Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Retia ReDat eXperience 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 for provisioning Retia ReDat eXperience System with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using Multiple Registrations.

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 Multiple Registrations recording method was used. Retia ReDat 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 Media 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

Note: the Voice Recorder does not monitor SIP Telephones.

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.

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 full interoperability of Retia ReDat eXperience to interoperate 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 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 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 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.

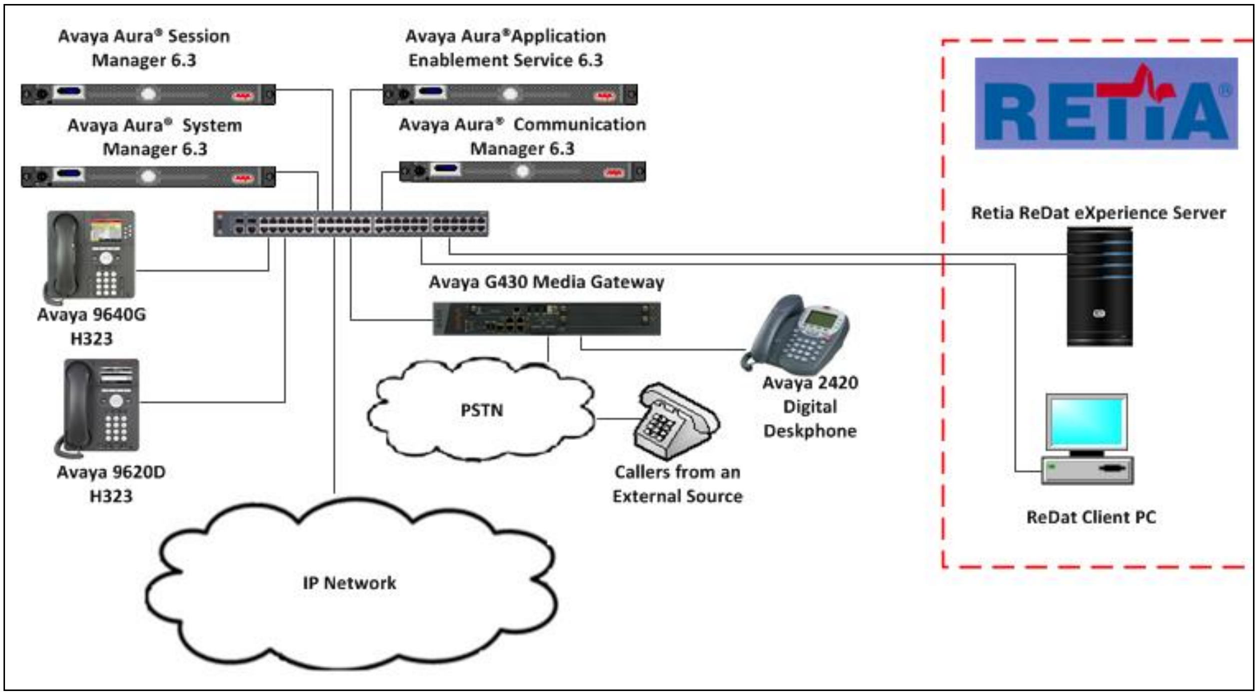

Avaya Aura® Session Manager 6.3
Avaya Aura®Application Enablement Service 6.3
Avaya Aura® System Manager 6.3
Avaya Aura® Communication Manager 6.3
RETIA
Retia ReDat eXperience Server
Avaya 9640G H323
Avaya G430 Media Gateway
Avaya 2420 Digital Deskphone
PSTN
Avaya 9620D H323
Callers from an External Source
ReDat Client PC
IP Network

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	R6.3 Build R016x.03.0.124.0 Update 03.0.124.0-20850
Avaya Aura® Session Manager	R6.3 Build 6.3.3.0.633004
Avaya Aura® System Manager	R 6.3 Build 6.3.0.8.5682-6.3.8.1814 Update 6.3.3.5.1719
Avaya Aura® Application Enablement Services	R6.3 Build 6.3.0.0.212-0
Avaya G430 Media Gateway	31.22.0/1
Avaya 96xx IP phones	
9640G	3.1.05S
9620D	3.1.01S
Avaya 2420 Digital phone	Rel 6.0, FWV 6
Retia Equipment	**Software Version**
ReDat VoIP Recorder	Version 1.12 r37
ReDat eXperience Server running on Windows 2003 Server SP2	Version 1.04 r29
Apache web server	2.2.21
PHP	5.3.10
MS SQL	2008 R2 Express SP2
Java	1.7
Microsoft .NET	3.5 and 4
ReDat client PC	
Windows XP	
Adobe flash plugin	
Mozilla Firefox	24.1.1 ESR
ReDat eXperience player	plugin 1.40

Table 1: Hardware and Software Version Numbers

5. Configure Avaya Aura® Communication Manager

Configuration and verification operations on the Communication Manager illustrated in this section were all performed using Avaya Site Administrator Emulation Mode. The information provided in this section describes the configuration of the Communication Manager for this solution. It is implied a working system is already in place. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**. The configuration operations described in this section can be summarized as follows:

- Verify system-parameters customer-options
- Create Node Name for the Avaya Aura® Application Enablement Services

- Create a CTI Link to the Avaya Aura® Application Enablement Services
- Define the Avaya Aura® Application Enablement Services Link
- Configure Stations
- Configure Hunt Group

5.1. Verify system-parameters customer-options

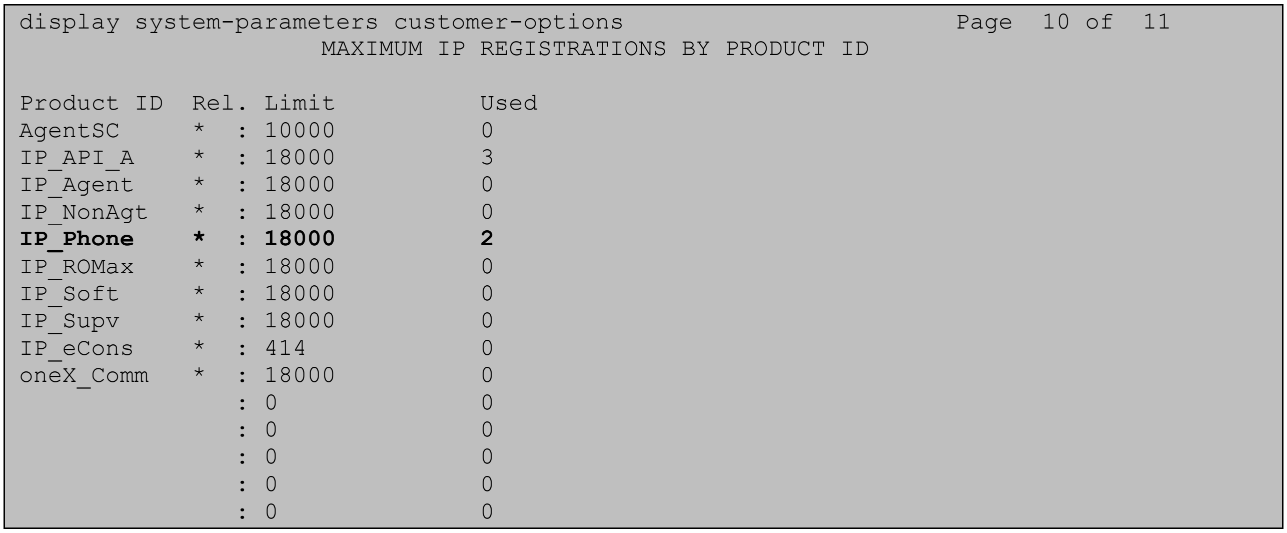
Use the **display system-parameters customer options** command to verify that Communication Manager is configured to meet the minimum requirements to run ReDat. Those items shown in **bold** indicate required values or minimum capacity requirements. If these are not met in the configuration, please contact an Avaya representative for further assistance.On **Page 2** the **Maximum Concurrently Registered IP Stations** must be sufficient to support the total number of IP stations.

```
   display system-parameters customer-options                       Page   2 of  11
                                   OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 12000 14
           Maximum Concurrently Registered IP Stations: 18000 5
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 41000 1
                   Maximum Video Capable IP Softphones: 18000 4
                       Maximum Administered SIP Trunks: 24000 120
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
```

On **Page 4**, **IP Stations** must be set to **y**.

```
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? y                         ISDN Feature Plus? n
                 Enhanced EC500? y         ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                          ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                 ISDN-PRI? y
              ESS Administration? y               Local Survivable Processor? n
         Extended Cvg/Fwd Admin? y                     Malicious Call Trace? y
     External Device Alarm Admin? y                 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? y                 Multifrequency Signaling? y
      Global Call Classification? y         Multimedia Call Handling (Basic)? y
            Hospitality (Basic)? y      Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y               Multimedia IP SIP Trunking? y
                      IP Trunks? y
          IP Attendant Consoles? y
```

On **Page 10**, **IP_Phone** must be set to the number of IP stations plus 1 for each station which is to be monitored.



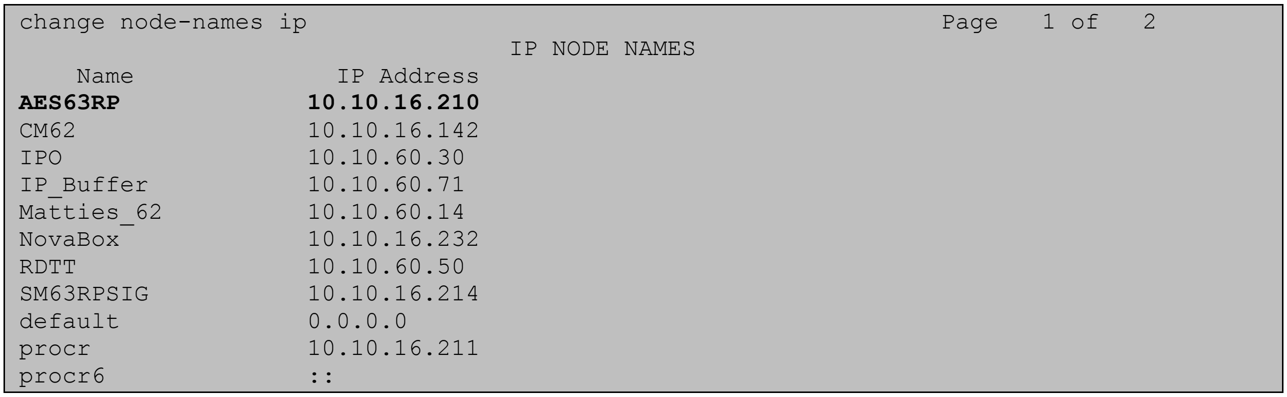
```
display system-parameters customer-options                      Page  10 of  11
                    MAXIMUM IP REGISTRATIONS BY PRODUCT ID

Product ID  Rel. Limit          Used
AgentSC     *  : 10000          0
IP_API_A    *  : 18000          3
IP_Agent    *  : 18000          0
IP_NonAgt   *  : 18000          0
IP_Phone    *  : 18000          2
IP_ROMax    *  : 18000          0
IP_Soft     *  : 18000          0
IP_Supv     *  : 18000          0
IP_eCons    *  : 414            0
oneX_Comm   *  : 18000          0
               : 0              0
               : 0              0
               : 0              0
               : 0              0
               : 0              0
```

5.2. Create Node Name for the Avaya Aura® Application Enablement Services

A Node Name needs to be created to associate the Communication Manager with the AES. Use the **change node-names ip** command to configure the following:
Page **1**

- **Name** Enter an informative name (i.e., **AES63RP)**
- **IP address** Enter the IP address of the **AES** (10.10.16.210)

Note the **procr** IP address as it is required in **Section 6.3**.
Press **f3** button to save the new settings.



```
change node-names ip                                             Page   1 of   2
                                 IP NODE NAMES
    Name              IP Address
AES63RP             10.10.16.210
CM62                10.10.16.142
IPO                 10.10.60.30
IP_Buffer           10.10.60.71
Matties_62          10.10.60.14
NovaBox             10.10.16.232
RDTT                10.10.60.50
SM63RPSIG           10.10.16.214
default             0.0.0.0
procr               10.10.16.211
procr6              ::
```

5.3. Create a CTI Link to the Avaya Aura® Application Enablement Services

A CTI Link needs to be created to enable the Communication Manager to interoperate with the AES. Use the **add cti-link** command to configure the following:

Page **1**

- **Extension** Enter a unused extension (i.e., 1999)
- **TYPE** Enter **ADJ-IP**
- **Name** Enter **AES63RP** (as created in **Section 5.2**)

Press **f3** button to save the new settings.

```
add cti-link 1                                              Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 1999
     Type: ADJ-IP
                                                                       COR: 1

     Name: AES63RP
```

5.4. Define the Avaya Aura® Application Enablement Services Link

To define the AES link use the **change ip-services** command and enter the following:

Page **1**

- **Service Type** Enter **AESVCS**
- **Enabled** Enter **y**
- **Local Node** Enter **procr**
- **Local Port** Enter **8765**

```
change ip-services                                             Page   1 of   4

                                               IP SERVICES
 Service      Enabled      Local         Local        Remote       Remote
  Type                     Node          Port         Node         Port
AESVCS          y      procr             8765
```

Navigate to **Page 4** and enter the following:

- **Server ID** Enter **1**
- **AE Services** Enter **AES63RP** (The node created in **section 5.2**)
- **Password** Enter a password. This password will be used in **Section 6.3** to enable the AES to communicate with the Communication Manager.
- **Enabled** Enter **y**

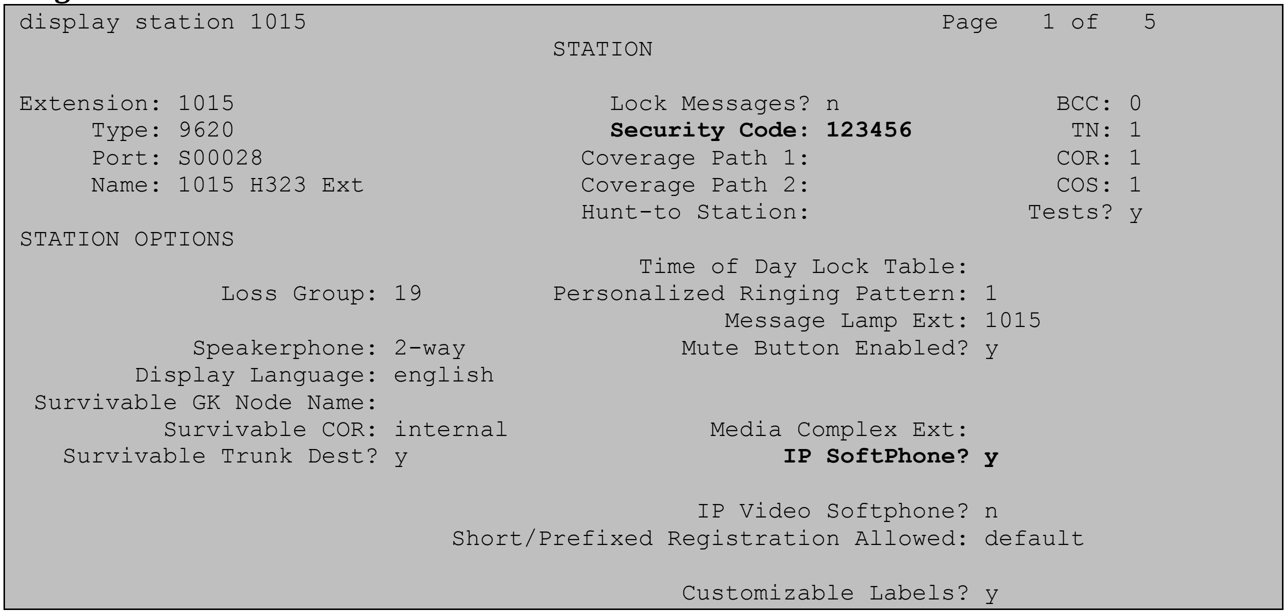
Press **f3** button to save the new settings.

```
change ip-services                                             Page   4 of   4
                             AE Services Administration

   Server ID    AE Services        Password          Enabled    Status
                   Server
      1:      AES63RP          Avayapassword123      y         in use
```

5.5. Configure Stations

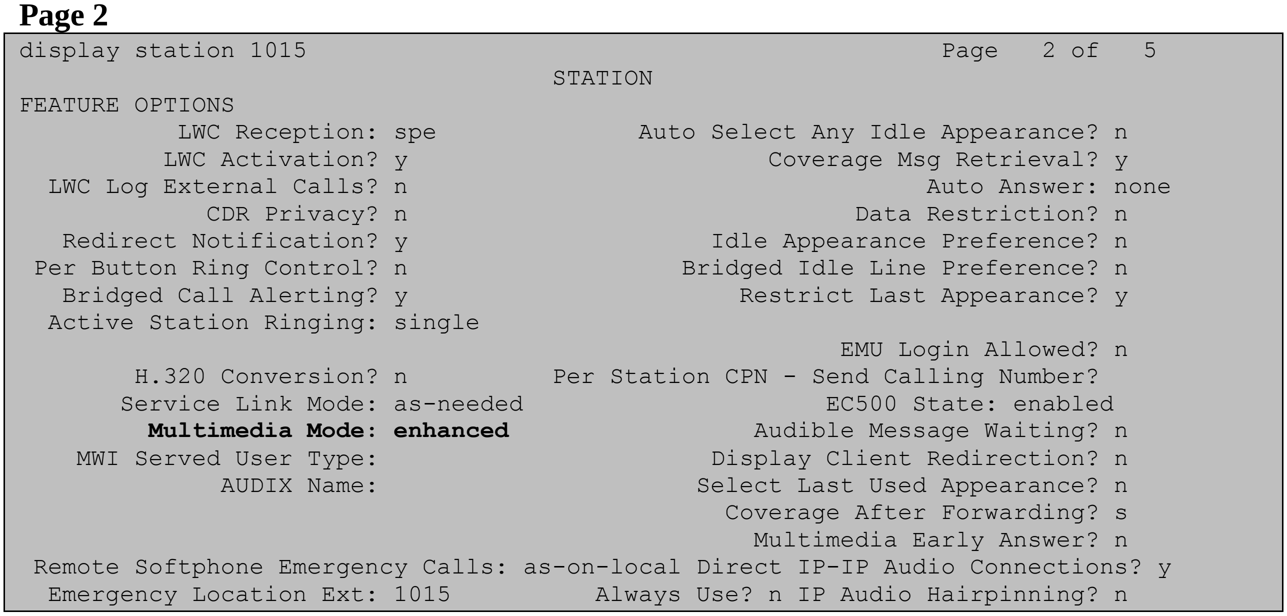
For each Station to be monitored must have **IP Softphone** set to **y** on page 1 and **Multimedia Mode** set to **enhanced** on page 2. The example below shows the configuration of an IP station 1015 (note, TDM stations must also have **IP Softphone** set to **y** on page 1 and **Multimedia Mode** set to **enhanced** on page 2). Note the **Security Code** as this will be required by the Retia ReDat system in **Section 7.2**.

Page 1



```
display station 1015                                            Page   1 of   5
                                     STATION

Extension: 1015                          Lock Messages? n               BCC: 0
     Type: 9620                          Security Code: 123456           TN: 1
     Port: S00028                      Coverage Path 1:                 COR: 1
     Name: 1015 H323 Ext               Coverage Path 2:                 COS: 1
                                       Hunt-to Station:               Tests? y
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 1015
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? y

                                               IP Video Softphone? n
                              Short/Prefixed Registration Allowed: default

                                              Customizable Labels? y
```

Page 2

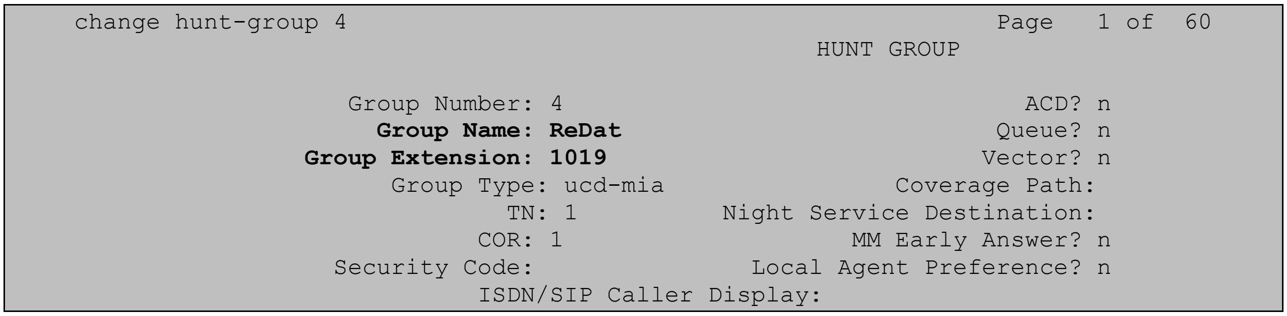


```
display station 1015                                            Page   2 of   5
                                     STATION
FEATURE OPTIONS
           LWC Reception: spe              Auto Select Any Idle Appearance? n
          LWC Activation? y                         Coverage Msg Retrieval? y
  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? y                       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: 1015          Always Use? n IP Audio Hairpinning? n
```

5.6. Configure Hunt Group

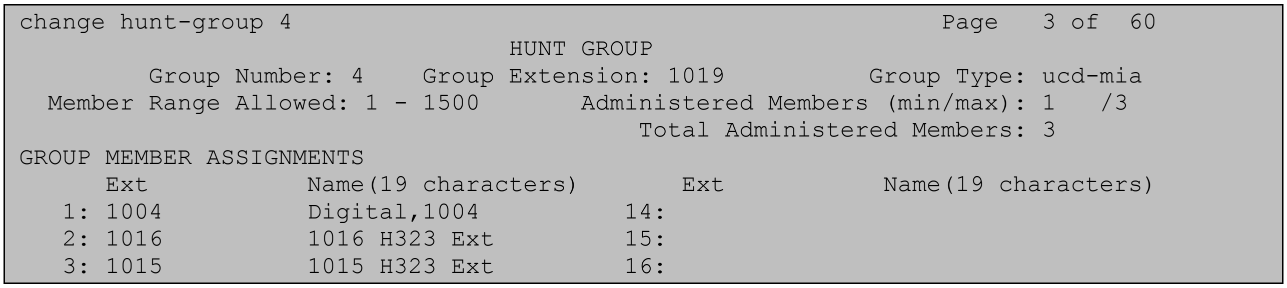
Use the **add hunt-group x** command where x is an available hunt group number to create a hunt group which is used to test the ability of the ReDat system to monitor hunt groups. Assign an unused extension as the **Group Extension**. Add extensions of the telephones to the hunt group which are monitored by the ReDat system. The following was used during compliance testing:
Page **1**

- **Group Name:** Enter an informative name (i.e. **ReDat**)
- **Group Extension:** Enter an unused extension which is compatible with the dial plan (i.e., **1019**)



```
    change hunt-group 4                                             Page   1 of  60
                                                        HUNT GROUP

                       Group Number: 4                                ACD? n
                         Group Name: ReDat                          Queue? n
                    Group Extension: 1019                          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:
```

Navigate to **Page 3** and add the extensions which are to be assigned to the hunt group. Extensions 1004 and 1016 were used during compliance testing.
Press **f3** button to save the new settings.



```
change hunt-group 4                                             Page   3 of  60
                                  HUNT GROUP
         Group Number: 4    Group Extension: 1019          Group Type: ucd-mia
  Member Range Allowed: 1 - 1500       Administered Members (min/max): 1   /3
                                           Total Administered Members: 3
GROUP MEMBER ASSIGNMENTS
      Ext           Name(19 characters)       Ext           Name(19 characters)
   1: 1004          Digital,1004          14:
   2: 1016          1016 H323 Ext         15:
   3: 1015          1015 H323 Ext         16:
```

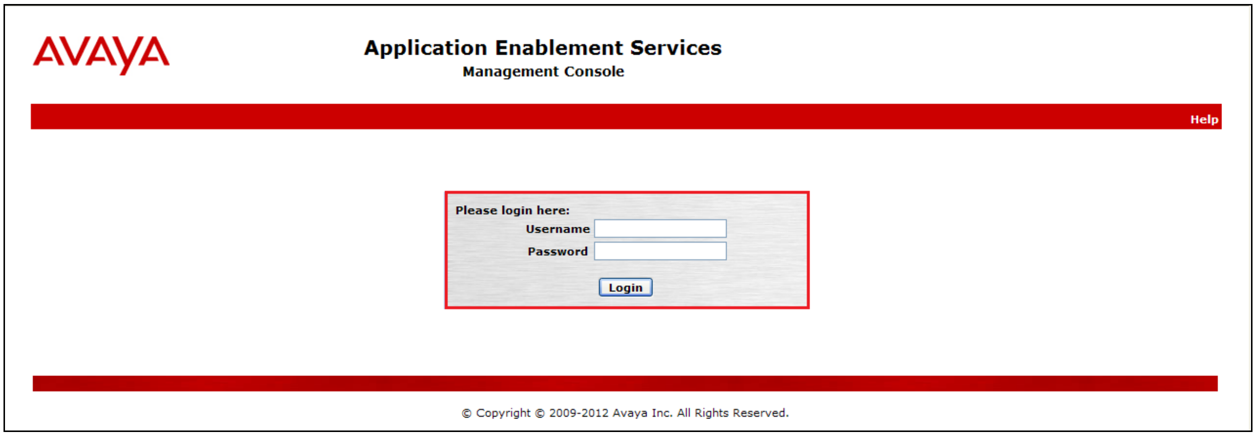
6. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Avaya Application Enablement Services (Avaya AES). It is implied a working Avaya AES is already in place and the Security Database (SDB) is configured. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**. The configuration operations described in this section can be summarized as follows:

- Logging into Avaya Aura® Application Enablement Services
- Verify Avaya Aura® Application Enablement Services License
- Create a Communication Manager Switch Connection
- Create a TSAPI Link
- Create CTI User
- Configure DMCC Port

6.1. Logging into the Avaya Aura® Application Enablement Services

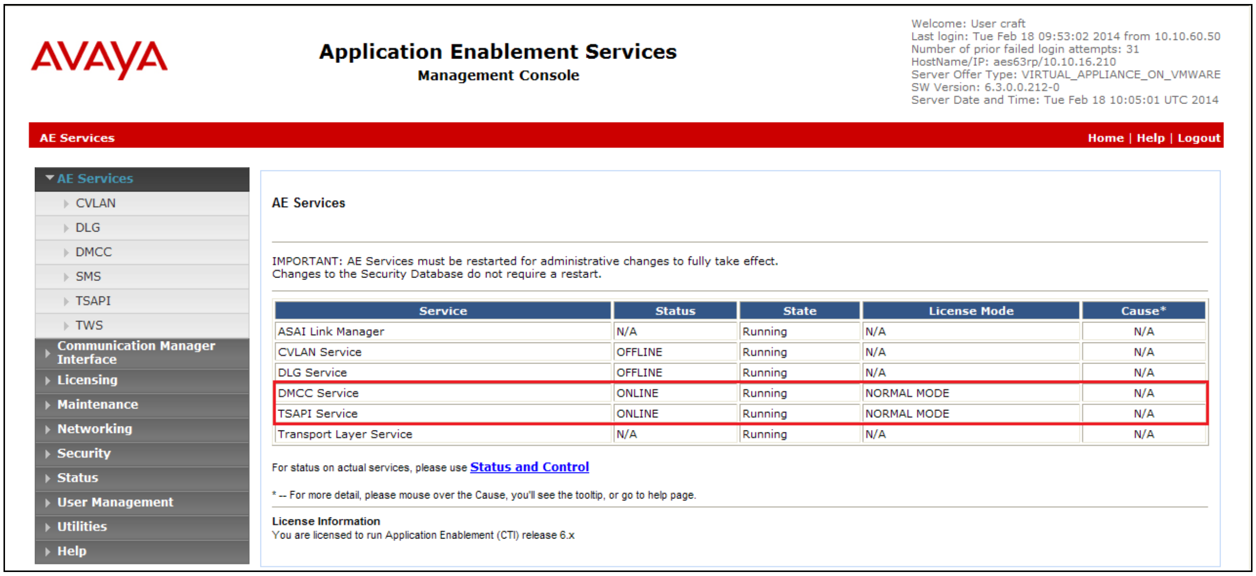
To access the OAM web-based interface of the Application Enablement Services Server, use the URL **http://x.x.x.x**, where **x. x. x. x** is the selected IP address of the AES. The **Management console** is displayed. Log in using the appropriate credentials.



© Copyright © 2009-2012 Avaya Inc. All Rights Reserved.

6.2. Verify Avaya Aura® Application Enablement Services License

Select **AE Services** on the left pane and verify that the **DMCC** and **TSAPI Services** are licensed by ensuring that **DMCC** and **TSAPI Services** are in the list of services and that the **License Mode** is showing **NORMAL MODE**. If this is not the case, please contact an Avaya representative regarding licensing.



Welcome: User craft
Last login: Tue Feb 18 09:53:02 2014 from 10.10.60.50
Number of prior failed login attempts: 31
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Feb 18 10:05:01 UTC 2014

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

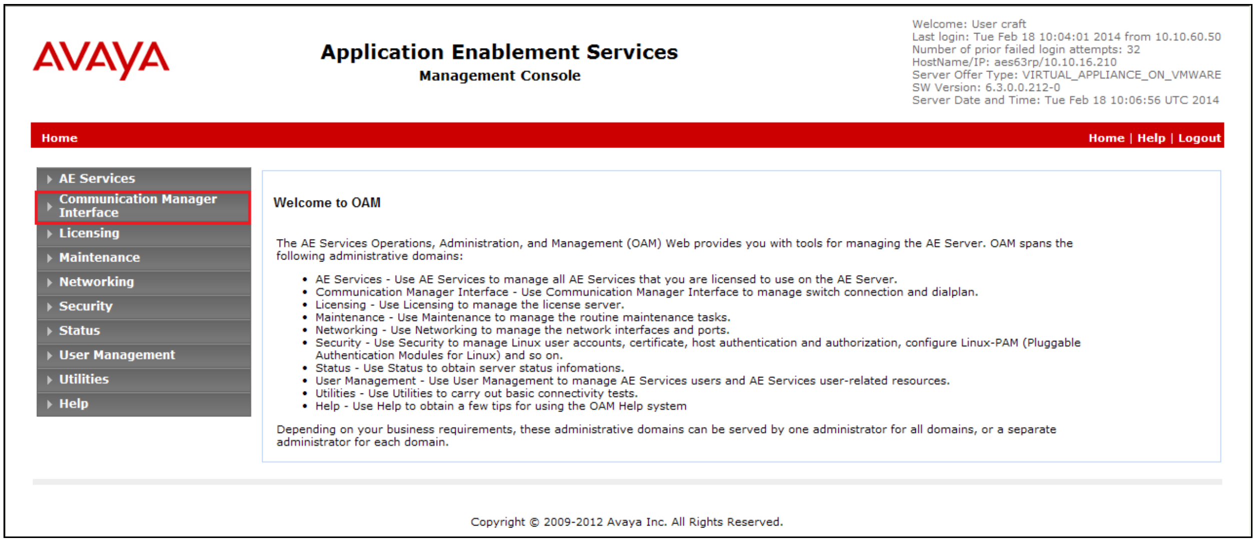
For status on actual services, please use Status and Control

* -- 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) release 6.x

6.3. Create a Communication Manager Switch Connection

A Communication Manager Switch Connection needs to be created to enable the AES to communicate with the Communication Manager. Select **Communication Manager Interface**.



Application Enablement Services
Management Console

Welcome: User craft
Last login: Tue Feb 18 10:04:01 2014 from 10.10.60.50
Number of prior failed login attempts: 32
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Feb 18 10:06:56 UTC 2014

Welcome to OAM

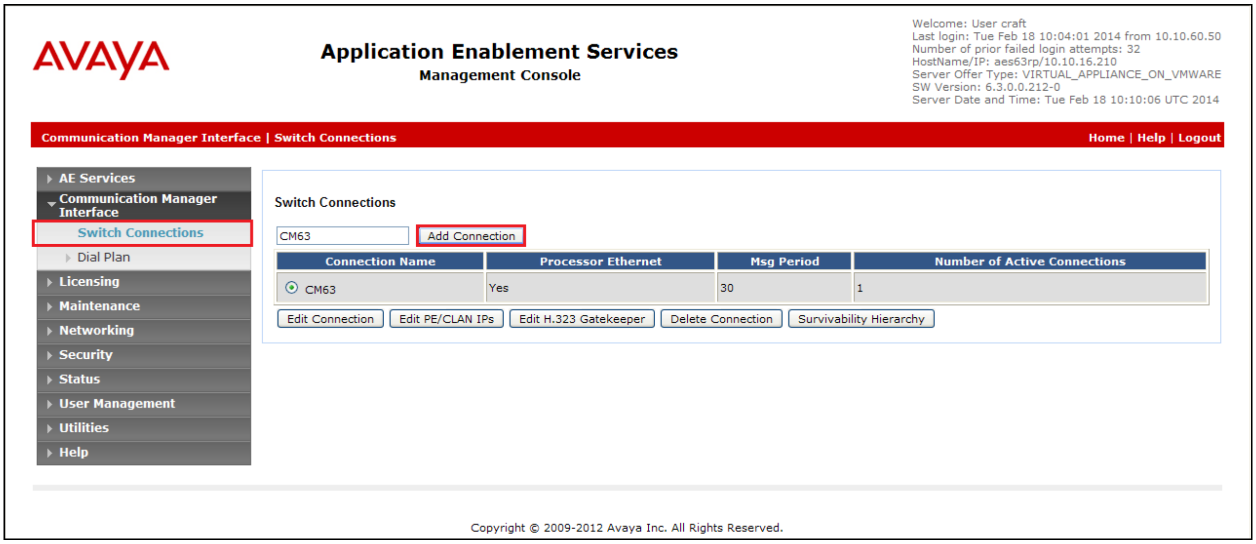
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- 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 infomations.
- 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.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

Copyright © 2009-2012 Avaya Inc. All Rights Reserved.

Select **Switch Connections** and enter an informative name for the Communication Manager (i.e., CM63). Click on the **Add Connection** button.



Application Enablement Services
Management Console

Welcome: User craft
Last login: Tue Feb 18 10:04:01 2014 from 10.10.60.50
Number of prior failed login attempts: 32
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Feb 18 10:10:06 UTC 2014

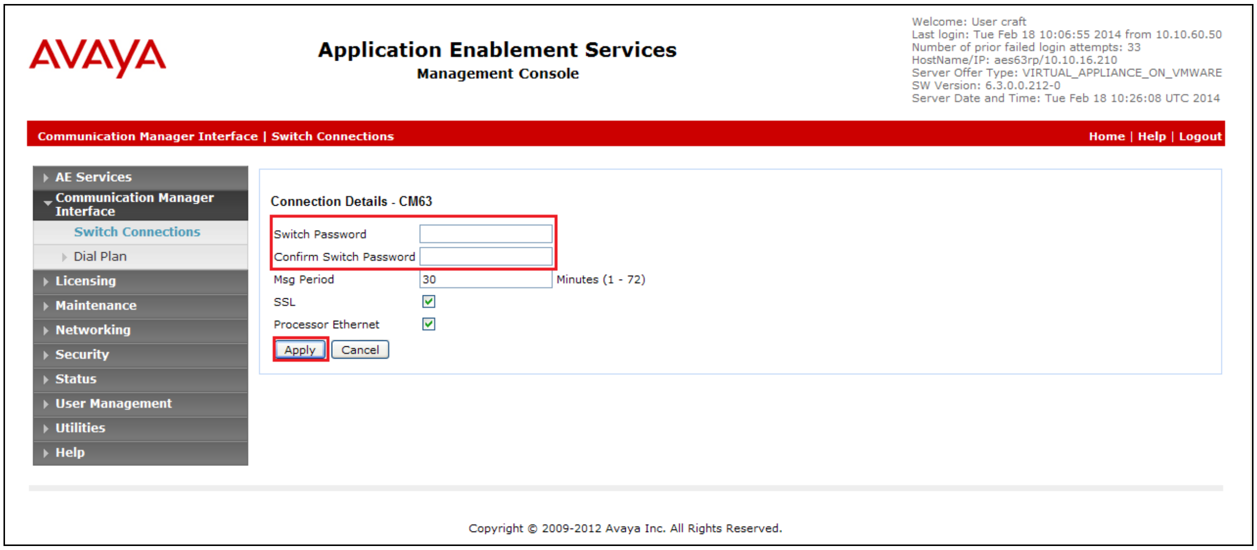
Switch Connections

CM63 [Add Connection]

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● CM63	Yes	30	1

Copyright © 2009-2012 Avaya Inc. All Rights Reserved.

Once the **Connection Details** window opens, enter the **Switch Password** as was configured in **Section 5.4** then **Confirm Switch Password.** Click on the **Apply** button.



Welcome: User craft
Last login: Tue Feb 18 10:06:55 2014 from 10.10.60.50
Number of prior failed login attempts: 33
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Feb 18 10:26:08 UTC 2014

Connection Details - CM63

Switch Password

Confirm Switch Password

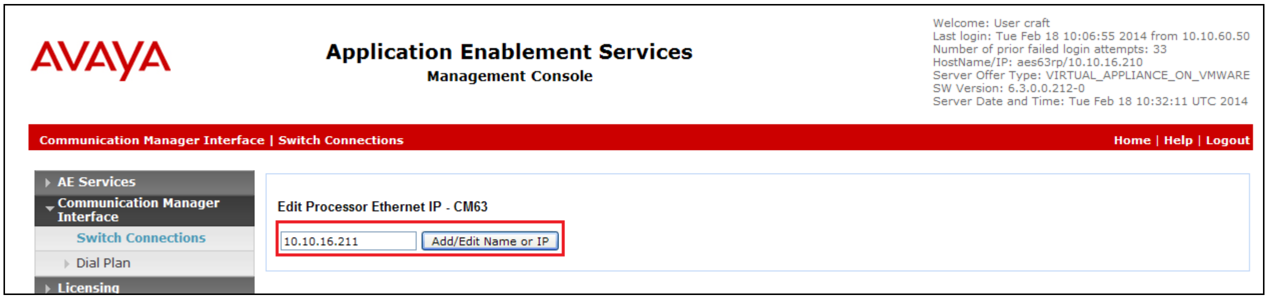
Msg Period 30 Minutes (1 - 72)

SSL ☑

Processor Ethernet ☑

Copyright © 2009-2012 Avaya Inc. All Rights Reserved.

Click the **Edit PE/CLAN IPs** button (not shown). Enter the IP address of the Processor Ethernet interface (procr. IP address, see **Section 5.3**) that Application Enablement Services will use for communication with the Communication Manager, and click the **Add/Edit Name or IP** button.

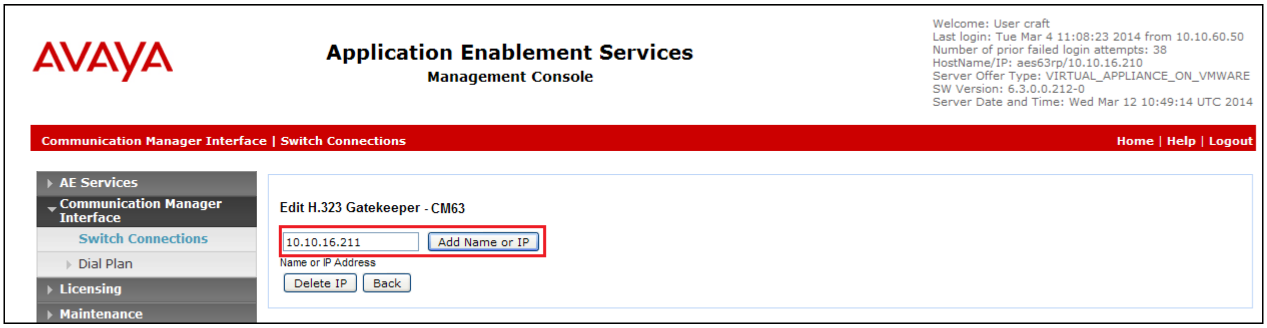

AVAYA
Application Enablement Services
Management Console
Communication Manager Interface | Switch Connections
Home | Help | Logout
AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Add/Edit Name or IP

Welcome: User craft
Last login: Tue Feb 18 10:06:55 2014 from 10.10.60.50
Number of prior failed login attempts: 33
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Feb 18 10:32:11 UTC 2014

Edit Processor Ethernet IP - CM63

10.10.16.211

Click the **Edit H.323 Gatekeeper** button (not shown). Enter the IP address of the Processor Ethernet interface (procr. IP address, see **Section 5.3**). Click the **Add Name or IP** button.



Welcome: User craft
Last login: Tue Mar 4 11:08:23 2014 from 10.10.60.50
Number of prior failed login attempts: 38
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Wed Mar 12 10:49:14 UTC 2014

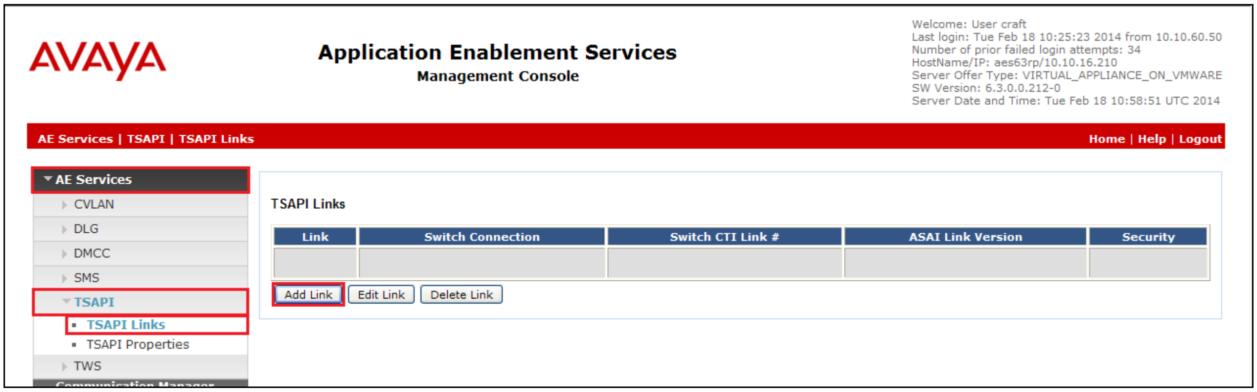
Edit H.323 Gatekeeper - CM63

10.10.16.211

Name or IP Address

6.4. Create a TSAPI Link

A TSAPI Link needs to be created to interoperate with the ReDat. Navigate to **AE Services →** **TSAPI → TSAPI Links** and click on the **Add Link** button.



Welcome: User craft
Last login: Tue Feb 18 10:25:23 2014 from 10.10.60.50
Number of prior failed login attempts: 34
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Feb 18 10:58:51 UTC 2014

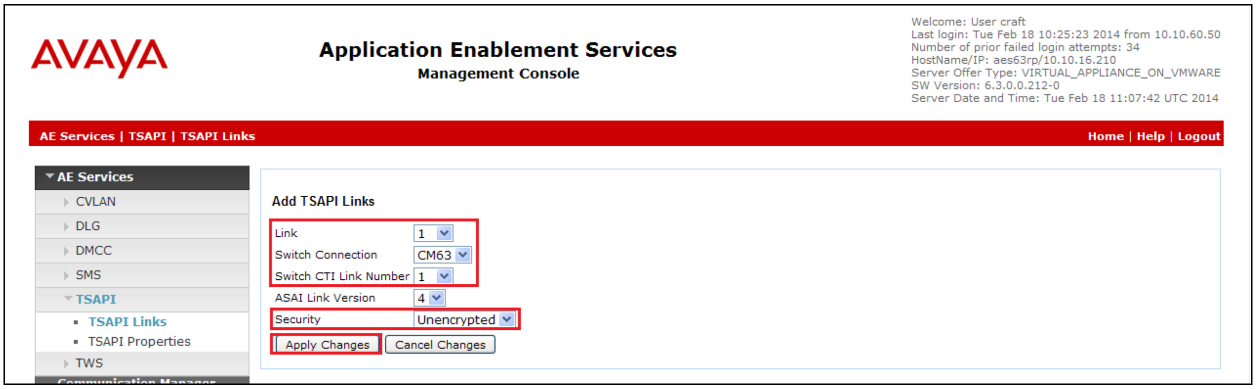
TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security

Once the **Add TSAPI Links** window opens enter the following:

- **Link** Select the next available Link from the dropdown box
- **Switch Connection** Select **CM63** from the dropdown box. (The Switch connection as created in **Section 63**)
- **Switch CTI Link Number** Select **1** from the dropdown box. (The CTI link as created in **Section 5.2**)
- **Security** Select **Unencrypted** from the dropdown box

Click on the **Apply Changes** button.



Welcome: User craft
Last login: Tue Feb 18 10:25:23 2014 from 10.10.60.50
Number of prior failed login attempts: 34
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Feb 18 11:07:42 UTC 2014

Add TSAPI Links

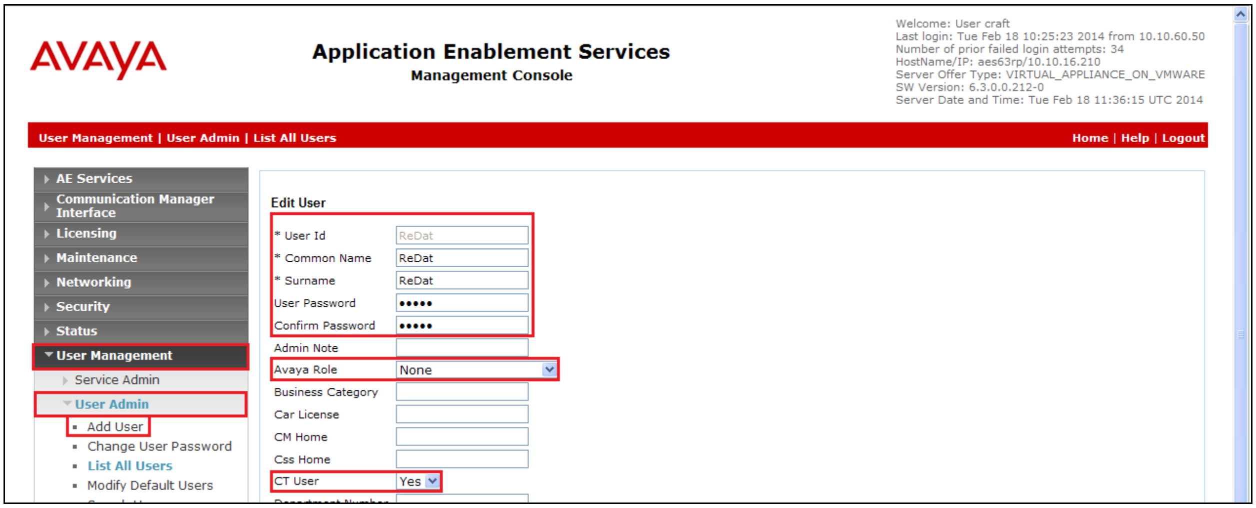
Link	1
Switch Connection	CM63
Switch CTI Link Number	1
ASAI Link Version	4
Security	Unencrypted

6.5. Create CTI User

Navigate to **User Management → User Admin**, and select **Add User**. On the **Add User** screen enter the following:

- **User Id** Enter an informative name (i.e., **ReDat**. This ID is required for the ReDat configuration in **Section 7.2**
- **Common Name** Enter a Common Name (i.e., **ReDat**)
- **Surname** Enter a Surname (i.e., **ReDat**)
- **User Password** Enter a password. This password is be required for the ReDat configuration in section **Section 7.2**
- **Confirm Password** Confirm the password
- **Avaya Role** Select **None** from the dropdown box
- **CT User** Select **Yes** from the dropdown box

Click the **Apply button** at the bottom of the screen (not shown).



Welcome: User craft
Last login: Tue Feb 18 10:25:23 2014 from 10.10.60.50
Number of prior failed login attempts: 34
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Feb 18 11:36:15 UTC 2014

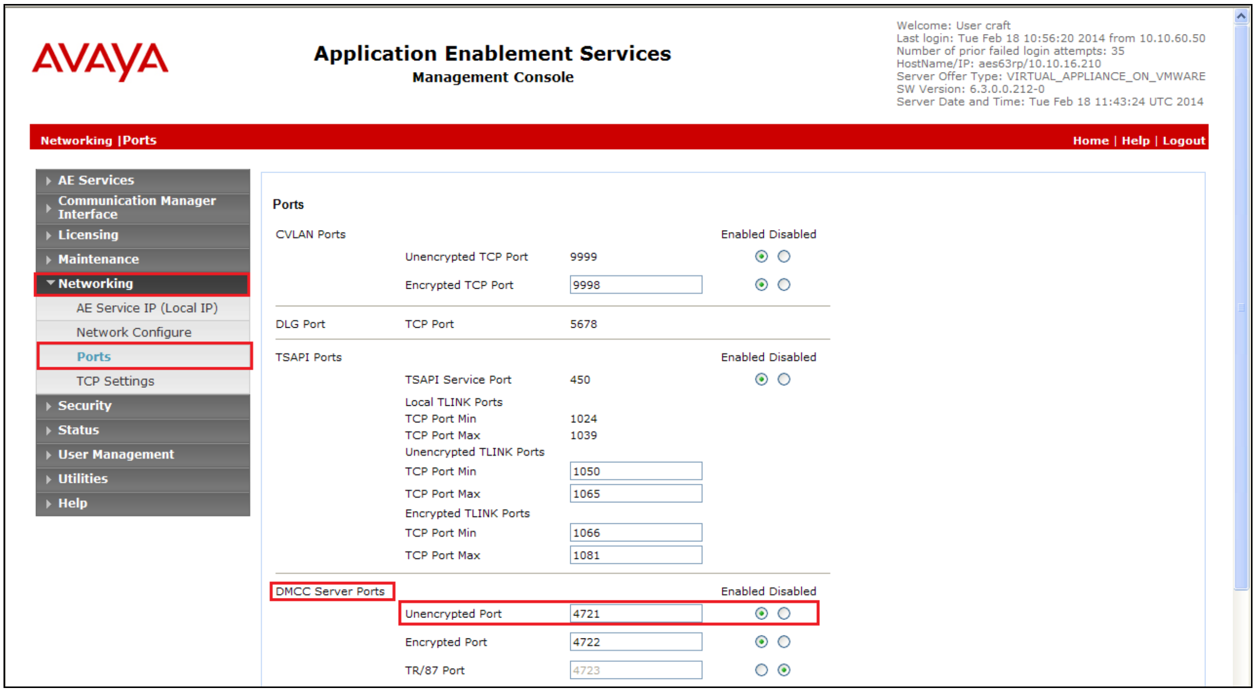
Edit User

* User Id	ReDat
* Common Name	ReDat
* Surname	ReDat
User Password	•••••
Confirm Password	•••••
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes

6.6. Configure DMCC Port

Navigate to **Networking → Ports**. In the **DMCC Server Ports** area, enter **4721** in the **Unencrypted Port** box and click on the **Enabled** radio button. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process.

Note: Although the TSAPI feature is used the DMCC port is configured.



Welcome: User craft
Last login: Tue Feb 18 10:56:20 2014 from 10.10.60.50
Number of prior failed login attempts: 35
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Feb 18 11:43:24 UTC 2014

Ports

			Enabled	Disabled
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	○	●

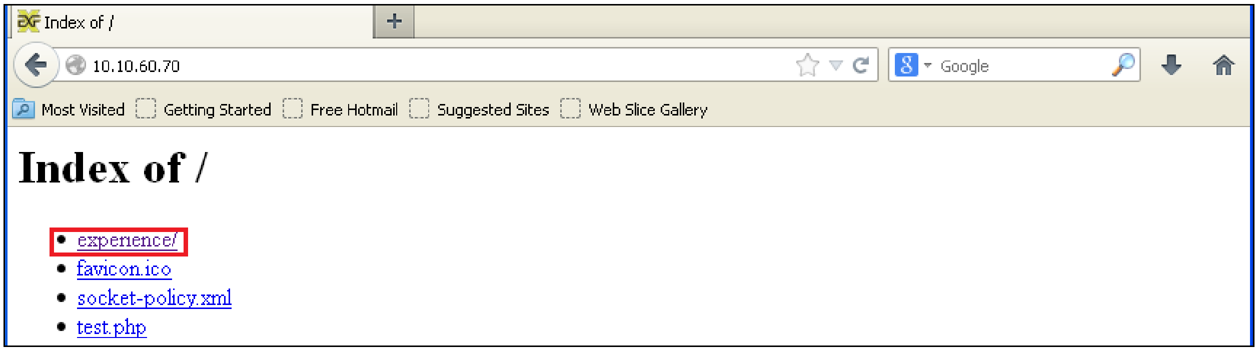
7. Configure Retia ReDat eXperience

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
- Configure Extensions
- Restart active recording Service

7.1. Logging into the ReDat server

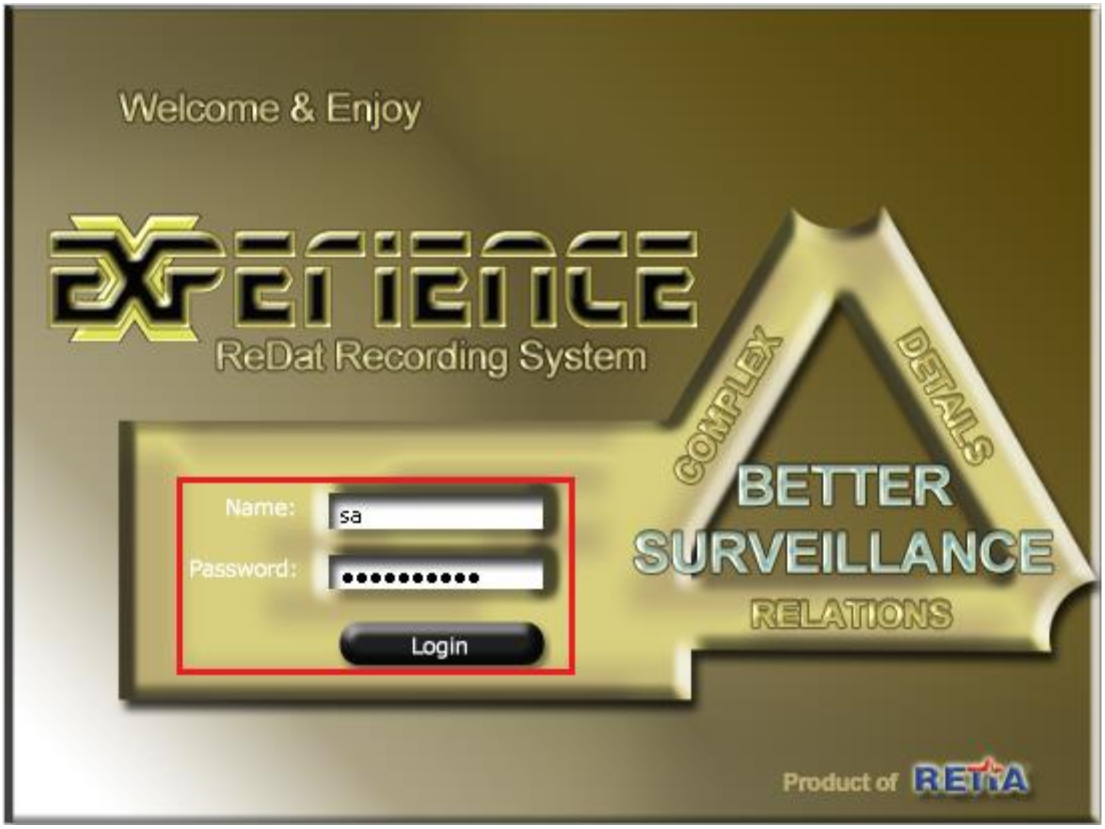
Browse to the IP Address of the ReDat server and select the **experience** link.



Index of /

- experience/
- favicon.ico
- socket-policy.xml
- test.php

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

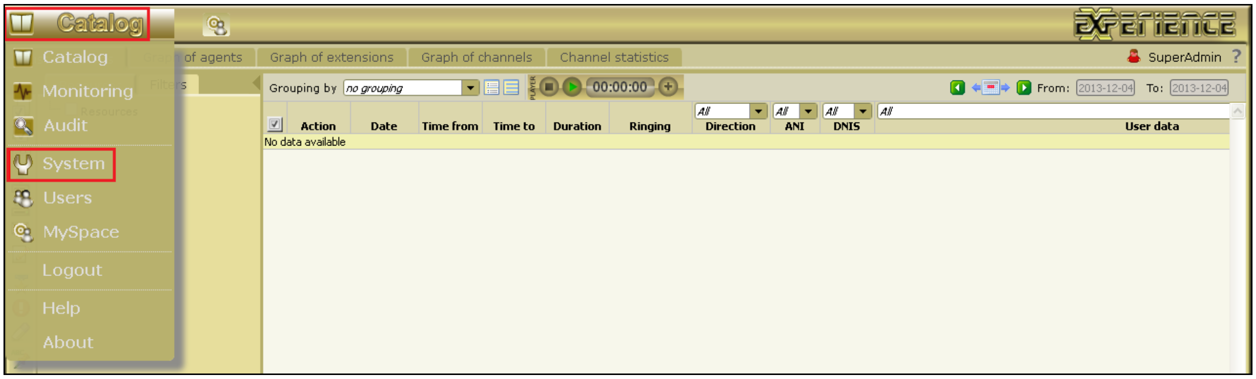


Name: sa

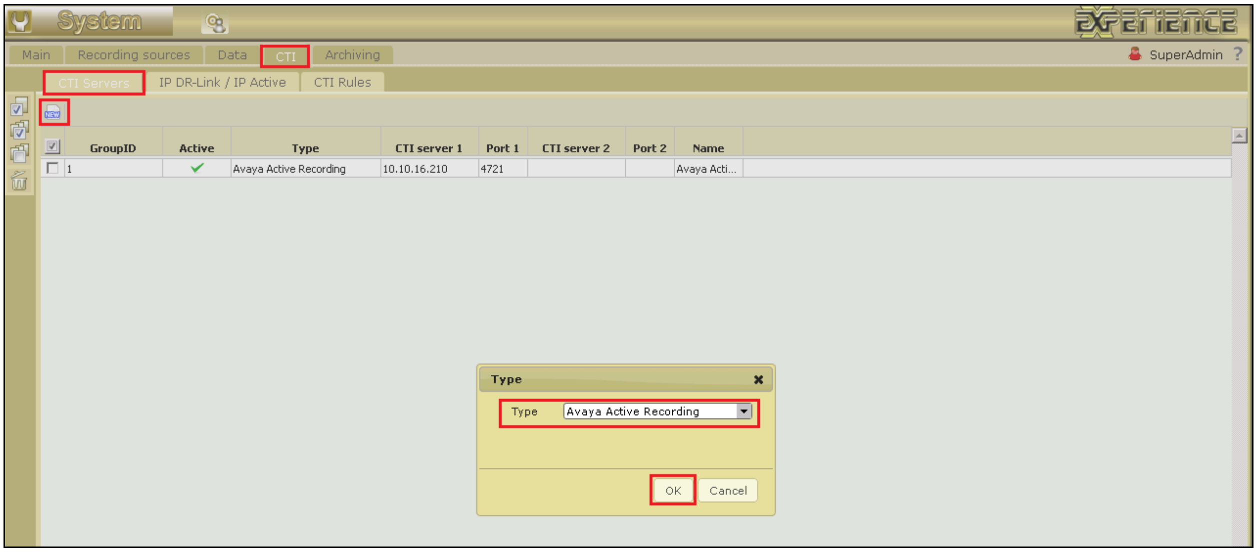
Password: ●●●●●●●●●●●

7.2. Configure CTI

Once the **Catalog** page opens, navigate to **Catalog** → **System**.



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



	GroupID	Active	Type	CTI server 1	Port 1	CTI server 2	Port 2	Name
□	1	✓	Avaya Active Recording	10.10.16.210	4721			Avaya Acti...

Type

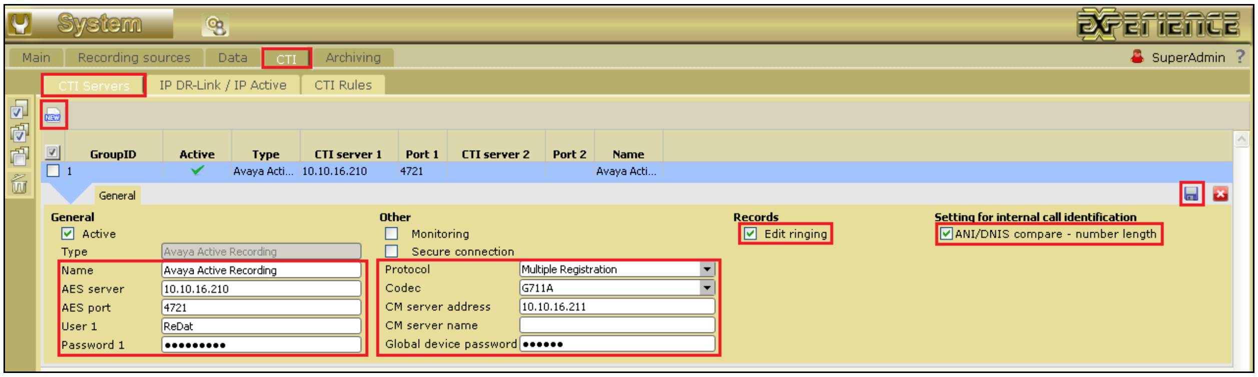
Type: Avaya Active Recording

When the new page opens click on the **New** icon highlighted, enter the following:

Name	Enter **Avaya Active Recording**
AES Server	Enter the IP address of the AES Server (10.10.16.210)
AES port	Enter **4721** (**Unencrypted Port** as configured in **Section 6.6**)
User 1	Enter **Redat (User ID** as configured in **Section 6.5**)
Password 1	Enter the **User Password** as configured in **Section 6.5**
Protocol	Select **Multiple Registration** from the dropdown box
Codec	Select **G711A** from the dropdown box
CM Server address	Enter the procr IP address, see **Section 5.3**
Global device password	Enter the Security Code configured for the IP Station shown in **Section 5.5**

Check the **Edit ringing** and **ANI/DNIS compare – number length** check boxes.

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



	GroupID	Active	Type	CTI server 1	Port 1	CTI server 2	Port 2	Name
□	1	✓	Avaya Acti...	10.10.16.210	4721			Avaya Acti...

General

General
☑ Active
Type: Avaya Active Recording
Name: Avaya Active Recording
AES server: 10.10.16.210
AES port: 4721
User 1: ReDat
Password 1: •••••••••

Other
□ Monitoring
□ Secure connection
Protocol: Multiple Registration
Codec: G711A
CM server address: 10.10.16.211
CM server name:
Global device password: ••••••

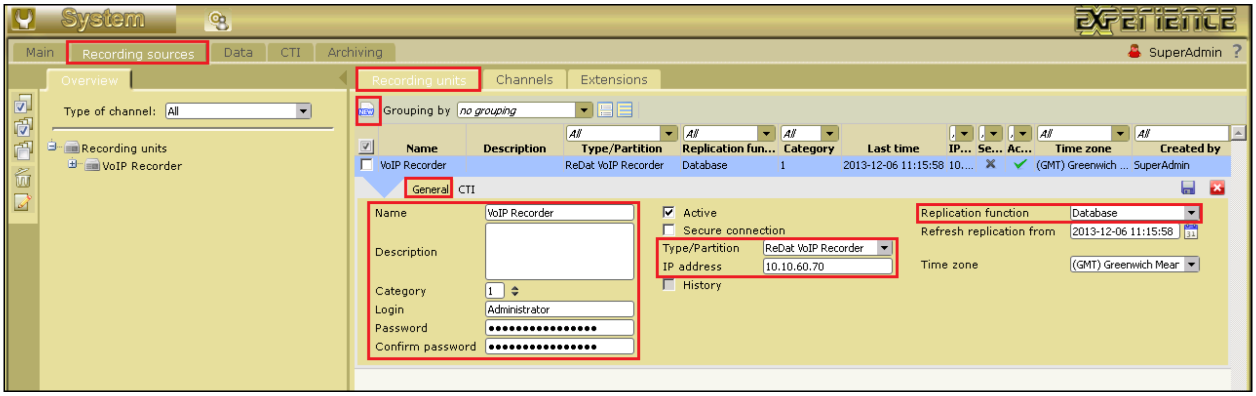
Records
☑ Edit ringing

Setting for internal call identification
☑ ANI/DNIS compare - number length

7.3. Configure Recording units

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

- **Name** Enter an informative name (i.e., VoIP Recorder)
- **Category** Select **1**
- **Login** Enter **Administrator**
- **Password** Enter the Administrator 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** from the dropdown box



Type of channel: All

Grouping by: no grouping

☑	Name	Description	Type/Partition	Replication fun...	Category	Last time	IP...	Se...	Ac...	Time zone	Created by
□	VoIP Recorder		ReDat VoIP Recorder	Database	1	2013-12-06 11:15:58	10....	✗	✓	(GMT) Greenwich ...	SuperAdmin

General | CTI

Name: VoIP Recorder

Description:

Category: 1

Login: Administrator

Password: ●●●●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●●●●

☑ Active

□ Secure connection

Type/Partition: ReDat VoIP Recorder

IP address: 10.10.60.70

□ History

Replication function: Database

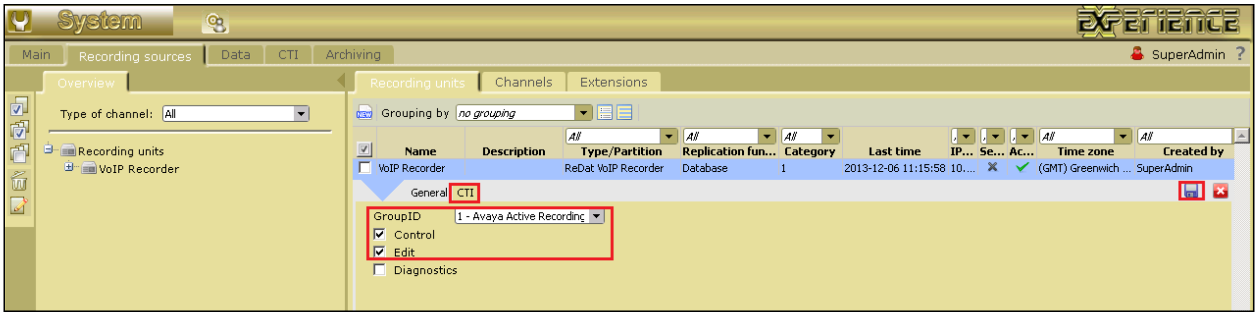
Refresh replication from: 2013-12-06 11:15:58

Time zone: (GMT) Greenwich Mear

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

- **Group ID** Select **Avaya Active Recording** 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.



Type of channel: All

Grouping by: no grouping

☑	Name	Description	Type/Partition	Replication fun...	Category	Last time	IP...	Se...	Ac...	Time zone	Created by
□	VoIP Recorder		ReDat VoIP Recorder	Database	1	2013-12-06 11:15:58	10....	✗	✓	(GMT) Greenwich ...	SuperAdmin

General | CTI

GroupID: 1 - Avaya Active Recordinç

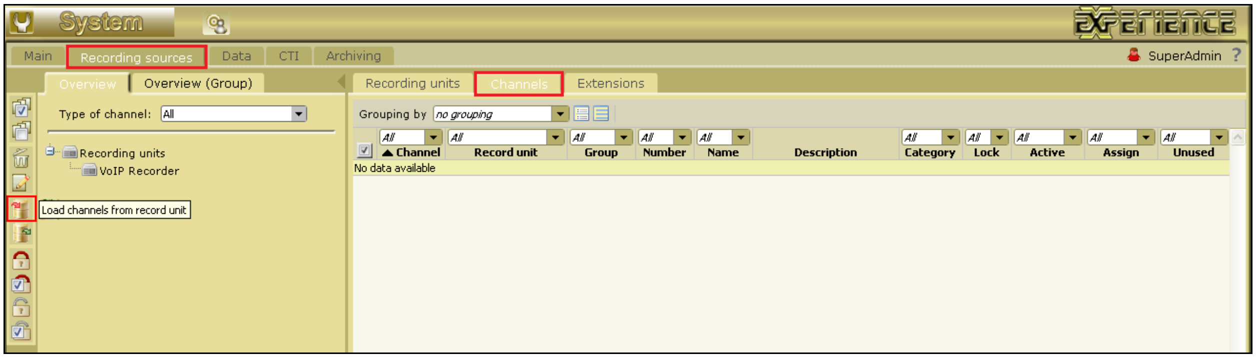
☑ Control

☑ Edit

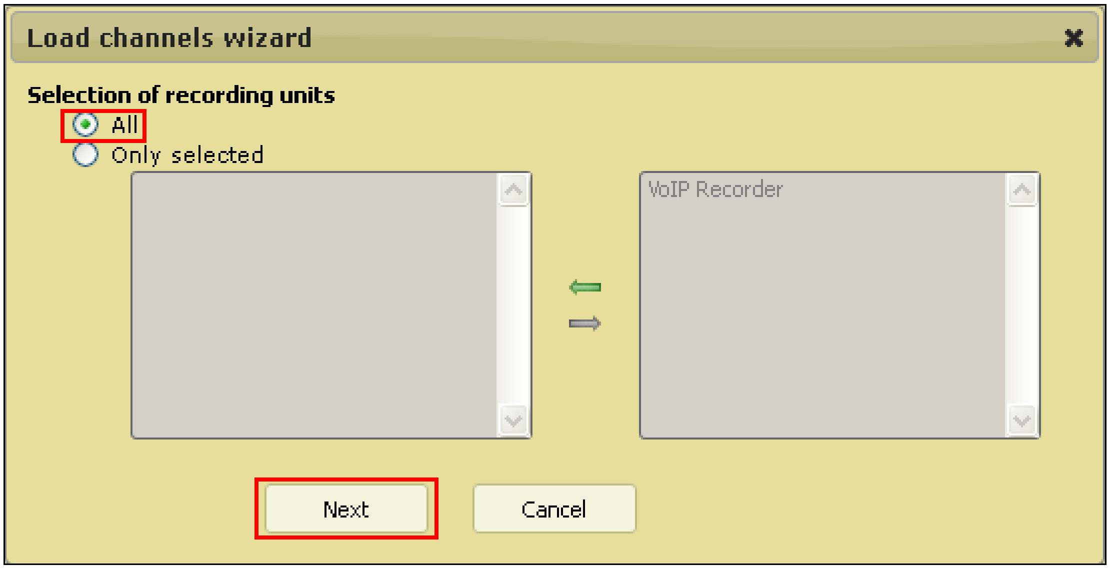
□ Diagnostics

7.4. Configure Channels

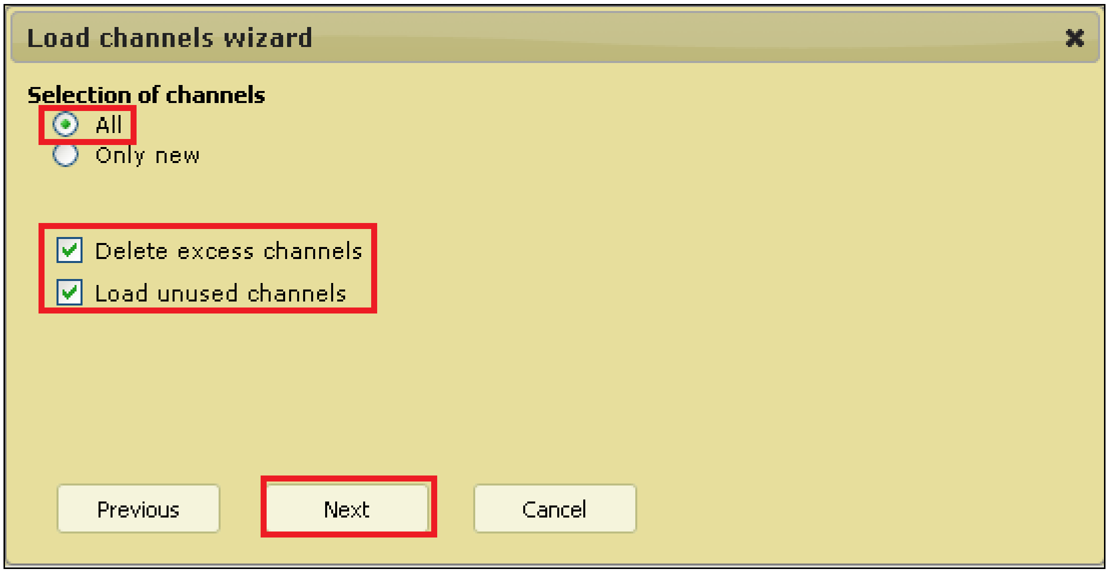
Click on the **Recording sources** tab followed by the **Channels** tab. Click on the **Load channels from record unit** icon highlighted.



When the **Load channels wizard** window opens, click on the **All** radio button followed by the **Next** button to continue.



When the next window opens, click on the **All** radio button and check the **Delete excess channels** and **Load unused channels** check boxes. Click on the **Next** button to continue.

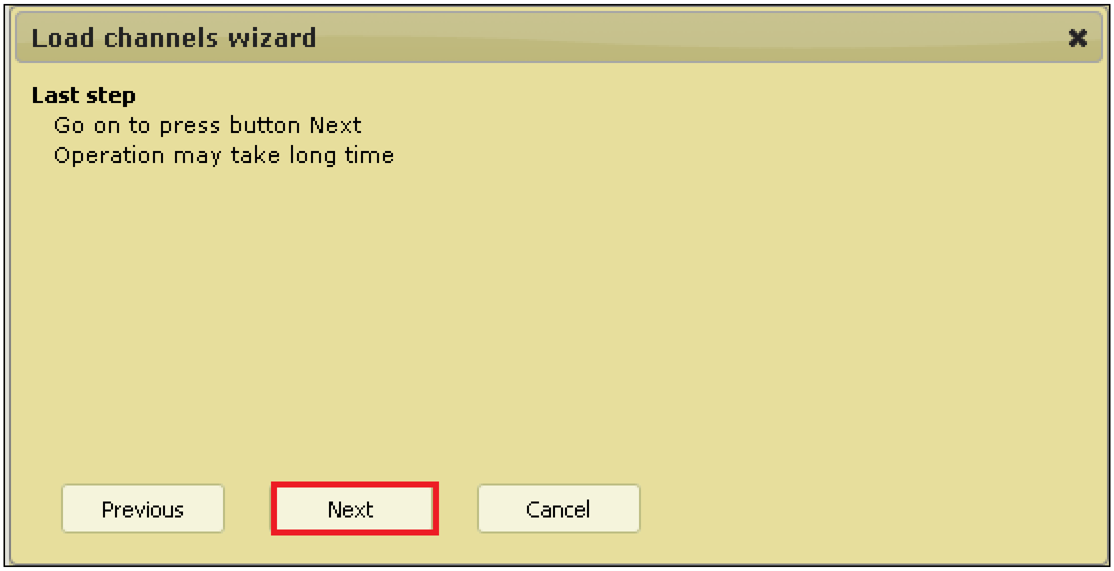


Selection of channels

● All
○ Only new

☑ Delete excess channels
☑ Load unused channels

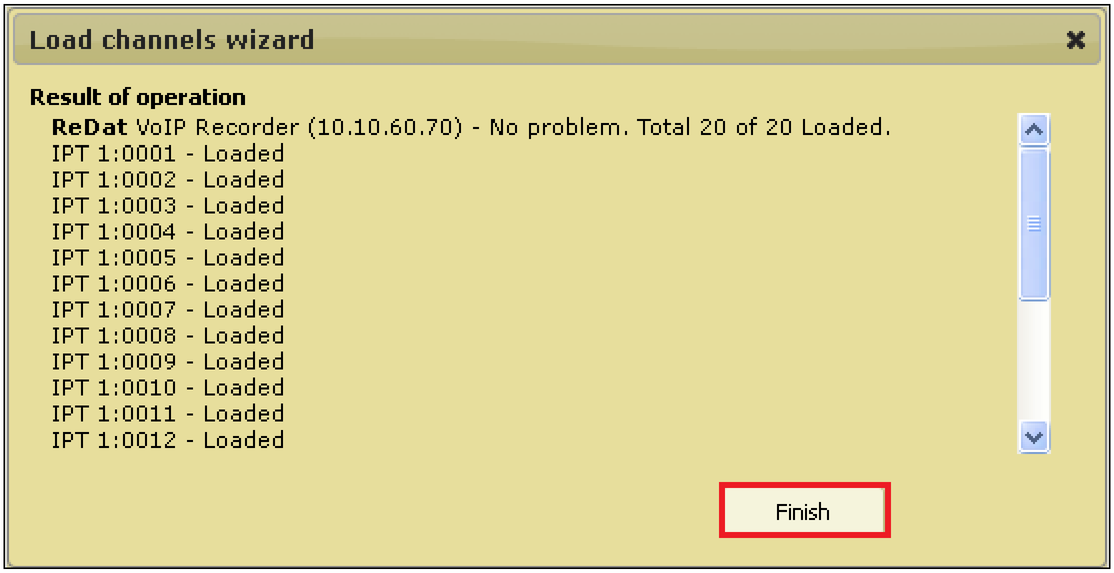
Click on the **Next** button to continue.



Last step

Go on to press button Next
Operation may take long time

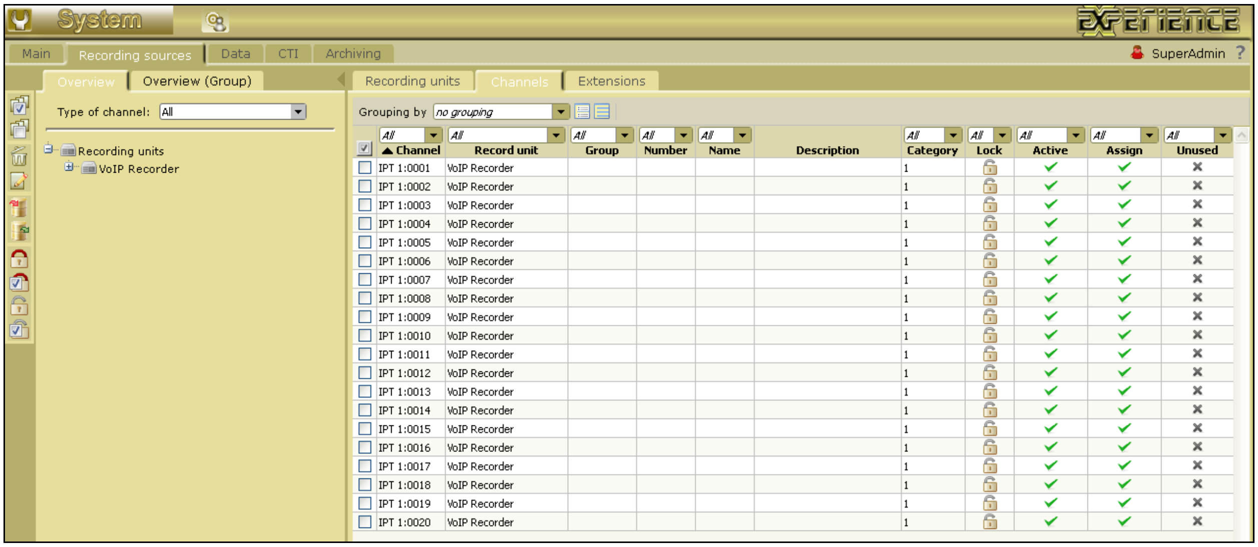
Click on the **Finish** button to finish the channel configuration.



Result of operation

ReDat VoIP Recorder (10.10.60.70) - No problem. Total 20 of 20 Loaded.
IPT 1:0001 - Loaded
IPT 1:0002 - Loaded
IPT 1:0003 - Loaded
IPT 1:0004 - Loaded
IPT 1:0005 - Loaded
IPT 1:0006 - Loaded
IPT 1:0007 - Loaded
IPT 1:0008 - Loaded
IPT 1:0009 - Loaded
IPT 1:0010 - Loaded
IPT 1:0011 - Loaded
IPT 1:0012 - Loaded

When the channel configuration is completed the following window will appear.



Type of channel: All

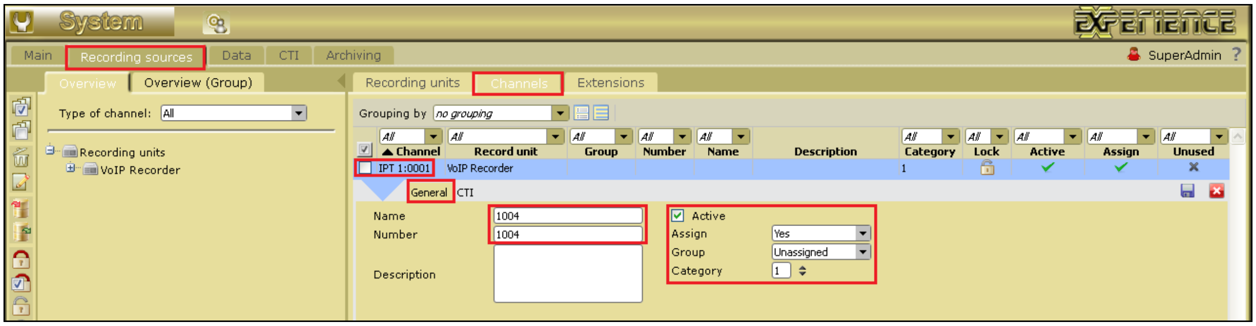
Grouping by no grouping

☑	Channel	Record unit	Group	Number	Name	Description	Category	Lock	Active	Assign	Unused
	All	All	All	All	All		All	All	All	All	All
□	IPT 1:0001	VoIP Recorder					1	🔓	✓	✓	✗
□	IPT 1:0002	VoIP Recorder					1	🔓	✓	✓	✗
□	IPT 1:0003	VoIP Recorder					1	🔓	✓	✓	✗
□	IPT 1:0004	VoIP Recorder					1	🔓	✓	✓	✗
□	IPT 1:0005	VoIP Recorder					1	🔓	✓	✓	✗
□	IPT 1:0006	VoIP Recorder					1	🔓	✓	✓	✗
□	IPT 1:0007	VoIP Recorder					1	🔓	✓	✓	✗
□	IPT 1:0008	VoIP Recorder					1	🔓	✓	✓	✗
□	IPT 1:0009	VoIP Recorder					1	🔓	✓	✓	✗
□	IPT 1:0010	VoIP Recorder					1	🔓	✓	✓	✗
□	IPT 1:0011	VoIP Recorder					1	🔓	✓	✓	✗
□	IPT 1:0012	VoIP Recorder					1	🔓	✓	✓	✗
□	IPT 1:0013	VoIP Recorder					1	🔓	✓	✓	✗
□	IPT 1:0014	VoIP Recorder					1	🔓	✓	✓	✗
□	IPT 1:0015	VoIP Recorder					1	🔓	✓	✓	✗
□	IPT 1:0016	VoIP Recorder					1	🔓	✓	✓	✗
□	IPT 1:0017	VoIP Recorder					1	🔓	✓	✓	✗
□	IPT 1:0018	VoIP Recorder					1	🔓	✓	✓	✗
□	IPT 1:0019	VoIP Recorder					1	🔓	✓	✓	✗
□	IPT 1:0020	VoIP Recorder					1	🔓	✓	✓	✗

7.5. Configure Extensions

Each extension to be monitored must be assigned to a channel. In the example below extension **1004** is assigned to the first channel (**IPT 1:0001**) that was previously configured. To assign the extension click on the **Recording sources** tab, followed by the **Channels** tab. Double click on the first channel and select the **General** tab, and enter the following:

- **Number** Enter an extension that will be monitored (Station number)
- **Name** Enter the name assigned to the Extension
- **Active** Click the **Active** check box
- **Assign** Select **Yes** from the dropdown box
- **Group** Select **Unassigned** from the dropdown box
- **Category** Select **1**



Channel	Record unit	Group	Number	Name	Description	Category	Lock	Active	Assign	Unused
All	All	All	All	All		All	All	All	All	All
□ IPT 1:0001	VoIP Recorder					1	🔓	✓	✓	✗

General | CTI

Name 1004
Number 1004
Description

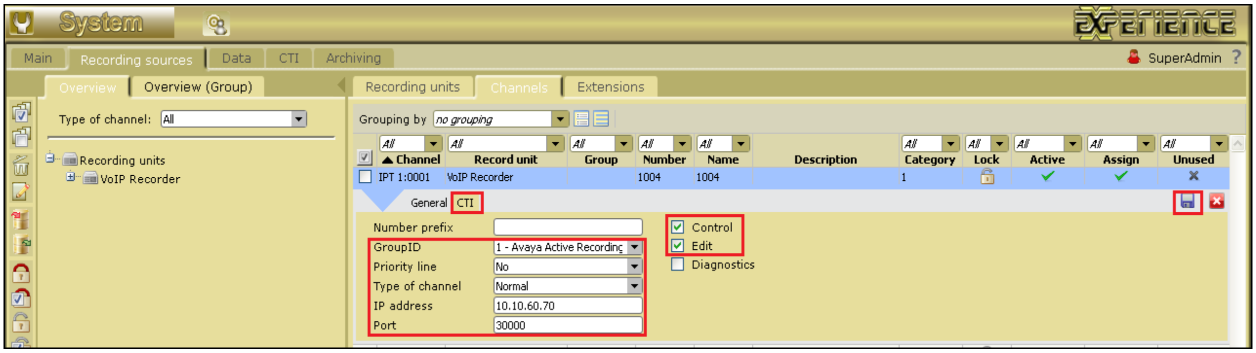
☑ Active
Assign Yes
Group Unassigned
Category 1

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

- **Group ID** Select **Avaya Active Recording** from the dropdown box
- **Priority line** Select **No** from the dropdown box
- **Type of channel** Select **Normal** from the dropdown box
- **IP address** Enter the IP address of the ReDat server
- **Port** Enter **3000**

Check the **Control** and **Edit** check boxes. Click on the **Save** icon highlighted to save.

Note: Repeat these steps for each extension that is to be monitored**.** Also note that 2 ports are required for each extension, therefore the next port should be 3002 and so on.



Channel	Record unit	Group	Number	Name	Description	Category	Lock	Active	Assign	Unused
All	All	All	All	All		All	All	All	All	All
□ IPT 1:0001	VoIP Recorder		1004	1004		1	🔓	✓	✓	✗

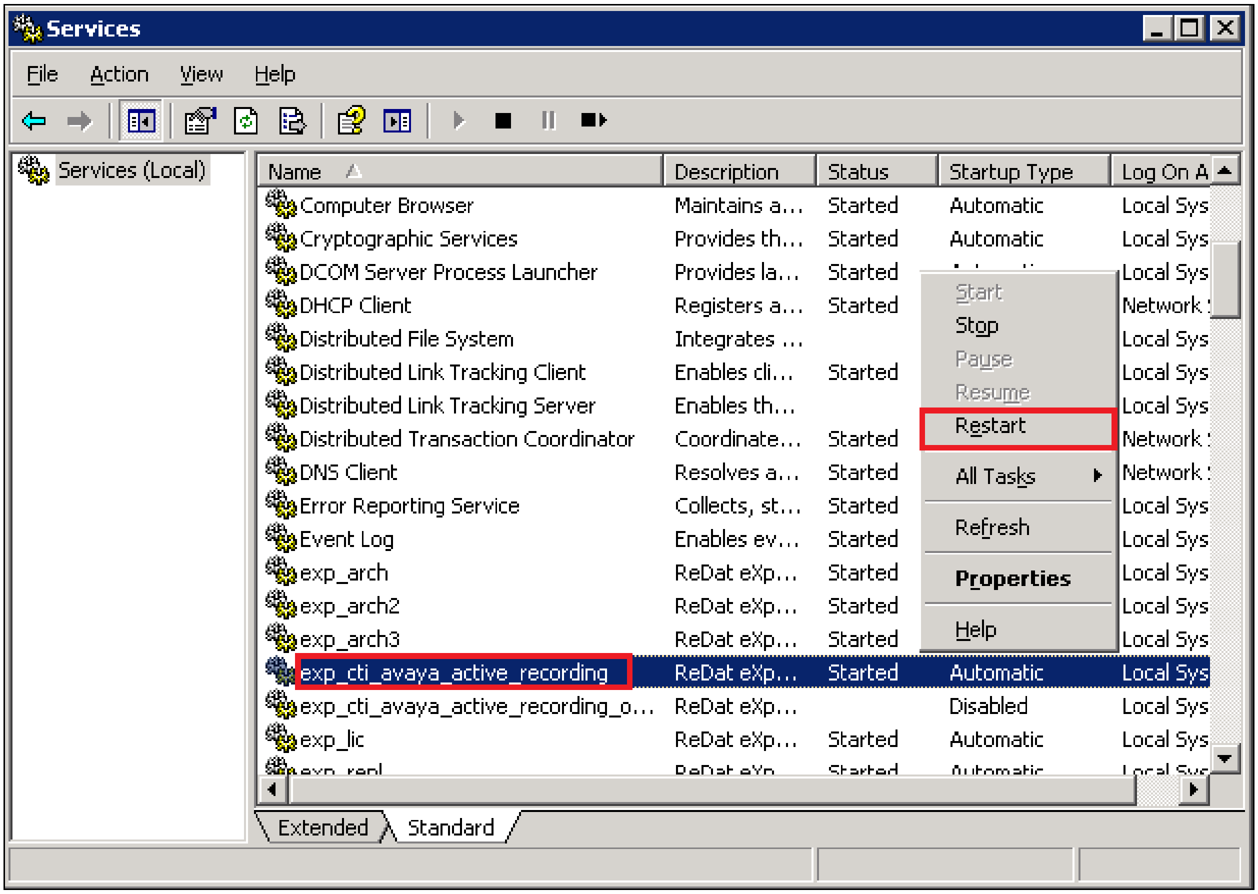
General | CTI

Number prefix
GroupID 1 - Avaya Active Recording
Priority line No
Type of channel Normal
IP address 10.10.60.70
Port 30000

☑ Control
☑ Edit
□ Diagnostics

7.6. 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**.



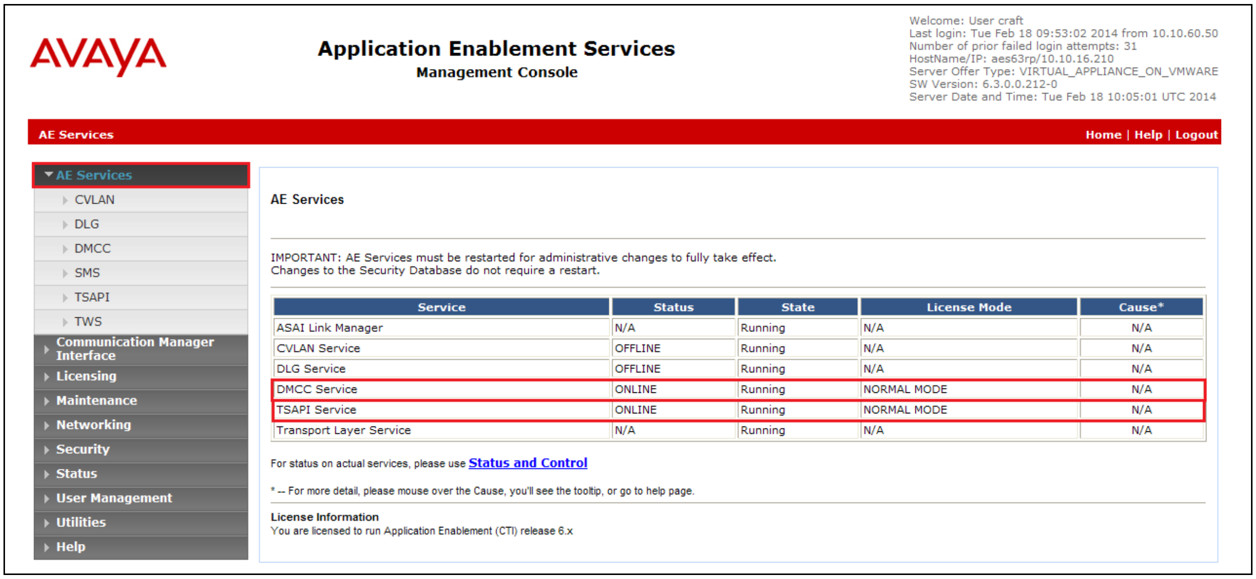
Name	Description	Status	Startup Type	Log On A
Computer Browser	Maintains a...	Started	Automatic	Local Sys
Cryptographic Services	Provides th...	Started	Automatic	Local Sys
DCOM Server Process Launcher	Provides la...	Started		Local Sys
DHCP Client	Registers a...	Started		Network :
Distributed File System	Integrates ...			Local Sys
Distributed Link Tracking Client	Enables cli...	Started		Local Sys
Distributed Link Tracking Server	Enables th...			Local Sys
Distributed Transaction Coordinator	Coordinate...	Started		Network :
DNS Client	Resolves a...	Started		Network :
Error Reporting Service	Collects, st...	Started		Local Sys
Event Log	Enables ev...	Started		Local Sys
exp_arch	ReDat eXp...	Started		Local Sys
exp_arch2	ReDat eXp...	Started		Local Sys
exp_arch3	ReDat eXp...	Started		Local Sys
exp_cti_avaya_active_recording	ReDat eXp...	Started	Automatic	Local Sys
exp_cti_avaya_active_recording_o...	ReDat eXp...		Disabled	Local Sys
exp_lic	ReDat eXp...	Started	Automatic	Local Sys
exp_repl	ReDat eXp...	Started	Automatic	Local Sys

8. Verification Steps

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



Welcome: User craft
Last login: Tue Feb 18 09:53:02 2014 from 10.10.60.50
Number of prior failed login attempts: 31
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Feb 18 10:05:01 UTC 2014

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.

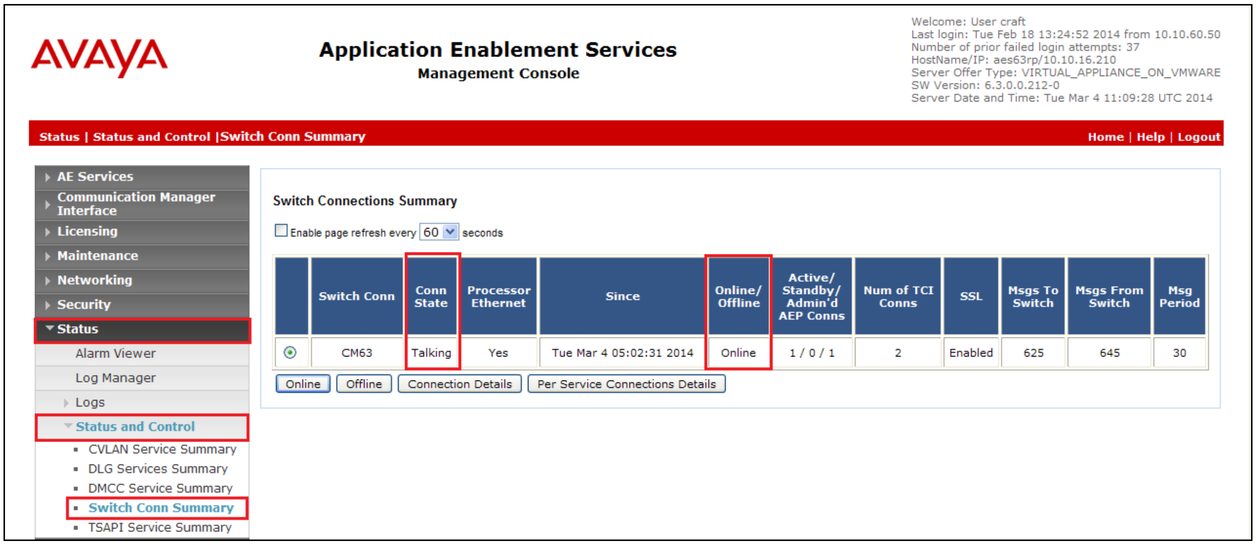
Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A

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) release 6.x

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



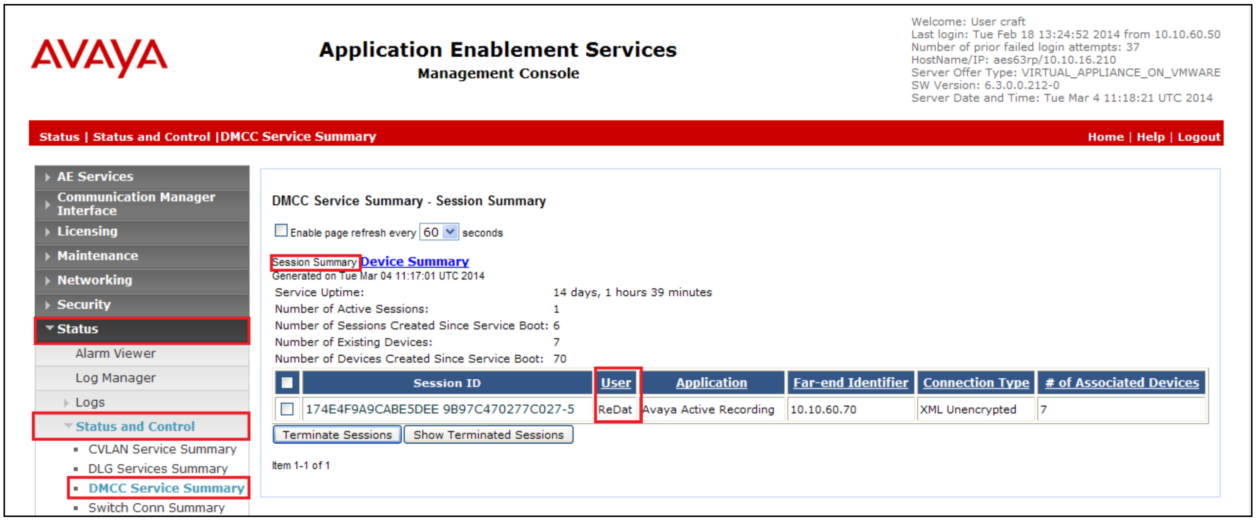
Welcome: User craft
Last login: Tue Feb 18 13:24:52 2014 from 10.10.60.50
Number of prior failed login attempts: 37
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Mar 4 11:09:28 UTC 2014

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

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



Welcome: User craft
Last login: Tue Feb 18 13:24:52 2014 from 10.10.60.50
Number of prior failed login attempts: 37
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Mar 4 11:18:21 UTC 2014

DMCC Service Summary - Session Summary

☐ Enable page refresh every 60 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

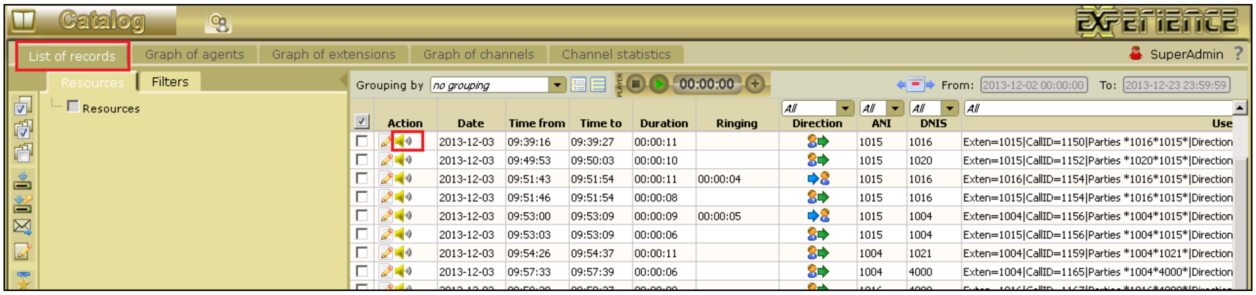
☐	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
☐	174E4F9A9CABE5DEE 9B97C470277C027-5	ReDat	Avaya Active Recording	10.10.60.70	XML Unencrypted	7

Terminate Sessions | Show Terminated Sessions

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.



Grouping by: no grouping

From: 2013-12-02 00:00:00 To: 2013-12-23 23:59:59

☑	Action	Date	Time from	Time to	Duration	Ringing	Direction	ANI	DNIS	Use
							All	All	All	All
☐	✎🔊	2013-12-03	09:39:16	09:39:27	00:00:11		👤→	1015	1016	Exten=1015|CallID=1150|Parties *1016*1015*|Direction
☐	✎🔊	2013-12-03	09:49:53	09:50:03	00:00:10		👤→	1015	1020	Exten=1015|CallID=1152|Parties *1020*1015*|Direction
☐	✎🔊	2013-12-03	09:51:43	09:51:54	00:00:11	00:00:04	→👤	1015	1016	Exten=1016|CallID=1154|Parties *1016*1015*|Direction
☐	✎🔊	2013-12-03	09:51:46	09:51:54	00:00:08		👤→	1015	1016	Exten=1015|CallID=1154|Parties *1016*1015*|Direction
☐	✎🔊	2013-12-03	09:53:00	09:53:09	00:00:09	00:00:05	→👤	1015	1004	Exten=1004|CallID=1156|Parties *1004*1015*|Direction
☐	✎🔊	2013-12-03	09:53:03	09:53:09	00:00:06		👤→	1015	1004	Exten=1015|CallID=1156|Parties *1004*1015*|Direction
☐	✎🔊	2013-12-03	09:54:26	09:54:37	00:00:11		👤→	1004	1021	Exten=1004|CallID=1159|Parties *1004*1021*|Direction
☐	✎🔊	2013-12-03	09:57:33	09:57:39	00:00:06		👤→	1004	4000	Exten=1004|CallID=1165|Parties *1004*4000*|Direction

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 Multiple Registrations. 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 6.3, October 2013, Document Number 03-300509, Issue 9.0.*

[2] *Avaya Aura® Communication Manager Feature Description and Implementation, Release 6.3, May 2013, Document Number 555-245-205, Issue 10.0.*

[3] *Administering Avaya Aura® Session Manager, Release 6.3, Issue 3 October 2013*

[4] *Administering Avaya Aura® System Manager, Release 6.3, Issue 3, October, 2013*

[5] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide, Release 6.3, Issue 2 October 2013*

Technical documentation for Retia can be found at the following location:
http://www.redat.eu/en/

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*.