Avaya Solution & Interoperability Test Lab

# Application Notes for Controlled Networks Call Witness Version 2.0 with Avaya Aura® Communication Manager R7.1 and Avaya Aura® Application Enablement Services R7.1 – Issue 1.0

## Abstract

These Application Notes describe the configuration steps required for the Controlled Networks Call Witness solution to interoperate with Avaya Aura® Communication Manager R7.1 and Avaya Aura® Application Enablement Services R7.1.

Controlled Networks Call Witness uses the Avaya Aura® Application Enablement Services' Telephony Software Application Program Interface (TSAPI) and Device, Media and Call Control (DMCC) Interface to capture real-time CTI data and RTP streams from Avaya Aura® Communication Manager to produce recordings of phone activity for agents and knowledge workers.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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

Controlled Networks Call Witness (Call Witness) system interfaces with Avaya Aura® Communication Manager (Communication Manager) and Avaya Aura® Application Enablement Services (AES); TSAPI to obtain call event information and the DMCC to obtain audio.

The compliance testing focused on the monitoring and recording performed by Call Witness for calls placed to and/or from Analog, Digital, IP H323, IP SIP telephones, and Vector Directory Numbers (VDNs) supported by Communication Manager and Avaya Aura® Session Manager.

Call Witness uses TSAPI interface of AES to monitor extensions and obtain call events and in some instances, to add virtual recorder stations to calls via Single Step Conference and DMCC interface to register DMCC softphones (virtual extensions) with Communication Manager in order to record devices that DMCC cannot register multiple terminals with (SIP and Analog endpoints). In this mode, the DMCC softphones are used as recording devices. When a call is to be recorded, Call Witness uses Single Step Conference to add a DMCC softphone into the call and obtain the audio.

# 2. General Test Approach and Test Results

The compliance test focused on the ability for calls to be recorded. Calls were manually placed from the public switched telephone network (PSTN) directly to and from recorded devices, and to Agent IDs via VDN. For each recorded station in a call, there is one recording generated. Once a call is completed, the recordings are reviewed for their quality, completeness (number of recordings beginning to end, etc.), and accuracy of tagging information (owner, calling party, called party, etc.).

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

This test was conducted in a lab environment simulating a basic customer enterprise network environment. The testing focused on the standards-based interface between the Avaya solution and the third party solution. The results of testing are therefore considered to be applicable to either a premise-based deployment or to a hosted or cloud deployment where some elements of the third party solution may reside beyond the boundaries of the enterprise network, or at a different physical location from the Avaya components.

Readers should be aware that network behaviors (e.g. jitter, packet loss, delay, speed, etc.) can vary significantly from one location to another, and may affect the reliability or performance of the overall solution. Different network elements (e.g. session border controllers, soft switches, firewalls, NAT appliances, etc.) can also affect how the solution performs.

If a customer is considering implementation of this solution in a cloud environment, the customer should evaluate and discuss the network characteristics with their cloud service provider and network organizations, and evaluate if the solution is viable to be deployed in the cloud.

The network characteristics required to support this solution are outside the scope of these Application Notes. Readers should consult the appropriate Avaya and third party documentation for the product network requirements. Avaya makes no guarantee that this solution will work in all potential deployment configurations.

## 2.1. Interoperability Compliance Testing

The compliance test validated the ability of Call Witness to successfully record calls routed to and from Analog, Digital, and IP endpoints as well as softphone clients. Common call scenarios including hold/resume, mute/unmute, transfer, and conference calls were exercised during the test. Additional tests included the ability to monitor live associated with a recorded station.

Additionally, serviceability testing was performed to confirm the ability for Call Witness to recover from common outages such as network outages and server reboots.

## 2.2. Test Results

All test cases passed with the following observations,

- Call Witness is does not support agent recording at this time, but it is able to record calls from agent’s station extension if these are contact center calls and are routed to agent’s stations via VDNs.

## 2.3. Support

Technical support on Controlled Networks Call Witness can be obtained through the following:

- Phone: 1.800.800-4445
- Web: http://www.controllednetworks.com
- Email: info@controllednetworks.com

# 3. Reference Configuration

**Figure 1** illustrates the compliance test configuration consisting of:

- Avaya Aura® Communication Manager R7.1
- Avaya Aura® Application Enablement Services R7.1
- Various IP, Digital, and analog endpoints
- Avaya one-X® Agent softphone
- Controlled Networks Call Witness server installed on a standalone machine

Calls routed to and from Communication Manager used PRI trunks to connect to the PSTN.

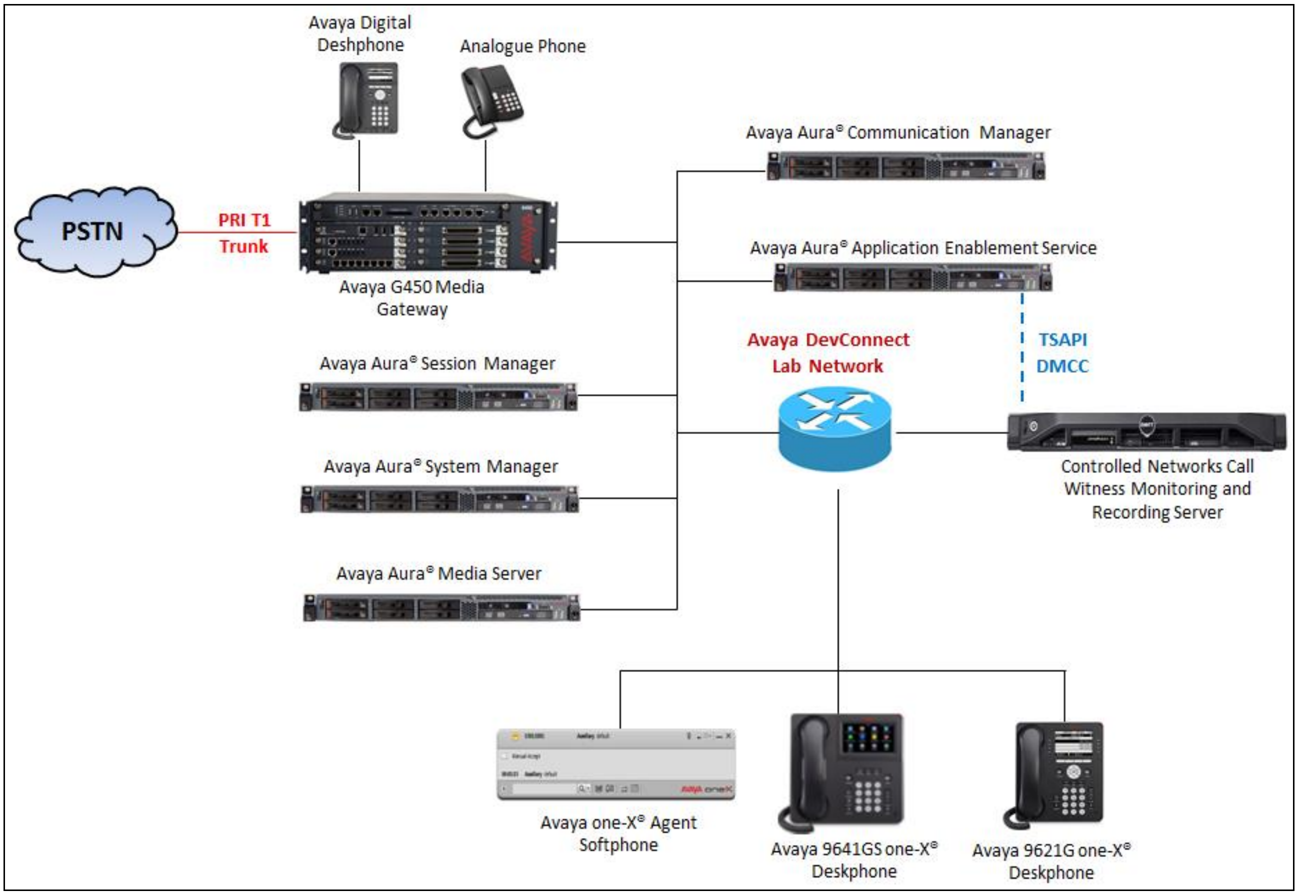

Avaya Digital Deshphone
Analogue Phone
Avaya Aura® Communication Manager
PSTN
PRI T1 Trunk
Avaya Aura® Application Enablement Service
Avaya G450 Media Gateway
Avaya DevConnect Lab Network
TSAPI
DMCC
Avaya Aura® Session Manager
Avaya Aura® System Manager
Controlled Networks Call Witness Monitoring and Recording Server
Avaya Aura® Media Server
Avaya one-X® Agent Softphone
Avaya 9641GS one-X® Deskphone
Avaya 9621G one-X® Deskphone

**Figure 1 – Call Witness Compliance Test Configuration**

# 4. Equipment and Software Validated

The following equipment and version were used in the reference configuration described above:

| Equipment/Software | Release/Version |
|---|---|
| Avaya Aura® Communication Manager running on virtualized environment | R017x.01.0.532.0 |
| Avaya Aura® Application Enablement Services running on virtualized environment | 7.1.0.0.0.17 |
| Avaya Aura® Session Manager running on virtualized environment | 7.1.0.0.710028 |
| Avaya Aura® System Manager | 7.1.0.0.116662 |
| Avaya Aura® Media Server | 7.8 |
| Avaya G450 Media Gateway | FW 38.18.0/1 |
| Avaya 96x1 Series IP Telephone<br>• 9641GS (H.323)<br>• 9621G (SIP) | <br>6.64<br>7.1 |
| Avaya 1416 Digital Telephones | FW 1 |
| 2500 analog phone | - |
| Desktop PC running Avaya One-X® Agent (H.323) | 2.5.8.6 |
| Controlled Network Call Witness running under Windows 2012 R2 Standard Server | 2.0 |

# 5. Configure Avaya Aura® Communication Manager

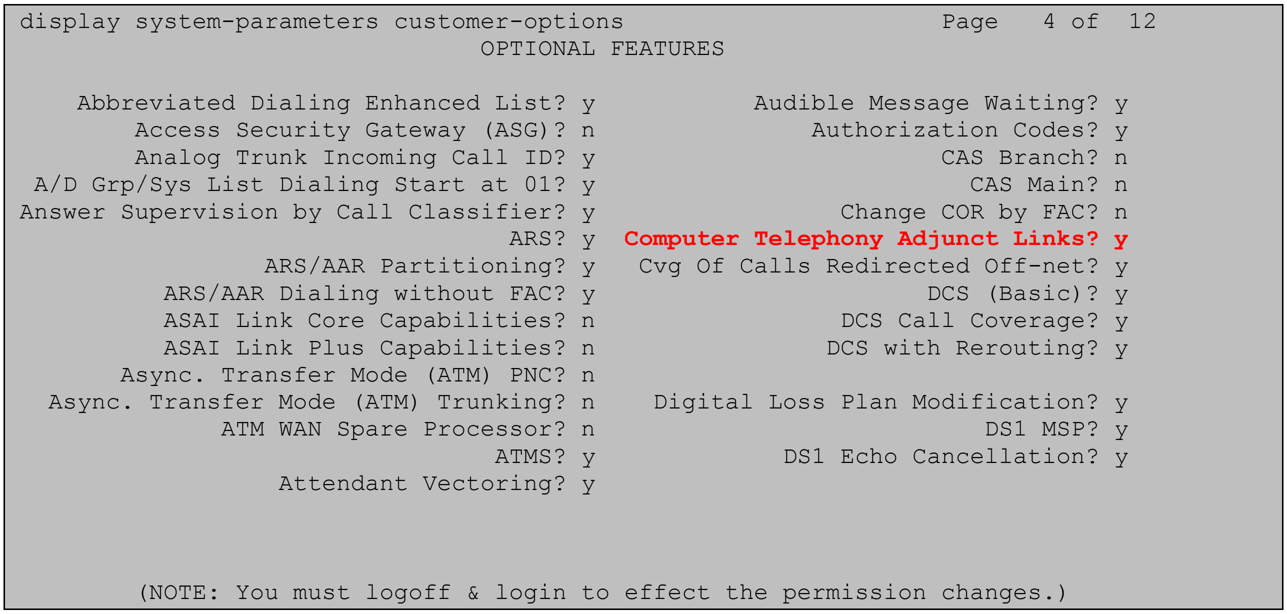
This section provides the procedures for configuring Communication Manager. The procedures fall into the following areas:

- Verify Feature and License for the integration
- Administer Communication Manager System Features
- Administer IP Services for Application Enablement Services
- Administer Computer Telephony Integration (CTI) Link
- Add SMS User Account
- Verify Recorded Extensions
- Add Virtual Stations

All the configuration changes in this section for Communication Manager are performed through the System Access Terminal (SAT) interface. For more details on configuring Communication Manager, refer to the Avaya product documentation in **Section 10**.

## 5.1. Verify Feature and License

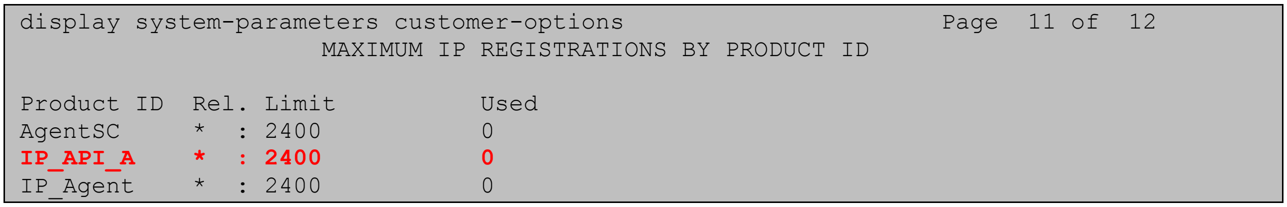
Enter the **display system-parameters customer-options** command and ensure that **Computer Telephony Adjunct Links** is set to **y.** If this option is not set to **y**, contact the Avaya sales team or business partner for a proper license file.



```
display system-parameters customer-options                      Page   4 of  12
                                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? y                      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



        (NOTE: You must logoff & login to effect the permission changes.)
```

Each recording port or virtual station extension the recorder will use to record agent phones will require an **IP_API_A** license if not licensed on Application Enablement Services.

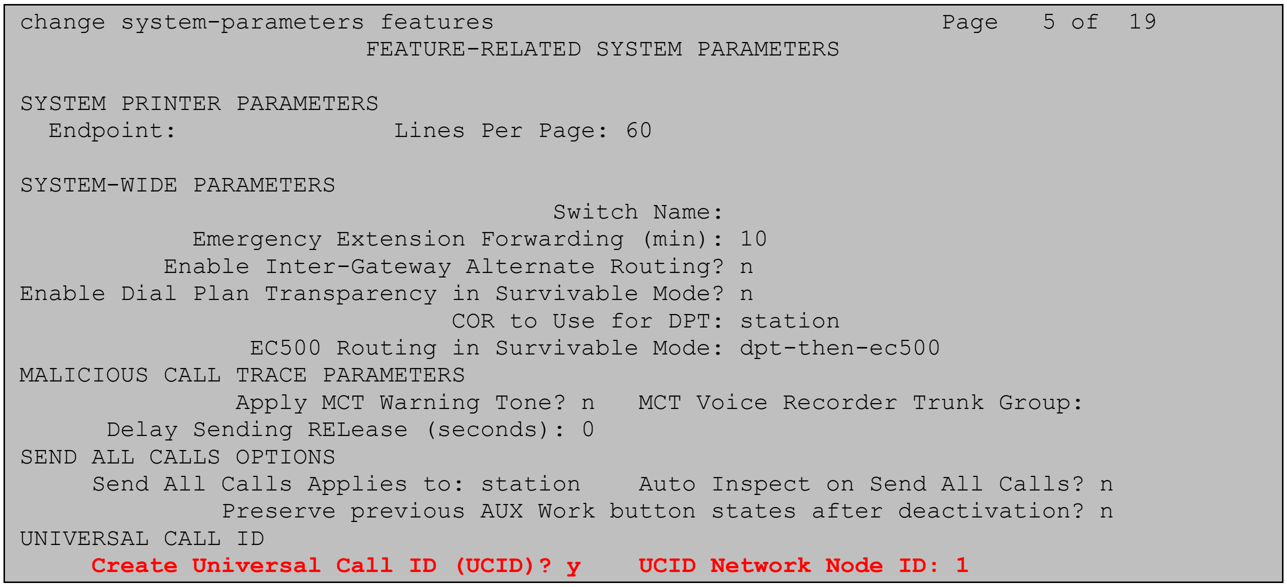
Each recording port or virtual station extension on the recorder used to record agent phones will require an **IP_API_A** license when a **VALUE_AES_DMCC_DMC** license is not available on Application Enablement Services.



```
display system-parameters customer-options                      Page  11 of  12
                     MAXIMUM IP REGISTRATIONS BY PRODUCT ID

Product ID  Rel. Limit            Used
AgentSC     *   : 2400            0
IP_API_A    *   : 2400            0
IP_Agent    *   : 2400            0
```

## 5.2. Administer Communication Manager System Features

Enter the **change system-parameters features** command and ensure that on page 5 **Create Universal Call ID (UCID)** is enabled and a relevant **UCID Network Node ID** (**1** was used in the test) is defined. Also ensure that on page 13 that **Send UCID to ASAI** is set to **y**. Call Witness 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
                EC500 Routing in Survivable Mode: dpt-then-ec500
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

            Agent/Caller Disconnect Tones? n
          Interruptible Aux Notification Timer (sec): 3
             Zip Tone Burst for Callmaster Endpoints: double

  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
         Send Connect Event to ASAI For Announcement Answer? n
  Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```

## 5.3. Administer IP-Services for Application Enablement Services

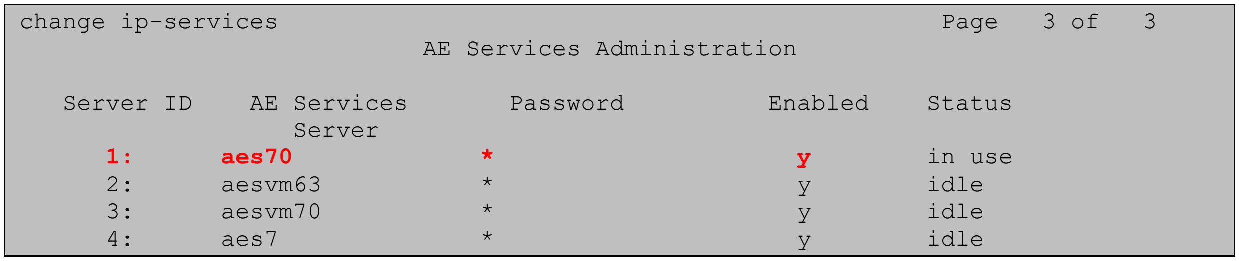
Add an IP-Services entry for Application Enablement Services as described below:

- 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.

```
change ip-services                                              Page   1 of    3

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

On Page 3 of the IP Services form, enter the following values:

- In the **AE Services Server** field, type the host name of the Application Enablement Services server.
- In the **Password** field, type the same password to be administered on the Application Enablement Services server in **Section 6**, **Step 1**.
- In the **Enabled** field, type **y**.

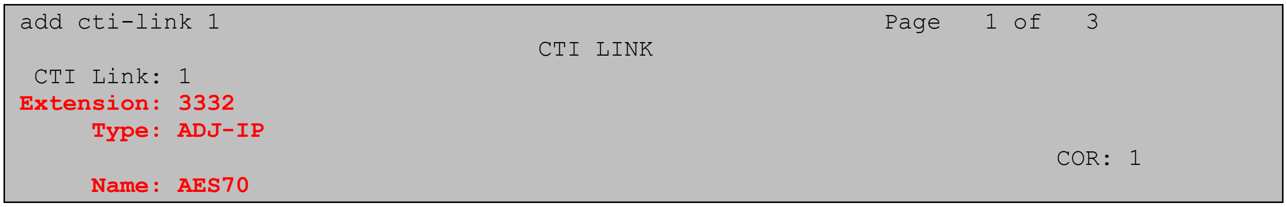


```
change ip-services                                              Page   3 of   3
                            AE Services Administration

   Server ID    AE Services        Password          Enabled    Status
                   Server
      1:       aes70           *                       y        in use
      2:       aesvm63         *                       y        idle
      3:       aesvm70         *                       y        idle
      4:       aes7            *                       y        idle
```

## 5.4. Administer Computer Telephony Integration (CTI) Link

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

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

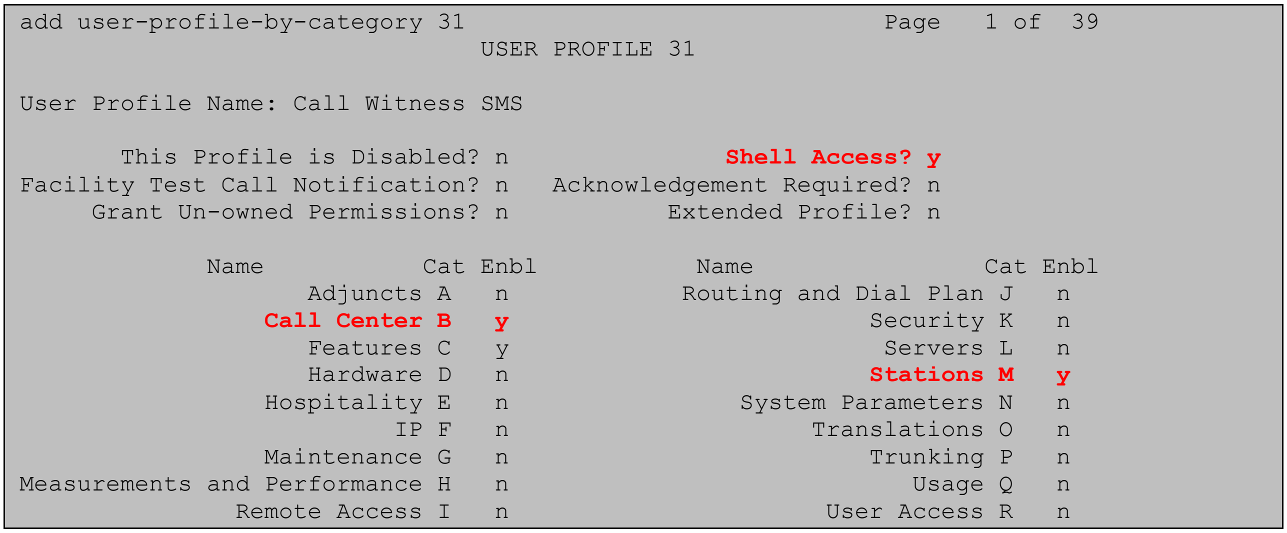


```
add cti-link 1                                              Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 3332
     Type: ADJ-IP
                                                                        COR: 1

     Name: AES70
```

## 5.5. Add SMS User Account

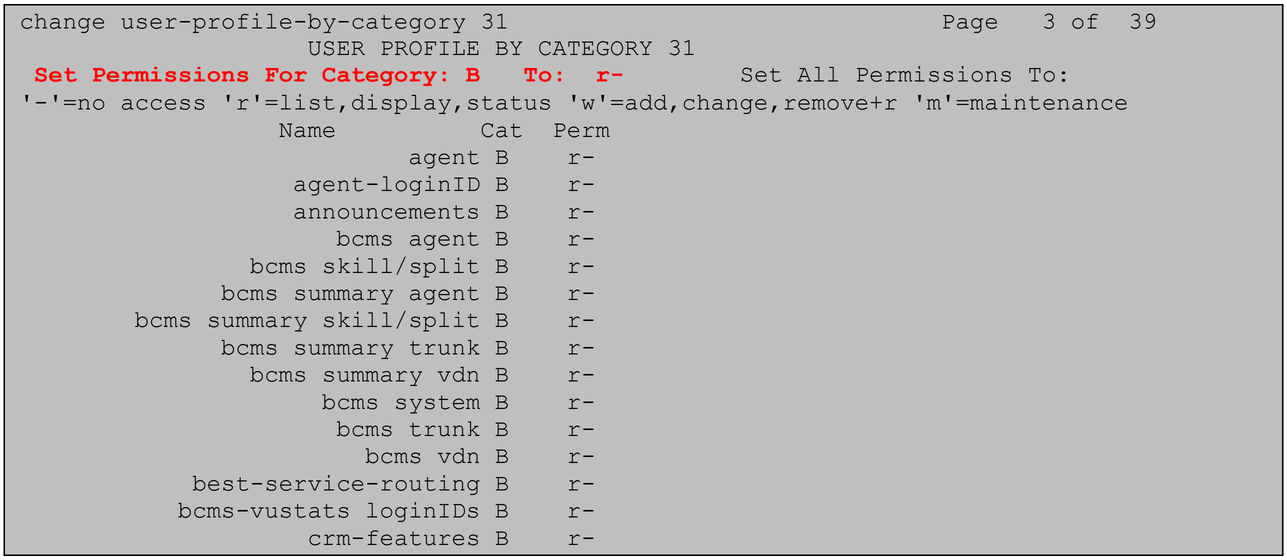
Call Witness uses the Application Enablement Services SMS interface to query for administered Stations and Agents for use in administering the application.

A privileged user was used in this test; however, a local administrator would 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, the **add user-profile-by-category 31** command was used to create the profile used in the test as shown below. The **Shell Access**, **Call Center B** and **Stations M** fields were set to **y**.

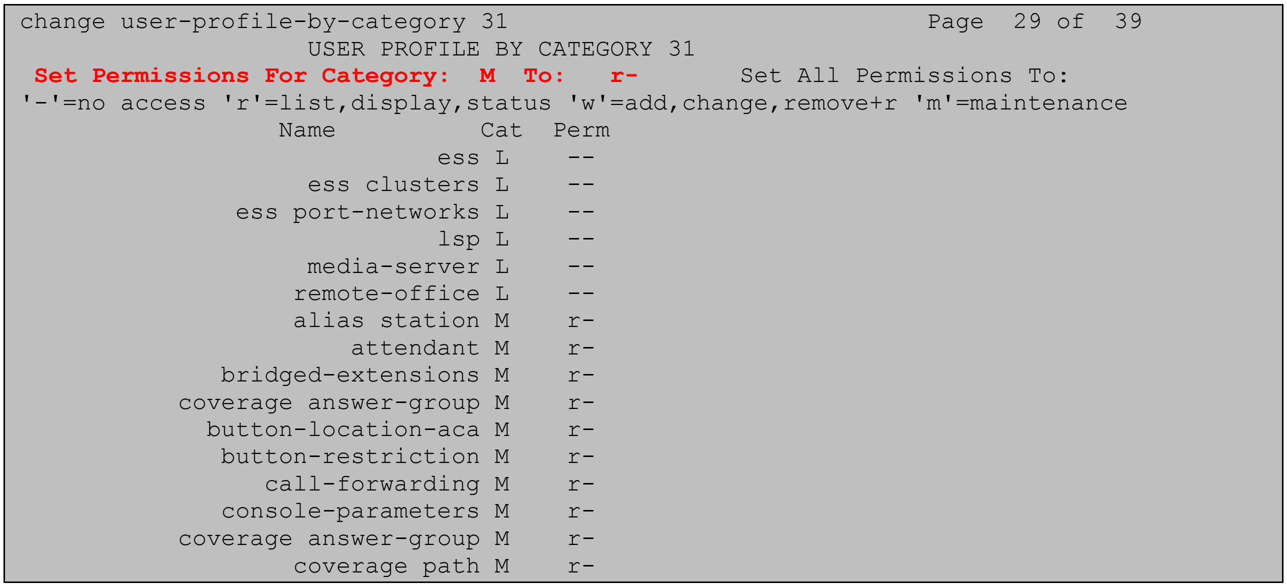


```
add user-profile-by-category 31                             Page   1 of  39
                                USER PROFILE 31

User Profile Name: Call Witness 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    y                         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-by-category xx** form. This requires two separate transactions, so repeat for each category. Please note that this profile will be used later in this section.

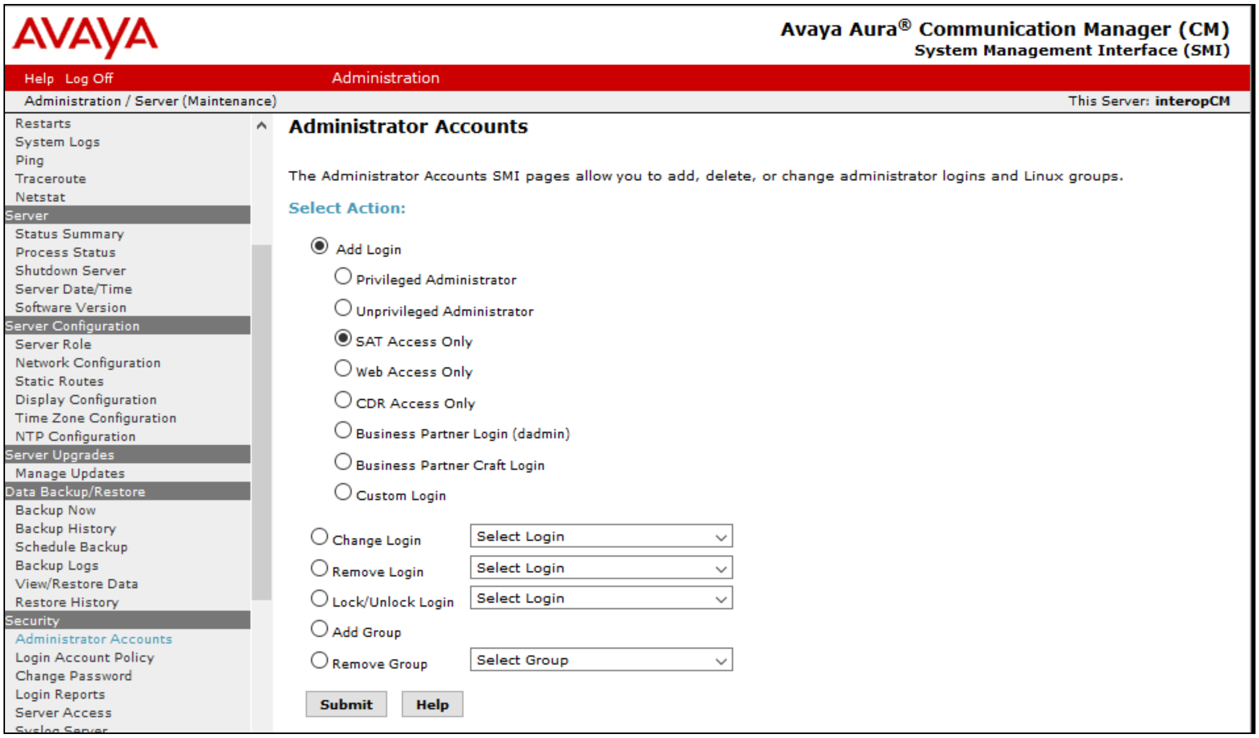


```
change user-profile-by-category 31                              Page   3 of  39
                    USER PROFILE BY CATEGORY 31
 Set Permissions For Category: B   To:  r-        Set All Permissions To:
'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance
                  Name          Cat  Perm
                           agent B    r-
                   agent-loginID B    r-
                   announcements B    r-
                      bcms agent B    r-
                bcms skill/split B    r-
              bcms summary agent B    r-
        bcms summary skill/split B    r-
              bcms summary trunk B    r-
                bcms summary vdn B    r-
                     bcms system B    r-
                      bcms trunk B    r-
                        bcms vdn B    r-
            best-service-routing B    r-
           bcms-vustats loginIDs B    r-
                    crm-features B    r-
```



```
change user-profile-by-category 31                             Page  29 of  39
                    USER PROFILE BY CATEGORY 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
                             ess L    --
                    ess clusters L    --
               ess port-networks L    --
                             lsp L    --
                    media-server L    --
                   remote-office L    --
                   alias station M    r-
                       attendant M    r-
              bridged-extensions M    r-
           coverage answer-group M    r-
             button-location-aca M    r-
              button-restriction M    r-
                 call-forwarding M    r-
              console-parameters M    r-
           coverage answer-group M    r-
                   coverage path M    r-
```

Create a user account on the Communication Manager **System Management Interface** web page by navigating to the **Administer Accounts** page and selecting the radio button **Add Login** and **SAT Access Only**. Click **Submit** to continue the process.



**Administrator Accounts**

The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups.

Select Action:

● Add Login
- ○ Privileged Administrator
- ○ Unprivileged Administrator
- ● SAT Access Only
- ○ Web Access Only
- ○ CDR Access Only
- ○ Business Partner Login (dadmin)
- ○ Business Partner Craft Login
- ○ Custom Login

○ Change Login — Select Login

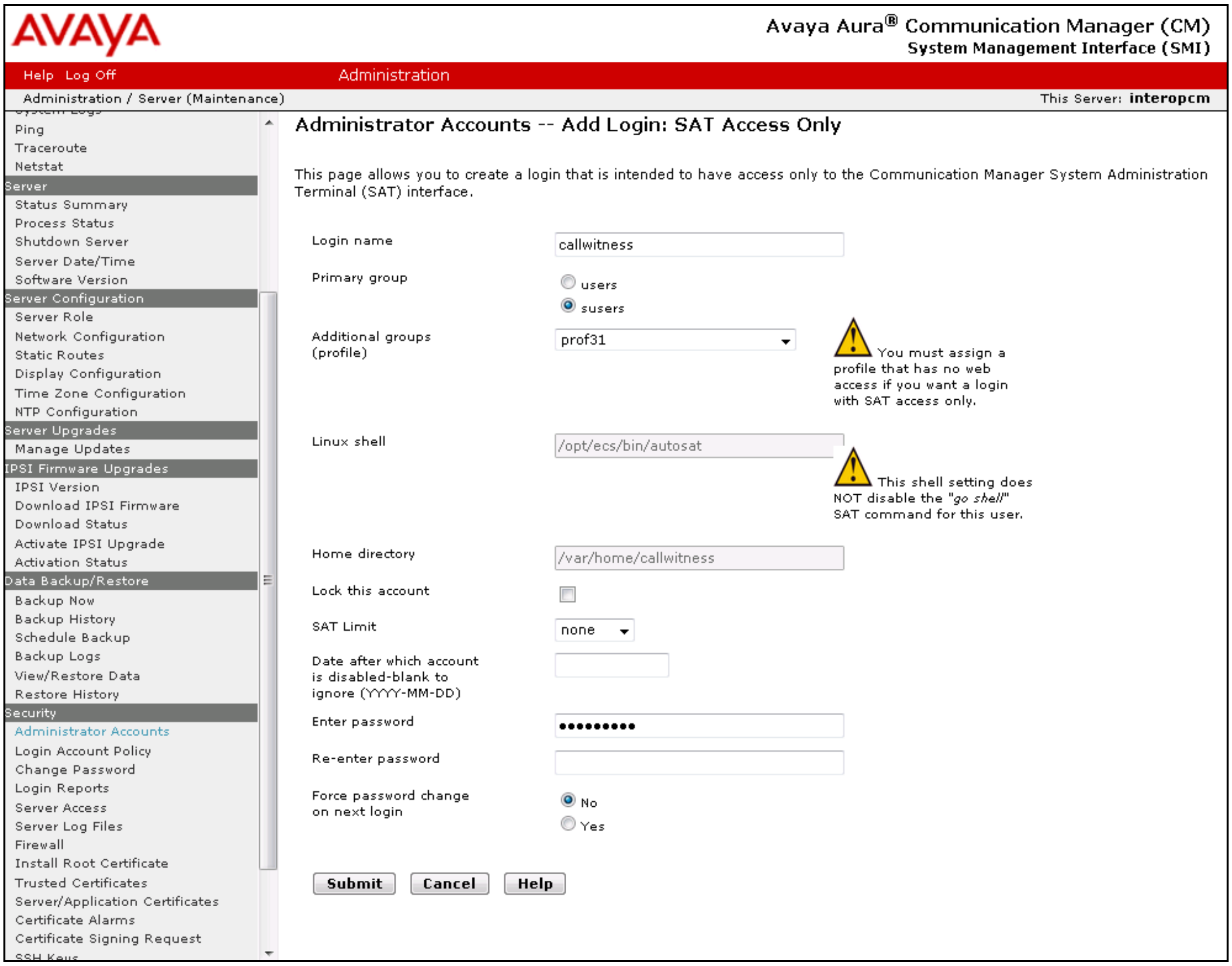
○ Remove Login — Select Login

○ Lock/Unlock Login — Select Login

○ Add Group

○ Remove Group — Select Group

The **Add Login** screen is displayed. Enter a name to the **Login name** field and select the profile defined in earlier in this section (**prof31**) in the **Additional groups (profile)** field. Select **Password** for the **Select type of authentication** field and enter a **Password**.



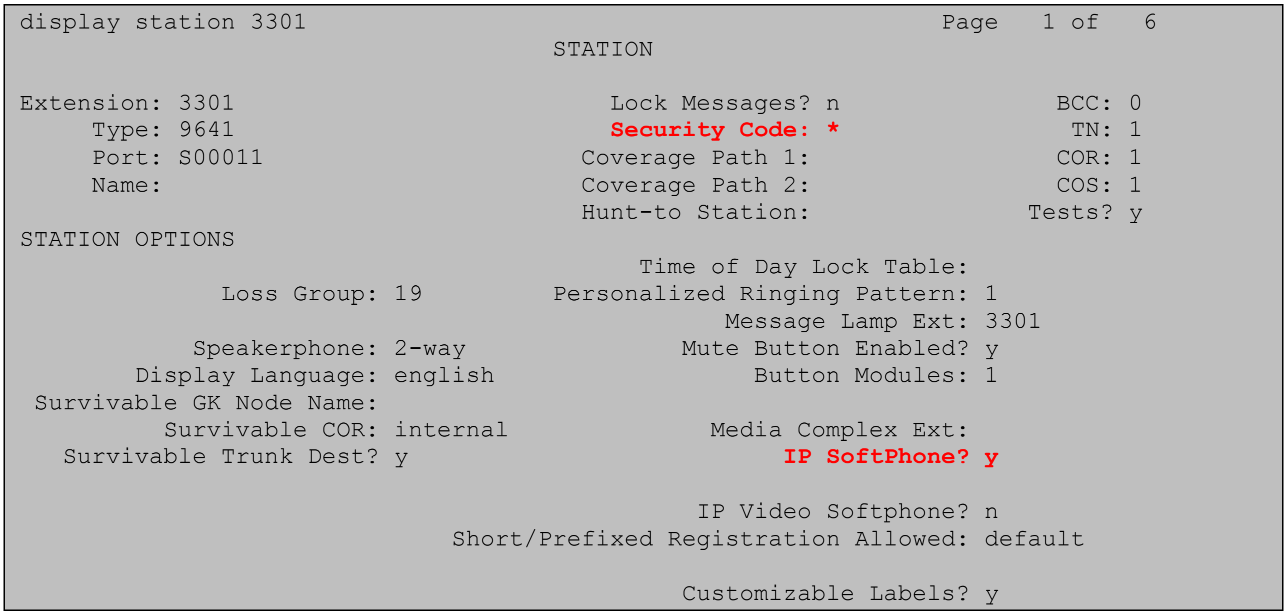
**Administrator Accounts -- Add Login: SAT Access Only**

This page allows you to create a login that is intended to have access only to the Communication Manager System Administration Terminal (SAT) interface.

| | |
|---|---|
| Login name | callwitness |
| Primary group | ○ users<br>● susers |
| Additional groups (profile) | prof31 ▾<br>You must assign a profile that has no web access if you want a login with SAT access only. |
| Linux shell | /opt/ecs/bin/autosat<br>This shell setting does NOT disable the "*go shell*" SAT command for this user. |
| Home directory | /var/home/callwitness |
| Lock this account | □ |
| SAT Limit | none ▾ |
| Date after which account is disabled-blank to ignore (YYYY-MM-DD) | |
| Enter password | ••••••••• |
| Re-enter password | |
| Force password change on next login | ● No<br>○ Yes |

## 5.6. Verify Recorded Extensions

All stations (H.323 and Digital) that will be recorded using the Multiple Registration method must have **IP Softphone** enabled, and the application needs to know the **Security Code** in order to successfully register. For stations (SIP and Analog) that are unable to support Softphone, or which the administrator prefers to record using Single Step Conference, leave the **IP Softphone** setting disabled. Use the **display station n** command to verify information, or **change station n** to make changes if necessary.

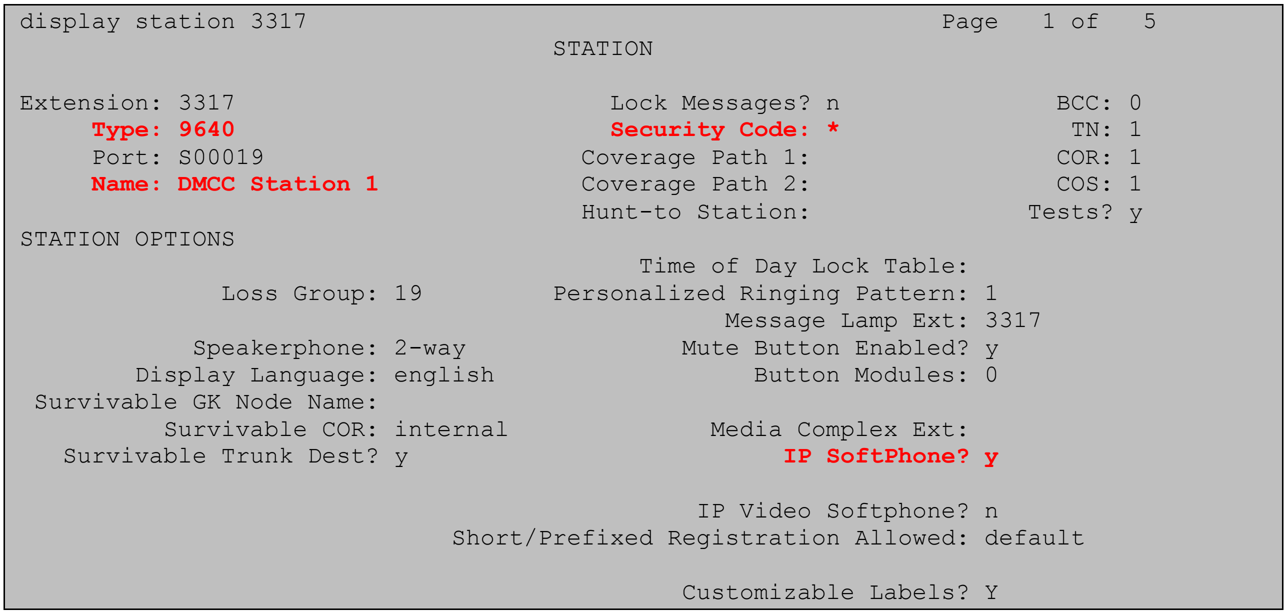


```
display station 3301                                            Page   1 of   6
                                     STATION

Extension: 3301                          Lock Messages? n               BCC: 0
     Type: 9641                          Security Code: *                TN: 1
     Port: S00011                      Coverage Path 1:                 COR: 1
     Name:                             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: 3301
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                  Button Modules: 1
 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
```

## 5.7. Add Virtual Stations

Virtual stations are used by Call Witness to do Single Step Conference based call recording for stations (SIP and Analog) that are not capable of supporting IP Softphone or have the IP Softphone setting disabled. Add a virtual station using **the add station <n>** command; where **<n>** is an available extension number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- In the **Type** field, enter a station type such as **9640**
- In the **Name** field, enter a name containing the **DMCC** string (e.g. **DMCC Station 1**).
- In the **Security Code** field, enter a code as same as extension number. Call Witness uses the same number of extension for the security code to register to DMCC station.
- Set the **IP SoftPhone** field to **y**



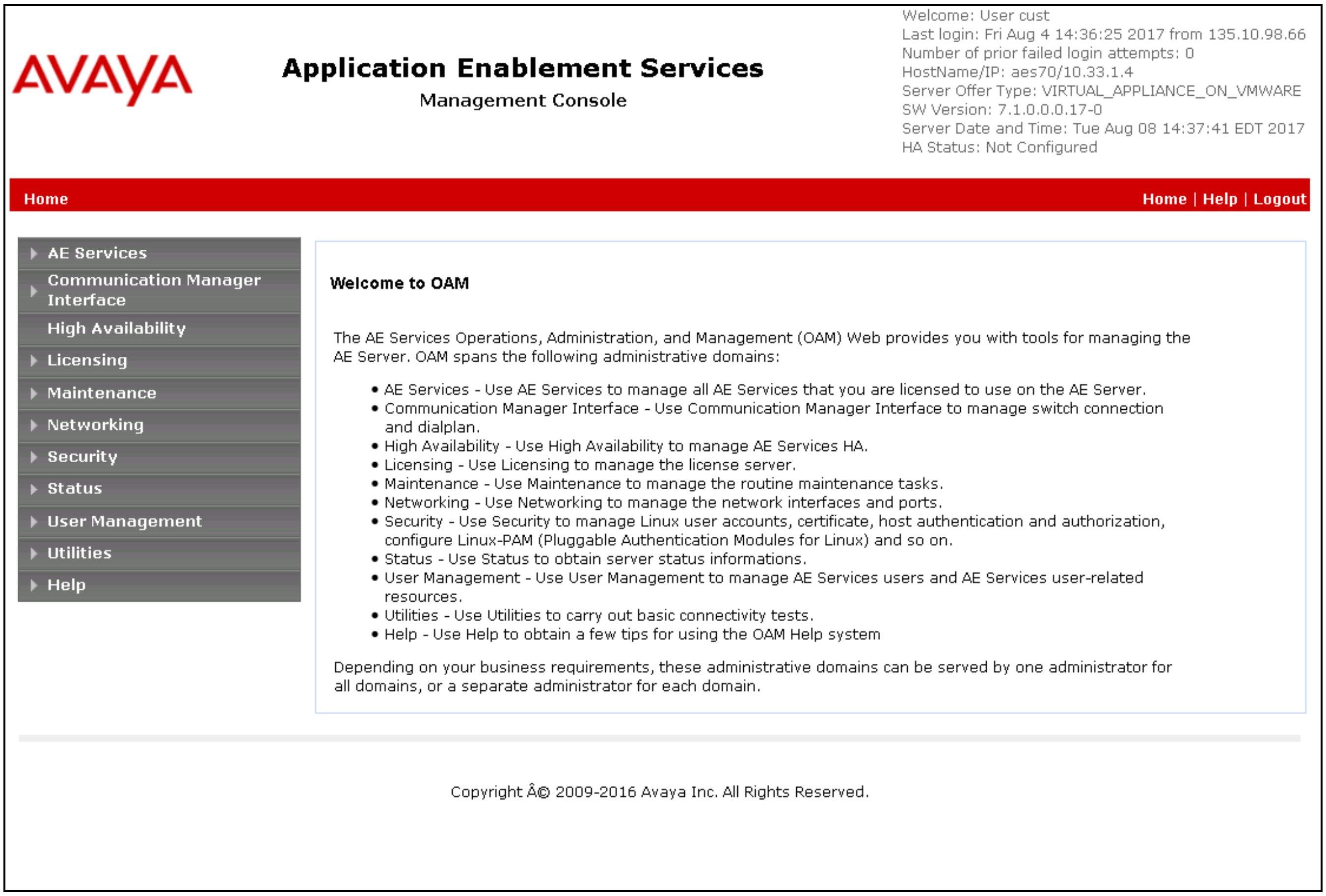
```
display station 3317                                            Page   1 of   5
                                     STATION

Extension: 3317                          Lock Messages? n               BCC: 0
     Type: 9640                          Security Code: *                TN: 1
     Port: S00019                      Coverage Path 1:                 COR: 1
     Name: DMCC Station 1              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: 3317
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                  Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal                Media Complex Ext:
   Survivable Trunk Dest? y                            IP SoftPhone? y

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

                                              Customizable Labels? Y
```

# 6. Configure Avaya Aura® Application Enablement Services

All administration of Application Enablement Services is performed via a web browser. Enter https://<ip-addr> in the URL field of a web browser where <ip-addr> is the IP address of the Application Enablement Services server. After a login step, the **Welcome to OAM** page is displayed. Note that all navigation is performed by clicking links in the Navigation Panel on the left side of the screen, context panels will then appear on the right side of the screen.

The procedures fall into the following areas:

- Configure Communication Manager Switch Connections
- Configure Call Witness User
- Confirm TSAPI and DMCC Licenses



Welcome: User cust
Last login: Fri Aug 4 14:36:25 2017 from 135.10.98.66
Number of prior failed login attempts: 0
HostName/IP: aes70/10.33.1.4
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.0.0.0.17-0
Server Date and Time: Tue Aug 08 14:37:41 EDT 2017
HA Status: Not Configured

**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:

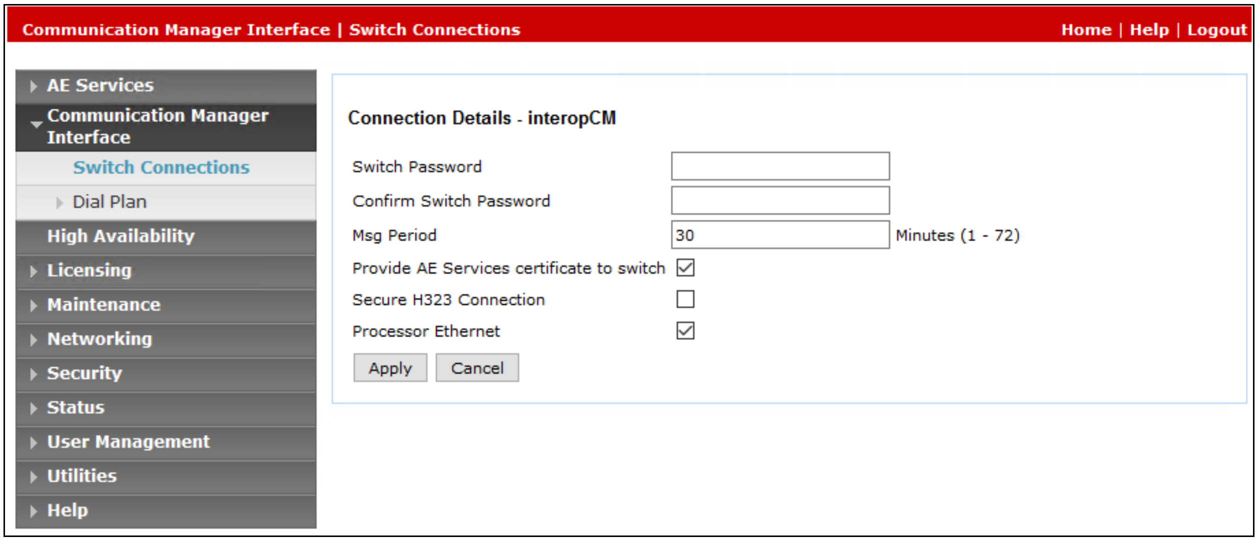
- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- 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 Â© 2009-2016 Avaya Inc. All Rights Reserved.

## 6.1. Configure Communication Manager Switch Connections

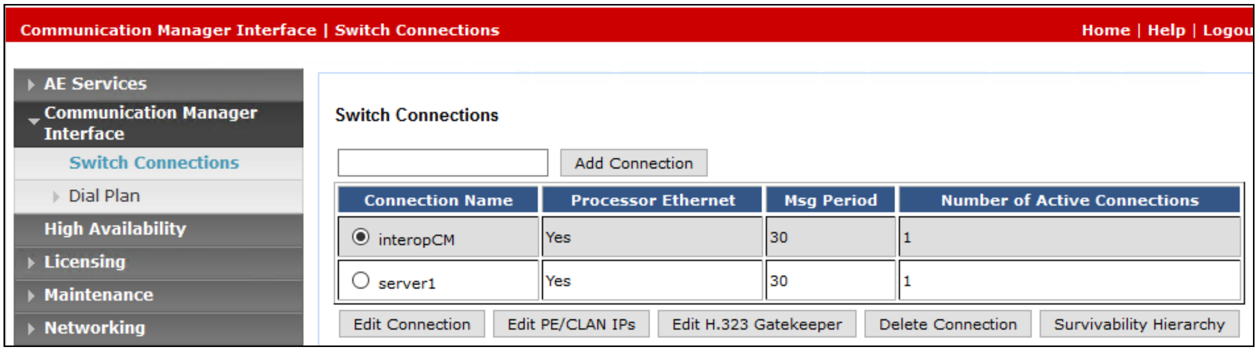
To add links to Communication Manager, navigate to the **Communication Manager Interface → Switch Connections** page and enter a name for the new switch connection (e.g. **interopCM**) and click the **Add Connection** button (not shown). The **Connection Details** screen is shown. Enter the **Switch Password** configured in **Section 5.3** and check the **Processor Ethernet** box if using the **procr** interface. Click **Apply**.



Connection Details - interopCM

| | | |
|---|---|---|
| Switch Password | | |
| Confirm Switch Password | | |
| Msg Period | 30 | Minutes (1 - 72) |
| Provide AE Services certificate to switch | ☑ | |
| Secure H323 Connection | □ | |
| Processor Ethernet | ☑ | |

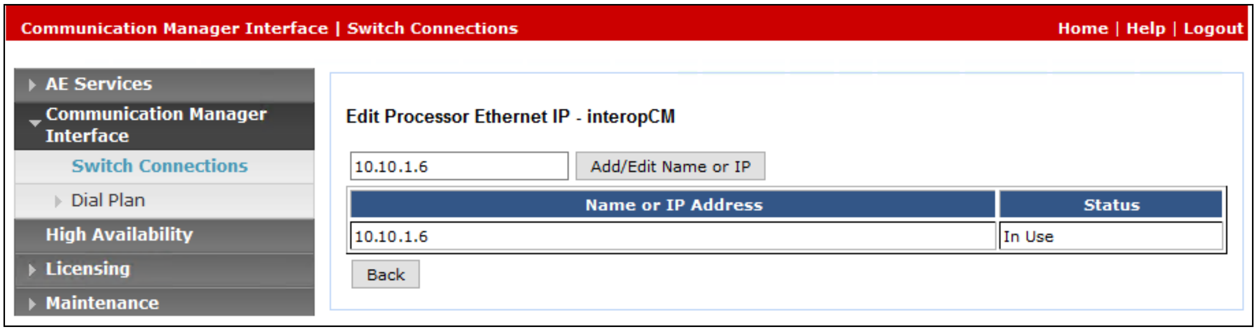
The display returns to the **Switch Connections** screen which shows that the **interopCM** switch connection has been added.



Switch Connections

| Connection Name | Processor Ethernet | Msg Period | Number of Active Connections |
|---|---|---|---|
| ● interopCM | Yes | 30 | 1 |
| ○ server1 | Yes | 30 | 1 |

Click the **Edit PE/CLAN IPs** button on the **Switch Connections** screen to configure the **procr** or **CLAN** IP Address(es) for TSAPI message traffic. The **Edit Processor Ethernet IP** screen is displayed. Enter the IP address of the **procr** interface and click the **Add/Edit Name or IP** button.

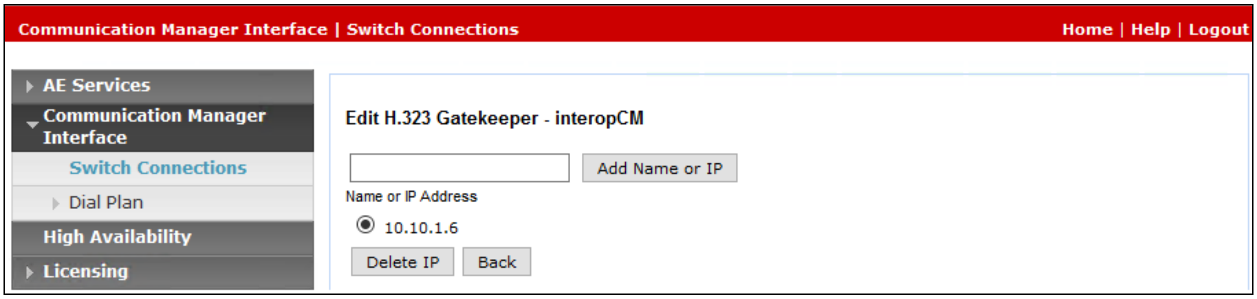


Edit Processor Ethernet IP - interopCM

10.10.1.6

| Name or IP Address | Status |
|---|---|
| 10.10.1.6 | In Use |

Click the **Edit H.323 Gatekeeper** button on the **Switch Connections** screen to configure the **procr** or **CLAN** IP Address(es) for DMCC registrations. The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of the **procr** interface and click the **Add Name or IP** button.



Edit H.323 Gatekeeper - interopCM

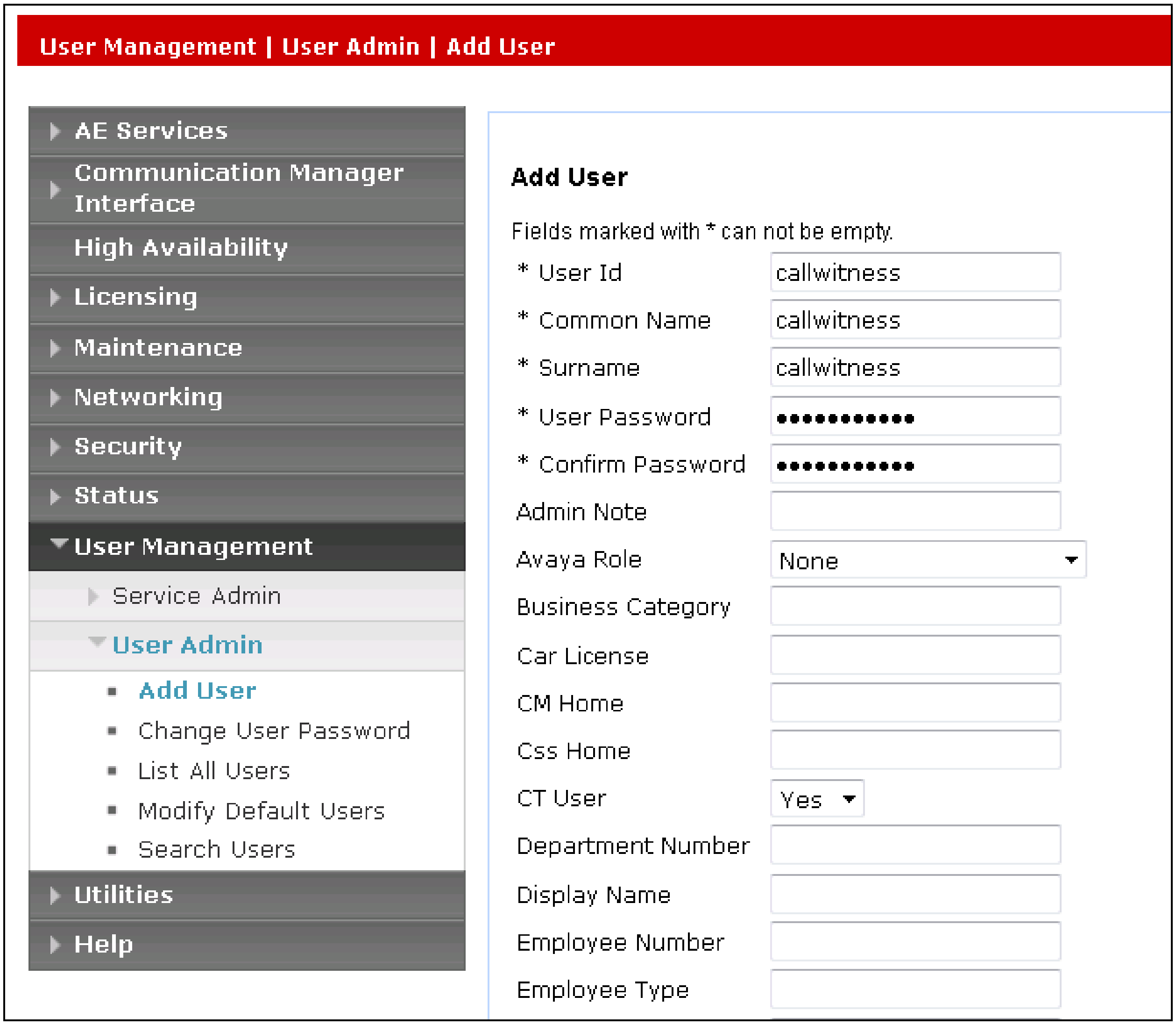
Name or IP Address

● 10.10.1.6

## 6.2. Configure a Call Witness User

In the Navigation Panel, select **User Management → User Admin → Add User**. The **Add User** panel will display as shown below. Enter an appropriate **User Id, Common Name, Surname,** and **User Password**. Select **Yes** from the **CT User** dropdown list.

Click **Apply** (not shown) at the bottom of the pages to save the entries.



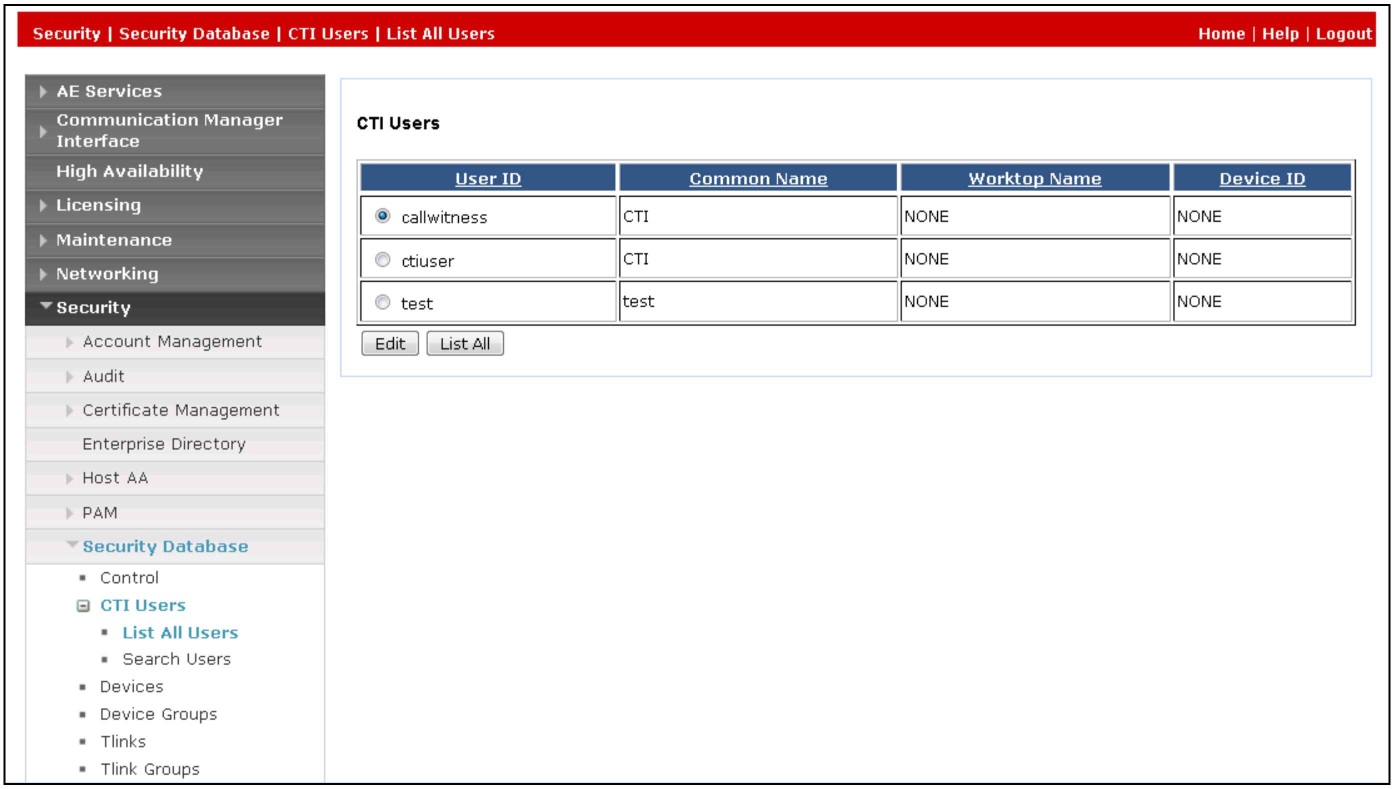
**Add User**

Fields marked with * can not be empty.

| | |
|---|---|
| * User Id | callwitness |
| * Common Name | callwitness |
| * Surname | callwitness |
| * User Password | ●●●●●●●●●●● |
| * Confirm Password | ●●●●●●●●●●● |
| Admin Note | |
| Avaya Role | None |
| Business Category | |
| Car License | |
| CM Home | |
| Css Home | |
| CT User | Yes |
| Department Number | |
| Display Name | |
| Employee Number | |
| Employee Type | |

If the Security Database (SDB) is enabled on Application Enablement Services, set the callwitness user account to Unrestricted Access to enable any device (station, ACD extension, DMCC virtual station) to be used implicitly. This step avoids the need to duplicate administration.

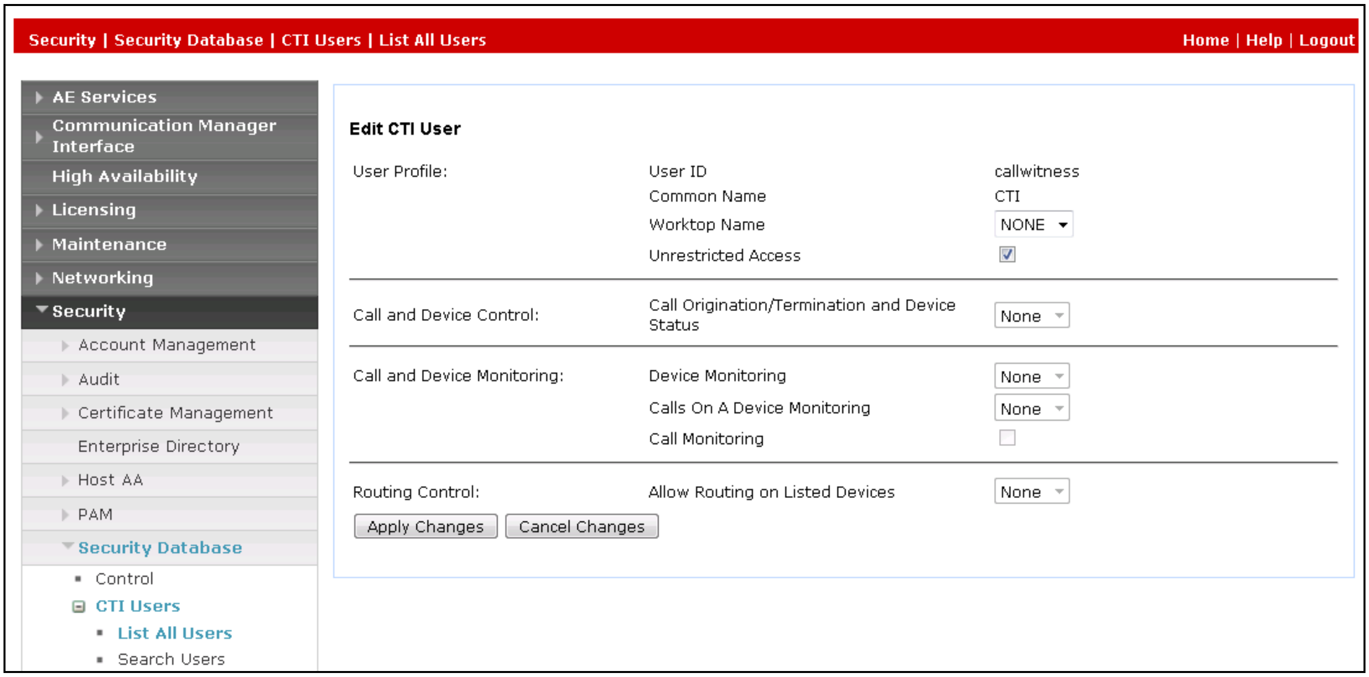
Navigate to **Security → Security Database → CTI Users → List All Users** and select the **callwitness** user and click **Edit**.



CTI Users

| User ID | Common Name | Worktop Name | Device ID |
|---|---|---|---|
| ● callwitness | CTI | NONE | NONE |
| ○ ctiuser | CTI | NONE | NONE |
| ○ test | test | NONE | NONE |

On the **Edit CTI User** panel, check the **Unrestricted Access** box and click the **Apply Changes** button. Click **Apply** when asked to confirm the change on the **Apply Changes to CTI User Properties** dialog.



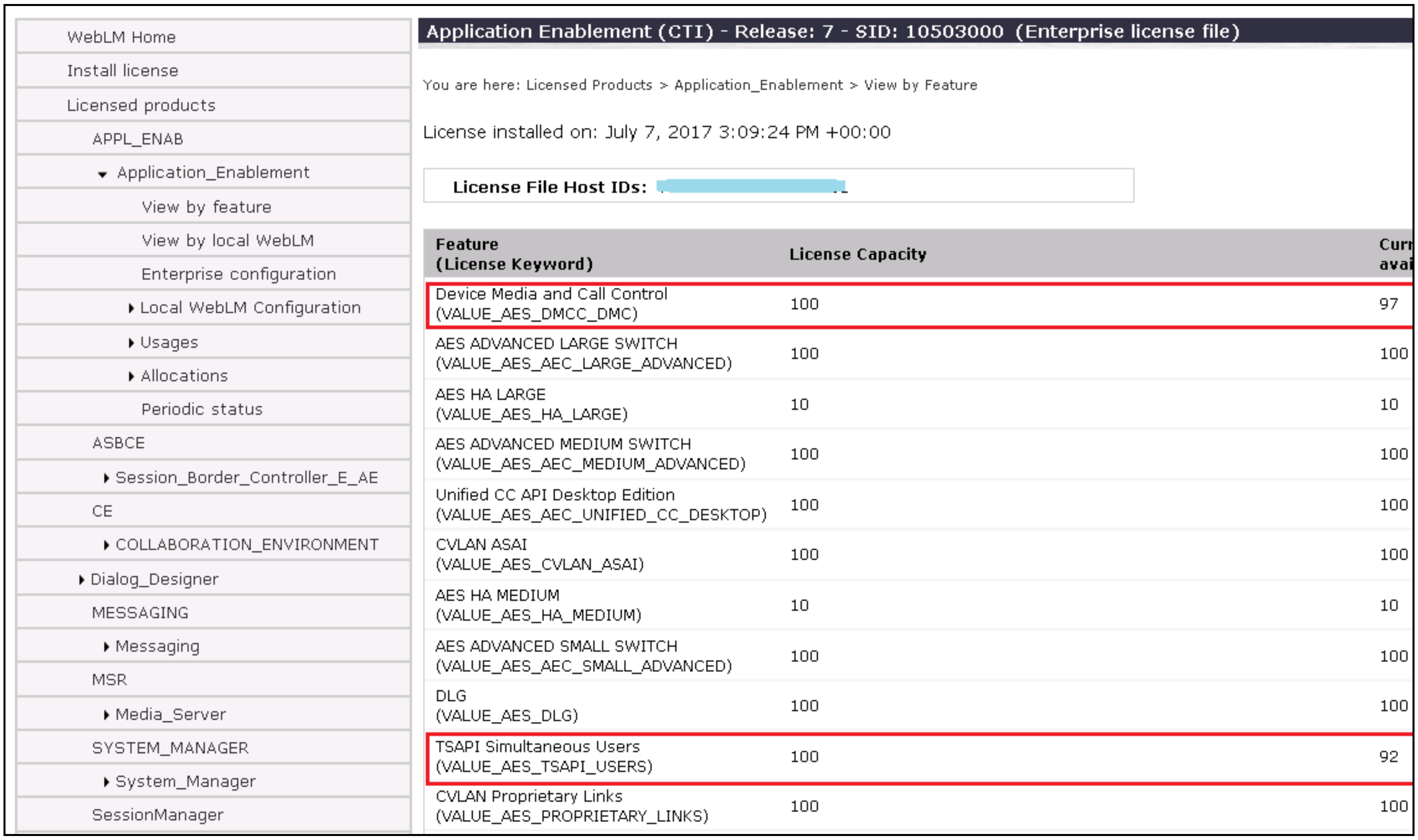
**Edit CTI User**

| | | |
|---|---|---|
| User Profile: | User ID | callwitness |
| | Common Name | CTI |
| | Worktop Name | NONE |
| | Unrestricted Access | ☑ |
| Call and Device Control: | Call Origination/Termination and Device Status | None |
| Call and Device Monitoring: | Device Monitoring | None |
| | Calls On A Device Monitoring | None |
| | Call Monitoring | ☐ |
| Routing Control: | Allow Routing on Listed Devices | None |

## 6.3. Confirm TSAPI and DMCC Licenses

Call Witness consumes a TSAPI Basic (**VALUE_AES_TSAPI_USERS**) license for each station being monitored for call events. Call Witness also consumes a DMCC license for each recording port.  A DMCC license is normally a **VALUE_AES_DMCC_DMC** from AE Services' WebLM. As a fall back, when a **VALUE_AES_DMCC_DMC** license is not available, an **IP_API_A** license from Communication Manager can be utilized in place of **VALUE_AES_DMCC_DMC**.  Please consult product offer documentation for more details. If the licensed quantities are not sufficient for the implementation, contact the Avaya sales team or business partner for a proper license file.

From the left pane menu on Application Enablement Services  Management Console, click **Licensing → WebLM Server Access**. A **Web License Manager** login window is displayed. Enter proper credentials to log in. Click **Licensed products → APPL_ENAB → Application_Enablement** from the left pane. The Application Enablement Services license is displayed in the right pane. Ensure that there are enough **VALUE_AES_DMCC_DMC** and **VALUE_AES_TSAPI_USERS** licenses available.



Application Enablement (CTI) - Release: 7 - SID: 10503000 (Enterprise license file)

You are here: Licensed Products > Application_Enablement > View by Feature

License installed on: July 7, 2017 3:09:24 PM +00:00

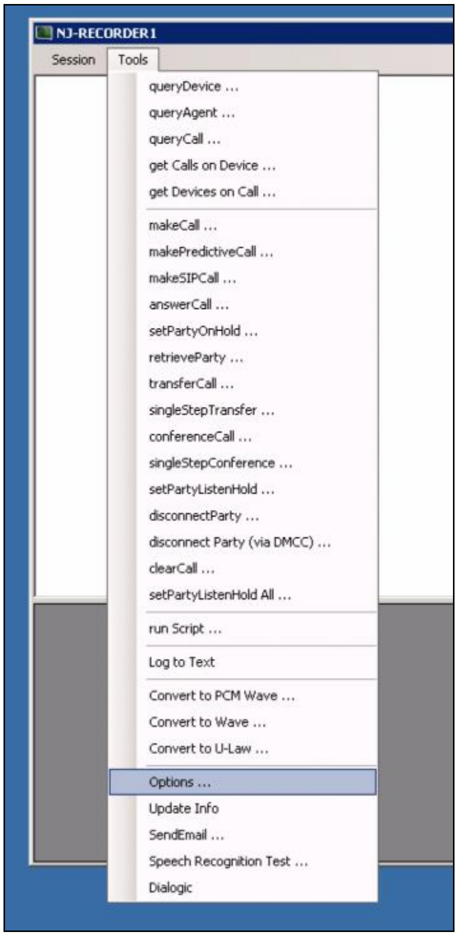
**License File Host IDs:** [redacted]

| **Feature**<br>**(License Keyword)** | **License Capacity** | **Curr**<br>**avai** |
|---|---|---|
| Device Media and Call Control<br>(VALUE_AES_DMCC_DMC) | 100 | 97 |
| AES ADVANCED LARGE SWITCH<br>(VALUE_AES_AEC_LARGE_ADVANCED) | 100 | 100 |
| AES HA LARGE<br>(VALUE_AES_HA_LARGE) | 10 | 10 |
| AES ADVANCED MEDIUM SWITCH<br>(VALUE_AES_AEC_MEDIUM_ADVANCED) | 100 | 100 |
| Unified CC API Desktop Edition<br>(VALUE_AES_AEC_UNIFIED_CC_DESKTOP) | 100 | 100 |
| CVLAN ASAI<br>(VALUE_AES_CVLAN_ASAI) | 100 | 100 |
| AES HA MEDIUM<br>(VALUE_AES_HA_MEDIUM) | 10 | 10 |
| AES ADVANCED SMALL SWITCH<br>(VALUE_AES_AEC_SMALL_ADVANCED) | 100 | 100 |
| DLG<br>(VALUE_AES_DLG) | 100 | 100 |
| TSAPI Simultaneous Users<br>(VALUE_AES_TSAPI_USERS) | 100 | 92 |
| CVLAN Proprietary Links<br>(VALUE_AES_PROPRIETARY_LINKS) | 100 | 100 |

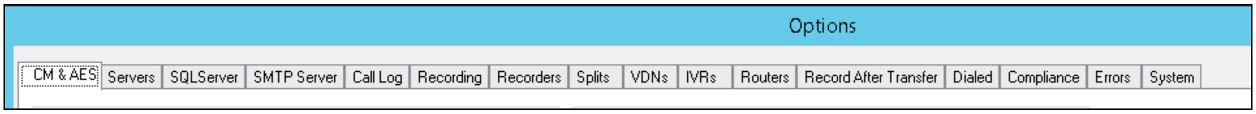
# 7. Configure Controlled Networks Call Witness

The initial configuration of the Call Witness server is typically performed by Controlled Networks technicians or authorized installers. These Application Notes will only cover the steps necessary to configure the Call Witness solution to interoperate with Communication Manager and Application Enablement Services.

To configure Call Witness server, follow the steps below, all the configurations are done in the Core Administration Panel. From the Call Witness server, navigate to **Tools →Options** to access the configuration Options navigate.

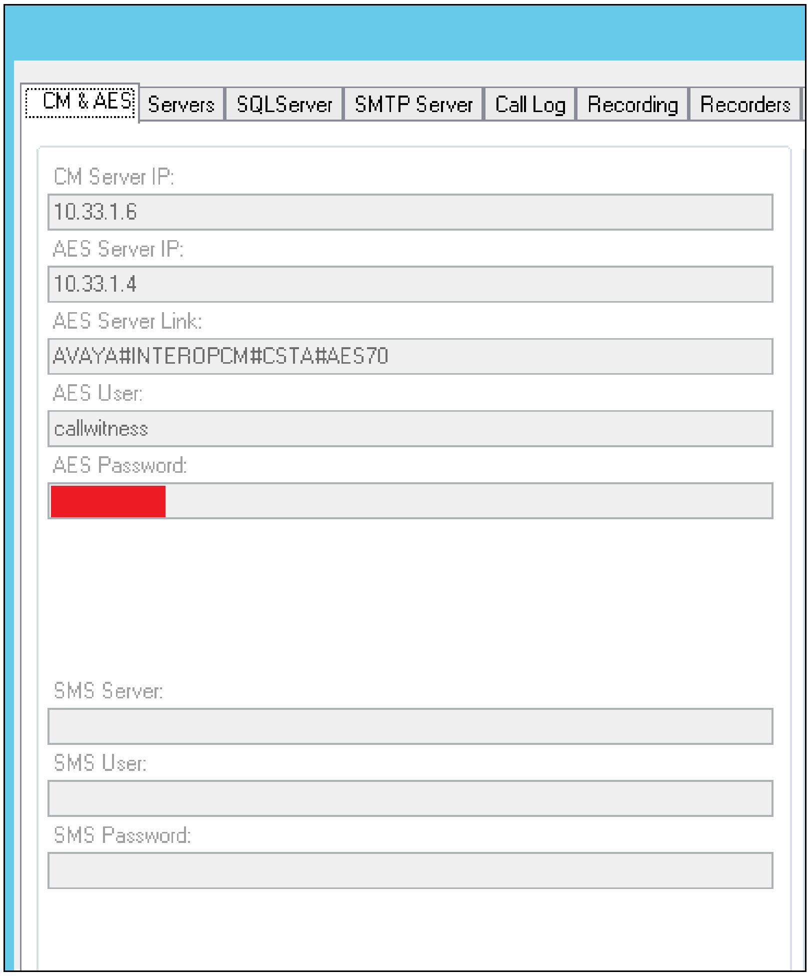


The following menu **tabs** will appear at the top of the menu screen.



1. To access and configure the **Communication Manager** and the **Application Enablement Services** settings, select the **CM & AES** tab. Enter the appropriate **CM Server IP, AES Server IP, AES Server Link, AES User,** and **AES Password** as shown in the picture below.

   Click **Save** button at the bottom of the pages to save the entries.



CM Server IP: 10.33.1.6

AES Server IP: 10.33.1.4

AES Server Link: AVAYA#INTEROPCM#CSTA#AES70

AES User: callwitness

AES Password: [redacted]

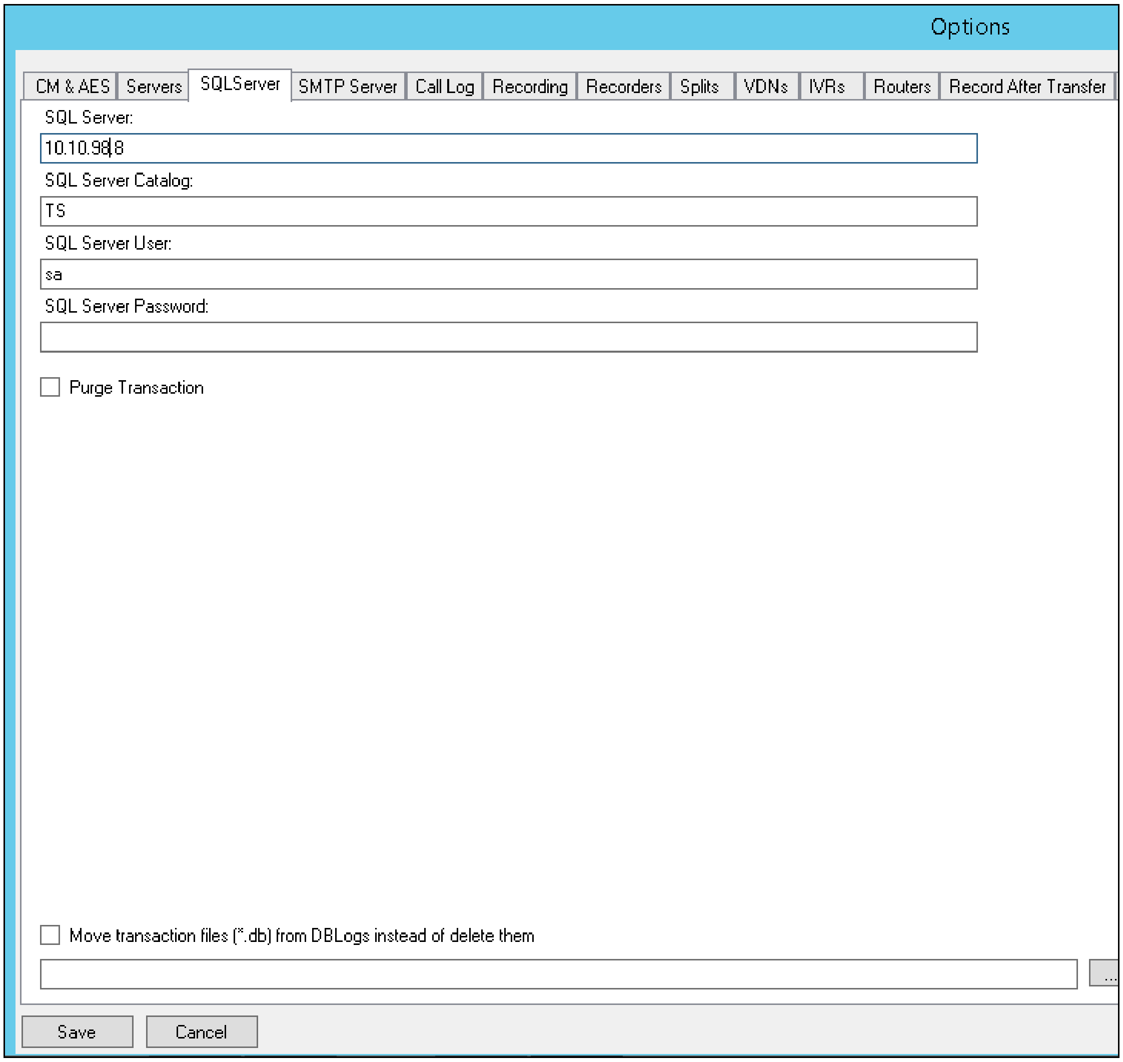
SMS Server:

SMS User:

SMS Password:

2. To configure the **SQL Server** Settings, select the **SQL Server** tab. Enter the appropriate **SQL Server IP, SQL Server Catalog, SQL Server User, SQL Server Password**, and keep other settings at default as shown below.

   Click **Save** at the bottom of the pages to save the entries.



SQL Server: 10.10.98.8

SQL Server Catalog: TS

SQL Server User: sa

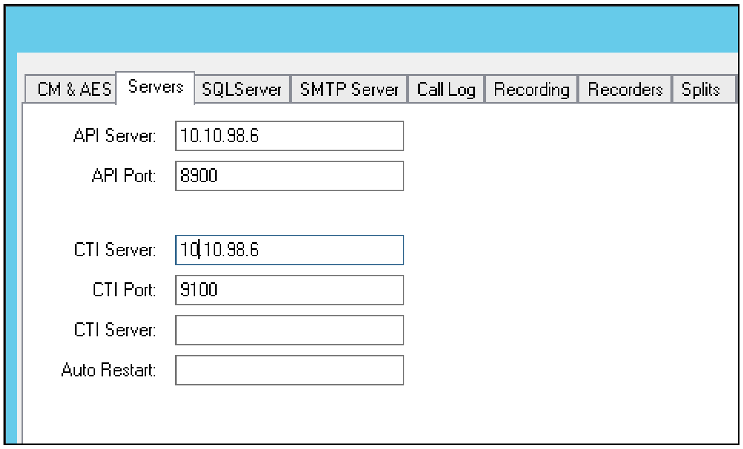
SQL Server Password:

□ Purge Transaction

□ Move transaction files (*.db) from DBLogs instead of delete them

3. To configure the **API Server** Settings, select the **Servers** tab. Enter the appropriate **API Server IP, API Port, CTI Server IP, CTI Port, CTI Server**.

   Click **Save** at the bottom of the pages to save the entries.



API Server: 10.10.98.6

API Port: 8900

CTI Server: 10.10.98.6

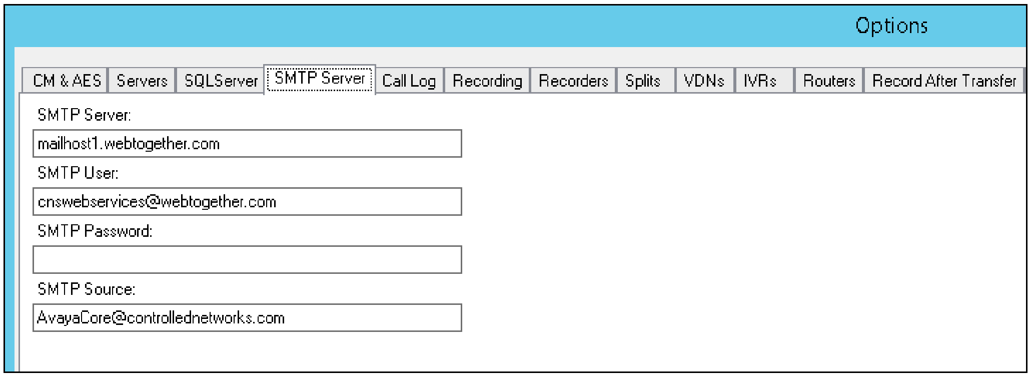
CTI Port: 9100

CTI Server:

Auto Restart:

4. To configure the **SMTP Server** Settings, select the **SMTP Server** tab. Enter the appropriate **SMTP Server IP, SMTP User, SMTP Password, SMTP Source,** define the **Call Reporting URL Path** and **select the V3 Version.**

   Click **Save** at the bottom of the pages to save the entries.



SMTP Server:
mailhost1.webtogether.com

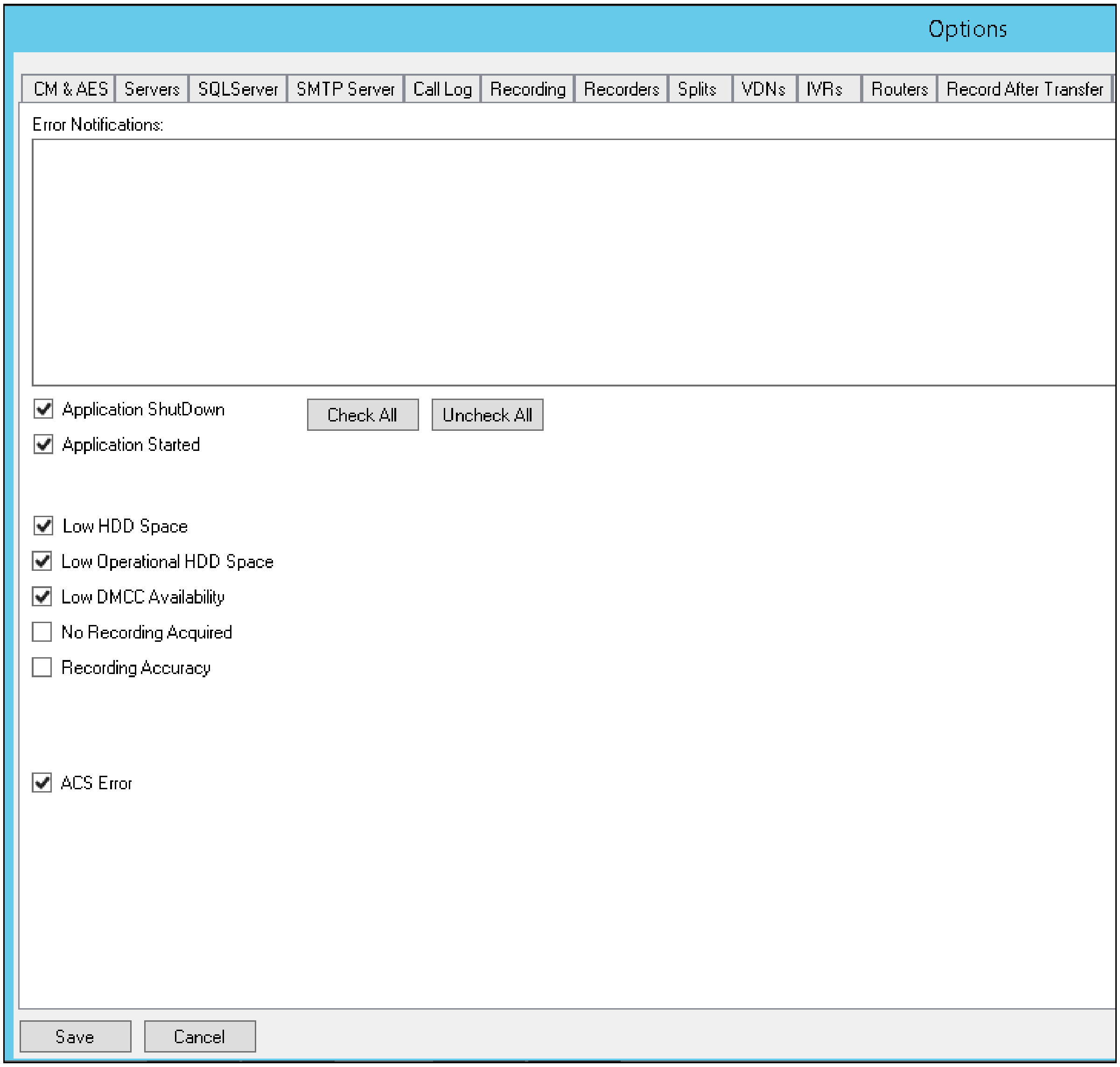
SMTP User:
cnswebservices@webtogether.com

SMTP Password:

SMTP Source:
AvayaCore@controllednetworks.com

5. To configure the **Error Notifications** Settings, select the **Errors** Tab. Enter the appropriate **Error Notifications** email addresses you would like to notify in the event of a failure of alerts. Select the following boxes: **Application Shutdown, Application Started, Low HDD Space**, **Low Operational HDD Space** and **Low DMCC Availability** and keep other settings at default as shown below.

   Click **Save** at the bottom of the pages to save the entries.



Error Notifications:

☑ Application ShutDown

☑ Application Started

☑ Low HDD Space

☑ Low Operational HDD Space

☑ Low DMCC Availability

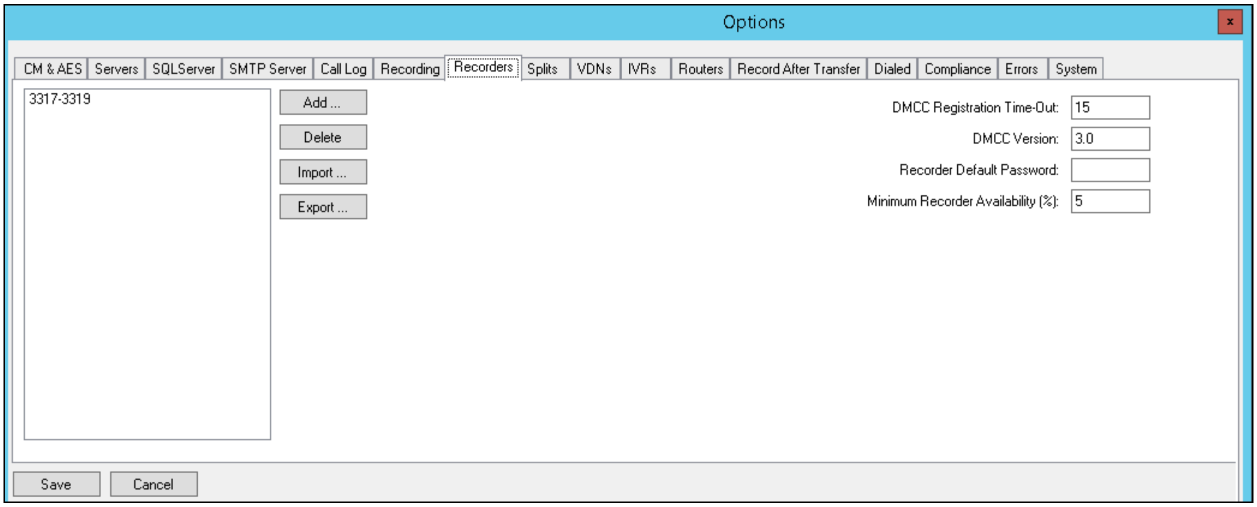
□ No Recording Acquired

□ Recording Accuracy

☑ ACS Error

6. To access and configure the DMCC Settings, select the **Recorders Tab**. Add the DMCC virtual station configured in **Section 5.7** and keep other settings at default as shown in the picture below. Call Witness registers to the virtual DMCC stations through AES.

   Click **Save** at the bottom of the pages to save the entries.



3317-3319

DMCC Registration Time-Out: 15

DMCC Version: 3.0

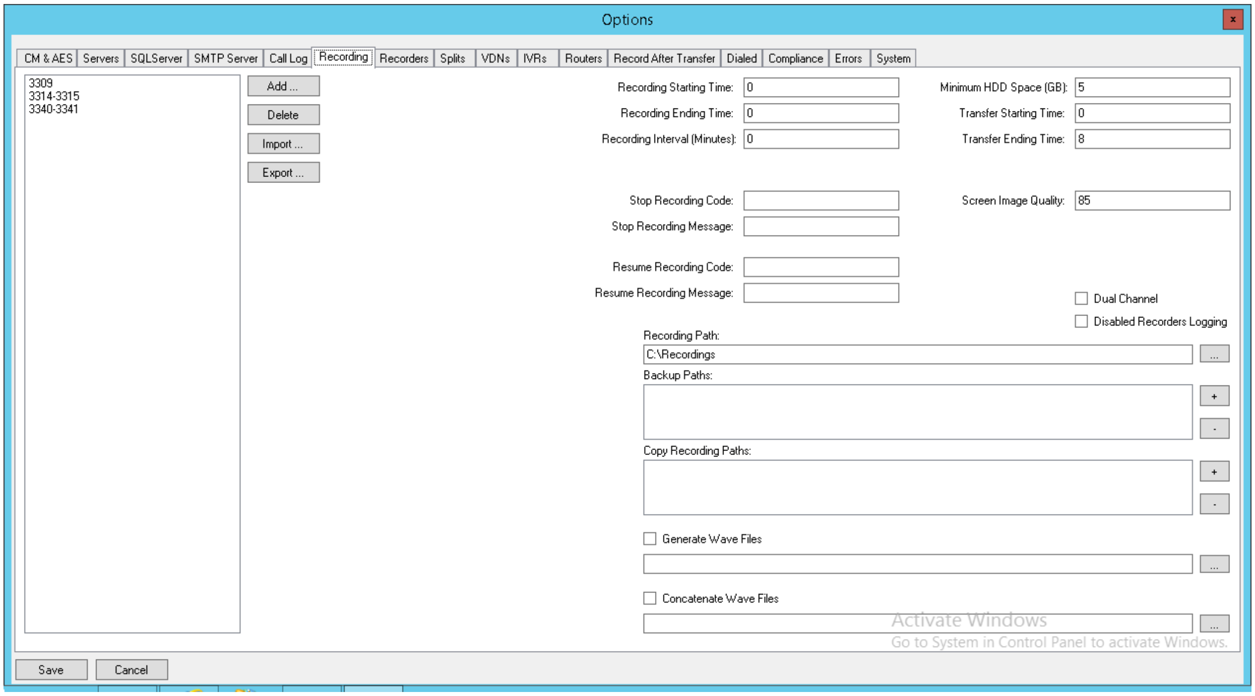
Recorder Default Password:

Minimum Recorder Availability (%): 5

7. To configure the **Recording** Settings, select the **Recording** Tab. Select **Add** button to add recording stations that include H.323, SIP, Digital, Analog and VDN extensions and keep other settings at the default as shown in the picture below.

   Specify the recording file in the Recording Path field and do not check **Generate Wave Files Box** and **Concatenate Waves Files Box**.

   Click **Save** at the bottom of the pages to save the entries.



Options
CM & AES | Servers | SQLServer | SMTP Server | Call Log | Recording | Recorders | Splits | VDNs | IVRs | Routers | Record After Transfer | Dialed | Compliance | Errors | System
Add ...
Delete
Import ...
Export ...
Save
Cancel

3309
3314-3315
3340-3341

Recording Starting Time: 0
Recording Ending Time: 0
Recording Interval (Minutes): 0
Minimum HDD Space (GB): 5
Transfer Starting Time: 0
Transfer Ending Time: 8
Stop Recording Code:
Stop Recording Message:
Screen Image Quality: 85
Resume Recording Code:
Resume Recording Message:
☐ Dual Channel
☐ Disabled Recorders Logging
Recording Path: C:\Recordings
Backup Paths:
Copy Recording Paths:
☐ Generate Wave Files
☐ Concatenate Wave Files

Activate Windows
Go to System in Control Panel to activate Windows.

# 8. Verification Steps

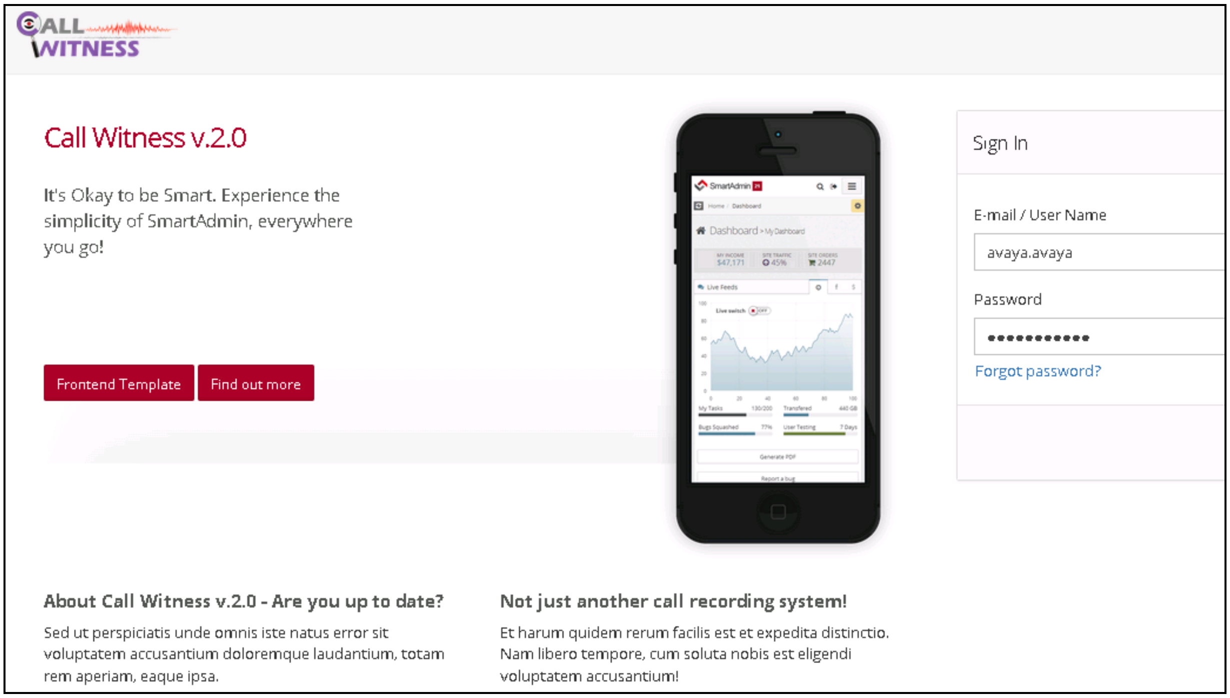
The following steps may be used to verify the configuration:

## 8.1. Verify using SAT command

- Verify that the interface on Communication Manager to Application Enablement Services is enabled and in **listening** status (use the **status aesvcs interface** command on the Communication Manager SAT).
- Verify that the link between Communication Manager and Application Enablement Services is transmitting and receiving messages (use the **status aesvcs link** command on the SAT).
- Verify that the **con state** of the Switch Connection is **talking** (on Application Enablement Services web page, navigate to **Status → Status and Control → Switch Conn Summary**).
- Verify that the **service state** of the CTI link is **established** (use the **status aesvcs cti-link** command on the SAT).
- Verify that the Call Witness recording ports are registered as **IP_API_A** stations in Communication Manager (use the **list registered-ip-stations** command on the SAT).
- Verify the Call Witness server has successfully monitored the stations using TSAPI (use the **list monitored-stations** command on the SAT).
- Verify that calls may be successfully completed to and from stations and VDN. Verify that the call recordings are accurate and complete.

## 8.2. Verify Recording and Playback

Access the Call Witness web-based user interface using the URL **http://<ip-address>** in a browser window, where **<ip-address>** is the address of the Call Witness server. The Log In screen is displayed as shown below. Use appropriate credentials to log in.



Call Witness v.2.0

It's Okay to be Smart. Experience the simplicity of SmartAdmin, everywhere you go!

E-mail / User Name: avaya.avaya

Password: ●●●●●●●●●●●●

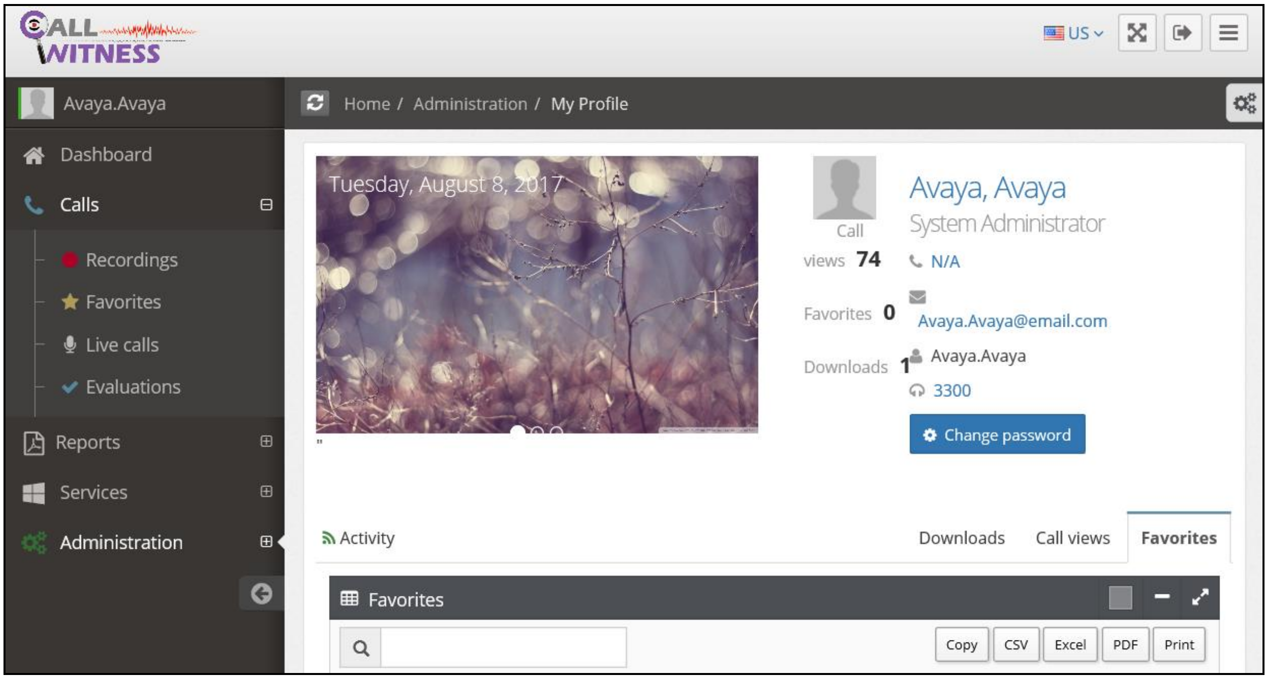
About Call Witness v.2.0 - Are you up to date?

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa.

Not just another call recording system!

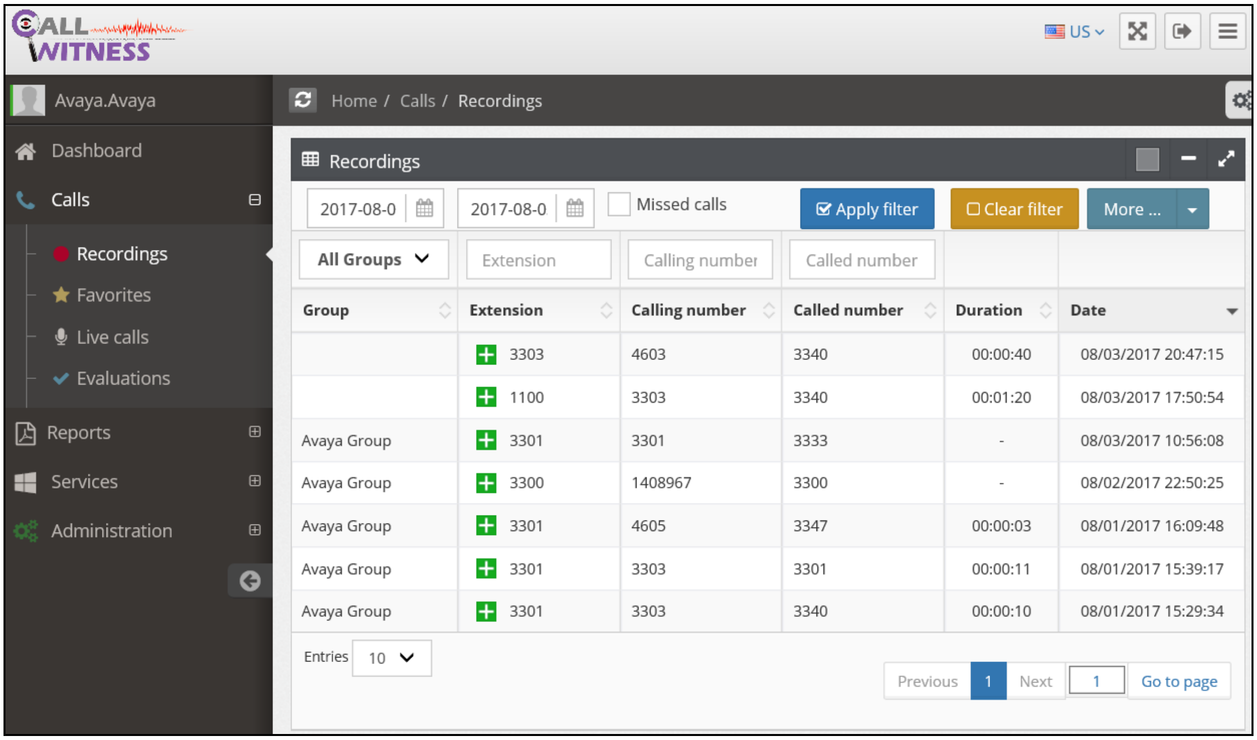
Et harum quidem rerum facilis est et expedita distinctio. Nam libero tempore, cum soluta nobis est eligendi voluptatem accusantium!

Once logged in, navigate to **Calls → Recordings** from the left navigation pane to reach the **Recordings** page.



Avaya, Avaya
System Administrator
Call views 74
Favorites 0
Downloads 1
N/A
Avaya.Avaya@email.com
Avaya.Avaya
3300

On the **Recordings** page, it displays all call records that are recently recorded. The filter can be applied by entering the date, Calling number, Called number...etc.

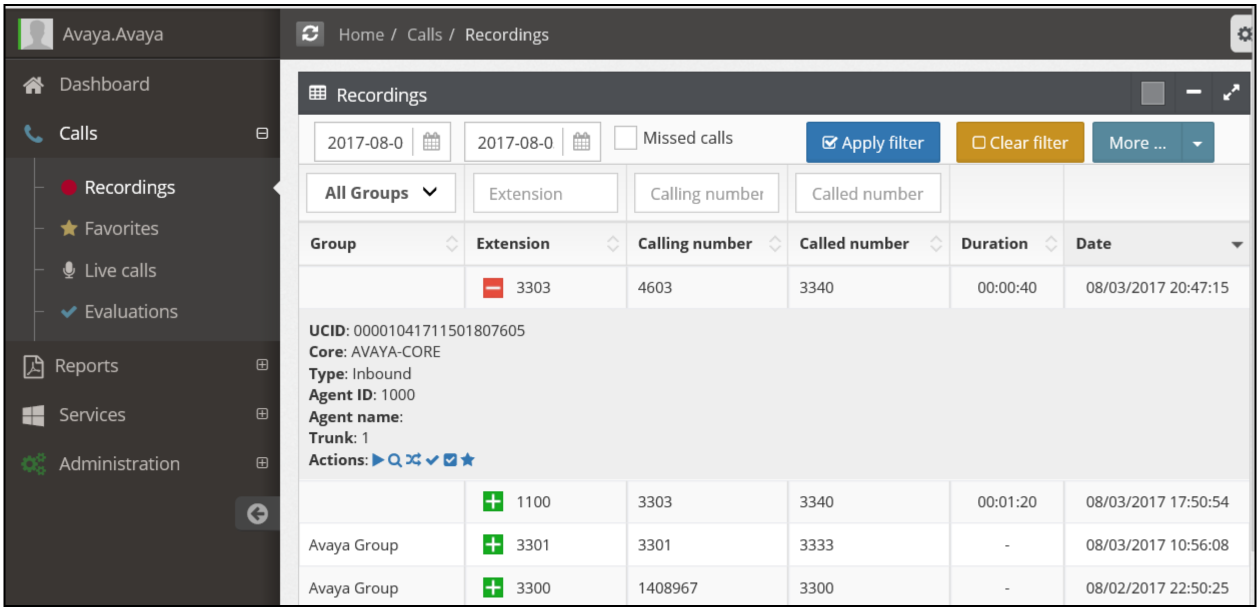


2017-08-0 | 2017-08-0 | □ Missed calls

| Group | Extension | Calling number | Called number | Duration | Date |
|---|---|---|---|---|---|
| | 3303 | 4603 | 3340 | 00:00:40 | 08/03/2017 20:47:15 |
| | 1100 | 3303 | 3340 | 00:01:20 | 08/03/2017 17:50:54 |
| Avaya Group | 3301 | 3301 | 3333 | - | 08/03/2017 10:56:08 |
| Avaya Group | 3300 | 1408967 | 3300 | - | 08/02/2017 22:50:25 |
| Avaya Group | 3301 | 4605 | 3347 | 00:00:03 | 08/01/2017 16:09:48 |
| Avaya Group | 3301 | 3303 | 3301 | 00:00:11 | 08/01/2017 15:39:17 |
| Avaya Group | 3301 | 3303 | 3340 | 00:00:10 | 08/01/2017 15:29:34 |

Entries 10

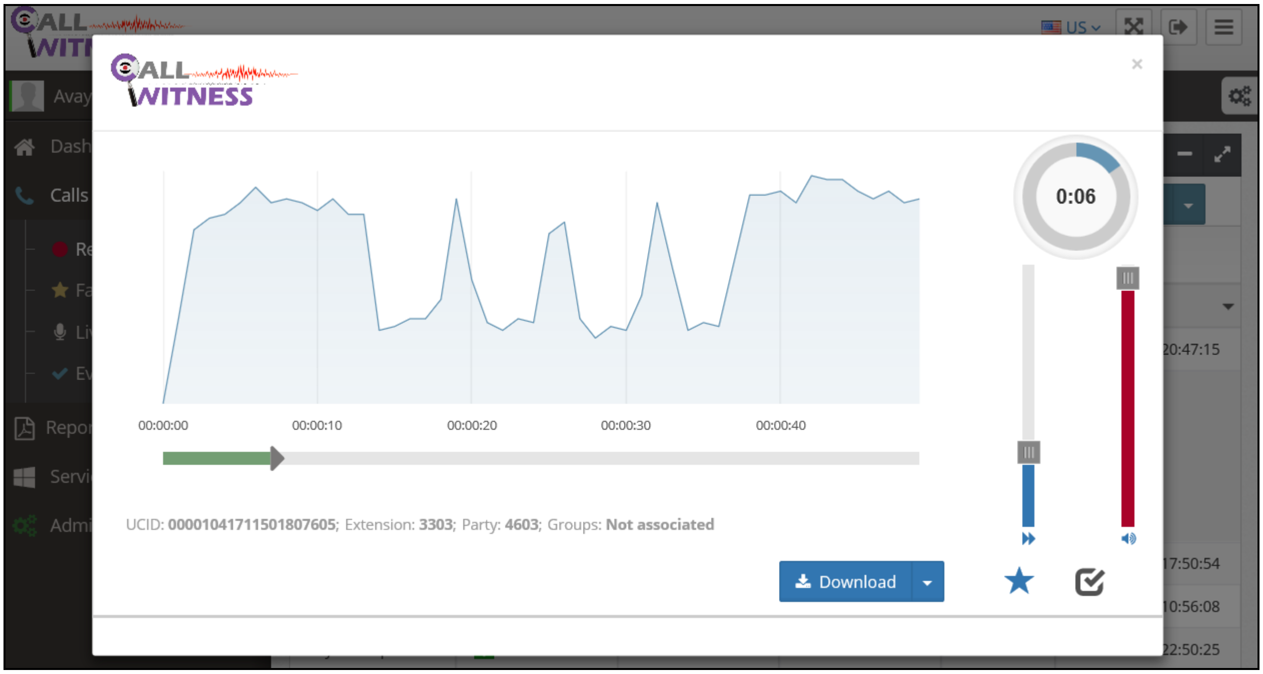
Select a call of interest and click the green plus sign to expand call record information.



| Group | Extension | Calling number | Called number | Duration | Date |
|---|---|---|---|---|---|
| | ⊟ 3303 | 4603 | 3340 | 00:00:40 | 08/03/2017 20:47:15 |
| | ⊞ 1100 | 3303 | 3340 | 00:01:20 | 08/03/2017 17:50:54 |
| Avaya Group | ⊞ 3301 | 3301 | 3333 | - | 08/03/2017 10:56:08 |
| Avaya Group | ⊞ 3300 | 1408967 | 3300 | - | 08/02/2017 22:50:25 |

**UCID**: 00001041711501807605
**Core**: AVAYA-CORE
**Type**: Inbound
**Agent ID**: 1000
**Agent name**:
**Trunk**: 1
**Actions**:

Click on Play button to launch a playback window as shown below.



UCID: **00001041711501807605**; Extension: **3303**; Party: **4603**; Groups: **Not associated**

# 9. Conclusion

These Application Notes describe the procedures for configuring Controlled Network Call Witness to monitor and record calls placed to and from agents and phones on Avaya Aura® Communication Manager. All feature and serviceability test cases were completed and passed with the observations noted in **Section 2.2**.

# 10. Additional References

Product documentation for Avaya products may be found at http://support.avaya.com.

1. *Administering Avaya Aura® Communication Manager*, Release 7.0, 03-300509.
2. *Administering and Maintaining Avaya Aura® Application Enablement Services*, Release 7.0.

Product documentation related to Call Witness can be obtained directly from Controlled Networks.

1. *Call Witness V.2.0 User Guide*
2. *Call Witness Call Recording General*

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.