



Avaya Solution & Interoperability Test Lab

Application Notes for NICE Uptivity with Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes cover the interoperability compliance testing of the NICE Uptivity recording solution with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services (AES).

In the compliance testing, NICE Uptivity used various registration features from the Avaya Aura® Application Enablement Services Device, Media, and Call Control interface to capture media associated with monitored agent stations for call recording.

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

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

Table of Contents

1.	INTRODUCTION.....	3
2.	GENERAL TEST APPROACH AND TEST RESULTS	4
2.1.	Interoperability Compliance Testing	5
2.2.	Test Results.....	5
2.3.	Support	5
3.	REFERENCE CONFIGURATION	6
4.	EQUIPMENT AND SOFTWARE VALIDATED.....	7
5.	CONFIGURE AVAYA AURA® COMMUNICATION MANAGER.....	7
5.1.	Verify Feature and License for the integration.....	8
5.2.	Administer Communication Manager System Features	10
5.3.	Administer IP Services for Application Enablement Services.....	11
5.4.	Administer Computer Telephony Integration (CTI) Link.....	11
5.5.	Verify Recorded Extensions & Add Virtual Stations	12
6.	CONFIGURE AVAYA AURA® APPLICATION ENABLEMENT SERVICES	15
6.1.	Configure Communication Manager Switch Connections.....	16
6.2.	Configure TSAPI Links.....	17
6.3.	Note the TLink Information	18
6.4.	Configure a CTI User for NICE Uptivity	19
6.5.	Enable Unrestricted Access for the NICE Uptivity User	19
6.6.	Confirm TSAPI and DMCC Licenses	20
6.7.	Restart TSAPI Service.....	21
7.	CONFIGURE NICE UPTIVITY	22
7.1.	Create Voice Board.....	23
7.2.	Create Schedule.....	26
7.3.	Create CTI Cores.....	27
8.	VERIFICATION STEPS.....	30
8.1.	Verify Communication Manager Status	30
8.2.	Verify Application Enablement Services Status	32
8.3.	Verify Recording and Playback.....	33
9.	CONCLUSION.....	34
10.	ADDITIONAL REFERENCES	34

1. Introduction

These Application Notes describe the configuration steps for the Uptivity recording solution from NICE to interoperate with the Avaya solution consisting of Avaya Aura® Communication Manager R7.1.3, Avaya Aura® Session Manager R7.1.3, and Avaya Aura® Application Enablement Services R7.1.3. Uptivity uses Communication Manager's Multiple Registration and/or Single Step Conference (SSC) 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 endpoints, listed in **Section 4**.

The NICE Uptivity system interfaces with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services, using the Telephony Service API (TSAPI) to obtain call event information and the Device, Media & Call Control (DMCC) API to obtain audio via various Registration methods.

DMCC allows software vendors to create soft phones on a recording server, and use them to monitor and record Avaya phones. This is purely a software solution and does not require telephony boards or any wiring beyond a typical network infrastructure.

The compliance testing focused on the monitoring and recording performed by NICE Uptivity of calls placed to and/or from digital, H.323, and SIP telephones, H.323 and SIP softphones, agents, hunt groups and Vector Directory Numbers (VDNs) supported by Communication Manager. NICE Uptivity uses:

- The TSAPI interface of AES to monitor extensions and hunt groups to obtain call and login events.
- The DMCC interface of AES to register the recorder with Communication Manager in order to record devices.

2. General Test Approach and Test Results

The feature test cases were performed manually. Upon start of the NICE Uptivity application, the application established a DMCC Stream with Application Enablement Services to register the recorder as a Main or (In)Dependent IP Endpoint for each of the virtual or target stations on Communication Manager, and to receive Third Party call events via a TSAPI Stream.

Each call was handled manually at the agent station with generation of unique audio content for recording. Necessary agent actions such as hold and reconnect were performed from the Desk Phone or Softphone to test various call scenarios.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to NICE Uptivity and Application Enablement Services.

The verification of tests included use of status screens, logs for proper message exchanges and use of the NICE Uptivity web interfaces for proper logging and playback of call recordings.

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 interfaces between Avaya systems and NICE Uptivity utilized enabled capabilities of TLS for Application links between Application Enablement Services and CM, and streams between Application Enablement Services and NICE Uptivity. However, SRTP is not currently supported with the NICE Uptivity solution so all media sessions between the Gateways and recorder utilized Advanced Encryption Standard (AES) encrypted media.

This test was conducted in a lab environment simulating a basic customer network environment. The testing focused on the standards-based interface between the Avaya solution and the NICE Uptivity solution.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing.

The feature testing focused on verifying the following on NICE Uptivity:

- Handling of call events.
- Use of DMCC registration services to register the IP softphones.
- Use of TSAPI and/or DMCC monitoring services and media control events to obtain the media and call events from the phones.
- Proper recording, logging, and playback of calls for scenarios involving hold, reconnect, conference, transfer.

Serviceability testing focused on verifying the ability of NICE Uptivity to recover from adverse conditions, such as disconnecting and reconnecting the Ethernet connection to NICE Uptivity and Application Enablement Services.

2.2. Test Results

All Test cases were executed and verified. The only observations were the current lack of support for SRTP media streams although as stated, AES encryption is supported. Also, on consultative calls (transfers and conference), the internal station to station meta data is tagged to the second leg of the call, not the original external caller data. Blind transfer and conference tag original caller data to both legs of the call.

2.3. Support

Technical support on NICE Uptivity can be obtained through the following:

- 1-888-922-5526
- Or on the web at <https://help.incontact.com/>

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**.

The agent station extensions used in the compliance testing were 30001 through 30006. Virtual extensions 33001-33009 were also available for testing.

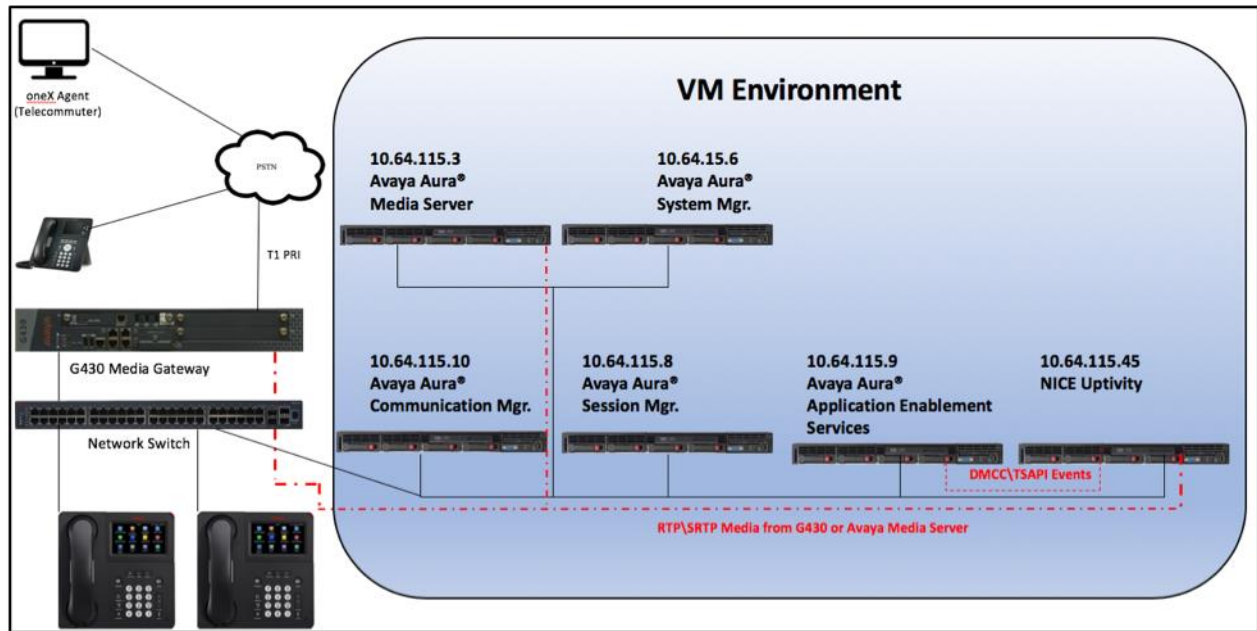


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on VMWare ESXi 6.0	R7.1.3 (Feature Pack 3) (7.1.3.0.0.532.0-24515)
Avaya Aura® Application Enablement Services running on VMWare ESXi 6.0	R7.1.3 (7.1.3.0.1.7-0)
Avaya G430 Media Gateway	38.20.1/1
Avaya Aura® Media Server running on VMWare ESXi 6.0	7.8.0.333
Avaya 6408D Digital Station	N/A
Avaya 9670G	3.280A (H.323)
Avaya 9641G	7.1.1.09 (SIP)
Avaya 9611G	6.6506 (H.323)
Avaya 9630G	2.6.17 (SIP)
Avaya oneX® Agent	2.5.60129.0 (H.323)
NICE Uptivity on Microsoft Windows (running on VMWare) Avaya DMCC .NET	17.3.0605.652 2012R2 Standard ESXi 6.0 6.3.3

5. Configure Avaya Aura® Communication Manager

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

- Verify Feature and License for the integration
- Administer Communication Manager System Features
- Administer IP Services for Application Enablement Services
- Administer Computer Telephony Integration (CTI) Link
- Verify Recorded Extensions & Add Virtual Stations

All configuration changes in this section for Communication Manager are performed through the System Access Terminal (SAT) interface. For more details on configuring Communication Manager, refer to the Avaya product documentation in **Section 10**.

The test environment consisted of a mix of phones. PRI trunks connect the test systems to the PSTN enabling calls and EC500 interactions with external devices. These Application Notes do not cover the full environment, much of it is standard implementation. Rather, these notes focus on the parts that impact the integration with the tested application.

Recording can be performed via DMCC using one of three methods, depending on the target station types. Understanding this will help with perspective in this document. Bold indicates the methods used in the tested solution.

Target Endpoint Type	Multi-Registration	Service Observe	Single Step Conference
SIP	No	Yes (Main Mode)	Yes (Main Mode)
SIP Dual-Reg	Yes (Independent Mode)	Yes (Main Mode)	Yes (Main Mode)
H.323	Yes (Dependent Mode)	Yes (Main Mode)	Yes (Main Mode)
Digital	Yes (Dependent Mode)	Yes (Main Mode)	Yes (Main Mode)
Analog	N/A	Yes (Main Mode)	Yes (Main Mode)

The NICE Uptivity application uses Dependent (Multiple Registration) to record Digital and H.323 endpoints, Independent Mode (Multiple Registration) to record SIP Dual-Registration devices, and Single Step conference virtual extensions using Main mode to record any target that cannot use Multiple Registration.

5.1. Verify Feature and License for the integration

For recording solutions, the following license are required on Communication Manager:

- Recorders that use Single Step Conference or Service Observation (i.e. Registering using the MAIN option), will use a virtual extension to join the recorder to calls. Each recording port using these methods will consume a **Station** license when administered.

display system-parameters customer-options		Page 1 of 12
OPTIONAL FEATURES		
G3 Version: V17	Software Package: Enterprise	
Location: 2	System ID (SID): 1	
Platform: 28	Module ID (MID): 1	
		USED
Platform Maximum Ports: 6400	94	
Maximum Stations: 2400	16	
Maximum XMOBILE Stations: 2400	0	
Maximum Off-PBX Telephones - EC500: 9600	1	
Maximum Off-PBX Telephones - OPS: 9600	3	
Maximum Off-PBX Telephones - PBFMC: 9600	0	
Maximum Off-PBX Telephones - PVFMC: 9600	0	
Maximum Off-PBX Telephones - SCCAN: 0	0	
Maximum Survivable Processors: 313	0	

- Recorders using the Multiple Registration (ie. Registering using the DEPENDENT or INDEPENDENT option) do not require additional station license. All methods will consume a **Concurrently Registered IP Station** license:

display system-parameters customer-options		Page 2 of 12
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	4000	0
Maximum Concurrently Registered IP Stations:	2400	11
Maximum Administered Remote Office Trunks:	4000	0
Maximum Concurrently Registered Remote Office Stations:	2400	0
Maximum Concurrently Registered IP eCons:	68	0
Max Concur Registered Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	2400	0
Maximum Video Capable IP Softphones:	2400	0
Maximum Administered SIP Trunks:	4000	55
Maximum Administered Ad-hoc Video Conferencing Ports:	4000	0
Maximum Number of DS1 Boards with Echo Cancellation:	80	0

- In previous versions of Communication Manager, the IP_API_A (DMCC) may have been enforced on Communication Manager, and/or Application Enablement. With version 7 of Communication Manager, this RTU is completely controlled by Application Enablement Services (DMCC_DMC).
- Customers who purchase Application Enablement will have ASAI capabilities enabled on the Communication Manager. These include **ASAI Link Core Capabilities** and/or **Computer Telephony Adjunct Links** (enabled when TSAPI Basic RTU are purchased):

display system-parameters customer-options		Page 4 of 12
OPTIONAL FEATURES		
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? y	
Access Security Gateway (ASG)? y	Authorization Codes? y	
Analog Trunk Incoming Call ID? y	CAS Branch? n	
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n	
Answer Supervision by Call Classifier? y	Change COR by FAC? n	
ARS? y	Computer Telephony Adjunct Links? y	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? y	DCS (Basic)? y	
ASAI Link Core Capabilities? y	DCS Call Coverage? y	
ASAI Link Plus Capabilities? y	DCS with Rerouting? y	
Async. Transfer Mode (ATM) PNC? n		
Async. Transfer Mode (ATM) Trunking? n	Digital Loss Plan Modification? y	
ATM WAN Spare Processor? n	DS1 MSP? y	
ATMS? y	DS1 Echo Cancellation? y	
Attendant Vectoring? y		

5.2. Administer Communication Manager System Features

If UCID is desired, make the following changes using an appropriate Node ID based on the customer requirements.

```
change system-parameters features                               Page 5 of 19
                        FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:                Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                        Switch Name: SIL Denver
  Emergency Extension Forwarding (min): 10
  Enable Inter-Gateway Alternate Routing? n
  Enable Dial Plan Transparency in Survivable Mode? n
                        COR to Use for DPT: station
                        EC500 Routing in Survivable Mode: dpt-then-ec500
MALICIOUS CALL TRACE PARAMETERS
  Apply MCT Warning Tone? n    MCT Voice Recorder Trunk Group:
  Delay Sending RElease (seconds): 0
SEND ALL CALLS OPTIONS
  Send All Calls Applies to: station    Auto Inspect on Send All Calls? n
  Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
  Create Universal Call ID (UCID)? y    UCID Network Node ID: 1
```

```
change system-parameters features                               Page 13 of 19
                        FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER MISCELLANEOUS
  Callr-info Display Timer (sec): 10
                        Clear Callr-info: next-call
  Allow Ringer-off with Auto-Answer? n

  Reporting for PC Non-Predictive Calls? n

  Agent/Caller Disconnect Tones? n
  Interruptible Aux Notification Timer (sec): 3
  Zip Tone Burst for Callmaster Endpoints: double

ASAI
  Copy ASAI UII During Conference/Transfer? n
  Call Classification After Answer Supervision? n
                        Send UCID to ASAI? y
  For ASAI Send DTMF Tone to Call Originator? y
  Send Connect Event to ASAI For Announcement Answer? n
  Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? y
```

5.3. Administer IP Services for Application Enablement Services

Use the **change ip-services** command to Enable IP-Services for Application Enablement Services:

change ip-services				Page 1 of 3	
IP SERVICES					
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port
AESVCS	y	procr	8765		

On page 3, add the **hostname** for the Application Enablement Services server, and a **password** that will be entered in the AES setup in the next section.

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

5.4. Administer Computer Telephony Integration (CTI) Link

Add a CTI-Link with **ADJ-IP** link Type, the name is not critical:

add cti-link 1		Page 1 of 3	
CTI LINK			
CTI Link: 1			
Extension: 30000			
Type: <u>ADJ-IP</u>			
COR: <u>1</u>			
Name: SILDVAES			

5.5. Verify Recorded Extensions & Add Virtual Stations

For recording solutions using MAIN registration type (Single Step Conference or Service Observe), virtual extensions are administered for each recording port. In this test environment, stations 33000 – 33009 were previously built as:

- **Type** = 9630
- **Security Code** = eg: 123456 (this will be required when setting up the recorder)
- **IP Softphone** = y
- **COR** = 1 (note, only relevant for Service Observe methods)

```
change station 33000                                     Page 1 of 5
STATION
Extension: 33000                                         Lock Messages? n          BCC: 0
  Type: 9630                                           Security Code: *      TN: 1
Port: S00002                                           Coverage Path 1:          COR: 1
Name: DMCC1                                           Coverage Path 2:          COS: 1
                                           Hunt-to Station:        Tests? y

STATION OPTIONS
Loss Group: 19                                         Time of Day Lock Table:
Personalized Ringing Pattern: 1
Message Lamp Ext: 33000
Speakerphone: 2-way                                   Mute Button Enabled? y
Display Language: english                             Button Modules: 0
Survivable GK Node Name:
Survivable COR: internal                               Media Complex Ext:
Survivable Trunk Dest? y                               IP SoftPhone? y
IP Video Softphone? n
Short/Prefixed Registration Allowed: default
Customizable Labels? y
```

- All other settings may be left at defaults.

For Multiple Registration methods, the agent extensions must be administered as follows:

- **Security Code** = eg: 123456 (this will be required when setting up the recorder)
- **IP Softphone** = y

Agent Stations that will be recorded using Service Observation or Single Step Conference do not require IP Softphone to be enabled.

For SIP endpoints to be able to be recorded using Multiple Registration, the SIP user profile must be associated with an H.323 station (Dual-Registration). Else, these endpoints can be recorded using Service Observe or Single Step Conference.

The relevant settings in the System Manager User Profile for a Dual-Registration user are shown below:

Session Manager Profile *

SIP Registration

Primary Session Manager: silvsm1

Secondary Session Manager: Q

Survivability Server: Q

Max. Simultaneous Devices: 1

Block New Registration When Maximum Registrations Active? ☐

Application Sequences

Origination Sequence: SIP Users

Termination Sequence: SIP Users

Emergency Calling Application Sequences

Emergency Calling Origination Sequence: (None)

Emergency Calling Termination Sequence: (None)

Call Routing Settings

Home Location: Data Center

Conference Factory Set: (None)

Call History Settings

Enable Centralized Call History? ☒

CM Endpoint Profile *

System: SILCM

Profile Type: Endpoint

Extension: 30001 View Endpoint

Set Type: 9630

Security Code: *****

Port: S00019

Voice Mail Number:

Preferred Handle: 30001@silidnver.org

Calculate Route Pattern ☐

Sip Trunk:

Enhanced Call-Info display for 1-line phones ☐

Delete Endpoint on Unassign of Endpoint from User or on Delete User. ☒

Override Endpoint Name and Localized Name ☒

Allow H.323 and SIP Endpoint Dual Registration ☒

H323 Station type, not SIP

Additionally, for Dual-registered devices, the station mapping must be manually entered to enable the SIP device to receive the media for calls to that station:

change off-pbx-telephone station-mapping 30001							Page 1 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode
30001	OPS	-		30001	aar	1	

Call Center and routing administration tasks in Communication Manager were minimal, and not covered in these notes.

To ensure the recorder received media matching its requirements, the IP Address of the Application Enablement Services server was associated with network-region 2, which used ip-codec-set 2 as shown below. Shuffling (IP-IP Direct Audio) was disabled for this network region.

display ip-network-map					Page 1 of 63
IP ADDRESS MAPPING					
IP Address	Subnet Bits	Network Region	VLAN	Emergency Location	Ext
FROM: 10.64.115.9	/	2	n		
TO: 10.64.115.9					
FROM: 10.64.115.33	/	1	n		
TO: 10.64.115.255					

change ip-network-region 2		Page 1 of 20
IP NETWORK REGION		
Region: 2	NR Group: 2	
Location: 1	Authoritative Domain: sildenver.org	
Name: recorder	Stub Network Region: n	
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: no
Codec Set: 2		Inter-region IP-IP Direct Audio: no
UDP Port Min: 2048		IP Audio Hairpinning? n
UDP Port Max: 3329		

change ip-codec-set 2

Page1 of 2

IP MEDIA PARAMETERS

Codec Set: 2

	Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1:	<u>G.711MU</u>	<u>n</u>	<u>2</u>	20
2:				

Media Encryption

Encrypted SRTPC: enforce-unenc-srtpc

1:	<u>1-srtp-aescm128-hmac80</u>
2:	<u>aes</u>
3:	none

6. Configure Avaya Aura® Application Enablement Services

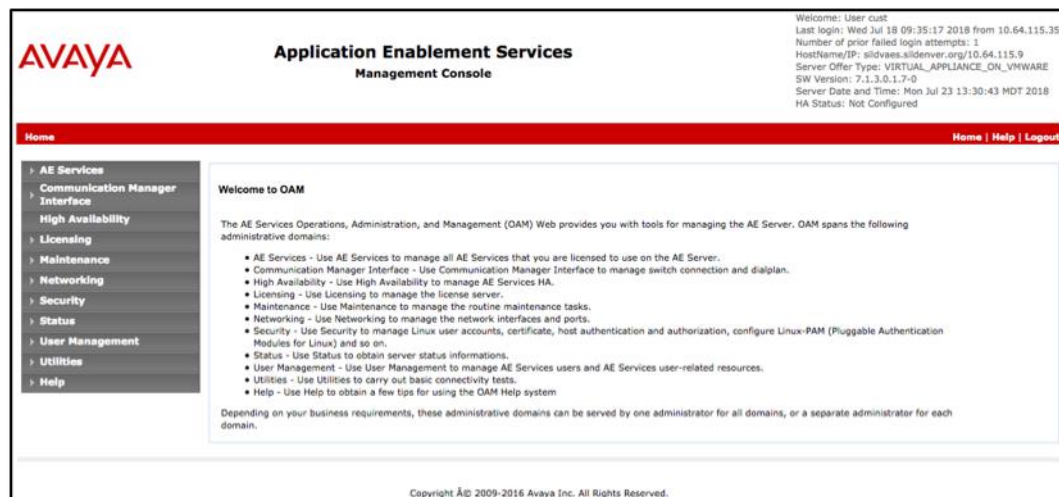
All administration of Application Enablement Services is performed via a web browser. Enter <https://<ip-addr>> in the URL field of a web browser where <ip-addr> is the IP address of the Application Enablement Services server. After a login step, the **Welcome to OAM** page is displayed. All navigation is performed by clicking links in the Navigation Panel on the left side of the screen, context panels will then appear on the right side of the screen.

Note that this server was updated during the testing to version 7.1.3.0.1.7-0, some screenshots display the previous version.

All connections were secure, meaning the rootCA from System Manager was installed on Communication Manager, Application Enablement Services, and the NICE Uptivity server. Identity certificates were generated in System Manager for the Avaya Aura components. By installing the rootCA on the NICE Uptivity server, secure DMCC links and media were possible using a Shared Key methodology. For more secure needs, a Mutual Authentication methodology is supported but was not tested.

The procedures fall into the following areas:

- Configure Communication Manager Switch Connections
- Add TSAPI Links
- Note the TLink Information
- Configure a CTI User for NICE Uptivity
- Enable Unrestricted Access for the NICE Uptivity User
- Confirm TSAPI and DMCC Licenses
- Restart TSAPI Service



6.1. Configure Communication Manager Switch Connections

Navigate to the **Communication Manager Interface > Switch Connections** page and enter a name for the new switch connection (e.g. **SILDVCM1**) and click the **Add Connection** button (not shown). The **Connection Details** screen is shown. Enter the **Switch Password** configured in [Section 5.3](#) and check the **Secure H323 Connection** and **Processor Ethernet** box if using the **procr** interface. Click **Apply**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with options: AE Services, Communication Manager Interface (selected), Switch Connections (selected), Dial Plan, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled 'Connection Details - SILDVCM1' and contains the following fields and checkboxes:

- Switch Password: [Text Input]
- Confirm Switch Password: [Text Input]
- Msg Period: 30 Minutes (1 - 72)
- Provide AE Services certificate to switch: ☒
- Secure H323 Connection: ☒
- Processor Ethernet: ☒

At the bottom of the form are 'Apply' and 'Cancel' buttons. The top right corner displays system information: 'Welcome: User cust', 'Last login: Wed Apr 25 11:13:08 2018 from 10.64.115.35', 'Number of prior failed login attempts: 0', 'HostName/IP: sildvaes.sildenvr.org/10.64.115.9', 'Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE', 'SW Version: 7.1.1.0.0.5-0', 'Server Date and Time: Thu Apr 26 14:46:58 MDT 2018', and 'HA Status: Not Configured'. The footer indicates 'Copyright © 2009-2016 Avaya Inc. All Rights Reserved.'

Once applied, the **Switch Connections** list will confirm the addition of the connection.

This screenshot is identical to the one above, showing the 'Connection Details - SILDVCM1' configuration page. It displays the same navigation menu, form fields (Switch Password, Confirm Switch Password, Msg Period, Provide AE Services certificate to switch, Secure H323 Connection, Processor Ethernet), and system information at the top right. The footer also reads 'Copyright © 2009-2016 Avaya Inc. All Rights Reserved.'

Click on the **Edit PE/CLAN IPs** button and enter the IP Address for the PROCR of Communication Manager:

Welcome: User cust
Last login: Wed Apr 25 11:13:08 2018 from 10.64.115.35
Number of prior failed login attempts: 0
HostName/IP: silvvaes.sildenver.org/10.64.115.9
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Thu Apr 26 15:00:00 MDT 2018
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

Edit Processor Ethernet IP - SILDVCM1

10.64.115.10 Add/Edit Name or IP

Name or IP Address	Status
10.64.115.10	In Use

Back

Repeat for the **Edit H.323 Gatekeeper**:

Welcome: User cust
Last login: Wed Apr 25 11:13:08 2018 from 10.64.115.35
Number of prior failed login attempts: 0
HostName/IP: silvvaes.sildenver.org/10.64.115.9
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Thu Apr 26 15:00:00 MDT 2018
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

Edit Processor Ethernet IP - SILDVCM1

10.64.115.10 Add/Edit Name or IP

Name or IP Address	Status
10.64.115.10	In Use

Back

6.2. Configure TSAPI Links

Navigate to **AE Services > TSAPI > TSAPI Links** and click **Add Link** (not shown).

Select the **Switch Connection** created in **Section 6.1** in the drop-down menu (SILDVCM1), choose the **Switch CTI Link Number** that matches the link created in [Section 5.4](#) above. Choose an **ASAI Link Version**, 8 is generally recommended. For **Security**, choose either **Both** or **Encrypted**. Both will permit applications not capable of using secure streams to connect, while Encrypted will force all applications to use Encrypted streams. Click **Apply Changes**.

Welcome: User cust
Last login: Thu Apr 26 14:42:53 2018 from 192.168.120.21
Number of prior failed login attempts: 0
HostName/IP: silvvaes.sildenver.org/10.64.115.9
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue May 01 10:18:49 MDT 2018
HA Status: Not Configured

AE Services | TSAPI | TSAPI Links Home | Help | Logout

AE Services
CVLAN
DLG
DMCC
SMS
TSAPI
TSAPI Links
TSAPI Properties
TWS
Communication Manager Interface
High Availability
Licensing

Edit TSAPI Links

Link 1

Switch Connection SILDVCM1

Switch CTI Link Number 1

ASAI Link Version 8

Security Both

Apply Changes Cancel Changes Advanced Settings

This returns to the **TSAPI Links** pages which will confirm the new CTI Link:

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with options like CVLAN, DLG, DMCC, SMS, TSAPI, and Communication Manager. The main content area is titled 'TSAPI Links' and displays a table with the following data:

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	SILDVCM1	1	8	Both

Below the table are buttons for 'Add Link', 'Edit Link', and 'Delete Link'. The top right corner of the console shows system information including the user 'User cust', last login time, and server details.

6.3. Note the TLink Information

From the **TSAPI Links** page, click **Edit Link**, then **Advanced Settings** (not shown) and take note of the Tlinks Configured.

If **Both** was selected for Security in **Section 6.2** above, two Tlinks will appear with the format AVAYA#SwitchLinkName#CSTA#AESHostName. The link with CSTA-S is the secure link that will be used when configuring the NICE Uptivity application in **Section 7**.

The screenshot shows the 'TSAPI Link - Advanced Settings' page. It displays the 'Tlinks Configured' section with two entries:

- AVAYA#SILDVCM1#CSTA-S#SILDVAES
- AVAYA#SILDVCM1#CSTA#SILDVAES

Other settings include 'Max Flow Allowed' (2000), 'TSDI Size' (5242880), and 'TSDI High Water Mark' (80 % of TSDI Size). At the bottom are buttons for 'Apply Changes', 'Cancel Changes', and 'Restore Defaults'.

6.4. Configure a CTI User for NICE Uptivity

Navigate to **User Management > User Admin > Add User**. Enter an appropriate **User Id**, **Common Name**, **Surname**, and **User Password**. Select **Yes** from the **CT User** dropdown list.

Click **Apply** at the bottom of the pages to save the entries.

The screenshot shows the 'Edit User' form in the Avaya User Management interface. The left sidebar contains a navigation menu with the following items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management (expanded), Service Admin, User Admin (expanded), Add User, Change User Password, List All Users, Modify Default Users, Search Users, Utilities, and Help. The main form area is titled 'Edit User' and contains the following fields: * User Id (Uptivity), * Common Name (Uptivity), * Surname (Nice), User Password, Confirm Password, Admin Note, Avaya Role (None), Business Category, Car License, CM Home, Cms Home, CT User (Yes), Department Number, Display Name, Employee Number, Employee Type, Enterprise Handle, Given Name, Home Phone, Home Postal Address, Initials, Labeled URI, Mail, MM Home, Mobile, Organization, Pager, Preferred Language (English), Room Number, and Telephone Number. At the bottom of the form are two buttons: 'Apply Changes' and 'Cancel Changes'.

6.5. Enable Unrestricted Access for the NICE Uptivity User

If the Security Database (SDB) is enabled on Application Enablement Services, set the NICE Uptivity user account to Unrestricted Access to enable any device (station, ACD extension, DMCC virtual station) to be used implicitly. This step avoids the need to duplicate administration.

Navigate to **Security → Security Database → CTI Users → List All Users** and select the **NICE Uptivity** user and click **Edit** (not shown).

On the **Edit CTI User** panel, check the **Unrestricted Access** box and click the **Apply Changes** button. Click **Apply** when asked to confirm the change on the **Apply Changes to CTI User Properties** dialog.

6.6. Confirm TSAPI and DMCC Licenses

NICE Uptivity uses a DMCC (**VALUE_AES_DMCC_DMC**) license for each recording port. Additionally, a TSAPI Basic (**VALUE_AES_TSAPI_USERS**) license is used for each agent station being monitored, as well as each hunt group being monitored. Additionally, recorder ports that will use Single Step Conference or Service Observation will require a TSAPI license to add these ports to calls.

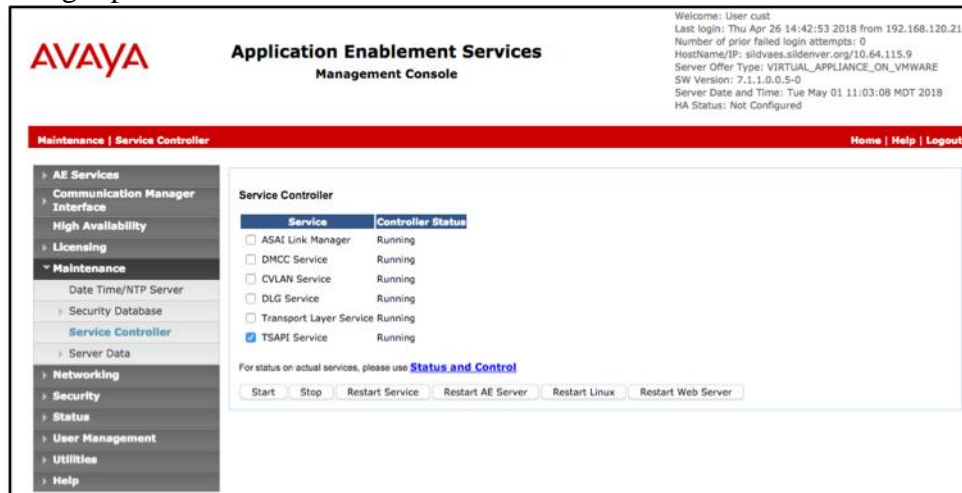
With version 7 and later, WebLM is typically installed and configured on Avaya Aura® System Manager. A **Web License Manager** login window is displayed. Enter proper credentials to log in. Click **Licensed products** → **APPL_ENAB** → **Application_Enablement** from the left pane. The Application Enablement Services license is displayed in the right pane. Ensure enough **VALUE_AES_DMCC_DMC** and **VALUE_AES_TSAPI_USERS** licenses are available.

Licensed products	License installed on: October 18, 2017 7:17:36 PM +00:00		
APPL_ENAB			
▼ Application_Enablement			
View license capacity	License File Host IDs: V3-BE-05-A8-96-95-01		
View peak usage			
CMM	Licensed Features		
► Communication_Manager_Messaging			
Configure Centralized Licensing	10 Items Show All		
COMMUNICATION_MANAGER			
► Call_Center			
► Communication_Manager			
Configure Centralized Licensing			
MSR			
► Media_Server			
SYSTEM_MANAGER			
► System_Manager			
SessionManager			
► SessionManager			
Uninstall license			
Server properties			

Feature (License Keyword)	Expiration date	Licensed capacity
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	3
DLG VALUE_AES_DLG	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	3
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	1000

6.7. Restart TSAPI Service

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

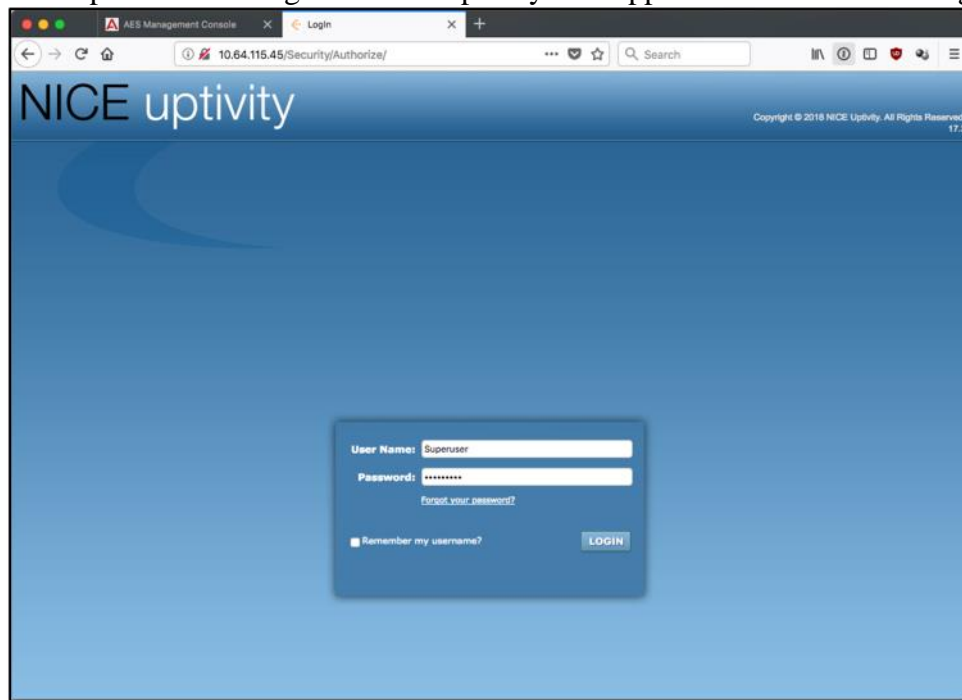


7. Configure NICE Uptivity

The initial configuration of the NICE Uptivity server is typically performed by NICE technicians or authorized installers. These Application Notes will only cover the steps necessary to configure the solution to interoperate with Communication Manager and Application Enablement Services.

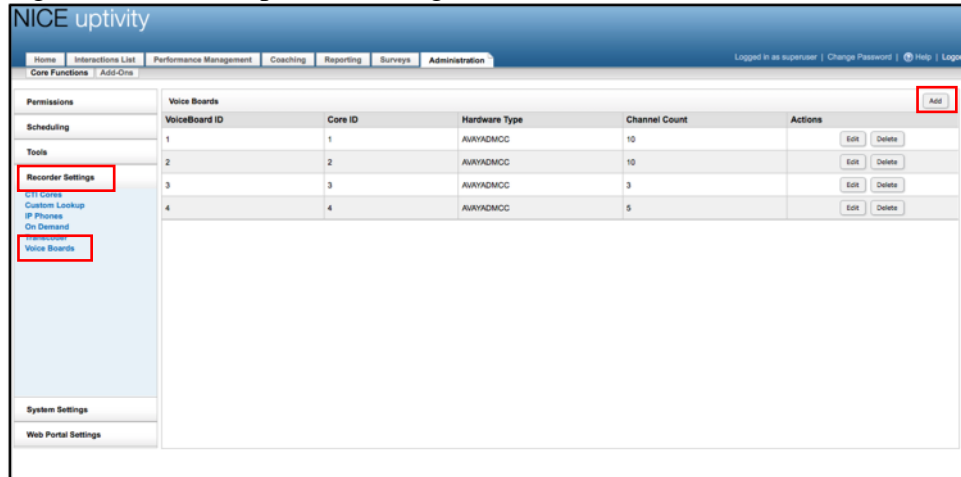
The Uptivity application is the next generation solution incorporating elements from previous products Call Copy and inContact, some UI elements use the legacy naming conventions.

Configuration is performed using the NICE Uptivity web application on the recording server.

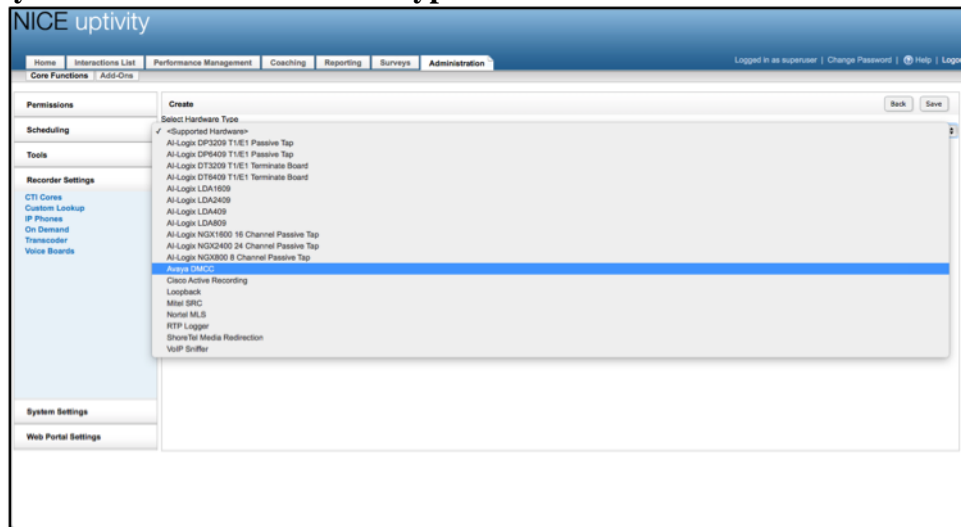


7.1. Create Voice Board

Click on the **Administration** tab and select **Recorder Settings > Voice Boards** in the left window, click on **Add** at the top right of the main window. This screenshot displays the four boards configured for the compliance testing.



Select **Avaya DMCC** as the **Hardware Type**:



Enter the **AES/DMCC Host** information which will be the IP Address of the AES. The DMCC Connection can be secure or unsecure, for compliance testing **Secure DMCC Connection** was set to **Yes**. The **DMCC Port** for a secure connection is set to the DMCC default **4722**. Choose a suitable **DMCC Application Name** and enter the **DMCC User** and **DMCC Password** as per [Section 6.4](#). Set the **DMCC Protocol Version** to **6.3.3**. Enter the IP Address of the Communication Manager PROCR in the **Avaya Call Manager Host** field, and the IP Address of the Uptivity Server in the **DMCC Station Endpoint Host** field. Finally, set the **DMCC Codec** to **G.711 – Mu-Law**.

The screenshot shows the 'Edit VoiceBoard #1' configuration page. The left sidebar contains a navigation menu with categories: Permissions, Scheduling, Tools, Recorder Settings (highlighted), System Settings, and Web Portal Settings. Under 'Recorder Settings', there are links for CTI Cores, Custom Lookup, IP Phones, On Demand, Transcoder, and Voice Boards. The main content area is titled 'General Board Settings (Avaya DMCC)' and contains the following fields:

- AES/DMCC Host: 10.64.115.9
- Secure DMCC Connection: Yes
- Encrypted RTP Stream: Yes
- DMCC Port: 4722
- DMCC Application Name: CallCopy
- DMCC User: Uptivity
- DMCC Password: (masked with asterisks)
- DMCC Protocol Version: 6.3.3
- DMCC Protocol Session Cleanup Delay: 5
- DMCC Protocol Session Duration: 180
- Avaya Call Manager Host: 10.64.115.10
- DMCC Station Endpoint Host: 10.64.115.45
- DMCC Codec: G.711 - Mu-Law

Scroll the page to complete the remaining settings. The value for the RTP Listening Interface (NIC) can be obtained from either Wireshark or from the program cc_interfaceBrowser.exe as shown in Appendix A.

The screenshot shows the bottom section of the configuration page with the following fields:

- DMCC Codec: G.711 - Mu-Law
- RTP Listening Interface (NIC): ED29E7F1-4282-4253-80C9-78503518725D
- DMCC Station Endpoint Initial Port: 7000
- Temp Recording Location: c:\default_rec
- Use Voice Board Reloading: No

Further down on the page, enter the Number of Channels to Add, this will determine the number of simultaneous recording ports that will be used by this voice board. For this board, 2 were chosen allowing each port to be associated with a different Communication Manager extension. This Voice Board was configured to record agent extensions 30002 and 30004 using a **Dedicated Record Voice Port**. When all information is entered, scroll to the top of the page and click **Save**.

Channel ID	Assign	Station	Password	Name	
1	Dedicated Record Voice Port	30002	123456		Delete
2	Dedicated Record Voice Port	30004	123456		Delete
3	Not in use				Delete
4	Not in use				Delete
5	Not in use				Delete
6	Not in use				Delete
7	Not in use				Delete
8	Not in use				Delete
9	Not in use				Delete
10	Not in use				Delete

Channels: Number of Channels to Add: 1 Add

Pages: 1 25 Items per page (10) Go to page: 1 of 1 Go

Repeat the above steps for as many Voice Boards as will be needed for the site. In the compliance test, 4 were configured. The second board was configured identical to the above using a **Dedicated Record Voice Port** for agent station 30001 (the Dual-Registered SIP\H.323 station).

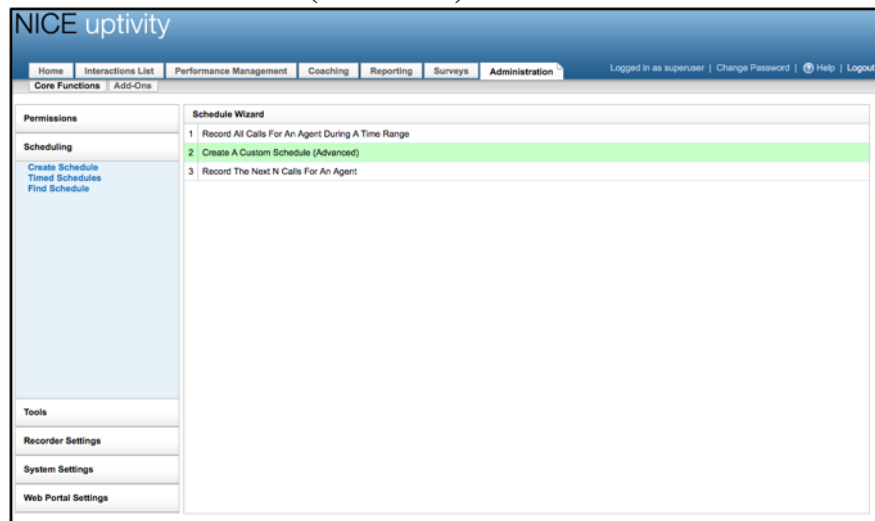
The third board was configured for Single Step Conference using the following Channels, these are virtual extensions in Communication Manager designated for use by the recording application to be registered using the MAIN registration type. The Channel assignment was set to **Anything** on these ports:

Channel ID	Assign	Station	Password	Name	
61	Anything	33000	123456		Delete
62	Anything	33001	123456		Delete
63	Anything	33002	123456		Delete

The fourth board was identical, but used only one channel for Single Step Conference to record the Digital set using virtual extension 33003.

7.2. Create Schedule

Remain in the **Administration** tab and select **Scheduling > Create Schedule** in the left window, click on **Create a Custom Schedule (Advanced)** in the main window.



Enter a suitable name for the schedule. For compliance testing the following were set,

- **Type** Set to **Percentage**
- **Target Percent** Set to **100**
- **Direction** Set to **Both**
- **Schedule Requirements** **Voice Port Greater Than 0**

The other values can be left as default. Click on **Save Schedule** to save this.

	Value Type	Comparison	Value	Case Sensitive
1	Voice Port	Greater Than (>)	0	<input type="checkbox"/>
2				<input type="checkbox"/>
3				<input type="checkbox"/>
4				<input type="checkbox"/>
5				<input type="checkbox"/>

7.3. Create CTI Cores

Remain in the **Administration** tab and select **Recorder Settings > CTI Cores** in the left window, click on **Add Core** at the top right of the main window. One CTI Core was created for each of the four Voice Boards created in **Section 7.1**.

The first Core was used for Multi-Registration to record the H.323 stations 30002/30004. Enter a suitable name for the Core. For compliance testing the following were set,

- **Host** Set to **IP Address of the Uptivity Server**
- **Record Method** Set to **Passive**
- **Enable Event Interface** Set to **Yes**

Note that **Single Step Conference** recording method was specified in the Cores configured to record the Digital and SIP devices, otherwise, all settings were the same.

Voice Board 1 was associated with this Core, as was the **Record All** Schedule:

With the Board and Schedule selected, click on the drop-down menu highlighted and select **Avaya DMCC**, with this selected click on **Add CTI Module**.

From the drop-down menu select **Avaya TSAPI** and click on **Add CTI Module**.

Each new CTI Module needs to be edited, click on the edit icon as shown below and edit each CTI core starting with **cc_AvayaDMCC** as shown below.

The settings below show the DMCC configuration used during compliance testing.

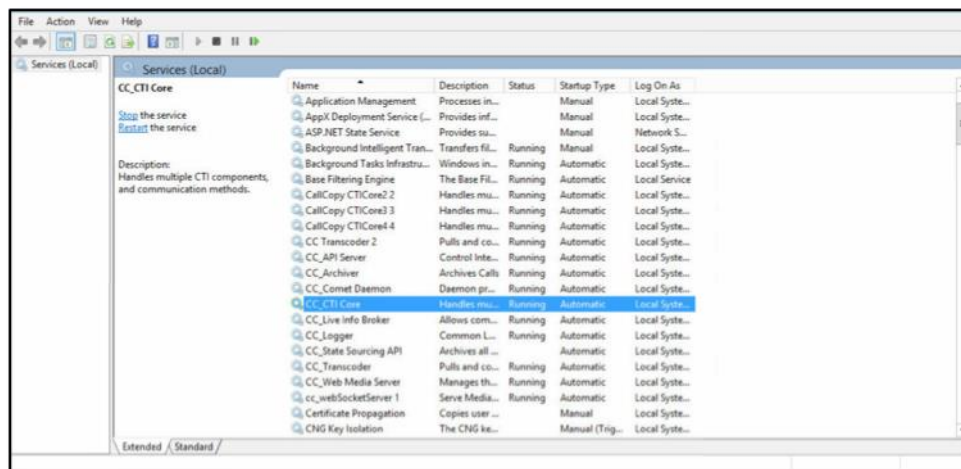
Similarly, edit the **cc_AvayaTSAPIFx** module.

Enter the TLINK information (found from [Section 6.3](#)) into the Server Name box. Enter the CTI user and password as per [Section 6.4](#) for the Server Username and Server Password. The other information can be left as default. Scroll down to Monitors, each device that needs to be monitored can be added here, as shown below these are Agent and Hunt Group extensions 30002, 30004, 31000. Click **Save** when all entries are complete.

ID	Monitor Type
30002	device
30004	device
31000	group

Repeat these steps for the remaining 3 Cores, associating them with the remaining Voice Boards and entering the TSAPI devices to be monitored for each Core.

At this point, the four CTI Cores can be started from the Windows Services control panel.



8. Verification Steps

8.1. Verify Communication Manager Status

From a Communication Manager SAT session, the **list registered-ip-stations** command will show an IP_API_A registration with the Application Enablement server address for Multi-Registration (eg. 30001, 30002, 30004) and Virtual Extensions (eg. 33000) registered to the Uptivity application.

list registered-ip-stations

Page 1

REGISTERED IP STATIONS

Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	Station IP Address/ Gatekeeper IP Address	Skt
30001	9630	IP_API_A	10.64.115.9	tls
	2	3.2040	10.64.115.10	
30002	9611	IP_Phone	10.64.115.36	tls
	1	6.6506	10.64.115.10	
30002	9611	IP_API_A	10.64.115.9	tls
	2	3.2040	10.64.115.10	
30004	9650	IP_Phone	10.64.115.31	tcp
	1	3.280A	10.64.115.10	
30004	9650	IP_API_A	10.64.115.9	tls
	2	3.2040	10.64.115.10	
30007	4621	IP_Phone	10.64.115.37	tcp
	1	2.9020	10.64.115.10	
33000	9630	IP_API_A	10.64.115.9	tls
	2	3.2040	10.64.115.10	
33001	9630	IP_API_A	10.64.115.9	tls
	2	3.2040	10.64.115.10	
33002	9630	IP_API_A	10.64.115.9	tls
	2	3.2040	10.64.115.10	
33003	9630	IP_API_A	10.64.115.9	tls
	2	3.2040	10.64.115.10	

The **list monitored-station** command will show stations with TSAPI monitors.

list monitored-station									
MONITORED STATION									
Associations:	1	2	3	4	5	6	7	8	
Station Ext	CTI	CTI	CTI	CTI	CTI	CTI	CTI	CTI	
	Lnk	CRV	Lnk	CRV	Lnk	CRV	Lnk	CRV	
30001	1	0003							
30002	1	0008							
30003	1	0016							
30004	1	0001							
30005	1	0002							
30006	1	0015							

With an active call, the **status station** command can demonstrate the media properties of a call being recorded. The recorder is 10.64.115.45 connected to the G430 with g711u and aes encrypted media, the station is connected to the Avaya Media Server (AMS) with g729a and srtp encrypted in the example below:

```

status station 30002                                     Page 7 of 9
                                SRC PORT TO DEST PORT TALKPATH
src port: S00005
S00005:TX:10.64.115.36:2328/g729a/20ms/1-srtp-aescm128-hmac80 - station 30002
AMS1:RX:10.64.115.3:6142/g729a/20ms/1-srtp-aescm128-hmac80:TX:cnfID:0 - AMS
AMS1:RX:cnfID:0:TX:10.64.115.3:6144/g729/20ms/1-srtp-aescm128-hmac80 - AMS
001V012:RX:10.64.115.2:2050/g729/20ms/1-srtp-aescm128-hmac80:TX:ctxID:233 - G430
001V011:RX:ctxID:233:TX:10.64.115.2:2056/g711u/20ms/aes
S00003:RX:10.64.115.45:7000/g711u/20ms/aes - recorder

```

The following captures the audio channels involved in the connections with AMS to station 30002 using G.729a, and G430 to the application via AES using G.711MU:

```

status station 30002                                     Page 5 of 9
                                AUDIO CHANNEL Port: S00005
G.729A          Switch-End Audio Location: AMS1
                IP Address          Port  Node Name      Rgn
Other-End: 10.64.115.3              6142  sildvams       1
Set-End: 10.64.115.36              2328                      1
Audio Connection Type: ip-tdm

                                AUDIO CHANNEL Shared Port: S00003
G.711MU          Switch-End Audio Location: MGI
                IP Address          Port  Node Name      Rgn
Other-End: 10.64.115.2              2056                      1
Set-End: 10.64.115.9               7000                      2
Audio Connection Type: ip-tdm

```

The following captures the Call Control associations for the devices registered to station 30002:

```

status station 30002                                     Page 4 of 9
                                CALL CONTROL SIGNALING
Port: S00005          Switch-End IP Signaling Loc: PROCR  H.245 Port:
                IP Address          Port  Node Name      Rgn
Switch-End: 10.64.115.10            1300  procr           1
Reg Set End:10.64.115.36            47482                      1
Alt Set End:not applicable
H.245 Near:
H.245 Set:
Shared Port: S00003  Switch-End IP Signaling Loc: PROCR
                IP Address          Port  Node Name      Rgn
Switch-End:10.64.115.10            1300  procr           1
Reg Set End:10.64.115.9            27341                      2

```

8.2. Verify Application Enablement Services Status

From Application Enablement Services, the **Status > DMCC Service Summary > Session Summary** will reflect the Secure DMCC sessions the recorder Voice Boards have established.

The screenshot shows the AVAYA Application Enablement Services Management Console. The left sidebar contains a navigation menu with categories: AE Services, Communication Manager, Interface, High Availability, Licensing, Maintenance, Networking, Security, and Status. The Status category is expanded, showing options like Alarm Viewer, Logs, Log Manager, Status and Control, CVLAN Service Summary, DLG Services Summary, DMCC Service Summary (selected), Switch Conn Summary, and TSAPI Service Summary. The main content area displays the 'DMCC Service Summary - Session Summary' page. It includes a 'Please do not use back button' warning, a refresh timer set to 60 seconds, and session statistics: Session Summary Device Summary, Generated on Tue Jul 24 11:13:43 MDT 2018, Service Uptime: 6 days, 20 hours 32 minutes, Number of Active Sessions: 4, Number of Sessions Created Since Service Boot: 8, Number of Existing Devices: 7, and Number of Devices Created Since Service Boot: 17. Below this is a table of active sessions.

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	102F6A1FA680E3FE2 AD02CDE59985D09-7	Uptivity	CallCopy	10.64.115.45	XML Encrypted	1
<input type="checkbox"/>	546FB27918650901D FD5664CF22CA71F-5	Uptivity	CallCopy	10.64.115.45	XML Encrypted	1
<input type="checkbox"/>	1091282E770C678E1 901CB848A84F66-4	Uptivity	CallCopy	10.64.115.45	XML Encrypted	2
<input type="checkbox"/>	642ADB120CA7E35C9 83C12ED8A195A80-6	Uptivity	CallCopy	10.64.115.45	XML Encrypted	3

At the bottom, there are buttons for 'Terminate Sessions' and 'Show Terminated Sessions', and a pagination control showing 'Item 1-4 of 4'.

The **Status > TSAPI Service Summary > User Status** should display one stream for each of the CTI Cores:

The screenshot shows the AVAYA Application Enablement Services Management Console. The left sidebar is the same as in the previous screenshot, with the Status category expanded and TSAPI Service Summary selected. The main content area displays the 'TSAPI Service Summary - CTI User Status' page. It includes a refresh timer set to 60 seconds, a dropdown menu for 'CTI Users' set to 'All Users', and a 'Submit' button. Below this, it shows 'Open Streams: 6' and 'Closed Streams: 4'. A table lists the open streams.

Name	Time Opened	Time Closed	Trunk Name
DMCCCLCUserDoNotModify	Tue 17 Jul 2018 02:41:10 PM MDT		AVAYA#SILDVCM1#CSTA#SILDVAES
DMCCCLCUserDoNotModify	Tue 17 Jul 2018 02:41:10 PM MDT		AVAYA#SILDVCM1#CSTA#SILDVAES
Uptivity	Wed 18 Jul 2018 09:37:43 AM MDT		AVAYA#SILDVCM1#CSTA-S#SILDVAES
Uptivity	Wed 18 Jul 2018 09:37:48 AM MDT		AVAYA#SILDVCM1#CSTA-S#SILDVAES
Uptivity	Wed 18 Jul 2018 09:37:52 AM MDT		AVAYA#SILDVCM1#CSTA-S#SILDVAES
Uptivity	Wed 18 Jul 2018 09:37:55 AM MDT		AVAYA#SILDVCM1#CSTA-S#SILDVAES

At the bottom, there are buttons for 'Show Closed Streams', 'Close All Opened Streams', and 'Back'.

The **Status > DMCC Service Summary > Device Summary** will reflect the registrations that the recorder has established.

The screenshot shows the AVAYA Application Enablement Services Management Console. The left sidebar contains a navigation menu with options like AE Services, Communication Manager, Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, Alarm Viewer, Logs, Log Manager, Status and Control, and User Management. The main content area displays the 'DMCC Service Summary - Device Summary' page. It includes a 'Session Summary' section with statistics such as 'Service Uptime: 6 days, 20 hours and 37 minutes', 'Number of Active Sessions: 4', 'Number of Sessions Created Since Service Boot: 8', 'Number of Existing Devices: 7', and 'Number of Devices Created Since Service Boot: 17'. Below this is a table listing devices with columns for Device ID, Gatekeeper IP address, State, and Associated Sessions. The table shows seven registered devices, all with a state of 'REGISTERED' and one associated session each.

Device ID	Gatekeeper IP address	State	Associated Sessions
30001:SILDVCM1:10.64.115.10:0	10.64.115.10	REGISTERED	1
30002:SILDVCM1:10.64.115.10:0	10.64.115.10	REGISTERED	1
30004:SILDVCM1:10.64.115.10:0	10.64.115.10	REGISTERED	1
33000:SILDVCM1:10.64.115.10:0	10.64.115.10	REGISTERED	1
33001:SILDVCM1:10.64.115.10:0	10.64.115.10	REGISTERED	1
33002:SILDVCM1:10.64.115.10:0	10.64.115.10	REGISTERED	1
33003:SILDVCM1:10.64.115.10:0	10.64.115.10	REGISTERED	1

8.3. Verify Recording and Playback

Using a browser, access the NICE Uptivity user interface and navigate to the **Interactions List** tab and click on the date you wish to search for calls. Note there are more refined searches that can be performed, the following will display all recordings the logged in user has rights to view based on permissions administered elsewhere in the web application. In most browsers, the way form will display in the Playback Details section of the screen.

The screenshot shows the NICE Uptivity user interface. The top navigation bar includes tabs for Home, Interactions List, Performance Management, Coaching, Reporting, Surveys, and Administration. The 'Interactions List' tab is active. Below the navigation bar, there is a 'Filter' section with 'Previous Filter' and 'Current Filter: Time Recorded'. A table of call records is displayed with columns for Record ID, First Name, Last Name, Voice Port, Time Recorded, Duration, Caller ID ANI, Call Direction, Agent Number, Number Called DNIS, ACD Gate, and Total H. The table shows several call records, with the last record (Record ID 76) highlighted in green. Below the table, there is a 'Web Player' section with a 'Layer Details' table and a 'Playback Details' section showing a progress bar and a play button.

Record ID	First Name	Last Name	Voice Port	Time Recorded	Duration	Caller ID ANI	Call Direction	Agent Number	Number Called DNIS	ACD Gate	Total H
84			30004	7/19/18 1:15:04 PM	00:00:08	3035383421	I	30004	17209772879		
83			30002	7/19/18 1:14:49 PM	00:00:20	3035383421	I	30002	17209772879		
82			30003	7/19/18 1:08:47 PM	00:01:17	30007	I	30003	30003		
81			30005	7/19/18 1:07:32 PM	00:00:33	30005	O	30005	30004		
80			30004	7/19/18 1:07:32 PM	00:00:33	30005	I	30004	30004		
79			30002	7/19/18 1:05:56 PM	00:00:39	30001	I	30002	30002		
78			30001	7/19/18 1:05:56 PM	00:00:39	30001	O	30001	30002		
77			30003	7/19/18 10:18:03 AM	00:00:52	30003	O	30003	30002		
76			30002	7/19/18 10:18:03 AM	00:00:52	30003	I	30002	30002		

9. Conclusion

These Application Notes describe the procedures for configuring NICE Uptivity to monitor and record calls placed to and from agents and phones on Avaya Aura® Communication Manager. In the configuration described in these Application Notes, NICE Uptivity uses the Device and Media Control Services of Avaya Aura® Application Enablement Services to perform recording. During compliance testing, NICE Uptivity successfully recorded calls placed to and from agents and stations.

Refer to **Section 2.2** for details regarding secure media limitations.

10. Additional References

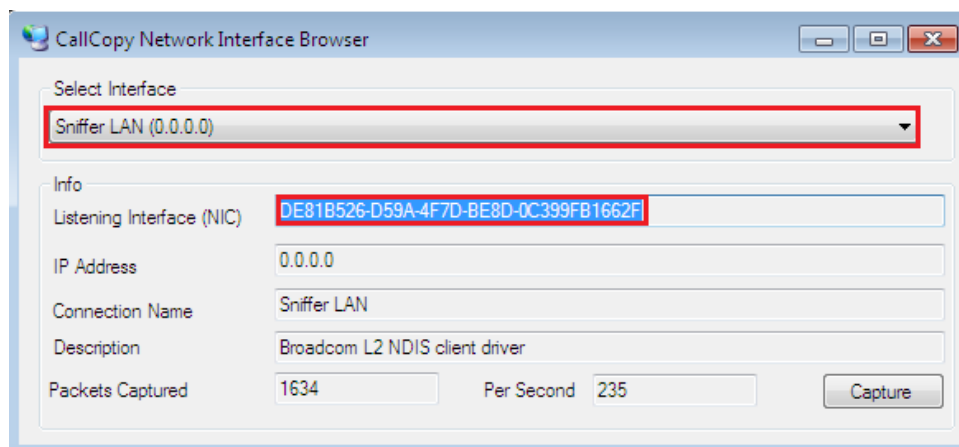
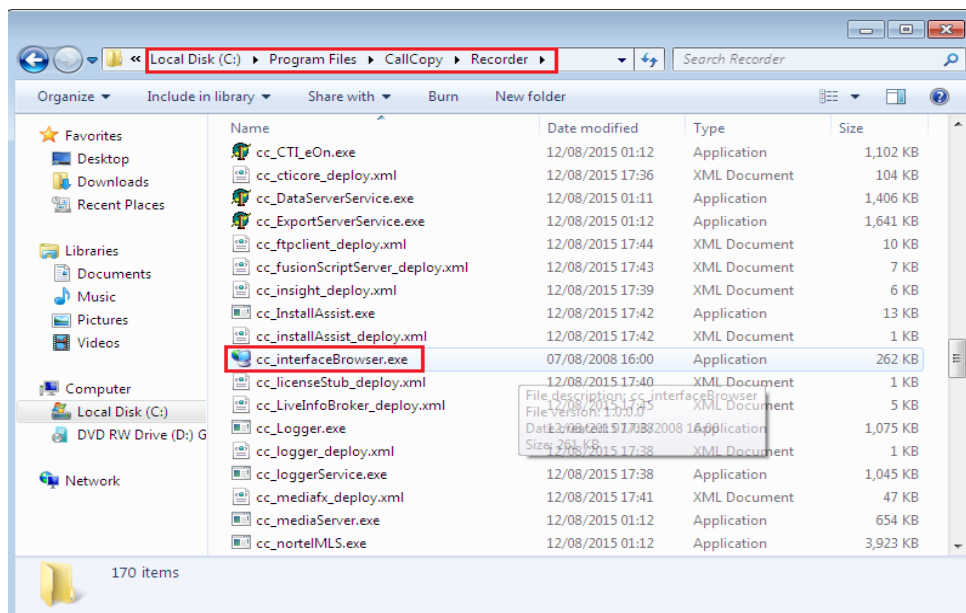
Product documentation for Avaya products may be found at <http://support.avaya.com>.

- *Administering Avaya Aura® Communication Manager*, Release 7.1.1, Issue 2, August 2017
- *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 7.1.1, Issue 3, September 2017
- *Avaya Aura® Application Enablement Services Device, Media and Call Control .NET API Programmers Guide Release 7.1.1*, Issue 1, Document Number 02-602658

Appendix A

Open the application called cc_interfaceBrowser.exe, this should be located in Program Files → CallCopy → Recorder folder.

Select the correct Network Interface which is used to capture the RTP from the data switch. The Listening Interface should then be populated and this is used for the setup of the NICE Uptivity Call Recording server in **Section 7**.



©2018 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.