



Avaya Solution & Interoperability Test Lab

Application Notes for NICE Inform Recorder 9.2 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 R8.1 and Avaya Aura® Application Enablement Services R8.1 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 R8.1 and two Avaya Aura® Application Enablement Services R8.1 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 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.

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 Multi-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. The following issue was noted. When a call is Parked and Unparked, the first leg is recorded, the second leg (unparked call) is recorded but there is no RTP present when a SIP phone is unparking the call. Avaya is investigating the issue.

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 Multi-Registration to record calls. The NICE server is setup for DMCC Multi-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.

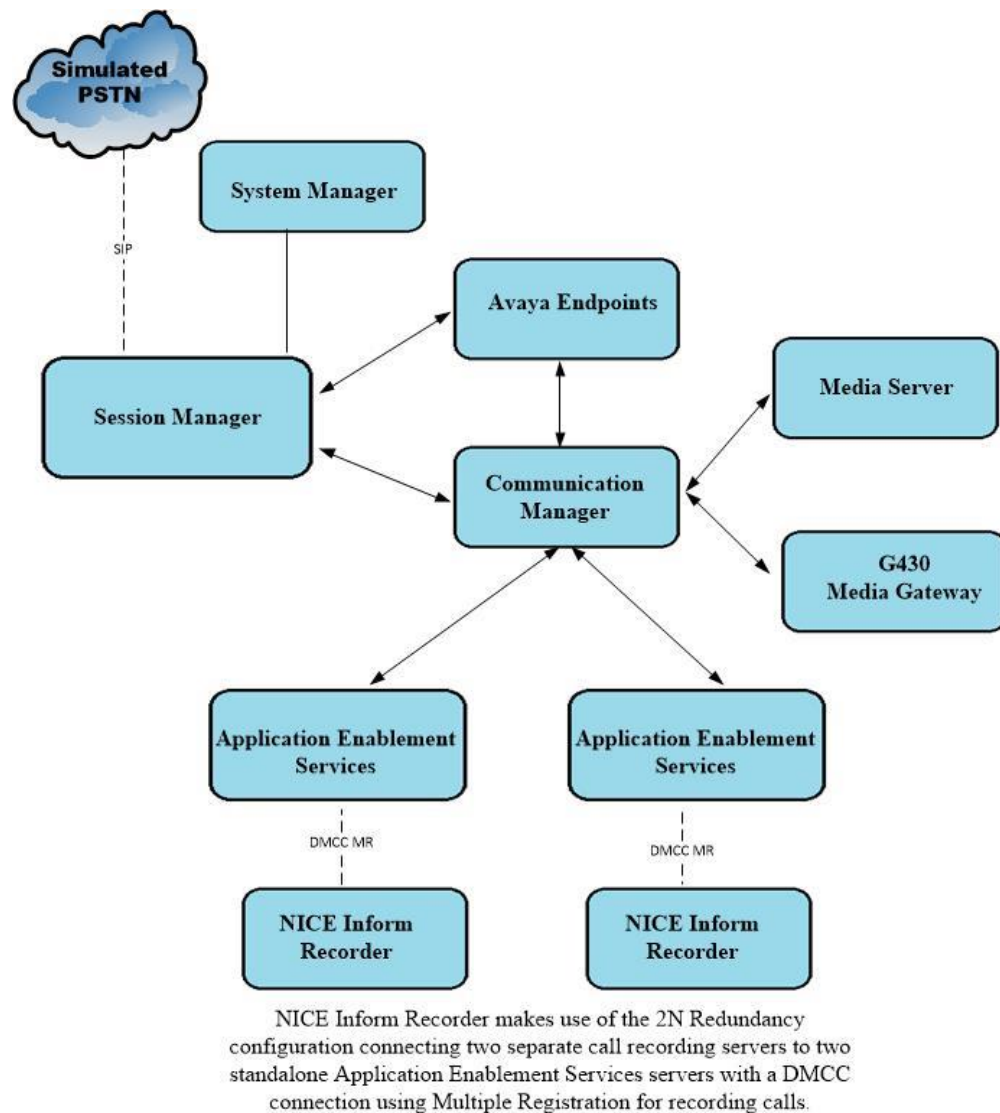


Figure 1: Connection of solution redundancy of NICE Inform Recorder with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Application Enablement Services R8.1 in a 2N redundancy configuration

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 running on a virtual server	8.1.3.1 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.3.1.1012493 Service Pack 1
Avaya Aura® Session Manager running on a virtual server	8.1.3.1 Build No. – 8.1.3.1.813113
Avaya Aura® Communication Manager running on a virtual server	8.1.3.1 – FP3SP1 R018x.01.0.890.0 Update ID 01.0.890.0-26766
Avaya Aura® Application Enablement Services Primary Server running on VMware	8.1.3.1 Build 8.1.3.1.0.7-0
Avaya Aura® Application Enablement Services Secondary Server running on VMware	8.1.3.1 Build 8.1.3.1.0.7-0
Avaya Session Border Controller for Enterprise	8.1.1.0-26-19214
Avaya Aura® Media Server	8.0.2.184
Avaya G430 Media Gateway	41.16.0/1
Avaya J179 H.323 Deskphone	6.8304
Avaya J159 SIP Deskphone	4.0.7.1.5
Avaya 9408 Digital Phone	2.00
Avaya Agent for Desktop	2.0.6.8.3002
NICE Inform Recorder (NIR) “All-in-one” configuration, running on Windows Server 2019	NIR 9.2.1 Avaya DMCC Integration 80.3.1

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 3**, ensure that **Computer Telephony Adjunct Links?** is set to **y** as shown below.

display system-parameters customer-options		Page	3 of 11
OPTIONAL FEATURES			
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? y		
Access Security Gateway (ASG)? n	Authorization Codes? y		
Analog Trunk Incoming Call ID? y	CAS Branch? n		
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n		
Answer Supervision by Call Classifier? y	Change COR by FAC? n		
ARS? y	Computer Telephony Adjunct Links? y		
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y		
ARS/AAR Dialing without FAC? y	DCS (Basic)? y		
ASAI Link Core Capabilities? n	DCS Call Coverage? y		
ASAI Link Plus Capabilities? n	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	10.10.40.52		
default	0.0.0.0		
g450	10.10.40.15		
procr	10.10.40.37		

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	4
IP SERVICES							
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote 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 **aesredundnacy1**.
- **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 4**, one for **aesredundancy1** and another for **aesredundancy2**.

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 4 of 4
AE Services Administration				
Server ID	AE Services Server	Password	Enabled	Status
1:	aesredundnacy1	*****	y	idle
2:	aesredundancy2	*****	y	idle
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: 4497		
Type: ADJ-IP		
		COR: 1
Name: aesredundancy1		

5.5. Configure H.323 Stations for Multi-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 Multi-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” is set to “Avaya” and “Softphone” set to “Yes”. 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.

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.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

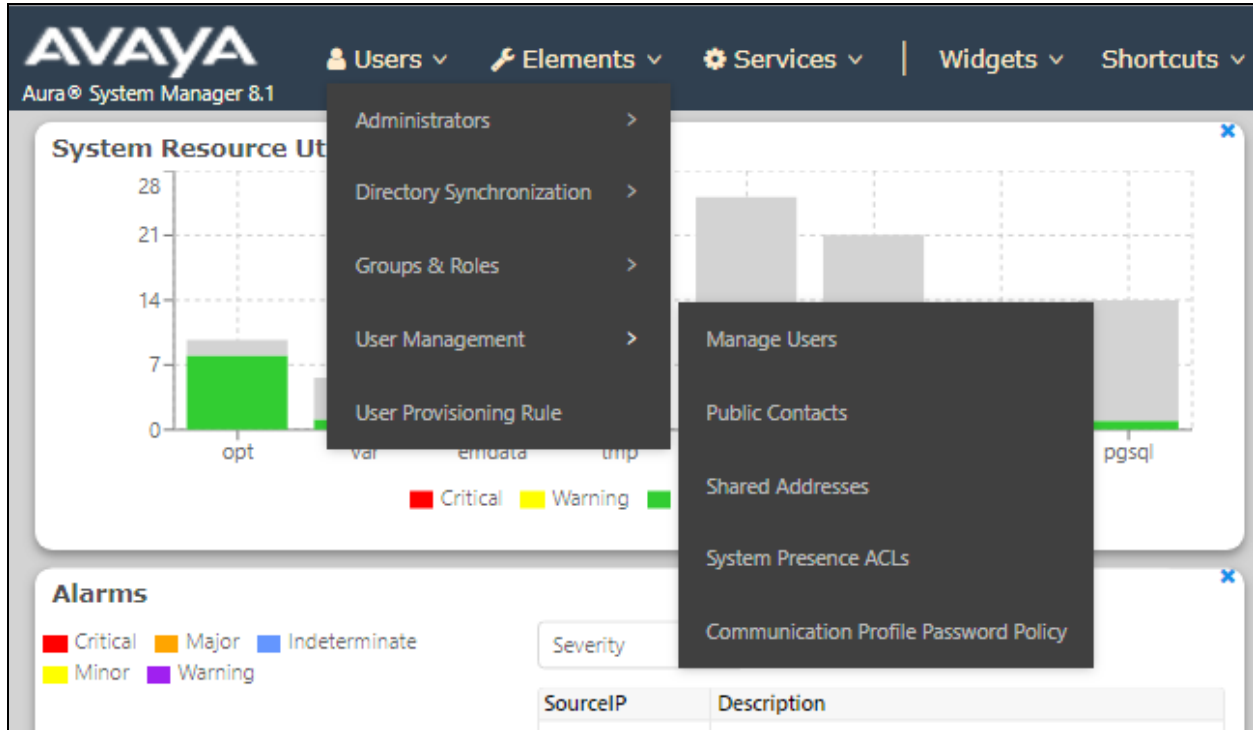
User ID:

Password:

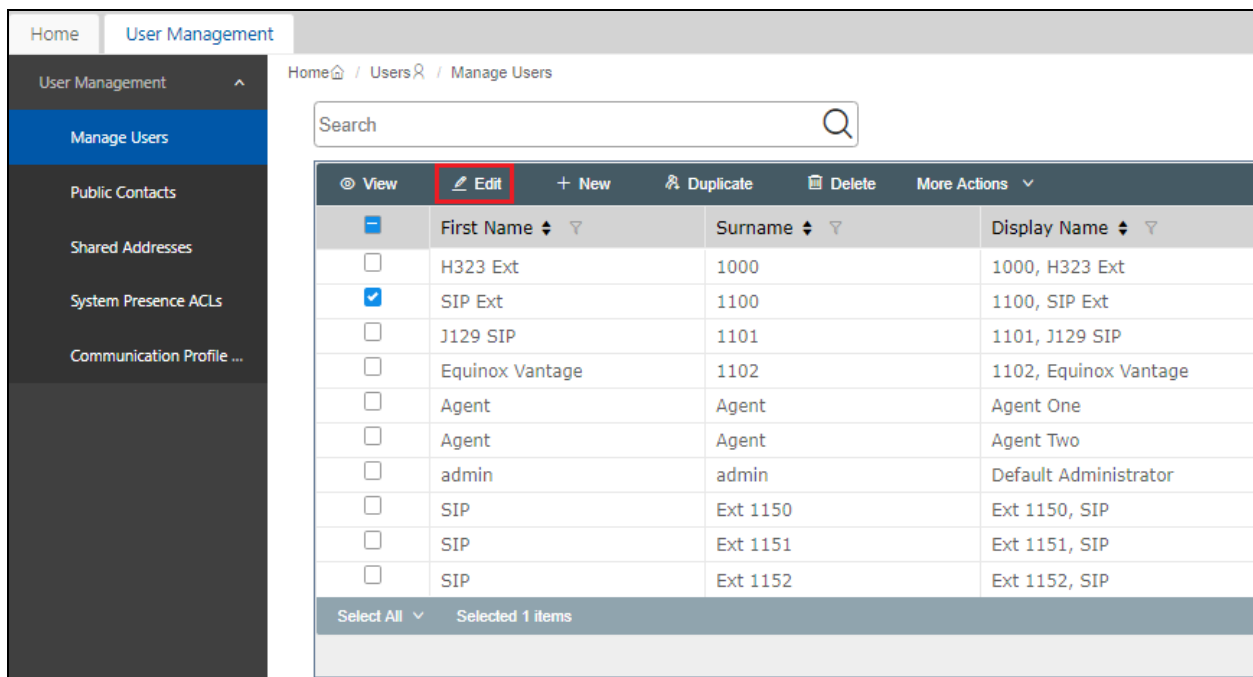
[Change Password](#)

Supported Browsers: Internet Explorer 11.x or Firefox 65.0, 66.0 and 67.0.

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.

User Profile | Edit | 1100@devconnect.local

Identity | **Communication Profile** | Membership | Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile ☒

Avaya BreezeS Profile ☐

CM Endpoint Profile ☒

* System : cm\$1xvmpg

* Profile Type : Endpoint

Use Existing Endpoints : ☐

* Extension : 1100

Template : Start typing...

* Set Type : 9641SIPCC

Security Code : Enter Security Code

Port : S000002

Voice Mail Number : 6666

Preferred Handle : Select

Calculate Route Pattern : ☐

Sip Trunk : aar

SIP URI : Select

Enhanced Callr-Info Display for 1-line phones : ☐

Delete on Unassign from User or on Delete User : ☒

Override Endpoint Name and Localized Name : ☒

Allow H.323 and SIP Endpoint Dual Registration : ☐

Commit & Continue | **Commit** | Cancel

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

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 : 1100

* Tenant Number : 1

* SIP Trunk : aar

Coverage Path 1

Lock Message : ☐

Multibyte Language : Not Applicable

* Class Of Service (COS) : 1

* Message Lamp Ext. : 1100

Type of 3PCC Enabled : **Avaya**

Coverage Path 2

Localized Display Name : 1100, SIP Ext

Enable Reachability for Station Domain Control : system

SIP URI

Primary Session Manager

IPv4 : 10.10.40.32 | IPv6 :

Secondary Session Manager

Click on the **Feature Options** tab and ensure that **IP Softphone** is ticked as shown. Click on **Done**, at the bottom of the screen, once this is set.

The screenshot shows the 'Feature Options' tab selected. The 'IP SoftPhone' checkbox is checked and highlighted with a red box. Other settings include 'Active Station Ringing' set to 'single', 'MWI Served User Type' set to 'sip-adjunct', 'Per Station CPN - Send Calling Number' set to 'None', 'IP Phone Group ID' set to an empty field, 'Remote Soft Phone Emergency Calls' set to 'as-on-local', 'LWC Reception' set to 'spe', 'AUDIX Name' set to an empty field, 'Short/Prefixed Registration Allowed' set to 'default', 'Voice Mail Number' set to an empty field, 'Auto Answer' set to 'none', 'Coverage After Forwarding' set to 'system', 'Display Language' set to 'english', 'Hunt-to Station' set to an empty field, 'Loss Group' set to '19', 'Survivable COR' set to 'internal', 'Time of Day Lock Table' set to 'None', and 'Music Source' set to an empty field. The 'Features' section includes checkboxes for 'Always Use', 'IP Audio Hairpinning', 'Bridged Call Alerting', 'Bridged Idle Line Preference', 'Coverage Message Retrieval' (checked), 'Data Restriction', 'Survivable Trunk Dest' (checked), 'Bridged Appearance Origination Restriction', 'Restrict Last Appearance' (checked), 'Idle Appearance Preference', 'IP SoftPhone' (checked and highlighted), 'LWC Activation' (checked), 'CDR Privacy', 'Direct IP-IP Audio Connections' (checked), 'H.320 Conversion', 'IP Video Softphone', and 'Per Button Ring Control'.

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

The screenshot shows the 'User Profile | Edit | 1100@devconnect.local' interface. The 'Commit' button is highlighted with a red box. The 'CM Endpoint Profile' is selected under 'PROFILES'. The 'System' is set to 'cm\$1xvmpg', 'Profile Type' is 'Endpoint', 'Extension' is '1100', 'Set Type' is '9641SPCC', 'Port' is 'S000002', 'Voice Mail Number' is '6666', and 'SIP URI' is 'Select'. Other settings include 'Use Existing Endpoints' (unchecked), 'Template' (Start typing...), 'Security Code' (Enter Security Code), 'Calculate Route Pattern' (unchecked), 'SIP URI' (Select), 'Enhanced Callr-Info Display for 1-line phones' (unchecked), 'Delete on Unassign from User or on Delete User' (checked), 'Allow H.323 and SIP Endpoint Dual Registration' (unchecked), and 'Override Endpoint Name and Localized Name' (checked).

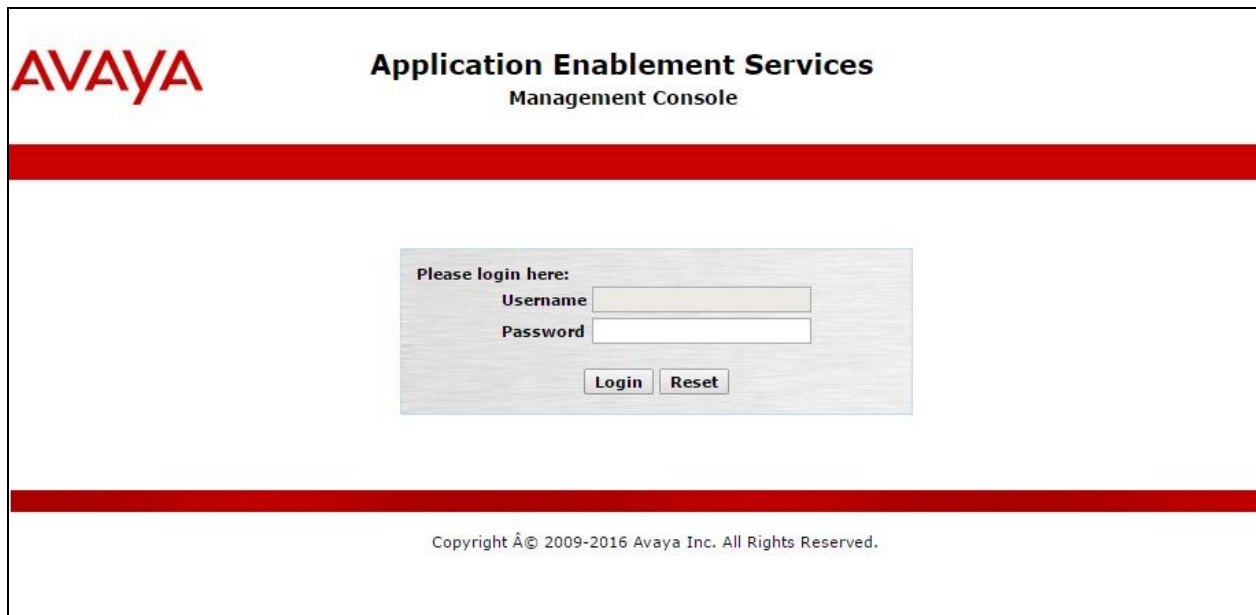
6. Configure Avaya Aura® Application Enablement Services

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
- Enable Control for DMCC
- Create CTI User
- Associate Devices with CTI User

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 page. 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 thick red horizontal bar spans the width of the page below the header. In the center of the page is a light gray rectangular box containing the login form. The form has the text "Please login here:" followed by two input fields: "Username" and "Password". Below these fields are two buttons: "Login" and "Reset". Another thick red horizontal bar is located below the login form. At the bottom of the page, centered, is the copyright notice: "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

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 selected. 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 with the following data:

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, it says: 'For status on actual services, please use [Status and Control](#)'. A footnote states: '* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.' At the bottom, 'License Information' states: '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' selected. The main content area is titled 'Licensing' and contains instructions: 'If you are setting up and maintaining the WebLM, you need to use the following:' followed by a bullet point 'WebLM Server Address'. Then, 'If you are importing, setting up and maintaining the license, you need to use the following:' followed by a bullet point 'WebLM Server Access'. Finally, 'If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:' followed by a bullet point 'Reserved Licenses'. 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**.

AVAYA

Application Enablement Services
Management Console

Welcome: User cust

Last login: Thu May 13 15:41:17 2021 from 192.168.40.240

Number of prior failed login attempts: 0

HostName/IP: aes81xvmppg/10.10.40.38

Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE

SW Version: 8.1.3.1.0.7-0

Server Date and Time: Thu Jun 10 10:04:56 IST 2021

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

Security

Switch Connections

Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input type="radio"/> cm81large	Yes	30	0
<input checked="" type="radio"/> cm81xvmppg	Yes	30	1

Edit Connection

Edit PE/CLAN IPs

Edit H.323 Gatekeeper

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 5.3**. A secure connection was established between the AES and Communication Manager, so the appropriate boxes were ticked, as shown below. Click **Apply** to save changes.

Communication Manager Interface | Switch Connections

Connection Details - cm81xvmpg

Switch Password: [password field]

Confirm Switch Password: [password field]

Msg Period: 30 Minutes (1 - 72)

Provide AE Services certificate to switch: ☒

Secure H323 Connection: ☒

Processor Ethernet: ☒

Enable TLS Certificate Hostname 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 - cm81xvmpg

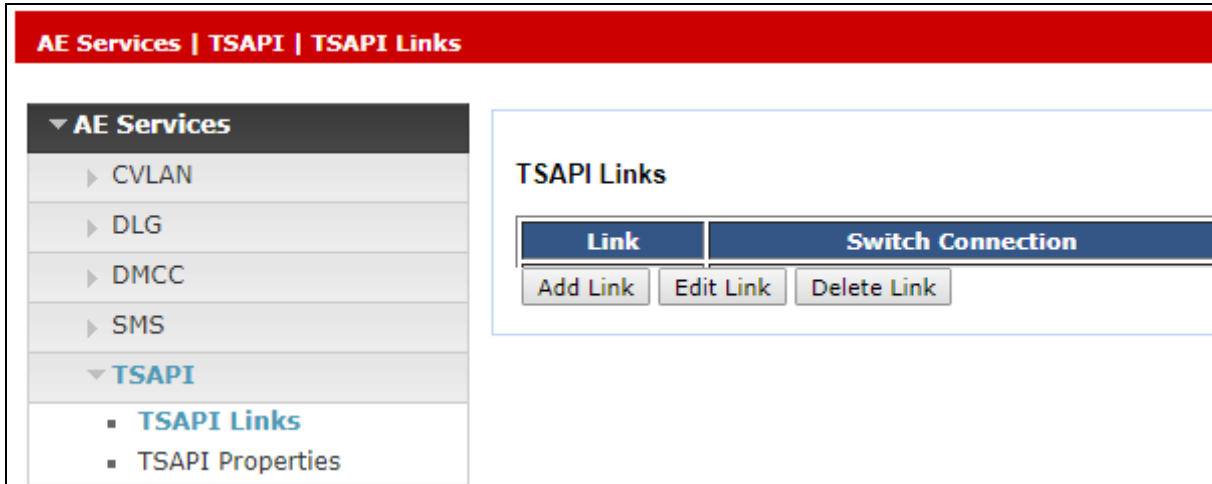
10.10.40.37 Add/Edit Name or IP

Name or IP Address	Status
10.10.40.37	In Use

Back

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.



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 **cm81xvmpg**, 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:** **11** 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' configuration form. It contains the following fields and values:

Field	Value
Link	1
Switch Connection	cm81xvmpg
Switch CTI Link Number	1
ASAI Link Version	11
Security	Both

At the bottom of the form 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	cm81xvmpg	1	8	Both
<input type="button" value="Add Link"/> <input type="button" value="Edit Link"/> <input type="button" value="Delete Link"/>				

The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, navigate to **Maintenance** → **Service Controller**. On the Service Controller screen, tick the **TSAPI Service** and select **Restart Service**.



Application Enablement Services
Management Console

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

▶ User Management

▶ Utilities

▶ Help

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 checked="" type="checkbox"/> TSAPI Service	Running

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

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**.

The screenshot shows a web interface for the Avaya Security Database. The breadcrumb navigation at the top reads "Security | Security Database | Tlinks". On the left is a sidebar menu with categories: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, and Security. The Security category is expanded, showing sub-items like Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, and Security Database. The Security Database is further expanded to show Control, CTI Users, Devices, Device Groups, Tlinks (highlighted in blue), Tlink Groups, and Worktops. The main content area on the right is titled "Tlinks" and contains a "Tlink Name" section with two radio button options: "AVAYA#CM81XVMGP#CSTA#AES81XVMGP" and "AVAYA#CM81XVMGP#CSTA-S#AES81XVMGP". Below these options is a "Delete Tlink" button.

Security | Security Database | Tlinks

Tlinks

Tlink Name

☐ AVAYA#CM81XVMGP#CSTA#AES81XVMGP

☐ AVAYA#CM81XVMGP#CSTA-S#AES81XVMGP

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**.

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	
	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 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).

The screenshot shows the 'Add User' screen in the Avaya Application Enablement Services Management Console. The interface includes a sidebar with navigation options and a main form area.

AVAYA **Application Enablement Services Management Console**

User Management | User Admin | Add User

Add User

Fields marked with * can not be empty.

* User Id	NICE1
* Common Name	NICE1
* Surname	NICE1
* User Password	*****
* Confirm Password	*****
Admin Note	
Avaya Role	None ▼
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes ▼
Department Number	
Display Name	
Employee Number	
Employee Type	

Navigation Sidebar:

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▼ **User Management**
 - ▶ Service Admin
 - ▼ **User Admin**
 - **Add User**
 - Change User Password
 - List All Users
 - Modify Default Users
 - Search Users
- ▶ Utilities
- ▶ Help

6.7. 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**.

AVAYA

Application Enablement Services
Management Console

Welcome: User cust
Last login: Wed Aug 29 11:46:12 2018 from 10.10.40.240
Number of prior failed login attempts: 0
HostName/IP: aesredundancy1/10.10.40.125
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.9.10-0
Server Date and Time: Wed Sep 05 09:41:10 UTC 2018
HA Status: Not Configured

Security | Security Database | CTI Users | List All Users

Home | Help | Logout

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

List All Users

Search Users

CTI Users

User ID	Common Name	Worktop Name	Device ID
NICE1	NICE1	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

Common Name

Worktop Name

Unrestricted Access

NICE1

NICE1

NONE ▼

☒

Call and Device Control:

Call Origination/Termination and Device Status

None ▼

Call and Device Monitoring:

Device Monitoring

Calls On A Device Monitoring

Call Monitoring

None ▼

None ▼

☐

Routing Control:

Allow Routing on Listed Devices

None ▼

Apply Changes

Cancel Changes

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.

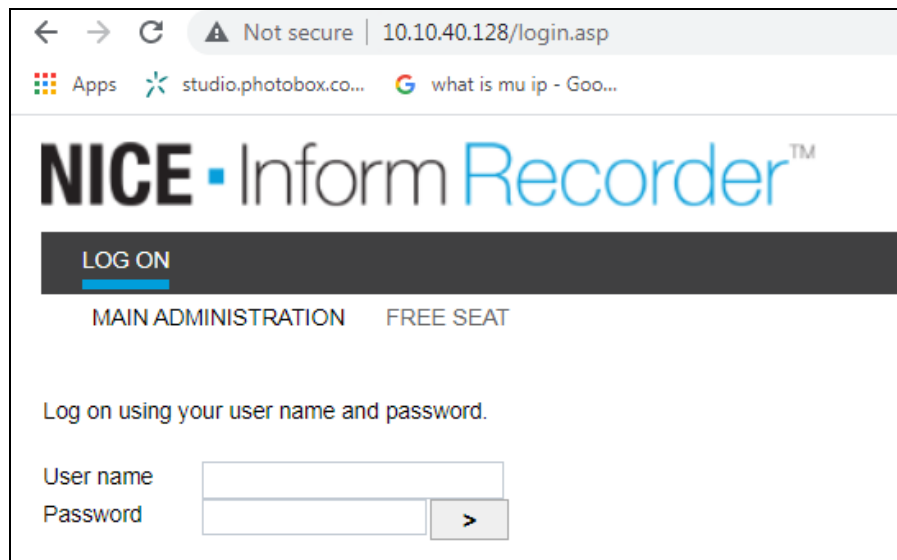
7. Configure NICE Inform Recorder

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: Some IP addresses may show different as some of these screenshots are simply examples of what should be setup.

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/CM 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 "LOG ON" button. Underneath the button are two links: "MAIN ADMINISTRATION" and "FREE SEAT". A message states "Log on using your user name and password." Below this message are two input fields: "User name" and "Password". The "Password" field has a small ">" button 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**, 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 is active, showing three panels for 'user account service (2)':

- 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).

Buttons for 'Cancel' and 'Save changes' are at the bottom right.

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 and a setup form below.

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

Below the table is the 'CTI server setup' form for the selected server:

- 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 icon opposite the link as highlighted.

The screenshot shows the NICE Inform Recorder web interface. The top navigation bar includes tabs like MY ACCOUNT, SYSTEM INSTALLATION, CTI INTEGRATION, SYSTEM CONFIGURATION, USER ADMINISTRATION, SYSTEM STATUS, and RECORDED CALLS. The 'LINKS' tab is selected. Below the navigation bar, there's a table titled 'Overview of all links' with columns: Link alias, Link name, CTI server name, Link enabled, Connection..., Auto-discovery enabled, Link state, Link group, and Date last modified. The first row shows 'AvayaAes1' with link name 'AVAYALNK01', CTI server name 'CTI server 1', and link state 'Logged in'. An edit icon (pencil) is highlighted in the 'Link state' column. Below the table, there are two panels: 'General link settings' and 'Connection settings'. The 'General link settings' panel shows fields for Link alias (AvayaAes1), Link name (AVAYALNK01), CTI server name (CTI server 1), Link enabled (checked), Auto-discovery enabled (unchecked), and Link parameters (a text area with various settings). The 'Connection settings' panel shows fields for Connection host (10.10.40.38), IP port (4721), Connection user (nice1), Connection password (masked with dots), Password (retype) (masked with dots), SSL enabled (unchecked), and Link group (Avaya Link Group 1). At the bottom, a status bar shows the time 12:30:06 and the message 'You are editing an existing record.'

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.

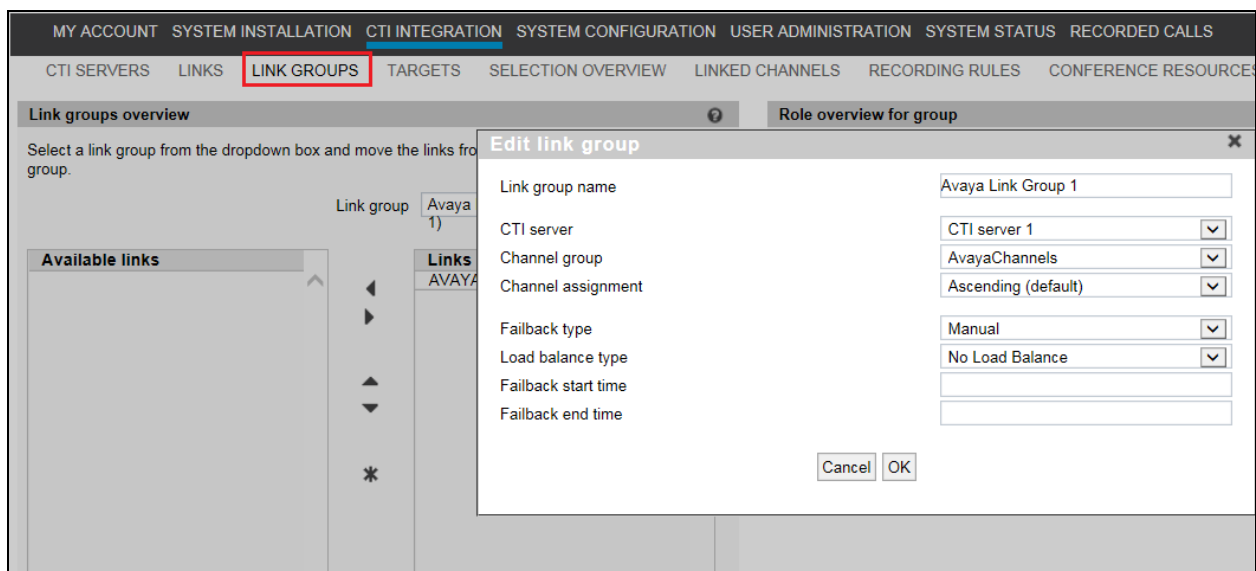
Note: If there was one AES and two NICE recorders these two recorders could use the same User ID and Password again only requiring one user to be setup on the AES for both recorders

This screenshot is a close-up of the 'Connection settings' panel from the previous image. It shows the following fields: Connection host (10.10.40.38), IP port (4721), Connection user (nice1), Connection password (masked with dots), Password (retype) (masked with dots), SSL enabled (unchecked), and Link group (Avaya Link Group 1).

The following MR specific parameters can also be added should they be required, **RecordTargetExtensionOnly** and **ReRegistrationDelayMR**.

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 highlighted, 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 existing link that was created during installation is now added to the newly created link group.

Link groups overview

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

Link group: Avaya Link Group 1 (CTI server 1) + -

Available links

Links in selected group

AVAYALNK01 (CTI server 1)

Role overview for group

Role name	Role type	Status	Targets managed
AVAYALNK01	Primary	Active	4

Link role properties

Link alias	AvayaAes1
Link name	AVAYALNK01
CTI server name	CTI server 1
Link group	Avaya Link Group 1
Channel group	AvayaChannels
Link enabled	Yes

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 and the details of **J179 H323** are shown by clicking on the edit icon, highlighted.

NICE Inform Recorder

Logged on user: , service (service) Logout

TARGETS

Overview of all link targets

Target name	Target selection	Link group	Target type	Target value	Date last modified	
J179 H323	✓	Avaya Link Grou...	Extension MR	1001	2021-06-10	
J189 SIP	✓	Avaya Link Group 1	Extension MR	1101	2021-06-10	
AATD SIP	✓	Avaya Link Group 1	Extension MR	1110	2021-06-10	

Target settings

Target name	J179 H323
Link group	Avaya Link Group 1
Target type	Extension MR
Target value	
Password	
Target selection	<input checked="" type="checkbox"/>

Target settings

ACD Split / Hunt Group
Extension
Extension MR
Extension MR SIP
Extension SO
Extension Trunk

Cancel Save changes

Once the + icon is pressed a new window is opened as shown below. Here the information on the new Avaya extension is entered, this new extension being **9408 Digital**. Note that the **Target Type** can be chosen from the list of options below. For “Multi-Registration” recording **Extension MR** is selected as shown below.

Add target

Target name(s): 9408 Digital

Link group: Avaya Link Group 1 (CTI server 1)

Target type(s): Extension MR

Target value range start: 1050

Target value range end (leave empty for single target):

Password: •••••

Target selection: ☒

Cancel OK

This newly added target is displayed below.

NICE Inform Recorder™ Logged on user: , service (service) Logout

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

CTI SERVERS LINKS LINK GROUPS **TARGETS** SELECTION OVERVIEW LINKED CHANNELS RECORDING RULES CONFERENCE RESOURCES TARGET GROUPS

Overview of all link targets

Target name	Target selection	Link group	Target type	Target value	Date last modified
J179 H323	✓	Avaya Link Grou...	Extension MR	1001	2021-06-10
9408 Digital	✓	Avaya Link Group 1	Extension MR	1050	2021-06-10
J189 SIP	✓	Avaya Link Group 1	Extension MR	1101	2021-06-10
AAFD SIP	✓	Avaya Link Group 1	Extension MR	1110	2021-06-10

Navigation: << < > >> | 1 |

The selection overview tab provides a list of all the monitored devices as well as any VDN's hunt groups or any other monitored endpoints on Communication Manager (not shown).

This concludes the setup of the NICE Application Server for DMCC Multi-Registration recording.

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	11	no	aesredundancy1	established	865	865	
2	11	no	aesredundancy2	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**.

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

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	cm81xvmpg	1	Talking	Sat May 22 18:25:51 2021	Online	18	8	21	22	30
<input type="radio"/>	2	cm81large	1	Switch Down	Wed Apr 14 15:25:43 2021	Online	18	0	0	0	30

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

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.

- 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

CTI User Status

☐ Enable page refresh every 60 seconds

CTI Users: All Users

Open Streams: 5
Closed Streams: 25

Open Streams

Name	Time Opened	Time Closed	Tlink Name
nice1	Thu 03 Jun 2021 04:00:07 PM IST		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
DMCCLCSUserDoNotModify	Wed 14 Apr 2021 03:27:12 PM IST		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
DMCCLCSUserDoNotModify	Wed 14 Apr 2021 03:27:12 PM IST		AVAYA#CM81LARGE#CSTA#AES81XVMPG
DMCCLCSUserDoNotModify	Wed 14 Apr 2021 03:27:13 PM IST		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
DMCCLCSUserDoNotModify	Wed 14 Apr 2021 03:27:13 PM IST		AVAYA#CM81LARGE#CSTA#AES81XVMPG

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 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
 - 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 Thu Jun 10 10:11:08 IST 2021

Service Uptime: 56 days, 18 hours 44 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 15

Number of Existing Devices: 4

Number of Devices Created Since Service Boot: 103

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	C345763F74D6AB6E7B97B17FE990947B-47	nice1	Avaya_Link	10.10.40.128	XML Unencrypted	4

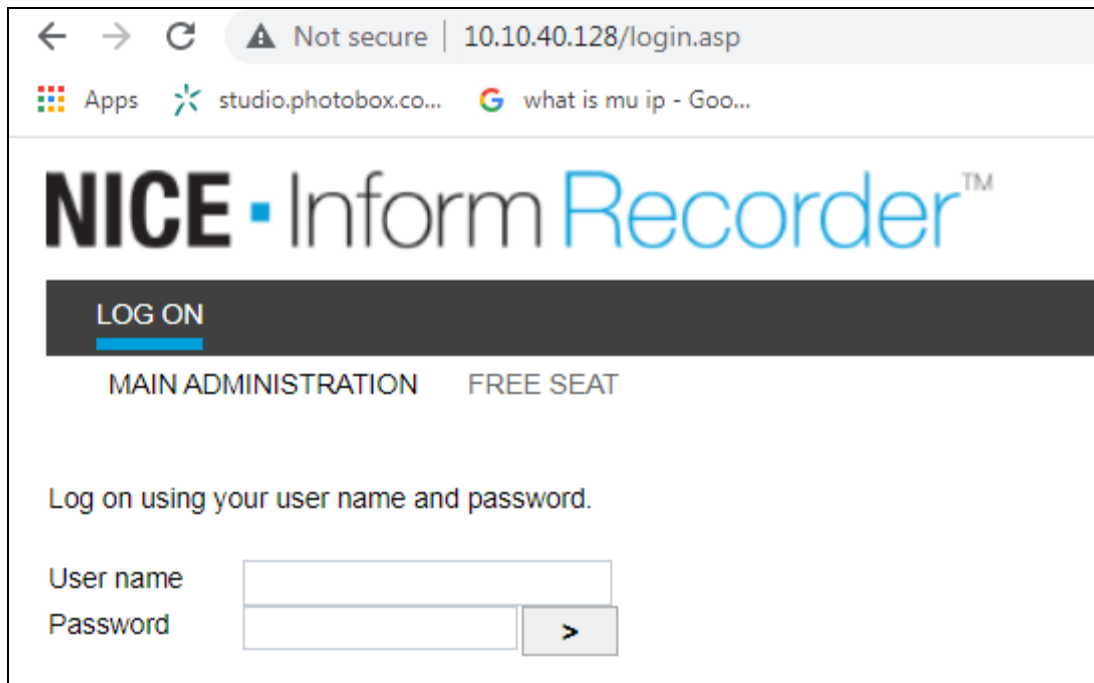
Item 1-1 of 1
1 Go

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 the NICE Inform Recorder server.

Note: Recorded calls can also be replayed using the NICE Inform suite of applications.

Open a browser session to the NICE server as is shown below. Enter the appropriate credentials and log in.



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, the text "MAIN ADMINISTRATION" and "FREE SEAT" is visible. The main content area says "Log on using your user name and password." followed by two input fields: "User name" and "Password". A grey button with a right-pointing arrow is positioned to the right of the password field.

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 COLUMN SELECTION CALLS LISTING CALL STATISTICS

Search form

▼ Date span
Selection: Calls made last WEEK

> Call
> User details
> Duration
> Remarks
> Connectivity
> Number info (CLJ)
> Marks
> Custom database fields
> Online storage

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**

1

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 25

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	

Navigation: < << >> >

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 25

Ca...	U...	Ch...	Start date	Duration	Phon...	Direction	CTI Calling Party	CTI Called Party	CTI Call ID	AgentID	ACDSplit
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		

Navigation: < << >> >

Audio player

00:00 00:10 00:20 00:00:01.645

11:43:42 The call is available for playback (return code 3: Fingerprint matches, file is authentic).

Call details

Main properties

Call ID	784	Start date	2021-06-03 16:02:25
End date	2021-06-03 16:02:45	Duration	00:00:20
Direction	Incoming	Channel	3
User handle		Status	Available
Mark	Normal calls		
CLI Data			
CTI Call ID	00037030861622732544	CTI Calling Party	35391847001
CTI Called Party	35391731050		

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 R8.1 and two Avaya Aura® Application Enablement Services R8.1 in a 2N Redundancy configuration using DMCC Multi-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® Communication Manager*, Release 8.1.x, Issue 7, October 2020.
- [2] *Administering Avaya Aura® Application Enablement Services*, Release 8.1.x Issue 10 April 2021.
- [3] *Administering Avaya Aura® System Manager* for Release 8.1.x, Issue 8, November 2020.
- [4] *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 7, October 2020.
- [5] *Administering Avaya Session Border Controller for Enterprise*, Release 8.1.x, Issue 3, August 2020.
- [6] *Implementing and Administering Avaya Aura® Media Server*. Release 8.0.x, Issue 11, October 2020.
- [7] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [8] *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)

©2021 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



13th October 2021

To whom it may concern

NICE NIR and NTR recording platforms interoperability with Avaya Aura 8.1

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](#) .

Graham Vail

G M Vail

Product Manager - NICE Public Safety