



Avaya Solution & Interoperability Test Lab

Application Notes for NICE Inform Recorder with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using DMCC Multiple Registration in a 2N Dual Redundancy configuration - Issue 1.0

Abstract

These Application Notes describe the configuration steps for NICE Inform Recorder R9.2 to interoperate with the Avaya solution consisting of an Avaya Aura® Communication Manager R10.1 and Avaya Aura® Application Enablement Services R10.1 in a 2N dual redundancy configuration. Calls were recorded using DMCC Multiple Registration.

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 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 for the solution redundancy of NICE Inform Recorder R9.2 to interoperate with the Avaya solution consisting of an Avaya Aura® Communication Manager R10.1 and two Avaya Aura® Application Enablement Services R10.1 in a 2N Redundancy configuration. The Recorder uses Communication Manager's Multiple Registration feature via the Application Enablement Services (AES) Device, Media, and Call Control (DMCC) interface and the Telephony Services API (TSAPI) to capture the audio and call details for call recording on various Communication Manager H.323, SIP, Softphone and Digital endpoints, listed in **Section 4**.

NICE Trading Recorder (NTR) is a product equivalent to NICE Inform Recorder (NIR). NIR was used in this testing. **Attachment 1** is a Conformance Letter in which NICE declares the equivalency of the two products, the equivalent SW versions, and that testing with one product applies to both. For additional information contact NICE support as shown in **Section 2.3**.

The redundancy consists of two NICE servers connected to two AESs in a 2N redundancy configuration (Active/Active), which means that NICE server 1 is only connected to AES server 1 and NICE server 2 connected to AES server 2. There are no high availability options between servers, this is a 2N connection where the NICE to AES connection is duplicated with a second NICE to AES connection. Each of the two NICE servers operates independently making their own duplicate recordings of the calls. For testing purposes, the NICE Recording "All-in-One" deployment was chosen. 2N redundancy is also supported for the semi-distributed and fully distributed deployments.

The Avaya Telephony Services API (TSAPI) integration allows NIR to receive call-related events and metadata from AES. This integration must be paired with an audio capture method, in this case DMCC Multiple Registration 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 AE Services DMCC service to register itself as a recording device at the target extension. When the target extension joins a call, the application automatically receives the call's aggregated RTP media stream via the recording device and records the call.

NICE Inform Recorder is fully integrated into a LAN (Local Area Network) and includes easy-to-use Web based applications (i.e., NICE Application) that works with the Microsoft .NET framework and used to retrieve telephone conversations from a comprehensive long-term calls database. This application registers an extension with Communication Manager and waits for that extension to be dialed. NICE Inform Recorder contains tools for audio retrieval, centralized system security authorization, system control, and system status monitoring. Also included is a call parameters database that tightly integrates via CTI link PABXs and ACD's including optional advanced audio archive database management, search tools, a wide variety of

Recording-on-Demand capabilities, and comprehensive long-term call database for immediate retrieval.

2. General Test Approach and Test Results

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

The focus of these Application Notes and the compliance testing was on the redundancy capabilities of the NICE servers in a 2N configuration with AES. After each call was placed, recordings on both NICE servers were observed and verified. Various failure scenarios were played out by pulling the LAN cables from each of the NICE servers and the AES's.

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 Avaya systems and NICE Inform Recorder did not include use of any specific encryption features as requested by NICE.

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.
- **Feature calls** - Test call recording for using features such as Call Park and Call Pickup.

- **Calls to Elite Agents** – Test call recording for calls to Communication Manager Agents. These include calls to VDN's and to Hunt Groups.
- **Redundancy testing** - The behavior of NICE Inform Recorder under different simulated LAN failure conditions.

Redundancy Testing focuses on the following failover scenarios.

Failure and recovery to each component.

1. Pull LAN cable on AES 1, make test calls and observe recordings on NICE server 1 and NICE server 2.
2. Plug back in LAN cable on AES1, make test calls and observe recordings on NICE server 1 and server 2.
3. Pull LAN cable on AES 2, make test calls and observe recordings on NICE server 1 and server 2.
4. Plug back in LAN cable on AES2, make test calls and observe recordings on NICE server 1 and server 2.
5. Pull LAN cable on NICE_Rec1, make test calls and observe recordings on NICE server 1 and server 2.
6. Plug back in LAN cable on NICE_Rec1, make test calls and observe recordings on NICE server 1 and server 2.
7. Pull LAN cable on NICE_Rec2, make test calls and observe recordings on NICE server 1 and server 2.
8. Plug back in LAN cable on NICE_Rec2, make test calls and observe recordings on NICE server 1 and server 2.

Failure and recovery to each side.

9. Pull LAN cable on AES 1 and NICE_Rec1, make test calls and observe recordings on NICE server 1 and server 2.
10. Plug back in cable on AES 1 and NICE_Rec1, make test calls and observe recordings on NICE server 1 and server 2.
11. Pull LAN cable on AES 2 and NICE_Rec2, make test calls and observe recordings on NICE server 1 and server 2.
12. Plug back in cable on AES 2 and NICE_Rec2, make test calls and observe recordings on NICE server 1 and server 2.

Total AES failure.

13. Pull LAN cable on AES 1 and AES 2, make test calls and observe recordings on NICE server 1 and server 2. (Only need to test one call here as no recordings expected).
14. Plug back in AES 1 and AES 2, make test calls and observe recordings on NICE server 1 and server 2.

Total NICE failure.

15. Pull LAN cable on NICE_Rec1 and NICE_Rec2, make test calls and observe recordings on NICE server 1 and server 2. (Only need to test one call here as no recordings expected).

16. Plug back in NICE_Rec1 and NICE_Rec2, make test calls and observe recordings on NICE server 1 and server 2.

2.2. Test Results

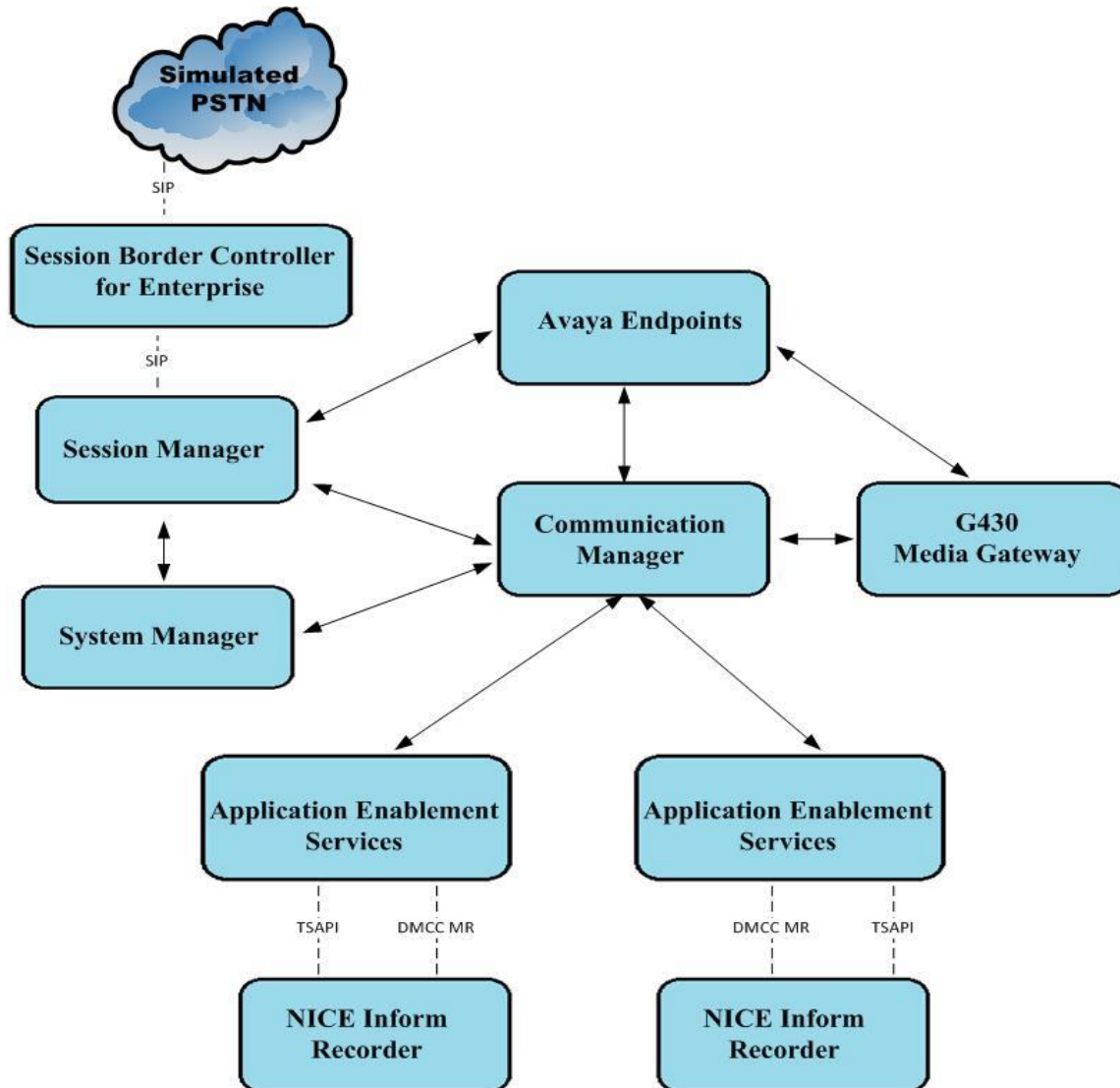
All functionality and redundancy test cases were completed successfully. There were no issues observed during compliance testing. The following observation was noted, for conference or transferred calls there may be multiple recordings present as each of the endpoints may be monitored and would result in duplicate recordings.

2.3. Support

Product documentation for NICE products may be found on ExtraNICE at:
<https://www.extranice.com/Security/Pages/default.aspx>
(ExtraNICE user account and password required)

3. Reference Configuration

The configuration in **Figure 1** was used to compliance test NICE Inform Recorder with the Avaya solution using DMCC Multiple Registration to record calls. The NICE server is setup for DMCC Multiple Registration mode and connects to the AES. The setup below is a “2N” redundancy configuration with the NICE to AES connection doubled. Communication Manager then has two “switch connections” to AES.



NICE Inform Recorder makes use of the 2N Redundancy configuration connecting two separate call recording servers to two standalone Application Enablement Services servers with a DMCC connection using Multiple Registration for recording calls.

Figure 1: Connection of solution redundancy of NICE Inform Recorder 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	10.1.0.0 Build No. – 10.1.0.0.537353 SW Update Revision No: 10.1.0.0.0614254
Avaya Aura® Session Manager	10.1 Build No. – 10.1.0.0.1010105
Avaya Aura® Communication Manager	10.1.0.1.0-SP1 Update ID 01.0.974.0-27372
Avaya Aura® Application Enablement Services Primary Server	10.1.0 Build 10.1.0.1.0.7-0
Avaya Aura® Application Enablement Services Secondary Server	10.1.0 Build 10.1.0.1.0.7-0
Avaya Session Border Controller for Enterprise	8.1.3.0-31-21052
Avaya G430 Media Gateway	41.16.0/1
Avaya J100 Series (H.323)	6.8304
Avaya J100 Series (SIP)	4.0.7.1.5
Avaya 9408 Digital Phone	2.00
Avaya Agent for Desktop (SIP)	2.0.6.23.3005
Avaya Workplace for Windows	3.28.0.73
NICE Inform Recorder (NIR) “All-in-one” configuration, running on Windows Server 2019 Avaya TSAPI Client Avaya DMCC .NET Note: This NIR integration version is equivalent to NTR integration version 10.5.22.	NIR 9.2.1 with UP2 NICE Avaya DMCC Integration 80.3.4 8.0.1 4.7.1

Note: The Avaya Aura® platform is running 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? n	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			

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

Display the procr IP address by using the command **display node-names ip** and noting the IP address for the **procr**.

display node-names ip		Page	1 of 2
		IP NODE NAMES	
Name	IP Address		
SM100	10.10.40.12		
aespril01x	10.10.40.16		
aessecl01x	10.10.40.46		
g450	10.10.40.15		
procr	10.10.40.13		

5.3. 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 3
IP SERVICES						
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port	
AESVCS	y	procr	8765			

Go to **Page 3** 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 the AES server.
- **Enabled:** Set to **y**.

Note: The two AES server links will be added on **Page 3**, one for **aespri101x** and another for **aessec101x**.

Note: The password entered for **Password** field must match the password on the AES server 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	3 of 3
AE Services Administration					
Server ID	AE Services Server	Password	Enabled	Status	
1:	aespri101x	*****	y	in use	
2:	aessec101x	*****	y	in use	
3:					

5.4. 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.

Note: If CTI links are already configured on Communication Manager the next available CTI links will be used.

Note: This step will be repeated for the second AES server by adding CTI link 2.

add cti-link 1		Page 1 of 3
CTI LINK		
CTI Link: 1		
Extension: 3990		
Type: ADJ-IP		
		COR: 1
Name: aespri101x		

5.5. Configure H.323 Stations for Multiple Registration

All endpoints that are to be monitored by NICE will need to have IP Softphone set to Y. IP Softphone must be enabled in order for Multiple Registration to work. Type **change station x** where x is the extension number of the station to be monitored also note this extension number for configuration required during the NICE recorder setup in **Section 7**. Note the **Security Code** and ensure that **IP SoftPhone** is set to **y**.

change station x		Page 1 of 6
STATION		
Extension: x	Lock Messages? n	BCC: 0
Type: 9608	Security Code: 1234	TN: 1
Port: S00101	Coverage Path 1:	COR: 1
Name: Extension	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Time of Day Lock Table:		
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 1591	
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	

5.6. Configure SIP Stations for Multiple Registration

Each Avaya SIP endpoint or station that needs to be monitored for call recording will need to have “Type of 3PCC Enabled” set to “Avaya” and “IP Softphone” enabled. Changes to SIP phones on Communication Manager must be carried out from System Manager. Access the System Manager using a Web Browser by entering **http://<FQDN>/network-login**, where **<FQDN>** is the fully qualified domain name of System Manager or the IP address of System Manager can be used as an alternative to the FQDN. 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.

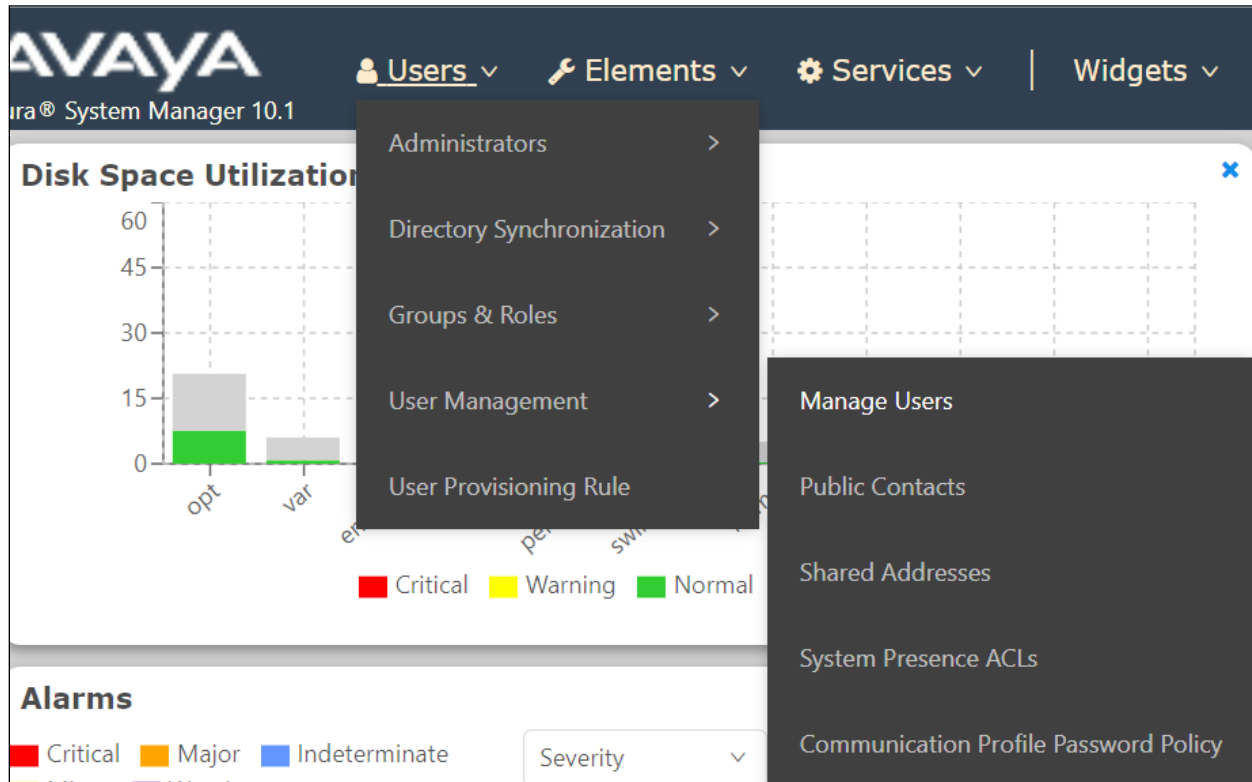
User ID:

Password:

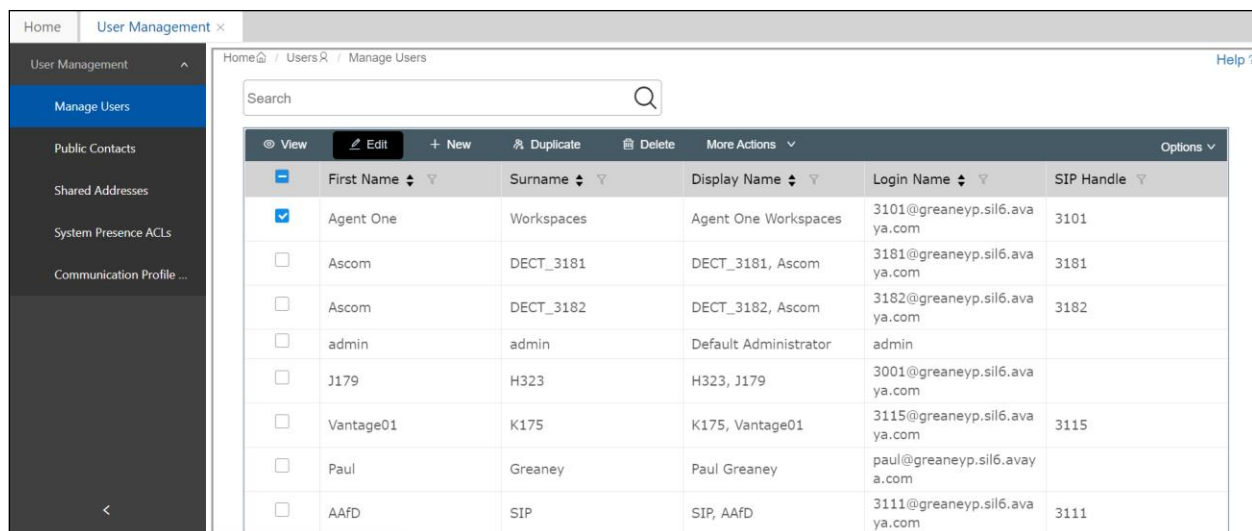
[Change Password](#)

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 shown below.



Click on **Manager Users** in the left window. Select the station to be edited and click on **Edit**.



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

In the **General Options** tab ensure that **Type of 3PCC Enabled** is set to **Avaya** as is shown below.

Click on the **Feature Options** tab and ensure that **IP Softphone** is ticked as shown. Click on **Done**, at the bottom of the screen (not shown), once this is set.

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 MWI Served User Type Per Station CPN - Send Calling Number IP Phone Group ID Remote Soft Phone Emergency Calls LWC Reception AUDIX Name Short/Prefixed Registration Allowed Voice Mail Number Bridging Tone for This Extension	single None None as-on-local spe None default 6667 no	Auto Answer Coverage After Forwarding Display Language Hunt-to Station Loss Group Survivable COR Time of Day Lock Table Music Source	none system english 19 internal None	
Features <div> <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 type="checkbox"/> Idle Appearance Preference <input checked="" type="checkbox"/> IP SoftPhone <input checked="" type="checkbox"/> LWC Activation <input type="checkbox"/> CDR Privacy <input checked="" type="checkbox"/> Precedence Call Waiting </div>				

Click on **Commit** once this is done to save the changes.

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
*** Extension :** 3101
*** Set Type :** 9641SIPCC
Port : S000003
Preferred Handle : Select
Sip Trunk : aar

Use Existing Endpoints :
Template :
Security Code :
Voice Mail Number : 6667
Calculate Route Pattern :

6. Configure Avaya Aura® Application Enablement Services

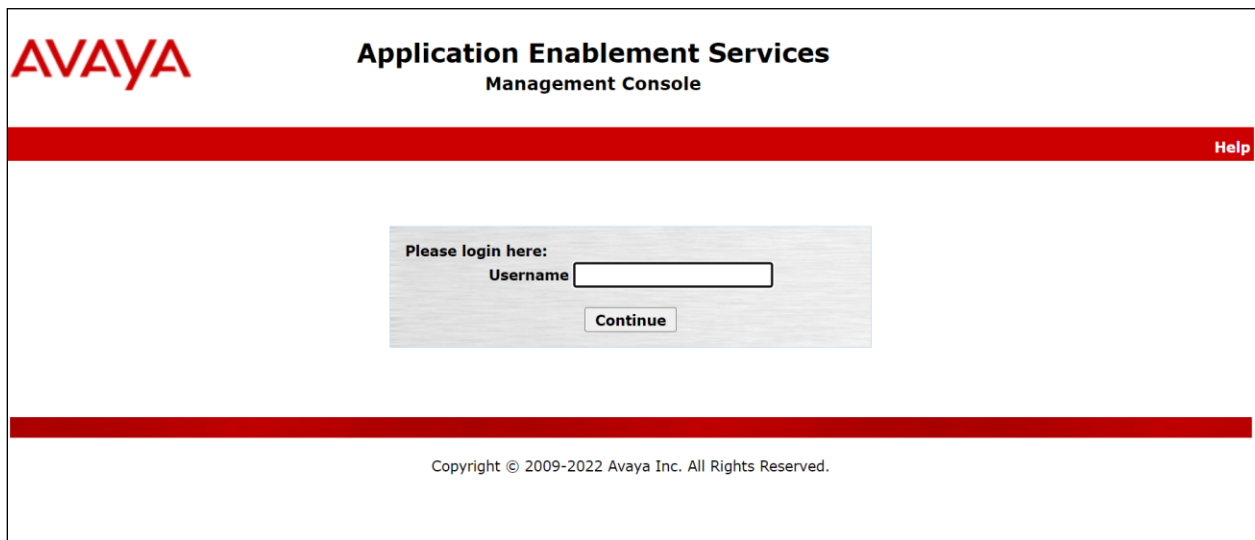
This section provides the procedures for configuring Application Enablement Services. The procedures fall into the following areas:

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

Note: With the Avaya setup using two AES servers, the same configuration will be performed on aespri101x and aessec101x. For compliance testing a TSAPI user nice1 was configured on aespri101x and nice2 on aessec101x, the following shows the configuration on aespri101x only.

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 displays 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' is displayed in a large, bold font, with 'Management Console' in a smaller font below it. A red horizontal bar spans the width of the page, containing a 'Help' link on the right. The main content area features a light gray box with the text 'Please login here:' followed by a 'Username' label and a text input field. Below the input field is a 'Continue' button. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice 'Copyright © 2009-2022 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 and DMCC Services are licensed by ensuring that **TSAPI Service** and **DMCC Service** are in the list of **Services** and that the **License Mode** is showing **NORMAL MODE**. If not, contact an Avaya support representative to acquire the appropriate license.

The screenshot shows the 'AE Services' management console. On the left is a navigation menu with options like CVLAN, DLG, DMCC, SMS, TSAPI, TWS, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The 'Licensing' option is highlighted. The main content area is titled 'AE Services' and contains an important note: 'IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.' Below this is a table listing services and their status.

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
AE Services HA	Not Configured	N/A	N/A	N/A

Below the table, there is a note: 'For status on actual services, please use [Status and Control](#)'. Another note says: '* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.' At the bottom, there is a 'License Information' section stating: 'You are licensed to run Application Enablement (CTI) release 8.x'.

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.

The screenshot shows the 'Licensing' management console. The left navigation menu has 'Licensing' highlighted. The main content area is titled 'Licensing' and contains instructions for setting up and maintaining the WebLM. It lists three options: 'WebLM Server Address', 'WebLM Server Access', and 'Reserved Licenses'. The 'WebLM Server Access' option is highlighted in blue. A red note at the bottom states: '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. Switch Connection to Avaya Aura® Communication Manager

Typically, the connection between the AES and Communication Manager is setup as part of the initial installation and would not usually be outlined in these Application Notes. Due to the nature of this particular setup with two connections from Communication Manager to two separate AES's the switch connection will be displayed on this section. From the AES Management Console navigate to **Communication Manager Interface → Switch Connections**, the connection to Communication Manager should be present as shown below but if one is not present one can be added by clicking on **Add Connection**.

Application Enablement Services

Management Console

Welcome: User cust

Last login: Fri Sep 9 17:54:25 2022 from 192.168.40.240

Number of prior failed login attempts: 0

HostName/IP: aespri101x/10.10.40.16

Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE

SW Version: 10.1.0.1.0.7-0

Server Date and Time: Tue Sep 20 15:52:43 IST 2022

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

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

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 5.3**. A connection from the NICE server to the AES could not be made with **Secure H323 Connection** ticked and so this was left unticked, as shown below. Click **Apply** to save changes.

Communication Manager Interface | Switch Connections

Connection Details - cm101x

Switch Password: [Masked]

Confirm Switch Password: [Masked]

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 (not shown), see screen at the bottom of the previous page. 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


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.



Application Enablement Services
Management Console

Welcome: User cust
Last login: Fri Sep 9 17:54:25 2022 from 192.168.40.240
Number of prior failed login attempts: 0
HostName/IP: aespri101x/10.10.40.16
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.1.0.7-0
Server Date and Time: Tue Sep 20 15:52:43 IST 2022
HA Status: Not Configured

Communication Manager Interface | Switch ConnectionsHome | Help | Logout

▶ AE Services

▼ Communication Manager Interface

Switch Connections

▶ Dial Plan

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

Switch Connections

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

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

Name or IP Address

☒ 10.10.40.13

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' interface. 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 a table with headers 'Link' and 'Switch Connection'. Below the table are 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 5.4** which is **1**.
- **ASAI Link 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**.

Once completed, select **Apply Changes**.

The screenshot shows the 'Edit TSAPI Links' screen. The sidebar is similar to the previous screen but includes 'TWS' and 'Communication Manager Interface' under 'TSAPI'. The main area is titled 'Edit TSAPI Links' and contains the following fields: 'Link' (set to 1), 'Switch Connection' (set to cm101x), 'Switch CTI Link Number' (set to 1), 'ASAI Link Version' (set to 12), and 'Security' (set to Both). At the bottom are three buttons: 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'.

Another screen appears for confirmation of the changes made. Choose **Apply**.

Apply Changes to Link
Warning! Are you sure you want to apply the changes?
These changes can only take effect when the TSAPI server restarts.
 **Please use the Maintenance -> Service Controller page to restart the TSAPI server.**

When the TSAPI Link is completed, it should resemble the screen below.

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<input checked="" type="radio"/> 1	cm101x	1	12	Both

6.4. Identify Tlinks

Navigate to **Security** → **Security Database** → **Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure NICE Inform Recorder in **Section 7**.

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. Enable TSAPI and DMCC 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**.

▶ 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			Enabled	Disabled
CVLAN Ports				
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"/>
DLG Port				
TCP Port	5678			
TSAPI Ports				
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"/>			
DMCC Server Ports				
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"/>

6.6. Create CTI User

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

Note: In the example below a user called nice1 was created for AES1 and nice2 created for AES2. The same username 'nice' could be created on both AES's.

Note: If there was one AES and two NICE recorders these two recorders could use the same User ID and Password again only requiring one user to be setup on the AES for both recorders.

User Management | User Admin

User Admin

User Admin provides you with the following options for managing AE Services users:

- 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 NICE Inform Recorder setup in **Section 7**.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with the NICE Inform Recorder setup in **Section 7**.
- **CT User** - Select **Yes** from the drop-down menu.

Click on **Apply Changes** at the bottom of the screen (not shown).

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	

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.

The screenshot shows a web-based configuration interface. On the left is a navigation menu with the following items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security (expanded), Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database (expanded), 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.

SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services	
<input type="checkbox"/>	Enable SDB for DMCC Service
<input checked="" type="checkbox"/>	Enable SDB for TSAPI Service, JTAPI and Telephony Web Services
<button>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**.

The screenshot shows the 'CTI Users' interface. On the left is a navigation menu with categories: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, and Security. Under Security, the 'Security Database' is expanded, showing 'CTI Users' with sub-options 'List All Users' and 'Search Users'. The main area displays a table of CTI 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

Below the table are 'Edit' and 'List All' buttons.

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

The 'Edit CTI User' form displays configuration options for the selected user 'nice1'.

User Profile:	User ID	nice1
	Common Name	nice1
	Worktop Name	NONE ▾
	Unrestricted Access	<input checked="" type="checkbox"/>
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	<input type="checkbox"/>
Routing Control:	Allow Routing on Listed Devices	None ▾

At the bottom are 'Apply Changes' and 'Cancel Changes' buttons.

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](#)

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart 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.

RestartCancel

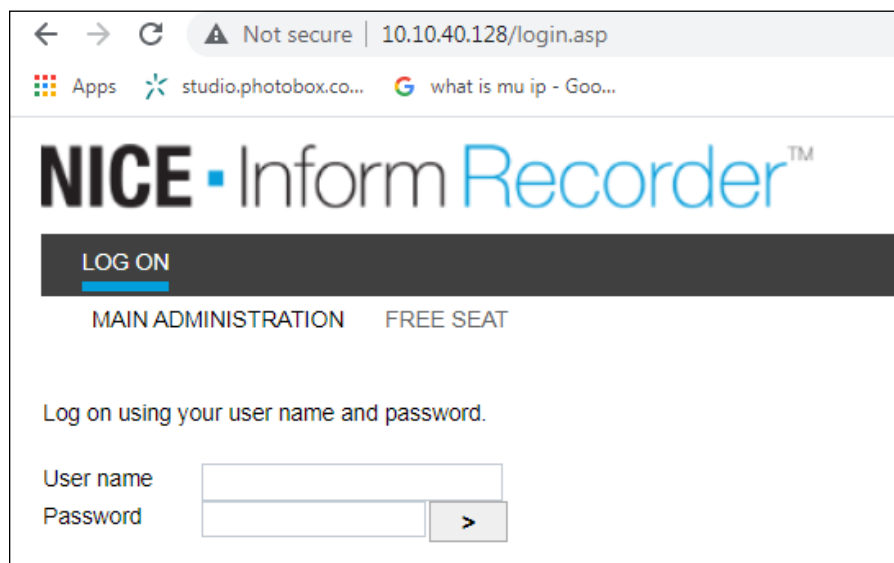
7. Configure NICE Inform Recorder

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

The following sections will outline the process involved in connecting NICE Inform Recorder to the Avaya solution. All configuration of NICE Inform Recorder for connection with the AES is performed using a web browser connecting to the NICE Inform Recorder Application Server. Open a web browser as shown navigate to **http://<NICE ServerIP>/** as shown below and enter the appropriate credentials and log in.

Note: Internet Explorer 11 or Edge (Chromium) should be used to connect to NICE Inform Recorder.

Note: Information on the connection to Avaya is gathered prior to any installation. This information includes the connection to the AES as well as devices to be monitored along with any AES usernames, passwords that need to be used for the connection. During the installation the connections to AES/Communication Manager are setup and created and therefore these Application Notes can only show the existing connections that were created during setup.



The screenshot shows a web browser window with the address bar displaying "10.10.40.128/login.asp". The page title is "NICE Inform Recorder™". Below the title is a dark grey bar with the text "LOG ON" in white. Underneath this bar are two links: "MAIN ADMINISTRATION" and "FREE SEAT". The main content area contains the text "Log on using your user name and password." followed by two input fields: "User name" and "Password". The "Password" field has a small grey button with a right-pointing arrow next to it.

Once logged in, click on the **CTI INTEGRATION** tab.

The screenshot shows the NICE Inform Recorder interface. The top navigation bar includes: MY ACCOUNT, SYSTEM INSTALLATION, CTI INTEGRATION (highlighted), SYSTEM CONFIGURATION, USER ADMINISTRATION, SYSTEM STATUS, and RECORDED CALLS. The user is logged in as 'service (service)' with a 'Logout' link. The 'MY SETTINGS' section contains three panels:

- Details for user account service (2)**: Fields for User name (service), Old password, New password, New password confirmation, First name (service), Last name, and Email addresses.
- Properties for user account service (2)**: Fields for User authentication method (System authentication), Seating (No seat), Fixed seating channel, Free seating extension, Group (Administrators), and User language (Dict. 0: [ENG] English).
- Calls preferences for user account service (2)**: Fields for Default search query (Default query: Calls made last week), Default calls listing view (Avaya view), and Auto start playback (checked).

At the bottom right are 'Cancel' and 'Save changes' buttons.

Within this tab there are other tabs as shown in the screen below, **cti servers**, **links**, **link groups**, **targets** etc. Clicking on the **CTI SERVERS** tab will show the CTI server set up during the installation. By clicking on the edit icon, changes can be made to this if deemed necessary.

The screenshot shows the NICE Inform Recorder interface with the 'CTI INTEGRATION' tab selected. The sub-tab 'CTI SERVERS' is active, showing a table of CTI servers. The table has columns: CTI server ID, CTI server alias, Computer name, and IP-address. There is one server listed: ID 1, alias 'CTI server 1', computer name 'NICENIR-A', and IP address '10.10.40.128'. Below the table is a 'CTI server setup' section with fields for CTI server alias (CTI server 1), CTI server host name (NICENIR-A), and CTI server host IP address (10.10.40.128).

CTI server ID	CTI server alias	Computer name	IP-address
1	CTI server 1	NICENIR-A	10.10.40.128

CTI server setup

CTI server alias: CTI server 1
CTI server host name: NICENIR-A
CTI server host IP address: 10.10.40.128

The link to AES is configured during the installation of NICE Inform Recorder, however this connection may need to be altered and if so, click on the edit icon as shown below.

Under the **LINKS** tab the existing link to AES is shown and can be edited by clicking on the pencil icon opposite the link.

Link alias	Link name	CTI server name	Link en...	Connection...	Auto-discovery en...	Link state	Link group	Date last modif...
AvayaAes1	AVAYALNK01	CTI server 1	✓	TCP / IP	—	Logged in	Avaya Link Group 1	2022-09-20

General link settings

Link alias: AvayaAes1

Link name: AVAYALNK01

CTI server name: CTI server 1

Link enabled: ☒

Auto-discovery enabled: ☐

Link parameters: SwitchName=cm101x
TSAPIServerName=AVAYA#CM101X#CSTA#AESPRI101X
ConnectionProtocol=7.0.0
UseSRTP=No
KeyOnLabel=RecorderOn
KeyOffLabel=RecorderOff

Connection settings

Connection host: 10.10.40.16

IP port: 4721

Connection user: nice1

Connection password:

Password (retype):

SSL enabled: ☐

Link group: Avaya Link Group 1

Pressing the edit button above will allow changes to be made to the following. The **Connection host**, **IP port**, the **Connection user** and **password** should not need any editing as these will be added as part of the original installation. In the event that there is a bad connection, these fields can be re-entered as shown below.

Note: In the example below a user called **nice1** was created for AES1 and nice2 created for AES2. The same username could be used on both AES's if preferred.

Note: If there was one AES and two NICE recorders these two recorders could use the same User ID and Password again only requiring one user to be setup on the AES for both recorders

General link settings

Link alias: AvayaAes1

Link name: AVAYALNK01

CTI server name: CTI server 1

Link enabled: ☒

Auto-discovery enabled: ☐

Link parameters: SwitchName=cm101x
TSAPIServerName=AVAYA#CM101X#CSTA#AESPRI101X
ConnectionProtocol=7.0.0
UseSRTP=No
KeyOnLabel=RecorderOn
KeyOffLabel=RecorderOff

Connection settings

Connection host: 10.10.40.16

IP port: 4721

Connection user: nice1

Connection password:

Password (retype):

SSL enabled: ☐

Link group: Avaya Link Group 1

The following MR specific parameters can also be added should they be required, **RecordTargetExtensionOnly** and **ReRegistrationDelayMR**. This was not tested during compliance testing.

RecordTargetExtensionOnly=	Only available for the Multiple Registrations recording method. Default: No. If set to No (default), all (supported) calls to and from the target are recorded. Enter Yes to record only calls to and from the target's main extension, and not those to and from other bridged extensions.
ReRegistrationDelayMR=	For the Multiple Registrations recording method only. Sets the delay (in milliseconds) from failure of the registration of a recording device to re- registration. The step 'unregister' is skipped. Min. delay 1000 ms, no max. Default: 10000.

A link group must be added, and this is done by first clicking on the **LINK GROUPS** tab as shown below. Then click on the + icon (not shown), this will open a new window where the link information can be entered and saved by clicking on **OK**. A suitable **Link group name** is given, the **CTI server** that was added during the installation is chosen. The **Channel assignment** was **Ascending** for compliance testing, the others were left as default as shown below.

The screenshot displays the Avaya system configuration interface. The top navigation bar includes tabs: MY ACCOUNT, SYSTEM INSTALLATION, CTI INTEGRATION (selected), SYSTEM CONFIGURATION, USER ADMINISTRATION, SYSTEM STATUS, and RECORDED CALLS. Below this, a sub-navigation bar shows: CTI SERVERS, LINKS, LINK GROUPS (highlighted with a red box), TARGETS, SELECTION OVERVIEW, LINKED CHANNELS, RECORDING RULES, and CONFERENCE RESOURCES. The main content area is titled 'Link groups overview' and contains a dropdown menu for 'Link group' (currently showing 'Avaya 1') and a list of 'Available links'. An 'Edit link group' dialog box is open, showing the following fields: 'Link group name' (Avaya Link Group 1), 'CTI server' (CTI server 1), 'Channel group' (AvayaChannels), 'Channel assignment' (Ascending (default)), 'Failback type' (Manual), 'Load balance type' (No Load Balance), 'Failback start time', and 'Failback end time'. The dialog box has 'Cancel' and 'OK' buttons at the bottom right.

The link that was created during installation is now added to the newly created link group.

MY ACCOUNTSYSTEM INSTALLATIONCTI INTEGRATIONSYSTEM CONFIGURATIONUSER ADMINISTRATIONSYSTEM STATUSRECORDED CALLS

CTI SERVERSLINKSLINK GROUPSTARGETSSELECTION OVERVIEWLINKED CHANNELSRECORDING RULESCONFERENCE RESOURCESTARGET GROUPS

Link groups overview

Select a link group from the dropdown box and move the links from 'Available Links' to the selected group.

Link groupAvaya Link Group 1 (CTI server 1)

Available links

Links in selected group

AVAYALNK01 (CTI server 1)

Role overview for group

AVAYALNK01PrimaryActiveTargets managed: 4

Link role properties

Link aliasAvayaAes1

Link nameAVAYALNK01

CTI server nameCTI server 1

Link groupAvaya Link Group 1

Channel groupAvayaChannels

Link enabledYes

Targets can be added by clicking on the **TARGETS** tab and clicking on the + icon below. Targets are Avaya phones that need to be monitored. The screen below shows an existing list of phones that are already being monitored. A new Target is added for the Avaya Digital phone.

MY ACCOUNTSYSTEM INSTALLATIONCTI INTEGRATIONSYSTEM CONFIGURATIONUSER ADMINISTRATIONSYSTEM STATUSRECORDED CALLS

CTI SERVERSLINKSLINK GROUPSTARGETSSELECTION OVERVIEWLINKED CHANNELSRECORDING RULESCONFERENCE RESOURCESTARGET GROUPS

Overview of all link targets

Target name	Target selection	Link group	Target type	Target value	Date last modified	
H323 J179	✓	Avaya Link Group 1	Extension MR	3001	2022-09-20	
SIP J189	✓	Avaya Link Group 1	Extension MR SIP	3101	2022-09-20	
AAID	✓	Avaya Link Grou...	Extension MR SIP	3111	2022-09-20	

Enter a suitable **Target name**, the **Link group** should already be populated by the link already configured. **Target type** must be set to **Extension MR** and the **Target value range start** as well as the **Password** is added as per the Communication Manager station information.

Add target

Target name(s)

Digital

Link group

Avaya Link Group 1 (CTI server 1) ▾

Target type(s)

Extension MR ▾

Target value range start

3050

Target value range end (leave empty for single target)

Password

••••

Target selection

☒

Cancel

OK

8. Verification Steps

This section provides the steps that can be taken to verify correct configuration of NICE Inform Recorder and Application Enablement Services.

8.1. Verify Avaya Aura® Communication Manager CTI Service State

Before checking the connection between NICE Inform Recorder and AES, 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	865	865	
2	12	no	aessec101x	established	413	413	

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**. There were six devices monitored during compliance testing and so **Associations** is showing **6** below.

Status | Status and Control | TSAPI 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

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 Sep 14 18:19:00 2022	Online	20	6	21	23	30

OnlineOffline

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

TSAPI Service StatusTLink StatusUser Status

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

CTI User Status

☐ Enable page refresh every seconds

CTI Users

Open Streams 3

Closed Streams 24

Open Streams

Name	Time Opened	Time Closed	Tlink Name
DMCCLCSUserDoNotModify	Fri 09 Sep 2022 06:27:34 PM IST		AVAYA#CM101X#CSTA#AESPRI101X
DMCCLCSUserDoNotModify	Fri 09 Sep 2022 06:27:34 PM IST		AVAYA#CM101X#CSTA#AESPRI101X
nice1	Wed 14 Sep 2022 06:26:31 PM IST		AVAYA#CM101X#CSTA#AESPRI101X

A similar status is shown for **nice2** on the second AES.

CTI User Status

☐ Enable page refresh every seconds

CTI Users

Open Streams 3

Closed Streams 0

Open Streams

Name	Time Opened	Time Closed	Tlink Name
DMCCLCSUserDoNotModify	Wed 21 Sep 2022 01:51:01 PM IST		AVAYA#CM101X#CSTA#AESSEC101X
DMCCLCSUserDoNotModify	Wed 21 Sep 2022 01:51:01 PM IST		AVAYA#CM101X#CSTA#AESSEC101X
DMCCLCSUserDoNotModify	Wed 21 Sep 2022 01:51:03 PM IST		AVAYA#CM101X#CSTA-S#AESSEC101X
nice2	Wed 21 Sep 2022 01:51:01 PM IST		AVAYA#CM101X#CSTA#AESSEC101X

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 **10.10.40.128**, which is the first NICE server. Both screens below show that five devices were being monitored using DMCC Multiple Registration.

Status | Status and Control | DMCC 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

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Tue Sep 20 16:03:23 IST 2022

Service Uptime: 10 days, 21 hours 35 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 13

Number of Existing Devices: 3

Number of Devices Created Since Service Boot: 67

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	C679467E72BA1608F 1120F3831087D4F-37	nice1	Avaya_Link	10.10.40.128	XML Unencrypted	5

Terminate Sessions

Show Terminated Sessions

Item 1-1 of 1

Go

The screen below shows that the user **nice2** is connected from the IP address **10.10.40.129**, which is the second NICE server.

Status | Status and Control | DMCC 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

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Tue Sep 20 17:25:45 IST 2022

Service Uptime: 13 days, 1 hours 2 minutes

Number of Active Sessions: 3

Number of Sessions Created Since Service Boot: 17

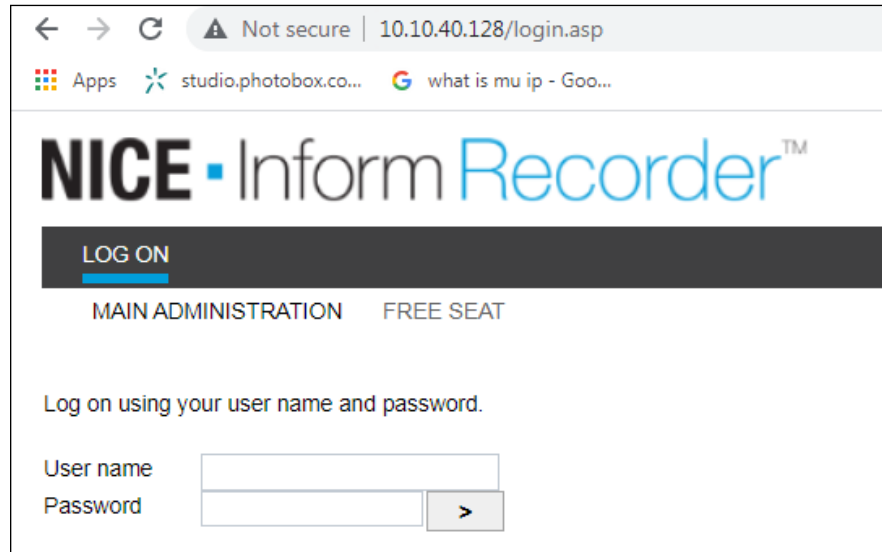
Number of Existing Devices: 5

Number of Devices Created Since Service Boot: 77

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	00FCD32F2D545112A B9E417344EE53E8-33	nice2	Avaya_Link	10.10.40.129	XML Unencrypted	5
<input type="checkbox"/>	CAA2B00D7643D5A2D AF9E59884DEC767-31	wspaces	Khepri Call Server Connector	10.10.40.53	XML Encrypted	0
<input type="checkbox"/>	DC6AF71C76781D650 60B8C7ED3AE6E87-30	wspaces	Khepri Call Server Connector	10.10.40.52	XML Encrypted	0

8.4. Verify connection from NICE server

Open a web browser (must be Internet Explorer to allow IE to load the “Audio Player” applet into the recorder web browser. Edge does not support Silverlight applications unless it is run in “IE mode”) to the NICE server, **http://<NICE IP>**. Log in with the appropriate credentials.



← → ↻ ⚠ Not secure | 10.10.40.128/login.asp

Apps studio.photobox.co... what is mu ip - Goo...

NICE · Inform Recorder™

LOG ON

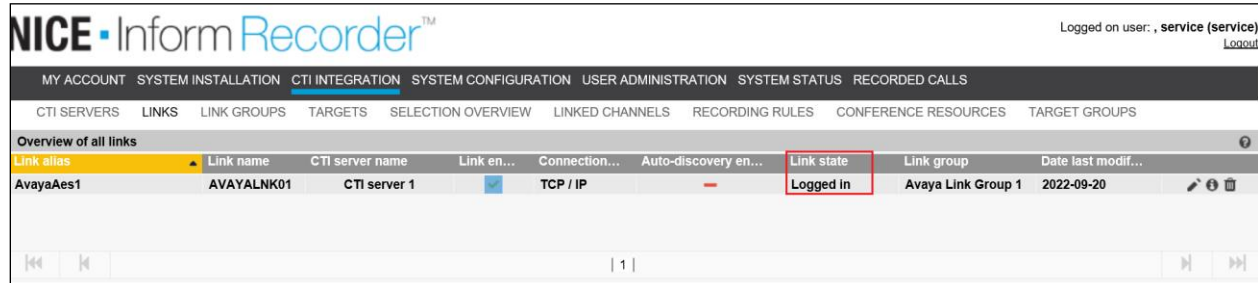
MAIN ADMINISTRATION FREE SEAT

Log on using your user name and password.

User name

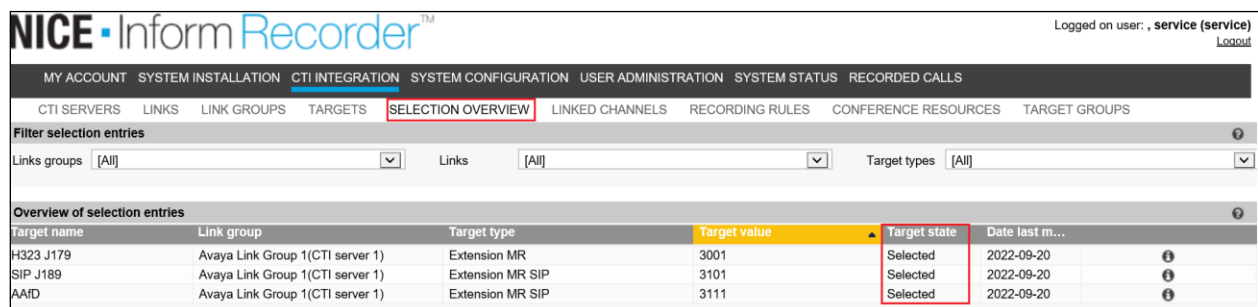
Password >

Click on CTI Integration, the **Link state** should show **Logged in**, as shown below.



Link alias	Link name	CTI server name	Link en...	Connection...	Auto-discovery en...	Link state	Link group	Date last modif...
AvayaAes1	AVAYALNK01	CTI server 1	<input checked="" type="checkbox"/>	TCP / IP	-	Logged in	Avaya Link Group 1	2022-09-20

Click on **Selection Overview**, the **Target state** should show as **Selected**.



Target name	Link group	Target type	Target value	Target state	Date last m...
H323 J179	Avaya Link Group 1(CTI server 1)	Extension MR	3001	Selected	2022-09-20
SIP J189	Avaya Link Group 1(CTI server 1)	Extension MR SIP	3101	Selected	2022-09-20
AAFD	Avaya Link Group 1(CTI server 1)	Extension MR SIP	3111	Selected	2022-09-20

8.5. 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 the NICE Inform Recorder server.

Note: The primary method for performing search and replay is the NICE Inform suite of applications.

From the home page, click on **recorded calls** at the top of the screen.

NICE Inform Recorder™

MY ACCOUNT SYSTEM INSTALLATION CTI INTEGRATION SYSTEM CONFIGURATION USER ADMINISTRATION SYSTEM STATUS **RECORDED CALLS**

MY SETTINGS

Details for user account service (2)

User name: service
Old password:
New password:
New password confirmation:
First name: service
Last name:
Email addresses:

Properties for user account service (2)

User authentication method: System authentication
Seating: No seat
Fixed seating channel:
Free seating extension:
Group: Administrators
User language: Dict. 0: [ENG] English

Calls preferences for user account service (2)

Default search query: "Default query: Calls made last week"
Default calls listing view: "Avaya view"
Auto start playback: ☒

Enter an appropriate **Date span** and click on **Submit query**.

NICE Inform Recorder™

Logged on user: , service (service) Logout

MY ACCOUNT SYSTEM INSTALLATION CTI INTEGRATION SYSTEM CONFIGURATION USER ADMINISTRATION SYSTEM STATUS **RECORDED CALLS**

CALLS SEARCH

Search form:
Date span:
Selection:

Stored search queries

Query name	Shared	Created	Owner
Default query: Calls made last week	✓	2009-01-23	
Example: All 555-1234 calls in Q1 2005	✓	2009-01-23	
Example: All long incoming calls to Mike Johnson	✓	2009-01-23	
Example: Incoming calls on channels 1-10	✓	2009-01-23	
Example: Outgoing calls with mark 0 in the last month	✓	2009-01-23	

Reset form Store query Submit query

Click on whatever recording is required for play back and this will play back the recording using the sound device on that PC to play back the call.

NICE · Inform Recorder™ Logged on user: , service (service) [Logout](#)

MY ACCOUNT SYSTEM INSTALLATION CTI INTEGRATION SYSTEM CONFIGURATION USER ADMINISTRATION SYSTEM STATUS **RECORDED CALLS**

CALLS SEARCH COLUMN SELECTION CALLS LISTING CALL STATISTICS

Search results 15 25 50

Ca...	U...	Ch...	Start date	Duration	Phon...	Direction	CTI Calling Party	CTI Called Party	CTI Call ID	AgentID
783		3	2021-06-03 16:01:52	00:00:06	1050	➡	35391847001	35391731050	00037030851622732511	
784		3	2021-06-03 16:02:25	00:00:20	1050	➡	35391847001	35391731050	00037030861622732544	
785		2	2021-06-03 16:03:42	00:00:40	1101	➡	35391847001	35391731101	00037030881622732621	
786		2	2021-06-03 16:04:26	00:00:33	1101	➡	35391847001	35391731101	00037030911622732665	

< 1 >

The call is played back as shown below.

NICE · Inform Recorder™ Logged on user: , service (service) [Logout](#)

MY ACCOUNT SYSTEM INSTALLATION CTI INTEGRATION SYSTEM CONFIGURATION USER ADMINISTRATION SYSTEM STATUS **RECORDED CALLS**

CALLS SEARCH COLUMN SELECTION CALLS LISTING CALL STATISTICS

Search results 15 25 50

C...	U...	Channel	Start date	Duration	Phone number	Direction	CTI Calling Party	CTI Called Party	CTI Call ID	AgentID
1379		1	2022-09-15 16:10:27	00:00:04	3001	➡	35391847002	3901	00101002421663251017	
1378		2	2022-09-15 16:07:50	00:00:07	3101	➡	3101		00101002381663250856	
1377		2	2022-09-15 16:07:42	00:00:08	3101	➡	3101	1601	00101002381663250856	
1376		2	2022-09-15 11:39:09	00:00:06	3101	➡	3101	3115	00101002381663234747	
1375		2	2022-09-15 11:38:59	00:00:05	3101	➡	3060	3101	00101002341663234738	

< 1 2 3 4 5 6 7 8 9 10 ... 12 >

Audio player

00:00:00.000

16:32:26 The call is available for playback (return code 3: Fingerprint matches, file is authentic).

Call details

▼ Main properties

Call ID	1379	Start date	2022-09-15 16:10:27
End date	2022-09-15 16:10:31	Duration	00:00:04
Direction	Incoming	Channel	1
User handle		Status	Available
Mark	Normal calls		
CLI Data			
CTI Call ID	00101002421663251017	CTI Calling Party	35391847002

9. Conclusion

These Application Notes describe the configuration steps required for solution redundancy of NICE Inform Recorder R9.2 to interoperate with the Avaya solution consisting of an Avaya Aura® Communication Manager R10.1 and two Avaya Aura® Application Enablement Services R10.1 in a 2N Redundancy configuration using DMCC Multiple Registration to record calls. All feature functionality and serviceability test cases were completed successfully with some issues and observations noted in **Section 2.2**.

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 on ExtraNICE at:

<https://www.extranice.com/Security/Pages/default.aspx>
(ExtraNICE user account and password required)

©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.

NICE Systems
Tollbar Way
Hedge End
Southampton
Hampshire SO30 2ZP
United Kingdom

T+44 (0)1489 771 200 F+44 (0)1489 771 533
E info@nice.com



14th October 2022

To whom it may concern

NICE NIR and NTR recording platforms interoperability with Avaya Aura 10.1

NICE confirms that the NICE Inform Recorder (NIR) and NICE Trading Recorder (NTR) share a common software base. Both recording platforms offer a NICE-Avaya Aura DMCC integration which share common components, primarily the “Link Controller” to interface and interoperate with the Avaya Aura system.

The table below shows the version (feature) equivalence of the NIR and NTR integrations.

Recording Platform	Platform Version	Avaya Aura Integration	Applicability
NICE Inform Recorder (NIR)	9.2	80.3	NICE Public Safety Line of Business
NICE Trading Recorder (NTR)	6.7	10.5	Financial Markets Compliance Line of Business

The table below shows NIR and NTR feature differences with respect to the Avaya Aura integration

Recording Platform	Platform Version	Feature differences
NICE Inform Recorder (NIR)	9.2	Replay of recorded calls: NICE Inform suite of applications
NICE Trading Recorder (NTR)	6.7	Replay of recorded calls: NICE Compass suite of applications Avaya Integration: Support for Recording Announcement

Given the above information, we view the latest DevConnect Compliance Testing of NIR 9.2 with Avaya Aura DMCC integration 80.3 to also cover the NTR equivalent above.

A more detailed description of the integration between Avaya DMCC, NICE Inform Recorder, and NICE Trading Recorder can be found in the **NICE Avaya DMCC Integration 80.3 Release Note** here: [ExtraNICE \(Public Safety\) Avaya DMCC](#) and [ExtraNICE \(Enterprise\) Connectivity Guides > Avaya](#) .

Jurgen Wessel

J Wessel

Principal Product Owner - NICE Communications Compliance