



DevConnect Program

Application Notes for NICE CXone Multi-ACD v1.0 with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Application Enablement Services R10.1 using DMCC Single Step Conference - Issue 1.0

Abstract

These Application Notes describe the configuration steps for the NICE CXone Multi-ACD v1.0 to interoperate with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Application Enablement Services R10.1 using DMCC Single Step Conference to record telephone calls.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 0**, 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.

1. Introduction

These Application Notes describe the configuration steps for the NICE CXone Multi-ACD v1.0 to interoperate with the Avaya solution which consists of an Avaya Aura® Communication Manager R10.1, Avaya Aura® Session Manager R10.1, and Avaya Aura® Application Enablement Services R10.1.

NICE CXone (CXone) is a Contact Center as a Service (CCaaS) platform powered by Enlighten AI built for Customer Experience (CX) to ensure customer experiences flow, every time. The platform has the capability to connect with on-premises third party Automatic Call Distribution (ACD) to get the media (e.g., screen, voice, etc.). CXone uses the Avaya Aura® Communication Manager Single Step Conference feature via the Application Enablement Services (AES) Device, Media, and Call Control (DMCC) interface and the Telephony Services Application Programming Interface (TSAPI) to capture the audio and call details for call recording on various Communication Manager endpoints, listed in **Section 4**.

The TSAPI integration allows NICE CXone to receive call-related events and metadata from AES. This integration must be paired with an audio capture method, in this case DMCC Single Step Conference to provide an audio source for recordings.

DMCC works by allowing software vendors to create soft phones, in memory on a recording server, and use them to monitor and record other phones. This is purely a software solution and does not require telephony boards or any wiring beyond a typical network infrastructure. The DMCC API associated with the AES server monitors the digital and VoIP extensions. The application uses the AES DMCC to ‘record’ the target extension using Virtual Extensions on Communication Manager to do so. When the target extension joins a call, the application using Single Step Conference receives the call’s aggregated RTP media stream via the recording device and records the call.

2. General Test Approach and Test Results

The interoperability compliance testing evaluated the ability of the CXone to carry out call recording in a variety of scenarios using DMCC Single Step Conference with AES and Communication Manager. A range of Avaya endpoints were used in the compliance testing all of which are listed in **Section 4**.

Because NICE CXone is located on Amazon Cloud and the Avaya solution is ‘on premise’ a VPN connection is required to allow CXone to connect to Avaya Aura® Application Enablement Services. The connection to Application Enablement Services makes use of TSAPI to collect and monitor events from the Avaya telephones sets and agents. DMCC Single Step Conference is used to record the calls where the CXone is conferenced into the call to allow a call recording to take place. Again, due to the nature of the setup involved, the RTP must be encrypted and sent over the public internet from the Avaya Media Gateway or Media Server to the CXone call recording solution on Amazon Cloud.

Note: There are a number of different ways to setup a VPN using a multiple of different platforms and these Application Notes do not serve to display the setup and configuration of one type of VPN over another. For compliance testing a peer-to-peer VPN was configured using Strongswan on the DevConnect side, allowing the DevConnect subnet to talk to the subnet where CXone was located.

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

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

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

For the testing associated with these Application Notes, the interface between Application Enablement Services and NICE CXone did not include use of any specific encryption features as requested by NICE, seen as this connection made use of a VPN. The audio media was sent over the public internet, and it was encrypted using SRTP.

2.1. Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on placing and recording calls in different call scenarios with good quality audio recordings and accurate call records. The tests included:

- **Inbound/Outbound calls** – Test call recording for inbound and outbound calls to the Communication Manager to and from PSTN callers.
- **Hold/Transferred/Conference calls** – Test call recording for calls transferred to and in conference with PSTN callers.
- **EC500 Calls/Forwarded calls** - Test call recording for calls terminated on Avaya DECT handsets using EC500.
- **Feature calls** - Test call recording for calls that are parked or picked up using Call Park and Call Pickup.
- **Calls to Elite Agents** – Test call recording for calls to Communication Manager agents logged into Avaya Agent for Desktop.
- **Serviceability testing** - The behavior of NICE CXone under different simulated failure conditions.

2.2. Test Results

All functionality and serviceability test cases were completed successfully.

2.3. Support

Technical support can be obtained for NICE CXone from the website

[https://help.nice-incontact.com/content/integratedsolutions/cxoneopen/cxoneopen.htm?TocPath= CXone%20Multi-ACD%7CCXone%20Multi-ACD%20\(CXone%20Open\)%7C_____0](https://help.nice-incontact.com/content/integratedsolutions/cxoneopen/cxoneopen.htm?TocPath= CXone%20Multi-ACD%7CCXone%20Multi-ACD%20(CXone%20Open)%7C_____0)

3. Reference Configuration

The configuration in **Figure 1** was used to compliance test NICE CXone with the Avaya solution using DMCC Single Step Conference to record calls. The NICE solution located on Amazon Cloud and makes use of a VPN connection to connect to AES to use DMCC Single Step Conference. The media from the Avaya Media Gateway or Media Server is encrypted and sent over the public internet to the NICE CXone.

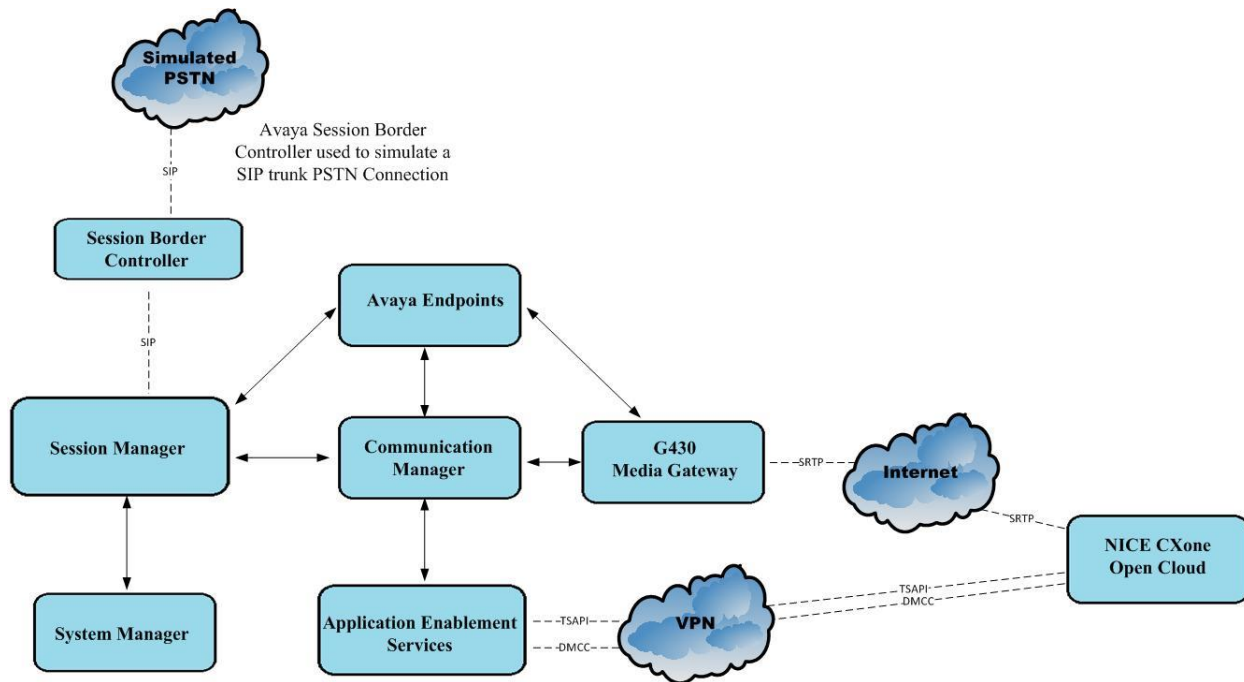


Figure 1: Connection of NICE CXone Multi-ACD v1.0 with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Application Enablement Services R10.1

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager	System Manager 10.1.3.0 Feature Pack 3 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.3.0.0715713
Avaya Aura® Session Manager	Session Manager R10.1 Build No. – 10.1.3.0.1013007
Avaya Aura® Communication Manager	R10.1.3.0 – FP3 R020x.01.0.974.0 Update ID 01.0.974.0-27893
Avaya Aura® Application Enablement Services	10.1.3 Build 10.1.3.0.0.11-0
Avaya Aura® Media Server	10.1.0.101
Avaya Media Gateway G430	42.7.0 /2
Avaya J100 Series (H323) Deskphone	6.8.5.3.2
Avaya J100 Series (SIP) Deskphone	4.0.14.0.7
Avaya 9404 Digital Deskphone	17.0
Avaya Agent for Desktop (SIP)	2.0.6.23.3005
Avaya Session Border Controller (to facilitate simulated PSTN)	10.1.0
Avaya DECT Handsets	3725 DH4 (R3.3.11) 3720 DH3 (R3.3.11)
NICE CXone Multi-ACD	1.0.0

All Avaya equipment is running on virtual servers on VMware.

5. Configure Avaya Aura® Communication Manager

The information provided in this section describes the configuration of Communication Manager relevant to this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

The configuration illustrated in this section was performed using Communication Manager System Administration Terminal (SAT).

5.1. Verify System Features

Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 4**, ensure that **Computer Telephony Adjunct Links?** is set to **y** as shown below.

display system-parameters customer-options		Page	4 of 12
OPTIONAL FEATURES			
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y
Access Security Gateway (ASG)?	y	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
Async. Transfer Mode (ATM) PNC?	n	Digital Loss Plan Modification?	y
Async. Transfer Mode (ATM) Trunking?	n	DS1 MSP?	y
ATM WAN Spare Processor?	n	DS1 Echo Cancellation?	y
ATMS?	y		
Attendant Vectoring?	y		
(NOTE: You must logoff & login to effect the permission changes.)			

5.2. Note procr IP Address for Avaya Aura® Application Enablement Services Connectivity

Display the Communication Manager (procr) IP address by using the command **display node-names ip** and note the IP address for the **procr** and the AES.

display node-names ip		Page	1 of 2
		IP NODE NAMES	
Name	IP Address		
SM100	10.10.40.12		
aespri101x	10.10.40.16		
default	0.0.0.0		
g450	10.10.40.15		
procr	10.10.40.13		

5.3. Configure IP-Codec

Use the **change ip-codec-set x** (where x is the ip-codec set used) command to designate a codec set compatible with CXone. During compliance testing the codecs shown below were offered to the CXone. The audio codec used between the stations may be different to the audio codec that is being used in single step conference but as long as the codec that is configure for CXone as per **Section 7.2** is listed below, and it is as **G.711A** is listed, the recording should be successful.

Because media is being sent over the public internet, Media Encryption must be used. Note that the **Media Encryption** set below must match that set in **Section 7.2**.

change ip-codec-set 1

Page 1 of 2

IP MEDIA PARAMETERS

Codec Set: 1

Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1: OPUS-SWB24K		1	20
2: G.722-64K		2	20
3: G.711A	n	2	20
4: G.711MU	n	2	20
5:			
6:			

Media Encryption

Encrypted SRTCP: best-effort

1: 1-srtp-aescm128-hmac80

2: none

3:

5.4. Configure Transport Link for Avaya Aura® Application Enablement Services Connectivity

To administer the transport link to AES, use the **change ip-services** command. On **Page 1** add an entry with the following values:

- **Service Type:** Should be set to AESVCS.
- **Enabled:** Set to y.
- **Local Node:** Set to the node name assigned for the “procr” in **Section 5.2**.
- **Local Port:** Retain the default value of **8765**.

change ip-services					Page	1 of	4
IP SERVICES							
Service	Enabled	Local	Local	Remote	Remote		
Type		Node	Port	Node	Port		
AESVCS	y	procr	8765				

Go to **Page 4** of the **ip-services** form and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case **aespri101x**.
- **Password:** Enter a password to be administered on AES.
- **Enabled:** Set to **y**.

Note: The password entered for **Password** field must match the password on AES in **Section 6.2**. The **AE Services Server** should match the administered name for the AES server; this is created as part of the AES installation and can be obtained from the AES server by typing **uname -n** at the Linux command prompt.

change ip-services				Page 4 of 4
AE Services Administration				
Server ID	AE Services Server	Password	Enabled	Status
1:	aespri101x	*****	y	in use
2:				
3:				

5.5. Configure CTI Link for TSAPI Service

Add a CTI link using the **add cti-link n** command. 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: 1990		
Type: ADJ-IP		
COR: 1		
Name: aespri101x		

5.6. Configure Virtual Stations for Single Step Conference

Add virtual stations to allow CXone record calls using Single Step Conference. Type **add station x** where x is the extension number of the station to be configured, also note this extension number for configuration required in **Section 7.3**. Note the **Security Code** and ensure that **IP SoftPhone** is set to **y**.

add station 33001		Page 1 of 6
STATION		
Extension: 33001	Lock Messages? n	BCC: 0
Type: 9620	Security Code: 1234	TN: 1
Port: S00101	Coverage Path 1:	COR: 1
Name: Recorder	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 33001	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english		
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	

5.7. Configure SIP Stations for Monitoring

Any SIP extension that is to be recorded requires some configuration changes to allow call recording. Changes of SIP phones on Communication Manager must be carried out from System Manager. Access the System Manager using a web browser by entering **https://<FQDNorIP>/SMGR**. Log in using appropriate credentials.

Note: The following shows changes a SIP extension and assumes that the SIP extension has been programmed correctly and is fully functioning.

System Manager

Not secure | https://10.10.40.10/network-login/

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

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.

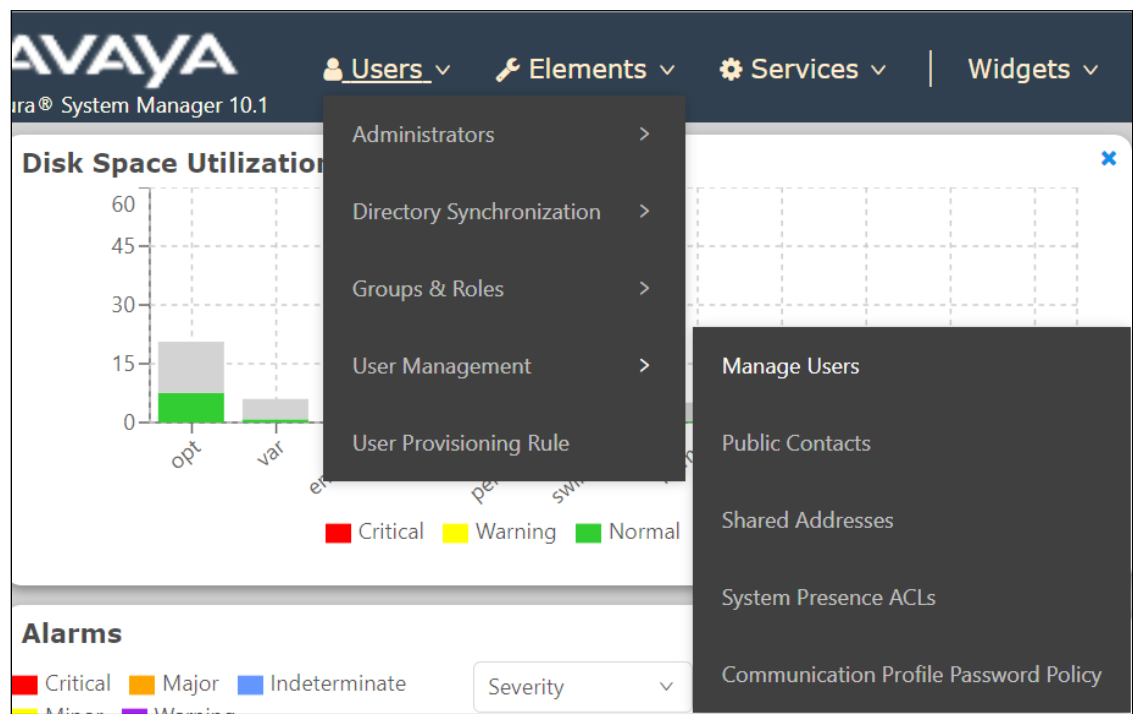
User ID:

Password:

[Change Password](#)

Supported Browsers: Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0).

From the home page click on **Users** → **User Management** → **Manage Users** as highlighted below.



Select the station to be edited and click on **Edit**. The example below shows that SIP extension **3101** is selected.

The screenshot shows the 'Manage Users' page in Avaya System Manager. The 'Edit' button is highlighted. A table lists users with columns: First Name, Surname, Display Name, Login Name, and SIP Handle. The first row, 'Agent One' with SIP Handle '3101', is selected.

	First Name	Surname	Display Name	Login Name	SIP Handle
<input checked="" type="checkbox"/>	Agent One	Workspaces	Agent One Workspaces	3101@greaney.sil6.ava ya.com	3101
<input type="checkbox"/>	Ascom	DECT_3181	DECT_3181, Ascom	3181@greaney.sil6.ava ya.com	3181
<input type="checkbox"/>	Ascom	DECT_3182	DECT_3182, Ascom	3182@greaney.sil6.ava ya.com	3182
<input type="checkbox"/>	admin	admin	Default Administrator	admin	
<input type="checkbox"/>	J179	H323	H323, J179	3001@greaney.sil6.ava ya.com	
<input type="checkbox"/>	Vantage01	K175	K175, Vantage01	3115@greaney.sil6.ava ya.com	3115
<input type="checkbox"/>	Paul	Greaney	Paul Greaney	paul@greaney.sil6.ava ya.com	
<input type="checkbox"/>	AAFD	SIP	SIP, AAFD	3111@greaney.sil6.ava ya.com	3111

Click on the **CM Endpoint Profile** tab in the left window. Click on **Endpoint Editor** to make changes to the SIP station.

Home / Users / Manage Users

Help ?

User Profile | Edit | 3101@greanep.sil6.avaya.com

Commit & Continue

Commit

Cancel

Identity

Communication Profile

Membership

Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile

Avaya Breeze® Profile

CM Endpoint Profile

* System : cm101x

* Profile Type : Endpoint

Use Existing Endpoints :

* Extension : 3101

Template : Start typing...

* Set Type : 9641SIPCC

Security Code : Enter Security Code

Port : S000003

Voice Mail Number : 6667

Preferred Handle : Select

Calculate Route Pattern :

Sip Trunk : aar

Editor

In the **General Options** tab ensure that **Class of Restriction** is set correctly. Set **Type of 3PCC Enabled** to **Avaya**. Click on **Done**, at the bottom of the screen once this is set, (not shown).

System cm101x

Extension 3101

Template Select

Set Type 9641SIPCC

Port S000003

Security Code

Name Agent One Workspaces

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)

* Class of Restriction (COR) 1

* Emergency Location Ext 3101

* Tenant Number 1

* SIP Trunk aar

Coverage Path 1

Lock Message

Multibyte Language Not Applicable

* Class Of Service (COS) 1

* Message Lamp Ext. 3101

Type of 3PCC Enabled Avaya

Coverage Path 2

Localized Display Name Agent One Workspaces

Enable Reachability for Station Domain Control system

SIP URI

Primary Session Manager

IPv4: 10.10.40.12

IPv6:

Click on **Commit** once this is done to save the changes (not shown).

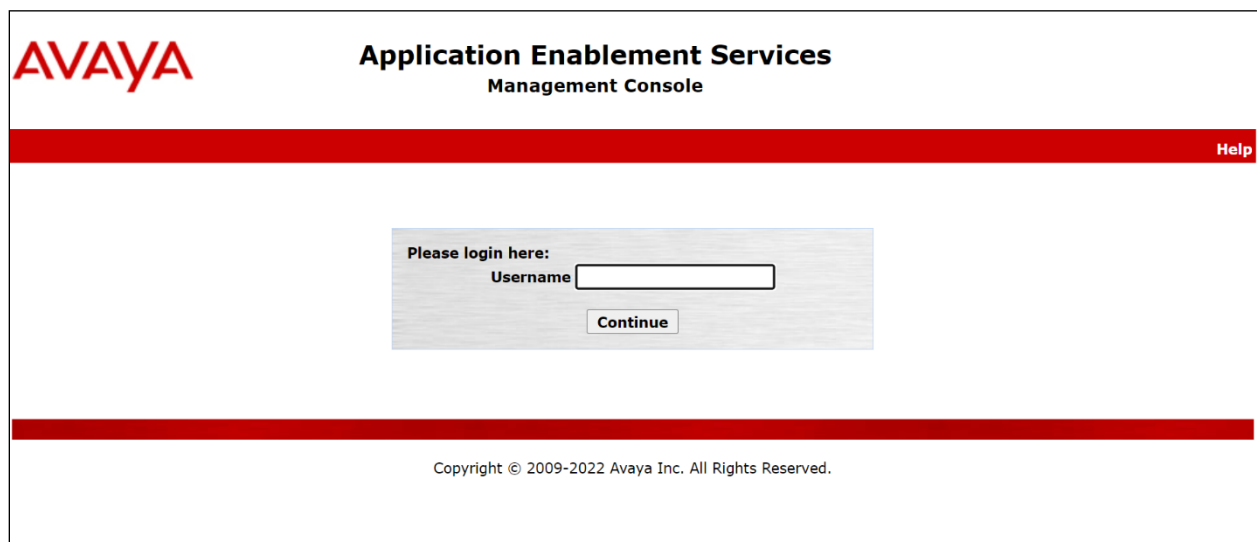
6. Configure Avaya Aura® Application Enablement Services

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

- Verify Licensing
- Create Switch Connection
- Administer TSAPI Link
- Identify Tlinks
- Configure Networking Ports
- Create CTI User
- Configure Security
- Restart AE Server

6.1. Verify Licensing

To access the AES Management Console, enter **https://<ip-addr>** as the URL in an internet browser, where <ip-addr> is the IP address of AES. At the login screen displayed, log in with the appropriate credentials and then select the **Login** button.



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 login box with the text "Please login here:" followed by a "Username" label and a text input field. A "Continue" button is positioned below the input field. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2022 Avaya Inc. All Rights Reserved." is displayed.

The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the **TSAPI Service** and **DMCC Service** are licensed by ensuring that the **License Mode** is showing **NORMAL MODE**. If not, contact an Avaya support representative to acquire the proper license for your solution.

AVAYA

Application Enablement Services

Management Console

Welcome: User cust

Last login: Wed Dec 6 15:03:14 G.M.T. 2023 from 10.10.40.242

Number of prior failed login attempts: 0

HostName/IP: aespri101x/10.10.40.16

Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE

SW Version: 10.1.3.1.0.49-0

Server Date and Time: Fri Dec 08 13:08:22 GMT 2023

HA Status: Not Configured

AE Services

Home | Help | Logout

▼ AE Services

▶ CVLAN

▶ DLG

▶ DMCC

▶ SMS

▶ TSAPI

▶ TWS

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

AE Services

DLG does not support Encrypted link. In case of GDPR (Data Privacy) enabled systems, use of DLG service will be site responsibility. By default DLG will be in running state

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A
Web Telephony Interface(WTI) Service	DOWN	Stopped	N/A	N/A
AE Services HA	Not Configured	N/A	N/A	N/A

The TSAPI and DMCC licenses are user licenses issued by the Web License Manager to which the Application Enablement Services server is pointed to. From the left window open **Licensing** and click on **WebLM Server Access** as shown below.

Licensing

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▼ Licensing

WebLM Server Address

WebLM Server Access

Reserved Licenses

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

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

NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page

The following screen shows the available licenses for **TSAPI** and **DMCC** users.

▼ Application_Enablement

View license capacity

View peak usage

ASBCE

▶ Session_Border_Controller_E_AE

AVAYA_OCEANA

▶ Avaya_Oceana

CCTR

▶ ContactCenter

CE

▶ COLLABORATION_ENVIRONMENT

COLLABORATION_DESIGNER

▶ Collaboration_Designer

COLLABORATIVE_BROWSING_SNAP-IN

▶ Collaborative_Browsing_Snap_In


COMMUNICATION_MANAGER

▶ Call_Center

▶ Communication_Manager

License File Host IDs:

Licensed Features

10 Items  Show

All ▼

Feature (License Keyword)	Expiration date	Licensed capacity
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	44
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	44
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	44
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	4
DLG VALUE_AES_DLG	permanent	44
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	44
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	4
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	44

6.2. Create Switch Connection

From the AES Management Console navigate to **Communication Manager Interface** → **Switch Connections** to set up a switch connection. Enter a name for the Switch Connection to be added and click the **Add Connection** button.

Application Enablement Services
Management Console

Welcome: User cust
Last login: Wed Dec 6 15:03:14 G.M.T. 2023 from 10.10.40.242
Number of prior failed login attempts: 0
HostName/IP: aespri101x/10.10.40.16
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.1.0.49-0
Server Date and Time: Fri Dec 08 13:09:31 GMT 2023
HA Status: Not Configured

Communication Manager Interface | Switch Connections
Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
High Availability
Licensing
Maintenance
Networking

Switch Connections

Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm101x	Yes	30	1

Edit Connection
Edit PE/CLAN IPs
Edit Signaling Details
Delete Connection
Survivability Hierarchy

In the resulting screen enter the **Switch Password**; the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.4**. Default values may be accepted for the remaining fields. Click **Apply** to save changes.

Communication Manager Interface | Switch Connections

AE Services

Communication Manager Interface

Switch Connections

Dial Plan

High Availability

Licensing

Maintenance

Networking

Security

Status

User Management

Connection Details - cm101x

Switch Password

.....

Confirm Switch Password

.....

Msg Period

30

Minutes (1 - 72)

Provide AE Services certificate to switch

☒

Secure H323 Connection

☐

Processor Ethernet

☒

Enable TLS Certificate Validation

☐

Apply

Cancel

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit PE/CLAN IPs** button. In the resulting screen, enter the IP address of the procr as shown in **Section 5.2** that will be used for the AES connection and select the **Add/Edit Name or IP** button.

Communication Manager Interface | Switch Connections

Home | Help | Logout

AE Services

Communication Manager Interface

Switch Connections

Dial Plan

High Availability

Licensing

Maintenance

Edit Processor Ethernet IP - cm101x

10.10.40.13

Add/Edit Name or IP

Name or IP Address	Status
10.10.40.13	In Use

Back

Clicking on **Edit Signaling Details** below brings up the H.323 Gatekeeper page.

AVAYA

Application Enablement Services
Management Console

Welcome: User cust
Last login: Wed Dec 6 15:03:14 G.M.T. 2023 from 10.10.40.242
Number of prior failed login attempts: 0
HostName/IP: aespri101x/10.10.40.16
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.1.0.49-0
Server Date and Time: Fri Dec 08 13:09:31 GMT 2023
HA Status: Not Configured

Communication Manager Interface | Switch Connections

Home | Help | Logout

AE Services

Communication Manager Interface

Switch Connections

Dial Plan

High Availability

Licensing

Maintenance

Networking

Switch Connections

Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm101x	Yes	30	1

Edit Connection

Edit PE/CLAN IPs

Edit Signaling Details

Delete Connection

Survivability Hierarchy

The IP address of Communication Manager is set for the **H.323 Gatekeeper**, as shown below.

Communication Manager Interface | Switch Connections

AE Services

Communication Manager Interface

Switch Connections

Dial Plan

High Availability

Licensing

Maintenance

Networking

Switch Connections

Edit H.323 Gatekeeper - cm101x

Add Name or IP

Name or IP Address

☒ 10.10.40.13

Delete IP

6.3. Administer TSAPI link

From the Application Enablement Services Management Console, select **AE Services** → **TSAPI** → **TSAPI Links**. Select **Add Link** button as shown in the screen below.

The screenshot shows the 'AE Services | TSAPI | TSAPI Links' console. On the left, a sidebar lists 'AE Services' (CVLAN, DLG, DMCC, SMS) and 'TSAPI' (TSAPI Links, TSAPI Properties). The main area is titled 'TSAPI Links' and contains three buttons: 'Add Link', 'Edit Link', and 'Delete Link'.

On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **cm101x**, which has already been configured in **Section 6.2** from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.5** which is **1**.
- **ASAI Link Version:** Version **12** was used for compliance testing but the latest version available can be chosen.
- **Security:** This can be left at the default value of **both**. An unencrypted TSAPI link was used.

Once completed, select **Apply Changes**.

The screenshot shows the 'AE Services | TSAPI | TSAPI Links' console with the 'Edit TSAPI Links' screen. The sidebar is the same as the previous screenshot. The main area is titled 'Edit TSAPI Links' and contains the following fields and buttons:

Link	Switch Connection	Switch CTI Link Number	ASAI Link Version	Security
1	cm101x	1	12	Both

Buttons: Apply Changes, Cancel Changes, Advanced Settings

6.4. Identify Tlinks

Navigate to **Security** → **Security Database** → **Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure the NICE CXone in **Section 7.2**. The Tlink for the unencrypted TSAPI link was used.

Security | Security Database | Tlinks

▶ **AE Services**

▶ **Communication Manager Interface**

High Availability

▶ **Licensing**

▶ **Maintenance**

▶ **Networking**

▼ **Security**

▶ Account Management

▶ Audit

▶ Certificate Management

Enterprise Directory

▶ Host AA

▶ PAM

▼ **Security Database**

▪ Control

⊕ CTI Users

▪ Devices

▪ Device Groups

▪ **Tlinks**

▪ Tlink Groups

▪ Worktops

Tlinks

Tlink Name

☒ AVAYA#CM101X#CSTA#AESPRI101X

☐ AVAYA#CM101X#CSTA-S#AESPRI101X

Delete Tlink

6.5. Configure Networking Ports

To ensure that TSAPI ports are enabled, navigate to **Networking → Ports**. Ensure that the TSAPI ports are set to **Enabled** as shown below. Ensure that the **DMCC Server Ports** are also **Enabled** and take note of the **Unencrypted Port 4721** which will be used later in **Section 7.2**.

Networking Ports				
<ul style="list-style-type: none"> ▶ 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			Enabled Disabled
		Unencrypted TCP Port	9999	<input checked="" type="radio"/> <input type="radio"/>
		Encrypted TCP Port	<input type="text" value="9998"/>	<input checked="" type="radio"/> <input type="radio"/>
	<hr/>			
	DLG Port	TCP Port	5678	
	<hr/>			
	TSAPI Ports			Enabled Disabled
		TSAPI Service Port	450	<input checked="" type="radio"/> <input type="radio"/>
		Local TLINK Ports		
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	<input type="text" value="1050"/>		
	TCP Port Max	<input type="text" value="1065"/>		
	Encrypted TLINK Ports			
	TCP Port Min	<input type="text" value="1066"/>		
	TCP Port Max	<input type="text" value="1081"/>		
<hr/>				
DMCC Server Ports			Enabled Disabled	
	Unencrypted Port	<input type="text" value="4721"/>	<input checked="" type="radio"/> <input type="radio"/>	
	Encrypted Port	<input type="text" value="4722"/>	<input checked="" type="radio"/> <input type="radio"/>	
	TR/87 Port	<input type="text" value="4723"/>	<input checked="" type="radio"/> <input type="radio"/>	
<hr/>				
H.323 Ports				
	TCP Port Min	<input type="text" value="20000"/>		
	TCP Port Max	<input type="text" value="29999"/>		
	Local UDP Port Min	<input type="text" value="20000"/>		
	Local UDP Port Max	<input type="text" value="29999"/>		
			Enabled Disabled	
	Server Media		<input checked="" type="radio"/> <input type="radio"/>	

6.6. Create CTI User

A User ID and password needs to be configured for the CXone to communicate with Application Enablement Services. Navigate to the **User Management** → **User Admin** screen then choose the **Add User** option.

The screenshot displays the 'User Management | User Admin' interface. On the left is a sidebar menu with the following items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management (expanded), Service Admin, User Admin (selected), Add User, Change User Password, List All Users, Modify Default Users, Search Users, Utilities, and Help. The main content area on the right is titled 'User Admin' and contains the text: 'User Admin provides you with the following options for managing AE Services users:'. Below this text is a bulleted list of options: Add User, Change User Password, List All Users, Modify Default User, and Search Users.

User Management User Admin	
<ul style="list-style-type: none">▶ AE Services▶ Communication Manager Interface▶ High Availability▶ Licensing▶ Maintenance▶ Networking▶ Security▶ Status▼ User Management<ul style="list-style-type: none">▶ Service Admin▼ User Admin<ul style="list-style-type: none">▪ Add User▪ Change User Password▪ List All Users▪ Modify Default Users▪ Search Users▶ Utilities▶ Help	<h3>User Admin</h3> <p>User Admin provides you with the following options for managing AE Services users:</p> <ul style="list-style-type: none">• Add User• Change User Password• List All Users• Modify Default User• Search Users

In the **Add User** screen shown below, enter the following values:

- **User Id** - This will be used by the CXone setup in **Section 7.2**.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with CXone setup in **Section 7.2**.
- **CT User** - Select **Yes** from the drop-down menu.

High Availability	* User Id	nice1
▶ Licensing	* Common Name	nice1
▶ Maintenance	* Surname	nice1
▶ Networking	User Password
▶ Security	Confirm Password
▶ Status	Admin Note	
▼ User Management	Avaya Role	None ▼
▶ Service Admin	Business Category	
▼ User Admin	Car License	
▪ Add User	CM Home	
▪ Change User Password	Css Home	
▪ List All Users	CT User	Yes ▼
▪ Modify Default Users	Department Number	
▪ Search Users	Display Name	
▶ Utilities	Employee Number	
▶ Help	Employee Type	
	Enterprise Handle	

Scroll down and click on **Apply Changes** (not shown).

6.7. Configure Security

The CTI user permissions and the database security are set under **Security Database**.

6.7.1. Configure Database Control

The security database can be set differently depending on the requirements of the customer in question. For compliance testing, the DevConnect lab was setup as shown below, however this may be changed by opening **Control** and ticking the boxes shown.

Note: Since the CTI user was given unrestricted access, as per **Section 6.7.2**, these values set here do not impact the overall setup.

The screenshot shows the 'Security' section of the Avaya DevConnect configuration interface. On the left is a navigation pane 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), 'Control' (selected), and 'CTI Users'. The main content area is titled 'SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services'. It contains two checkboxes: 'Enable SDB for DMCC Service' (unchecked) and 'Enable SDB for TSAPI Service, JTAPI and Telephony Web Services' (checked). Below the checkboxes is an 'Apply Changes' button.

Note: The AES Security Database (SDB) provides the ability to control a user's access privileges. The SDB stores information about Computer Telephony (CT) users and the devices they control. The DMCC service, the TSAPI service, and Telephony Web Services use this information for permission checking. Please look to **Section 10** for more information on this.

6.7.2. Associate Devices with CTI User

Navigate to **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the CTI user added in **Section 6.6** and click on **Edit Users**.

User ID	Common Name	Worktop Name	Device ID
<input checked="" type="radio"/> nice1	nice1	NONE	NONE
<input type="radio"/> paul1	paul1	NONE	NONE
<input type="radio"/> paul2	paul2	NONE	NONE
<input type="radio"/> sytel	Sytel	NONE	NONE

[Edit](#) [List All](#)

In the main window ensure that **Unrestricted Access** is ticked. Once this is done click on **Apply Changes**.

Edit CTI User

User Profile:

User ID: nice1
Common Name: nice1
Worktop Name: NONE ▾
Unrestricted Access: ☒

Call and Device Control:

Call Origination/Termination and Device Status: None ▾

Call and Device Monitoring:

Device Monitoring: None ▾
Calls On A Device Monitoring: None ▾
Call Monitoring: ☐

Routing Control:

Allow Routing on Listed Devices: None ▾

[Apply Changes](#) [Cancel Changes](#)

6.8. Restart AE Server

Once everything is configured correctly, it is best practice to restart AE Server (if possible), this will ensure that the new connections are brought up correctly. Click on the **Restart AE Server** button at the bottom of the screen.

Maintenance | Service Controller

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

Service Controller

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

A message confirming the restart will appear, click on **Restart** to proceed.

Maintenance | Service Controller

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

Restart AE Server

Warning! Are you sure you want to restart?
Restarting will cause all existing connections to be dropped and associations lost.

Restart

Cancel

7. Configure NICE CXone

The installation of CXone is usually carried out by an engineer from NICE and is outside the scope of these Application Notes. For information on the installation of the CXone contact NICE as per the information provided in **Section 2.3**.

The following sections will outline the process involved in connecting the NICE CXone to the Avaya Solution. All configuration of the CXone for connection with the AES is performed using a web browser connecting to the CXone. Open a web browser as shown navigate to **https://<CXoneIP>/** (not shown), enter the appropriate credentials and click on **Sign In**.

Sign In

paul_greaney@nice.com

Password

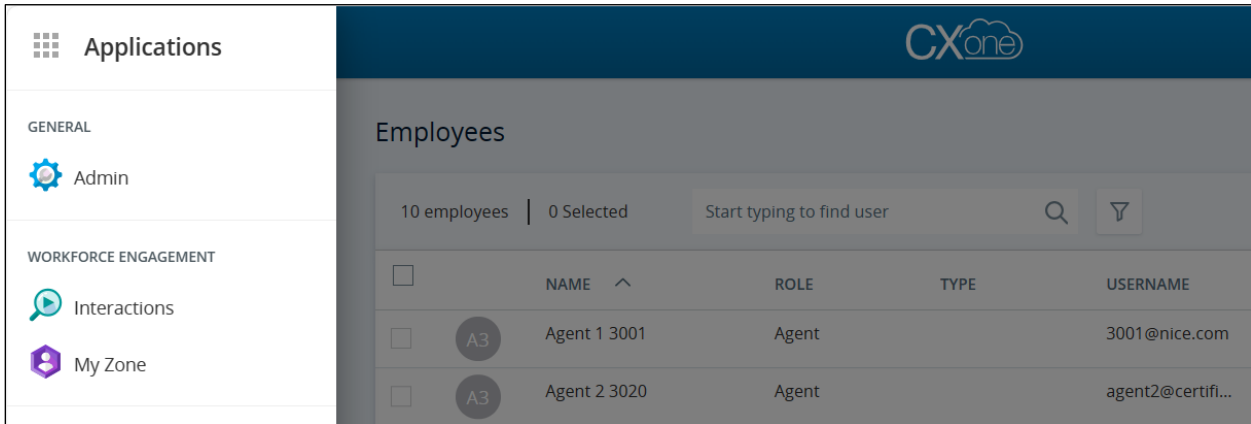
< Back Sign In

[Forgot your password?](#)

NICE · CXone

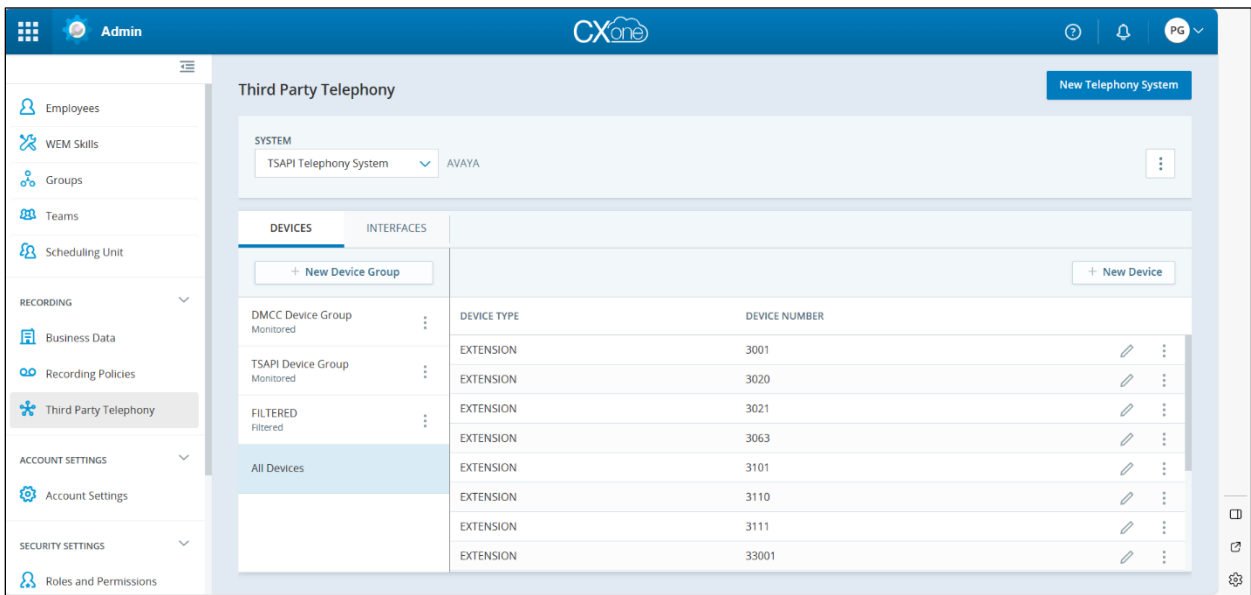
Copyright © 2005-2023 NICE LTD Inc. All Rights Reserved. [Contact Us](#)

Once logged in, ensure that the Admin Application is running. Click on **Applications** at the top left of the page and select **Admin**.



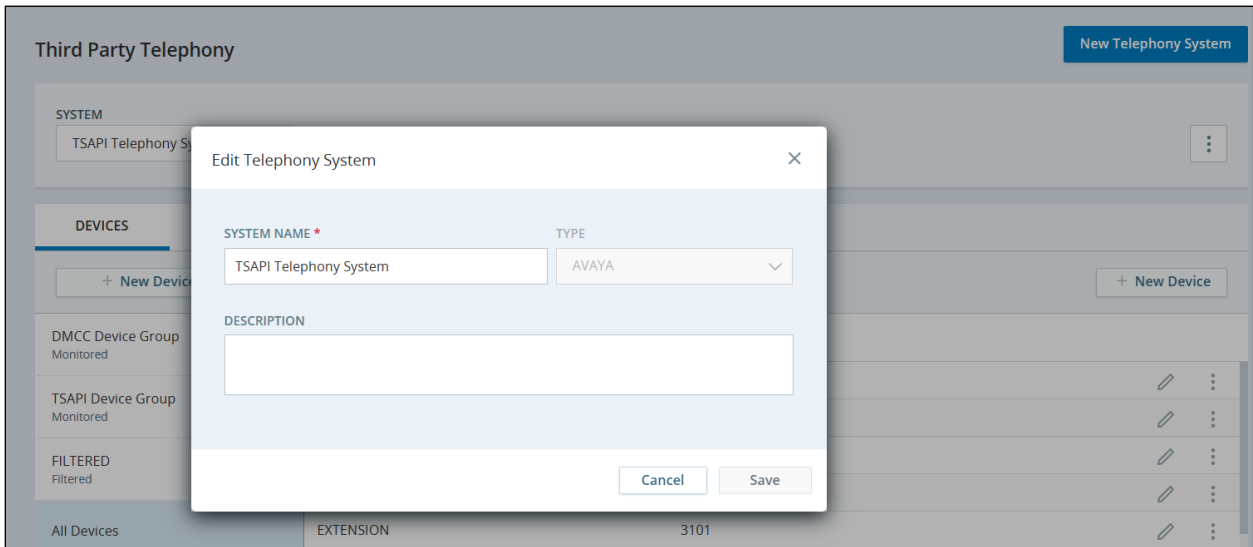
Under **Recording** in the left window, select **Third Party Telephony**. This section contains all the information on the connection to Application Enablement Services, both for TSAPI and DMCC. There are three areas that need to be configured.

- Telephony System
- Interfaces
- Devices



7.1. Configure Telephony System

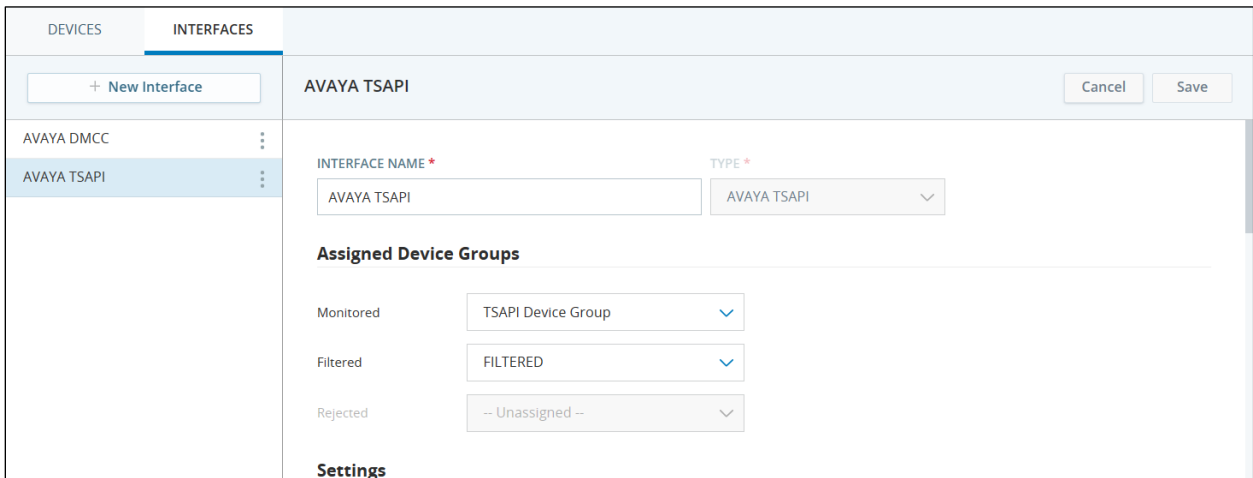
Like with everything else, this should be already configured during the initial installation. A new Telephony System can be added by clicking on **New Telephony System** at the top right of the screen. The screen below shows the existing system to show what needs to be configured for the connection to AES. Note that **Type** is set to **Avaya**.



The screenshot shows the 'Edit Telephony System' dialog box. The 'SYSTEM NAME' field contains 'TSAPI Telephony System'. The 'TYPE' dropdown is set to 'AVAYA'. The 'DESCRIPTION' field is empty. The dialog has 'Cancel' and 'Save' buttons. The background shows the 'Third Party Telephony' interface with a 'SYSTEM' tab and a 'DEVICES' tab.

7.2. Configure Interfaces

An Interface for both TSAPI and DMCC must be configured. A new Interface can be added by clicking on **+ New Interface** at the top left of the screen. The screen below shows details for the existing interface that was setup for TSAPI. Note that **Type** is set to **Avaya TSAPI** and the Device Group that was created for compliance testing is chosen for **Monitored**. Device Groups can be added under Devices which will be explained further in **Section 7.3**.



The screenshot shows the 'AVAYA TSAPI' interface configuration screen. The 'INTERFACE NAME' field contains 'AVAYA TSAPI'. The 'TYPE' dropdown is set to 'AVAYA TSAPI'. The 'Assigned Device Groups' section has three dropdowns: 'Monitored' (TSAPI Device Group), 'Filtered' (FILTERED), and 'Rejected' (-- Unassigned --). The 'Settings' section is visible at the bottom.

Scrolling down (from the previous screen), shows the **Avaya TSAPI Settings**. The **Server Name** should be the TLINK information from **Section 6.4**. The **Avaya IP Address** should be the IP address of the AES server. The **Login ID** and **Password** should match that of the CTI user created in **Section 6.6**. Once all the appropriate details have been entered click on **Save** to complete the TSAPI configuration (not shown).

AVAYA TSAPI

Settings

SERVER NAME *

AVAYA#CM101X#CSTA#AESPRI101X

AVAYA IP ADDRESS *

10.10.40.16

LOGIN ID *

nice1

PASSWORD *

.....

USE WARM STANDBY *

The Avaya DMCC interface can be configured as shown. A new Interface can be added by clicking on + **New Interface** at the top left of the screen. The screen below shows the existing interface that was configured for compliance testing. Note that **Type** is set to **Avaya DMCC** and **Monitored** is set to a preconfigured groups that was setup under **Devices**.

DEVICES

INTERFACES

+ New Interface

AVAYA DMCC

AVAYA TSAPI

AVAYA DMCC

INTERFACE NAME *

AVAYA DMCC

TYPE *

AVAYA DMCC

Assigned Device Groups

Monitored

DMCC Device Group

Filtered

-- Unassigned --

Rejected

-- Unassigned --

Settings

Cancel

Save

Scrolling down (from the previous page) shows the **Avaya DMCC Settings**. The **Symbolic Name** should match that of the name given to Communication Manager as per **Section 6.2**. The **Primary AES Server Address** will be that of the AES server and the **Primary AES DMCC Port** will either be **4721** or **4722** depending on whether a secure connection or unsecure connection is used. These port numbers should also be as per **Section 6.5**. The **Primary AES User Name** and **Password** should match that of the CTI user that was setup in **Section 6.6**.

AVAYA DMCC

Settings

SYMBOLIC NAME *

cm101x

PRIMARY AES SERVER ADDRESS *

10.10.40.16

PRIMARY AES DMCC PORT *

4721

PRIMARY AES USER NAME *

nice1

PRIMARY AES PASSWORD *

Scrolling down further (from the previous screen) shows the other configurations that were used for compliance testing.

AVAYA DMCC

PRIMARY AES PASSWORD *

.....

PRIMARY AES SECURED CONNECTION *

False

USE AES WARM STANDBY FEATURE *

False

SECONDARY AES SERVER ADDRESS

XXX.XXX.XXX.XXX

SECONDARY AES USER NAME

Scrolling down to the end reveals the **Device Password** that was entered and should match that of the password or 'security code' setup in **Section 5.6**. The **Codec** should match at least one of the Codecs in **Section 5.3**, along with the **Encryption Algorithm** that is being used. Click on **Save** to ensure any and all changes to the Avaya DMCC Interface are kept.

AVAYA DMCC Cancel Save

SECONDARY AES PASSWORD

DEVICE PASSWORD *

1234

CODEC *

G711A - 1

ENCRYPTION ALGORITHM *

AES_128_HMAC - 4

7.3. Configure Devices

Click on **Devices** in the left window, this will display all of the Devices that are to be monitored. For compliance testing the **DMCC Device Group** was added along with the **TSAPI Device Group**. The DMCC Device Group has all of the Virtual Stations (see **Section 5.6**) added, these are the stations that CXone uses for Single Step Conference to allow each call to be recorded. For compliance testing seven Avaya endpoints were being monitored so seven virtual stations were added so as all calls could be potentially recorded. A new extension/station can be added by clicking on + **New Device** at the right-hand side of the screen.

Third Party Telephony

New Telephony System

SYSTEM

TSAPI Telephony System

AVAYA

DEVICES

INTERFACES

+ New Device Group

+ New Device

	DEVICE TYPE	DEVICE NUMBER		
DMCC Device Group Monitored	EXTENSION	33002		
TSAPI Device Group Monitored	EXTENSION	33004		
FILTERED Filtered	EXTENSION	33001		
	EXTENSION	33003		
All Devices	EXTENSION	33007		
	EXTENSION	33005		
	EXTENSION	33006		

The following screen shows the configuration of extension **33001**.

Third Party Telephony

SYSTEM

TSAPI Telephony System

DEVICES

INTERFACES

+ New Device Group

DMCC Device Group Monitored

TSAPI Device Group Monitored

FILTERED Filtered

All Devices

EXTENSION

33006

EXTENSION *

33001

Assigned Device Groups

MONITORED

DMCC Device Group

FILTERED

FILTERED

REJECTED

-- Unassigned --

Cancel

Save

The **TSAPI Device Group** shows the list of Avaya endpoints that were monitored or recorded. A new group can always be added by clicking on + **New Device Group** at the left side of the screen, or a new device added to an existing group by clicking on + **New Device** at the right side of the screen. The **Device Numbers** shown below correspond with the station/extension numbers of the Avaya endpoints that were to be recorded.

DEVICES		INTERFACES	
+ New Device Group		+ New Device	
DMCC Device Group Monitored	⋮	DEVICE TYPE	DEVICE NUMBER
		EXTENSION	3020
TSAPI Device Group Monitored	⋮	EXTENSION	3021
		EXTENSION	3001
FILTERED Filtered	⋮	EXTENSION	3101
		EXTENSION	3063
All Devices		EXTENSION	3111
		EXTENSION	3110

Shown below is the configuration for extension **3001**, that was recorded.

Third Party Telephony

SYSTEM

TSAPI Telephony System

DEVICES

INTERFACES

+ New Device Group

DMCC Device Group
Monitored

TSAPI Device Group
Monitored

FILTERED
Filtered

All Devices

Edit Device

EXTENSION *

3001

Assigned Device Groups

MONITORED

TSAPI Device Group

FILTERED

-- Unassigned --

REJECTED

-- Unassigned --

Cancel

Save

EXTENSION

3110

8. Verification Steps

This section provides the steps that can be taken to verify correct configuration of the NICE CXone, Avaya Aura® Communication Manager, and Avaya Aura® Application Enablement Services.

8.1. Verify Avaya Aura® Communication Manager CTI Service State

Before the connection between the CXone and the AES is checked, check the connection between Communication Manager and AES to ensure it is functioning correctly. Check the AESVCS link status by using the command **status aesvcs cti-link**. Verify the **Service State** of the CTI link is **established**.

```
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	aespri101x	established	15	15
2	12	no	aessec101x	established	373	373
3	12	no	aes101xha	established	15	15

Use the command **list monitored-station** to get a list of stations that are being monitored. The list below should correspond with the same list of stations in **Section 7.3**.

```
list monitored-station
```

MONITORED STATION															
Associations:		1		2		3		4		5		6		7	
		CTI Lnk	CRV	CTI Lnk	CRV	CTI Lnk	CRV	CTI Lnk	CRV	CTI Lnk	CRV	CTI Lnk	CRV	CTI Lnk	CRV
Station Ext															
3001		1	0109												
3020		1	0107												
3021		1	0108												
3063		1	010B												
3101		1	010A												
3110		1	010D												
3111		1	010C												

Command successfully completed

8.2. Verify TSAPI Link

On the AES Management Console verify the status of the TSAPI link by selecting **Status** → **Status and Control** → **TSAPI Service Summary** to display the **TSAPI Link Details** screen. Verify the status of the TSAPI link by checking that the **Status** is **Talking** and the **State** is **Online**.

▶ 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	cm101x	1	Talking	Wed Dec 6 11:49:02 2023	Online	20	8	15	15	30

Online Offline

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

TSAPI Service Status TLink Status User Status

Clicking on **User Status** from the screen on the previous page should display something similar to that shown below, where the CXone user and corresponding **Tlink Name** are shown.

CTI User Status

☐ Enable page refresh every 60 seconds

CTI Users All Users Submit

Open Streams 4

Closed Streams 50

Open Streams

Name	Time Opened	Time Closed	Tlink Name
DMCCLCSUserDoNotModify	Thu 16 Nov 2023 01:15:02 PM GMT		AVAYA#CM101X#CSTA#AESPRI101X
DMCCLCSUserDoNotModify	Thu 16 Nov 2023 02:15:02 PM GMT		AVAYA#CM101X#CSTA#AESPRI101X
nice1	Wed 06 Dec 2023 11:49:04 AM GMT		AVAYA#CM101X#CSTA#AESPRI101X
nice1	Wed 06 Dec 2023 11:49:09 AM GMT		AVAYA#CM101X#CSTA#AESPRI101X

Show Closed Streams Close All Opened Streams Back

8.3. Verify DMCC link on AES

Verify the status of the DMCC link by selecting **Status** → **Status and Control** → **DMCC Service Summary** to display the **DMCC Service Summary – Session Summary** screen. The screen below shows that the user **nice1** is connected from the IP address **10.231.34.238**, which is the NICE CXone server's address. Note also that **7** is listed for the **# of Associated Devices** which corresponds to the seven recorders/virtual stations that were configured.

▶ 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 Dec 06 15:04:46 GMT 2023

Service Uptime: 20 days, 0 hours 49 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 1

Number of Existing Devices: 7

Number of Devices Created Since Service Boot: 7

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	AB04E752A2EBAC220 F67911B03705612-1	nice1	Avaya DMCC	10.231.34.238	XML Unencrypted	7

Terminate Sessions

Show Terminated Sessions

Item 1-1 of 1

1 Go

8.4. Verify calls are being recorded

From any of the monitored Avaya endpoints make a series of inbound and outbound calls. Once these calls are completed, they should be available for playback through a web browser to CXone.

Open a web browser as shown navigate to **https://<CXoneIP>/** (not shown), enter the appropriate credentials and click on **Sign In**.

Sign In

paul_greaney@nice.com

Password

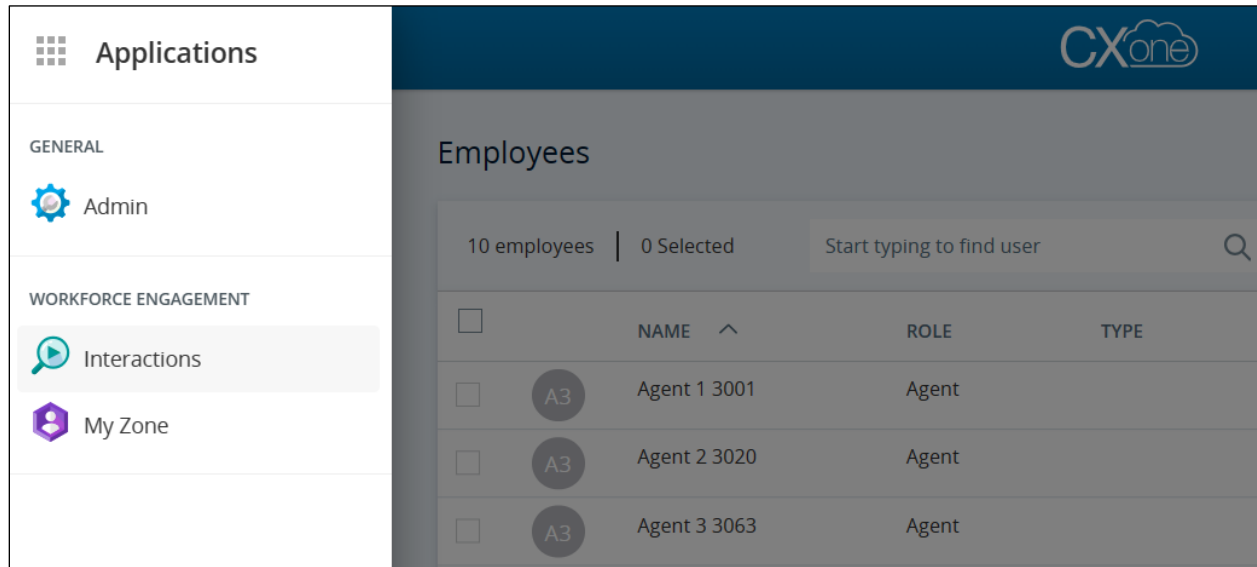
< Back Sign In

[Forgot your password?](#)

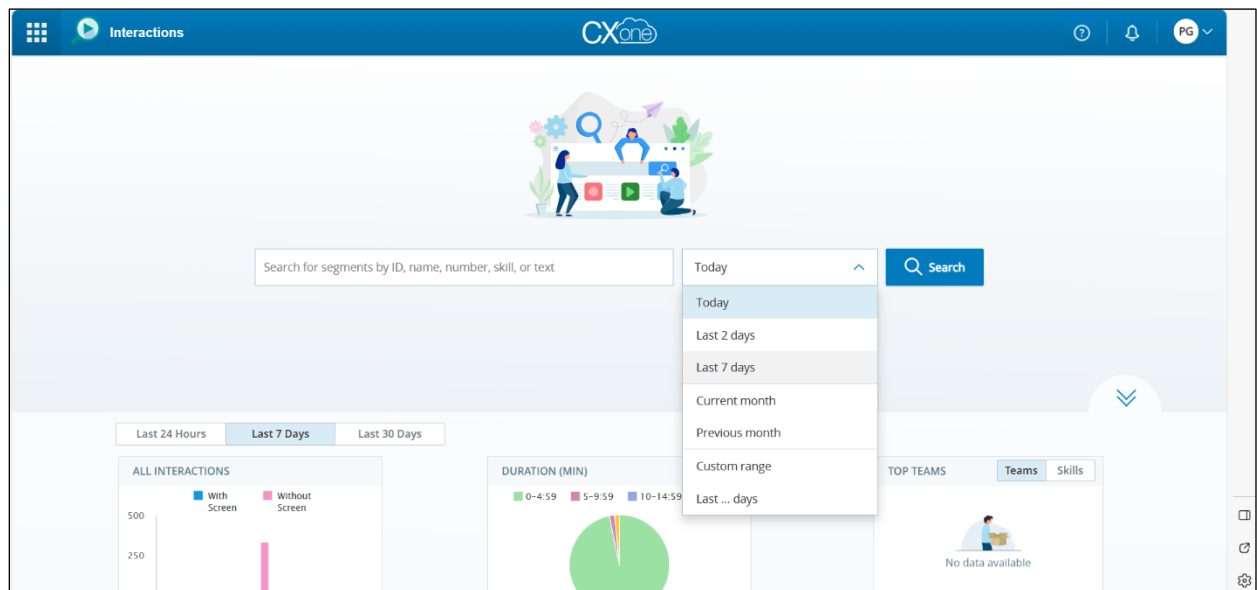
NICE · CXone

Copyright © 2005-2023 NICE LTD Inc. All Rights Reserved. [Contact Us](#)

Once logged in, select **Interactions** from the left window.



There are a number of ways to search for the appropriate recordings. One of the easiest ways is to select the last x number of days.



A list of recordings over the **Last 7 days** is shown. Clicking on the play icon on any one of these will play back that recording.

Found 329 segments | Dec 2, 2023 12:00:00 AM - Dec 8, 2023 11:59:59 PM

TYPE	AGENT NAME	START TIME	DURATION	DIRECT...	MASTER CONTACT	ORGANIZ...
	Agent 4 3101	Dec 6, 2023 11:51:18 AM	00:11 sec		3586681823	3539173...
	Agent 4 3101	Dec 6, 2023 11:49:30 AM	00:15 sec		3586681822	3539173...
	Agent 3 3063	Dec 6, 2023 11:47:21 AM	4:59:59 hrs		3586681821	...
	Agent 4 3101	Dec 6, 2023 11:47:14 AM	4:59:59 hrs		3586681819	3539173...
	Agent 1 3001	Dec 6, 2023 11:47:14 AM	01:11 min		3586681820	3539173...
	Agent 1 3001	Dec 6, 2023 11:43:17 AM	00:09 sec		3586681818	3539173...
	Agent 4 3101	Dec 6, 2023 11:43:13 AM	00:15 sec		3586681817	3539173...
	Agent 1 3001	Dec 6, 2023 11:42:29 AM	00:30 sec		3586681815	3539173...
	Agent 4 3101	Dec 6, 2023 11:42:29 AM	00:30 sec		3586681816	3539173...
	Agent 4 3101	Dec 6, 2023 11:40:51 AM	00:04 sec		3586681814	3539173...
	Agent 1 3001	Dec 6, 2023 11:38:17 AM	00:30 sec		3586681812	3539173...
	Agent 4 3101	Dec 6, 2023 11:38:17 AM	00:30 sec		3586681813	3539173...

A new window opens showing details of the recording and plays back the audio that was recorded.

Screen Recording Unavailable
Only audio recording can be played back.

Start: Dec 6, 2023 11:51:18 AM | End: Dec 6, 2023 11:51:29 AM | Playing 00:06 / 00:11

AUDIO RECORDING

Customer

Agent 4 3101

Interaction Details

TYPE	DIRECTION
CONTACT ID	START TIME
3586681823	Dec 6, 2023 11:51:18 AM
DURATION	AGENT NAME
11 sec	Agent 4 3101
AFTER CALL WORK	DISPOSITION
Not available	Not available

9. Conclusion

These Application Notes describe the configuration steps required for NICE CXone v1.0 to successfully interoperate with Avaya Aura® Communication Manager R10.1 using Avaya Aura® Application Enablement Services R10.1 to connect to using DMCC Single Step Conference to record calls. All feature functionality and serviceability test cases were completed successfully.

10. Additional References

This section references the Avaya and NICE product documentation that are relevant to these Application Notes.

Product documentation for Avaya products may be found at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® System Manager*. Release 10.1.x, Issue 6, June 2022.
- [2] *Administering Avaya Aura® Session Manager*. Release 10.1.x, Issue 3, April 2022.
- [3] *Administering Avaya Aura® Communication Manager*. Release 10.1, Issue 1, December 2021.
- [4] *Administering Avaya Aura® Application Enablement Services*. Release 10.1.x, Issue 4, April 2022.
- [5] *Implementing and Administering Avaya Aura® Media Server*. Release 10.1.x, Issue 2, July 2022.
- [6] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [7] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

Product documentation for NICE products may be found at:

[https://help.nice-incontact.com/content/integratedsolutions/cxoneopen/cxoneopen.htm?TocPath=CXone%20Multi-ACD%7CCXone%20Multi-ACD%20\(CXone%20Open\)%7C_____0](https://help.nice-incontact.com/content/integratedsolutions/cxoneopen/cxoneopen.htm?TocPath=CXone%20Multi-ACD%7CCXone%20Multi-ACD%20(CXone%20Open)%7C_____0)

©2024 Avaya LLC All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. 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.