



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Retia ReDat eXperience with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using Single Step Conference (SSC) and Selective Listening Hold (SLH) - Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning Retia ReDat eXperience with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services Using Single Step Conference and Selective Listening Hold.

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

1. Introduction

These Application Notes describe the configuration used to enable the Retia ReDat eXperience to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. The Retia ReDat eXperience offers various methods of voice recording. For the purpose of the tests described by these Application Notes, the Single Step Conference recording method was used. Two virtual extensions (recorders) are added to the call and SLH is applied to obtain separate outbound and inbound voices. The call record is then saved in the stereo format. ReDat Retia eXperience can be configured to monitor specific local endpoints, and record calls made to or from those endpoints. Calls between or among local endpoints which are each monitored produce multiple voice files: one for each monitored endpoint.

2. General Test Approach and Test results

The compliance testing done between Retia ReDat eXperience (ReDat) and Avaya Aura® Communication Manager (Communication Manager) was performed manually. The tests were all functional in nature, and no performance testing was done. The test method employed can be described as follows:

- The Communication Manager was configured to support various local IP telephones, as well as a connection to the PSTN
- An E1 PSTN interface was attached to Communication Manager via an Avaya G430 Gateway
- The ReDat was configured to monitor various telephones attached to Communication Manager
- The major ReDat features and functions were verified using the above-mentioned local and external telephones, including the ability to record calls made to and from:
 - Locally attached IP and digital telephones
 - Trunk calls to/from the PSTN via the E1 trunk
 - Trunk calls to/from the PSTN via a SIP Trunk

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 the ReDat eXperience did not include use of any specific encryption features as requested by Retia.

2.1. Interoperability Compliance Testing

The following tests were performed as part of the compliance testing:

- Basic call
- Hold/ Resume
- Consultative transfer/Blind transfer
- Conferencing
- Hunt group calls
- Calls to/from bridged appearances
- ReDat's robustness was tested by verifying its ability to recover from interruptions to its external connections including:
 - The LAN connection between ReDat and the network
 - The connection of the PBX to the network
- ReDat's robustness was further tested by verifying its ability to recover from power interruptions to the ReDat server

2.2. Test Results

Tests were performed to insure interoperability of Retia ReDat eXperience with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services (Application Enablement Services). All the test cases passed successfully.

2.3. Support

Technical support can be obtained for Retia products as follows:

Web: <http://www.redat.eu/en/>

3. Reference Configuration

Figure 1 illustrates the network configuration used during compliance testing. The Avaya solution consists of a Communication Manager, System Manager, Session Manager, Application Enablement Services, Avaya Media Server and an Avaya G430 Media Gateway. The Communication Manager is configured to communicate with the ReDat server via the Application Enablement Services. ReDat records voice conversations from telephones attached to the Communication Manager. The TSAPI and DMCC services provided by Application Enablement Services are used to monitor call activity and capture voice streams associated with telephones attached to the Communication Manager.

When a call is to be recorded, the ReDat system uses the Single Step Conference feature to initiate monitoring for calls which it wishes to record. The voice streams (two streams for each call if stereo recording is enabled) for such calls are received via the LAN interface to the Communication Manager. The ReDat Client is configured to allow users to replay the recorded calls which are stored on the ReDat eXperience Server.

Note: There are no distinctive requirements for stations to be used by ReDat eXperience.

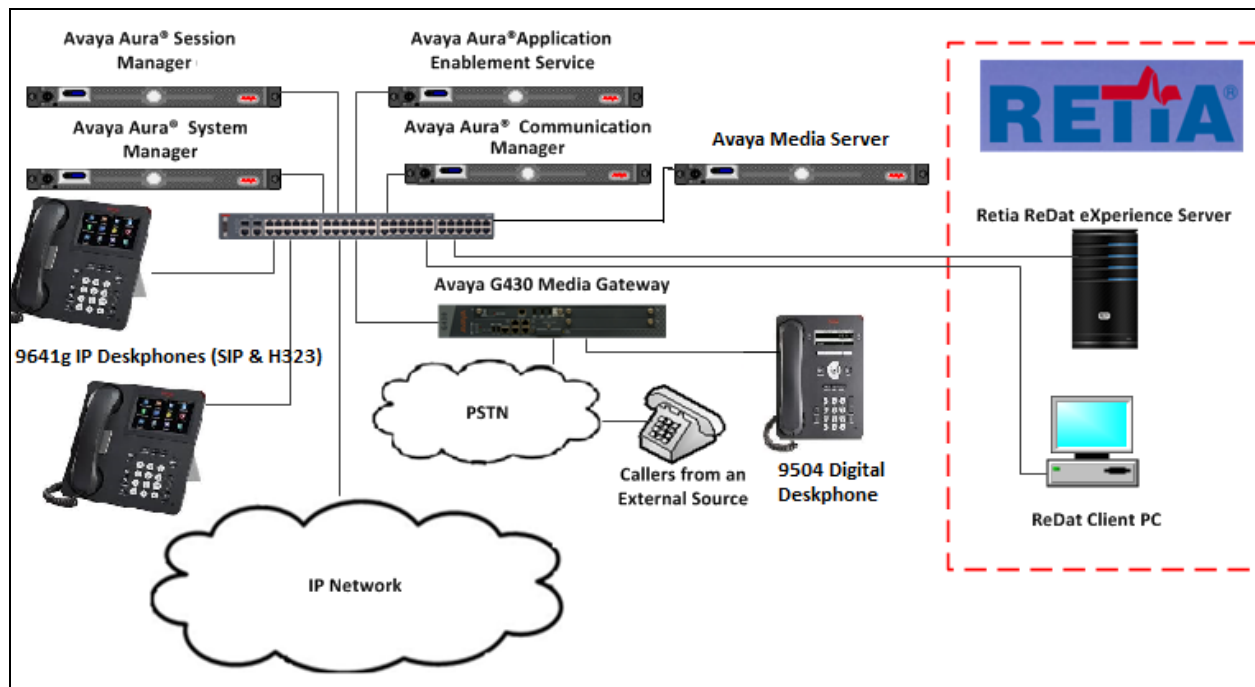


Figure 1: Avaya and Retia Reference Configuration

4. Equipment and Software Validated

The hardware and associated software used in the compliance testing is listed below.

Avaya Equipment	Software Version
Avaya Aura® Communication Manager VMware Virtual machine	R7.1.2 CM 7.1.2.0.0.532.24184 KERNEL-3.10.0-693.e17.AV1 PLAT-rhe17.2-0010
Avaya G430- Media Gateway	38.21.0/1
Avaya Aura® Application Enablement Services	R7.1.2.0.0.3-0
Avaya Media Server	v7.8.0.309
Avaya Aura® System Manager	R7.1.2.0 Build- 7.1.0.0.1125193 Update Revision – 7.1.2.0.057353 Feature Pack 2
Avaya Aura® Session Manager	7.1.2.0.712004
Avaya 9641g IP Telephone H323	6.6604
Avaya 9641g IP Telephone SIP	7.1.0.1.1
Retia Equipment	Software Version
ReDat VoIP Recorder ReDat eXperience Server running on Windows 2016 Standard Apache web server PHP MS SQL Java	v2.00 rel.47 v2.34.2 rel.062 v2.4.25 v5.6.30 SQL Server 2014 Java 8 update 144

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation as referenced in **Section 10**. The configuration operations described in this section can be summarized as follows:

- Verify System Parameters Customer Options
- Verify System Parameters Features
- Configure Service Observe
- Configure Target Stations to be Recorded
- Configure Station Button Assignments
- Configure virtual extensions for the recording pool
- Configure the Interface to AES

5.1. Verify System Parameters Customer Options

Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 3**, ensure that **Computer Telephony Adjunct Links?** is set to **y** as shown below.

display system-parameters customer-options		Page	3 of 11
OPTIONAL FEATURES			
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? n		
Access Security Gateway (ASG)? n	Authorization Codes? n		
Analog Trunk Incoming Call ID? n	CAS Branch? n		
A/D Grp/Sys List Dialing Start at 01? n	CAS Main? n		
Answer Supervision by Call Classifier? n	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? n		
ASAI Link Plus Capabilities? y	DCS with Rerouting? n		
Async. Transfer Mode (ATM) PNC? n	Digital Loss Plan Modification? n		
Async. Transfer Mode (ATM) Trunking? n	DS1 MSP? y		
ATM WAN Spare Processor? n	DS1 Echo Cancellation? y		
ATMS? n			
Attendant Vectoring? y			
(NOTE: You must logoff & login to effect the permission changes.)			

5.2. Verify System Parameters Features

On **Page 11** of the system-parameters features form, set **Allow Two Observers in Same Call?** to **y**.

change system-parameters features	Page 11 of 18
FEATURE-RELATED SYSTEM PARAMETERS	
CALL CENTER SYSTEM PARAMETERS	
EAS	
Expert Agent Selection (EAS) Enabled? y	
Minimum Agent-LoginID Password Length:	
Direct Agent Announcement Extension:	Delay:
Message Waiting Lamp Indicates Status For: station	
VECTORIZING	
Converse First Data Delay: 0	Second Data Delay: 2
Converse Signaling Tone (msec): 100	Pause (msec): 70
Reverse Star/Pound Digit For Collect Step? n	
Store VDN Name in Station's Local Call Log? n	
SERVICE OBSERVING	
Service Observing: Warning Tone? y	or Conference Tone? n
Service Observing Allowed with Exclusion? n	
Allow Two Observers in Same Call? y	

5.3. Configure Service Observe

For the purposes of Multi Registration, service observe must be enabled for the COR to which the Target Stations will be assigned. Using the command **change cor 1** set both **Can Be Service Observed?** and **Can Be A Service Observer?** to **y**.

change cor 1		Page 1 of 23
CLASS OF RESTRICTION		
COR Number: 1		
COR Description: Default		
FRL: 0		
APLT? y		
Can Be Service Observed? y		
Calling Party Restriction: none		
Can Be A Service Observer? y		
Called Party Restriction: none		
Time of Day Chart: 1		
Forced Entry of Account Codes? n		
Priority Queuing? n		
Direct Agent Calling? y		
Restriction Override: all		
Facility Access Trunk Test? n		
Restricted Call List? n		
Can Change Coverage? n		
Access to MCT? y		
Fully Restricted Service? n		
Group II Category For MFC: 7		
Hear VDN of Origin Annc.? y		
Send ANI for MFE? n		
Add/Remove Agent Skills? n		
MF ANI Prefix:		
Automatic Charge Display? n		
Hear System Music on Hold? y		
PASTE (Display PBX Data on Phone)? y		
Can Be Picked Up By Directed Call Pickup? y		
Can Use Directed Call Pickup? y		
Group Controlled Restriction: inactive		

On Page 2 set **Service Observing by Recording Device** to **y**.

change cor 1		Page 2 of 23
CLASS OF RESTRICTION		
MF Incoming Call Trace? n		
Brasil Collect Call Blocking? n		
Block Transfer Display? n		
Block Enhanced Conference/Transfer Displays? y		
Remote Logout of Agent? n		
Station Lock COR: 1		
TODSL Release Interval (hours):		
Station-Button Display of UI IE Data? n		
Service Observing by Recording Device? y		
Can Force a Work State Change? n		
Work State Change can be Forced? n		
Restrict Second Call Consult? n		

5.4. Configure Target Stations to be Recorded

Use the **add station** command to configure a station for each of the target stations to be recorded. Enter in a descriptive **Name** and **Security Code** for each one. The **Security Code** will be referenced by Quantify when setting up the recording extensions. Set the **IP Softphone?** to **y**.

add station 8237001		Page 1 of 5
STATION		
Extension: 8237001	Lock Messages? n	BCC: 0
Type: 9404	Security Code:1234	TN: 1
Port: S00040	Coverage Path 1:	COR: 1
Name: Redbox,Digital	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 2	Time of Day Lock Table:	
Data Option: none	Personalized Ringing Pattern: 1	
Speakerphone: 2-way	Message Lamp Ext: 4000	
Display Language: english	Mute Button Enabled? y	
	Expansion Module? n	
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	Remote Office Phone? n	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? y	

On **Page 2**, ensure that the **Multimedia Mode** is set to **enhanced**.

add station 4000		Page 2 of 5
STATION		
FEATURE OPTIONS		
LWC Reception: spe	Auto Select Any Idle Appearance? n	
LWC Activation? y	Coverage Msg Retrieval? y	
LWC Log External Calls? n	Auto Answer:	
none		
CDR Privacy? n	Data Restriction? n	
Redirect Notification? y	Idle Appearance Preference? n	
Per Button Ring Control? n	Bridged Idle Line Preference? n	
Bridged Call Alerting? n	Restrict Last Appearance? y	
Active Station Ringing: single		
	EMU Login Allowed? n	
H.320 Conversion? n	Per Station CPN - Send Calling Number?	
Service Link Mode: as-needed	EC500 State: enabled	
Multimedia Mode: enhanced	Audible Message Waiting? n	
MWI Served User Type:	Display Client Redirection? n	
AUDIX Name:	Select Last Used Appearance? n	
	Coverage After Forwarding? s	
	Multimedia Early Answer? n	
Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio		
Connections? y		
Emergency Location Ext: 201	Always Use? n IP Audio Hairpinning? n	

5.5. Configure Station Button Assignments

Use the **change station** command to configure the button assignments of the stations to be recorded, as required. Add the appropriate button assignments as shown on **Page 4** below. In this case there are three call appearance buttons **call-appr**. There are also buttons assigned for the call functions call-pickup, bridged appearance and call park: **call-pkup**, **brdg-appr**, **call-park**.

change station 4000		Page 4 of 5
STATION		
SITE DATA		
Room:		Headset? n
Jack:		Speaker? n
Cable:		Mounting: d
Floor:		Cord Length: 0
Building:		Set Color:
ABBREVIATED DIALING		
List1:	List2:	List3:
BUTTON ASSIGNMENTS		
1: call-appr	5: brdg-appr	B:1 E:4001
2: call-appr	6: call-park	
3: call-appr	7:	
4: call-pkup	8:	
voice-mail		

5.6. Configure virtual stations for the recording pool

Use the **add station** command to configure a station for each of the virtual stations to be used for the recorder channels. Enter in a descriptive **Name** and **Security Code** for each one. The **Security Code** will be referenced by Quantify when setting up the recording extensions. Set the **IP Softphone?** to y.

add station 8230099		Page	1 of	5
STATION				
Extension: 8230099	Lock Messages? n	BCC:	0	
Type: 9640	Security Code:1234	TN:	1	
Port: S00040	Coverage Path 1:	COR:	1	
Name: Redbox,Virtual	Coverage Path 2:	COS:	1	
	Hunt-to Station:			
STATION OPTIONS				
Loss Group: 2		Time of Day Lock Table:		
Data Option: none	Personalized Ringing Pattern: 1			
Speakerphone: 2-way	Message Lamp Ext: 4000			
Display Language: english	Mute Button Enabled? y			
	Expansion Module? n			
Survivable COR: internal	Media Complex Ext:			
Survivable Trunk Dest? y	IP SoftPhone? y			
	Remote Office Phone? n			
	IP Video Softphone? n			
	Short/Prefixed Registration Allowed: default			
	Customizable Labels? y			

5.7. Configure Interface to Avaya Aura® Application Enablement Services

In order for Communication Manager to establish a connection to Application Enablement Services, administer the CTI Link as shown below. Specify an available **Extension** number, set the **Type** as **ADJ-IP**, which denotes that this is a link to an IP connected adjunct, and name the link for easy identification, in this instance, the node-name is used.

add cti-link 1		Page	1 of	3
		CTI LINK		
CTI Link: 1				
Extension: 1111				
Type: ADJ-IP				
COR:				
1	Name: devconaes61			

Configure IP-Services for the AESVCS service using **change ip-services** command. Using the C-LAN node name as noted above i.e. **procr**

change ip-services						Page	1	of	4
IP SERVICES									
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port				
CDR1		CLAN	0	IPbuffer	9000				
CDR2		CLAN	0	RDTT	9001				
AESVCS	y	procr	8765						

Navigate to **Page 4**, set the **AE Services Server** node-name and the **Password** the AES Server will use to authenticate with Communication Manager.

change ip-services					Page	4	of	4
AE Services Administration								
Server ID	AE Services Server	Password	Enabled	Status				
1:	devconaes61	Avayapassword1	y	in use				

6. Configuration of Avaya Aura® Application Enablement Services

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

- Verify Licensing
- Create Switch Connection
- Create TSAPI link
- Create CTI User
- Enable CTI User
- Configure DMCC Port
- Enable Security Database

6.1. Verify Licensing

Access the Web License Manager used by the Application Enablement Services Server. The **Web License Manager** screen below is displayed. Select **Licensed products** → **APPL_ENAB** → **Application_Enablement** in the left pane, to display the **Licensed Features** screen in the right pane. Verify that there are sufficient licenses for **Device Media and Call Control**, as shown below. If not, consult with your Avaya Account Manager or Business Partner to acquire the proper license for your solution.

Install License

Licensed Products

APPL_ENAB

Application_Enablement

Uninstall License

Change Password

Server Properties

Manage Users

Logout

You are here: Licensed products > Application Enablement (CTI)

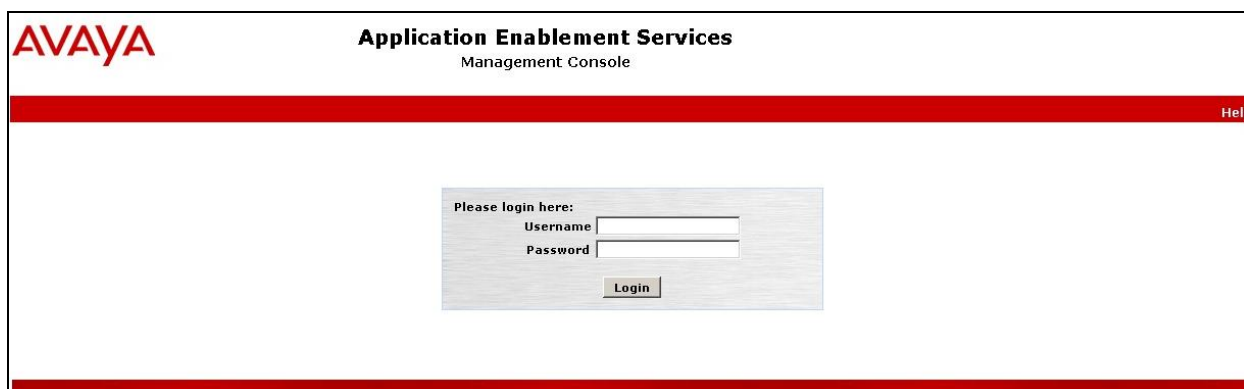
View Peak Usage

Licensed Features

Feature (Keyword)	Expiration Date	Licensed	Acquired
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	2011/11/05	100	0
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	2011/11/05	10	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	2011/11/05	10	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	2011/11/05	100	0
Product Notes (VALUE_NOTES)	2011/11/05	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP,,, CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted;	Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	2011/11/05	10	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	2011/11/05	100	0
DLG (VALUE_AES_DLG)	2011/11/05	100	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	2011/11/05	100	0
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	2011/11/05	10	0

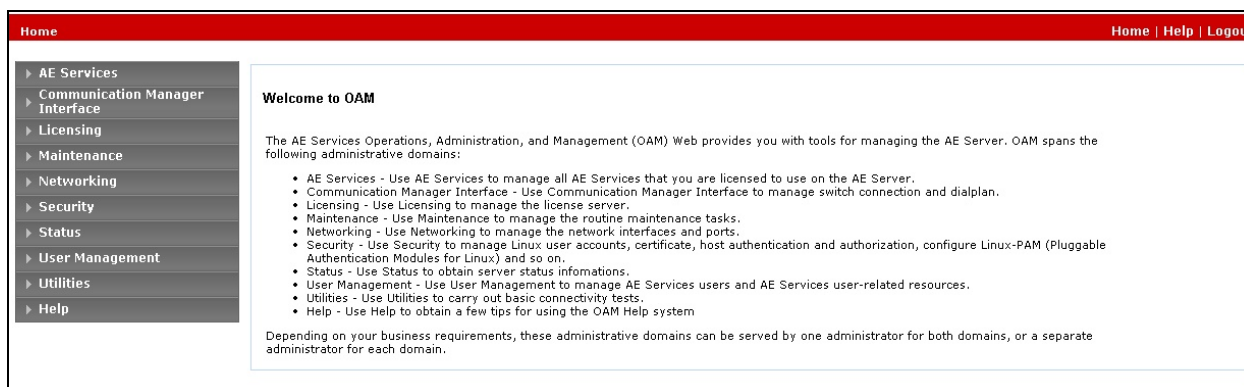
6.2. Create Switch Connection

Access the OAM web-based interface of the Application Enablement Services Server, using the URL `https://<Server_IP>`. The Management console is displayed, login using the appropriate credentials.



The screenshot shows the Avaya Application Enablement Services Management Console login page. At the top left is the Avaya logo. To its right, the text 'Application Enablement Services' is displayed in bold, with 'Management Console' underneath it. A red horizontal bar spans the width of the page, with the word 'Help' in the top right corner. In the center of the page is a login box with the text 'Please login here:'. Inside this box are two input fields: 'Username' and 'Password'. Below these fields is a 'Login' button.

The **Welcome to OAM** screen is displayed next.



The screenshot shows the 'Welcome to OAM' screen. At the top, a red horizontal bar contains the word 'Home' on the left and 'Home | Help | Logout' on the right. On the left side, there is a vertical navigation menu with the following items: 'AE Services', 'Communication Manager Interface', 'Licensing', 'Maintenance', 'Networking', 'Security', 'Status', 'User Management', 'Utilities', and 'Help'. The main content area on the right is titled 'Welcome to OAM'. It contains a paragraph: 'The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:'. This is followed by a bulleted list of domains and their functions: 'AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.', 'Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.', 'Licensing - Use Licensing to manage the license server.', 'Maintenance - Use Maintenance to manage the routine maintenance tasks.', 'Networking - Use Networking to manage the network interfaces and ports.', 'Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.', 'Status - Use Status to obtain server status informations.', 'User Management - Use User Management to manage AE Services users and AE Services user-related resources.', 'Utilities - Use Utilities to carry out basic connectivity tests.', and 'Help - Use Help to obtain a few tips for using the OAM Help system'. At the bottom of the main content area, a paragraph states: 'Depending on your business requirements, these administrative domains can be served by one administrator for both domains, or a separate administrator for each domain.'

To establish the connection between Communication Manager and the Application Enablement Services Server, click **Communication Manager Interface** → **Switch Connections**. In the field next to next to **Add Connection**, enter **CM** and click on **Add Connection**, the following screen will be displayed.

Communication Manager Interface | Switch Connections Home | Help | Logout

▶ AE Services
 ▼ Communication Manager Interface
 Switch Connections
 ▶ Dial Plan
 ▶ Licensing
 ▶ Maintenance
 ▶ Networking
 ▶ Security
 ▶ Status
 ▶ User Management
 ▶ Utilities
 ▶ Help

Connection Details - CM

Switch Password

Confirm Switch Password

Msg Period Minutes (1 - 72)

SSL ☒

Processor Ethernet ☐

Complete the configuration as shown and enter the password specified in **Section 5.7** when configuring AESVCS in ip-services. In this instance **Avayapassword1**. Click on **Apply**, the screen below will be displayed.

Communication Manager Interface | Switch Connections Home | Help | Logout

▶ AE Services
 ▼ Communication Manager Interface
 Switch Connections
 ▶ Dial Plan
 ▶ Licensing
 ▶ Maintenance
 ▶ Networking
 ▶ Security
 ▶ Status
 ▶ User Management
 ▶ Utilities
 ▶ Help

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
CM	No	30	1

Click on **Edit PE/CLAN IPs** (at the bottom of the last screenshot) in order to specify the IP address of the Communication Manager. Next to **Add Name or IP**, enter the IP address of the Communication Manager and click on **Add Name or IP**.

Communication Manager Interface | Switch Connections Home | Help | Logout

- ▶ AE Services
- ▼ Communication Manager Interface
 - Switch Connections
 - ▶ Dial Plan
 - ▶ Licensing
 - ▶ Maintenance
 - ▶ Networking
 - ▶ Security
 - ▶ Status
 - ▶ User Management
 - ▶ Utilities
 - ▶ Help

Edit CLAN IPs - CM

Name or IP Address	Status
10.10.16.23	In Use

Click on **Back** and then click on **Edit H.323 Gatekeeper**. Enter the IP address of the Communication Manager and click on **Add Name or IP**

Communication Manager Interface | Switch Connections Home | Help | Logout

- ▶ AE Services
- ▼ Communication Manager Interface
 - Switch Connections
 - ▶ Dial Plan
 - ▶ Licensing
 - ▶ Maintenance
 - ▶ Networking
 - ▶ Security
 - ▶ Status
 - ▶ User Management
 - ▶ Utilities
 - ▶ Help

Edit H.323 Gatekeeper - CM

Name or IP Address	Status
10.10.16.23	In Use

Select **AE Services** from the left hand menu and select **DMCC** to verify that the **DMCC Service** is licensed by ensuring that **DMCC Service** is in the list of services and that the **License Mode** is showing **NORMAL MODE**. If not, consult with your Avaya Account Manager or Business Partner to acquire the proper license for your solution.

AE Services Home | Help | Logout

▼ AE Services

- CVLAN
- DLG
- DMCC
- SMS
- TSAPI
- TWS
- Communication Manager Interface
- Licensing
- Maintenance
- Networking
- Security
- Status
- User Management
- Utilities
- Help

AE Services

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

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A

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

* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

License Information
You are licensed to run Application Enablement (CTI) version 6.0

6.3. Creat TSAPI Link

A TSAPI link is required to allow the ReDat recorder to connect to AES. From the left hand menu select **AE Services** → **TSAPI** → **TSAPI Links** and click on **Add Link**

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

▼ AE Services

- CVLAN
- DLG
- DMCC
- SMS
- TSAPI
 - TSAPI Links
 - TSAPI Properties
- TWS
- Communication Manager Interface

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<input type="button" value="Add Link"/> <input type="button" value="Edit Link"/> <input type="button" value="Delete Link"/>				

On the **Add TSAPI Link** page enter the **Link** number to be used, The Switch Connection added earlier and the Switch CTI Link Number added in **Section 5.7**. Click on **Apply Changes** to add the TSAPI Link

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

▼ AE Services

- CVLAN
- DLG
- DMCC
- SMS
- TSAPI
 - TSAPI Links
 - TSAPI Properties
- TWS
- Communication Manager Interface

Add TSAPI Links

Link:

Switch Connection:

Switch CTI Link Number:

ASAI Link Version:

Security:

When the TSAPI Link has been added it will be shown in the list.

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

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
 - TSAPI Links
 - TSAPI Properties
- ▶ TWS
- ▶ Communication Manager Interface

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	CN	1	7	Unencrypted

[Add Link](#) [Edit Link](#) [Delete Link](#)

6.4. Create CTI User

A user ID and password needs to be configured for the ReDat Experience to communicate as a DMCC Client with the Application Enablement Services. Select **User Management → User Admin → Add User** from the left hand menu, to display the **Add User** screen in the right pane. Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password** and **Confirm Password**. For **Avaya Role**, select **userservice.useradmin** from the drop down list. For **CT User**, select **Yes** from the drop-down list. Retain the default value in the remaining fields. Click **Apply** at the bottom of the screen (not shown below).

User Management | User Admin | Add User Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

- ▶ Service Admin
- ▼ User Admin
 - Add User
 - Change User Password
 - List All Users
 - Modify Default Users
 - Search Users
- ▶ Utilities
- ▶ Help

Add User

Fields marked with * can not be empty.

* User Id

* Common Name

* Surname

* User Password

* Confirm Password

Admin Note

Avaya Role

Business Category

Car License

CM Home

Cms Home

CT User

Department Number

6.5. Enable CTI User

Navigate to the users screen by selecting **Security** → **Security Database** → **CTI Users** → **List All Users**. In the **CTI Users** window, select the user that was set up in **Section 6.3** and select the **Edit** option.

The screenshot displays the 'CTI Users' management interface. On the left is a navigation menu with categories: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database, and CTI Users. The 'Security Database' and 'CTI Users' sections are expanded, with 'List All Users' selected. The main area shows a table of CTI Users. The user 'retia' is selected, highlighted with a red border, and has a red radio button next to its User ID. Below the table are 'Edit' and 'List All' buttons.

User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> John	John	NONE	NONE
<input type="radio"/> pc5	pc5	NONE	NONE
<input type="radio"/> pc5hd	pc5hd	NONE	NONE
<input type="radio"/> presence	presence	NONE	NONE
<input checked="" type="radio"/> retia	Retia	NONE	NONE
<input type="radio"/> scantalk	Scantalk	NONE	NONE
<input type="radio"/> synAES	synAES	NONE	NONE

The **Edit CTI User** screen appears. Tick the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen.

Security | Security Database | CTI Users | List All Users Home | Help | Logout

Edit CTI User

User Profile: User ID: retia
Common Name: Retia
Worktop Name: NONE
Unrestricted Access ☒

Call and Device Control: Call Origination/Termination and Device Status: NONE

Call and Device Monitoring: Device Monitoring: NONE
Calls On A Device Monitoring: NONE
Call Monitoring: ☐

Routing Control: Allow Routing on Listed Devices: NONE

Apply Changes **Cancel Changes**

6.6. Configure DMCC Port

On the AES Management Console navigate to **Networking → Ports** to set the DMCC server port. During the compliance test, the **Unencrypted Port** set to **4721** was **Enabled** as shown in the screen below. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process.

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▼ Networking

AE Service IP (Local IP)

Network Configure

Ports

TCP Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port 9999 ☒ ☐

Encrypted TCP Port 9998 ☒ ☐

DLG Port

TCP Port 5678

TSAPI Ports

TSAPI Service Port 450 ☒ ☐

Local TLINK Ports

TCP Port Min 1024

TCP Port Max 1039

Unencrypted TLINK Ports

TCP Port Min 1050

TCP Port Max 1065

Encrypted TLINK Ports

TCP Port Min 1066

TCP Port Max 1081

DMCC Server Ports

Unencrypted Port 4721 ☒ ☐

Encrypted Port 4722 ☒ ☐

TR/87 Port 4723 ☐ ☒

H.323 Ports

TCP Port Min 20000

TCP Port Max 23999

Local UDP Port Min 30000

Local UDP Port Max 33999

Server Media

RTP Local UDP Port Min* 40000

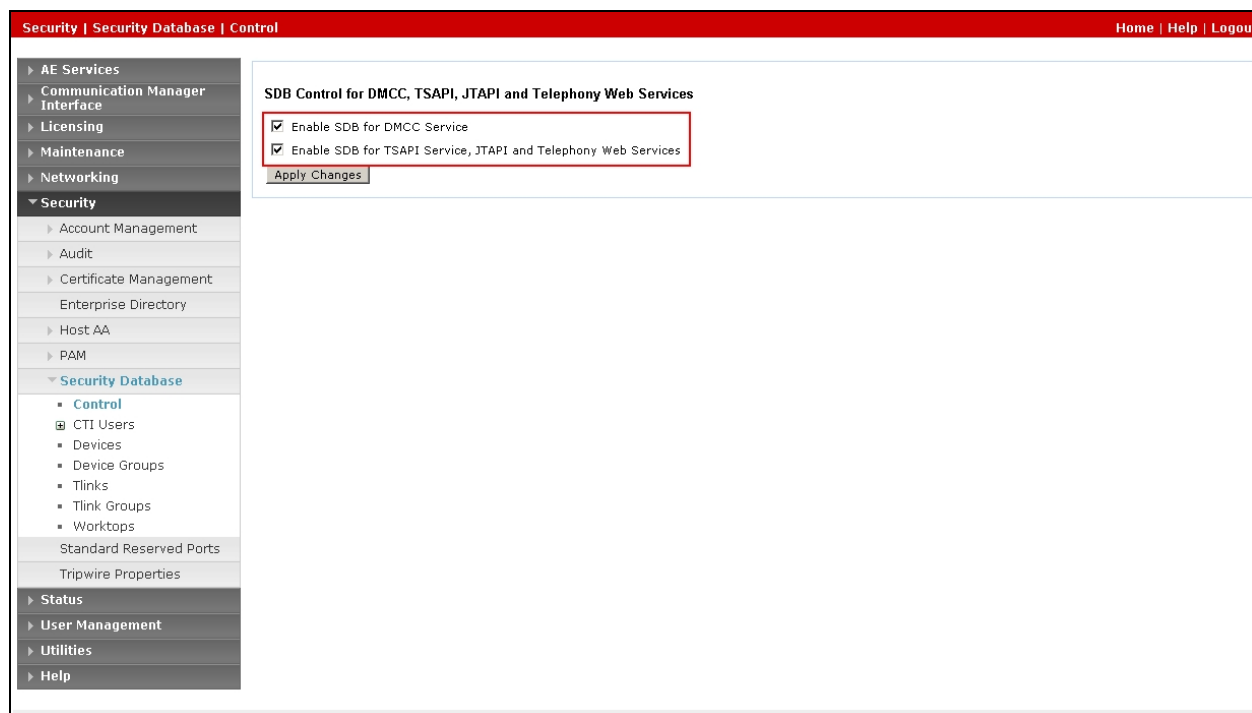
RTP Local UDP Port Max* 47999

Enabled Disabled ☒ ☐

* Note: The number of RTP ports needs to be double the number of extensions using server media.

6.7. Enable Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC and TSAPI** screen in the right pane. Check **Enable SDB for DMCC Service** and **Enable SDB TSAPI Service, JTAPI and Telephony Service**, and click **Apply Changes**.



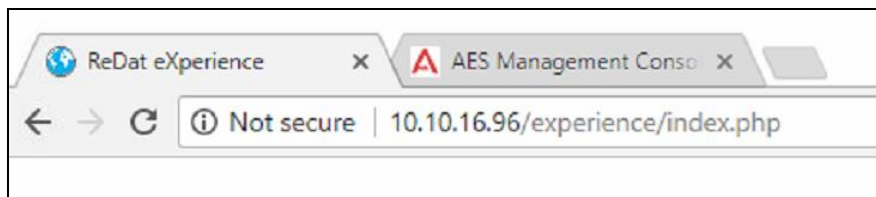
7. Configure Retia ReDat eXperience

It is implied that the ReDat server is installed including pre-requisite software and the correct licensing is in place. To configure the ReDat server, a standard browser is used. The configuration operations described in this section can be summarized as follows:

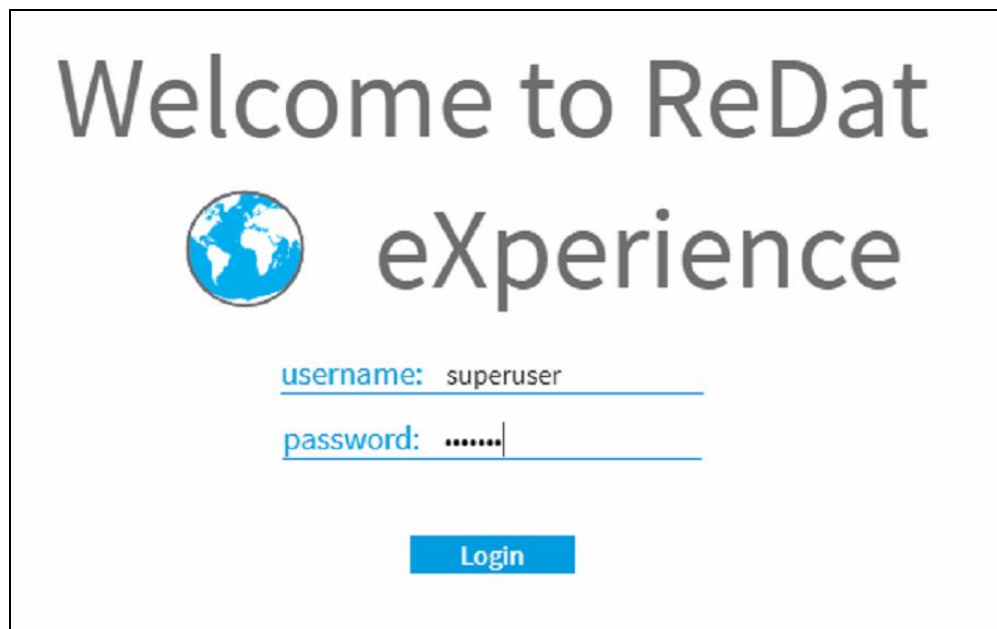
- Logging into the ReDat server
- Configure CTI
- Configure Recording units
- Configure Channels and real extensions
- Configure Hunt group extension
- Configure Virtual Extensions (SSC recorders)
- Restart active recording Service

7.1. Logging into the ReDat server

Browse to the IP Address of the ReDat server.

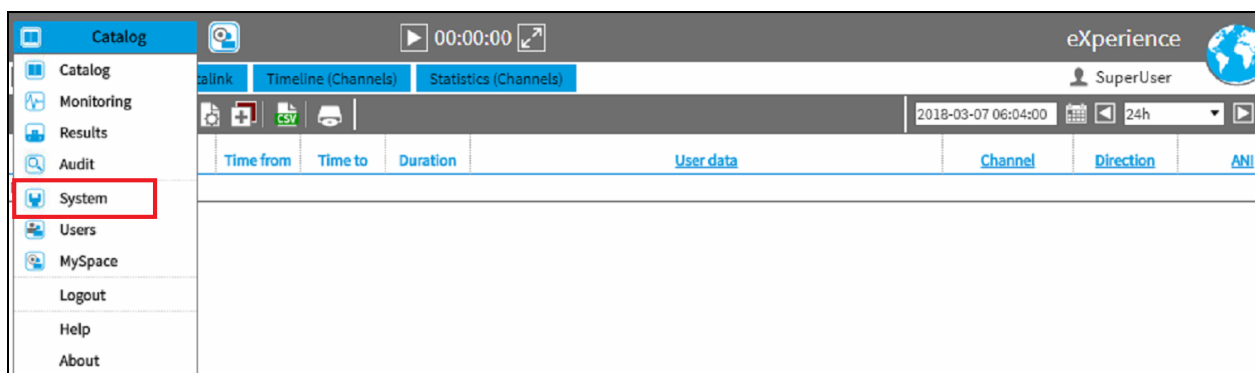


Once the new window opens, enter the appropriate credentials, and click **Login**.

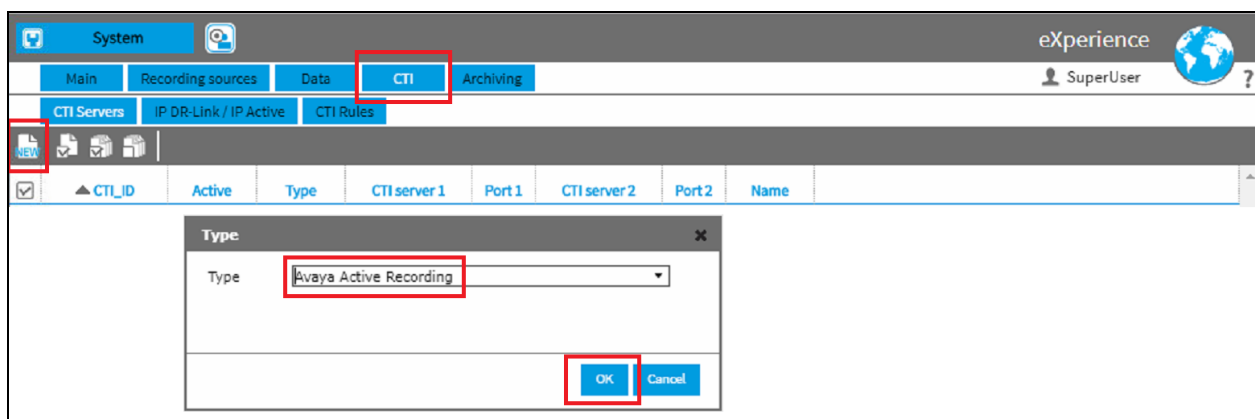
The login page for ReDat eXperience. It features the text 'Welcome to ReDat' in a large, dark font, followed by a blue globe icon and the word 'eXperience' in a large, dark font. Below this, there are two input fields: 'username: superuser' and 'password:'. A blue 'Login' button is positioned at the bottom center of the form.

7.2. Configure CTI

Click on **Catalog** and navigate to **Catalog → System**.



Once the **System** page opens, select the **CTI** tab followed by the **CTI Servers** tab and click on the **New** icon highlighted. Select **Avaya Active Recording** from the **Type** dropdown box and click the **OK** button.



When the new page opens, enter the following:

- **Name** Enter **Avaya Active**
- **AES Server** Enter the IP address of the AES Server (10.10.16.78)
- **AES port** Enter **4721** (**Unencrypted Port** as configured in **Section 6.6**)
- **User 1** Enter **retia** (**User ID** as configured in **Section 6.3**)
- **Password 1** Enter the **User Password** as configured in **Section 6.3**
- **Protocol** Select **Single Step Protocol** from the dropdown box
- **CM Server address** Enter the CM IP address (in this case 10.10.16.23)
- **Global device password** Enter the Security Code configured for the IP Station shown in.

Click on the **Save** Icon to save the configuration.

The screenshot shows the Avaya eXperience CTI configuration interface. The 'CTI' tab is selected in the top navigation bar. Below it, the 'CTI Servers' sub-tab is active. A table lists CTI servers, with the first entry 'Avaya Active' selected. The 'General' configuration panel for this server is shown, with fields for Name, AES server, AES port, User 1, Password 1, Protocol, CM server address, CM server name, and Global device password. The 'Protocol' dropdown is set to 'Single Step Protocol'. The 'CM server address' is set to '10.10.16.23'. The 'CM server name' is set to 'CMLeatest'. The 'Global device password' is masked with asterisks. The 'Name' field is set to 'Avaya Active'. The 'AES server' is set to '10.10.16.78'. The 'AES port' is set to '4721'. The 'User 1' is set to 'retia'. The 'Password 1' is masked with asterisks. The 'Active' checkbox is checked. The 'Monitoring' section has 'Secure connection' checked. The 'Records' section has 'Edit ringing' checked. The 'Setting for internal call identification' section has 'ANI/DNIS compare - number leng' checked.

7.3. Configure Recording units

Click on the **Recording sources** tab followed by the **Recording units** tab. Click on the **New** icon, select the **General** tab and enter the following:

- **Name** Enter an informative name (i.e., VoIP Recorder)
- **Login** Enter user account login of the ReDat server (retia)
- **Password** Enter the retia password of the ReDat server
- **Confirm password** Confirm password
- **Type/Partition** Select **ReDat VoIP Recorder** from the dropdown box
- **IP address** Enter the IP address of the ReDat server
- **Replication function** Select **Database+archiving** from the dropdown box

Select the **CTI** tab and enter the following:

- **CTI_ID** Select **1-Avaya Active** from the dropdown box
- **Control** Click on the **Control** check box
- **Edit** Click on the **Edit** check box

Click on the **Save** icon highlighted to save.

7.4. Configure Channels and real extensions that are to be recorded.

Click on the **Recording sources** tab followed by the **Channels** tab. Double click the first Channel and select the **General** tab. Fill in the **Name** and the **Number** of the recorded extension. Click on the **Save** icon.

The screenshot shows the Avaya system interface. The 'Recording sources' tab is selected, and the 'Channels' sub-tab is active. A table lists channels, with the first entry 'IPT 1:0001' selected. The 'General' sub-tab is open, showing fields for 'Name' (8230001), 'Number' (8230001), and 'MAC/IP'.

Channel	Recording unit	Group	Number	Name	Description	Active	Assign
IPT 1:0001	VoIP recorder	root	8230001	8230001	H323	✓	✓

Sub-tab: **General**

Name: 8230001
 Number: 8230001
 MAC/IP:

Click on the **Parameters of eXperience** tab and enter the following:

- **Description** May be used for the optional description
- **Active** Click the **Active** check box
- **Assign** Click the **Assign** check box

Click on the **Save** icon.

The screenshot shows the 'Parameters of eXperience' sub-tab. The 'Description' field contains 'H323'. The 'Active' and 'Assign' checkboxes are checked. Other fields include 'Group' (root), 'Type of channel' (Normal), 'Coupled channel' (empty), and 'Compression' (-- not selected --).

Sub-tab: **Parameters of eXperience**

Description: H323

Active: ☒ Assign: ☒

Group: root
 Type of channel: Normal
 Coupled channel:
 Compression: -- not selected --

Click on the **CTI** tab and check the following:

- **CTI_ID** **1-Avaya Active**
- **Control** **Control** check box is enabled
- **Edit** **Edit** check box is enabled

The screenshot shows the 'Recording sources' configuration page. The 'Channels' sub-tab is selected. A table lists recording units, with the first entry 'IPT 1:0001' selected. Below the table, the 'CTI' tab is active, showing configuration options for 'Control', 'Edit', and 'Diagnostics'. The 'CTI_ID' dropdown is set to '1 - Avaya Active'.

Channel	Recording unit	Group	Number	Name	Description	Active	
<input checked="" type="checkbox"/>	IPT 1:0001	VoIP recorder	root	8230001	8230001	H323	<input checked="" type="checkbox"/>

General	Parameters of eXperience	CTI	Parameters of recording unit	Usage
Number prefix		<input checked="" type="checkbox"/> Control <input checked="" type="checkbox"/> Edit <input type="checkbox"/> Diagnostics	Security code	
CTI_ID	1 - Avaya Active			
Priority line	No			

Repeat these steps for each channel to be recorded:

System										
Main Recording sources Data CTI Archiving										
Recording units Channels Extensions										
<input checked="" type="checkbox"/>	Channel	Recording unit	Group	Number	Name	Description	Active	Assign	Used	Control
<input checked="" type="checkbox"/>	IPT 1:0001	VoIP recorder	root	8230001	8230001	H323	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Control, Edit
<input type="checkbox"/>	IPT 1:0002	VoIP recorder	root	8230003	8230003	H323	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Control, Edit
<input type="checkbox"/>	IPT 1:0003	VoIP recorder	root	8237001	8237001	Digital	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Control, Edit

7.5. Configure a Hunt group extension

Click on the **Recording sources** tab followed by the **Extensions** tab. Click on the **New** icon, select the **General** tab and enter the following:

- **Number** Enter a hunt group that will be monitored
- **Name** Enter the name (optional)
- **Assign** Click the **Assign** check box
- **Active** Click the **Active** check box

Click on the **Save** icon.

The screenshot shows the Avaya system configuration interface. The 'Recording sources' tab is selected, and the 'Extensions' sub-tab is active. A new hunt group is being configured. The 'General' tab is selected, showing the following fields: Number (8233001), Name (Hunt group), Description, and Group (root). The 'Assign' and 'Active' checkboxes are checked. The 'CTI' and 'Usage' tabs are also visible.

Click on the **CTI** tab and enter the following:

- **CTI_ID** Select **1-Avaya Active** from the dropdown box
- **Extension type** Select **Huntgroup** from the dropdown box

Click on the **Save** icon.

The screenshot shows the 'CTI' tab for the hunt group configuration. The following fields are visible: Number prefix, CTI_ID (1 - Avaya Active), Priority line (No), and Extension type (Huntgroup). The 'Diagnostics' section is also visible, with fields for IP address and Port.

7.6. Configure Extensions (Virtual)

Click on the **Recording sources** tab followed by the **Extensions** tab. Click on the **New** Icon, select the **General** tab and enter the following:

- **Number** Enter an CTI extension number that will be used as the recorder for the monitored calls
- **Name** Enter the name assigned to the Extension (optional)
- **Assign** Uncheck the **Assign** check box
- **Active** Click the **Active** check box

Click on the **Save** icon highlighted to save.

The screenshot displays the Avaya system interface for configuring virtual extensions. The top navigation bar includes 'System' and a 'New' icon. Below this, a series of tabs are visible: 'Main', 'Recording sources', 'Data', 'CTI', and 'Archiving'. The 'Recording sources' tab is selected, and within it, the 'Extensions' sub-tab is active. A table lists existing extensions, with one entry highlighted: '8230090' with a green checkmark in the 'Active' column and a red 'X' in the 'Assign' column. Below the table, the 'General' tab for the selected extension is shown. It contains fields for 'Number' (8230090), 'Name', 'Description', and 'Group' (root). To the right of these fields are two checkboxes: 'Assign' (unchecked) and 'Active' (checked). Red boxes highlight the 'Recording sources' and 'Extensions' tabs, the 'General' tab, the 'Number' field, and the 'Assign' and 'Active' checkboxes.

Name	Number	Active	Assign	Group	Description	CTI_ID
	8230090	✓	✗	root		1

General | CTI | Usage

Number: 8230090

Name:

Description:

Group: root

☐ Assign

☒ Active

Click on the **CTI** tab and enter the following:

- **CTI_ID** **1- Avaya Active** from the dropdown box
- **Extension type** Select **Extension** from the dropdown box

Click on the **Save** icon.

Note: Repeat these steps for each extension that is to be monitored. Also note that 2 ports are required for each virtual extension, therefore the next port should be 61002 and so on.

The screenshot shows the 'System' configuration page with the 'Recording sources' tab selected. Under 'Recording sources', the 'Extensions' sub-tab is active. A table lists extensions, with 8230090 selected. Below the table, the 'CTI' sub-tab is selected, showing configuration fields for the selected extension. Red boxes highlight the 'CTI_ID' dropdown (set to '1 - Avaya Active') and the 'Extension type' dropdown (set to 'Extension').

Name	Number	Active	Assign	Group	Description	CTI_ID
8230090		✓	✗	root		1

General CTI Usage

Number prefix:

CTI_ID: **1 - Avaya Active**

Priority line: **No**

Extension type: **Extension**

☐ Diagnostics

IP address:

Port:

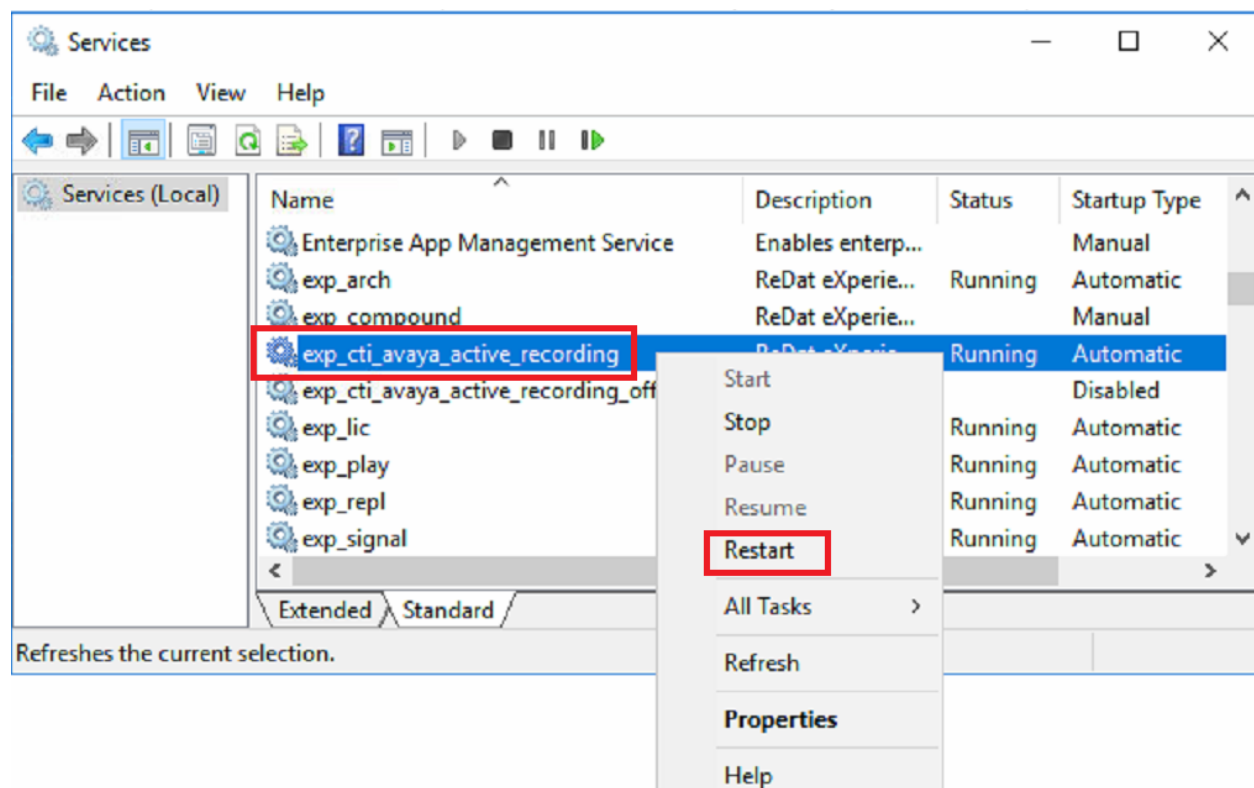
Note: Repeat these steps for all extensions that are to be configured:

The screenshot shows the 'System' configuration page with the 'Recording sources' tab selected. Under 'Recording sources', the 'Extensions' sub-tab is active. A table lists extensions from 8230090 to 8233001. The 'Active' column shows green checkmarks for all extensions, and the 'Assign' column shows red X marks for all extensions except the 'Hunt group'.

Name	Number	Active	Assign	Group	Description	CTI_ID	Number prefix
8230090		✓	✗	root		1	
8230091		✓	✗	root		1	
8230092		✓	✗	root		1	
8230093		✓	✗	root		1	
8230094		✓	✗	root		1	
8230095		✓	✗	root		1	
8230096		✓	✗	root		1	
8230097		✓	✗	root		1	
8230098		✓	✗	root		1	
8230099		✓	✗	root		1	
Hunt group	8233001	✓	✓	root		1	

7.7. Restart active recording Service

Once all the configurations are made to the ReDat server the exp_cti_avaya_active_recording service must be restarted. Click on **Start → Run** and enter **services.msc**. When the **Services** window opens, right click on **exp_cti_avaya_active_recording** and click on **Restart**.



8. Verification Steps

This section provides the tests that can be performed to verify correct configuration of the Avaya and Retia ReDat eXperience solution.

8.1. Verify Avaya Aura® Application Enablement Services status

Log in to Avaya Aura® Application Enablement Services, and navigate to the **AE Services** screen. Verify that the DMCC and TSAPI Services are **ONLINE**, and **Running**.

AE Services Home | Help | Logout

AE Services

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

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A

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

* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

Navigate to **Status** → **Status and Control** → **Switch Conn Summary**. Verify that the **Conn State** is **Talking** and the **Online/Offline** is **Online**.

Status | Status and Control | Switch Conn Summary Home | Help | Logout

Switch Connections Summary

☐ Enable page refresh every 60 seconds

Switch Conn	Conn State	Processor Ethernet	Since	Online/Offline	Active/Standby/Admin'd AEP Conns	Num of TCI Conns	SSL	Msgs To Switch	Msgs From Switch	Msg Period
CM63	Talking	Yes	Tue Mar 4 05:02:31 2014	Online	1 / 0 / 1	2	Enabled	625	645	30

[Online](#) [Offline](#) [Connection Details](#) [Per Service Connections Details](#)

Navigate to **Status** → **Status and Control** → **DMCC Service Summary** and click **Service Summary**. Verify that the ReDat system has established a session.

DMCC Service Summary - Session Summary

☐ Enable page refresh every seconds

Session Summary **Device Summary**

Generated on Tue Mar 04 11:17:01 UTC 2014

Service Uptime: 14 days, 1 hours 39 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 6

Number of Existing Devices: 7

Number of Devices Created Since Service Boot: 70

Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
174E4F9A9CABE5DEE 9B97C470277C027-5	retia	Avaya Active Recording	10.10.60.70	XML Unencrypted	7

Item 1-1 of 1

8.2. Verify ReDat

To verify that the ReDat server is recording calls, make some calls to/from monitored extensions. Log in to the ReDat server as per **Section 7.1**. Once logged in click on the **List of records** tab and it should be possible to see something similar to the screen shot below. To listen to one of the calls click on the **Speaker** icon highlighted. The call content is stored in the stereo format record (AUDIO=stereo flag is indicated in the User data item).

List of records | Datalink | Timeline (Channels) | Statistics (Channels)

2018-03-06 08:04:00 | 24h

Date	Time from	Time to	Dur...	User data	Channel	Direction	ANI	DNIS	C
2018-03-06	08:35:01	08:35:09	0:08	Exten=8230001 CallID=2827 Parties "8270001"8230001 Direction=IN CompoundID=2827 AUDIO=stereo	IPT 1:0001	→	8270001	8230001	Single
2018-03-06	08:35:42	08:35:49	0:07	Exten=8230001 CallID=2833 Parties "8270001"8230001 Direction=OUT CompoundID=2833 AUDIO=stereo	IPT 1:0001	→	8230001	8270001	Single
2018-03-06	09:36:02	09:36:12	0:10	Exten=8230001 CallID=2840 Parties "8270001"8230001 Direction=OUT CompoundID=2840 AUDIO=stereo	IPT 1:0001	→	8230001	8235001	Single
2018-03-06	12:44:15	12:44:24	0:09	Exten=8230001 CallID=2848 Parties "8270001"8230001 Direction=OUT CompoundID=2848 AUDIO=stereo	IPT 1:0001	→	8230001	8235001	Single
2018-03-06	12:44:30	12:44:37	0:07	Exten=8230001 CallID=2856 Parties "8270001"8230001 Direction=OUT CompoundID=2856 AUDIO=stereo	IPT 1:0001	→	8230001	8235002	Single

Context menu options: Play, Export of record, Send via e-mail..., Record audit, Insert value to column filter, Edit, Complete call, To incident

9. Conclusion

These Application Notes describe the configuration steps required for Retia ReDat eXperience with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using Single Step Conference and Selective Listening Hold. All test cases have passed and met the objectives outlined in **Section 2.2**.

10. Additional References

This section references the Avaya and Retia documentation that is relevant to these Application Notes.

Product documentation for Avaya products may be found at:

<http://support.avaya.com>

- [1] *Administering Avaya Aura® Communication Manager, Release 7.1, Document Number 03-300509.*
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation, Release 7.1, Document Number 555-245-205.*
- [3] *Administering Avaya Aura® Session Manager, Release 7.1,*
- [4] *Administering Avaya Aura® System Manager, Release 7.1.*
- [5] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide, Release 7.1.*

Technical documentation for Retia can be found at the following location:

<http://www.redat.eu/en/>

©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.