



Avaya Solution & Interoperability Test Lab

Application Notes for Retia ReDat Recording System with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services Using Single Step Conference – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Retia ReDat recording system to interoperate with Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services (AES) Device, Media, and Call Control (DMCC) interface using Single Step Conference to capture the media associated with the monitored endpoints for call recording.

Information in these Application Notes has been obtained through 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 recording system to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. The ReDat system 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.

ReDat 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.

1.1. Interoperability Compliance Testing

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

- The following test scenarios were used to test the various ReDat features:
 - Basic call
 - Hold/retrieve
 - 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 following components:
 - The ReDat server
 - The Avaya Aura® Communication Manager Server to which the ReDat is attached.

1.2. Support

Support for ReDat is available at:

<http://www.redat.cz/en/contacts/>

2. Reference Configuration

The following diagram shows the configuration used for compliance testing.

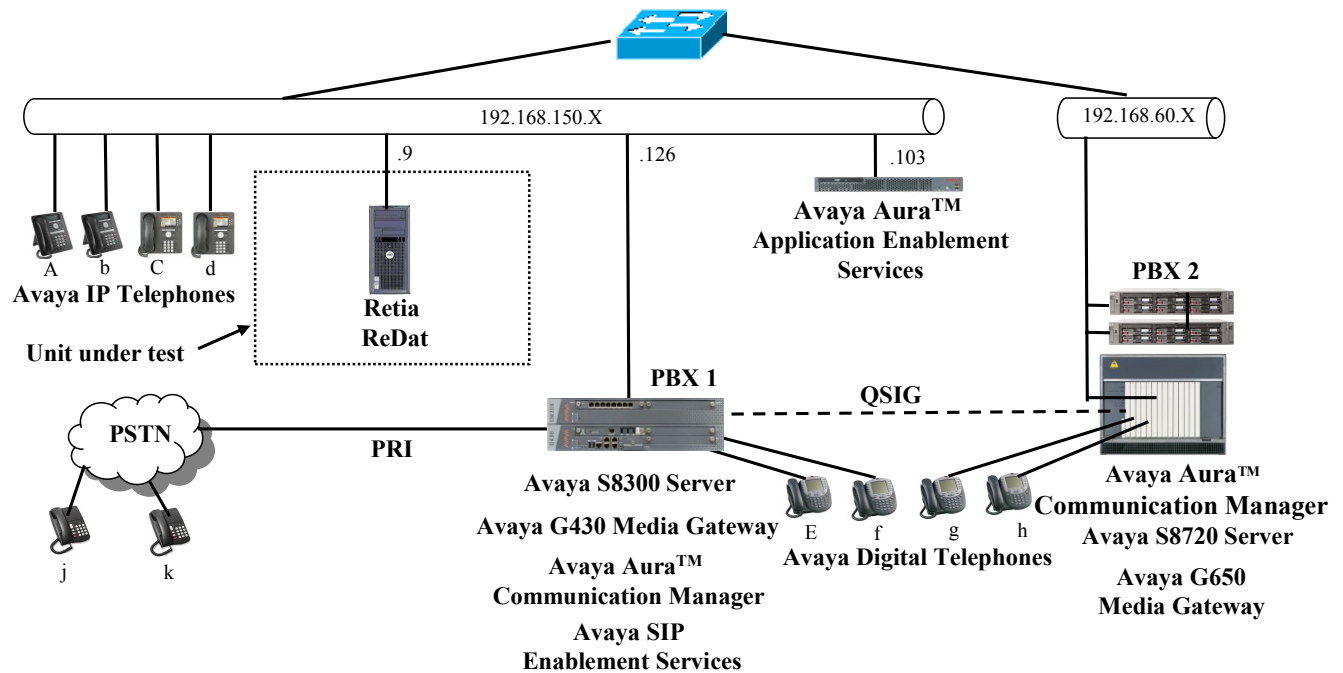


Figure 1: ReDat Test Configuration

In the above diagram, the Retia ReDat records voice conversations from telephones attached to PBX 1. The TSAPI and DMCC services provided by Application Enablement Services are used to monitor call activity and capture voice streams associated with PBX 1. The Retia ReDat is attached to PBX 1 via the local area network. PBX 2 is included in the configuration solely to test the ability to monitor conversations which traverse a trunk to a networked PBX. The stations attached to PBX 2 are not monitored by Retia ReDat.

When a call is to be recorded, the ReDat system uses the Avaya Aura® Communication Manager Single Step Conference feature to initiate monitoring for calls which it wishes to record. The voice stream for such calls is received via the LAN interface to PBX 1.

The PBX 2 system is attached to PBX 1 via an IP/QSIG interface, and is used as a networked PBX system. This allows remote networked telephones (g, h) to be included in the test.

The telephones depicted in these Application Notes are designated by an upper case letter if configured to be monitored by the ReDat system. A lower case letter designates those terminals which have been configured not to be monitored or are possibly unable to be monitored.

The following table contains additional information about each of the telephones shown in **Figure 1**. A “*” in the “Monitored” column indicated that the telephone is monitored by the ReDat voice recorder.

| Phone | Monitored | Model | Extension |
|-------|-----------|--------------------|--------------|
| A | * | Avaya 9640G | 10094 |
| b | | Avaya 9640G | 10184 |
| C | * | Avaya 9630G | 10183 |
| d | | Avaya 1608 | 10065 |
| E | * | Avaya 2410 | 10001 |
| f | | Avaya 2410 | 10002 |
| g | | Avaya 2410 | 60007 |
| h | | Avaya 2410 | 60008 |
| j | | N/A | 069 111 1111 |
| k | | N/A | 015 222 2222 |
| L | | Hunt Group (A & C) | 11304 |
| x | | CTI Station | 11401 |
| y | | CTI Station | 11402 |
| z | | CTI Station | 11403 |

Table 1: Device Monitor Configuration

3. Equipment and Software Validated

| Component | Version |
|--|---|
| Avaya G430 Media Gateway | 30.14.0 |
| Avaya Aura® Communication Manager | R015x.02.1.016.4 Patch: 18365 |
| Avaya Aura® Application Enablement Services | 5.2.2 |
| Avaya Aura® Application Enablement Services TSAPI Client | 5.2 Build 483 |
| Avaya 96xx H.323 Telephones | S3.110b |
| Avaya 16xx H.323 Telephones | 1.3 |
| Retia ReDat platform: MS Server 2003 | SP R2 |
| Retia ReDat | ReDat AS v3.13 ReDat VoIP recorder v1.10 |

Table 2: Hardware/Software Component Versions

4. Configure Avaya Aura® Communication Manager

The configuration information in this section covers only PBX 1 – the system to which the ReDat voice recorder is attached.

The configuration and verification operations illustrated in this section were all performed using the Avaya Aura® Communication Manager System Administration Terminal (SAT).

The information provided in this section describes the configuration of Avaya Aura® Communication Manager for this solution. For all other provisioning information, such as installation and configuration, please refer to the product documentation in references [1] and [2].

4.1. Verify system-parameters customer-options

Use the **display system-parameters customer options** command to verify that Communication Manager is configured to meet the minimum requirements to run ReDat. Those items shown in **bold** indicate required values or minimum capacity requirements. If these are not met in the configuration, please contact an Avaya representative for further assistance.

| Parameter | Usage |
|--|---|
| Maximum Concurrently Registered IP Stations (Page 2) | This must be sufficient to support the total number of IP stations. |
| IP Stations (Page 4) | This parameter must be set to “y”. |
| IP_Phone (Page 10) | This parameter must be set to the number of IP stations plus 1 for each station which is to be monitored. |

Table 3: System-Parameters Customer-Options Parameters

| | | |
|---|--|--------------|
| display system-parameters customer-options | | Page 2 of 11 |
| OPTIONAL FEATURES | | |
| IP PORT CAPACITIES | | USED |
| Maximum Administered H.323 Trunks: 100 | | 40 |
| Maximum Concurrently Registered IP Stations: 450 | | 3 |
| Maximum Administered Remote Office Trunks: 450 | | 0 |
| Maximum Concurrently Registered Remote Office Stations: 450 | | 0 |
| Maximum Concurrently Registered IP eCons: 0 | | 0 |
| Max Concur Registered Unauthenticated H.323 Stations: 0 | | 0 |
| Maximum Video Capable H.323 Stations: 0 | | 0 |
| Maximum Video Capable IP Softphones: 0 | | 0 |
| Maximum Administered SIP Trunks: 100 | | 30 |
| Maximum Administered Ad-hoc Video Conferencing Ports: 0 | | 0 |
| Maximum Number of DS1 Boards with Echo Cancellation: 0 | | 0 |
| Maximum TN2501 VAL Boards: 0 | | 0 |
| Maximum Media Gateway VAL Sources: 1 | | 1 |
| Maximum TN2602 Boards with 80 VoIP Channels: 0 | | 0 |
| Maximum TN2602 Boards with 320 VoIP Channels: 0 | | 0 |
| Maximum Number of Expanded Meet-me Conference Ports: 0 | | 0 |

Figure 2: System-Parameters Customer-Options Screen, Page 2

| | | |
|--|---|--------------|
| display system-parameters customer-options | | Page 4 of 11 |
| OPTIONAL FEATURES | | |
| Emergency Access to Attendant? y | IP Stations? y | |
| Enable 'dadmin' Login? y | | |
| Enhanced Conferencing? n | ISDN Feature Plus? n | |
| Enhanced EC500? y | ISDN/SIP Network Call Redirection? n | |
| Enterprise Survivable Server? n | ISDN-BRI Trunks? y | |
| Enterprise Wide Licensing? n | ISDN-PRI? y | |
| ESS Administration? n | Local Survivable Processor? n | |
| Extended Cvg/Fwd Admin? y | Malicious Call Trace? n | |
| External Device Alarm Admin? n | Media Encryption Over IP? n | |
| Five Port Networks Max Per MCC? n | Mode Code for Centralized Voice Mail? n | |
| Flexible Billing? n | | |
| Forced Entry of Account Codes? n | Multifrequency Signaling? y | |
| Global Call Classification? n | Multimedia Call Handling (Basic)? n | |
| Hospitality (Basic)? y | Multimedia Call Handling (Enhanced)? n | |
| Hospitality (G3V3 Enhancements)? n | Multimedia IP SIP Trunking? n | |
| IP Trunks? y | | |
| IP Attendant Consoles? n | | |

Figure 3: System-Parameters Customer-Options Screen, Page 4

| | | |
|--|--------------|---------------|
| display system-parameters customer-options | | Page 10 of 11 |
| MAXIMUM IP REGISTRATIONS BY PRODUCT ID | | |
| Product ID | Rel. Limit | Used |
| IP_API_A | : 100 | 0 |
| IP_API_B | : 100 | 0 |
| IP_API_C | : 100 | 0 |
| IP_Agent | : 100 | 0 |
| IP_IR_A | : 100 | 0 |
| IP_NonAgt | : 100 | 0 |
| IP_Phone | : 450 | 2 |
| IP_ROMax | : 450 | 0 |
| IP_Soft | : 100 | 0 |
| IP_Supv | : 100 | 0 |
| IP_eCons | : 68 | 0 |
| oneX_Comm | : 450 | 1 |

Figure 4: System-Parameters Customer-Options Screen Page 10

4.2. Configure Avaya Aura® Application Enablement Services Interface

Use the **change ip-services** command to configure the interface to the Application Enablement Services server, as shown in the following table.

| Parameter | Usage |
|-----------------------------|---|
| Service Type (Page 1) | Enter “AESVCS”. |
| Enabled (Page 1) | Enter “y” to enable the service. |
| Local Node (Page 1) | Enter the IP node name for the PROCR interface. |
| AE Services Server (Page 4) | Enter the name that was assigned to the Application Enablement Services server when it was installed. |
| Password (Page 4) | Enter the password that was assigned to the switch connection, as shown in Figure 16 . |
| Enabled (Page 4) | Enter “y” to enable the connection. |

Table 4: IP Services Parameters

| | | | | | | | | |
|--------------------|----------|--------------|-------------|-------------|-------------|------|------|---|
| change ip-services | | | | | | Page | 1 of | 4 |
| IP SERVICES | | | | | | | | |
| Service Type | Enabled | Local Node | Local Port | Remote Node | Remote Port | | | |
| AESVCS | y | procr | 8765 | | | | | |

Figure 5: IP Services Screen, Page 1

| | | | | | | | |
|----------------------------|--------------------|-------------------------|----------|--------|------|------|---|
| change ip-services | | | | | Page | 4 of | 4 |
| AE Services Administration | | | | | | | |
| Server ID | AE Services Server | Password | Enabled | Status | | | |
| 1: | AES | interop123456789 | y | in use | | | |

Figure 6: IP Services Screen, Page 4

4.3. Configure Stations

4.3.1. Configure IP Stations

Use the **add station** command to create each of the IP stations listed in **Table 1**, using the values shown in the following table.

| Parameter | Usage |
|---------------|--|
| Extension | Use an unassigned extension which is compatible with the dial plan. |
| Type | Use a type value which corresponds to the physical station to be used. |
| Name | Any alphanumeric string can be assigned as an extension name, which is used for identification purposes. |
| Security Code | Enter an appropriate numeric string to be used as a security code. |

Table 5: Configuration IP Stations

| | | |
|---------------------------|---------------------------------|-------------|
| add change station 10183 | | Page 1 of 5 |
| STATION | | |
| Extension: 10183 | Lock Messages? n | BCC: 0 |
| Type: 9630 | Security Code: 123456 | TN: 1 |
| Port: S00007 | Coverage Path 1: | COR: 1 |
| Name: extn 10183 | Coverage Path 2: | COS: 1 |
| | Hunt-to Station: | |
| STATION OPTIONS | | |
| | Time of Day Lock Table: | |
| Loss Group: 19 | Personalized Ringing Pattern: 1 | |
| | Message Lamp Ext: 10183 | |
| 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? n | |
| | IP Video Softphone? n | |
| | Customizable Labels? y | |

Figure 7: IP Station Screen

4.3.2. TDM Stations

Use the **add station** command to create each of the TDM stations listed in **Table 1**, using the values shown in the following table.

| Parameter | Usage |
|--------------------|--|
| Extension (page 1) | Use an unassigned extension which is compatible with the dial plan. |
| Type (page 1) | Use a type value which corresponds to the physical station to be used. |
| Name (page 1) | Any alphanumeric string can be assigned as an extension name, which is used for identification purposes. |

Table 6: Configuration IP Stations

| | | | | | |
|---------------------------|-------------------------------|-------|------|------|---|
| add station 10001 | | | Page | 1 of | 5 |
| STATION | | | | | |
| Extension: 10001 | Lock Messages? | n | BCC: | 0 | |
| Type: 2410 | Security Code: | | TN: | 1 | |
| Port: 001V601 | Coverage Path 1: | | COR: | 1 | |
| Name: exen 10001 | Coverage Path 2: | | COS: | 1 | |
| | Hunt-to Station: | | | | |
| STATION OPTIONS | | | | | |
| | Time of Day Lock Table: | | | | |
| Loss Group: 2 | Personalized Ringing Pattern: | 1 | | | |
| | Message Lamp Ext: | 10001 | | | |
| Speakerphone: 2-way | Mute Button Enabled? | y | | | |
| Display Language: english | | | | | |
| Survivable COR: internal | Media Complex Ext: | | | | |
| Survivable Trunk Dest? y | IP SoftPhone? | n | | | |
| | Remote Office Phone? | n | | | |
| | IP Video Softphone? | n | | | |
| | Customizable Labels? | y | | | |

Figure 8: TDM Station Screen

4.4. Configure Hunt Group

Use the **add hunt-group** command to create a hunt group which is used to test the ability of the ReDat system to monitor hunt groups. Assign an unused extension to the hunt group. Add extensions for telephones “A” and “C” to the hunt group, which are assigned to IP phones that are monitored by the ReDat system.

| Parameter | Usage |
|-----------------------------|--|
| Group Name (Page 1) | Any alphanumeric string can be used as a Group Name. |
| Group Extension (Page 1) | Use an unused extension which is compatible with the dial plan. |
| MEMBER ASSIGNMENTS (Page 4) | Add the extensions which are to be assigned to this hunt group to this list. For this test, extensions “A” and “C” are used. |

Table 7: Configuration IP Stations

| | | |
|--------------------------|----------------------------|--------------|
| add hunt-group 3 | HUNT GROUP | Page 1 of 60 |
| Group Number: 3 | ACD? n | |
| Group Name: A + C | Queue? n | |
| Group Extension: 11304 | Vector? n | |
| Group Type: ucd-mia | Coverage Path: | |
| TN: 1 | Night Service Destination: | |
| COR: 1 | MM Early Answer? n | |
| Security Code: | Local Agent Preference? n | |
| ISDN/SIP Caller Display: | | |

Figure 9: Hunt Group Screen, Page 1

| | | |
|--------------------------------|--------------------------------------|---------------------|
| add hunt-group 3 | HUNT GROUP | Page 3 of 60 |
| Group Number: 3 | Group Extension: 11304 | Group Type: ucd-mia |
| Member Range Allowed: 1 - 1500 | Administered Members (min/max): 1 /2 | |
| | Total Administered Members: 2 | |
| GROUP MEMBER ASSIGNMENTS | | |
| Ext | Name(19 characters) | Ext |
| 1: 10094 | extn 10094 | 14: |
| 2: 10183 | extn 10183 | 15: |
| 3: | | 16: |
| 4: | | 17: |
| 5: | | 18: |
| 6: | | 19: |
| 7: | | 20: |
| 8: | | 21: |
| 9: | | 22: |
| 10: | | 23: |
| 11: | | 24: |
| 12: | | 25: |
| 13: | | 26: |
| At End of Member List | | |

Figure 10: Hunt Group Screen, Page 3

5. Configure Avaya Aura® Application Enablement Services

The Avaya Aura® Application Enablement Services server is configured via a web browser by accessing the following URL:

https://<AES server address>/

Click “Continue To Login”.

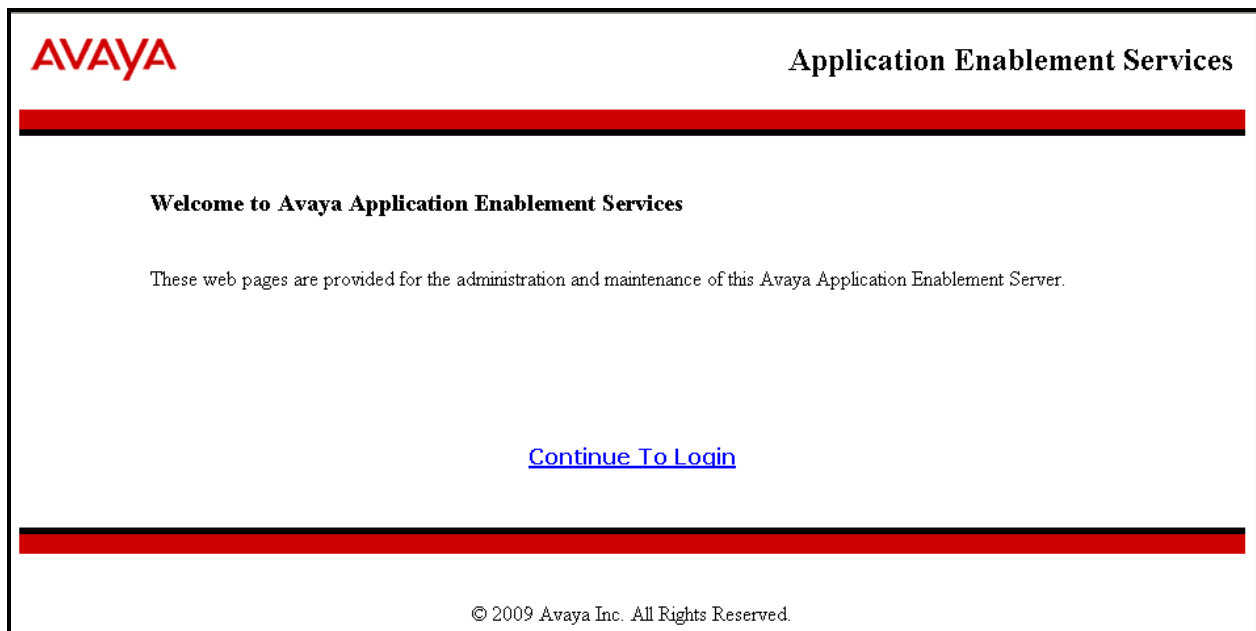
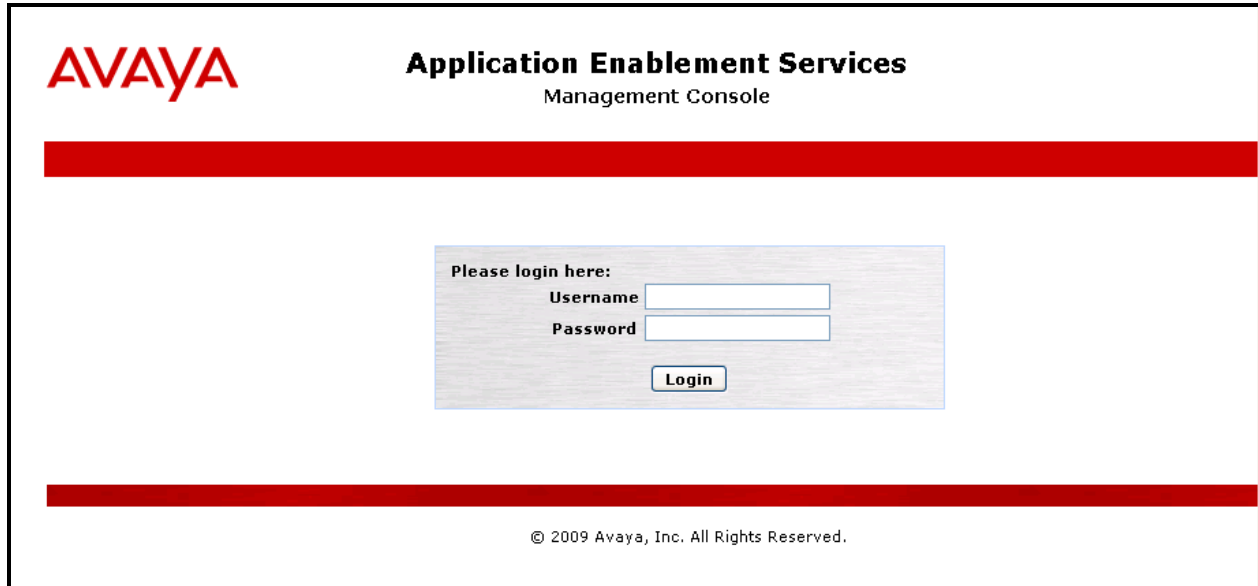


Figure 11: Avaya Aura® Application Enablement Services Welcome Screen

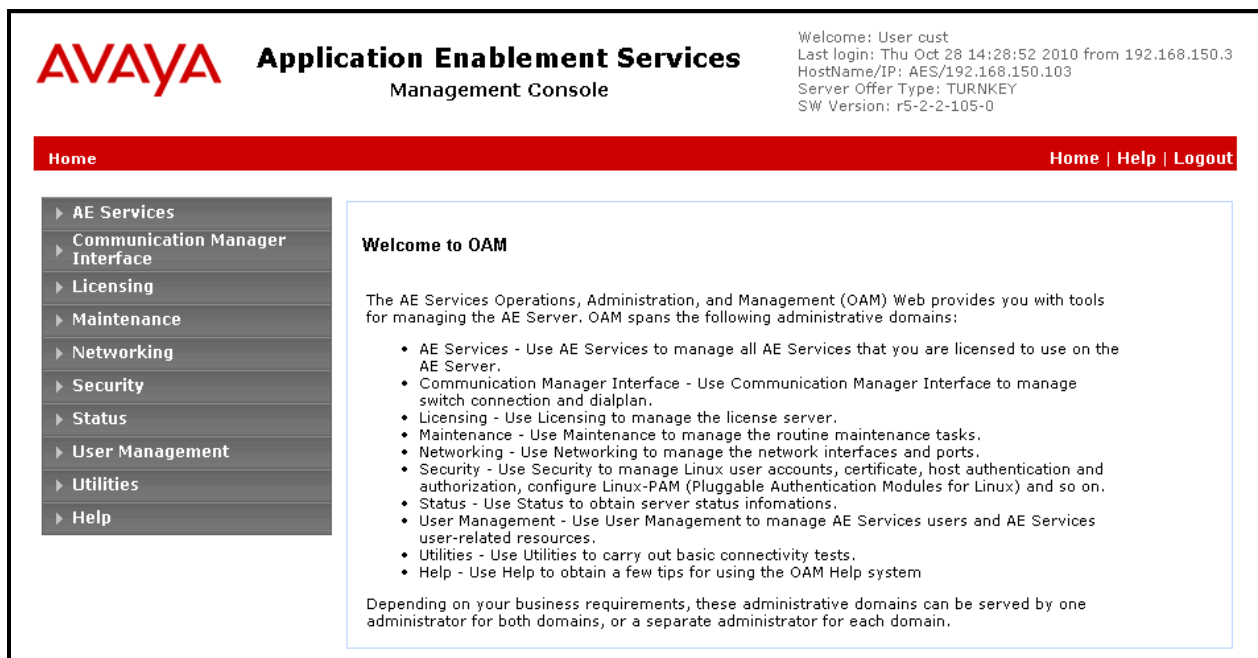
Once the login screen appears, enter the credentials for performing administrative activities.



The login screen features the Avaya logo in red on the left and the title "Application Enablement Services Management Console" in black on the right. A thick red horizontal bar spans the width of the page below the header. In the center, a light gray box contains the text "Please login here:" followed by "Username" and "Password" labels, each with a corresponding text input field. A "Login" button is positioned below the password field. Another thick red horizontal bar is located at the bottom of the page, above the copyright notice "© 2009 Avaya, Inc. All Rights Reserved."

Figure 12: Avaya Aura® Application Enablement Services Login Screen


Click “AE Services” in left frame.



The main screen displays the Avaya logo and "Application Enablement Services Management Console" on the left. On the right, a welcome message reads: "Welcome: User cust", "Last login: Thu Oct 28 14:28:52 2010 from 192.168.150.3", "HostName/IP: AES/192.168.150.103", "Server Offer Type: TURNKEY", and "SW Version: r5-2-2-105-0". Below the header is a red navigation bar with "Home" on the left and "Home | Help | Logout" on the right. A left-hand menu contains links: "AE Services", "Communication Manager Interface", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The main content area, titled "Welcome to OAM", explains that the OAM Web provides tools for managing the AE Server and lists administrative domains: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. It also notes that these domains can be served by one administrator for both or a separate administrator for each.

Figure 13: Avaya Aura® Application Enablement Services Main Screen

Verify that the Avaya Aura® Application Enablement Services server installation has a DMCC license. If this is not the case, please contact an Avaya representative regarding licensing.


Application Enablement Services
Management Console

Welcome: User cust
Last login: Thu Oct 28 14:28:52 2010 from 192.168.150.3
HostName/IP: AES/192.168.150.103
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

AE Services
Home | Help | Logout

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▶ TSAPI
- ▶ 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 5.0

Figure 14: Avaya Aura® Application Enablement Services Top Level Screen

Navigate to **Communication Manager Interface->Switch Connections**. Enter the name of the Switch Connection to be added, and click on the “Add Connection” button. This name should match what will be used by the Retia ReDat system in **section 6**.



Application Enablement Services
Management Console

Welcome: User cust
Last login: Thu Oct 28 14:28:52 2010 from 192.168.150.3
HostName/IP: AES/192.168.150.103
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

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 |
|-----------------|--------------------|------------|------------------------------|
| Evolution | Yes | 30 | 1 |

© 2009 Avaya, Inc. All Rights Reserved.

Figure 15: Switch Connection Screen

The **Communication Manager Interface | Switch Connections** page is presented. At this point, enter the screen fields as described in the following table, and click the “Apply” button.

| Parameter | Usage |
|--------------------|--|
| Switch Password | The Switch Password must be the same as was entered into the Avaya Aura® Communication Manager AE Services Administration form via the “change ip-services” command, described in Figure 6 . Passwords must consist of 12 to 16 alphanumeric characters |
| SSL | SSL (Secure Socket Layer) is enabled by default. Keep the default setting unless you are adding a Switch Connection for a DEFINITY Server CSI |
| Processor Ethernet | Check this box. |

Table 8: Configuration of Switch Password

AVAYA **Application Enablement Services**
Management Console

Welcome: User cust
Last login: Thu Oct 28 14:28:52 2010 from 192.168.150.3
HostName/IP: AES/192.168.150.103
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

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 - Evolution

Switch Password

Confirm Switch Password

Msg Period Minutes (1 - 72)

SSL ☒

Processor Ethernet ☒

Figure 16: Set Switch Password Screen

From the **Communication Manager Interface->Switch Connections** screen, click the “Edit PE/CLAN IPs” button, (not shown), to display the screen shown below. Enter the IP address of the Processor Ethernet interface that Avaya Aura® Application Enablement Services will use for communication with the switch, and click the “Add/Edit Name or IP” button.

The screenshot displays the Avaya Application Enablement Services Management Console. At the top left is the Avaya logo. To its right, the text reads 'Application Enablement Services' and 'Management Console'. In the top right corner, a welcome message states: 'Welcome: User cust', 'Last login: Thu Oct 28 14:28:52 2010 from 192.168.150.3', 'HostName/IP: AES/192.168.150.103', 'Server Offer Type: TURNKEY', and 'SW Version: r5-2-2-105-0'. Below this is a red navigation bar with 'Communication Manager Interface | Switch Connections' on the left and 'Home | Help | Logout' on the right. A left-hand sidebar contains a menu with items: 'AE Services', 'Communication Manager Interface' (expanded), 'Switch Connections' (highlighted), 'Dial Plan', 'Licensing', 'Maintenance', 'Networking', 'Security', 'Status', 'User Management', 'Utilities', and 'Help'. The main content area is titled 'Edit Processor Ethernet IP - Evolution'. It features a text input field containing '192.168.150.126' and a button labeled 'Add/Edit Name or IP'.

Figure 17: Edit Processor Ethernet IP Screen

Navigate to **User Management->User Admin->Add User**. The “CT User” field for this user must be set to “Yes”. In this case, the Avaya Aura® Application Enablement Services user is the ReDat application, which uses Avaya Aura® Application Enablement Services to monitor stations and initiate switching operations. The “User Id” and “User Password” must be the same as what will be configured for Retia ReDat in **Section 6**.

AVAYA **Application Enablement Services**
Management Console

Welcome: User cust
Last login: Thu Oct 28 14:28:52 2010 from 192.168.150.3
HostName/IP: AES/192.168.150.103
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

User Management | User Admin | Add User [Home](#) | [Help](#) | [Logout](#)

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

Csx Home

CT User

Department Number

Display Name

Employee Number

Figure 18: Add User Screen

Navigate to **Security -> Security Database -> CTI Users -> List All Users**, and then click “Edit User” for the newly added user “avaya”, (not shown). Enable “Unrestricted Access” and click “Apply Changes”.

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 login details. A red navigation bar shows the path: Security | Security Database | CTI Users | List All Users, with links for Home, Help, and Logout.

On the left is a sidebar menu with categories: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security (expanded), Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database (expanded), and Control.

The main content area is titled 'Edit CTI User'. It contains the following fields and controls:

- User Profile:**
 - User ID: avaya
 - Common Name: avaya
 - Worktop Name: NONE (dropdown menu)
 - Unrestricted Access: ☒
- Call Origination and Termination / Device Status:** None (dropdown menu)
- Call and Device Monitoring:**
 - Device: None (dropdown menu)
 - Call / Device: None (dropdown menu)
 - Call: ☐
- Routing Control:**
 - Allow Routing on Listed Devices: None (dropdown menu)

At the bottom of the form are two buttons: 'Apply Changes' and 'Cancel Changes'.

Figure 19: Edit CTI User Screen

Navigate to **Networking-> Ports** and configure the DMCC Server Ports as shown in the following table.

| Parameter | Usage |
|------------------|------------------------|
| Unencrypted Port | Set this port to 4721. |

Table 9: Avaya Aura® Application Enablement Services Port Parameters

AVAYA Application Enablement Services Management Console

Welcome: User cust
Last login: Thu Oct 28 14:28:52 2010 from 192.168.150.3
HostName/IP: AES/192.168.150.103
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Networking | Ports [Home](#) | [Help](#) | [Logout](#)

Ports

CVLAN Ports

| | | | Enabled | Disabled |
|----------------------|-----------------------------------|--|----------------------------------|-----------------------|
| Unencrypted TCP Port | 9999 | | <input checked="" type="radio"/> | <input type="radio"/> |
| Encrypted TCP Port | <input type="text" value="9998"/> | | <input checked="" type="radio"/> | <input type="radio"/> |

DLG Port

| | | | Enabled | Disabled |
|----------|------|--|----------------------------------|-----------------------|
| TCP Port | 5678 | | <input checked="" type="radio"/> | <input type="radio"/> |

TSAPI Ports

| | | | Enabled | Disabled |
|-------------------------|-----------------------------------|--|----------------------------------|-----------------------|
| TSAPI Service Port | 450 | | <input checked="" type="radio"/> | <input type="radio"/> |
| Local TLINK Ports | | | | |
| TCP Port Min | 1024 | | | |
| TCP Port Max | 1039 | | | |
| Unencrypted TLINK Ports | | | | |
| TCP Port Min | <input type="text" value="1050"/> | | | |
| TCP Port Max | <input type="text" value="1065"/> | | | |
| Encrypted TLINK Ports | | | | |
| TCP Port Min | <input type="text" value="1066"/> | | | |
| TCP Port Max | <input type="text" value="1081"/> | | | |

DMCC Server Ports

| | | | Enabled | Disabled |
|------------------|-----------------------------------|--|----------------------------------|----------------------------------|
| Unencrypted Port | <input type="text" value="4721"/> | | <input checked="" type="radio"/> | <input type="radio"/> |
| Encrypted Port | <input type="text" value="4722"/> | | <input checked="" type="radio"/> | <input type="radio"/> |
| TR/87 Port | <input type="text" value="4723"/> | | <input type="radio"/> | <input checked="" type="radio"/> |

Figure 20: Avaya Aura® Application Enablement Services Port Configuration

6. Configure Retia ReDat Server

Browse to the IP address of the ReDat server from a web browser. Select the desired language from the “Language” drop-down menu, enter the appropriate administrator credentials, and click “Login”.

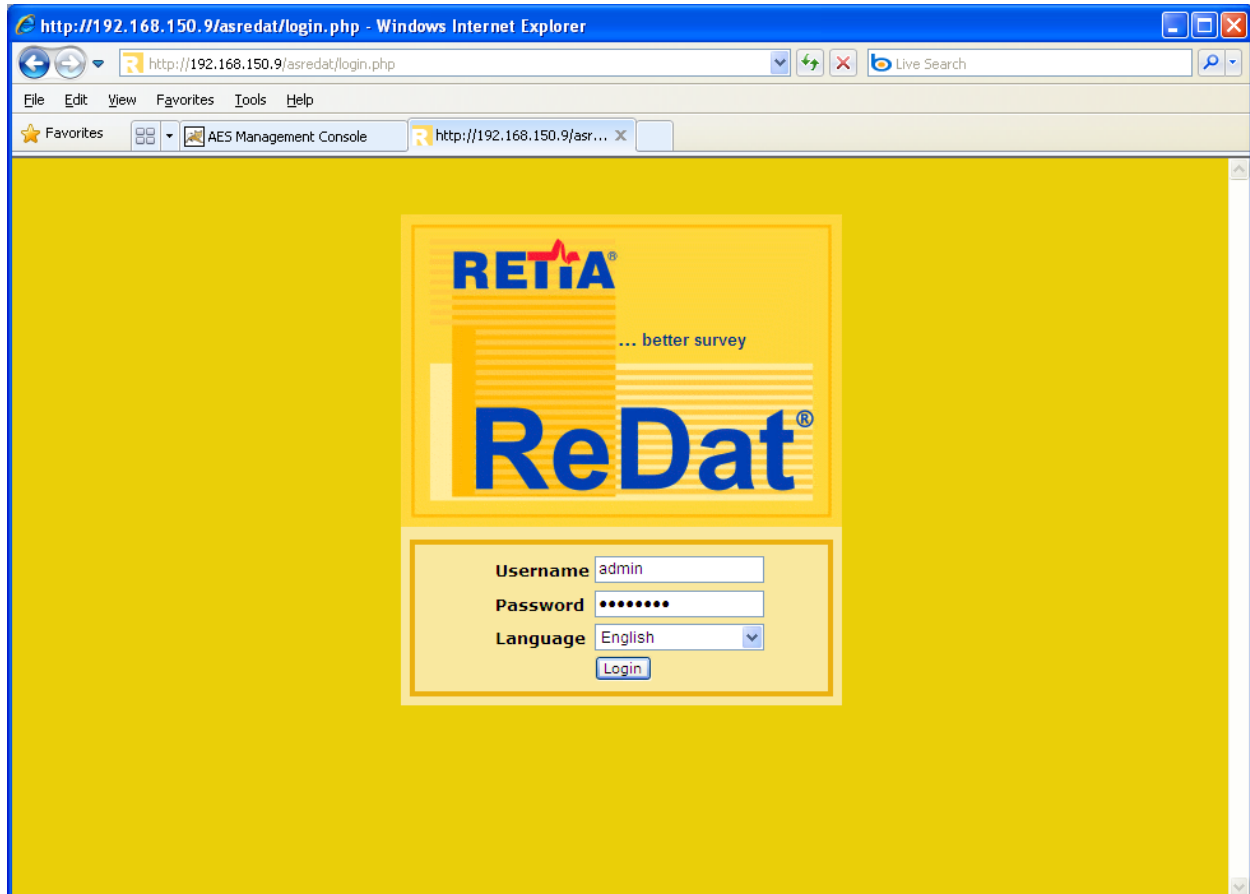


Figure 21: ReDat Login Screen

Select “Configuration”→ “Record units” from the tabs at the top of the screen, as shown below. Click on the “new” icon, which is highlighted.

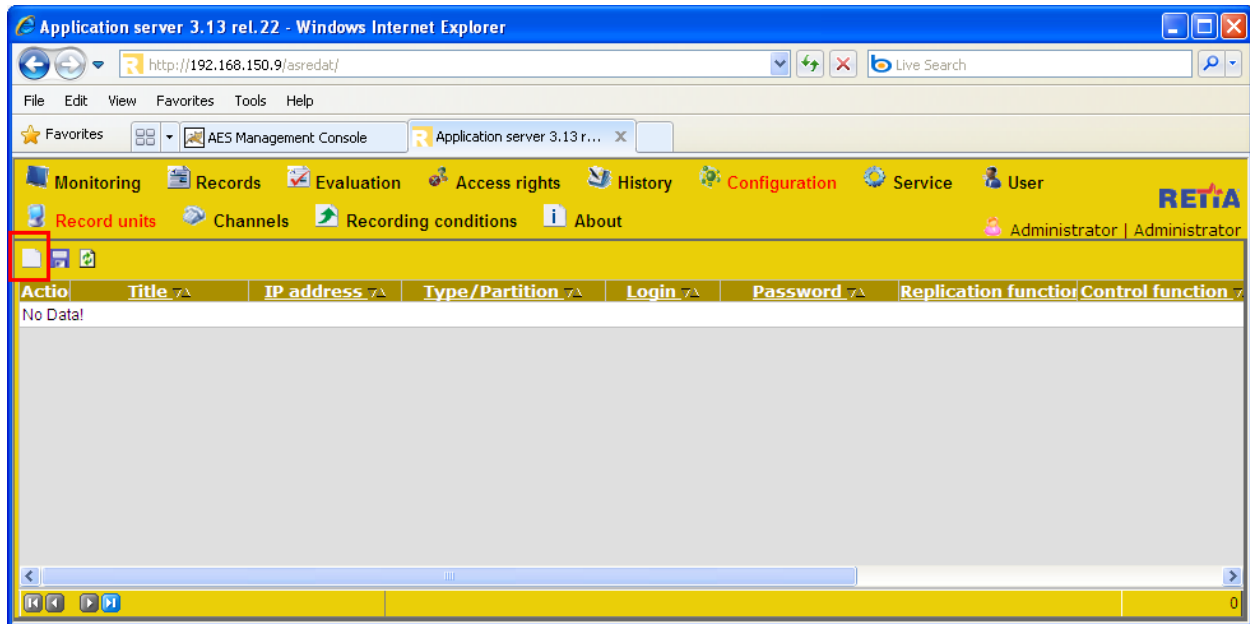


Figure 22: ReDat Record Units Screen

Select each of the empty fields and enter the parameters shown in the following table, then click the highlighted “save” icon.

| Parameter | Usage |
|----------------------|---|
| Title | Enter “localhost”. |
| IP address | Enter “127.0.0.1”. |
| Type/Partition | Select “ReDat VoIP Recorder” from the drop-down menu. |
| Replication function | Select “Database+archiving” from the drop-down menu. |
| Control function | Select “Control+Editing” from the drop-down menu. |
| Secure connection | Unselect this field. |
| Active | Select this field. |

Table 10: ReDat Record Units Parameters

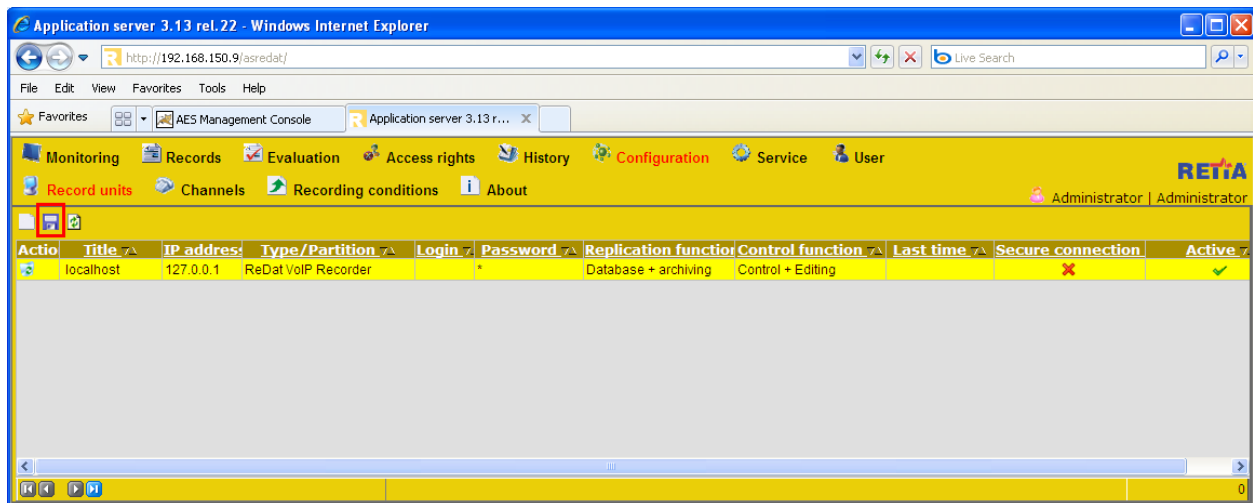


Figure 23: ReDat Completed Record Units Screen

Click “Channels”, select “localhost” from the drop-down “Record unit” menu, and click the “Get” button.

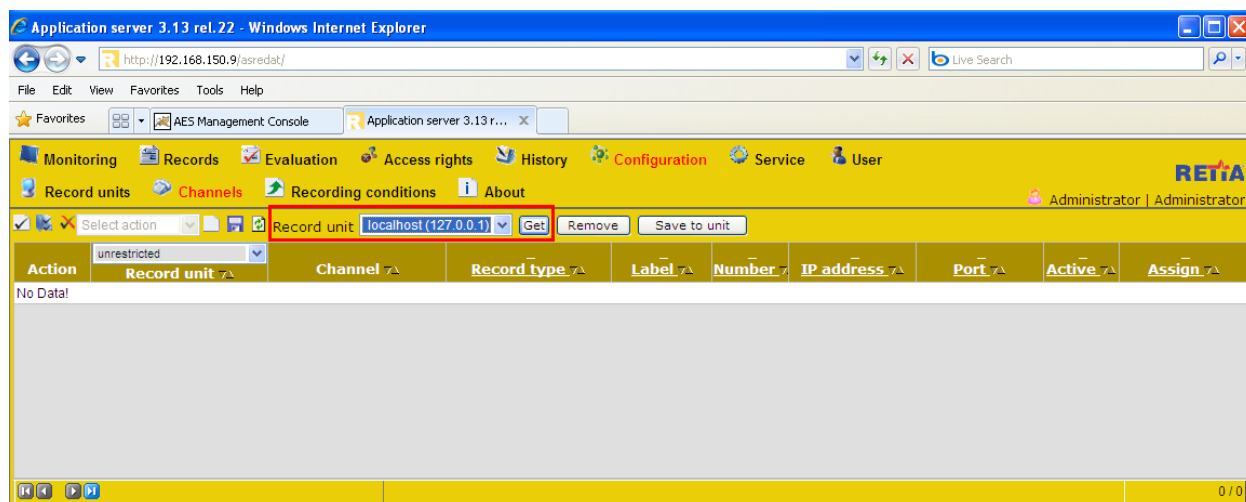


Figure 24: ReDat Channel Selection Screen

The menu is updated to show the recording channels available on the recording unit.

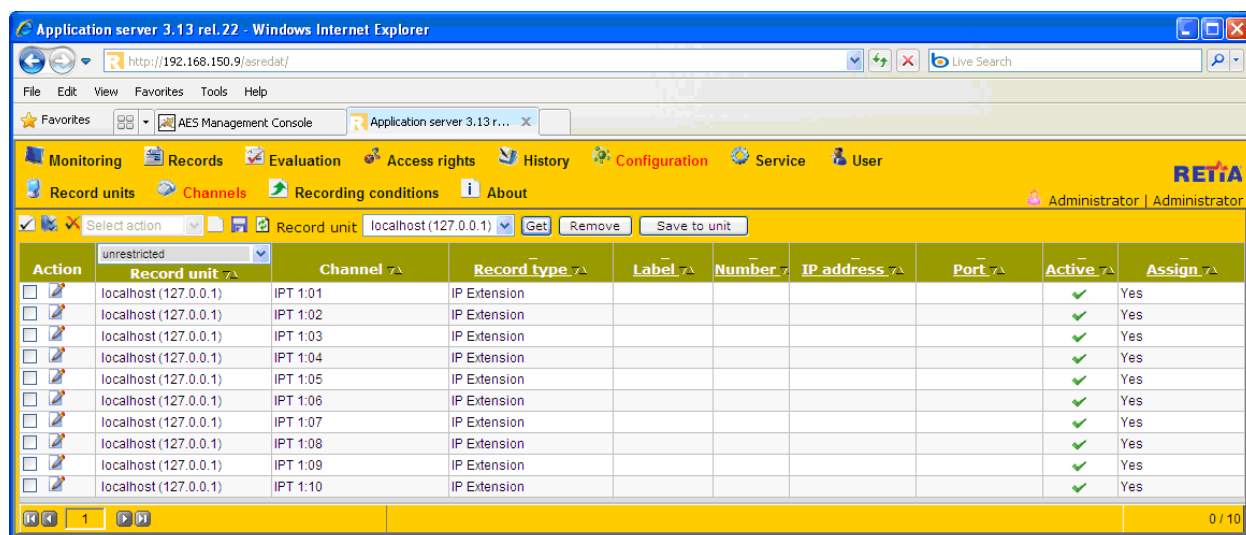


Figure 25: ReDat Available Channels Screen

For each of the CTI Stations shown in **Table 1**, configure one of the available record unit channels using the parameters shown in the following table and then click the “Save” icon.

| Parameter | Usage |
|-------------|--|
| Record type | Select “CTI Controlled” from the drop-down menu. |
| Number | Enter the number of the CTI Station. |
| IP address | Enter the IP address of the ReDat server. |
| Port | Enter a port number from a consecutive series beginning with 40000, with an increment of 2 for each entry. |
| Active | Set the entry to “checked”. |
| Assign | Set the entry to “No”. |

Table 11: ReDat Record Unit Channels Parameters for CTI Stations

For each of the Monitored Stations shown in **Table 1**, configure one of the available record unit channels using the parameters shown in the following table and then click the “Save” icon.

| Parameter | Usage |
|-------------|---|
| Record type | Select “IP Extension” from the drop-down menu. |
| Label | Enter a descriptive name to identify the extension. |
| Number | Enter the number of the extension to be monitored. |
| Active | Set the entry to “checked”. |
| Assign | Set the entry to “Yes”. |

Table 12: ReDat Record Unit Channels Parameters for Monitored Extensions

| Action | Record unit | Channel | Record type | Label | Number | Password | IP address | Port | Active | Record | Priority | Assign |
|--------------------------|-------------------|----------|----------------|-------|--------|----------|----------------|-------|--------|--------|----------|--------|
| <input type="checkbox"/> | | | CTI Controlled | | 11403 | * | 192.168.150.12 | 40004 | ✓ | Always | No | No |
| <input type="checkbox"/> | | | CTI Controlled | | 11402 | * | 192.168.150.12 | 40002 | ✓ | Always | No | No |
| <input type="checkbox"/> | | | IP Extension | A | 10094 | * | | | ✓ | Always | No | Yes |
| <input type="checkbox"/> | | | CTI Controlled | | 11401 | * | 192.168.150.12 | 40000 | ✓ | Always | No | No |
| <input type="checkbox"/> | | | IP Extension | C | 10183 | * | | | ✓ | Always | No | Yes |
| <input type="checkbox"/> | | | IP Extension | E | 10001 | * | | | ✓ | Always | No | Yes |
| <input type="checkbox"/> | Local (127.0.0.1) | IPT 1:01 | CTI Controlled | | | | | | ✓ | Always | No | No |
| <input type="checkbox"/> | Local (127.0.0.1) | IPT 1:02 | CTI Controlled | | | | | | ✓ | Always | No | No |
| <input type="checkbox"/> | Local (127.0.0.1) | IPT 1:03 | CTI Controlled | | | | | | ✓ | Always | No | No |

Figure 26: ReDat Channels configuration

Click “Service” and “CTI” from the tabs at the top of the screen, and enter the parameters shown in the following table.

| Parameter | Usage |
|-----------------------|---|
| AES ip address | Enter the IP address of the AES server. |
| Secure connection | Select “Yes” from the drop-down menu. |
| Username / Password | Enter the user credentials configured in Figure 18 . |
| IP address CM or CLAN | Enter the IP address of the CM Processor Ethernet interface. |
| Device password | Enter the password assigned to stations in Section 4.3 . |
| Recording type | Select “Single step conference” from the drop-down menu. |

Table 13: ReDat CTI Service Parameters

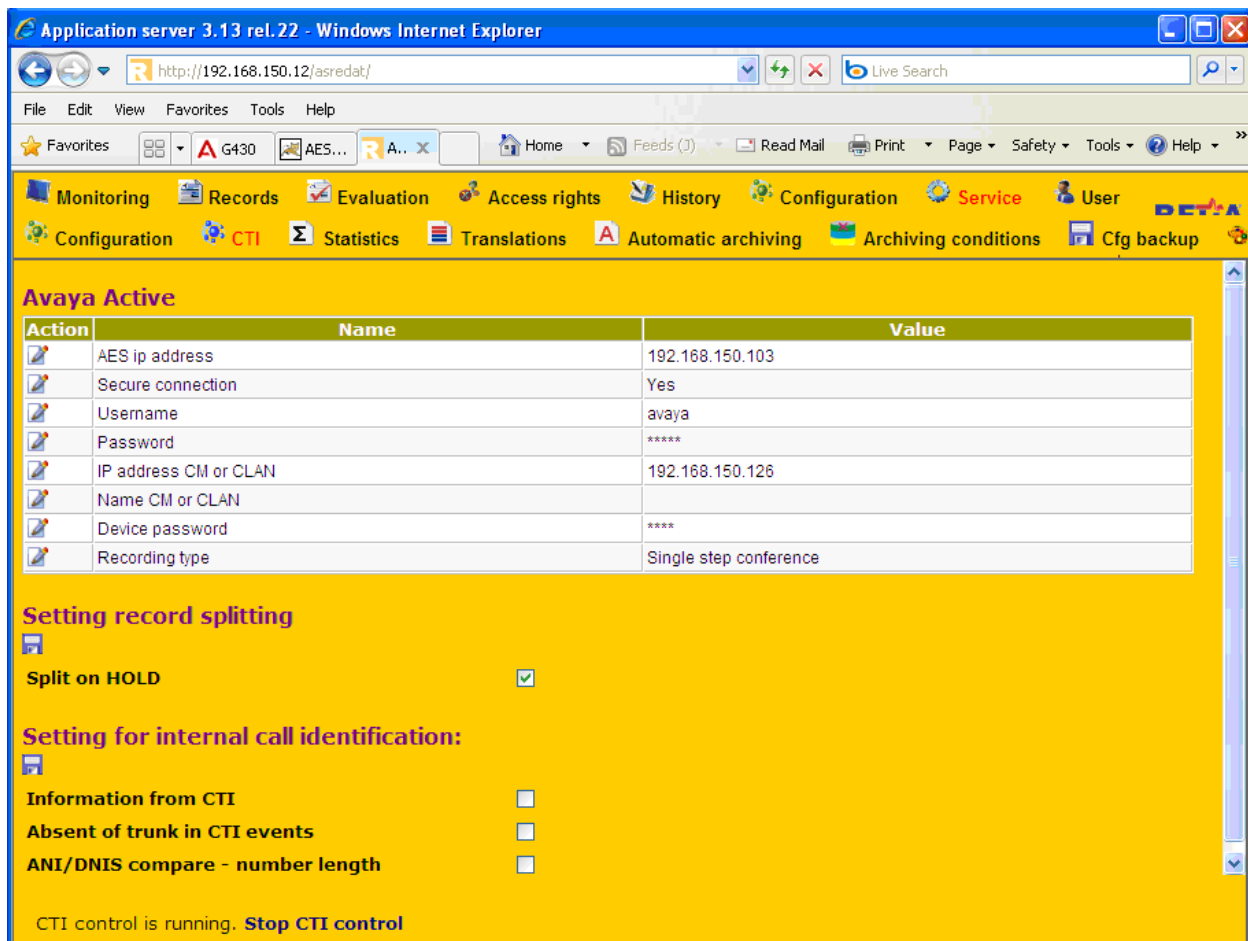


Figure 27: ReDat CTI Service Screen

7. General Test Approach and Test Results

The compliance testing done between Retia ReDat and Avaya Aura® 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:

- Avaya Aura® Communication Manager was configured to support various local IP telephones, as well as a networked PBX connection, and a PSTN connection.
- An E1 PSTN interface was attached to Avaya Aura® Communication Manager.
- The Retia ReDat was configured to monitor various telephones attached to Avaya Aura® Communication Manager.
- The major Retia 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
 - Telephones attached to the PSTN via the E1 trunk.
 - Telephones attached to a networked PBX via the QSIG trunk.

The tests which were performed are shown in **Section 1.1**. All tests which were performed produced the expected result.

8. Verification Steps

The correct installation and configuration of Retia ReDat voice recorder can be verified by performing the following steps using the Avaya Aura® Application Enablement Services administrative web interface:

- Login to Avaya Aura® Application Enablement Services, and navigate to the **AE Services** screen. Verify that the DMCC Service is licensed, ONLINE, and Running.

AVAYA Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Nov 15 09:37:10 2010 from 192.168.150.3
HostName/IP: AES/192.168.150.103
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

AE Services Home | Help | Logout

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▶ TSAPI
- ▶ 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 5.0

© 2009 Avaya, Inc. All Rights Reserved.

Figure 28: Avaya Aura® Application Enablement Services AE Services Screen

- Navigate to **Status -> Status and Control -> Switch Conn Summary** select the PBX 1, and click “Switch Connection Details”. Verify that the connection state is “Online” and “Talking”.

AVAYA Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Nov 15 09:37:10 2010 from 192.168.150.3
HostName/IP: AES/192.168.150.103
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

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

Navigation Menu:

- AE Services
- Communication Manager Interface
- Licensing
- Maintenance
- Networking
- Security
- Status**
 - Alarm Viewer
 - Logs
 - Status and Control**
 - CVLAN Service Summary
 - DLG Services Summary
 - DMCC Service Summary
 - Switch Conn Summary**
 - TSAPI Service Summary
 - User Management
 - Utilities
 - Help

Switch Connections Summary

☐ Enable page refresh every 60 seconds

| Switch Conn | Conn State | Since | Online/Offline | Active/Admin'd AEP Conns | Num of TCI Conns | SSL | Msgs To Switch | Msgs From Switch | Msg Period |
|-------------|------------|--------------------------|----------------|--------------------------|------------------|---------|----------------|------------------|------------|
| Evolution | Talking | Mon Nov 15 15:52:44 2010 | Online | 1 / 1 | 2 | Enabled | 696 | 768 | 30 |

Buttons: Online Offline Connection Details Per Service Connections Details

Figure 29: Avaya Aura® Application Enablement Services Switch Connections Summary Screen

- Navigate to **Status -> Status and Control -> DMCC Service Summary** and click “Service Summary”. Verify that the Retia ReDat system has established a session.

The screenshot shows the AVAYA Application Enablement Services Management Console in a Windows Internet Explorer browser. The address bar shows the URL: <https://192.168.150.103/aesvcs/view/statcntrl/sessionSummPage.xhtml?cid=>. The page title is "AVAYA Application Enablement Services Management Console". The navigation bar includes "Status | Status and Control | DMCC Service Summary" and "Home | Help | Logout". The left sidebar shows the "Status" menu expanded, with "Status and Control" selected. The main content area displays the "DMCC Service Summary - Session Summary" page. It includes a checkbox for "Enable page refresh every 60 seconds" and a "Session Summary" link. The session summary text indicates it was generated on Mon Nov 15 16:19:18 CET 2010, with a service uptime of 5 days, 2 hours, and 8 minutes. It also lists the number of active sessions (1), sessions created since service boot (64), existing devices (6), and devices created since service boot (316). A table shows the session details for a specific session ID (2FA0288BEFC20B378, 80D716F2F5E40A4-66) with user 'avaya', application 'Retia Cti Avaya active', far-end identifier '192.168.150.12', connection type 'XML Encrypted', and 6 associated devices. Buttons for "Terminate Sessions" and "Show Terminated Sessions" are present. The page indicates "Item 1-1 of 1".

Figure 30: DMCC Service Summary – Session Summary Screen

- Navigate to **Status -> Status and Control -> DMCC Service Summary** and click “Device Summary”. Verify that the Retia ReDat system has registered each of the CTI stations.

AVAYA Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Nov 15 09:37:10 2010 from 192.168.150.3
HostName/IP: AES/192.168.150.103
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Status | Status and Control | DMCC Service Summary [Home](#) [Help](#) [Logout](#)

DMCC Service Summary - Device Summary

☐ Enable page refresh every seconds

Session Summary Device Summary
Generated on Mon Nov 15 16:18:15 CET 2010

Service Uptime: 5 days, 2 hours and 7 minutes
Number of Active Sessions: 1
Number of Sessions Created Since Service Boot: 64
Number of Existing Devices: 6
Number of Devices Created Since Service Boot: 316

| | Device ID | State | Associated Sessions |
|--------------------------|-----------------------------------|------------|---------------------|
| <input type="checkbox"/> | 10001:Evolution:192.168.150.126:0 | IDLE | 1 |
| <input type="checkbox"/> | 10094:Evolution:192.168.150.126:0 | IDLE | 1 |
| <input type="checkbox"/> | 10183:Evolution:192.168.150.126:0 | IDLE | 1 |
| <input type="checkbox"/> | 11401:Evolution:192.168.150.126:0 | REGISTERED | 1 |
| <input type="checkbox"/> | 11402:Evolution:192.168.150.126:0 | REGISTERED | 1 |
| <input type="checkbox"/> | 11403:Evolution:192.168.150.126:0 | REGISTERED | 1 |

[Terminate Devices](#)
Item 1-6 of 6

Figure 31: DMCC Service Summary - Device Summary Screen

Log in to the ReDat configuration interface as shown in **Figure 21**, and navigate to “monitoring” → “Channels”. Initiate a call between monitored endpoints and verify that the entry in the “Record” column changes to an upward-pointing green arrow, as shown in the following figure.

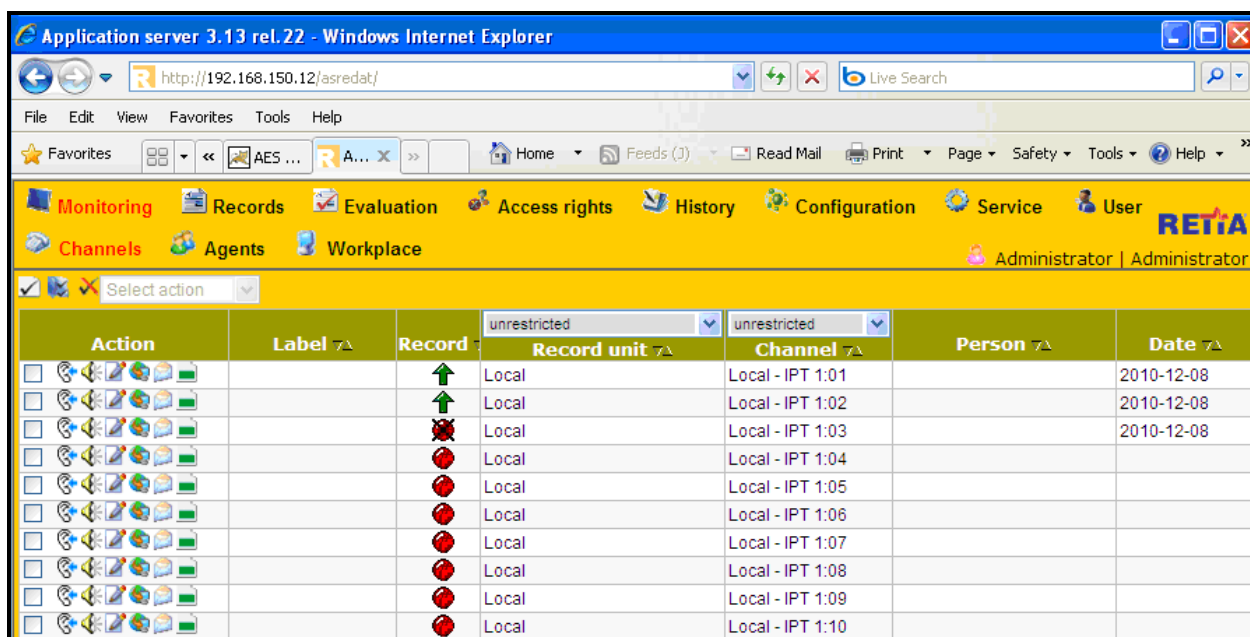


Figure 32: ReDat Channel Status Screen

9. References

- [1] *Administering Avaya Aura® Communication Manager*, May 2009, Document Number 03-300509.
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, May 2009, Issue 7, Document Number 555-245-205.
- [3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, November 2009, Document Number 02-300357
- [4] Retia product descriptions: <http://www.redat.cz/en/products-and-services/>

10. Conclusion

These Application Notes describe the compliance testing of the Retia ReDat recording system with Avaya Aura® Communication Manager. Silent monitoring via the Single Step Conference recording method offered by the ReDat system was tested. A detailed description of the configuration required for both the Avaya and the Retia equipment is documented within these Application Notes. The ReDat system passed all of the tests performed, which included both functional and robustness tests.

©2011 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.