Avaya Solution & Interoperability Test Lab

Application Notes for Retia ReDat Recording System with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services Using Multiple Registrations – 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 the Avaya Aura® Application Enablement Services (AES) Device, Media, and Call Control (DMCC) interface and Multiple Registrations 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 Multiple Registrations 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.

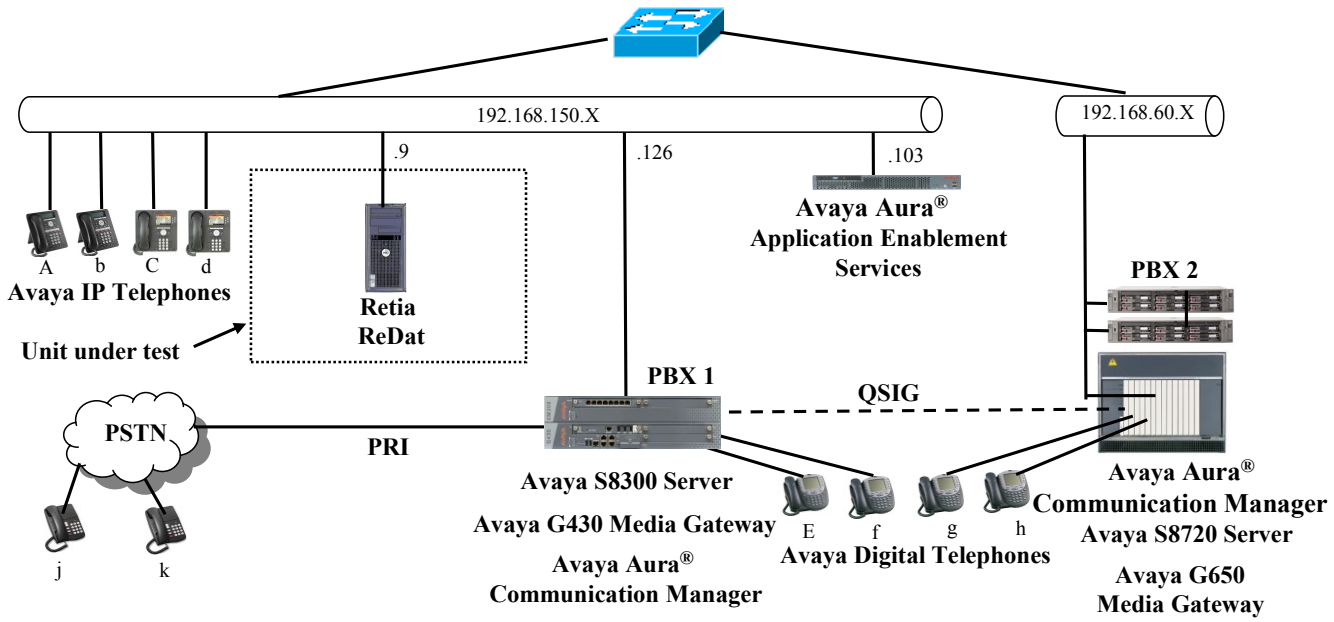

Figure 1: **ReDat Test Configuration**

In the above diagram, the Retia ReDat records voice conversations from telephones attached to PBX 1. The DMCC service provided by Application Enablement Services is used to monitor call activity and capture voice streams associated with PBX 1. The Retia ReDat is connected to the same local area network as PBX 1. 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 uses the Communication Manager Multiple Registrations feature to initiate monitoring for calls which it wishes to record. The voice stream for such calls is received via the LAN interface used to communicate with 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 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 (Phones A & C)	11304

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 Application Enablement Services	5.2.2
Avaya 96xx H.323 Telephones	S3.110b
Avaya 16xx H.323 Telephones	1.3
Avaya 24xx Digital Telephones	Not Applicable
Retia ReDat platform: MS Server 2008	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 the ReDat voice recorder uses to monitor phones and record calls.

The configuration and verification operations illustrated in this section were all performed using the 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 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 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 CLAN interface or Processor Ethernet.
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 18**.
Enabled (Page 4)	Enter "y" to enable the connection.

Table 4: IP Services Parameters

```
change ip-services                                              Page   1 of   4

                                  IP SERVICES
 Service     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        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       Password          Enabled    Status
                  Server
      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 unused 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.
IP SoftPhone	This value must be set for all stations which are to be monitored via the Multiple Registrations method.
Multimedia mode (page 2)	This value must be set to "enhanced" for all stations which are to be monitored via the Multiple Registrations method.

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? y

                                               IP Video Softphone? n


                                              Customizable Labels? y
```

Figure 7: IP Station Screen, Page 1

```
add station 10183                                          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: disabled
        Multimedia Mode: enhanced
    MWI Served User Type:                        Display Client Redirection? n
             AUDIX Name:                        Select Last Used Appearance? n
                                                  Coverage After Forwarding? s

 Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? y
  Emergency Location Ext: 10183         Always Use? n IP Audio Hairpinning? n
```

Figure 8: IP Station Screen, Page 2

4.3.2. TDM 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 (page 1)	Use an unused 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.
Security Code (page 1)	Enter an appropriate numeric string to be used as a security code.
IP SoftPhone (page 1)	This value must be set for all stations which are to be monitored via the Multiple Registrations method.
Multimedia mode (page 2)	This value must be set to "enhanced" for all stations which are to be monitored via the Multiple Registrations method.

Table 6: Configuration IP Stations

```
add station 10001                                          Page   1 of   5
                                     STATION

Extension: 10001                        Lock Messages? n               BCC: 0
     Type: 2410                         Security Code: 123456           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? y
                                              Remote Office Phone? n
                                               IP Video Softphone? n


                                              Customizable Labels? y
```

Figure 9: TDM Station Screen, Page 1

```
add station 10001                                          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
    MWI Served User Type:                        Display Client Redirection? n
             AUDIX Name:                        Select Last Used Appearance? n
                                                  Coverage After Forwarding? s

 Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? y
  Emergency Location Ext: 10001         Always Use? n IP Audio Hairpinning? n
```

Figure 10: TDM Station Screen, Page 2

4.4. Configure Hunt Group

Use the **add hunt-group** command to create a hunt group which is used to test the ability of ReDat 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 which are monitored by ReDat.

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 3)	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                                                Page   1 of  60
                                   HUNT GROUP

            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 11: Hunt Group Screen, Page 1

```
add hunt-group 3                                                Page   3 of  60
                                   HUNT GROUP
         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           Name(19 characters)
   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 12: Hunt Group Screen, Page 3

5. Configure Avaya Aura® Application Enablement Services

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

https://<AES server address>/

Click "Continue To Login".

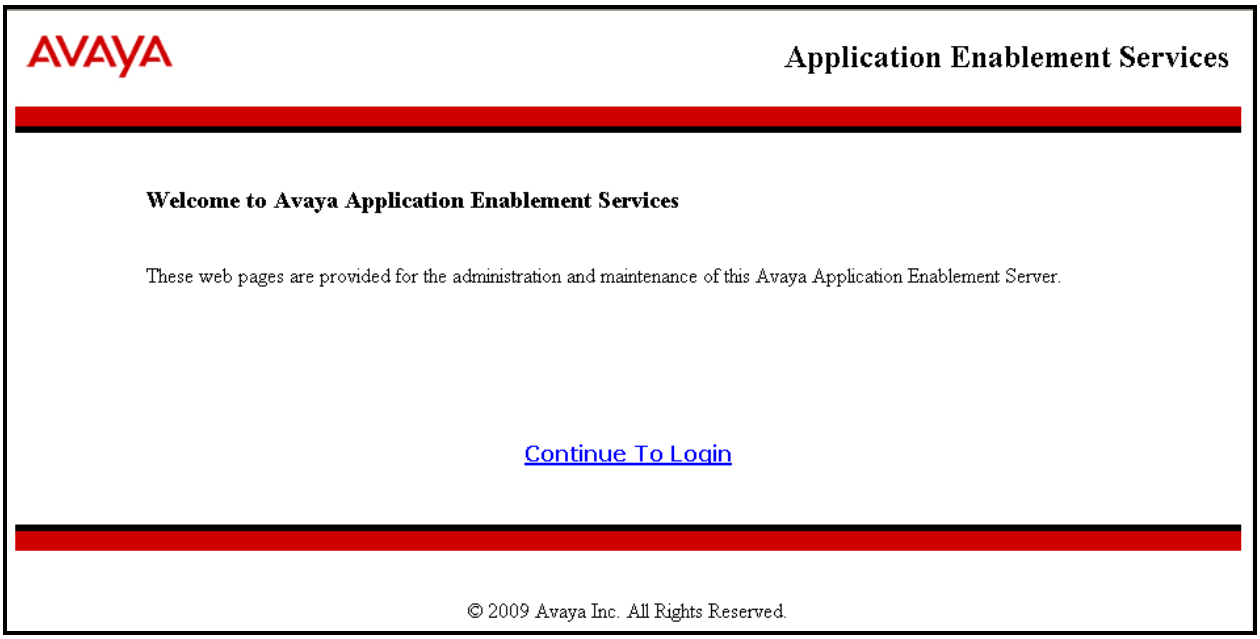

Figure 13: Avaya Application Enablement Services Welcome Screen

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

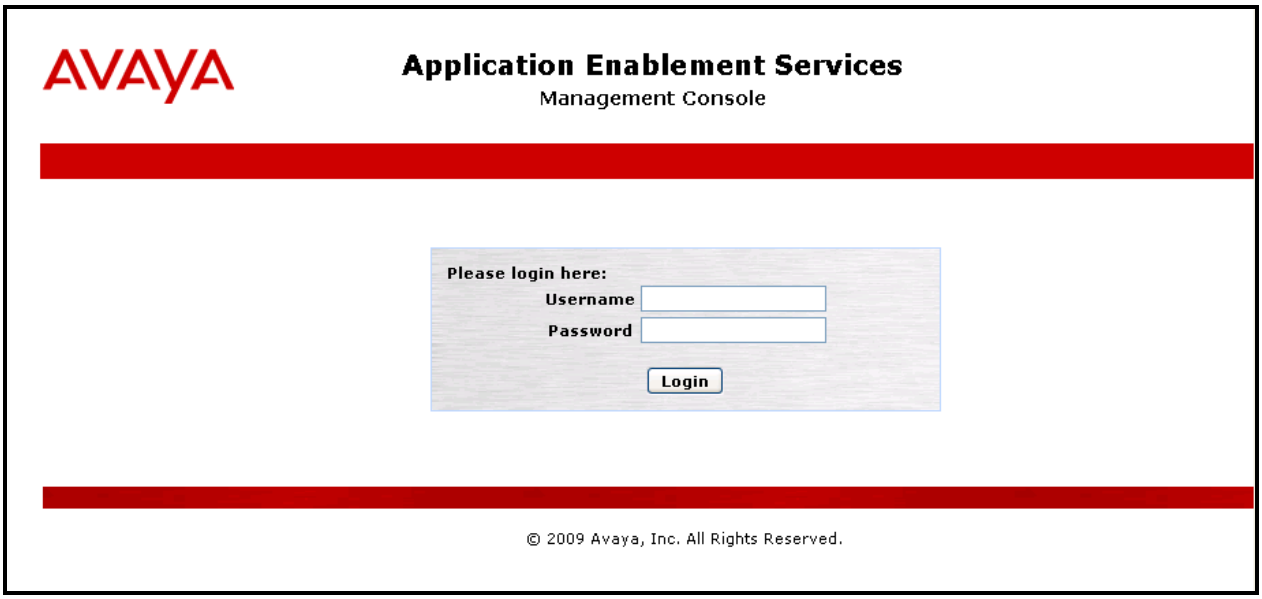

Figure 14: Application Enablement Services Login Screen

Click "AE Services" in left frame.

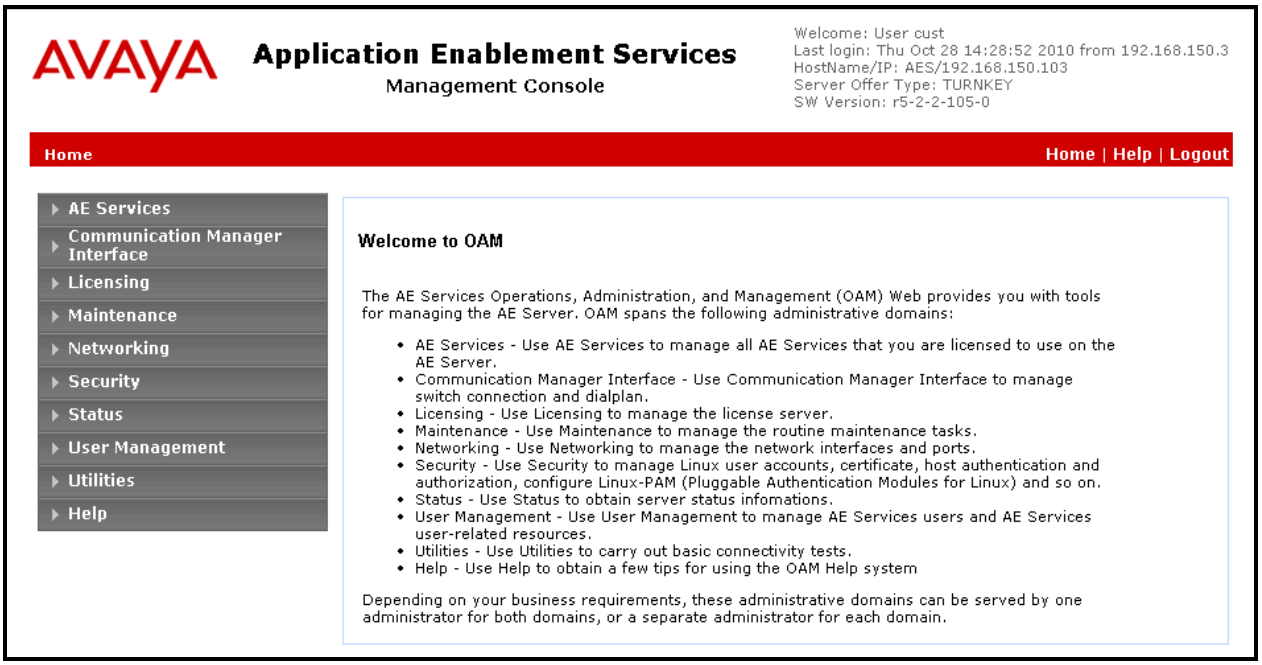

Figure 15: Application Enablement Services Main Screen

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

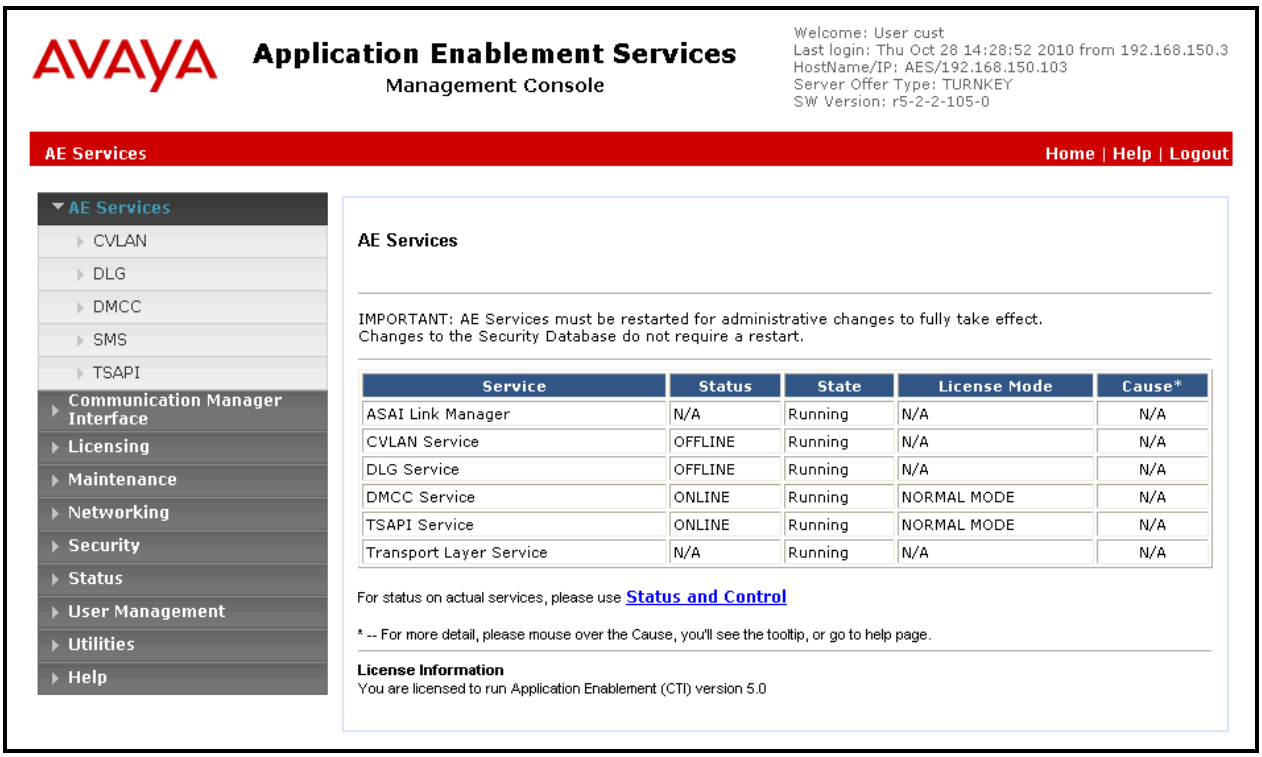

Figure 16: Application Enablement Services Top Level Screen

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 in **Section 6.**

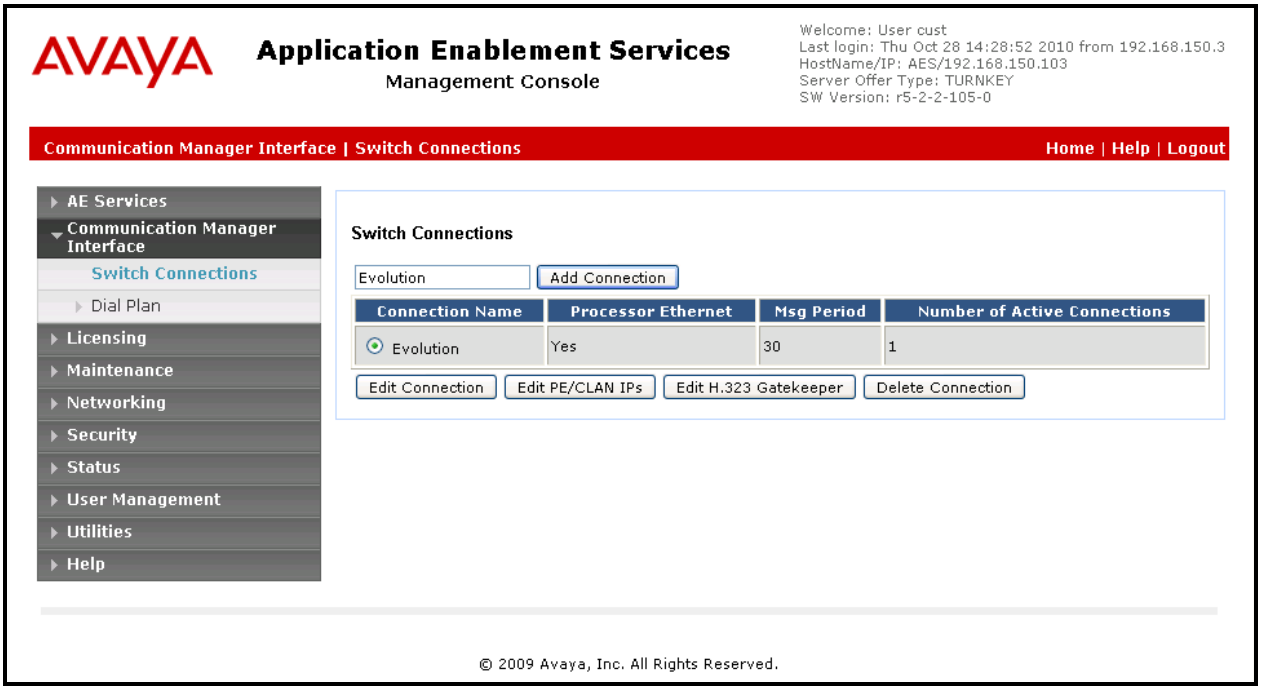

Figure 17: Switch Connection Screen

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 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 if a Processor Ethernet is being used.

Table 8: Configuration of Switch Password

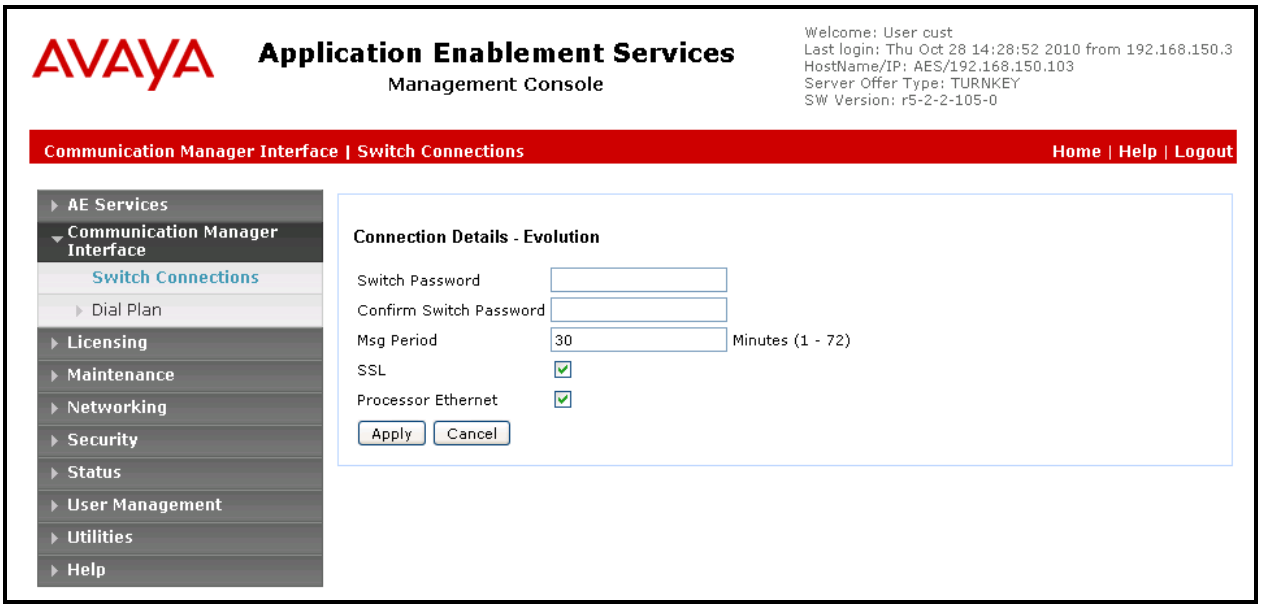

Figure 18: Set Switch Password Screen

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 Application Enablement Services will use for communication with the switch, and click the "Add/Edit Name or IP" button.

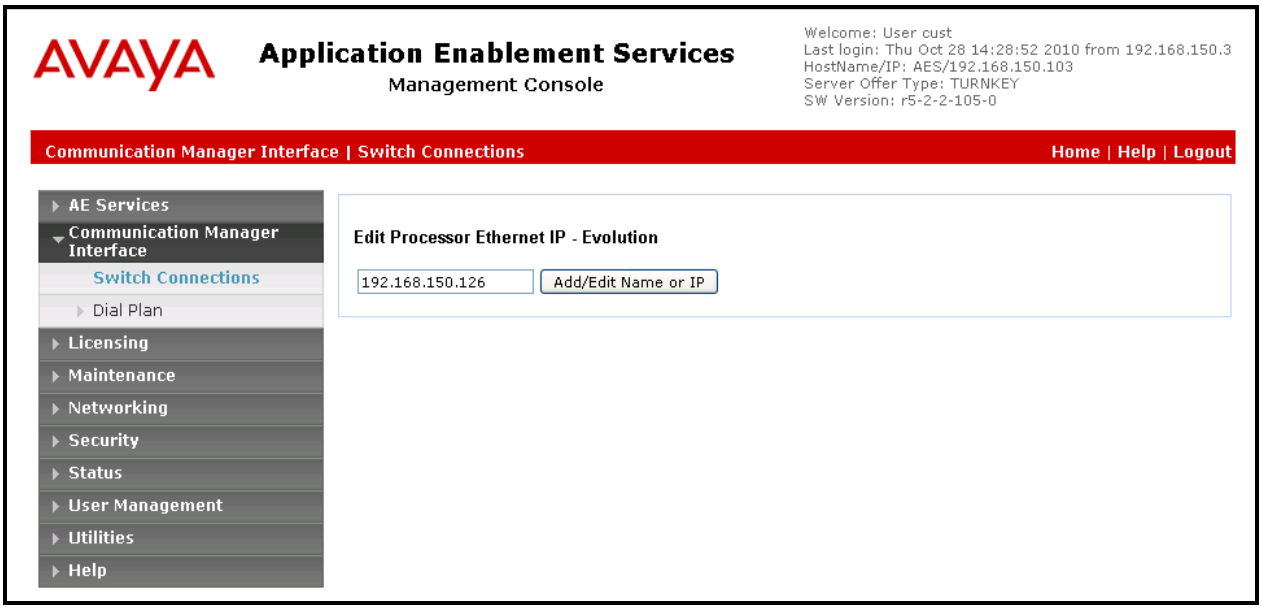

Figure 19: Edit Processor Ethernet IP Screen

Navigate to **User Management→User Admin→Add User**. The "CT User" field for this user must be set to "Yes". In this case, the Application Enablement Services user is the ReDat application, which uses 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**.

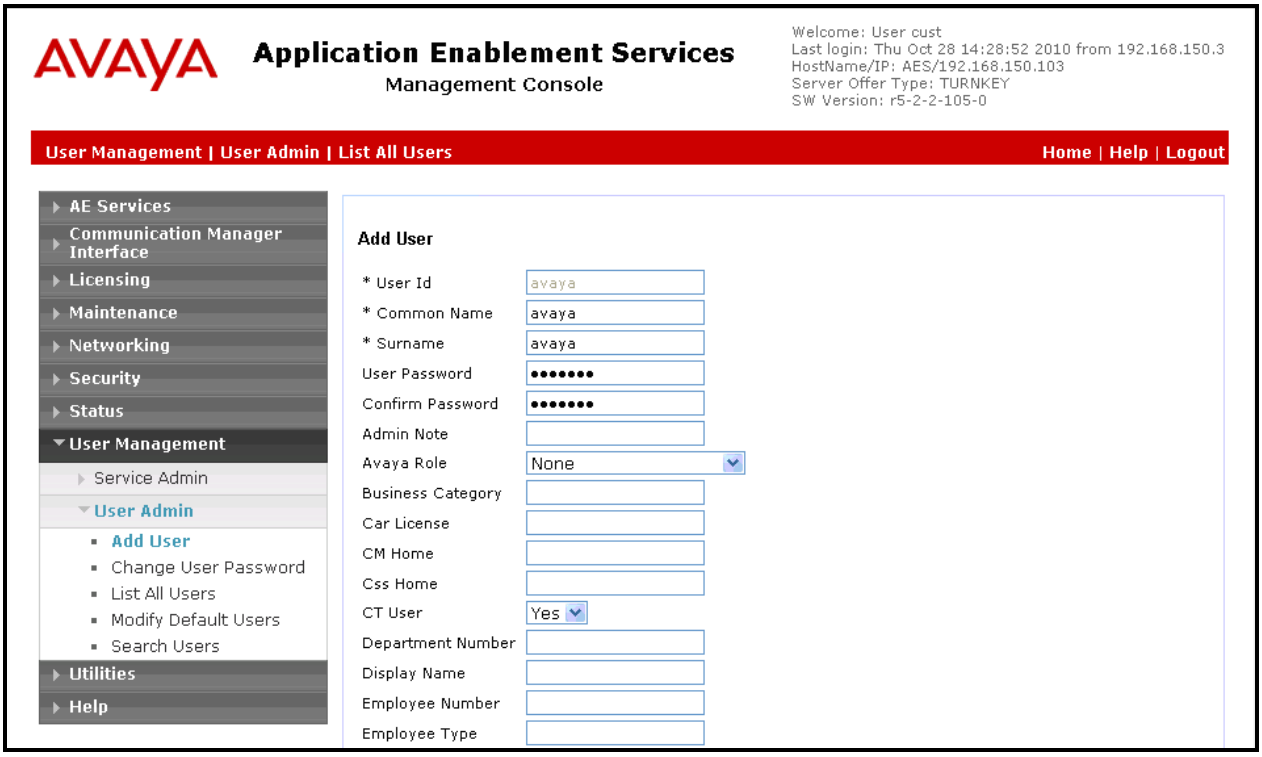

Figure 20: Add User Screen

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".

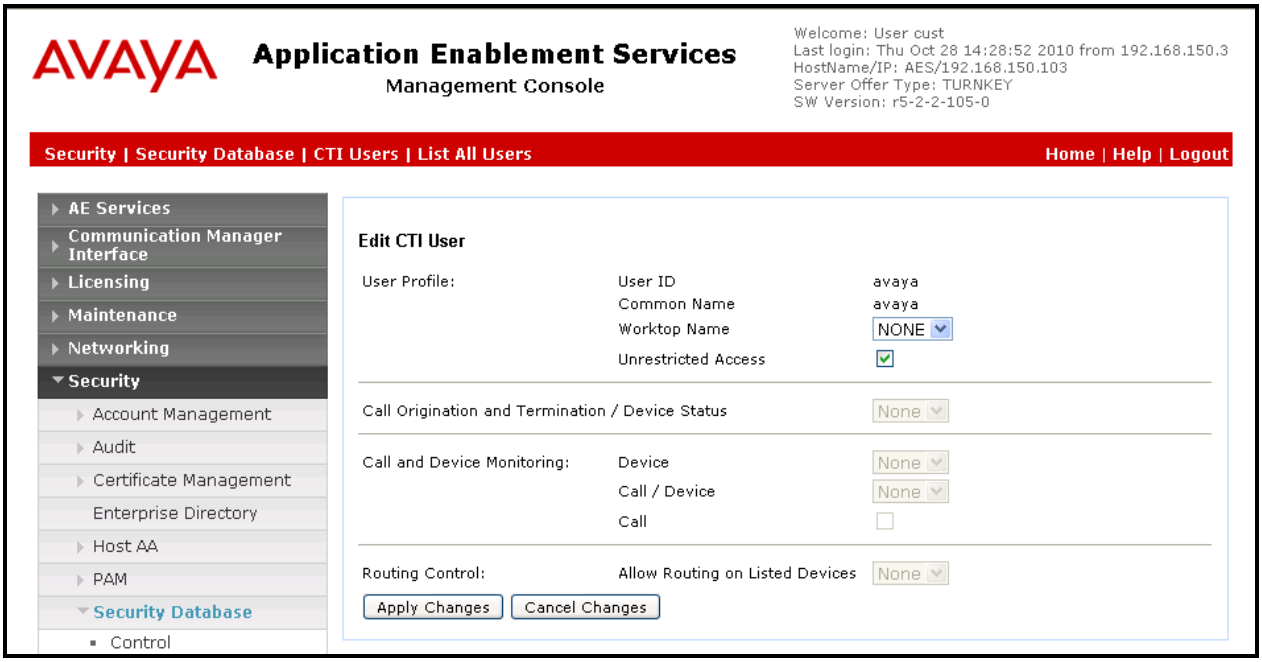

Figure 21: Edit CTI User Screen

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

Parameter	Usage
Unencrypted Port	Enable and set this port to 4721.

Table 9: Avaya Aura® Application Enablement Services Port Parameters

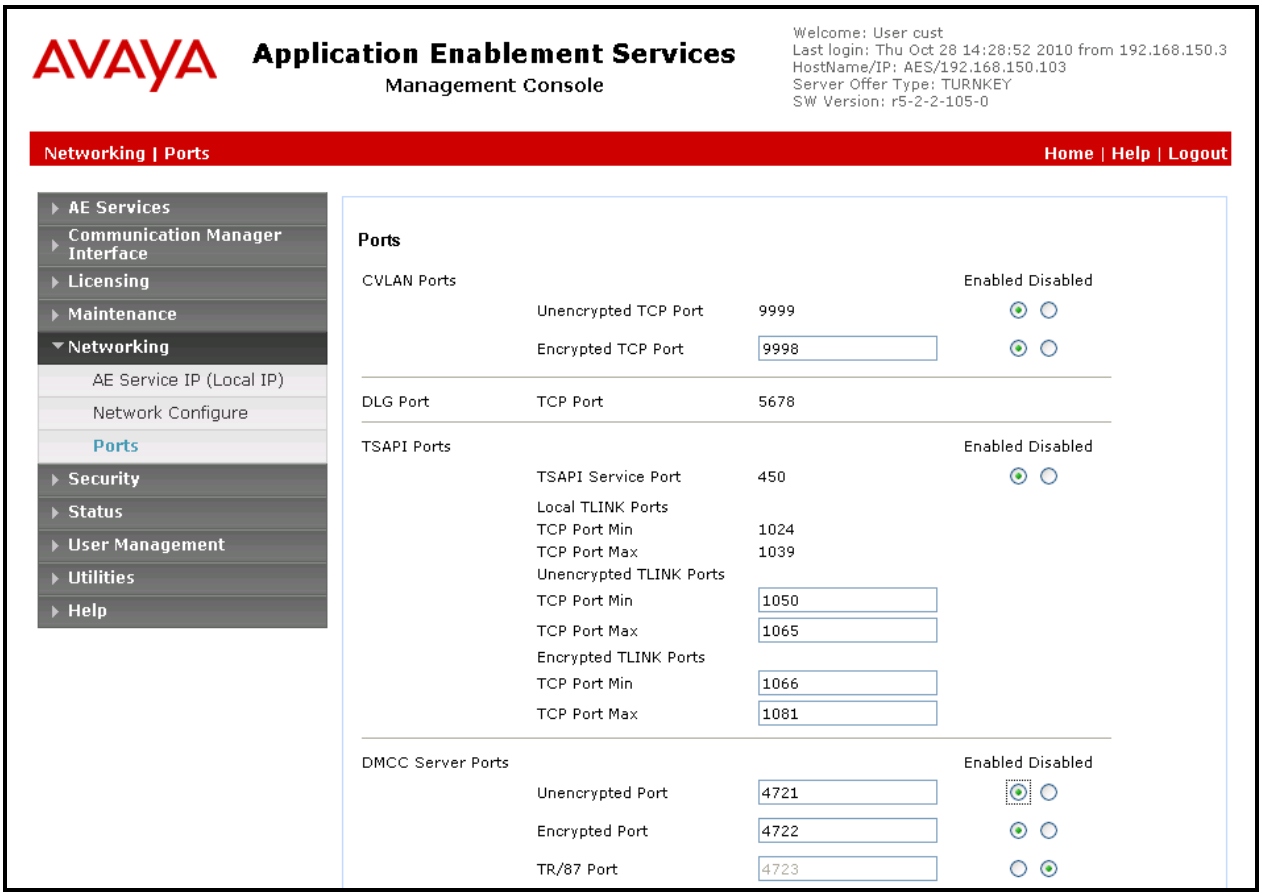

Figure 22: Application Enablement Services Port Configuration

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".

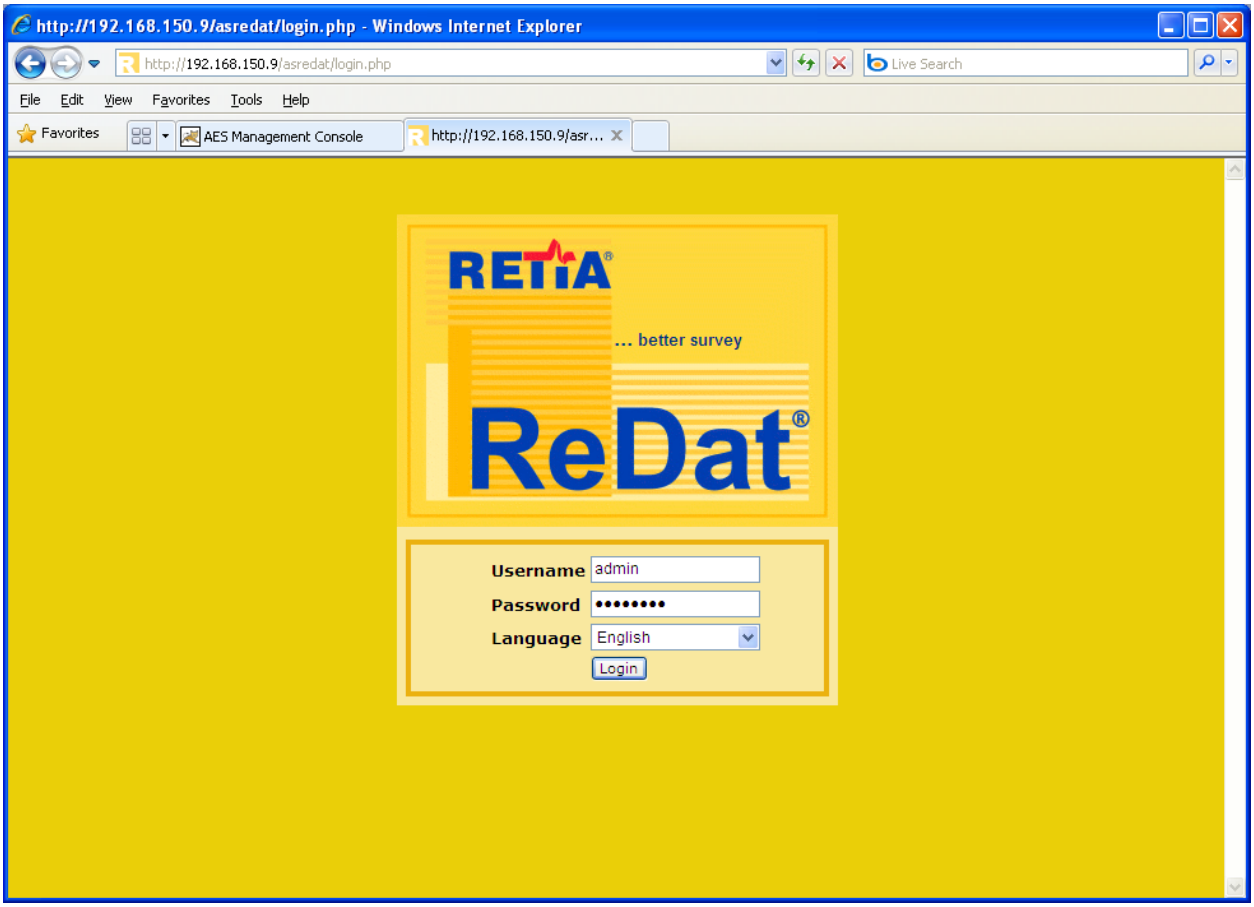

Figure 23: ReDat Login Screen

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

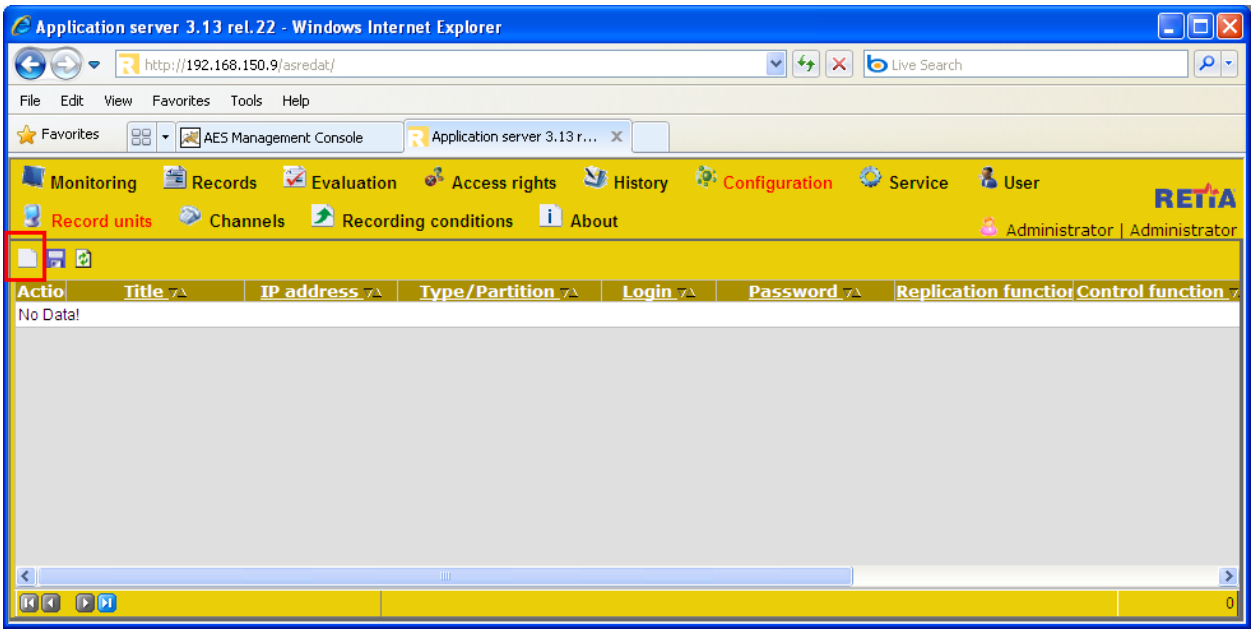

Figure 24: ReDat Record Units Screen

Select each of the empty fields and entering the parameters shown in the following table, and 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

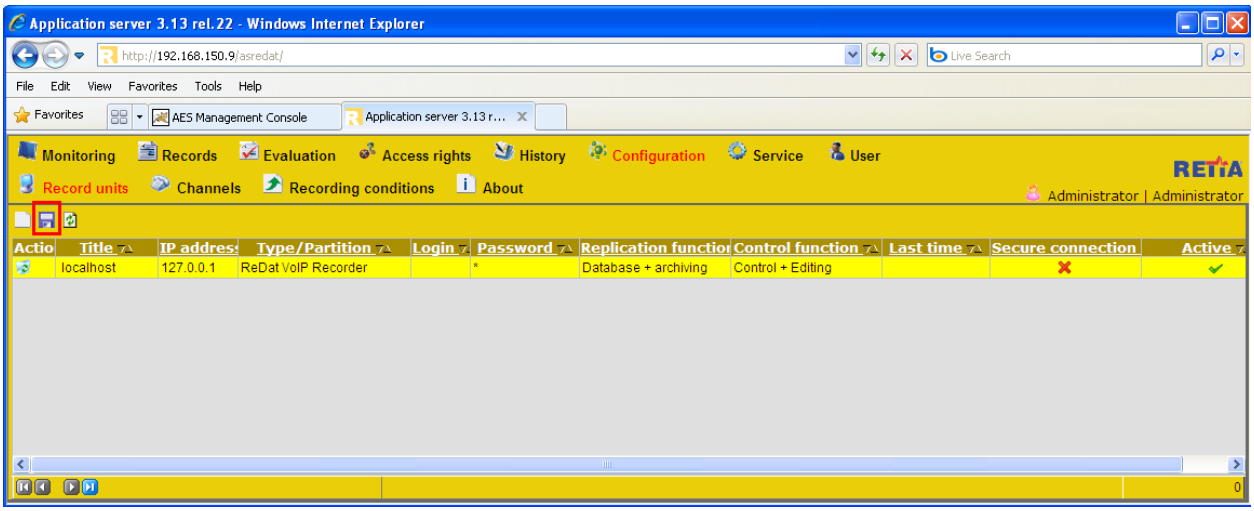

Figure 25: ReDat Completed Record Units Screen

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

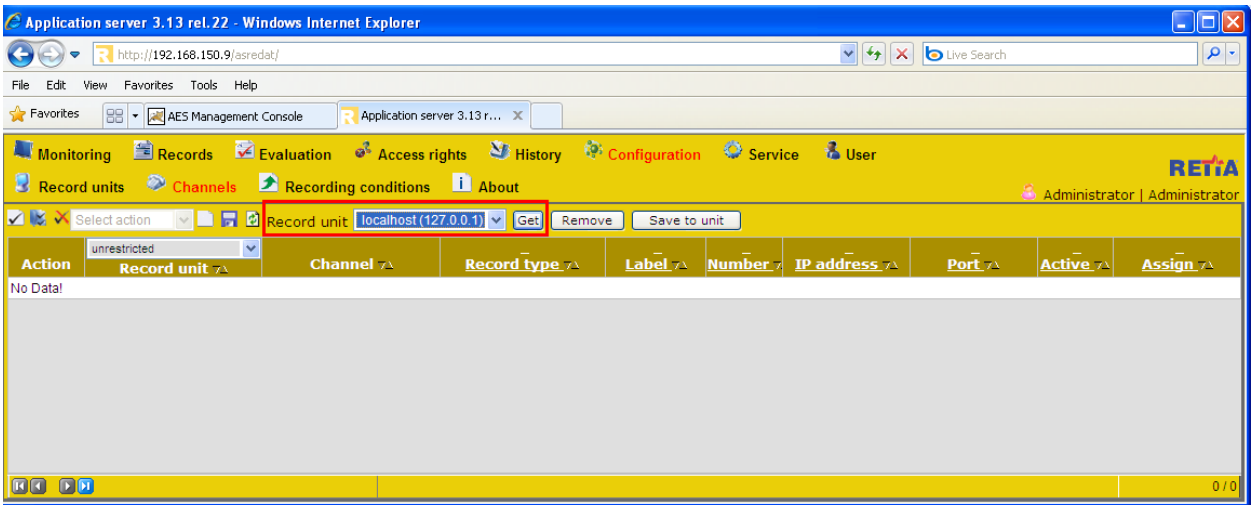

Figure 26: ReDat Channel Selection Screen

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

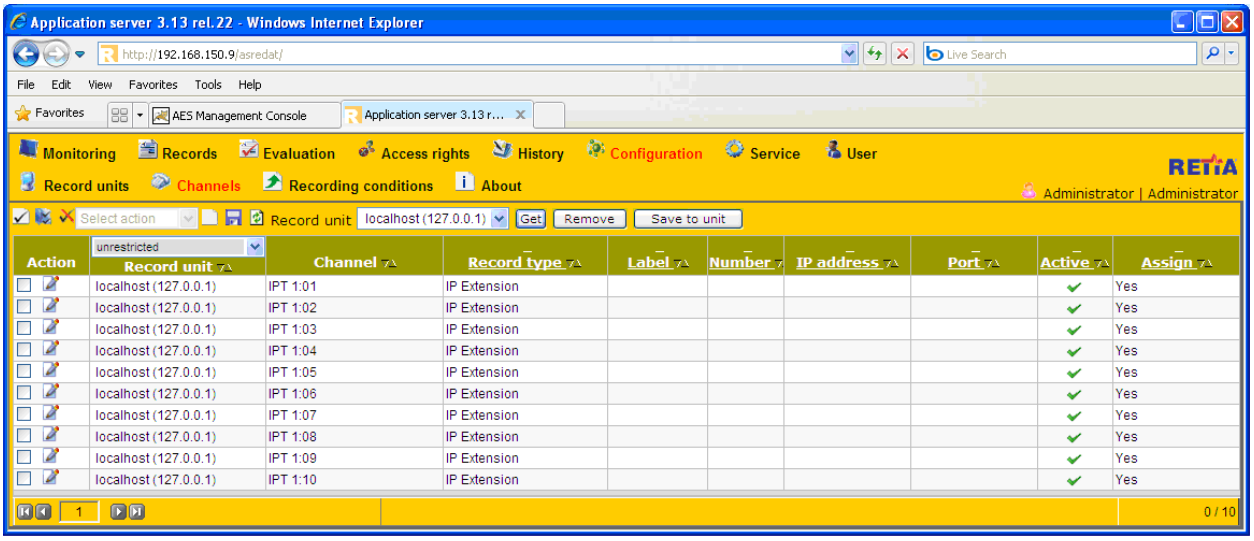

Figure 27: ReDat Available Channels Screen

For each of the extensions to be monitored shown in **Table 1**, enter the parameters shown in the following table and click the "Save" icon and then click "Save to unit" button.

Parameter	Usage
Record type	Select "CTI Controlled" from the drop-down menu.
Label	Enter a descriptive name to identify the extension.
Number	Enter the number of the extension to be monitored.
IP address	Enter the IP address of the ReDat server.
Port	Enter a port number from a consecutive series beginning with 2000, with an increment of 2 for each entry.
Active	Set the entries which correspond to monitored extension to "checked", and the remainder to "unchecked".

Table 11: ReDat Record Units Parameters

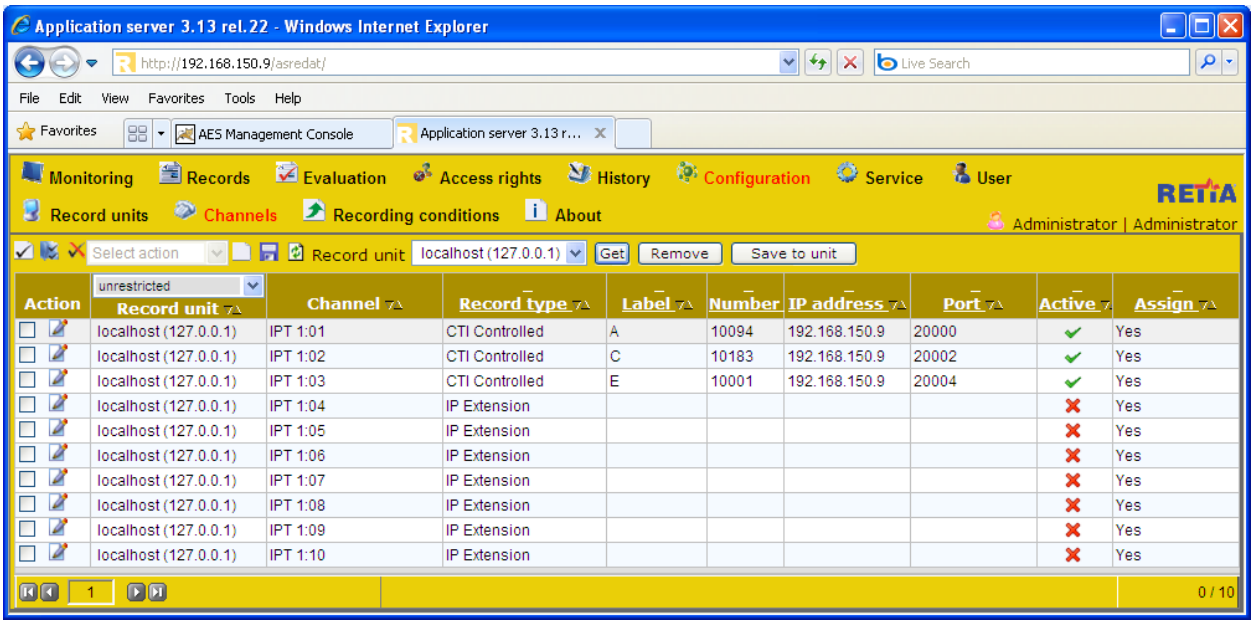

Figure 28: ReDat Configured Channels Screen

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 20.**
IP address CM or CLAN	Enter the IP address of the CM Processor Internet interface.
Device password	Enter the password assigned to stations in **Section 4.3**.
Recording type	Select “Multiple registration” from the drop-down menu.

Table 12: ReDat CTI Service Parameters

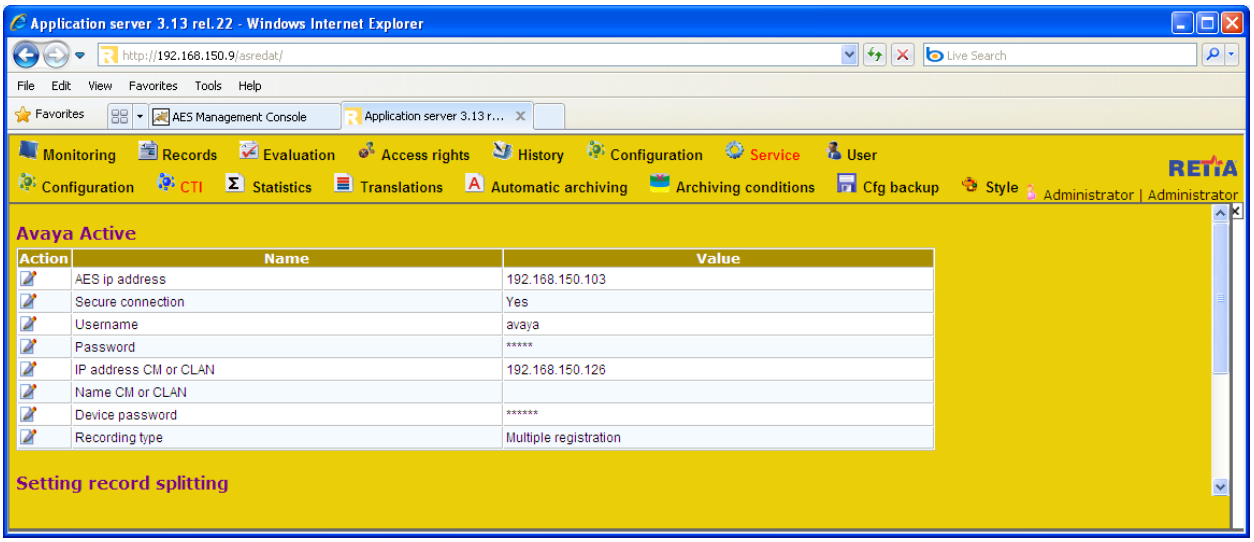

Figure 29: ReDat CTI Service Screen

7. General Test Approach and Test Results

The compliance testing done between Retia ReDat and Communication Manager was performed manually. The functional and robustness tests were done, but 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 E1 trunk.
  - Telephones attached to a networked PBX via QSIG trunk.

The tests which were performed are shown is **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.

- Navigate to **Status →Status and Control→Switch Conn Summary.** Select the PBX 1, and click "Connection Details". Verify that the connection state is "Online" and "Talking".

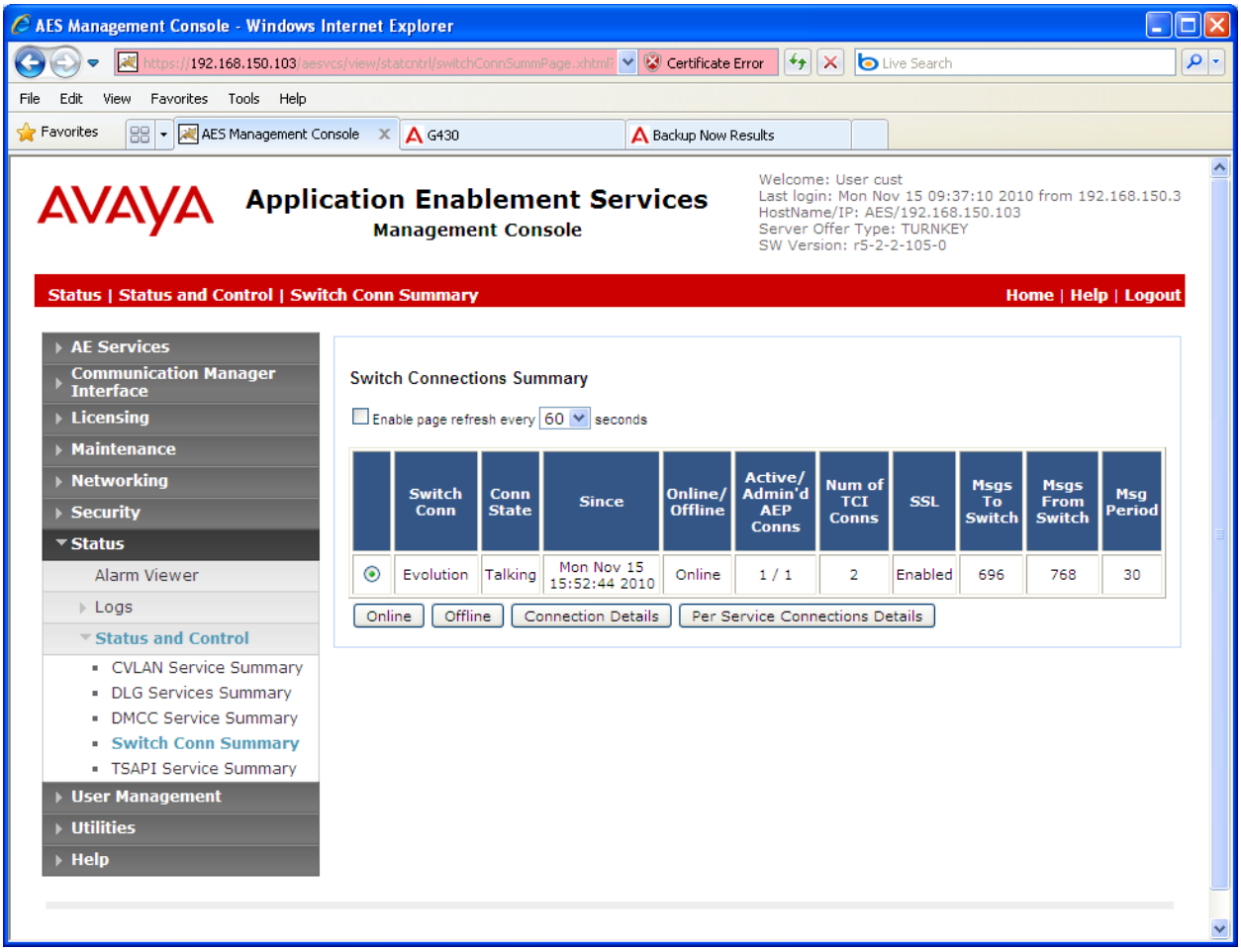

Figure 30: Application Enablement Services Switch Connection Details Screen

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

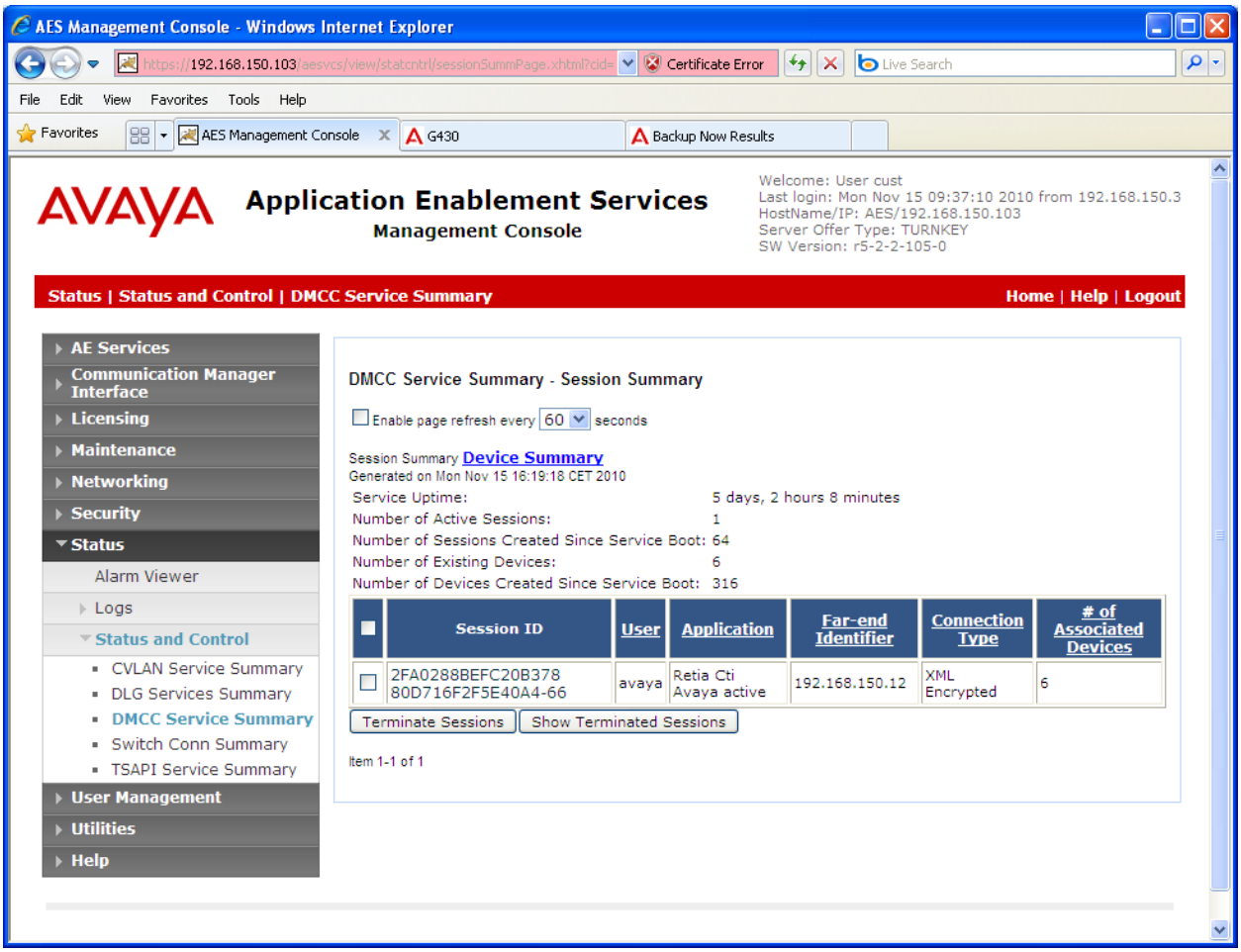

Figure 31: DMCC Service Summary Screen

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

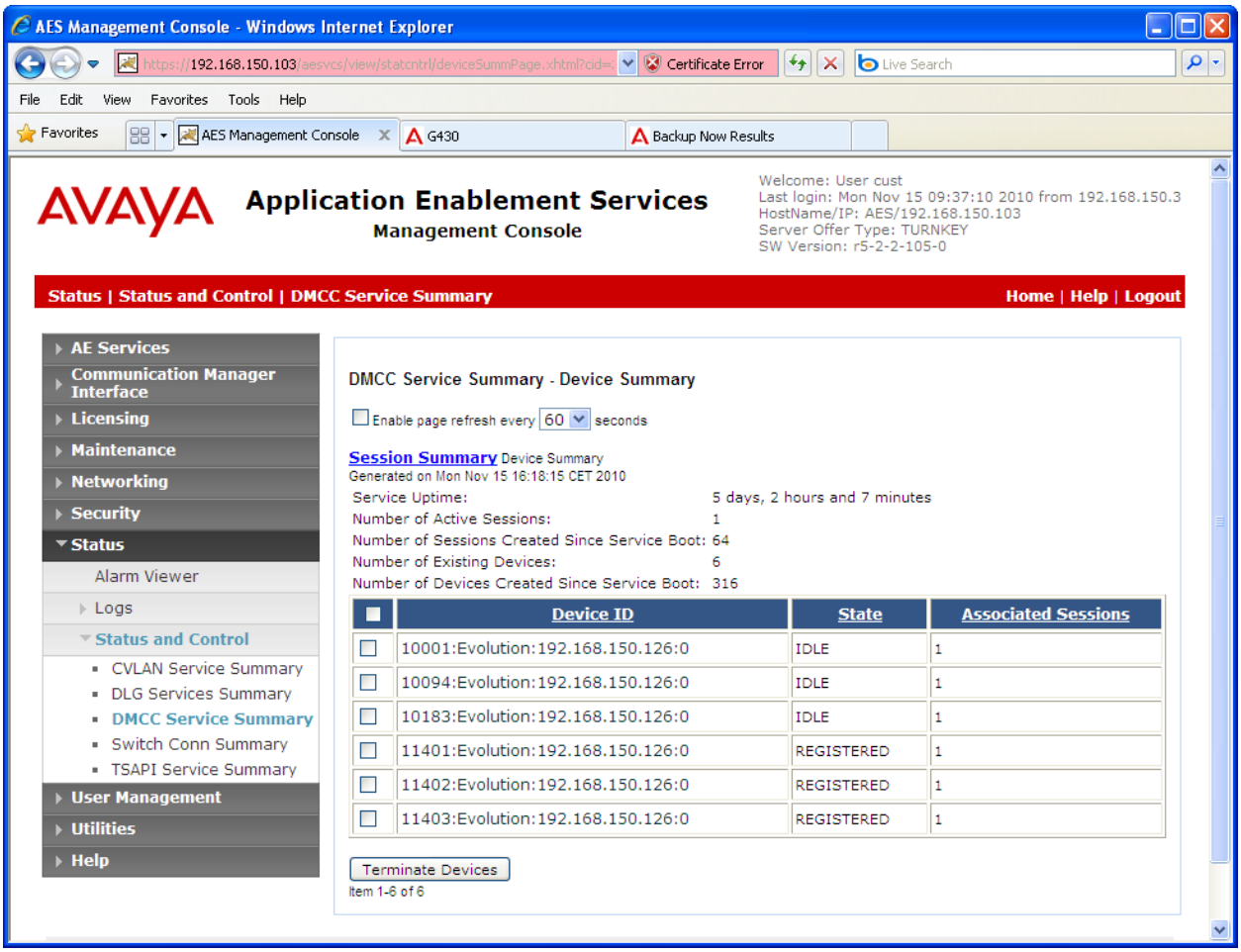

Figure 32: DMCC Device Summary Screen

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 Multiple Registrations recording method offered by the ReDat 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 passed all of the tests performed, which included both functional and robustness tests.

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.