



Avaya Solution & Interoperability Test Lab

Application Notes for Numonix Recite Interaction Recording Solution with Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes outline how to configure the Numonix Recite recording solution to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services (AES).

In the compliance testing, Numonix Recite used the Multiple Registration feature 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.

1. Introduction

Numonix's Recite solution is an interaction recording suite designed to boost business success. Recite delivers insights into employee-customer interactions by capturing content from multiple media modalities, including voice, video, screen and chat/IM.

The Numonix Recite 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 the Multiple Registrations method.

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

Recite uses:

- The TSAPI interface of AES (via DMCC) to monitor extensions to obtain call events.
- The DMCC interface of AES to register the recorder as an additional registered endpoint with Communication Manager in order to record devices.

Serviceability tests were also conducted to assess the reliability of the Recite solution.

2. General Test Approach and Test Results

The feature test cases were performed manually. Upon start of the Recite application, the application automatically established a DMCC stream with AES to register the recorder as a Dependent additional IP Endpoint for each of the target stations on Communication Manager, and to receive third party call events via TSAPI through the DMCC stream.

Each call was handled manually at the agent 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 Recite and Avaya components.

The verification of tests included use of logs for proper message exchanges and use of the Recite 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 interface between Avaya systems and Numonix Recite utilized enabled capabilities of TLS for Application links between Application Enablement and CM, and streams between Application Enablement and Recite. Further, SRTP was used to encrypt all media streams.

This test was conducted in a lab environment simulating a basic customer enterprise network environment. The testing focused on the standards-based interface between the Avaya solution and the Numonix solution. The results of testing are therefore considered to be applicable to either a premise-based deployment or to a hosted or cloud deployment where some elements of the Numonix solution may reside beyond the boundaries of the enterprise network, or at a different physical location from the Avaya components.

Readers should be aware that network behaviors (e.g. jitter, packet loss, delay, speed, etc.) can vary significantly from one location to another and may affect the reliability or performance of the overall solution. Different network elements (e.g. session border controllers, soft switches, firewalls, NAT appliances, etc.) can also affect how the solution performs.

If a customer is considering implementation of this solution in a cloud environment, the customer should evaluate and discuss the network characteristics with their cloud service provider and network organizations and evaluate if the solution is viable to be deployed in the cloud.

The network characteristics required to support this solution are outside the scope of these Application Notes. Readers should consult the appropriate Avaya and Numonix documentation for the product network requirements. Avaya makes no guarantee that this solution will work in all potential deployment configurations.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing.

The feature testing focused on verifying the following on Recite:

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

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

2.2. Test Results

All test cases were executed and verified. The following observations were made from the compliance testing.

- Held calls appear as two calls in the playback query, each with meta data identifying the parties on the call. A reviewer would know these were related by the context of the audio recorded.

2.3. Support

Technical support on Numonix Recite can be obtained through the following:

- Email: support@numonixrecording.com
- Phone: +1-561-952-2600 opt 2.
- Web: <https://numonixrecording.com/contact-support/>

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.

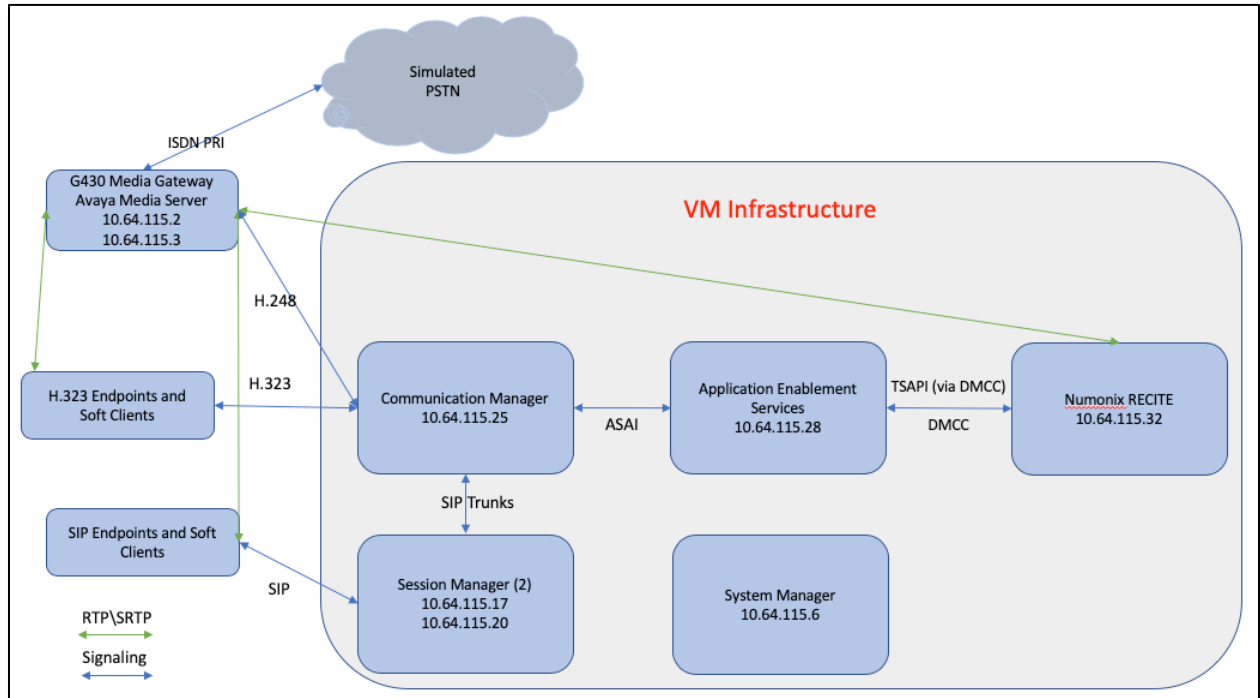


Figure 1: Numonix Recite Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Version
Avaya Aura® Communication Manager running on virtualized environment	R018x.00.0.822.0
Avaya Aura® Application Enablement Services running on virtualized environment	8.0.1.0.3.5-0
Avaya Aura® Session Manager running on virtualized environment	8.0.0.0.800035
Avaya Aura® System Manager	8.0.0.0.098174
Avaya Aura® Media Server	
Avaya G450 Media Gateway	FW 38.20.1/1
Avaya 96x1 Series IP Telephone <ul style="list-style-type: none">96x1 (H.323)96x1 (SIP)	6_6_5_06-080917 7.0.1
Avaya 1416 Digital Telephones	FW 1
Desktop PC running Avaya One-X® Agent	2.5.60129.0 (H.323)
Numonix RECITE	3.0.4.2
Windows 2012R2 Standard Server	2012 R2
VMWare (Host)	ESXi 6.0
DMCC .NET SDK	6.3.3.14

5. Configure Avaya Aura® Communication Manager

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

- Confirm Licensing
- 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 (see **Section 4** for details on these). 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.

The Numonix Recite application uses Dependent (Multiple Registration) to record Digital and H.323 endpoints, Independent Mode (Multiple Registration) to record SIP devices.

5.1. Confirm Licensing

The Multiple Registration DMCC recording method does not require additional “Virtual Extensions” built for the recorder to register and use to join calls like Single Step Conference and Service Observe recording methods do.

- Recorders using the Multiple Registration (i.e., 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 Services 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. Note, these changes are outlined in Bold.

```

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 Avaya Aura® Application Enablement Services

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

```

change ip-services                                               Page 1 of 3

                                IP SERVICES
Service      Enabled      Local      Local      Remote      Remote
Type         Type         Node       Port       Node        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      Password      Enabled      Status
              Server
1:      sildvaes      *              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: ADJ-IP
                                COR: 1
    Name: SILDVAES

```

5.5. Verify Recorded Extensions & Add Virtual Stations

For recording solutions using Dependent or Independent mode registration type, agent extensions are administered as follows to allow the recording port to register.

- **Type** = 9630
- **Security Code** = eg: 123456 (this will be required when setting up the recorder)
- **IP Softphone** = y

```
change station 30001                                     Page 1 of 5
                                                         STATION
Extension: 30001                                         Lock Messages? n          BCC: 0
Type: 9630                                             Security Code: *         TN: 1
Port: S00002                                           Coverage Path 1:            COR: 1
Name: Agent1                                           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
```

To ensure the recorder received media matching its requirements, the IP Address of the AES server was associated with network-region 2, which used ip-codec-set 2 as shown on next page. 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	Emergency Location	Ext
FROM: 10.64.115.28	/	2	n	
TO: 10.64.115.28				
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: sildDenver.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
```

IP Codec used for compliance testing.

change ip-codec-set 2

Page 1 of 2

IP MEDIA PARAMETERS

Codec Set: 2

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

Media Encryption

1: 1-srtp-aescm128-hmac80

2: aes

3: none

Encrypted SRTCP: enforce-unenc-srtcp

6. Configure Avaya Aura® Application Enablement Services

All administration of the AES 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 AES 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.

All connections were secure, meaning the root CA from System Manager was installed on Communication Manager, AES, and the Numonix Recite server. Identity certificates were generated in System Manager for the Avaya Aura components. By installing the root CA on the Recite 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
- Configure TSAPI Links
- Note the TLink Information
- Configure a CTI User for Recite
- Enable Unrestricted Access for the Recite User
- Confirm TSAPI and DMCC Licenses
- Restart TSAPI Service

The screenshot displays the Avaya Application Enablement Services Management Console. At the top, the Avaya logo is on the left, and the title 'Application Enablement Services Management Console' is in the center. On the right, a 'Welcome' message provides system details: 'User cust', 'Last login: Tue Jun 18 13:35:06 2019 from 10.64.10.210', 'Number of prior failed login attempts: 0', 'HostName/IP: sildvaes8.sildenvr.org/10.64.115.28', 'Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE', 'SW Version: 8.0.1.0.3.5-0', 'Server Date and Time: Mon Aug 12 14:07:14 MDT 2019', and 'HA Status: Not Configured'. Below the title bar, a red navigation bar contains 'Home', 'Help', and 'Logout'. On the left, a vertical navigation panel lists menu items: 'AE Services', 'Communication Manager Interface', 'High Availability', 'Licensing', 'Maintenance', 'Networking', 'Security', 'Status', 'User Management', 'Utilities', and 'Help'. The main content area, titled 'Welcome to OAM', contains a paragraph explaining the OAM Web's purpose and a bulleted list of administrative domains: 'AE Services', 'Communication Manager Interface', 'High Availability', 'Licensing', 'Maintenance', 'Networking', 'Security', 'Status', 'User Management', 'Utilities', and 'Help'. A footer note states: 'Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.' The bottom of the page features the copyright notice: 'Copyright © 2009-2018 Avaya Inc. All Rights Reserved.'

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. **SILDVCM8**) 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 - SILDVCM8'. It contains the following fields and options:

- 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: ☒
- Buttons: Apply, Cancel

At the top right, a welcome message is displayed: 'Welcome: User cust. Last login: Tue Jun 18 13:35:06 2019 from 10.64.10.210. Number of prior failed login attempts: 0. HostName/IP: sildvaes8.sildenvr.org/10.64.115.28. Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE. SW Version: 8.0.1.0.3.5-0. Server Date and Time: Mon Aug 12 14:09:54 MDT 2019. HA Status: Not Configured'.

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

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Switch Connections'. It contains a table with the following columns: Connection Name, Processor Ethernet, Msg Period, and Number of Active Connections. The table has one row with the connection name 'SILDVCM8'.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
SILDVCM8	Yes	30	1

Below the table, there are buttons: Edit Connection, Edit PE/CLAN IPs, Edit H.323 Gatekeeper, Delete Connection, and Survivability Hierarchy. At the top right, the same welcome message is displayed as in the previous screenshot.

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

AVAYA

Application Enablement Services
Management Console

Welcome: User cust
Last login: Tue Jun 18 13:35:06 2019 from 10.64.10.210
Number of prior failed login attempts: 0
HostName/IP: sildvaes8.sildenver.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.1.0.3.5-0
Server Date and Time: Mon Aug 12 14:11:26 MDT 2019
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

Status

User Management

Utilities

Help

Edit Processor Ethernet IP - SILDVCMS

10.64.115.25

Add/Edit Name or IP

Name or IP Address	Status
10.64.115.25	In Use

Back

Copyright © 2009-2018 Avaya Inc. All Rights Reserved.

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

AVAYA

Application Enablement Services
Management Console

Welcome: User cust
Last login: Tue Jun 18 13:35:06 2019 from 10.64.10.210
Number of prior failed login attempts: 0
HostName/IP: sildvaes8.sildenver.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.1.0.3.5-0
Server Date and Time: Mon Aug 12 14:12:19 MDT 2019
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

Status

User Management

Utilities

Help

Edit H.323 Gatekeeper - SILDVCMS

Add Name or IP

Name or IP Address

10.64.115.25

Delete IP

Back

Copyright © 2009-2018 Avaya Inc. All Rights Reserved.

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 (SILDVCM8), choose the **Switch CTI Link Number** that matches the link created in **Section 5.4** above.

Choose an **ASAI Link Version**, 9 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**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with 'AE Services' expanded, showing 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (selected), 'TWS', 'Communication Manager Interface', 'High Availability', 'Licensing', 'Maintenance', 'Networking', 'Security', and 'Status'. The main content area is titled 'Edit TSAPI Links' and contains the following fields:

- Link: 1
- Switch Connection: SILDVCM8
- Switch CTI Link Number: 1
- ASAI Link Version: 9
- Security: Both

At the bottom of the form are three buttons: 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'. The top right of the console displays user information: 'Welcome: User cust', 'Last login: Tue Jun 18 13:35:06 2019 from 10.64.10.210', 'Number of prior failed login attempts: 0', 'HostName/IP: sildvaes8.sildenver.org/10.64.115.28', 'Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE', 'SW Version: 8.0.1.0.3.5-0', 'Server Date and Time: Mon Aug 12 14:15:00 MDT 2019', and 'HA Status: Not Configured'. The top navigation bar includes 'AE Services | TSAPI | TSAPI Links', 'Home | Help | Logout'.

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

The screenshot shows the Avaya Application Enablement Services Management Console with the 'TSAPI Links' page. The left sidebar is the same as in the previous screenshot. The main content area is titled 'TSAPI Links' and contains a table with the following data:

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	SILDVCM8	1	9	Both

Below the table are three buttons: 'Add Link', 'Edit Link', and 'Delete Link'. The top right of the console displays the same user information as in the previous screenshot. The top navigation bar includes 'AE Services | TSAPI | TSAPI Links', 'Home | Help | Logout'.

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 Recite application in **Section 7**.

The screenshot shows the AVAYA Application Enablement Services Management Console. The top navigation bar includes 'AE Services | TSAPI | TSAPI Links' and 'Home | Help | Logout'. The left sidebar lists various services, with 'TSAPI Links' selected under the 'TSAPI' category. The main content area is titled 'TSAPI Link - Advanced Settings' and displays the following information:

- Tlinks Configured: AVAYA#SILDVCM8#CSTA-S#SILDVAES8
- Max Flow Allowed: 2000
- TSDI Size: 5242880
- TSDI High Water Mark: 80 % of TSDI Size

At the bottom of the settings area are buttons for 'Apply Changes', 'Cancel Changes', and 'Restore Defaults'.

6.4. Configure a CTI User for Recite

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 AVAYA User Management console. The top navigation bar includes 'User Management | User Admin | List All Users' and 'Home | Help | Logout'. The left sidebar lists various services, with 'User Admin' selected under the 'User Management' category. The main content area is titled 'Edit User' and displays the following information:

- * User Id: Numonix
- * Common Name: Numonix
- * Surname: Recording
- User Password: [Empty field]
- Confirm Password: [Empty field]
- Admin Note: [Empty field]
- Avaya Role: None
- Business Category: [Empty field]
- Car License: [Empty field]
- CM Home: [Empty field]
- Css Home: [Empty field]
- CT User: Yes
- Department Number: [Empty field]

6.5. Enable Unrestricted Access for the Recite User

If the Security Database (SDB) is enabled on Application Enablement Services, set the Recite 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 **Numonix** 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.

The screenshot displays the 'Edit CTI User' web interface. The breadcrumb navigation at the top reads 'Security | Security Database | CTI Users | List All Users'. The left sidebar contains a tree view with categories: 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, Devices, Device Groups, Tlinks, Tlink Groups, and Worktops. The 'List All Users' item is selected. The main content area is titled 'Edit CTI User' and shows the configuration for the 'Numonix' user. The 'User Profile' section includes fields for 'User ID', 'Common Name', 'Worktop Name', and 'Unrestricted Access' (checked). The 'Call and Device Control' section has a dropdown for 'Call Origination/Termination and Device Status' set to 'None'. The 'Call and Device Monitoring' section has dropdowns for 'Device Monitoring' and 'Calls On A Device Monitoring' set to 'None', and an unchecked checkbox for 'Call Monitoring'. The 'Routing Control' section has a dropdown for 'Allow Routing on Listed Devices' set to 'None'. At the bottom are 'Apply Changes' and 'Cancel Changes' buttons.

Edit CTI User		
User Profile:		
User ID	Numonix	
Common Name	Numonix	
Worktop Name	NONE	
Unrestricted Access	<input checked="" type="checkbox"/>	
<hr/>		
Call and Device Control:	Call Origination/Termination and Device Status	None
<hr/>		
Call and Device Monitoring:	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	<input type="checkbox"/>
<hr/>		
Routing Control:	Allow Routing on Listed Devices	None
<hr/>		
<input type="button" value="Apply Changes"/> <input type="button" value="Cancel Changes"/>		

6.6. Confirm TSAPI and DMCC Licenses

Recite 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.

With version 7 and later, WebLM is typically installed and configured on 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**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "cust" with system details. A red navigation bar contains "Maintenance | Service Controller" and links for "Home | Help | Logout". The left sidebar lists various service categories, with "Maintenance" expanded to show "Service Controller" as the active selection. The main content area, titled "Service Controller", features a table of services and their statuses. The "TSAPI Service" is highlighted with a blue checkmark and is in a "Running" state. Below the table, there is a note about using "Status and Control" for actual services, followed by a row of action buttons: "Start", "Stop", "Restart Service", "Restart AE Server", "Restart Linux", and "Restart Web Server".

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

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

[Start](#) [Stop](#) [Restart Service](#) [Restart AE Server](#) [Restart Linux](#) [Restart Web Server](#)

7. Configure Numonix Recite

Numonix installers will perform most of the initial configuration of the system, some of the steps to enable connectivity to Communication Manager and AES are described below. Note that most of the configuration settings are contained in the *CTILinkService.app.config* XML file on the Recite server. Most other tasks are performed using a web browser.

7.1. Configure Extensions, ACD Queues and Agents

Click on the gear icon in the upper right of the web interface, choose Extensions, then click Add (not shown) to create stations to be recorded.

The screenshot displays the Numonix Recite web interface. The top navigation bar includes 'Calls', 'Quality Control', and 'Reports' tabs. The user is logged in as 'Numonix Admin'. The main content area is titled 'Extension Detail' and contains the following fields:

Extension Number*	30001	Extension Type	STATION
Physical Device ID		Physical Device Type	STATION
Link ID		Description	
Allocated User	Unallocated	Status	Active
Connection Type	Dynamic	Restricted	<input type="checkbox"/> Calls for extension cannot be accessed without password
Server	127.0.0.1:7500	Connection	Open: 'True' Result: 'SUCCESS'
Created on	1/10/2018 1:23:41 PM	Modified on	6/19/2019 11:41:26 AM by Numonix Admin.

At the bottom of the form are 'Save' and 'Cancel' buttons. A sidebar on the left provides instructions on how to use the extension configuration fields.

Repeat for all stations and confirm in the list shown below.

Extension	Type	Physical Device	Device Type	Link ID	Dynamic	Description	User	Status	Action
30001	STA		STA		✓		Unallocated	Active	Edit Delete
30002	STA		STA		✓	30002	Unallocated	Active	Edit Delete
30004	STA		STA		✓		Unallocated	Active	Edit Delete
30005	STA		STA		✓		Unallocated	Active	Edit Delete
31000	ACD		STA		✓	ACD Number	Unallocated	Active	Edit Delete

ACD Queues are configured as extensions, with an **ACDGROUP** Type:

Extension Detail

Please use the fields on the right to edit an existing extension configuration, or to add a new extension to the system. Please note, all fields marked with an asterisk are compulsory, and changes will reflect immediately.

Extension Number*	31000	Extension Type	ACDGROUP
Physical Device ID		Physical Device Type	STATION
Link ID		Description	ACD Number
Allocated User	Unallocated	Status	Active
Connection Type	Dynamic	Restricted	<input type="checkbox"/> Calls for extension cannot be accessed without password
Server	127.0.0.1:7500	Connection	Open: 'True' Result: 'SUCCESS'
Created on	1/12/2018 4:26:16 PM	Modified on	6/18/2019 6:32:47 PM by Numonix Admin.

[Save](#) [Cancel](#)

Users are created similarly and can be configured to allow playback of calls for specific extensions.

The screenshot displays the RECITE user management interface. The top navigation bar includes 'Calls', 'Quality Control', and 'Reports'. The user is logged in as 'Numonix Admin'. The main content area is titled 'Users' and contains a table of user records. On the left, there is a 'Search for Users' sidebar with filters for Email Address, Extension, and Name, along with a 'Hide disabled Users' checkbox and 'Add New Users' buttons.

First Name	Last Name	Email Address	Domain Account	Extension	Status	Action
Numonix	Admin	admin	numonix\admin	???	Active	Edit Delete Call
Test	User 30001	30001@sil.lab	sil.lab\30001	No Extension	Active	Edit Delete Call
Test	User 30002	30002@sil.lab	sil.lab\30002	No Extension	Active	Edit Delete Call
Test	User 30003	30003@sil.lab	sil.lab\30003	No Extension	Active	Edit Delete Call
Test	User 30004	30004@sil.lab	sil.lab\30004	No Extension	Active	Edit Delete Call
Test	User 30005	30005@sil.lab	sil.lab\30005	No Extension	Active	Edit Delete Call
Test	User 30006	30006@sil.lab	sil.lab\30006	No Extension	Active	Edit Delete Call
ACD	User 32001	32001@sil.lab	sil.lab\32001	No Extension	Active	Edit Delete Call
ACD	User 32002	32002@sil.lab	sil.lab\32002	No Extension	Active	Edit Delete Call
ACD	User 32003	32003@sil.lab	sil.lab\32003	No	Active	Edit Delete Call

Similarly, agents are created:

The screenshot displays the RECITE user management interface. The top navigation bar includes 'Calls', 'Quality Control', and 'Reports'. The user is logged in as 'Numonix Admin'. The main content area is titled 'Add/Update User' and contains a form with the following fields:

- Account Info:** Avatar (Browse... button, 150px x 150px), First Name* (ACD), Last Name* (User 32001), Work Telephone, Agent ID (32001), Fax Number, Status (Active dropdown), Assigned Extensions (checkboxes for N/A, 30001, 30002, 30004, 30005), Created on (1/13/2018 2:30:39 AM).
- Security:** Password* (masked), Email Address* (32001@sil.lab), Domain User* (sil.lab\32001), Mobile Telephone, Restrict to DID.
- Quality Control:** (Empty field)

At the bottom of the form are 'Save' and 'Cancel' buttons. The 'Created on' and 'Modified on' (8/8/2019 2:24:15 PM by Numonix Admin) timestamps are displayed.

7.2. Configure Recite for Avaya Aura® Application Enablement Services Device Registrations

In the web interface, create a new “Registration” Group containing all targeted users.

Note: Confirm all Users’ extensions are associated with their profile before adding the User to the Registration Group.

The screenshot displays the 'Security' section of the Avaya Aura web interface, specifically the 'Groups' configuration page. On the left, a sidebar contains links for 'Roles', 'Permissions', 'Groups', 'Viewable Groups', and 'Widgets'. The main area shows a table of existing groups, with the 'Registration' group highlighted in blue. To the right, there are two panels: 'Available Users' and 'Available Roles'. The 'Available Users' panel lists various users, including Numonix Admin, Unknown, Test User 30001-30006, and ACD User 32001-32004. The 'Available Roles' panel lists roles such as Guest, Administrator, Agent, QC Supervisor, Supervisor, System Admin, Senior Supervisor, Super Administrator, and Junior Supervisor.

Name	Retention Interval	Retention Value	Ti	AD Mapped Group/Criteria
Unallocated		0		
Sales		0		
Support		0		
Engineering		0		
Administration		0		
Registration		0		

Available Users:

- Numonix Admin
- Unknown
- Test User 30001
- Test User 30002
- Test User 30003
- Test User 30004
- Test User 30005
- Test User 30006
- ACD User 32001
- ACD User 32002
- ACD User 32003
- ACD User 32004

Available Roles:

- Guest
- Administrator
- Agent
- QC Supervisor
- Supervisor
- System Admin
- Senior Supervisor
- Super Administrator
- Junior Supervisor

Configure this Registration Group in CTILink under “RegistrationGroupName” in the file *CTILinkService.app.config* on the Recite server. This XML file is where all of the connection settings are configured as well.

```
<MaxConcurrentCommandOperations Value="3" />
<CommandOperationTimeout Value="5" />
<CommandOperationRetryCount Value="2" />
</AsyncCommandProvider>
<DomainRequired Value="true" />
<RemotePartyHeaderName Value="" />
<NormalizePhoneNumber Value="true" />
<EnableNATMapping Value="false" />
<ExtensionRecordingOptions Value="Any" />
<ApplicationInstanceID Value="" />
<Priority Value="1" />
<MessageCredentialType Value="Windows" />
<EnableTargetActivationTimer Value="true" />
<EnableAutoStopReplacedCalls Value="false" />
<CertificateName Value="Avaya" />
<CMSwitchName Value="SILDVCM8" />
<CMSwitchAddress Value="10.64.115.25" />
<UseSSL Value="true" />
<AppName Value="Recite" />
<VersionNumeric Value="8.0.1" />
<Version Value="http://www.ecma-international.org/standards/ecma-323/csta/ed3/privC" />
<DeviceInstance Value="2" />
<DependencyMode Value="1" />
<EnableRegistration Value="true" />
<EnableNATAutoMapping Value="false" />
<ExcludePayloadTypes Value="" />
<SupportedCodecs Value="g711U,g711A,g729A,g726A,g723" />
<SupportedEncryptionModes Value="srtp-aescm128-hmac80,none" />
<RegistrationGroupName Value="Registration" />
<EnableMetaDataMap Value="false" />
<ExcludeAudioPayloadTypes Value="G7221/32000:bitrate=48000,SIREN14/16000:bitrate=48000" />
<ExcludePayloadFormatDetails Value="true" />
<EnableDeviceSnapshot Value="false" />
<ResetTargetOnActivationTimeout Value="false" />
<TargetHeartbeatTimeout Value="3900" />
<ScreenRecordGroupName Value="ScreenRecord" />
</Link001>
```

7.3. Set Agent passwords

Create a new “Registration User” and make this user a “Group Viewer” of the Registrations Group in Step 1 and member of the Registrations groups.

The screenshot shows the 'Add/Update User' dialog box with the 'Quality Control' tab selected. The 'Groups' list on the left has 'Registration' selected. The 'Roles' list on the right has 'Registration' selected. The 'Viewable Extensions' and 'Viewable Groups' lists are also visible, both with 'Registration' selected. The 'Save' and 'Cancel' buttons are at the bottom.

Add/Update User
Please use the fields on the right to edit current user details or to add a new user to the system. Please note, all fields marked with an asterisk are compulsory.

Account Info **Security** **Quality Control**

Groups

- ☐ Administration
- ☐ Engineering
- ☒ Registration
- ☐ Sales
- ☐ Support

Viewable Extensions
select all/none

- ☐ 30001
- ☐ 30002
- ☐ 30004
- ☐ 30005
- ☐ 31000

Roles

- ☐ Guest
- ☐ Administrator
- ☐ Agent
- ☐ QC Supervisor
- ☐ Supervisor

Viewable Groups
select all/none

- ☐ Administration
- ☐ Engineering
- ☒ Registration
- ☐ Sales
- ☐ Support

Save **Cancel**

The password for the Registration User must match the registration password for every extension.

The screenshot shows the 'Add/Update User' dialog box with the 'Account Info' tab selected. The 'First Name' field is 'Test', 'Last Name' is 'User 30001', 'Email Address' is '30001@sil.lab', and 'Domain User' is 'sil.lab\30001'. The 'Status' is 'Active'. The 'Assigned Extensions' list has '30001' selected. The 'Avatar' field has a 'Browse...' button. The 'Password' field is masked with dots.

Add/Update User
Please use the fields on the right to edit current user details or to add a new user to the system. Please note, all fields marked with an asterisk are compulsory.

Account Info **Security** **Quality Control**

Avatar **Browse...** 150px x 150px

First Name* Test

Last Name* User 30001

Work Telephone

Agent ID

Fax Number

Status Active

Assigned Extensions
select all/none

- ☐ N/A
- ☒ 30001
- ☐ 30002
- ☐ 30004
- ☐ 30005

Password*

Email Address* 30001@sil.lab

Domain User* sil.lab\30001

Mobile Telephone

Restrict to DID

Security

Roles
Permissions
Groups
Viewable Groups
Widgets

Viewable Groups

Name
Unallocated
Sales
Support
Engineering
Administration
Registration

Available Users

Numonix Admin
Unknown
Test User 30001
Test User 30002
Test User 30003
Test User 30004
Test User 30005
Test User 30006
ACD User 32001
ACD User 32002
ACD User 32003
ACD User 32004

7.4. Configure Recite for Free Seating

Base Device Extensions should be entered as STA type devices.

Extension	Type	Physical Device	Device Type	Link ID	Dynamic	Description	User	Status	Action
30001	STA		STA		✓		Unallocated	Active	✎ 🗑
30002	STA		STA		✓	30002	Unallocated	Active	✎ 🗑

Each skill group number should be entered as an ACD type device.

Extension	Type	Physical Device	Device Type	Link ID	Dynamic	Description	User	Status	Action
31000	ACD		STA		✓	ACD Number	Unallocated	Active	✎ 🗑

The PBX AgentID/AgentPIN number must be entered in the associated User form in the **Agent ID** input box.

With the above configured, the user with correlating agent ID in their profile will be associated with the extension.

If the Avaya environment is not running the Avaya EAS (Expert Agent Selection) then the above config will be invalid for the site and free seating will not be supported. In this case the base extensions will be loaded as STA devices and assigned directly to the user.

The property setting “EnableDeviceSnapshot” is a Link level property and should be set to “false” when Avaya EAS is not enabled, this is set in the file *CTILinkService.app.config*.

```
<CommandOperationTimeout Value="5" />
<CommandOperationRetryCount Value="2" />
</AsyncCommandProvider>
<DomainRequired Value="true" />
<RemotePartyHeaderName Value="" />
<NormalizePhoneNumber Value="true" />
<EnableNATMapping Value="false" />
<ExtensionRecordingOptions Value="Any" />
<ApplicationInstanceID Value="" />
<Priority Value="1" />
<MessageCredentialType Value="Windows" />
<EnableTargetActivationTimer Value="true" />
<EnableAutoStopReplacedCalls Value="false" />
<CertificateName Value="Avaya" />
<CMSwitchName Value="SILDVCM8" />
<CMSwitchAddress Value="10.64.115.25" />
<UseSSL Value="true" />
<AppName Value="Recite" />
<VersionNumeric Value="8.0.1" />
<Version Value="http://www.ecma-international.org/standards/ecma-323/csta/ed3/privC" />
<DeviceInstance Value="2" />
<DependencyMode Value="1" />
<EnableRegistration Value="true" />
<EnableNATAutoMapping Value="false" />
<ExcludePayloadTypes Value="" />
<SupportedCodecs Value="g711U,g711A,g729A,g726A,g723" />
<SupportedEncryptionModes Value="srtp-aescm128-hmac80,none" />
<RegistrationGroupName Value="Registration" />
<EnableMetaDataMap Value="false" />
<ExcludeAudioPayloadTypes Value="G7221/32000:bitrate=48000,SIREN14/16000:bitrate=48000" />
<ExcludePayloadFormatDetails Value="true" />
<EnableDeviceSnapshot Value="false" />
<ResetTargetOnActivationTimeout Value="false" />
<TargetHeartbeatTimeout Value="3900" />
<ScreenRecordGroupName Value="ScreenRecord" />
</Link001>
```

8. Verification Steps

This section describes various methods for verifying aspects of the solution.

8.1. Communication Manager

On Communication Manager, use the **status station** command to verify the application has registered to the agent's stations. The first screenshot is a SIP_CC device.

status station 30001		Page 6 of 7	
IP ENDPOINT DATA			
Port: S00011			
Product ID-Release:		H.245 Tunneled? does not apply	
Registration Status: unregistered		MAC Address:	
Native NAT Address:			
ALG NAT WAN Address:			
Shared Port: S00012		Shd Signal Status: connected	
Product ID-Release: IP_API_A 3.2040		H.245 Tunneled? does not apply	
Registration Status: registered-authenticated		MAC Address: unavailable	
Authentication Type: DES-56-plus		Dependency Mode: independent	
Native NAT Address: not applicable			
ALG NAT WAN Address: not applicable			

With an active call on a H.323 station, the IP station (10.64.115.36) is registered to Communication Manager (10.64.115.25), and the shared port connection is with AES (10.64.115.28):

status station 30002		Page 4 of 10	
CALL CONTROL SIGNALING			
Port: S00005	Switch-End IP Signaling Loc: PROCR		H.245 Port:
IP Address	Port	Node Name	Rgn
Switch-End: 10.64.115.25	61441	procr	1
Reg Set End:10.64.115.36	1720		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:10.64.115.25	61441	procr	1
Reg Set End:10.64.115.28	23097	sildvaes8	2

The audio connections show the station connected with the G430, and AES:

status station 30002

Page 5 of 10

AUDIO CHANNEL Port: S00005

G.729A Switch-End Audio Location: MG1

IP Address	Port	Node Name	Rgn
Other-End: 10.64.115.2	2058	sildvmg1	1
Set-End: 10.64.115.36	2982		1

Audio Connection Type: ip-tdm

AUDIO CHANNEL Shared Port: S00003

G.729A Switch-End Audio Location: MG1

IP Address	Port	Node Name	Rgn
Other-End: 10.64.115.2	2056	sildvmg1	1
Set-End: 10.64.115.28	20000	sildvaes8	2

Audio Connection Type: ip-tdm

status station 30002

Page 6 of 7

IP ENDPOINT DATA

Port: S00005

Product ID-Release: IP_Phone 6.6506 H.245 Tunneled? does not apply

Registration Status: registered-authenticated MAC Address: 50:cd:22:b2:62:42

Authentication Type: DES-56-plus Dependency Mode: main

Native NAT Address: not applicable

ALG NAT WAN Address: not applicable

Shared Port: S00003 Shd Signal Status: connected

Product ID-Release: IP_API_A 3.2040 H.245 Tunneled? does not apply

Registration Status: registered-authenticated MAC Address: unavailable

Authentication Type: DES-56-plus Dependency Mode: independent

Native NAT Address: not applicable

ALG NAT WAN Address: not applicable

With an active call, use **status station** on H.323 and DCP stations, or status trunk port x for SIP stations to view audio connection status. In the below screenshot, this verifies the SRTP media connection between the Recite recorder (10.64.115.30) and the gateway.

status station 30002		Page 8 of 10	
SRC PORT TO DEST PORT TALKPATH			
src port: S00005			
S00005:TX:10.64.115.36:2982/g729a/20ms/1-srtp-aescm128-hmac80			
001V011:RX:10.64.115.2:2058/g729/20ms/1-srtp-aescm128-hmac80:TX:ctxID:275			
001V011:RX:ctxID:275:TX:10.64.115.2:2056/g729/20ms/1-srtp-aescm128-hmac80			
S00003:RX:10.64.115.32:20000/g729a/20ms/1-srtp-aescm128-hmac80			
status station 30002		Page 9 of 10	
SRC PORT TO DEST PORT TALKPATH			
src port: S00005			
S00005:TX:10.64.115.36:2982/g729a/20ms/1-srtp-aescm128-hmac80			
001V011:RX:10.64.115.2:2058/g729/20ms/1-srtp-aescm128-hmac80:TX:ctxID:275			
001V011:RX:ctxID:275:TX:10.64.115.2:2060/g729/20ms/1-srtp-aescm128-hmac80			
T00001:RX:10.64.115.30:5004/g729/20ms/1-srtp-aescm128-hmac80			


Use the **list monitored-station** command to verify ASAI associations to provide TSAPI events and control to the application:

```
list monitored-station
```

MONITORED STATION										
Associations:	1	2	3	4	5	6	7	8		
	CTI	CTI	CTI	CTI	CTI	CTI	CTI	CTI		
Station Ext	Lnk CRV	Lnk CRV	Lnk CRV	Lnk CRV	Lnk CRV	Lnk CRV	Lnk CRV	Lnk CRV	Lnk CRV	Lnk CRV
30001	1	0001								
30002	1	0006								
30003	1	000C								
30004	1	0005								
30005	1	0009								

8.2. Avaya Aura® Application Enablement Services

On the AES, navigate to **Status → Status and Control → DMCC Service Summary** to verify Recite is connected using an encrypted session:



Application Enablement Services
Management Console

Welcome: User cust
Last login: Tue Jun 18 13:35:06 2019 from 10.64.10.210
Number of prior failed login attempts: 0
HostName/IP: sildvaes8.sildenvr.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.1.0.3.5-0
Server Date and Time: Tue Aug 13 09:27:25 MDT 2019
HA Status: Not Configured

Status | Status and Control | **DMCC Service Summary**
Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Status
Alarm Viewer
Logs
Log Manager
Status and Control
CVLAN Service Summary
DLG Services Summary
DMCC Service Summary
Switch Conn Summary
TSAPI Service Summary

DMCC Service Summary - Session Summary
Please do not use back button
☐ Enable page refresh every 60 seconds
Session Summary [Device Summary](#)
Generated on Tue Aug 13 09:27:15 MDT 2019
Service Uptime: 55 days, 22 hours 26 minutes
Number of Active Sessions: 1
Number of Sessions Created Since Service Boot: 26
Number of Existing Devices: 5
Number of Devices Created Since Service Boot: 54

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	14B3CACC6E21DDAF3 9BEE3DC20AAA0BB-657	avaya	Recite	10.64.115.32	XML Encrypted	5

Item 1-1 of 1
1 Go

Click on the **Device Summary** link to view the registrations:

Application Enablement Services

Management Console

Welcome: User cust
Last login: Tue Jun 18 13:35:06 2019 from 10.64.10.210
Number of prior failed login attempts: 0
HostName/IP: sildvaes8.sildenver.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.1.0.3.5-0
Server Date and Time: Tue Aug 13 09:28:12 MDT 2019
HA Status: Not Configured

[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
 - User Management

DMCC Service Summary - Device Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary Device Summary
Generated on Tue Aug 13 09:28:07 MDT 2019

Service Uptime: 55 days, 22 hours and 26 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 26

Number of Existing Devices: 5

Number of Devices Created Since Service Boot: 54

	Device ID	Gatekeeper IP address	State	Associated Sessions
<input type="checkbox"/>	30001:SILDVCM8:10.64.115.25:2	10.64.115.25	REGISTERED	1
<input type="checkbox"/>	30002:SILDVCM8:10.64.115.25:2	10.64.115.25	REGISTERED	1
<input type="checkbox"/>	30004:SILDVCM8:10.64.115.25:2	10.64.115.25	REGISTERED	1
<input type="checkbox"/>	30005:SILDVCM8:10.64.115.25:2	10.64.115.25	REGISTERED	1
<input type="checkbox"/>	31000:SILDVCM8:10.64.115.25:2	N/A	IDLE	1

[Terminate Devices](#)

8.3. Numonix Recite

On the Recite server, the following applet will show the current connected status of the recorder when lights are green (when a channel is actively recording, it will turn red):

Recite Recorder -- License: SUBSCRIPTION Duration: 336 EndDate: 7/15/2020

File Edit Tools Actions Help

NL-3024V
N-Link

Link
Act

Power Console

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32
33	35	37	39	41	43	45	47	49	51	53	55	57	59	61	63
34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64

Recorder Module

Connected to server '10.64.115.32:8500' SUCCESS at '11:43:41 AM' 001 / 064 11:52:19

RECITE
Calls 📞
Quality Control 🔧
Reports 📊
Logged in as: Numonix Admin

Filter Calls

From
3/1/2019 12:00 AM

To
8/8/2019 11:59 PM

Filter

Call Listing

Search by Catalog Index

Secure	Start Time	Duration	Direction	Flag	Extension	Agent	Caller Number	Caller Name
<input type="checkbox"/>	6/15/2019 12:07:39 AM	3m 9s	In		30004	Unknown	15613682948	
<input type="checkbox"/>	6/15/2019 12:07:29 AM	0m 10s	In		30004	Unknown	30002	
<input type="checkbox"/>	6/15/2019 12:06:43 AM	0m 46s	In		30002	Unknown	15613682948	
<input type="checkbox"/>	6/15/2019 12:05:12 AM	0m 7s	Out		30004	Unknown	Unknown	
<input type="checkbox"/>	6/15/2019 12:05:04 AM	0m 7s	In		30004	Unknown	15613682948	
<input type="checkbox"/>	6/15/2019 12:04:54 AM	0m 10s	In		30004	Unknown	30002	
<input type="checkbox"/>	6/15/2019 12:03:16 AM	1m 37s	In		30002	Unknown	15613682948	
<input type="checkbox"/>	6/15/2019 12:03:06 AM	0m 10s	In		30002	Unknown	15613682948	
<input checked="" type="checkbox"/>	6/15/2019 12:02:08 AM	0m 13s	Out		30004	Unknown	Unknown	
<input type="checkbox"/>	6/15/2019 12:02:03 AM	0m 5s	Out		30004	Unknown	Unknown	
<input type="checkbox"/>	6/15/2019 12:01:53 AM	0m 9s	In		30004	Unknown	30002	
<input checked="" type="checkbox"/>	6/15/2019 12:00:56 AM	0m 56s	In		30002	Unknown	15613682948	
<input type="checkbox"/>	6/15/2019 12:00:46 AM	0m 9s	In		30002	Unknown	15613682948	
<input type="checkbox"/>	6/10/2019 6:02:17 PM	0m 14s	Out		30004	Unknown	30004	
<input type="checkbox"/>	6/10/2019 5:57:15 PM	0m 13s	In		30004	Unknown	30002	
<input type="checkbox"/>	6/10/2019 5:57:01 PM	0m 14s	In		30004	Unknown	30002	

Existing Filters

- Show Matched Calls (True)
- Show Unmatched Calls (True)

Saved Searches

RECITE
Calls 📞
Quality Control 🔧
Reports 📊
Logged in as: Numonix Admin

Filter Calls

From
3/1/2019 12:00 AM

To
8/8/2019 11:59 PM

Filter

Call Listing

Search by Catalog Index

Secure	Start Time	Duration	Direction	Flag	Extension	Agent	Caller Number	Caller Name
<input type="checkbox"/>	6/15/2019 12:07:39 AM	3m 9s	In		30004	Unknown	15613682948	
<input type="checkbox"/>	6/15/2019 12:07:29 AM	0m 10s	In		30004	Unknown	30002	
<input type="checkbox"/>	6/15/2019 12:06:43 AM	0m 46s	In		30002	Unknown	15613682948	
<input type="checkbox"/>	6/15/2019 12:05:12 AM	0m 7s	Out		30004	Unknown	Unknown	
<input type="checkbox"/>	6/15/2019 12:05:04 AM	0m 7s	In		30004	Unknown	15613682948	
<input type="checkbox"/>	6/15/2019 12:04:54 AM	0m 10s	In		30004	Unknown	30002	
<input type="checkbox"/>	6/15/2019 12:03:16 AM	1m 37s	In		30002	Unknown	15613682948	
<input type="checkbox"/>	6/15/2019 12:03:06 AM	0m 10s	In		30002	Unknown	15613682948	
<input checked="" type="checkbox"/>	6/15/2019 12:02:08 AM	0m 13s	Out		30004	Unknown	Unknown	
<input type="checkbox"/>	6/15/2019 12:02:03 AM	0m 5s	Out		30004	Unknown	Unknown	
<input type="checkbox"/>	6/15/2019 12:01:53 AM	0m 9s	In		30004	Unknown	30002	
<input checked="" type="checkbox"/>	6/15/2019 12:00:56 AM	0m 56s	In		30002	Unknown	15613682948	
<input type="checkbox"/>	6/15/2019 12:00:46 AM	0m 9s	In		30002	Unknown	15613682948	
<input type="checkbox"/>	6/10/2019 6:02:17 PM	0m 14s	Out		30004	Unknown	30004	
<input type="checkbox"/>	6/10/2019 5:57:15 PM	0m 13s	In		30004	Unknown	30002	
<input type="checkbox"/>	6/10/2019 5:57:01 PM	0m 14s	In		30004	Unknown	30002	

Existing Filters

- Show Matched Calls (True)
- Show Unmatched Calls (True)

Saved Searches

Details about event data will appear in the **Trace Viewer** applet on the Recite server as shown below, this can be useful to see events in real-time:

```

Trace Viewer
08/08/19 14:34:21.794 : CTILINK : 04 : ProcessCallInfoAction() Key 'CallIndex', Value '30002'
08/08/19 14:34:21.794 : CTILINK : 05 : BaseDevice.CallInfo() Device = 'STA:30002'
08/08/19 14:34:21.794 : CTILINK : 05 : BaseDevice.HandleActionResult() Device = 'STA:30002'
08/08/19 14:34:21.794 : CTILINK : 03 : SwitchItem.SwitchItem.ActionReceived()
08/08/19 14:34:21.794 : CTILINK : 03 : ProcessCallDataAction() FieldCount '13'
08/08/19 14:34:21.794 : CTILINK : 03 : ActionProcessor.ProcessCallDataAction() Device: 'STA:30002', Connection 30002
08/08/19 14:34:21.794 : CTILINK : 05 : ActionProcessor.ProcessCallDataAction() Device: 'STA:30002', Key 'LinkID', Val
08/08/19 14:34:21.794 : CTILINK : 05 : ActionProcessor.ProcessCallDataAction() Device: 'STA:30002', Key 'Gateway', Ua
08/08/19 14:34:21.794 : CTILINK : 05 : ActionProcessor.ProcessCallDataAction() Device: 'STA:30002', Key 'AuxCallIndex
08/08/19 14:34:21.794 : CTILINK : 05 : ActionProcessor.ProcessCallDataAction() Device: 'STA:30002', Key 'PrimaryCallI
08/08/19 14:34:21.794 : CTILINK : 05 : ActionProcessor.ProcessCallDataAction() Device: 'STA:30002', Key 'Station', Ua
08/08/19 14:34:21.794 : CTILINK : 05 : ActionProcessor.ProcessCallDataAction() Device: 'STA:30002', Key 'StationType'
08/08/19 14:34:21.794 : CTILINK : 05 : ActionProcessor.ProcessCallDataAction() Device: 'STA:30002', Key 'AnsweringDev
08/08/19 14:34:21.794 : CTILINK : 05 : ActionProcessor.ProcessCallDataAction() Device: 'STA:30002', Key 'CallerNumber
08/08/19 14:34:21.794 : CTILINK : 05 : ActionProcessor.ProcessCallDataAction() Device: 'STA:30002', Key 'CalledNumber
08/08/19 14:34:21.794 : CTILINK : 05 : ActionProcessor.ProcessCallDataAction() Device: 'STA:30002', Key 'DialNumber
08/08/19 14:34:21.794 : CTILINK : 05 : ActionProcessor.ProcessCallDataAction() Device: 'STA:30002', Key 'GloballyUniq
08/08/19 14:34:21.794 : CTILINK : 05 : ActionProcessor.ProcessCallDataAction() Device: 'STA:30002', Key 'CallDirectio
08/08/19 14:34:21.810 : CTILINK : 05 : BaseDevice.CallData() Device = 'STA:30002'
  
```

9. Conclusion

These Application Notes describe the configuration steps required for Numonix Recite to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services to record audio calls. Recite passed all compliance test cases successfully, please refer to **Section 2.2** for results and any observations.

10. Additional References

This section references the product documentation relevant to these Application Notes. Product documentation for Avaya products may be found at <http://support.avaya.com>.

Avaya:

1. *Administering Avaya Aura® Communication Manager*, Release 8.0.x Issue 4, May 2019
2. *Administering Avaya Aura® Application Enablement Services*, Release 8.0.x Issue 3, August 2019

©2019 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.