
| 336 | Agent 65001 | 08:42:04 | 00:07 | | | Inbound | |

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

| Avaya Aura Call Id | Channel Name | Start Time | Duration | Calling Party | Called Party | Call Direction... | Annotations |
|--------------------|--------------|------------|----------|---------------|--------------|-------------------|-----------------------------|
| 338 | Agent 65001 | 08:42:51 | 01:17 | 12126630031 | | Inbound | "13035360001 has answered." |
| 337 | Agent 65001 | 08:42:11 | 00:03 | | | Outbound | |
| 336 | Agent 65001 | 08:42:04 | 00:07 | | | Inbound | |

10. Conclusion

These Application Notes describe the configuration steps required for Eventide NexLog DX-Series 2022.5 to successfully interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 using Multiple Registration. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

11. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 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. *Eventide NexLog DX Series User Manual*, Version 2022.3[2364], P/N: #141338, available via the NexLog configuration web interface.

©2022 Avaya Inc. All Rights Reserved.

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

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