Avaya Solution & Interoperability Test Lab

Application Notes for Calabrio Monitoring and Recording Services with Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the Calabrio Monitoring and Recording Services solution to interoperate with Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services. Calabrio Monitoring and Recording Services uses real-time CTI data and RTP streams from Communication Manager to capture and produce recordings of phone activity for agents and knowledge workers.

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

Calabrio Monitoring and Recording Services is a contact center and knowledge worker oriented recording solution. Using DMCC Multiple Registrations, and JTAPI, the recorder is able to register with Avaya Aura™ Communication Manger as an additional media endpoint for call activity occurring on the target agent and knowledge worker phones, with JTAPI providing call tagging data. These calls are recorded and stored with identifying information for cataloging and retrieval.

The interoperability of Monitoring and Recording Services with Avaya Aura™ Communication Manager is accomplished through Avaya Aura™ Application Enablement Services. These Application Notes describe the compliance test configuration used to test Calabrio Monitoring and Recording Services, with Avaya Aura™ Communication Manager running on an Avaya S8300D Server and an Avaya G450 Media Gateway.

Before Monitoring and Recording Services can start recording, it registers with Avaya Aura™ Application Enablement Services, performs an SMS service query to obtain a list of all of the Agents and Stations configured in Avaya Aura™ Communication Manager, and the administrator then associates this data with devices to be recorded by the application. The application uses a static assignment of Call Center agents, and Knowledge Workers, to the station that they work at. Dynamic assignment is not supported for any of the communication platforms supported by Monitoring and Recording Services. Future revisions of the application are expected to support dynamic assignment for free seating environments.
When the services are started on the Monitoring and Recording Services server, stations that are administered to be recorded are registered with Avaya Aura™ Communication Manager as a Dependent registration using the DMCC service on Avaya Aura™ Application Enablement Services. Once DMCC registration is successfully completed, Avaya Aura™ Communication Manager will send audio for all calls that originate or terminate on the registered stations to both the phone, and the recorder.

To ensure call records stored in the database are as rich as possible, the application uses the TSAPI/JTAPI capabilities of Avaya Aura™ Application Enablement Services to monitor the station activity. This occurs following successful DMCC registrations. If DMCC registration fails, the JTAPI associations are not requested by the application.

1.1. Interoperability Compliance Testing

Compliance testing focused on the following areas, covered in the DevConnect Test Plan for Communication Manager and Application Enablement Services and Monitoring and Recording Services:

Phase 1 Installation & Configuration

Phase 2 Calabrio/Avaya Feature Functionality Verification

Phase 3 Failover and Serviceability Tests

Installation and configuration testing focused on the setup of all components and the ability to interoperate. The functionality testing focused on verifying Monitoring and Recording Services ability to detect, record, and search calls, while recording and storing recordings appropriately with basic telephony features. Serviceability testing focused on verifying the ability of Monitoring and Recording Services to recover from adverse conditions.

1.2. Support

Technical support on Calabrio Monitoring and Recording Services can be obtained through the following:

- **Phone: +1 (763) 592-4680 or +1 (800) 303-1248**
- **Web: www.calabrio.com/support**
- **Email: calabriosupport@calabrio.com**

2. Reference Configuration

Calabrio Monitoring and Recording Services can be configured on a single Windows Server, or distributed across multiple servers for larger scale deployments. The compliance test configuration used a single server configuration.

The detailed administration of basic connectivity between Avaya Aura™ Communication Manager, Avaya Aura™ Application Enablement Services, and of contact center devices, are not the focus of these Application Notes and will not be fully described.

In the compliance testing, the Monitoring and Recording Services solution was configured to monitor three physical station extensions "6001 - 6003" on Avaya Aura™ Communication Manager as well as two IP Agent stations "6004 – 6005" with one configured in Telecommuter mode, the other in Road Warrior mode. As DMCC Multiple Registrations functionality does not support Extension to Cellular (EC500) functionality, this scenario was not tested.

The interoperability of Monitoring and Recording Services with Avaya Aura™ Communication Manager is accomplished through Avaya Aura™ Application Enablement Services. The compliance test configuration used to test Monitoring and Recording Services included the Avaya S8300D Server, the Avaya G450 Media Gateway, Avaya Aura™ Application Enablement Services, Windows 2008 Server, soft clients, and telephones. **Figure 1** provides a high level topology.

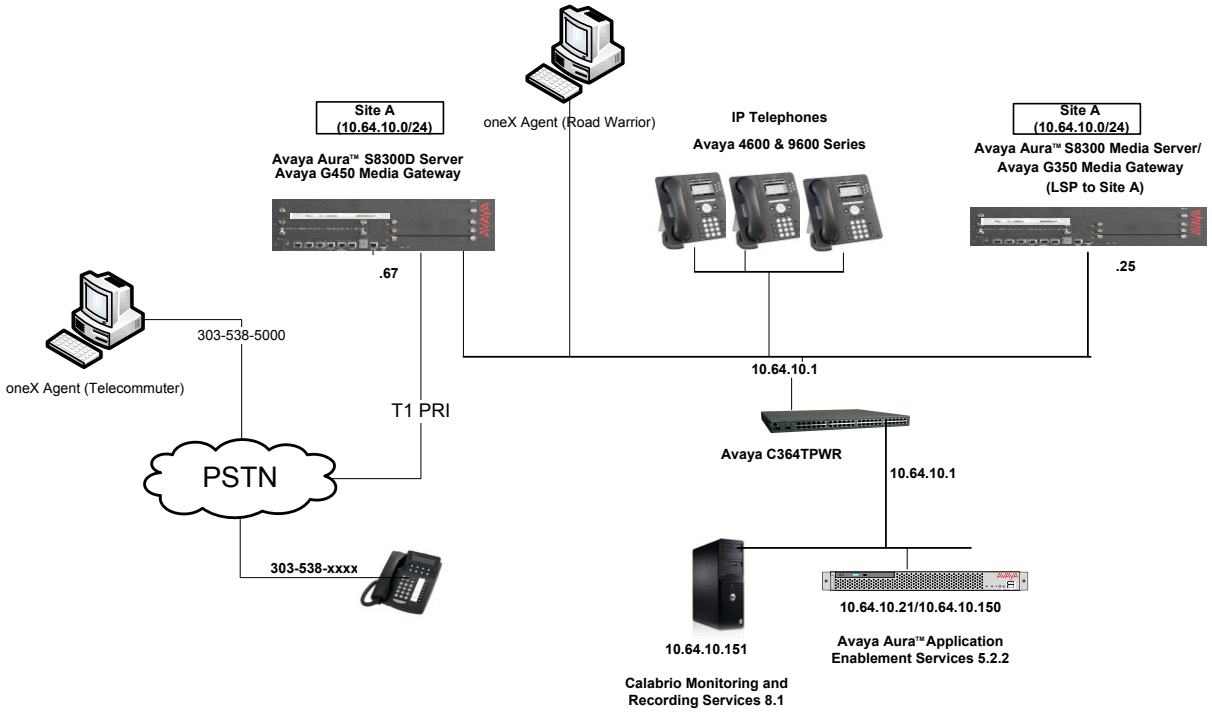


Figure 1: Calabrio Monitoring and Recording Services Compliance Test Sample Configuration

3. Equipment and Software Validated

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

Hardware/Software Component	Version/Description
Avaya S8300 Server and G450 Media Gateway	Avaya Aura™ Communication Manager 6.0 (R016x.00.0.345.0) with Cold Patch 18444
Avaya Aura™ Application Enablement Services	Release 5.2.2.105.0
Avaya 9600 and 2400 Series IP Telephones, and IP Agent	9620, 9630, 9640 (H.323), 2421 (H.323),
Avaya one-X™ Agent, Avaya IP Agent	R2, R7.0
Calabrio Monitoring and Recording Services on Windows 2008 Server, MS SQL 2008	8.1

4. Configure Avaya Aura™ Communication Manager

All the configuration changes in this section for Avaya Aura™ Communication Manager are performed through the System Access Terminal (SAT) interface. For more information on configuring Avaya Aura™ Communication Manager, refer to the Avaya product documentation, Reference [1].

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

- Verify Feature and License are adequate for the integration
- Administer Processor Ethernet Interface for Avaya Aura™ Application Enablement Services connectivity
- Administer Avaya Aura™ Communication Manager System Features
- Administer Computer Telephony Integration (CTI) Link
- Add SMS User Account
- Confirm Station Administration

The detailed administration of contact center entities, such as VDN, Skill, Split, Logical Agents and Station Extensions are assumed to be in place and are not covered in these Application Notes.

4.1. Verify Feature and License are adequate for the integration

Applications that use Application Enablement Services TSAPI must have **Computer Telephony Adjunct Links** enabled on Communication Manager. This feature entitlement is provided with each TSAPI license. TSAPI entitlements must be activated in both licenses. If this option is not set to "**y**", contact the Avaya sales team or business partner for a proper license file.

```
display system-parameters customer-options                    Page   3 of  11
                              OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                      CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                        CAS Main? n
Answer Supervision by Call Classifier? y                 Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n                       DCS (Basic)? y
          ASAI Link Core Capabilities? n                DCS Call Coverage? y
          ASAI Link Plus Capabilities? n               DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                          DS1 MSP? y
                                  ATMS? y              DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```

Unlike many DMCC recording solutions, the Calabrio Monitoring and Recording Services solution does not require additional stations to be configured, nor will it consume IP_API_A registration licenses due to only being supported on Communications Manager R5 or later and Application Enablement Services R5.1 or later and the fact that it uses the DMCC Multiple Registrations method.

4.2. Administer Processor Ethernet Interface for Application Enablement Services Connectivity

Enter the **change node-names ip** command. The Application Enablement Services and **procr** node-names need to be defined here. The actual IP address may vary.

```
change node-names ip                                          Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
aesserver2              10.64.10.21
default                 0.0.0.0
procr                   10.64.10.67
procr6                  ::
```

On most R6 servers, the Processor Ethernet Interface will already be administered in the ip-interface list. The **display ip-interface procr** command will display the parameters of the Processor Ethernet Interface.

```
display ip-interface procr                                    Page   1 of   2
                                  IP INTERFACES

                  Type: PROCR
                                                   Target socket load: 4800

      Enable Interface? y                        Allow H.323 Endpoints? y
                                                  Allow H.248 Gateways? y
        Network Region: 1                          Gatekeeper Priority: 5

                                 IPV4 PARAMETERS
             Node Name: procr                   IP Address: 10.64.10.67

            Subnet Mask: /24
```

```
display ip-interface procr                                    Page   2 of   2
                                  IP INTERFACES

                 Speed: 100Mbps
                Duplex: Full

                                 IPV6 PARAMETERS
             Node Name: procr6
            IP Address: ::

            Subnet Mask: /64
      Enable Interface? n
```

Add an entry for Application Enablement Services as described below:

- Enter the **change ip-services** command.
- In the **Service Type** field, type **AESVCS**.
- In the **Enabled** field, type **y**.
- In the **Local Node** field, type the Node name **procr** for the Processor Ethernet Interface.
- In the **Local Port** field, use the default of **8765**.
- Note that in installations using CLAN connectivity, each CLAN interface would require similar configuration [Reference 2].

```
change ip-services                                          Page   1 of   4

                                  IP SERVICES
 Service      Enabled     Local      Local       Remote      Remote
  Type                    Node       Port        Node        Port
AESVCS         y       procr          8765
CDR1                   procr          0       MTS             9000
CDR2                   procr          0       RDTT            9001
```

On Page 4 of the IP Services form, enter the following values:

- In the **AE Services Server** field, type the name obtained from the Application Enablement Services server.
- In the **Password** field, type the same password to be administered on the Application Enablement Services server.
- In the **Enabled** field, type **y**.

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

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:       aesserver2         *                   y        in use
```

Note that the name and password entered for the **AE Services Server** and **Password** fields must match the name and password on the Application Enablement Services server. The administered name for the Application Enablement Services server is created as part of the Application Enablement Services installation, and can be obtained from the Application Enablement Services server by typing **uname –n** at the Linux command prompt.

4.3. Administer Communication Manager System Features

Enter the **change system-parameters features** command and ensure that **Create Universal Call ID (UCID)** is enabled system wide on page 5, and that **Send UCID to ASAI** is set to "**y**" on page 13. Monitoring and Recording Services relies on UCID to track complex calls (Transfers and Conferences).

```
change system-parameters features                                Page   5 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:               Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                                    Switch Name:
           Emergency Extension Forwarding (min): 10
         Enable Inter-Gateway Alternate Routing? n
Enable Dial Plan Transparency in Survivable Mode? n
                             COR to Use for DPT: station

MALICIOUS CALL TRACE PARAMETERS
               Apply MCT Warning Tone? n   MCT Voice Recorder Trunk Group:
      Delay Sending RELease (seconds): 0
SEND ALL CALLS OPTIONS
     Send All Calls Applies to: station    Auto Inspect on Send All Calls? n
             Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
     Create Universal Call ID (UCID)? y    UCID Network Node ID: 1
```

```
change system-parameters features                                Page  13 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
 CALL CENTER MISCELLANEOUS
          Callr-info Display Timer (sec): 10
                         Clear Callr-info: next-call
       Allow Ringer-off with Auto-Answer? n

    Reporting for PC Non-Predictive Calls? n


          Interruptible Aux Notification Timer (sec): 3


  ASAI
            Copy ASAI UUI During Conference/Transfer? n
       Call Classification After Answer Supervision? n
                                  Send UCID to ASAI? y
          For ASAI Send DTMF Tone to Call Originator? y
```

4.4. Administer Computer Telephony Integration (CTI) Link

This section provides the steps required for configuring a CTI Link.

Enter the **add cti-link <link number>** command, where **<link number>** is an available CTI link number.

- In the **Extension** field, type **<station extension>**, where **<station extension>** is a valid station extension.
- In the **Type** field, type **ADJ-IP**.
- In the **Name** field, type a descriptive name.

```
add cti-link 1                                              Page   1 of   3
                                  CTI LINK
 CTI Link: 1
Extension: 6201
     Type: ADJ-IP
                                                                    COR: 1
     Name: AES-10.64.10.21
```

```
add cti-link 1                                              Page   2 of   3
                                  CTI LINK
FEATURE OPTIONS
      Event Minimization? n        Special Character for Restricted Number? n
      IC Adjunct Routing? n   Send Disconnect Event for Bridged Appearance? n
                                        Two-Digit Aux Work Reason Codes? n
                                            Block CMS Move Agent Events? n
```

```
add cti-link 1                                              Page   3 of   3
                                  CTI LINK
Bridged Appearance Origination Restriction? n

            SAC/CF Override: n
```

4.5. Add SMS User Account

Monitoring and Recording Services uses the Application Enablement Services SMS interface to query for administered Stations and Agents for use in administering the application.

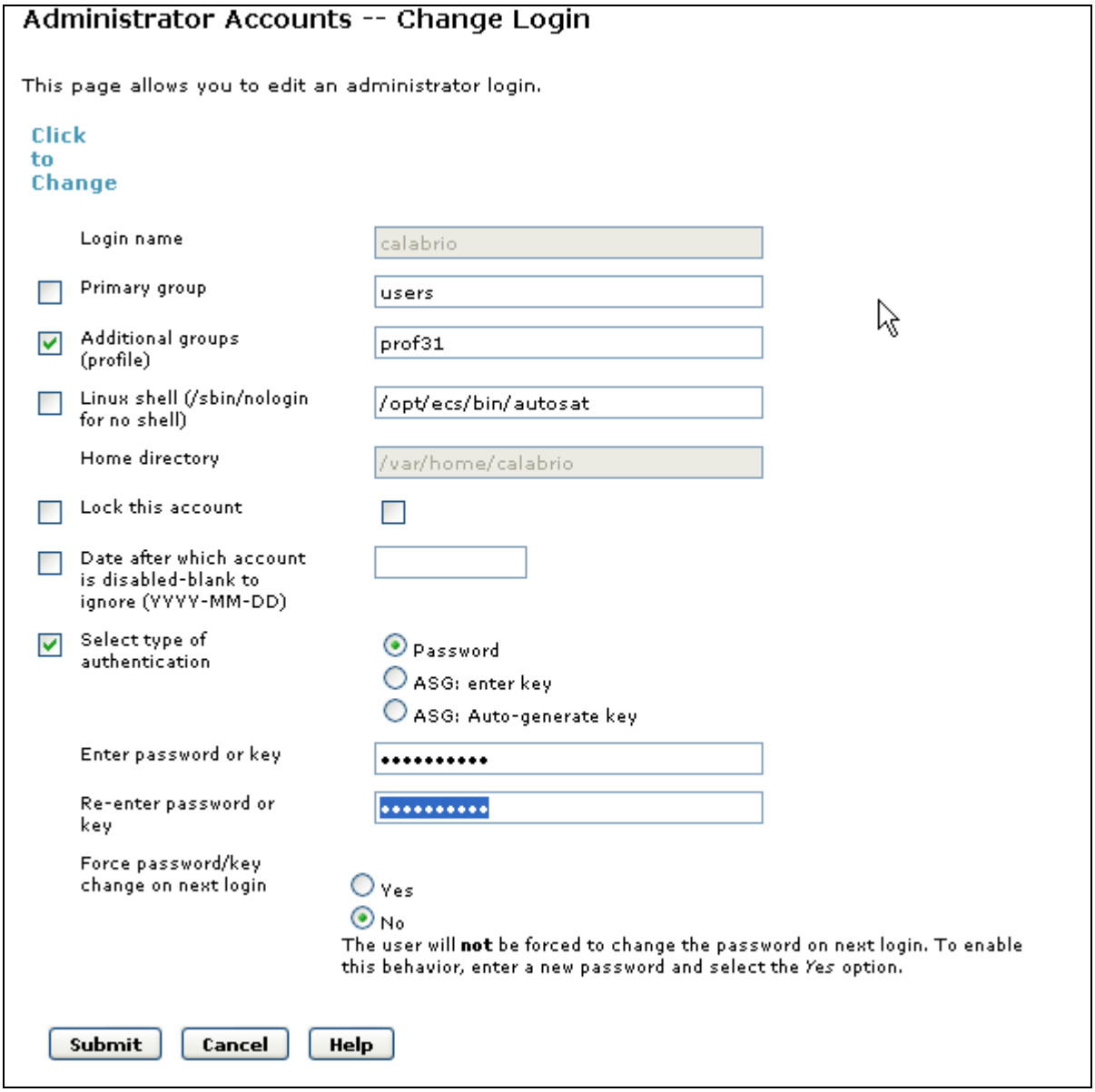
A privileged user was used in this test, however, a local administrator would likely want to restrict the user account. This involves creating a user profile at the SAT, and then creating and assigning that user to the profile in the web admin pages. To illustrate, **User Profile 31** was created as shown below:

```
add user-profile 31                                          Page   1 of  41
                              USER PROFILE 31

User Profile Name: Calabrio SMS

       This Profile is Disabled? n               Shell Access? y
Facility Test Call Notification? n   Acknowledgement Required? n
     Grant Un-owned Permissions? n          Extended Profile? n

             Name           Cat Enbl           Name                 Cat Enbl
                    Adjuncts A   n           Routing and Dial Plan J   n
                Call Center B   y                        Security K   n
                   Features C   n                         Servers L   n
                   Hardware D   n                        Stations M   y
                Hospitality E   n               System Parameters N   n
                         IP F   n                    Translations O   n
                Maintenance G   n                        Trunking P   n
Measurements and Performance H   n                           Usage Q   n
              Remote Access I   n                     User Access R   n
```

Read only access to Agents and Stations is required. Enter **'r-'** permissions for the **B** and **M** Categories on the **Set Permissions for Category:** entry on the **change user-profile xx** form (two separate transactions).

```
change user-profile 31                                       Page   3 of  41
                              USER PROFILE 31
 Set Permissions For Category: M  To: r-       Set All Permissions To:
'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance
                  Name          Cat  Perm
                     aesvcs link A    --
                   aesvcs-server A    --
                           agent B    r-
                   agent-loginID B    r-
                          alarms H    --
                   alias station M    r-
         alphanumeric-dial-table J    --
                   alternate-frl C    --
                         amw all G    --
                        amw asai G    --
                       amw audix G    --
                         amw pms G    --
           analog-testcall board G    --
```

Then, create a user account on the **System Management Interface** web page and assign the user account to the user-profile created above.



4.6. Confirm Station Administration

All stations that will be recorded must be IP Softphone enabled, and the application needs to know the **security code** in order to successfully register, shown below.

```
change station 6004                                          Page   1 of   4
                                  STATION

Extension: 6004                       Lock Messages? n              BCC: 0
     Type: 4620                       Security Code: 123456          TN: 1
     Port: S00147                   Coverage Path 1:                COR: 1
     Name: IP Agent #1              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: 6004
           Speakerphone: 1-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
```

5. Configure Avaya Aura™ Application Enablement Services

Avaya Aura™ Application Enablement Services enables applications to monitor and control telephony resources on Avaya Aura™ Communication Manager. The Avaya Aura™ Application Enablement Services server receives requests from applications and forwards them to Avaya Aura™ Communication Manager. Conversely, the Avaya Aura™ Application Enablement Services server receives responses and events from Avaya Aura™ Communication Manager and forwards them to the appropriate applications.

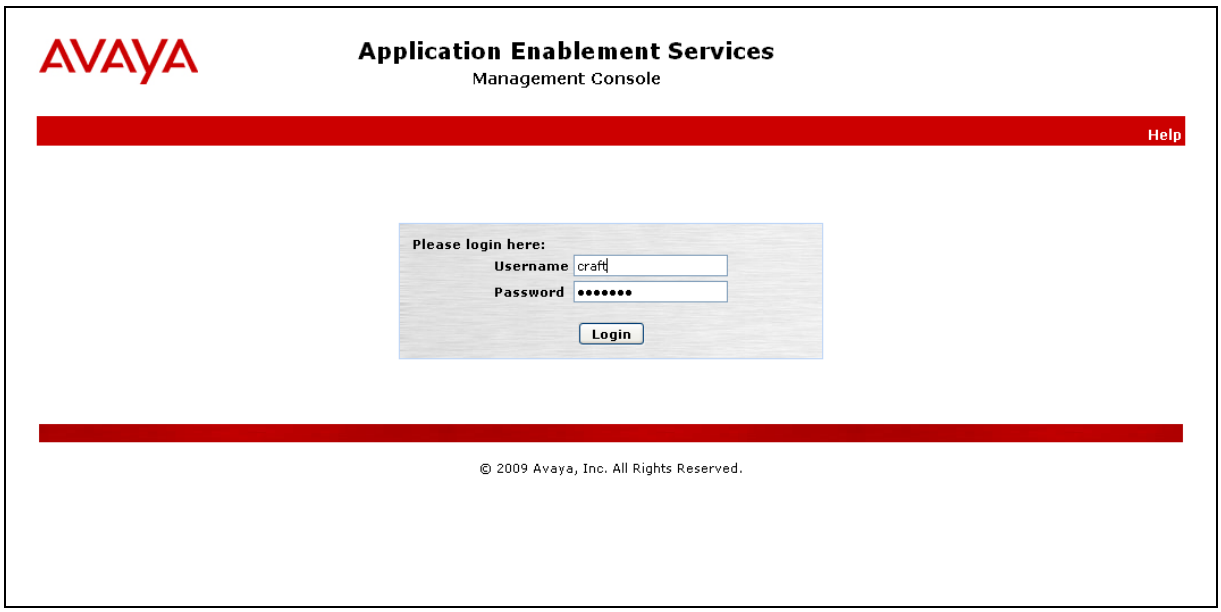
This section assumes that the installation and basic administration of the Avaya Aura™ Application Enablement Services server has already been performed. For more information on administering Avaya Aura™ Application Enablement Services, refer to the Avaya product documentation, Reference [2].

This section provides the procedures for configuring Avaya Aura™ Application Enablement Services. The procedures fall into the following areas:

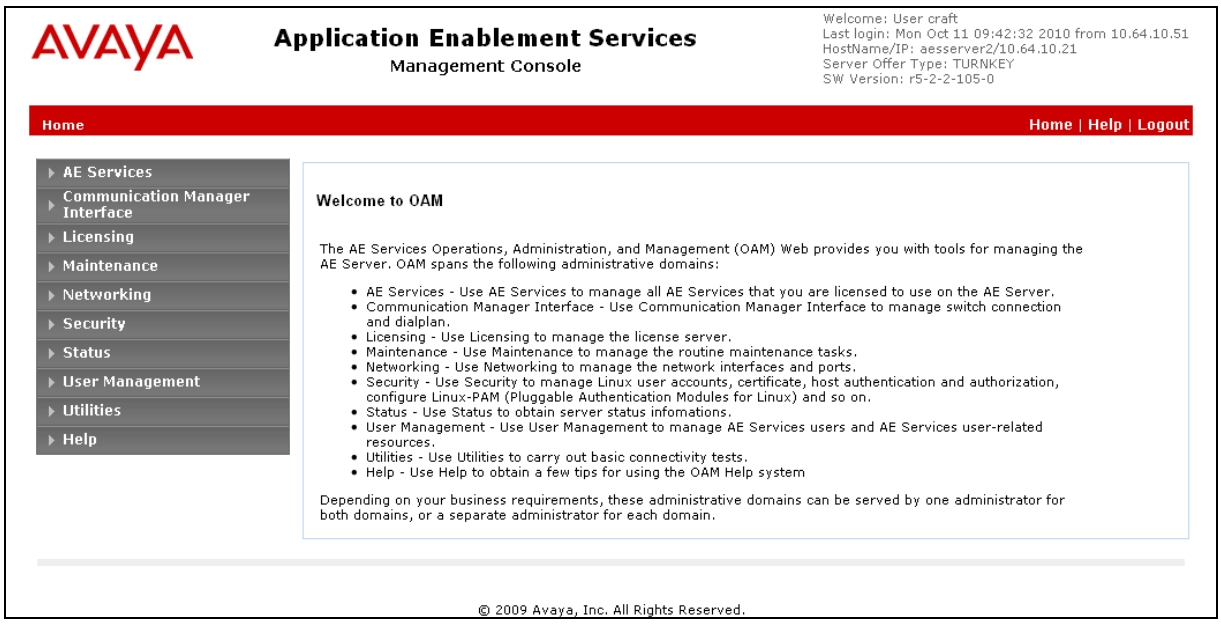
- Confirm Network Configuration
- Configure Avaya Aura™ Communication Manager Switch Connections
- Verify TSAPI and DMCC Licensing
- Add TSAPI Links

- Add CTI User
- Enable Unrestricted Access to the Security Database
- Note the T-Link Name

Access the web-based administration interface using **https://<ip-address>** in a browser where **<ip-address>** is the client interface address of the Avaya Aura™ Application Enablement server. Click on the **Continue to Login** link. Login using appropriate credentials.

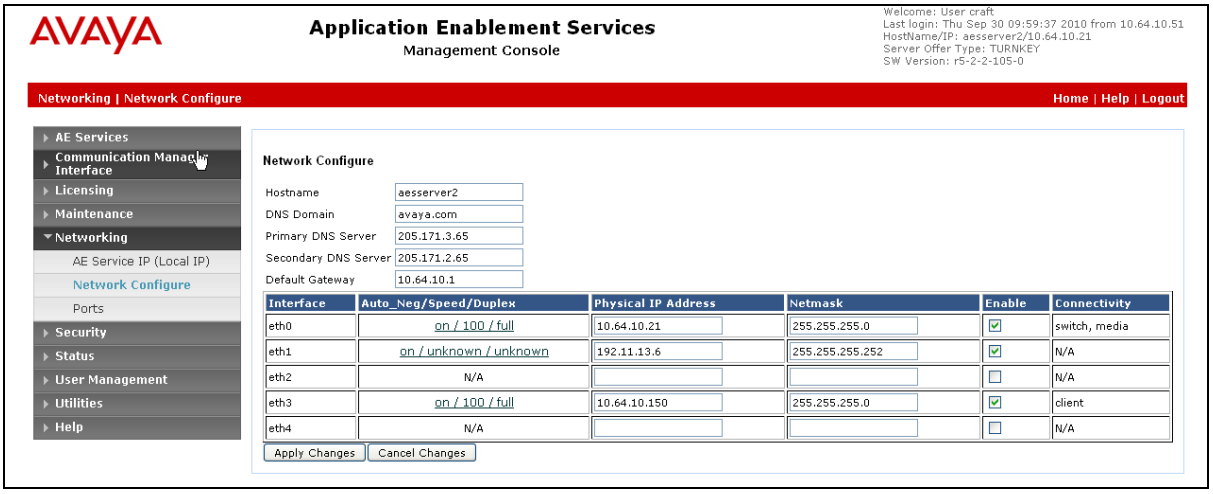


The **Welcome to OAM** screen is displayed next.



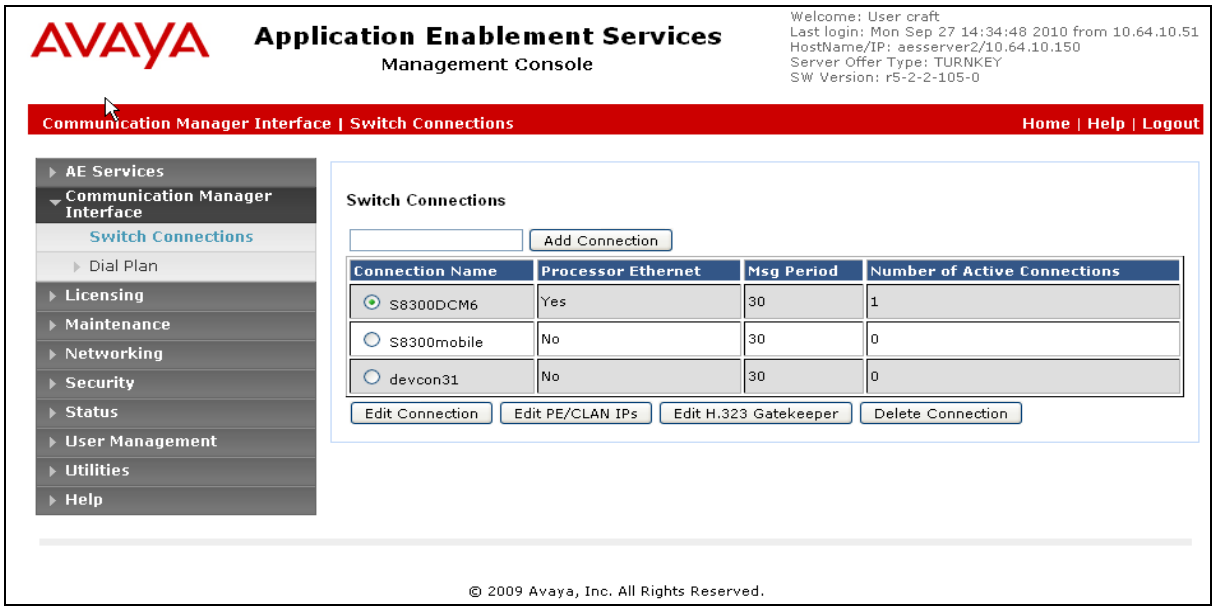
5.1. Confirm Network Configuration

Select **Networking > Network Configure** and note the client interface IP Address (**eth3** in this example) which will be used later in the application configuration. Application Enablement Services can be configured to use one or multiple NIC interfaces. It is preferable for security and performance reasons to use multiple interfaces and to have these on separate networks. The Communication Manager interface should always be bound to **eth0**.

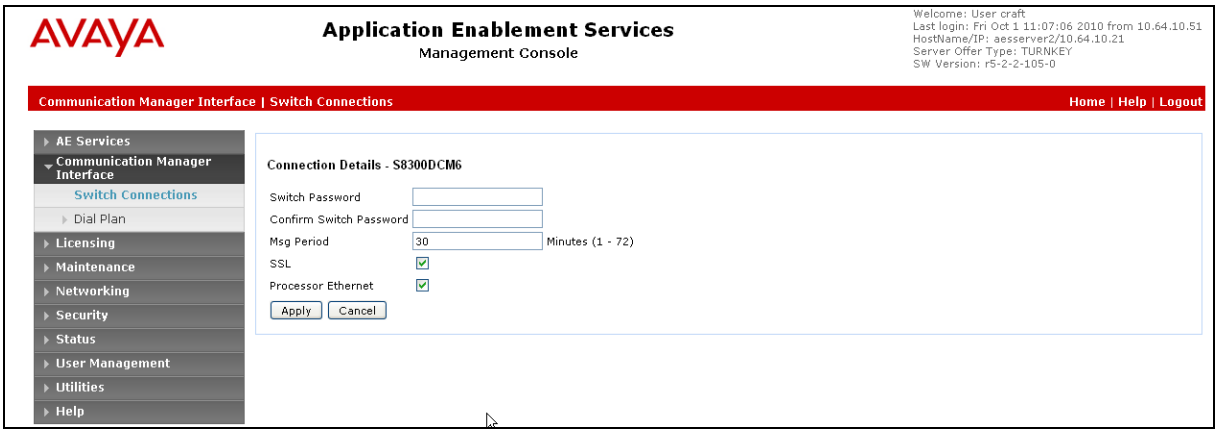


5.2. Configure Communication Manager Switch Connections

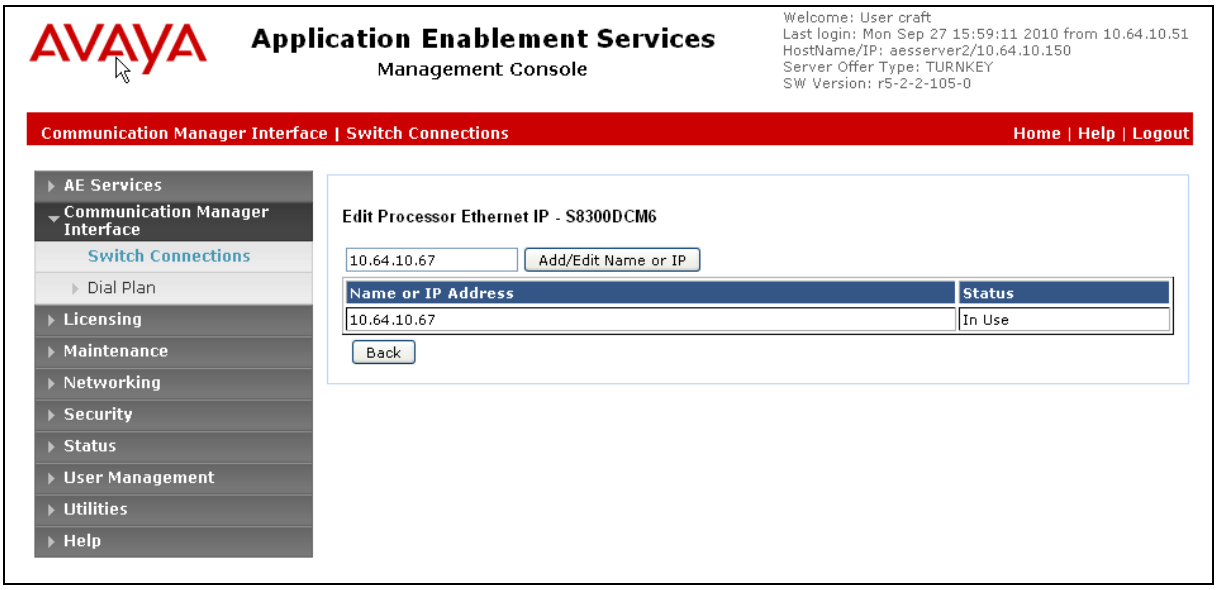
To add links to the Communication Manager, navigate to the **Communication Manager Interface > Switch Connections** page and enter a name for the new switch connection. This was previously configured as **S8300DCM6** for this test environment:



Use the **Edit Connection** button shown above to configure the **Switch Password**. This must match the password configured in section **4.2** above. Enter the **Switch Password** and check the **Processor Ethernet** box if using the **procr** interface, as shown below.



Use the **Edit PE/CLAN IPs** button (shown in this section's first screen shot above) to configure the **procr** or **CLAN** IP Address(es) for TSAPI message traffic.



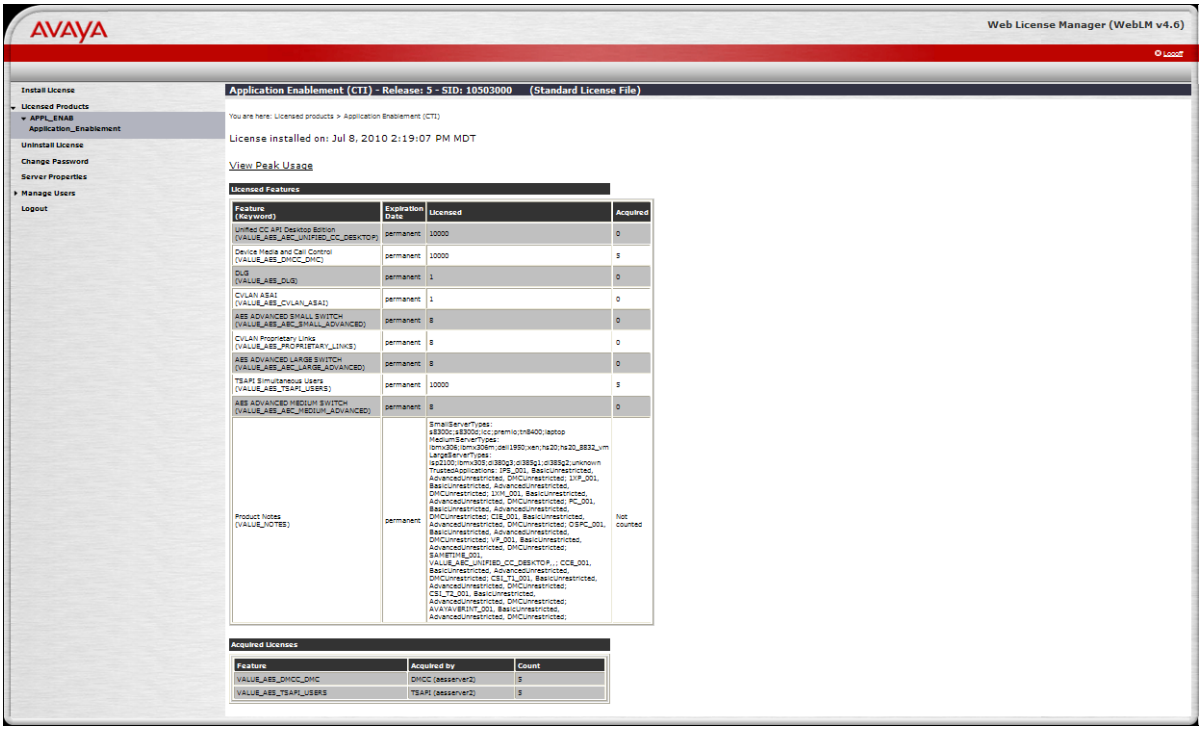
Use the **Edit H.323 Gatekeeper** button (shown in this section's first screen shot above) to configure the **procr** or **CLAN** IP Address(es) for DMCC registrations.

5.3. Verify TSAPI and DMCC Licensing

The Calabrio Monitoring and Recording Services application will consume a **TSAPI** and **DMCC_DMC** license for each station that is to be monitored and recorded. If the number of licenses are not adequate for the integration, contact Avaya sales or an authorized reseller.

Navigate to **Licensing > WebLM Server Access** and login using appropriate credentials. Select **Application_Enablement** under **Licensed Products > APPL_ENAB** to display entitlements and acquired licenses.

Note that integrations with older releases of Communication Manager will also consume an **IP_API_A** license in Communication Manager. With Communication Manager R5 and Application Enablement Services 4.1 and later, **IP_API_A** will only be consumed if adequate **DMCC_DMC** licenses are not available on Application Enablement Services.



The screenshot below gives a closer look at these license counts.

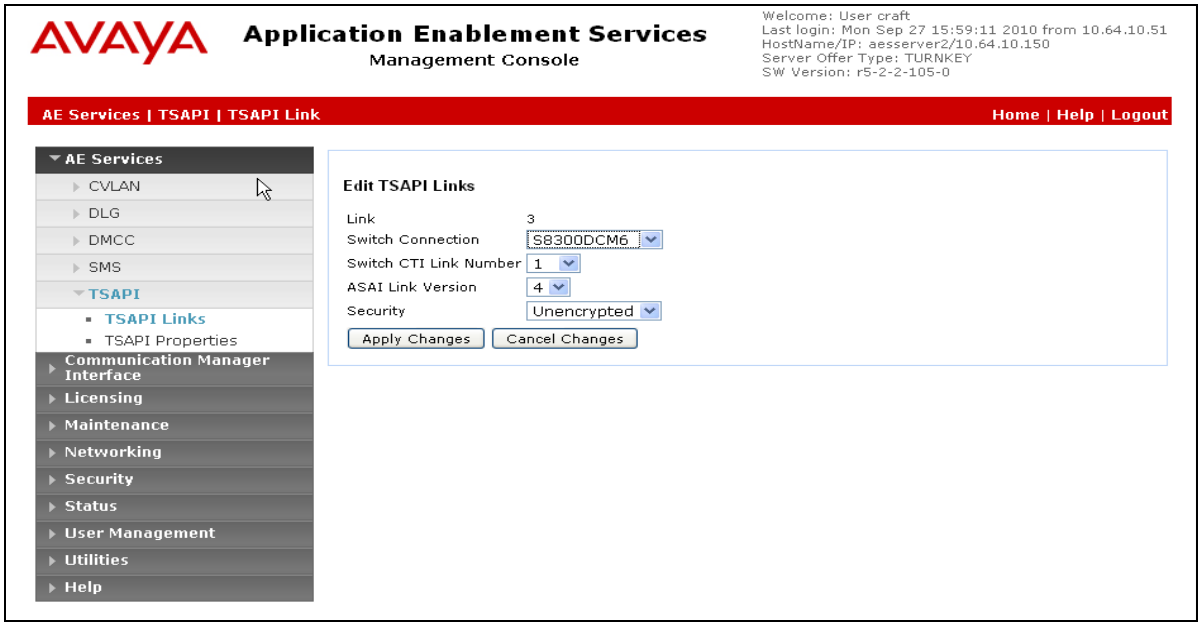
Feature (Keyword)	Expiration Date	Licensed	Acquired
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	10000	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	10000	5
DLG (VALUE_AES_DLG)	permanent	1	0
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	1	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	8	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	8	0
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	8	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	10000	5
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	permanent	8	0

5.4. Add TSAPI Links

Navigate to the **AE Services -> TSAPI -> TSAPI Links** page to add the TSAPI CTI Link. Click **Add Link**.

Select a Switch Connection using the drop down menu. Select the **Switch CTI Link Number** using the drop down menu. The CTI link number must match the number configured in the **cti-link** form in **Section 4.4**. Click **Apply Changes**.

If the application will use Encrypted Links, select **Encrypted** in the **Security** selection box.

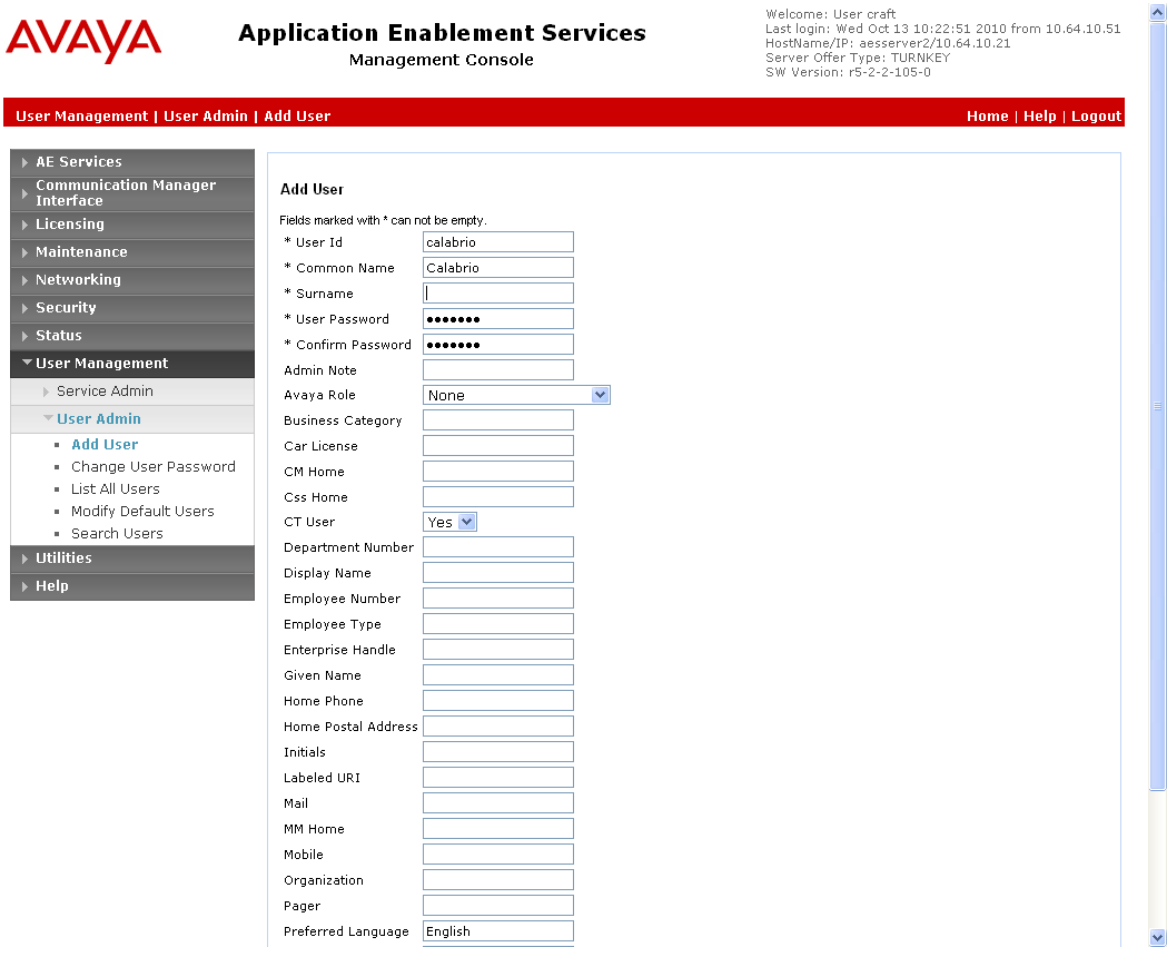


5.5. Add a CTI User

Monitoring and Recording Services requires a CTI user account to access Application Enablement Services. Select **User Management -> User Admin -> Add User** from the left pane.

In the **Add User** screen, enter the following values:

- In the **User Id** field, type a meaningful user id.
- In the **Common Name** field, type a descriptive name.
- In the **Surname** field, type a descriptive surname.
- In the **User Password** field, type a password for the user.
- In the **Confirm Password** field, re-enter the same password for the user.
- In the **Avaya Role** field, retain the default of **None**.
- In the **CT User** field, select **Yes** from the dropdown menu.
- Click **Apply** at the bottom of the screen (not shown here).

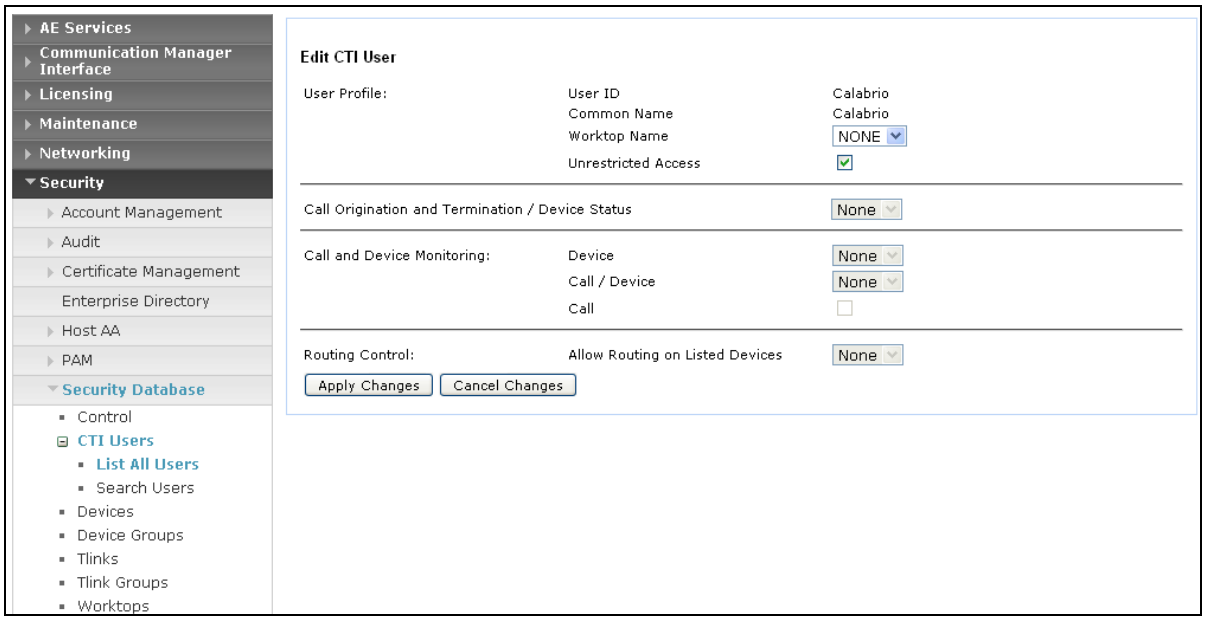


5.6. Enable Unrestricted Access to the Security Database

The Calabrio user account will require unrestricted SDB access in order to be able to access any of the Devices (stations) administered to be recorded in the application.

To change the security level for the CT User Select **Security -> Security Database -> CTI Users -> List All Users** from the left pane. Choose the CTI user, and click **Edit** (not shown below).

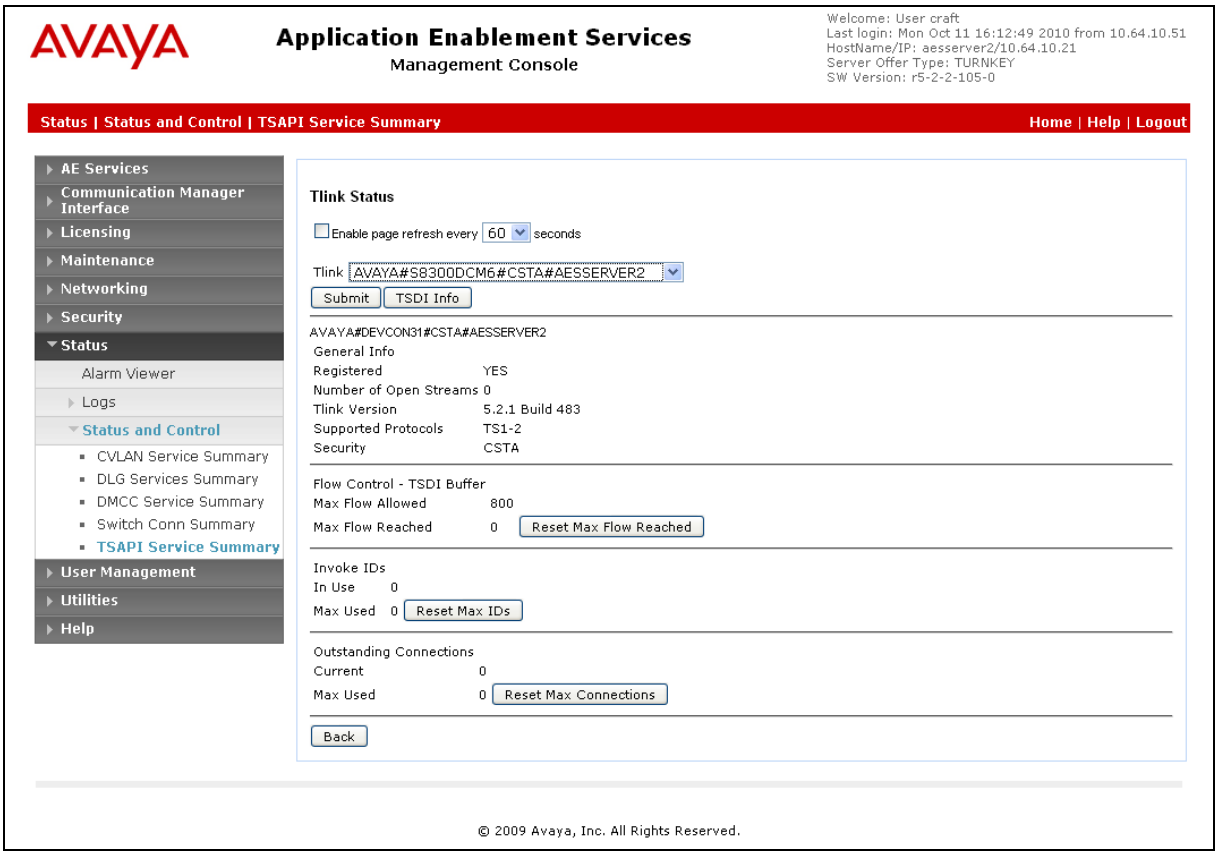
On the **Edit CTI User** page, check the **Unrestricted Access** option and click on **Apply Changes**.



5.7. Note the T-Link Name

This information will be used to confirm the application configuration below.

Select **Status > Status and Control > TSAPI Service Summary** from the left pane and select **Edit T-Links** (not shown below). Once at the **Edit T-Links** screen, this screen shows a select box of the Tlink names. A new Tlink name is automatically generated by the Application Enablement Services server upon creation of a new switch connection. Locate and select the Tlink name associated with the relevant switch connection which would use the name of the switch connection as part of the Tlink name (not shown below). This screen will also provide information on the status of the TLink as shown below:



6. Configure the Monitoring and Recording Services server

This section provides the procedures for configuring the Monitoring and Recording Services server. The procedures include the following areas:

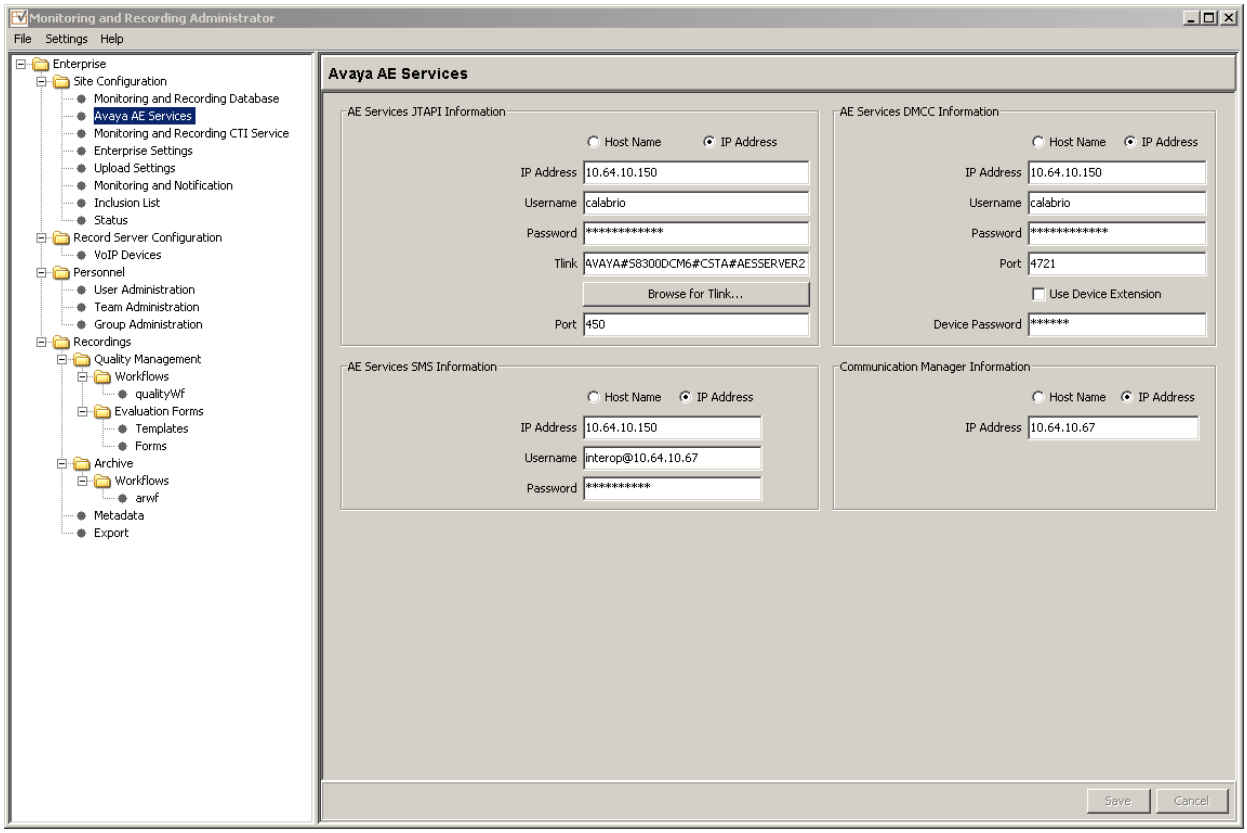
- Configuration of the Avaya Aura™ Application Enablement Interfaces
- Configuration of Devices and Agents
- Launch Calabrio User Interface
- View Recorded Calls

The initial configuration of the Monitoring and Recording Services server is typically performed by Calabrio technicians or authorized installers. The procedural steps are presented in these Application Notes for informational purposes.

6.1. Configuration of the Application Enablement Interfaces

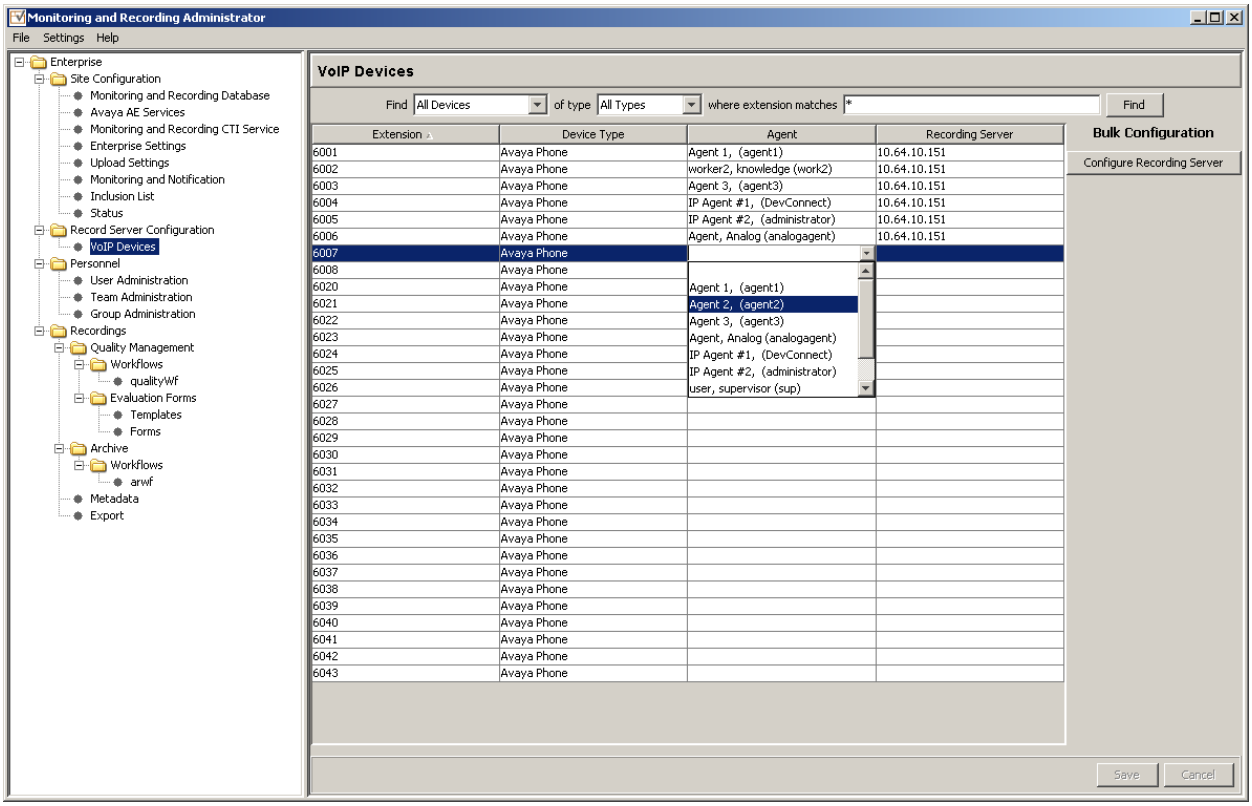
Before Monitoring and Recording Services can be configured for target devices, the interface must be defined. This is done via the **Monitoring and Recording Administrator** application which is installed on a workstation in the customer environment.

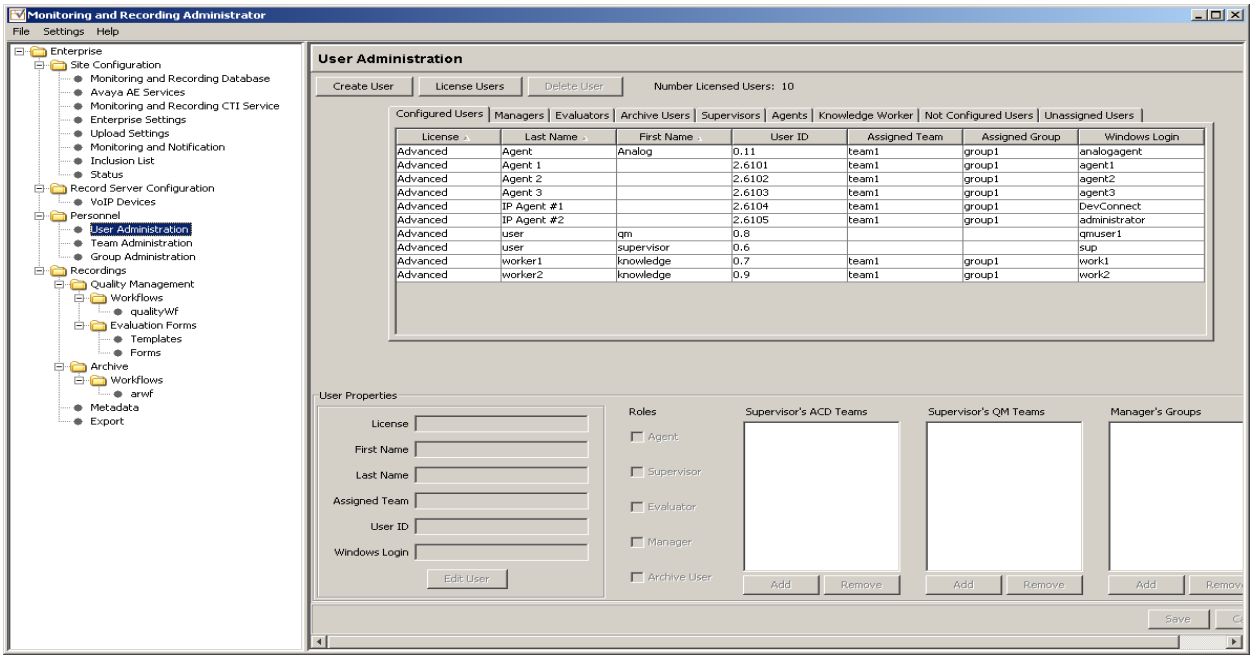
In CLAN configurations, using the **Host Name** of the switch connection defined in 5.2 in the **Communication Manager Information** entry will be preferred; this will allow Application Enablement Services and Communication Manager to pool resources on behalf of the application.



6.2. Configuration of Devices and Agents

When the SMS query completes, the devices to be recorded are configured by assigning a recording server to each device on the **VoIP Devices** page, and then assigning an Agent or Knowledge Worker to that device on the **User Administration** page. The configuration of these objects is illustrated below and covered in greater detail in the Installation Guide [Reference 3].



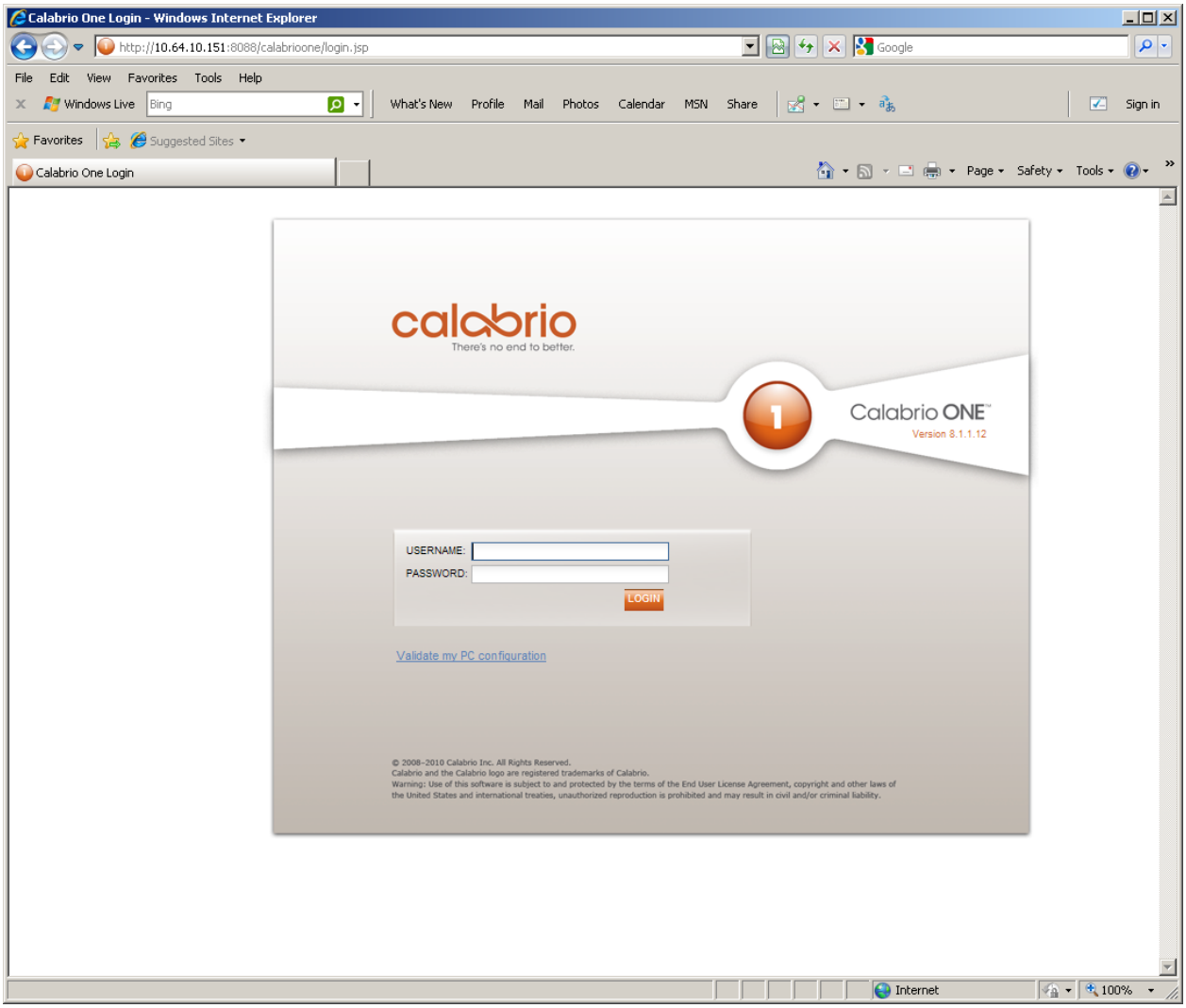


When the Monitoring and Recording services are started, the server establishes a Dependent Registration on each of the assigned devices, then initiates a TSAPI monitor on the station using the JTAPI service on Application Enablement Services. Once this is completed, the application is ready to record.

Recording can be initiated by configuring rules. Typically, every call is recorded, but not all recordings will be tagged for Quality purposes. Quality tagging enables the administrator to define rules such as time of day, call direction, called numbers (VDNs) and other criteria to assist in screening recordings for characteristics that are of interest to the user.

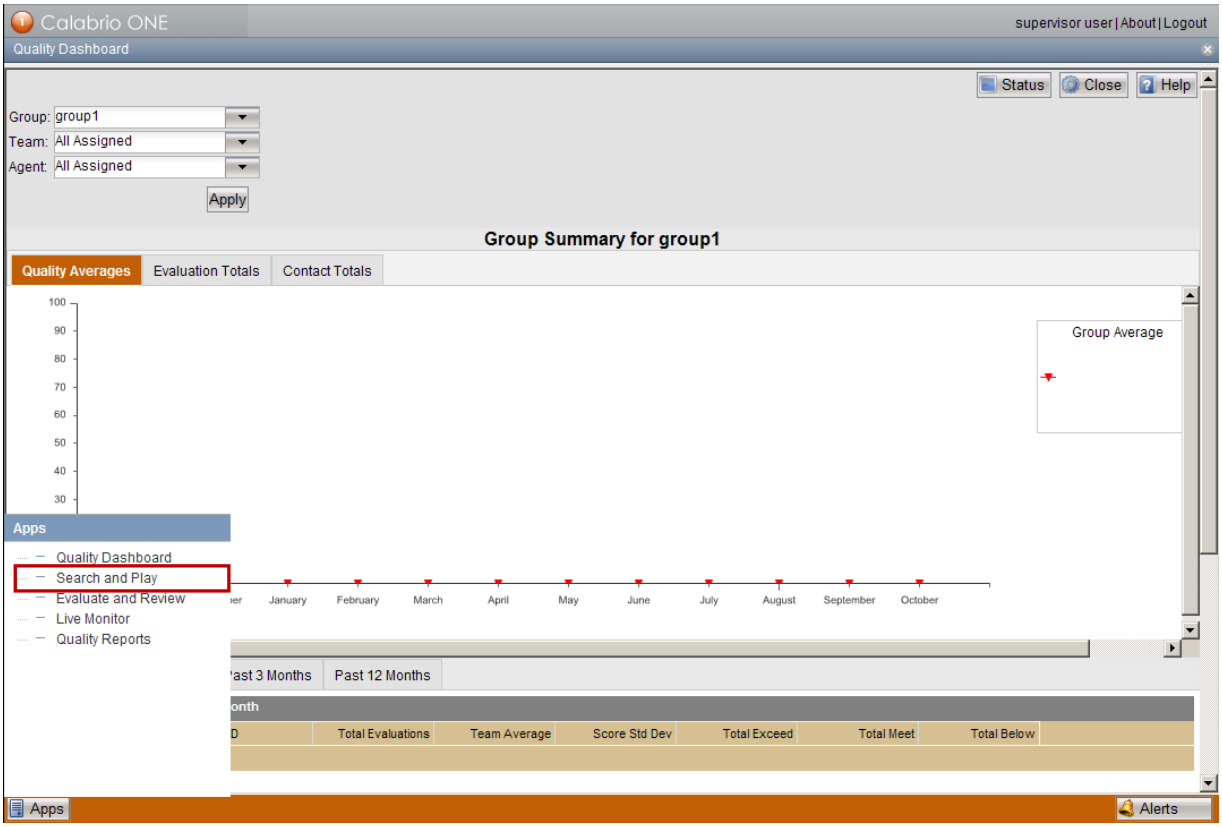
6.3. Launch Calabrio User Interface

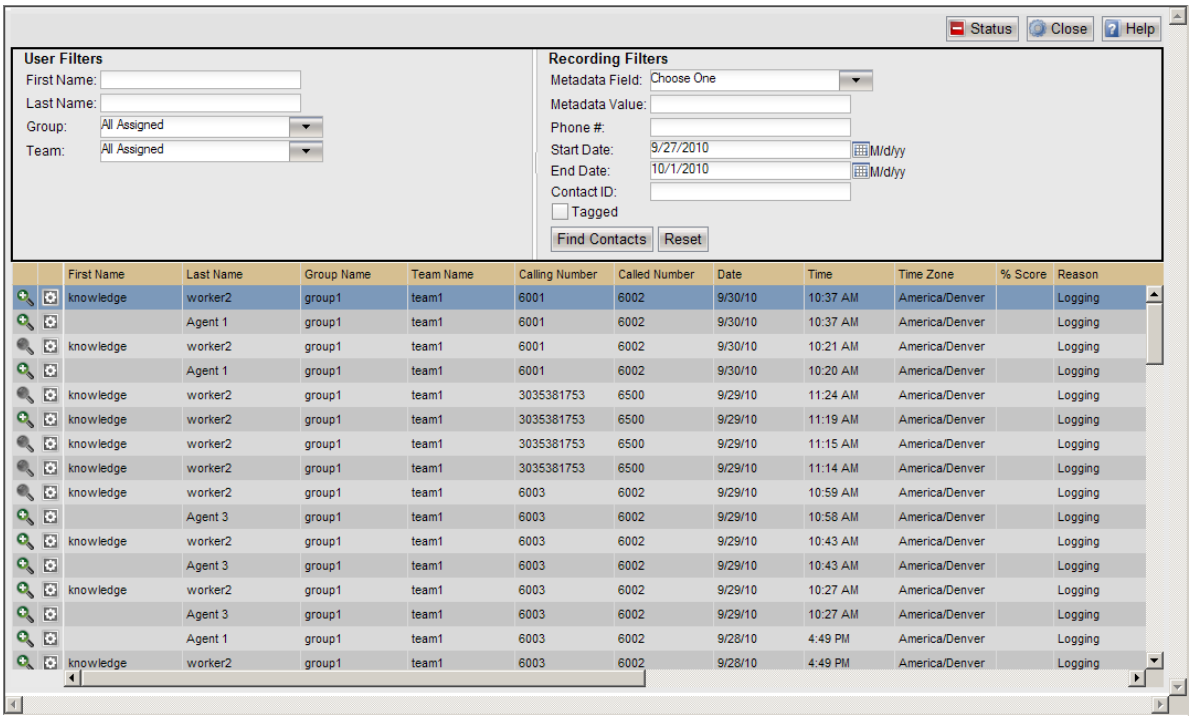
Access the web-based user interface using the URL **http://<ip-address>:8088/calabrioone** in a browser window, where **<ip-address>** is the address of the Monitoring and Recording Services server. The **Log In** screen is displayed as shown below. Log in using the appropriate credentials.



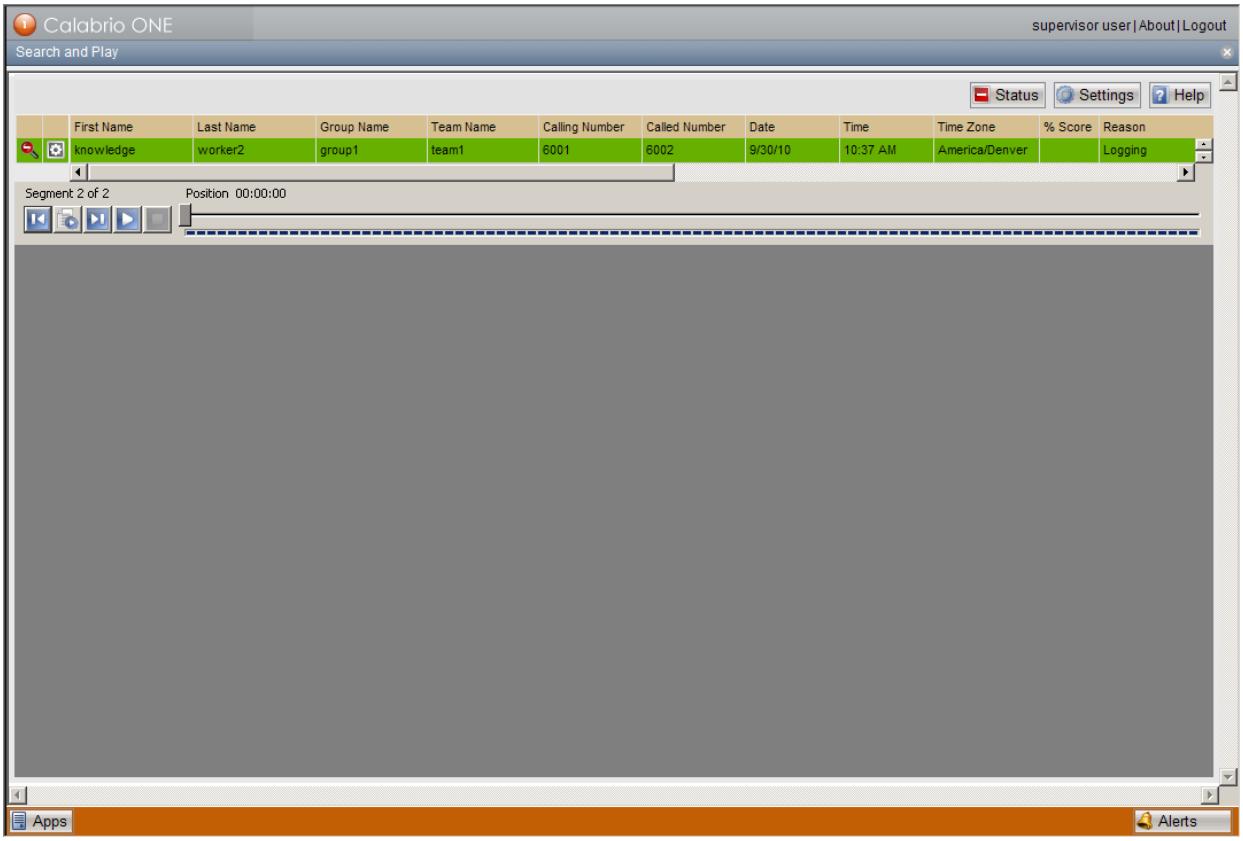
6.4. Viewing Recorded Calls

Once logged in, a user may launch the **Search and Play** interface and define search criteria for recorded calls.

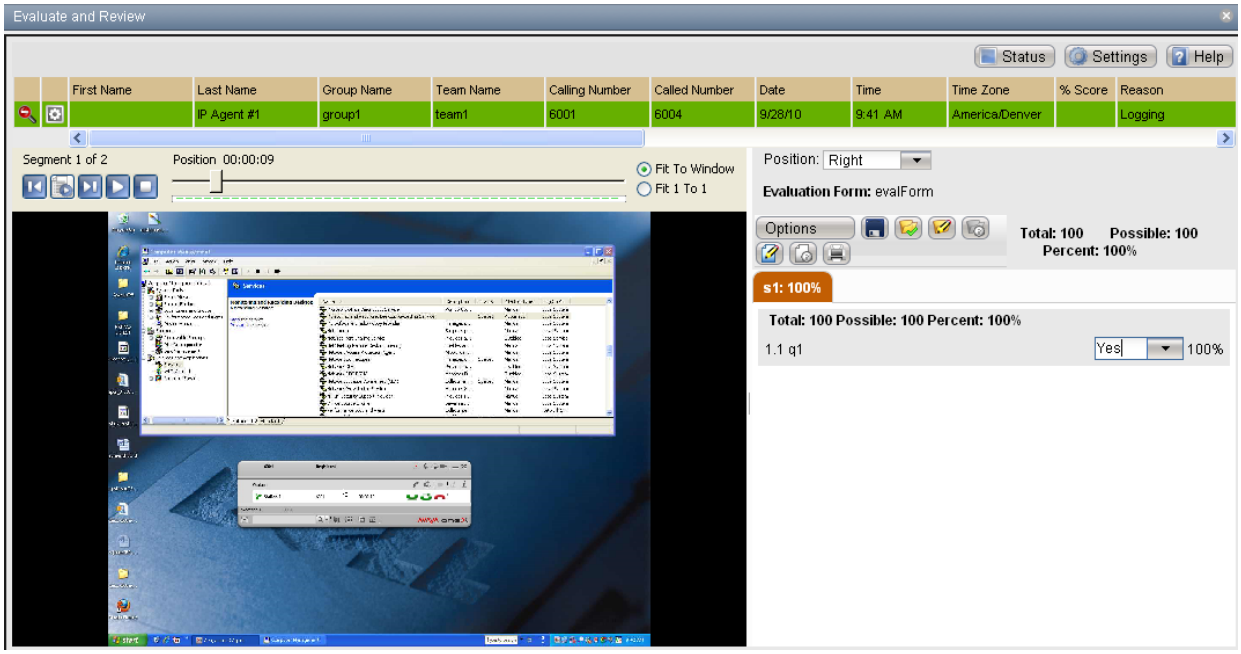




Selecting the icon in front of the item of interest will launch a playback window as demonstrated below. For Audio only recordings, it will look like this:



If the contact included screen recordings, it will appear like this:



7. General Test Approach and Test Results

All feature functionality test cases were performed manually to verify proper operation. The following scenarios were tested using the test configuration diagram shown in **Figure 1**.

The installation test cases were covered with the setup of Avaya Aura™ Communication Manager, Avaya Aura™ Application Enablement Services, and Calabrio Monitoring and Recording Services. The clean removal of the application was also covered in this section.

The functionality test cases were performed manually. Various calls were placed including incoming and outgoing PSTN calls to the monitored VDN, incoming and outgoing calls to and between the agents, and both telephones and soft clients. Calls were made with monitored and non-monitored agents, per test case specification.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet cable to the Monitoring and Recording Services server at different intervals, powering down Avaya Aura™ Communication Manager, powering down the Avaya Aura™ Application Enablement Services server, and also by stopping the CTI service on Avaya Aura™ Application Enablement Services.

The verification of tests included manually listening to recordings from the web, checking the timestamps and data of the recordings, and performing searches. All test cases passed. No errors were detected.

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura™ Communication Manager, Avaya Aura™ Application Enablement Services, and Calabrio Monitoring and Recording Services.

Check the service state of your Avaya Aura™ Communication Manager CTI links by entering the **status aesvcs cti-link** command. The link status should show **no** for maintenance busy (**Mnt Busy**) and the **Service State** should indicate **established**.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

CTI   Version  Mnt   AE Services      Service       Msgs     Msgs
Link           Busy  Server           State         Sent     Rcvd

1     4        no    aesserver2       established   15       15



Command successfully completed
Command:
```

The **status aesvcs interface** command should indicate the interface is listening, even before Avaya Aura™ Application Enablement Services is configured.

```
                          AE SERVICES INTERFACE STATUS

Local Node        Enabled?  Number of     Status
                            Connections

procr             yes       1            listening


Command successfully completed
Command:
```

The **status aesvcs link** command will indicate the number of messages sent from, and received at the CLAN interface (or procr), to and from Avaya Aura™ Application Enablement Services, including maintenance traffic.

```
status aesvcs link
                            AE SERVICES LINK STATUS

Srvr/  AE Services     Remote IP        Remote  Local Node      Msgs    Msgs
Link   Server                           Port                    Sent    Rcvd

01/01  aesserver2                       59815   procr           620     606
                       10.64.10.21

Command successfully completed
Command:
```

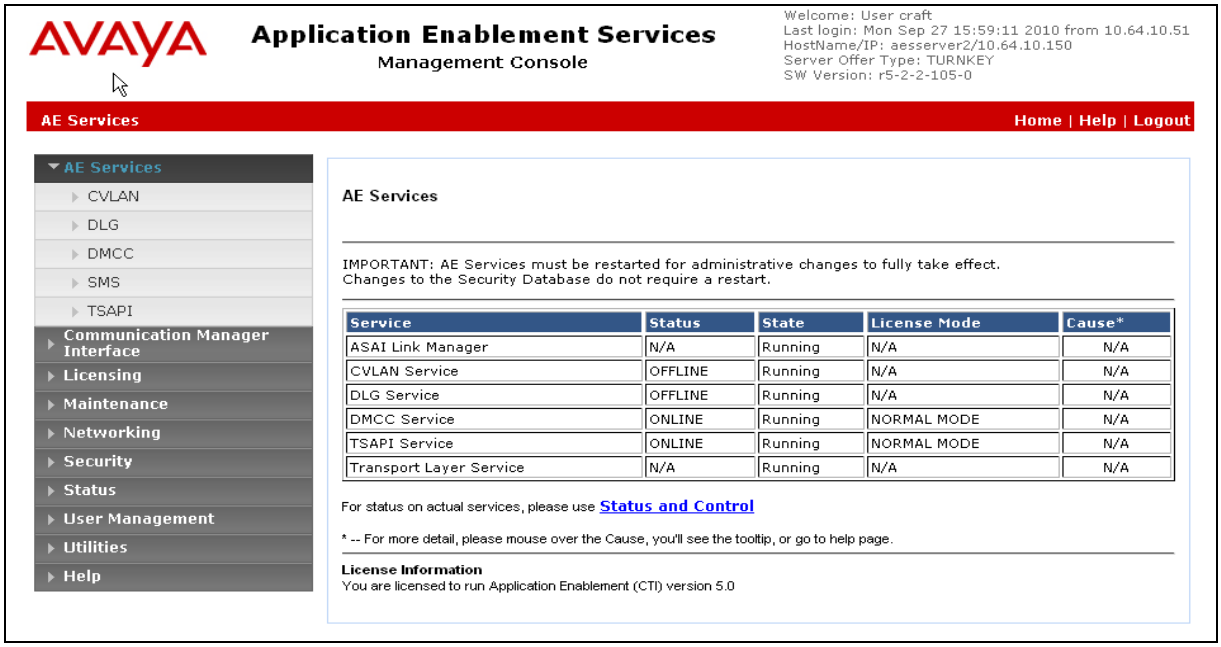
Once the Monitoring and Recording Services server is running, the **list registered-ip-stations** command will show both active phone registrations, and an entry for each station to be recorded that is associated with the Avaya Aura™ Application Enablement Services client link IP Address (**10.64.10.150**).

```
list registered-ip-stations                                          Page   1

                            REGISTERED IP STATIONS

Station Ext   Set Type/ Prod ID/   TCP Station IP Address/
or Orig Port  Net Rgn   Release    Skt Gatekeeper IP Address
------------- --------- ---------- --- ---------------------------------------
6001          9640      IP_Phone    y  10.64.10.44
              1         3.110b         10.64.10.67
6002          9620      IP_Phone    y  10.64.10.41
              1         3.110b         10.64.10.67
6002          9620      IP_API_A    y  10.64.10.150
              1         3.2040         10.64.10.67
6003          9630      IP_Phone    y  10.64.10.43
              1         3.110b         10.64.10.67
6003          9630      IP_API_A    y  10.64.10.150
              1         3.2040         10.64.10.67
6004          4620      IP_Agent    y  10.64.10.50
              1         9.0            10.64.10.67
6004          4620      IP_API_A    y  10.64.10.150
              1         3.2040         10.64.10.67

               press CANCEL to quit --  press NEXT PAGE to continue
ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh
```

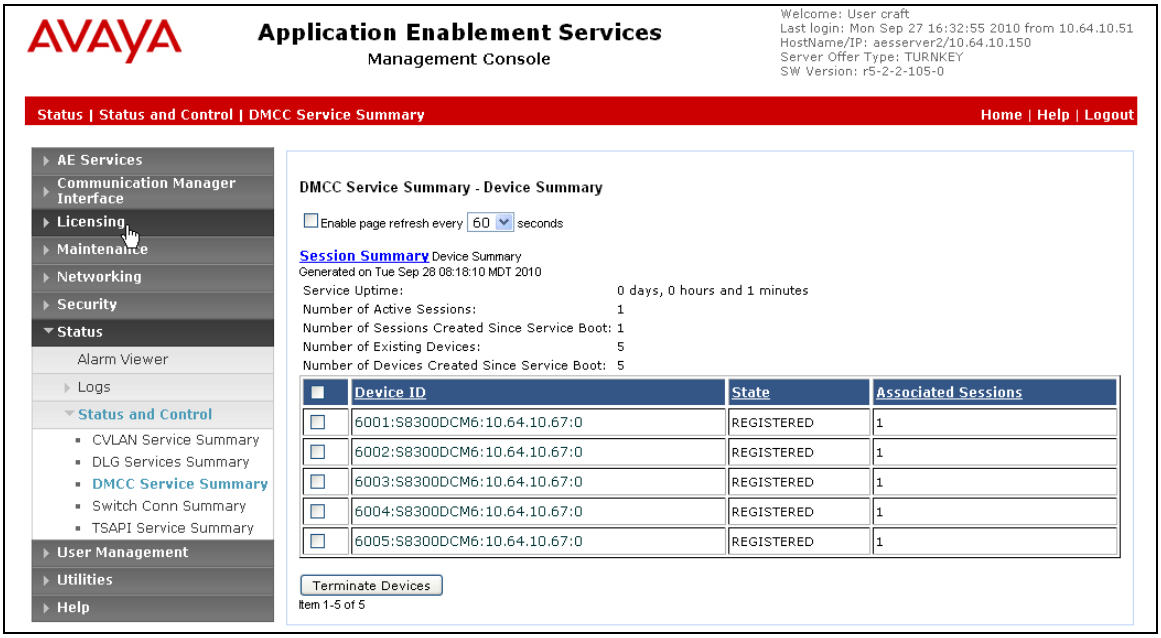
In addition, each station to be recorded will show an ASAI monitor association by using the **list monitored-station** command.

```
list monitored-station

                            MONITORED STATION

  Station     Association 1    Association 2    Association 3    Association 4
  Ext         CTI Link  CRV    CTI Link  CRV    CTI Link  CRV    CTI Link  CRV
  -------     ------------     -------------    -------------    -------------
6002           1          32
6003           1          12
6004           1          63
6005           1          41

Command successfully completed
Command:
```

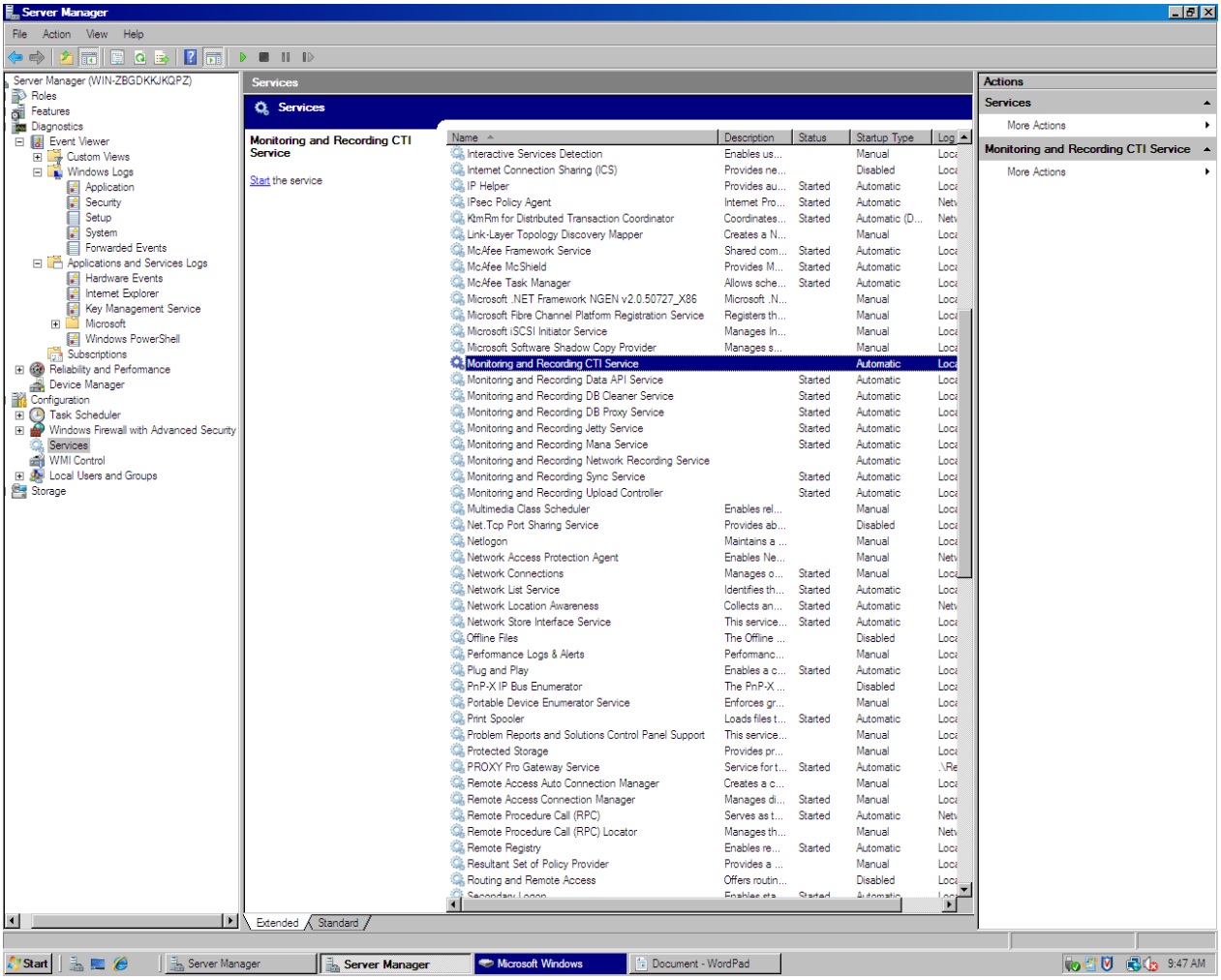
Navigate to **AE Services** on the Avaya Aura™ Application Enablement Services server to verify that services are **ONLINE** and **NORMAL MODE** for the TSAPI and DMCC Services, as shown in the screen below.



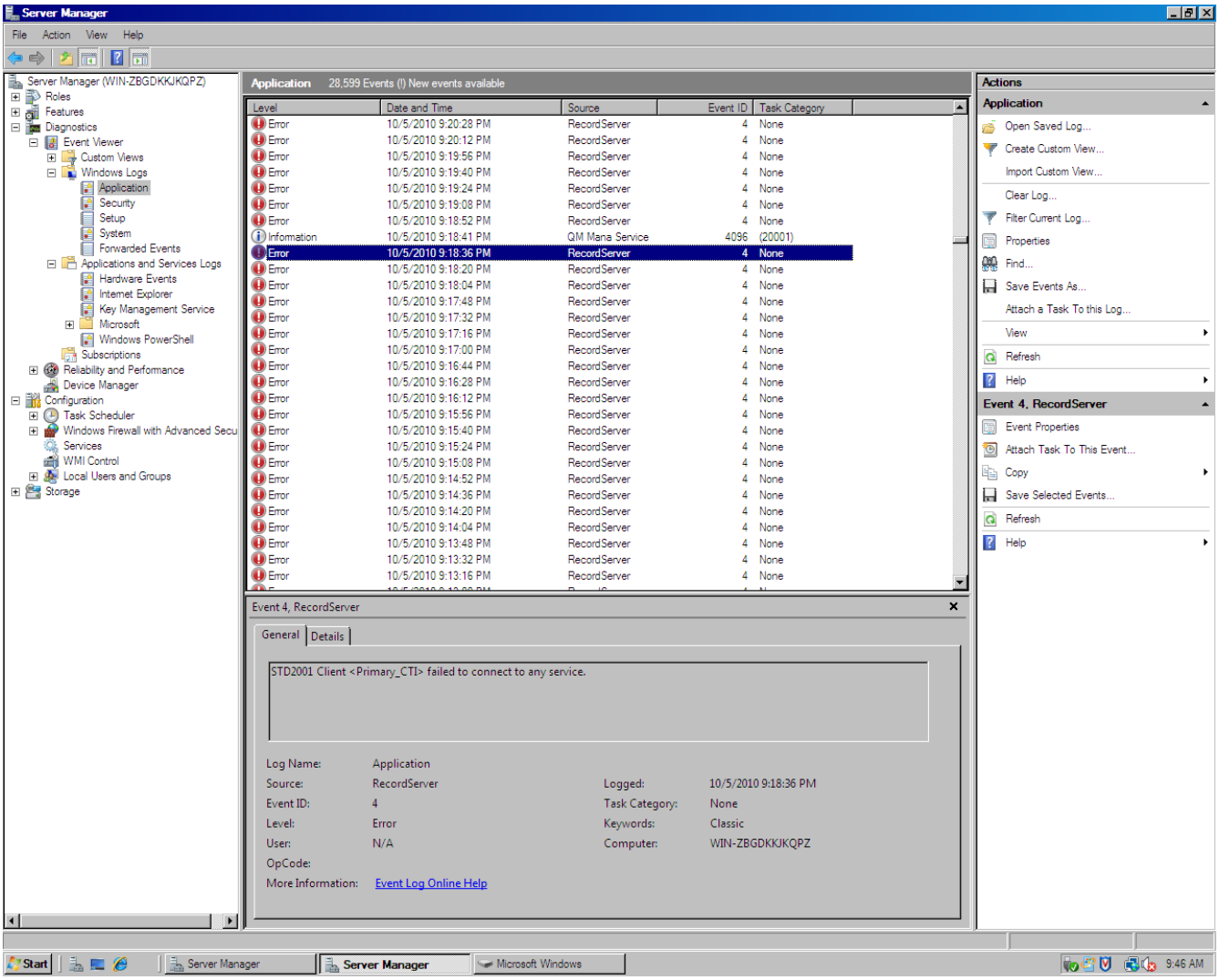
Once the application has successfully started, the **DMCC Service Summary** will show all of the stations to be recorded as **REGISTERED** devices.



To verify the setup from the Calabrio side, log in to the server and confirm the **Monitoring and Recording** services are **started** in the Windows **Services** manager page (NOTE: some services are not running in the screenshot below).



The Windows **Event Viewer** will list any status events of concern, and if configured, SNMP or email alarm notifications will be sent to alert the user of system alarms.



9. Conclusion

Calabrio Monitoring and Recording Services successfully captured and recorded phone activity for agents and knowledge workers. All test cases completed successfully.

10. Additional References

This section references the Avaya and Calabrio product documentation that are relevant to these Application Notes.

Avaya product documentation can be found at http://support.avaya.com:

[1] *Administering Avaya Aura™ Communication Manager*, Doc ID: 03-300509, Issue 6.0, Release 6.0, June 2010

[2] *Avaya MultiVantage Application Enablement Services Administration and Maintenance Guide*, Doc ID: 02-300357, Release 5.2, Issue 11, November 2009

[3] *Calabrio One Monitoring and Recording Services Installation Guide, Rev.8.1*

[4] *Calabrio One Monitoring and Recording Services Application User Guide, Rev. 8.0*

[5] *Calabrio One Monitoring and Recording Services Application Administrator User Guide, Rev. 8.1*

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.