Avaya Solution & Interoperability Test Lab

Application Notes for Equature Interactive Public Safety Response with Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes cover the interoperability compliance testing of the Equature Interactive Public Safety Response recording solution with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services (AES).

In the compliance testing, Equature used various Registration features from the Avaya Aura® Application Enablement Services Device, Media, and Call Control interface to capture media associated with monitored agent stations for call recording.

Readers should pay attention to Section 2, in particular the scope of testing as outlined in Section 2.1 as well as any 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

Equature Interactive Public Safety Response provides real-time interactive technology platforms to police, first responders, military, government agency officers and private security organizations. Equature enables originations to record, manage and utilize data from many sources for public safety, compliance, business intelligence and quality assurance.

The Equature system interfaces with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services, using the Telephony Service API (TSAPI) to obtain call event information and the Device, Media & Call Control (DMCC) API to obtain audio via various Registration methods.

The compliance testing focused on the monitoring and recording performed by Equature of calls placed to and/or from digital, IP, and SIP telephones, IP and SIP softphones, agents, hunt groups and Vector Directory Numbers (VDNs) supported by Communication Manager. Equature uses:

- The TSAPI interface of AES (via DMCC) to monitor extensions to obtain call events.
- The DMCC interface of AES to register the recorder as an additional registered endpoint with Communication Manager in order to record devices.

Serviceability tests were also conducted to assess the reliability of the Equature solution to recover from common network outages.

2. General Test Approach and Test Results

The feature test cases were performed manually. Upon start of the Equature application, the application automatically established a DMCC Stream with Application Enablement Services to register the recorder as a Main or Dependent IP Endpoint for each of the virtual or target stations on Communication Manager, and to receive Third Party call events via TSAPI through the DMCC stream.

Each call was handled manually at the agent station with generation of unique audio content for recording. Necessary agent actions such as hold and reconnect were performed from the Desk Phone or Softphone to test various call scenarios.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to Equature and Application Enablement Services.

The verification of tests included use of logs for proper message exchanges and use of the Equature web interfaces for proper logging and playback of call recordings.

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.

For the testing associated with these Application Notes, the interface between Avaya systems and Equature utilized enabled capabilities of TLS for Application links between Application Enablement Services and CM, and streams between Application Enablement Services and Equature. However, SRTP is not currently supported with the Equature solution so all media sessions between the Gateways and recorder were unsecured RTP.

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 Equature solution.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing.

The feature testing focused on verifying the following on Equature:

- Handling of call events.
- Use of DMCC registration services to register the virtual IP softphones.
- Use of DMCC monitoring services and media control events to obtain the media from the IP phones.
- Proper recording, logging, and playback of calls for scenarios involving hold, reconnect, conference, transfer.

The serviceability testing focused on verifying the ability of Equature to recover from adverse conditions, such as disconnecting and reconnecting the Ethernet connection to Equature and Application Enablement Services.

2.2. Test Results

All Test cases were executed and verified. The only observation is the current lack of support for SRTP media streams.

2.3. Support

Technical support on Equature can be obtained through the following:

- Phone: 888-305-3428
- Web: equature.com

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**.

The agent station extensions used in the compliance testing were 30001 through 30006. Virtual extensions 33001-33005 were also available for testing.

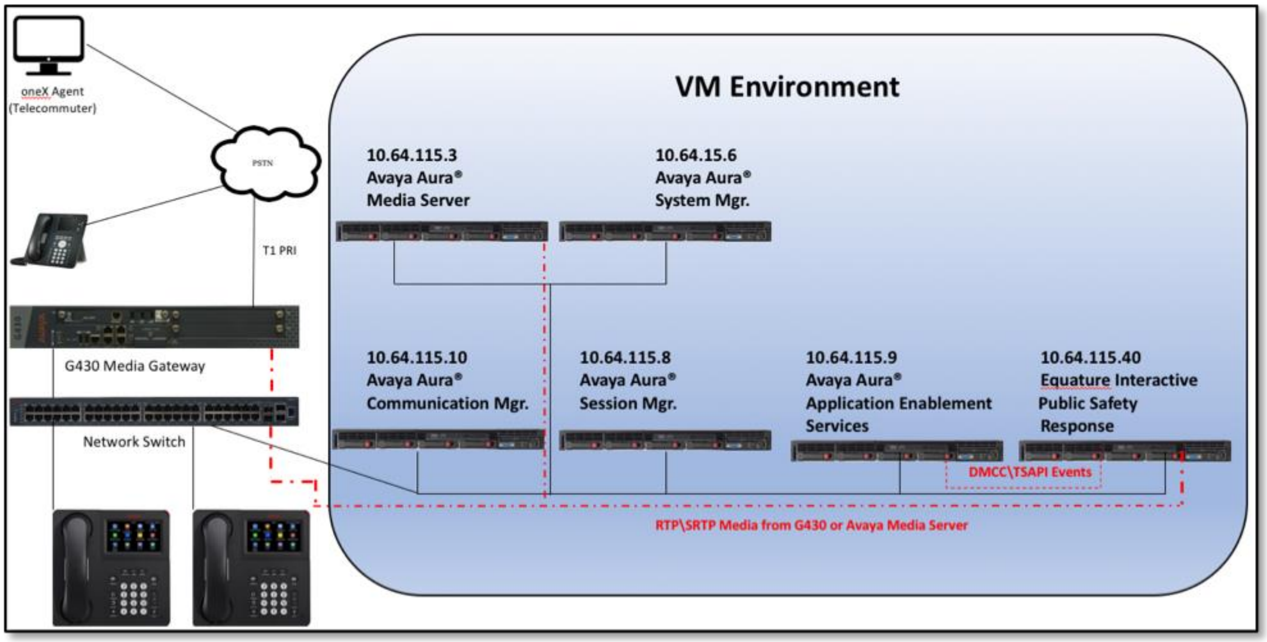


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on VMWare ESXi 6.0	R7.1.2 (Feature Pack 2) (7.1.2.0.0.532.0-24184)
Avaya Aura® Application Enablement Services running on VMWare ESXi 6.0	R7.1.1 (7.1.1.0.0.5-0)
Avaya G430 Media Gateway	38.20.1/1
Avaya Aura® Media Server running on VMWare ESXi 6.0	7.8.0.333
Avaya 6408D Digital Station	N/A
Avaya 9670G	3.280A (H.323)
Avaya 9641G	7.1.1.09 (SIP)
Avaya 9611G	6.6506 (H.323)
Avaya 9630G	2.6.17 (SIP)
Avaya oneX® Agent	2.5.60129.0 (H.323)
Equature Interactive Public Safety Response on Microsoft Windows 10 Pro (running on VMWare) Avaya DMCC XML	1.74 v.1709 ESXi 6.0 6.3.3.14

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
- 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**.

The test environment consisted of a mix of phones. PRI trunks connect the test systems to the PSTN enabling calls with external devices. These Application Notes do not cover the full environment as much of that is standard implementation. Rather, these notes focus on the parts that impact the integration with the tested application.

Recording can be performed via DMCC using one of three methods, depending on the target station types. Understanding this will help with perspective in this document. Bold indicates the methods used in the tested solution.

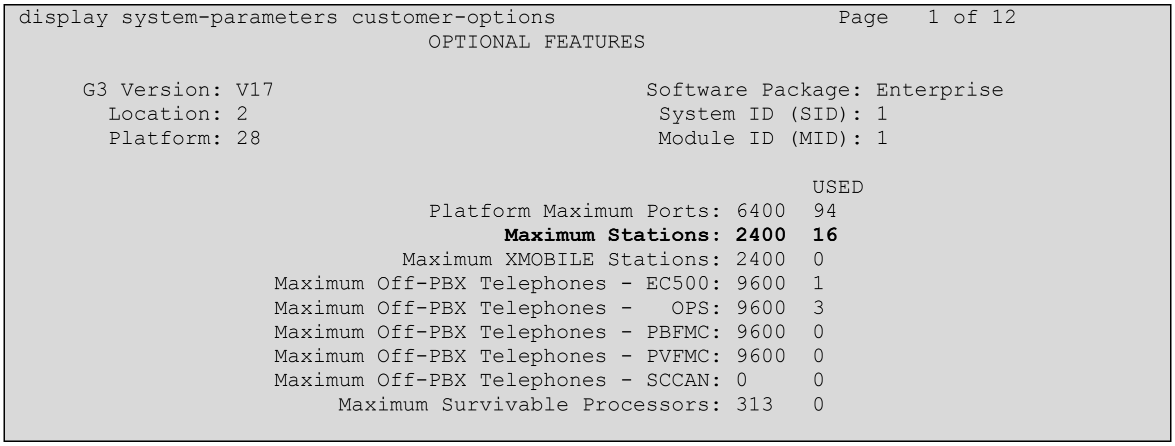
Target Endpoint Type	**Multi-Registration**	**Service Observe**	**Single Step Conference**
SIP	No	Yes	**Yes**
SIP Dual-Reg	Yes (Independent Mode)	Yes	**Yes**
H.323	**Yes (Dependent Mode)**	Yes	Yes
Digital	**Yes (Dependent Mode)**	Yes	Yes
Analog	N/A	Yes	Yes

The Equature application uses Dependent Mode (Multiple Registration) to record Digital and H.323 endpoints, and Single Step conference virtual extensions using Main mode to record any target that fails to register using Multiple Registration.

5.1. Verify Feature and License for the integration

For recording solutions, the following license are required on Communication Manager:

- Recorders that use Single Step Conference or Service Observation (ie. Registering using the MAIN option), will use a virtual extension to join the recorder to calls. Each recording port using these methods will consume a **Station** license when administered.



```
display system-parameters customer-options                      Page   1 of 12
                                OPTIONAL FEATURES

     G3 Version: V17                              Software Package: Enterprise
       Location: 2                                 System ID (SID): 1
       Platform: 28                                Module ID (MID): 1

                                                              USED
                                Platform Maximum Ports: 6400  94
                                      Maximum Stations: 2400  16
                              Maximum XMOBILE Stations: 2400  0
                    Maximum Off-PBX Telephones - EC500: 9600  1
                    Maximum Off-PBX Telephones -   OPS: 9600  3
                    Maximum Off-PBX Telephones - PBFMC: 9600  0
                    Maximum Off-PBX Telephones - PVFMC: 9600  0
                    Maximum Off-PBX Telephones - SCCAN: 0     0
                         Maximum Survivable Processors: 313   0
```

- Recorders using the Multiple Registration (ie. Registering using the DEPENDENT or INDEPENDENT option) do not require additional station license. All methods will consume a **Concurrently Registered IP Station** license:

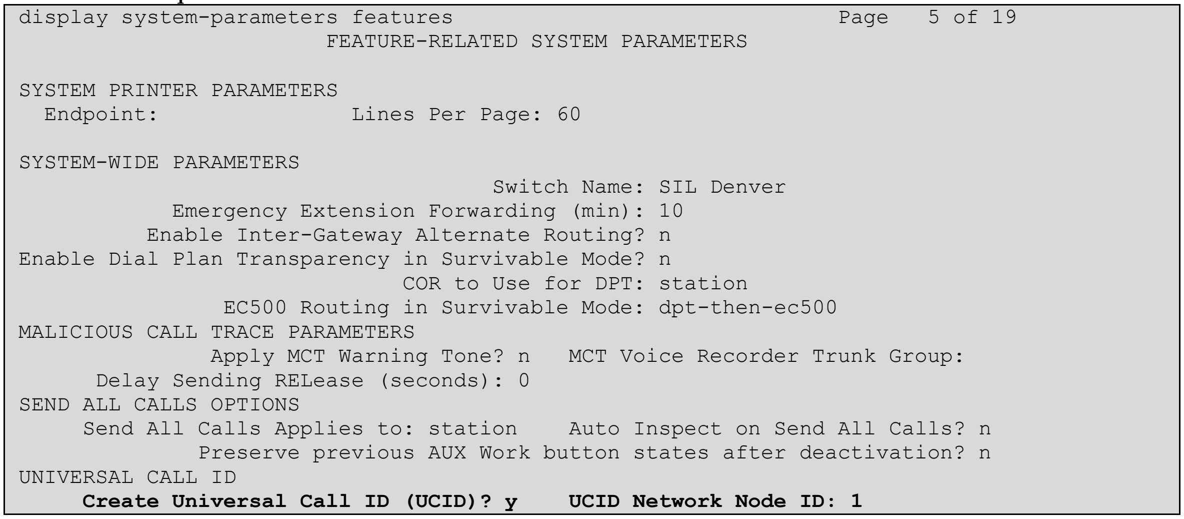
```
display system-parameters customer-options                      Page   2 of 12
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 4000  0
           Maximum Concurrently Registered IP Stations: 2400  11
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  0
                   Maximum Video Capable IP Softphones: 2400  0
                       Maximum Administered SIP Trunks: 4000  55
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
```

- In previous versions of Communication Manager, the IP_API_A (DMCC) may have been enforced on Communication Manager, and\or Application Enablement. With version 7 of Communication Manager, this RTU is completely controlled by Application Enablement Services (DMCC_DMC).
- Customers who purchase Application Enablement license will have ASAI capabilities enabled on the Communication Manager. These include **ASAI Link Core Capabilities** and\or **Computer Telephony Adjunct Links** (enabled when TSAPI Basic RTU are purchased):

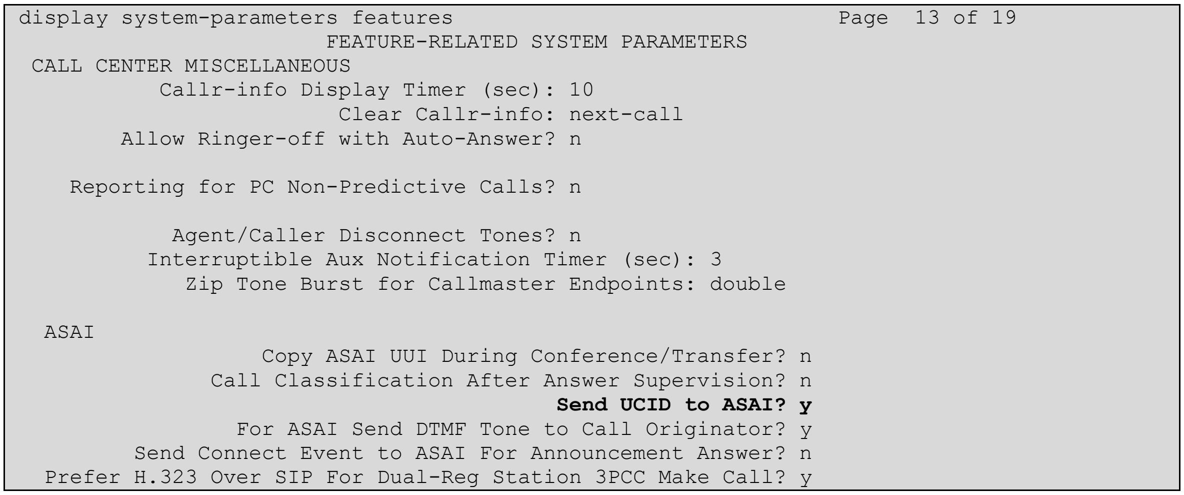
```
display system-parameters customer-options                      Page   4 of 12
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? y              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? y                DCS Call Coverage? y
          ASAI Link Plus Capabilities? y               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
```

5.2. Administer Communication Manager System Features

If UCID is desired, make the following changes using an appropriate Node ID based on the customer requirements.



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

SYSTEM PRINTER PARAMETERS
  Endpoint:               Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                                     Switch Name: SIL Denver
            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
```



```
display 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? y
```

5.3. Administer IP Services for Application Enablement Services

Use the **change ip-services** command to Enable IP-Services for Application Enablement Services:

```
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, add the **hostname** for the Application Enablement Services server, and a **password** that will be entered in the AES setup in the next section.

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

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

5.4. Administer Computer Telephony Integration (CTI) Link

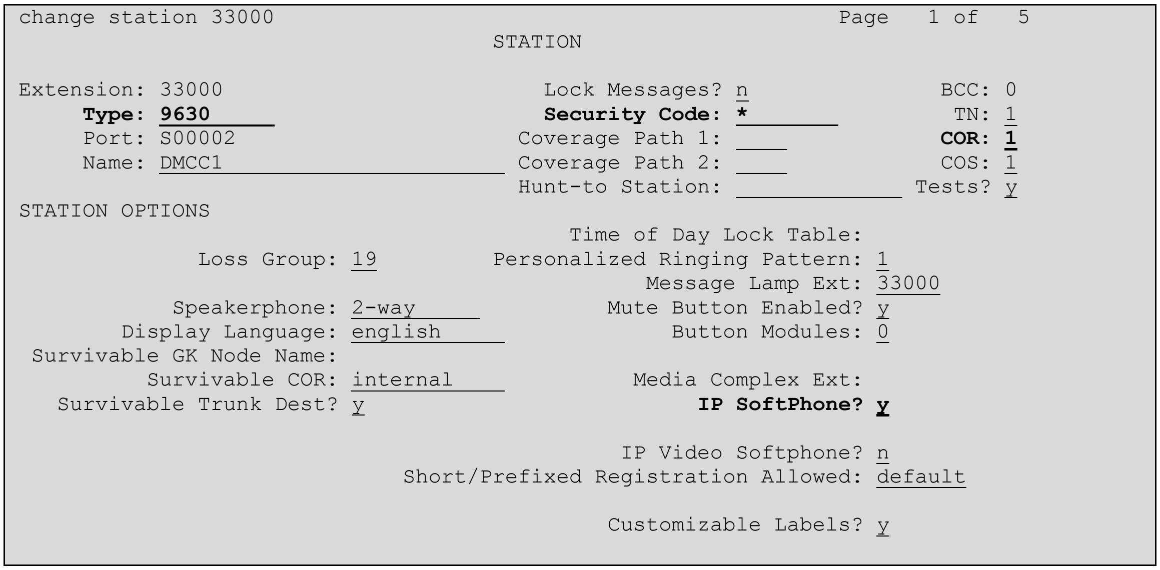
Add a CTI-Link with **ADJ-IP** link Type, the name is not critical:

```
add cti-link 1                                                  Page   1 of   3
                                           CTI LINK
 CTI Link: 1
Extension: 30000
     Type: ADJ-IP
                                                                        COR: 1
     Name: SILDVAES
```

5.5. Verify Recorded Extensions & Add Virtual Stations

For recording solutions using MAIN registration type (Single Step Conference or Service Observe), virtual extensions are administered for each recording port. In this test environment, stations 33000 – 33009 were previously built as:

- **Type** = 9630
- **Security Code** = eg: 123456 (this will be required when setting up the recorder)
- **IP Softphone** = y
- **COR** = 1 (note, only relevant for Service Observe methods)



```
change station 33000                                            Page   1 of   5
                                     STATION

Extension: 33000                         Lock Messages? n               BCC: 0
     Type: 9630                          Security Code: *                TN: 1
     Port: S00002                      Coverage Path 1:                 COR: 1
     Name: DMCC1                       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: 33000
            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
```

- All other settings may be left at defaults.

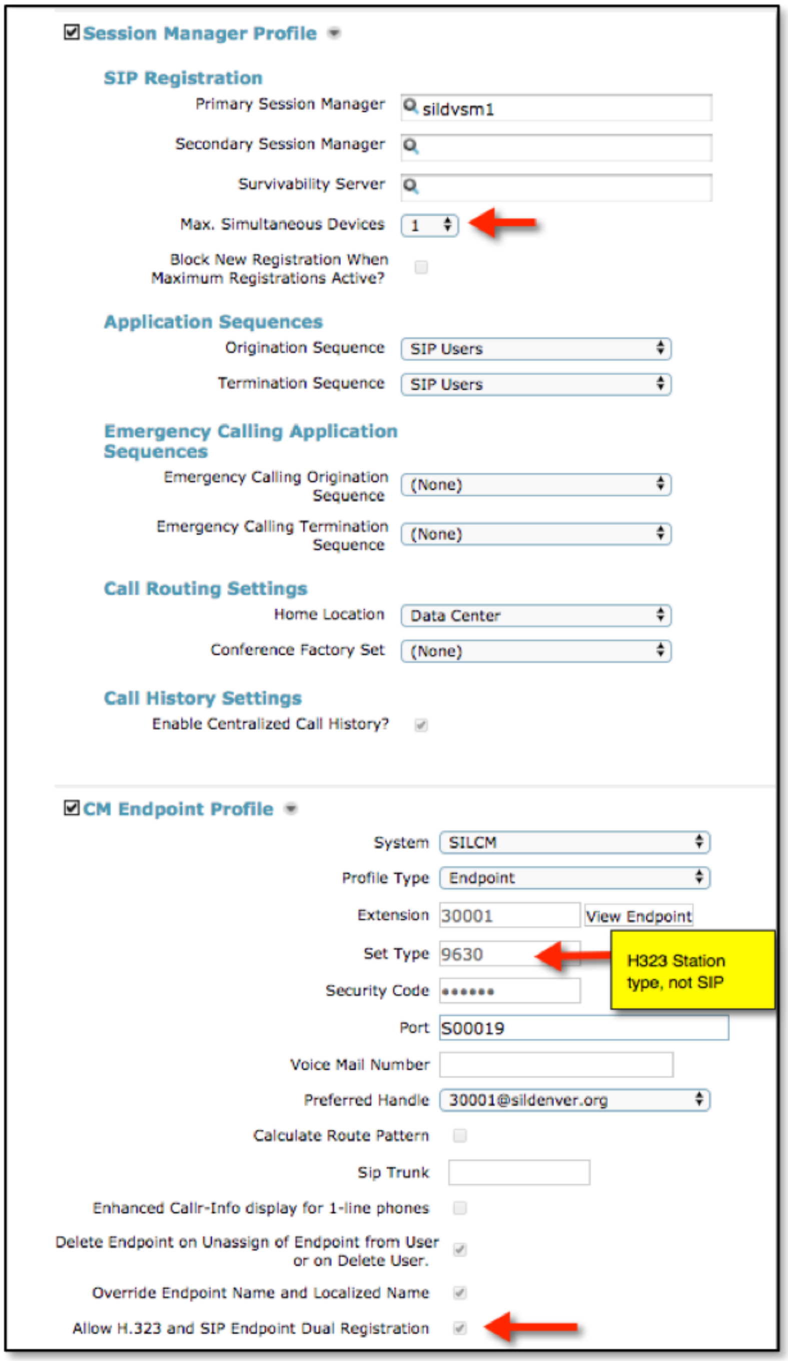
For Multiple Registration methods, the agent extensions must be administered as follows:

- **Security Code** = eg: 123456 (this will be required when setting up the recorder)
- **IP Softphone** = y

Agent Stations that will be recorded using Service Observation or Single Step Conference do not need IP Softphone enabled.

For SIP endpoints to be able to be recorded using Multiple Registration, the SIP user profile must be associated with an H.323 station (Dual-Registration). Else, SIP endpoints can be recorded using Service Observe or Single Step Conference.

The relevant settings in the System Manager User Profile for a Dual-Registration user are shown below:



☑ **Session Manager Profile**

SIP Registration

Primary Session Manager	sildvsm1
Secondary Session Manager	
Survivability Server	
Max. Simultaneous Devices	1
Block New Registration When Maximum Registrations Active?	□

Application Sequences

Origination Sequence	SIP Users
Termination Sequence	SIP Users

Emergency Calling Application Sequences

Emergency Calling Origination Sequence	(None)
Emergency Calling Termination Sequence	(None)

Call Routing Settings

Home Location	Data Center
Conference Factory Set	(None)

Call History Settings

Enable Centralized Call History?	☑

☑ **CM Endpoint Profile**

System	SILCM
Profile Type	Endpoint
Extension	30001
Set Type	9630
Security Code	••••••
Port	S00019
Voice Mail Number	
Preferred Handle	30001@sildenver.org
Calculate Route Pattern	□
Sip Trunk	
Enhanced Callr-Info display for 1-line phones	□
Delete Endpoint on Unassign of Endpoint from User or on Delete User.	☑
Override Endpoint Name and Localized Name	☑
Allow H.323 and SIP Endpoint Dual Registration	☑

H323 Station type, not SIP

Additionally, the station mapping must be manually entered to enable the SIP device to receive the media for calls to that station:

```
change off-pbx-telephone station-mapping 30001                 Page   1 of   3
                   STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                     Selection   Set     Mode
 30001            OPS          -      30001            aar        1
```

Equature does not currently use this method, but anticipates using the option at some point, so it is described here for future reference.

Call Center and routing administration tasks in Communication Manager were minimal, and not covered in these notes.

To ensure the recorder received media matching its requirements, the IP Address of the Application Enablement Services server was associated with network-region 2, which used ip-codec-set 2 as shown below. Shuffling (IP-IP Direct Audio) was disabled for this network region.

```
display ip-network-map                                          Page   1 of  63
                               IP ADDRESS MAPPING

                                                Subnet Network     Emergency
 IP Address                                     Bits   Region VLAN Location Ext
 ---------------------------------------------- ------ ------ ---- -------------
 FROM: 10.64.115.9                              /      2      n
   TO: 10.64.115.9
 FROM: 10.64.115.33                             /      1      n
   TO: 10.64.115.255
```

```
change ip-network-region 2                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 2       NR Group: 2
Location: 1       Authoritative Domain: sildenver.org
    Name: recorder             Stub Network Region: n
MEDIA PARAMETERS               Intra-region IP-IP Direct Audio: no
      Codec Set: 2             Inter-region IP-IP Direct Audio: no
   UDP Port Min: 2048                     IP Audio Hairpinning? n
   UDP Port Max: 3329
```

```
change ip-codec-set 2                                           Page   1 of   2

                          IP MEDIA PARAMETERS
    Codec Set: 2

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU          n          2        20
 2:

     Media Encryption                  Encrypted SRTCP: enforce-unenc-srtcp
 1: 1-srtp-aescm128-hmac80
 2: aes
 3: none
```

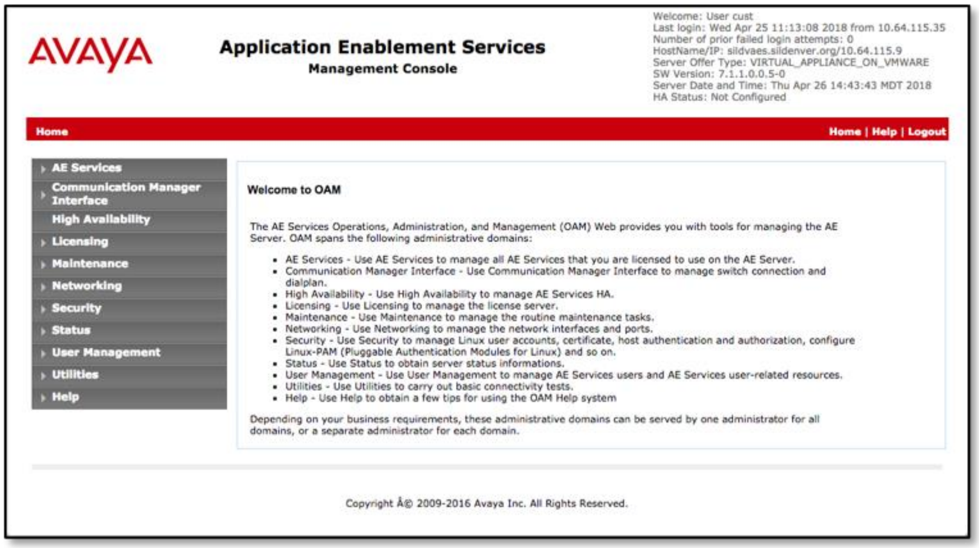
6. Configure Avaya Aura® Application Enablement Services

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.

All connections were secure, meaning the rootCA from System Manager was installed on Communication Manager, Application Enablement Services, and the Equature server. Identity certificates were generated in System Manager for the Avaya Aura components. By installing the rootCA on the Equature server, secure DMCC links and SRTP were possible using a Shared Key methodology. For more secure needs, a Mutual Authentication methodology is supported but was not tested.

The procedures fall into the following areas:

- Configure Communication Manager Switch Connections
- Add TSAPI Links
- Note the TLink Information
- Configure a CTI User for Equature
- Enable Unrestricted Access for the Equature User
- Confirm TSAPI and DMCC Licenses
- Restart TSAPI Service



Welcome: User cust
Last login: Wed Apr 25 11:13:08 2018 from 10.64.115.35
Number of prior failed login attempts: 0
HostName/IP: sildvaes.sildenver.org/10.64.115.9
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Thu Apr 26 14:43:43 MDT 2018
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:

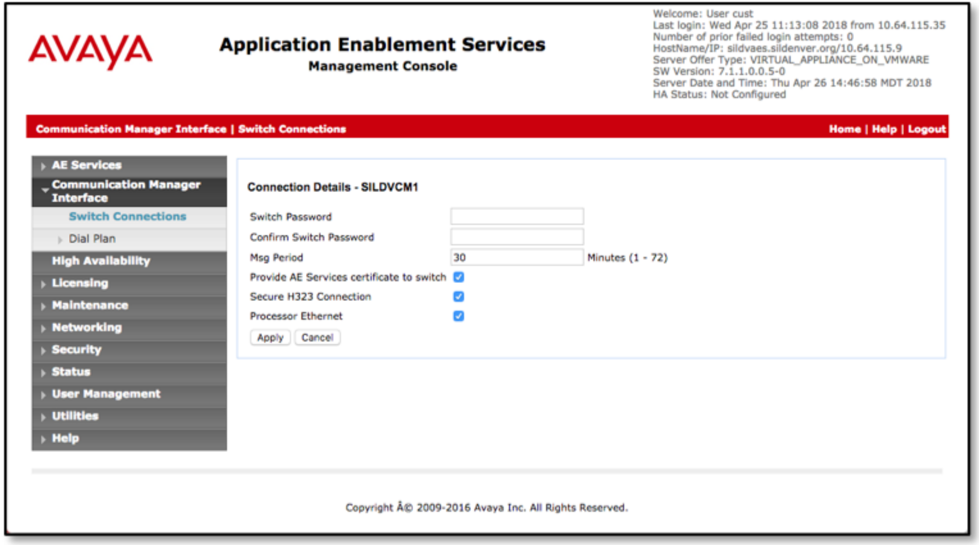
- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - 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

Navigate to the **Communication Manager Interface** > **Switch Connections** page and enter a name for the new switch connection (e.g. **SILDVCM1**) and click the **Add Connection** button (not shown). The **Connection Details** screen is shown. Enter the **Switch Password** configured in **Section 5, Step 3** and check the **Secure H323 Connection** and **Processor Ethernet** box if using the **procr** interface. Click **Apply**.



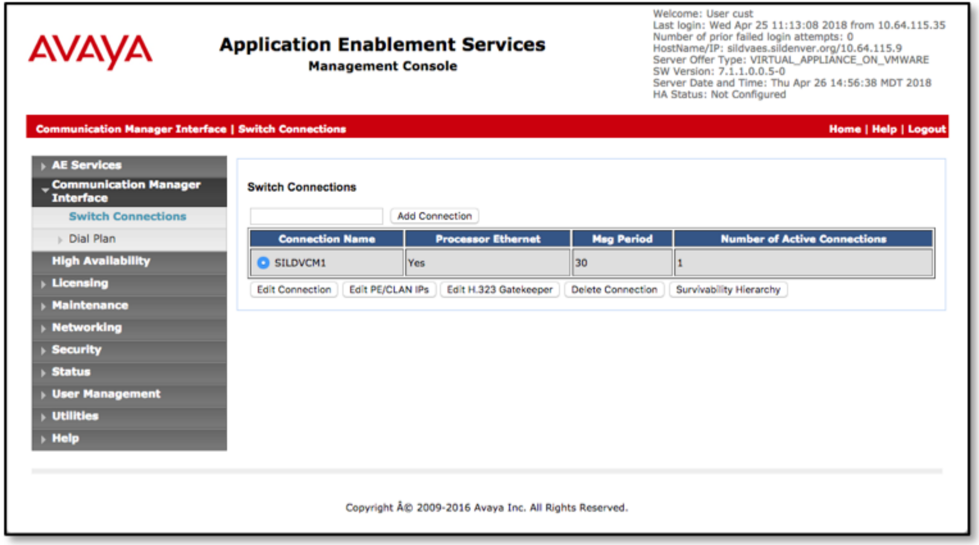
Welcome: User cust
Last login: Wed Apr 25 11:13:08 2018 from 10.64.115.35
Number of prior failed login attempts: 0
HostName/IP: sildvaes.sildenver.org/10.64.115.9
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Thu Apr 26 14:46:58 MDT 2018
HA Status: Not Configured

Connection Details - SILDVCM1

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

Copyright Â© 2009-2016 Avaya Inc. All Rights Reserved.

Once applied, the **Switch Connections** list will confirm the addition of the connection.



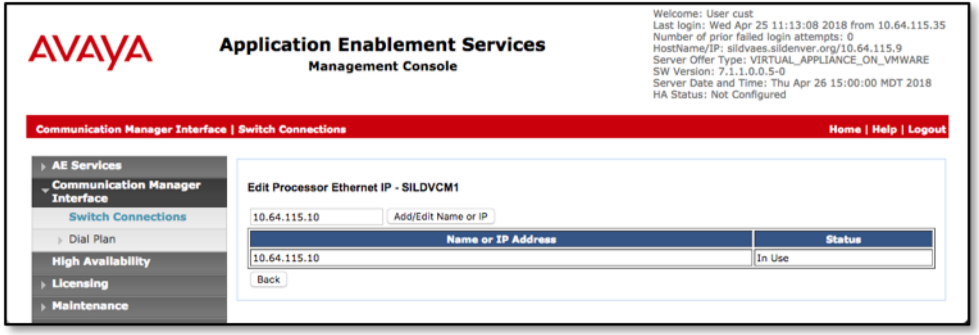
Welcome: User cust
Last login: Wed Apr 25 11:13:08 2018 from 10.64.115.35
Number of prior failed login attempts: 0
HostName/IP: sildvaes.sildenver.org/10.64.115.9
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Thu Apr 26 14:56:38 MDT 2018
HA Status: Not Configured

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● SILDVCM1	Yes	30	1

Copyright Â© 2009-2016 Avaya Inc. All Rights Reserved.

Click on the **Edit PE/CLAN IPs** button and enter the IP Address for the PROCR of Communication Manager:



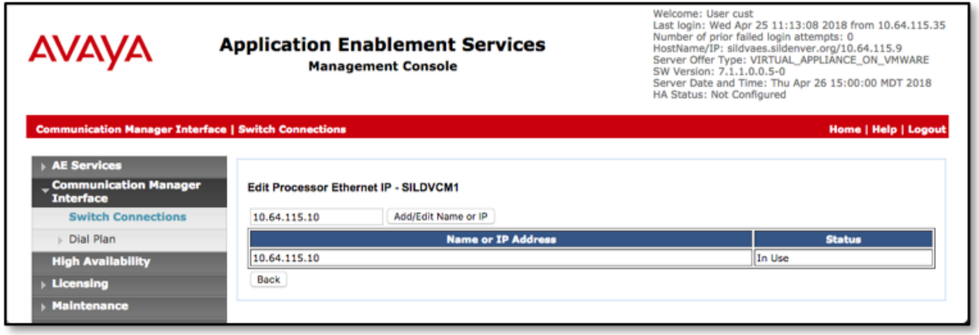
Welcome: User cust
Last login: Wed Apr 25 11:13:08 2018 from 10.64.115.35
Number of prior failed login attempts: 0
HostName/IP: sildvaes.sildenver.org/10.64.115.9
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Thu Apr 26 15:00:00 MDT 2018
HA Status: Not Configured

Edit Processor Ethernet IP - SILDVCM1

10.64.115.10

Name or IP Address	Status
10.64.115.10	In Use

Repeat for the **Edit H.323 Gatekeeper**:



Welcome: User cust
Last login: Wed Apr 25 11:13:08 2018 from 10.64.115.35
Number of prior failed login attempts: 0
HostName/IP: sildvaes.sildenver.org/10.64.115.9
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Thu Apr 26 15:00:00 MDT 2018
HA Status: Not Configured

Edit Processor Ethernet IP - SILDVCM1

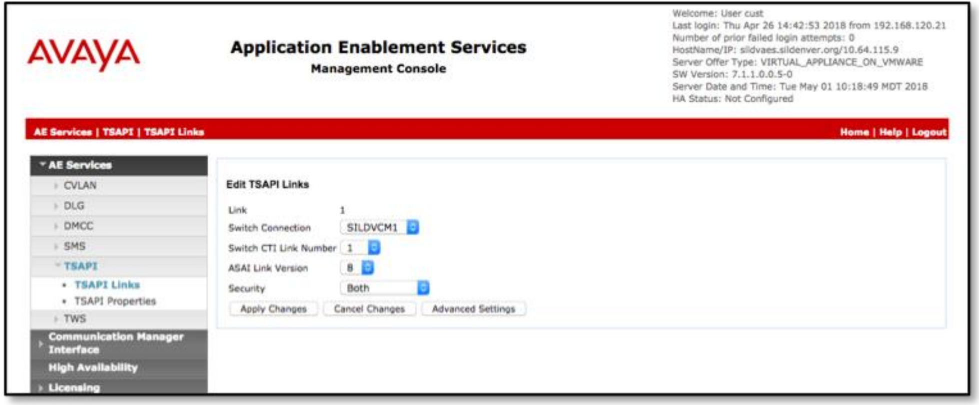
10.64.115.10

Name or IP Address	Status
10.64.115.10	In Use

6.2. Configure TSAPI Links

Navigate to **AE Services** > **TSAPI** > **TSAPI Links** and click **Add Link** (not shown).

Select the **Switch Connection** created in **6.1** in the drop-down menu (SILDVCM1), choose the **Switch CTI Link Number** that matches the link created in **Section 5.4** above. Choose an **ASAI Link Version**, 8 is generally recommended. For **Security**, choose either **Both** or **Encrypted**. Both will permit applications not capable of using secure streams to connect, while Encrypted will forces all applications to use Encrypted steams. Click **Apply Changes**.

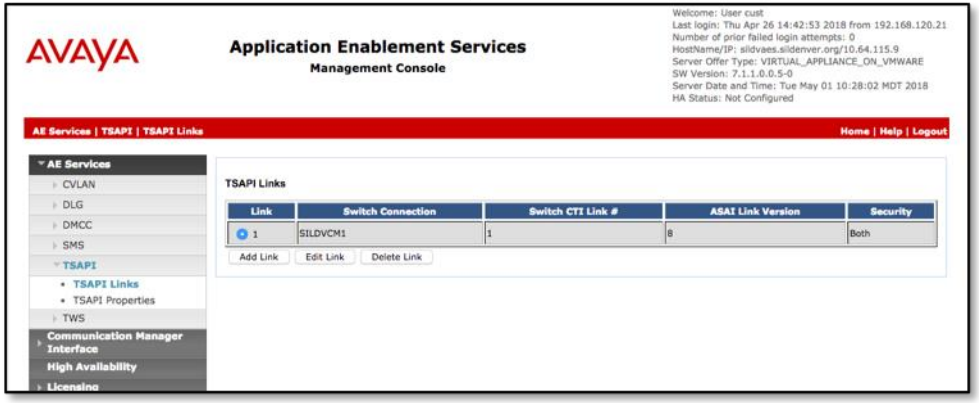


Welcome: User cust
Last login: Thu Apr 26 14:42:53 2018 from 192.168.120.21
Number of prior failed login attempts: 0
HostName/IP: sildvaes.sildenver.org/10.64.115.9
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue May 01 10:18:49 MDT 2018
HA Status: Not Configured

Edit TSAPI Links

Link	1
Switch Connection	SILDVCM1
Switch CTI Link Number	1
ASAI Link Version	8
Security	Both

This returns to the **TSAPI Links** pages which will confirm the new CTI Link:



Welcome: User cust
Last login: Thu Apr 26 14:42:53 2018 from 192.168.120.21
Number of prior failed login attempts: 0
HostName/IP: sildvaes.sildenver.org/10.64.115.9
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue May 01 10:28:02 MDT 2018
HA Status: Not Configured

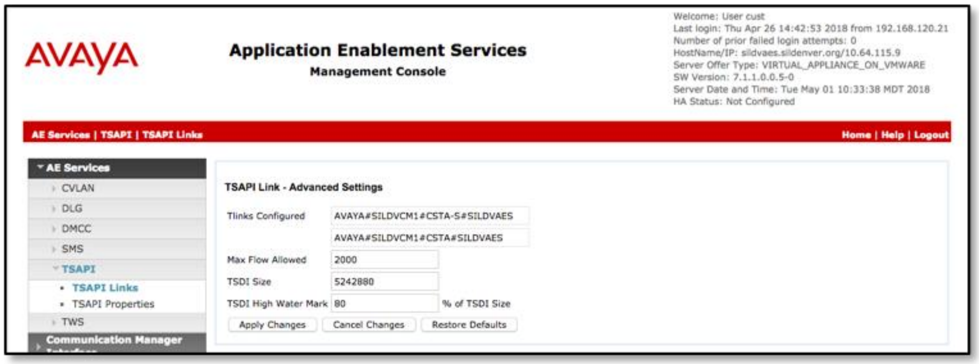
TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
● 1	SILDVCM1	1	8	Both

6.3. Note the TLink Information

From the **TSAPI Links** page, click **Edit Link**, then **Advanced Settings** (not shown) and take note of the Tlinks Configured.

If **Both** was selected for Security in **6.2** above, two Tlinks will appear with the format AVAYA#SwitchLinkName#CSTA#AESHostName. The link with CSTA-S is the secure link that will be used when configuring the Equature application in **Section 7**.



Welcome: User cust
Last login: Thu Apr 26 14:42:53 2018 from 192.168.120.21
Number of prior failed login attempts: 0
HostName/IP: sildvaes.sildenver.org/10.64.115.9
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue May 01 10:33:38 MDT 2018
HA Status: Not Configured

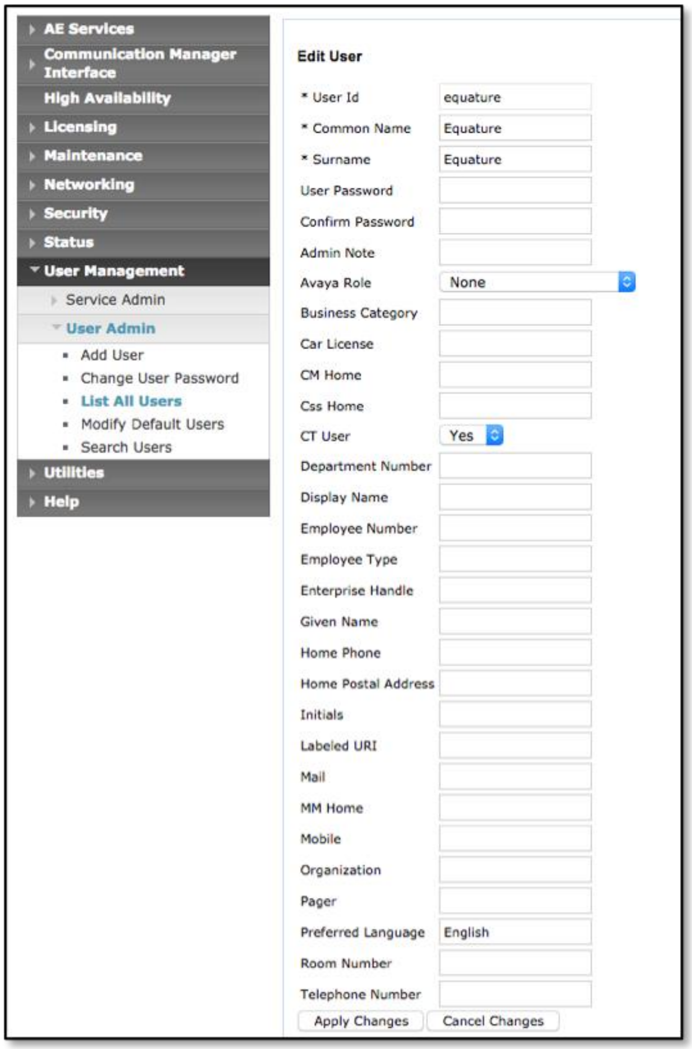
TSAPI Link - Advanced Settings

Tlinks Configured	AVAYA#SILDVCM1#CSTA-S#SILDVAES AVAYA#SILDVCM1#CSTA#SILDVAES
Max Flow Allowed	2000
TSDI Size	5242880
TSDI High Water Mark	80 % of TSDI Size

6.4. Configure a CTI User for Equature

Navigate to **User Management > User Admin > Add User**. Enter an appropriate **User Id, Common Name, Surname,** and **User Password**. Select **Yes** from the **CT User** dropdown list.

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



Edit User

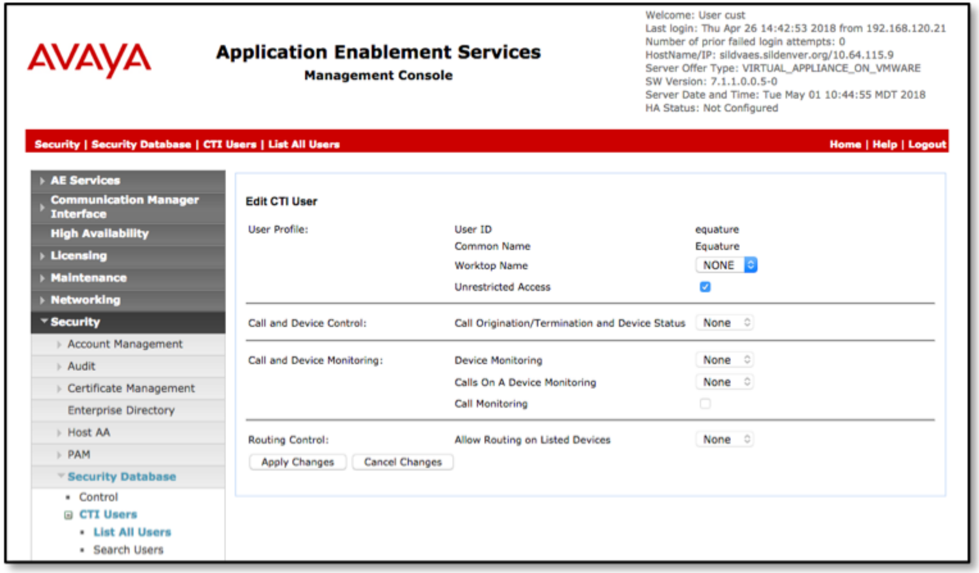
* User Id	equature
* Common Name	Equature
* Surname	Equature
User Password	
Confirm Password	
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	
Enterprise Handle	
Given Name	
Home Phone	
Home Postal Address	
Initials	
Labeled URI	
Mail	
MM Home	
Mobile	
Organization	
Pager	
Preferred Language	English
Room Number	
Telephone Number	

6.5. Enable Unrestricted Access for the Equature User

If the Security Database (SDB) is enabled on Application Enablement Services, set the Equature 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 **Equature** user and click **Edit** (not shown).

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.



Welcome: User cust
Last login: Thu Apr 26 14:42:53 2018 from 192.168.120.21
Number of prior failed login attempts: 0
HostName/IP: sildvaes.sildenver.org/10.64.115.9
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue May 01 10:44:55 MDT 2018
HA Status: Not Configured

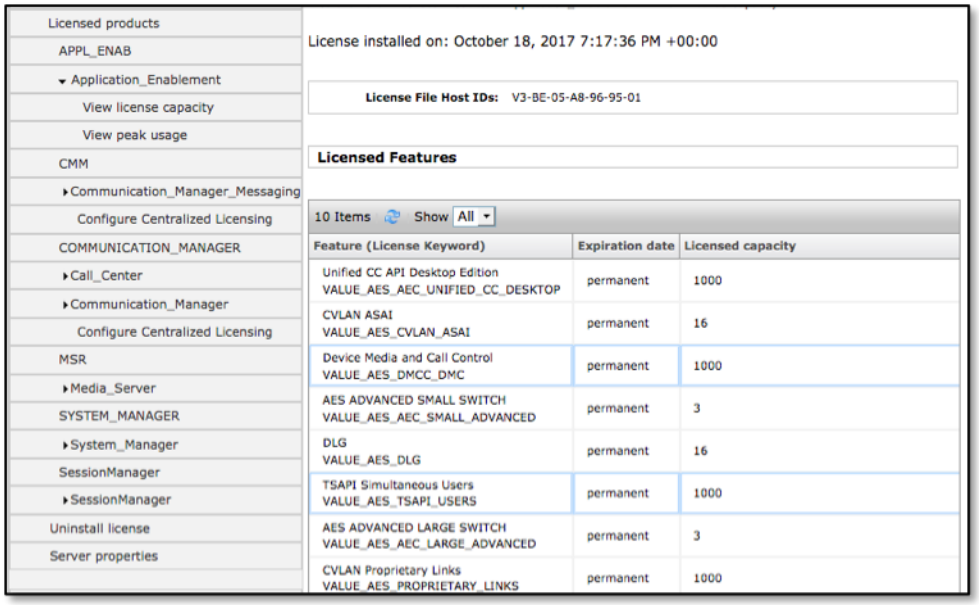
Edit CTI User

User Profile:	User ID	equature
	Common Name	Equature
	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

6.6. Confirm TSAPI and DMCC Licenses

Equature uses a DMCC (**VALUE_AES_DMCC_DMC**) license for each recording port. Additionally, a TSAPI Basic (**VALUE_AES_TSAPI_USERS**) license is used for each agent station being monitored, as well as each hunt group being monitored. Additionally, recorder ports that will use Single Step Conference or Service Observation will require a TSAPI license to add these ports to calls.

With version 7 and later, WebLM is typically installed and configured on Avaya Aura® System Manager. 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 enough **VALUE_AES_DMCC_DMC** and **VALUE_AES_TSAPI_USERS** licenses are available.



License installed on: October 18, 2017 7:17:36 PM +00:00

License File Host IDs: V3-BE-05-A8-96-95-01

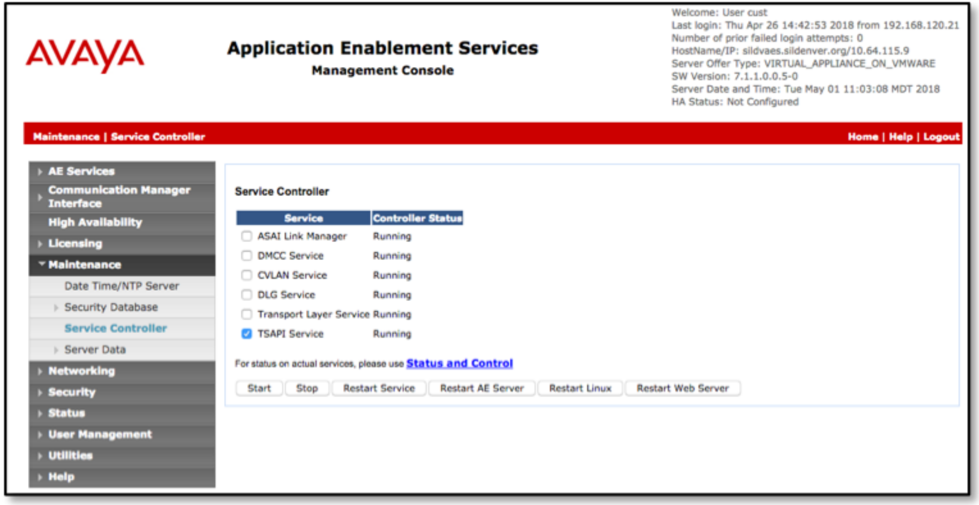
Licensed Features

10 Items Show All

Feature (License Keyword)	Expiration date	Licensed capacity
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	3
DLG VALUE_AES_DLG	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	3
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	1000

6.7. Restart TSAPI Service

Select **Maintenance → Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check the **TSAPI Service** and click **Restart Service**.



Welcome: User cust
Last login: Thu Apr 26 14:42:53 2018 from 192.168.120.21
Number of prior failed login attempts: 0
HostName/IP: sildvaes.sildenver.org/10.64.115.9
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue May 01 11:03:08 MDT 2018
HA Status: Not Configured

Service Controller

Service	Controller Status
☐ ASAI Link Manager	Running
☐ DMCC Service	Running
☐ CVLAN Service	Running
☐ DLG Service	Running
☐ Transport Layer Service	Running
☑ TSAPI Service	Running

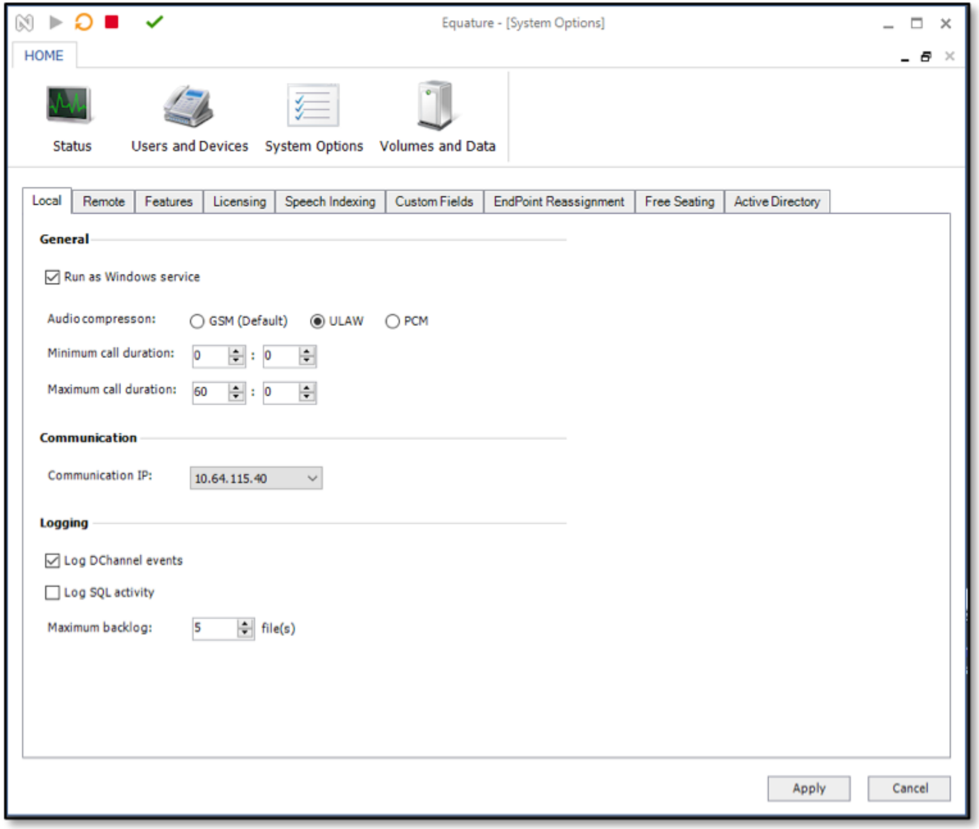
For status on actual services, please use **Status and Control**

7. Configure Equature Interactive Public Safety Response

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

Configuration is performed using the Equature application on the recording server.

On the **Local** tab, set the application to run as a service and set media properties. Also assign the local IP Address for the recorder to receive media on if there are multiple NICs on the server:



General

☑ Run as Windows service

Audio compresson: ○ GSM (Default) ● ULAW ○ PCM

Minimum call duration: 0 : 0

Maximum call duration: 60 : 0

Communication

Communication IP: 10.64.115.40

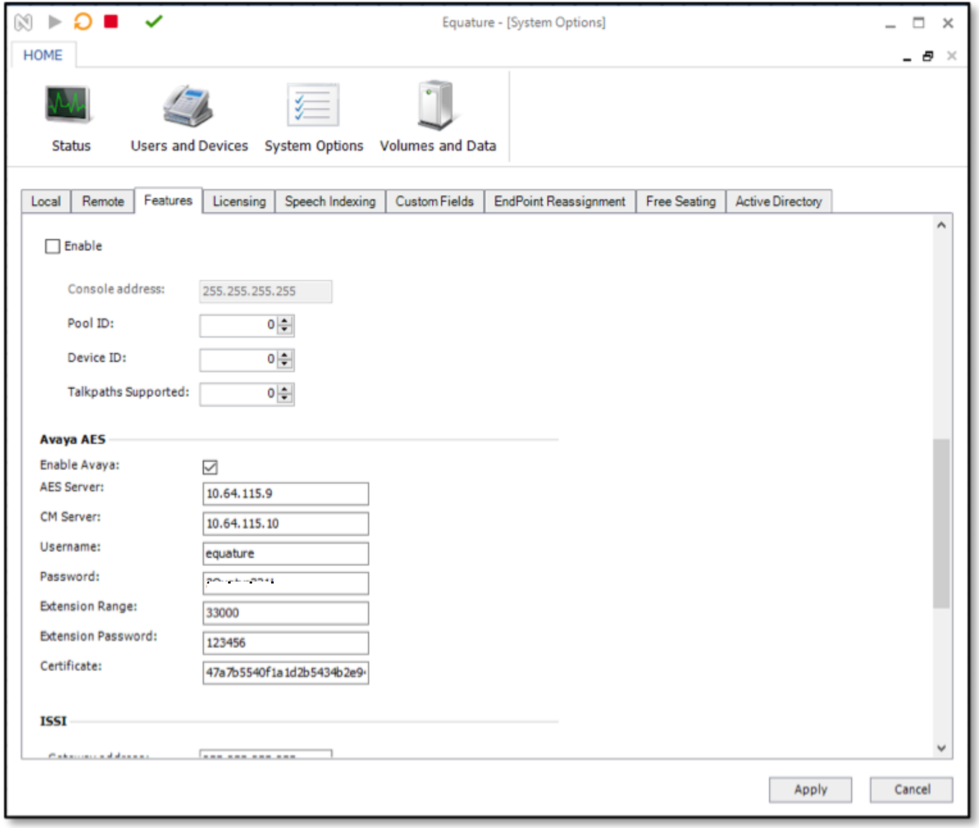
Logging

☑ Log DChannel events

□ Log SQL activity

Maximum backlog: 5 file(s)

On the **Features** tab, set Application Enablement Services connection properties and enter the root certificate signature:



□ Enable

Console address: 255.255.255.255

Pool ID: 0

Device ID: 0

Talkpaths Supported: 0

Avaya AES

Enable Avaya: ☑

AES Server: 10.64.115.9

CM Server: 10.64.115.10

Username: equature

Password: [redacted]

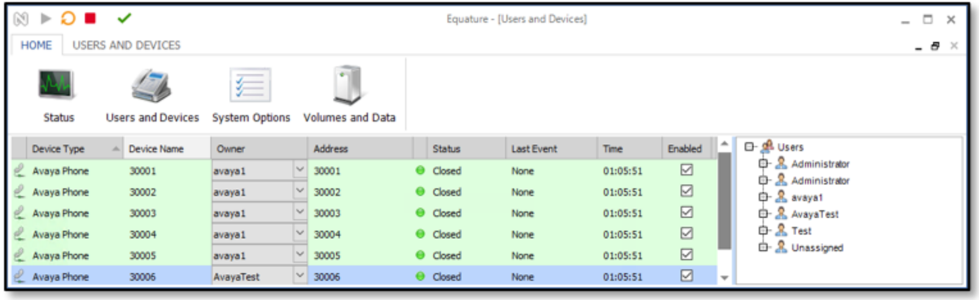
Extension Range: 33000

Extension Password: 123456

Certificate: 47a7b5540f1a1d2b5434b2e9

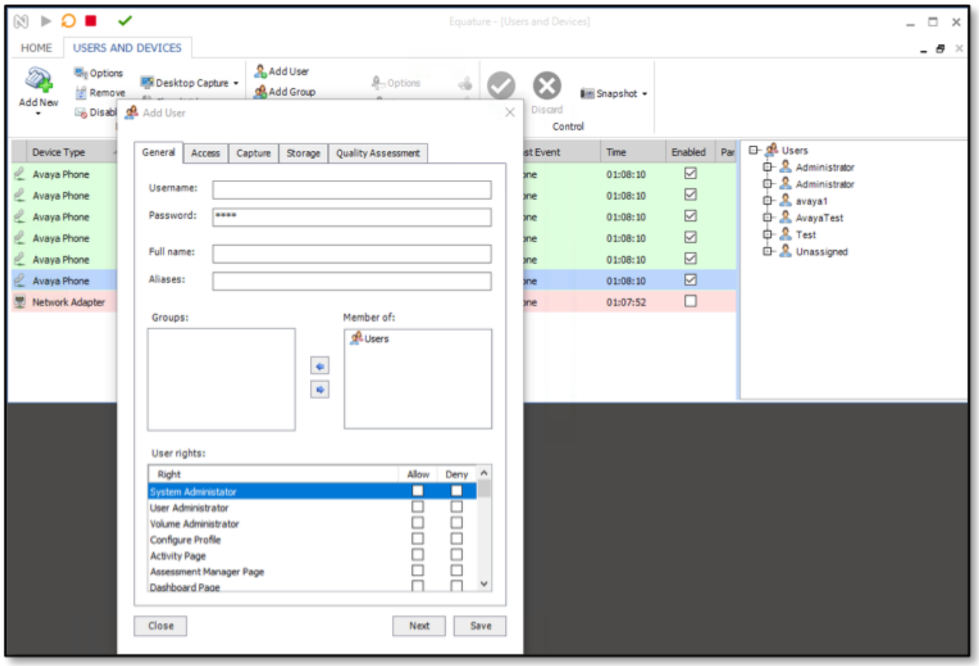
ISSI

Create Devices for each of the target stations to be recorded, and assign ownership:



Device Type	Device Name	Owner	Address	Status	Last Event	Time	Enabled
Avaya Phone	30001	avaya1	30001	● Closed	None	01:05:51	☑
Avaya Phone	30002	avaya1	30002	● Closed	None	01:05:51	☑
Avaya Phone	30003	avaya1	30003	● Closed	None	01:05:51	☑
Avaya Phone	30004	avaya1	30004	● Closed	None	01:05:51	☑
Avaya Phone	30005	avaya1	30005	● Closed	None	01:05:51	☑
Avaya Phone	30006	AvayaTest	30006	● Closed	None	01:05:51	☑

Add users as shown below:



Username:

Password: ****

Full name:

Aliases:

User rights:

Right	Allow	Deny
System Administator	□	□
User Administrator	□	□
Volume Administrator	□	□
Configure Profile	□	□
Activity Page	□	□
Assessment Manager Page	□	□
Dashboard Page	□	□

8. Verification Steps

8.1. Verify Communication Manager Status

From a Communication Manager SAT session, the **list registered-ip-stations** command will show an IP_API_A registration with the Application Enablement server address for Multi-Registration (eg. 30002) and Virtual Extensions (eg. 33001).

```
list registered-ip-stations                                           Page   1

                            REGISTERED IP STATIONS

Station Ext   Set Type/ Prod ID/       Station IP Address/
or Orig Port  Net Rgn   Release    Skt Gatekeeper IP Address
------------- --------- ---------- --- ---------------------------------------
30002         9611      IP_Phone   tls 10.64.115.36
              1         6.6506         10.64.115.10
30004         9650      IP_Phone   tcp 10.64.115.31
              1         3.280A         10.64.115.10
30004         9650      IP_API_A   tls 10.64.115.9
              2         3.2040         10.64.115.10
30005         6408D+    IP_API_A   tls 10.64.115.9
              2         3.2040         10.64.115.10
33000         9630      IP_API_A   tls 10.64.115.9
              2         3.2040         10.64.115.10
33001         9630      IP_API_A   tls 10.64.115.9
              2         3.2040         10.64.115.10
33004         9630      IP_API_A   tls 10.64.115.9
              2         3.2040         10.64.115.10
```

The **list monitored-station** command will show stations with TSAPI monitors. Note that these sessions are established through the DMCC service on Application Enablement:

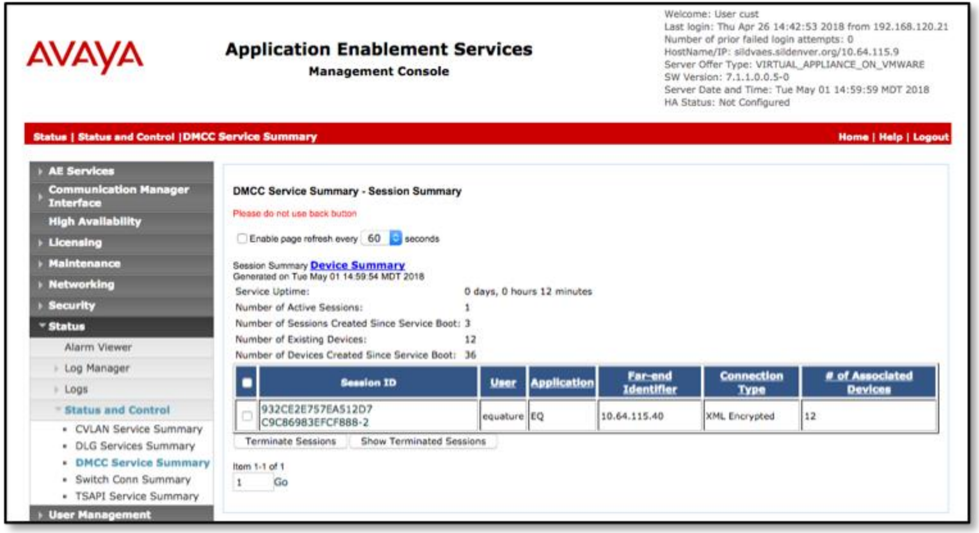
```
list monitored-station

                               MONITORED STATION

   Associations:     1       2       3       4       5       6       7       8
                  CTI     CTI     CTI     CTI     CTI     CTI     CTI     CTI
Station Ext       Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV
----------------- ------- ------- ------- ------- ------- ------- ------- -------
30001             1  0003
30002             1  0008
30003             1  0016
30004             1  0001
30005             1  0002
30006             1  0015
```

With an active call, the **status station** command can demonstrate the media properties of a call being recorded (recorder is 10.64.115.40 with g711u media transcoded while the stations is connected with g729a in the example below):

```
status station 30004                                            Page   8 of  10
                                 SRC PORT TO DEST PORT TALKPATH
src port: S00011
S00011:TX:10.64.115.31:3012/g729a/20ms/1-srtp-aescm128-hmac80
001V012:RX:10.64.115.2:2052/g729/20ms/1-srtp-aescm128-hmac80:TX:ctxID:166
001V011:RX:ctxID:166:TX:10.64.115.2:2054/g711u/20ms
S00002:RX:10.64.115.40:5500/g711u/20ms
```

8.2. Verify Application Enablement Services Status

From Application Enablement Services, the **Status > DMCC Service Summary > Session Summary** will reflect the Secure DMCC session the recorder has established.



Welcome: User cust
Last login: Thu Apr 26 14:42:53 2018 from 192.168.120.21
Number of prior failed login attempts: 0
HostName/IP: sildvaes.sildenver.org/10.64.115.9
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue May 01 14:59:59 MDT 2018
HA Status: Not Configured

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

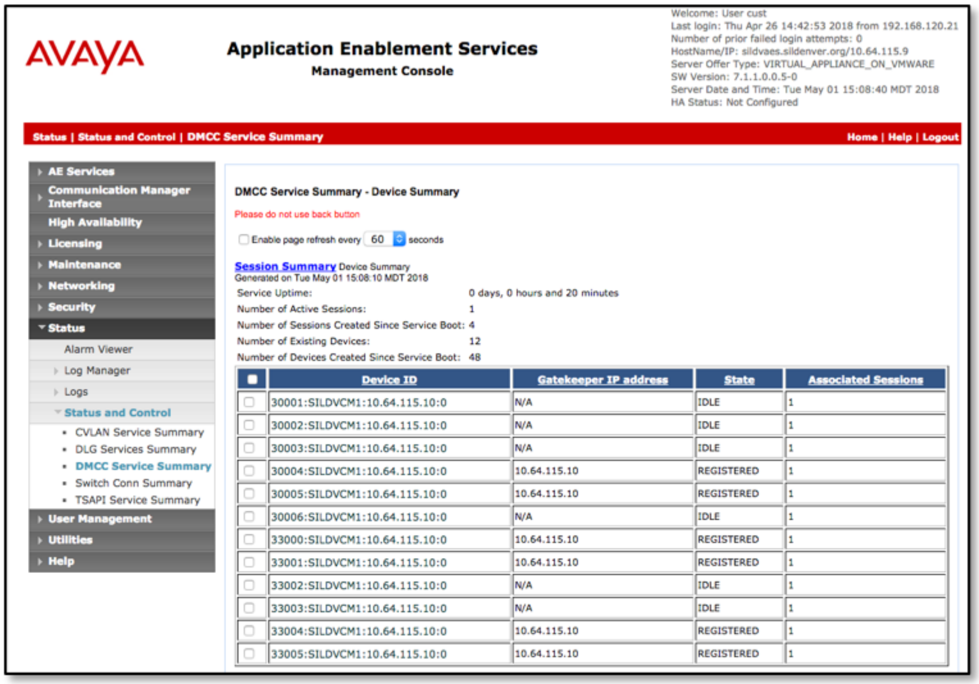
Session Summary Device Summary
Generated on Tue May 01 14:59:54 MDT 2018

Service Uptime:	0 days, 0 hours 12 minutes
Number of Active Sessions:	1
Number of Sessions Created Since Service Boot:	3
Number of Existing Devices:	12
Number of Devices Created Since Service Boot:	36

■	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
☐	932CE2E757EA512D7 C9C86983EFCF888-2	equature	EQ	10.64.115.40	XML Encrypted	12

Item 1-1 of 1
1

The **Status** > **DMCC Service Summary** > **Device Summary** will reflect the registrations that the recorder has established.



Welcome: User cust
Last login: Thu Apr 26 14:42:53 2018 from 192.168.120.21
Number of prior failed login attempts: 0
HostName/IP: sildvaes.sildenver.org/10.64.115.9
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue May 01 15:08:40 MDT 2018
HA Status: Not Configured

DMCC Service Summary - Device Summary

Please do not use back button

□ Enable page refresh every 60 seconds

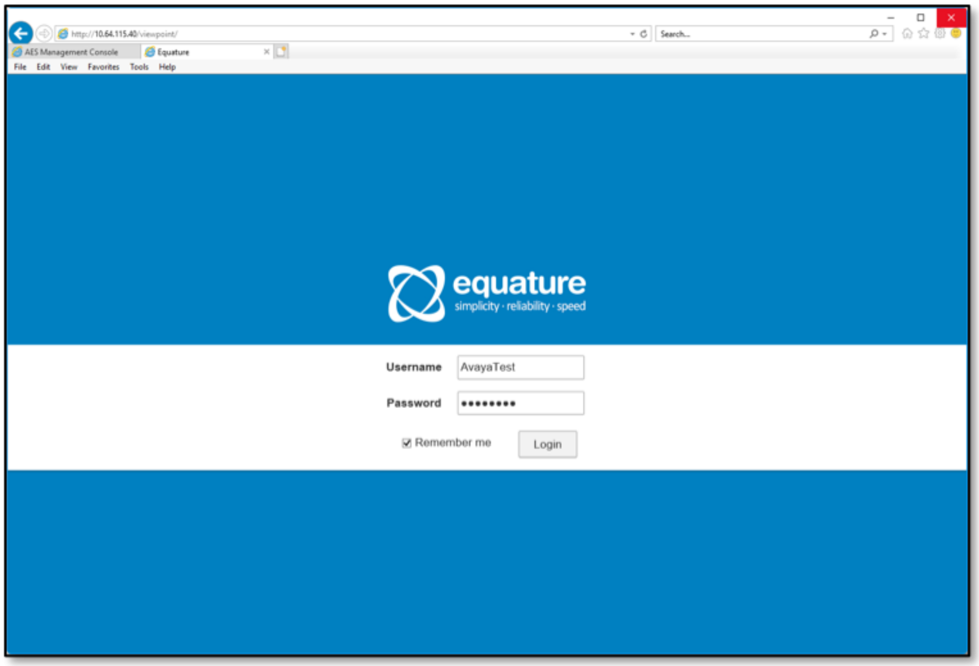
Session Summary Device Summary
Generated on Tue May 01 15:08:10 MDT 2018

Service Uptime:	0 days, 0 hours and 20 minutes
Number of Active Sessions:	1
Number of Sessions Created Since Service Boot:	4
Number of Existing Devices:	12
Number of Devices Created Since Service Boot:	48

■	Device ID	Gatekeeper IP address	State	Associated Sessions
□	30001:SILDVCM1:10.64.115.10:0	N/A	IDLE	1
□	30002:SILDVCM1:10.64.115.10:0	N/A	IDLE	1
□	30003:SILDVCM1:10.64.115.10:0	N/A	IDLE	1
□	30004:SILDVCM1:10.64.115.10:0	10.64.115.10	REGISTERED	1
□	30005:SILDVCM1:10.64.115.10:0	10.64.115.10	REGISTERED	1
□	30006:SILDVCM1:10.64.115.10:0	N/A	IDLE	1
□	33000:SILDVCM1:10.64.115.10:0	10.64.115.10	REGISTERED	1
□	33001:SILDVCM1:10.64.115.10:0	10.64.115.10	REGISTERED	1
□	33002:SILDVCM1:10.64.115.10:0	N/A	IDLE	1
□	33003:SILDVCM1:10.64.115.10:0	N/A	IDLE	1
□	33004:SILDVCM1:10.64.115.10:0	10.64.115.10	REGISTERED	1
□	33005:SILDVCM1:10.64.115.10:0	10.64.115.10	REGISTERED	1

8.3. Verify Recording and Playback

Using a browser, access the Equature user interface at http://[ipaddress or FQDN]/viewpoint.

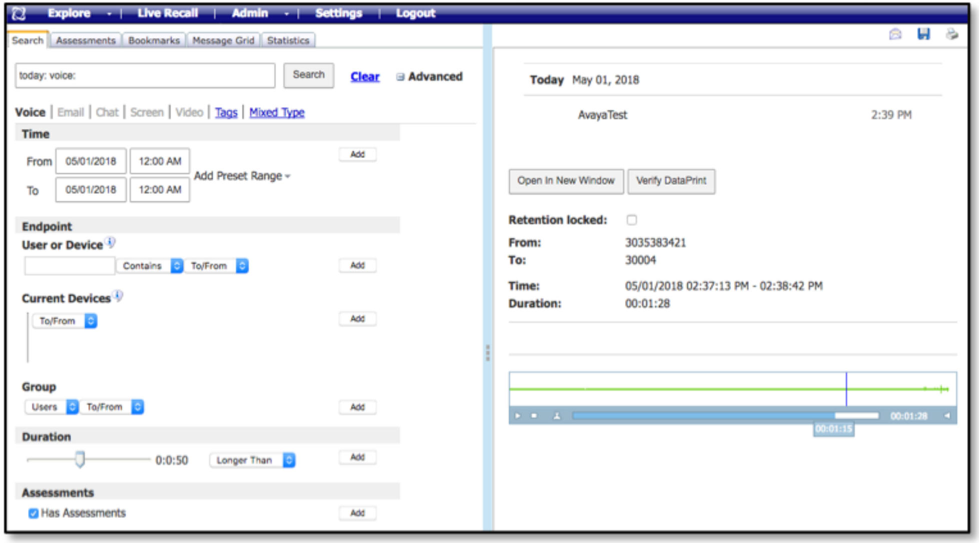

http://10.64.115.40/viewpoint/
Search...
AES Management Console
Equature
File Edit View Favorites Tools Help
equature
simplicity · reliability · speed

Username AvayaTest

Password ••••••••

☑ Remember me

Create a search parameter, such as Today from the Add Preset Range and press search:



today: voice:

Time

From 05/01/2018 12:00 AM

To 05/01/2018 12:00 AM

Endpoint

User or Device Contains To/From

Current Devices To/From

Group Users To/From

Duration 0:0:50 Longer Than

Assessments

☑ Has Assessments

Today May 01, 2018

AvayaTest 2:39 PM

Retention locked: □

From: 3035383421

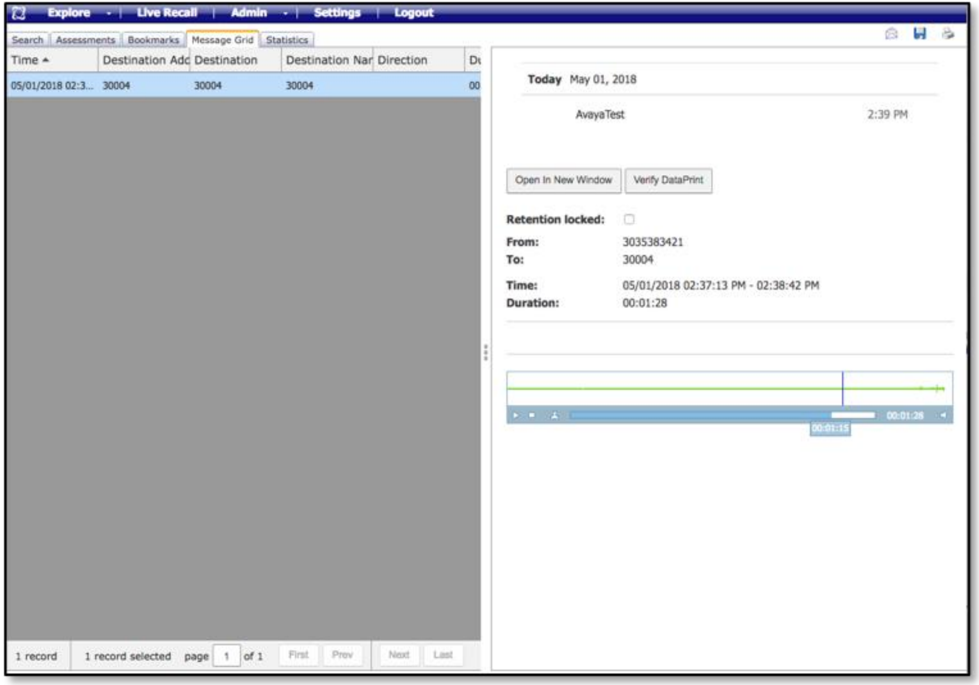
To: 30004

Time: 05/01/2018 02:37:13 PM - 02:38:42 PM

Duration: 00:01:28

00:01:15 00:01:28

Click on a recorded call and verify the audio plays back:



Time ▲	Destination Adc	Destination	Destination Nar	Direction	Du
05/01/2018 02:3...	30004	30004	30004		00

1 record 1 record selected page 1 of 1

Today May 01, 2018

AvayaTest 2:39 PM

Retention locked: □

From: 3035383421

To: 30004

Time: 05/01/2018 02:37:13 PM - 02:38:42 PM

Duration: 00:01:28

00:01:15 00:01:28

9. Conclusion

These Application Notes describe the procedures for configuring Equature Interactive Public Safety Response to monitor and record calls placed to and from agents and phones on Avaya Aura® Communication Manager. In the configuration described in these Application Notes, Equature uses the Device and Media Control Services of Avaya Aura® Application Enablement Services to perform recording. During compliance testing, Equature successfully recorded calls placed to and from agents and stations.

Refer to **Section 2.2** for details regarding secure media limitations.

10. Additional References

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

- *Administering Avaya Aura® Communication Manager*, Release 7.1.1, Issue 2, August 2017
- *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 7.1.1, Issue 3, September 2017
- *Avaya Aura® Application Enablement Services Device, Media and Call Control .NET API Programmers Guide Release 7.1.1*, Issue 1, Document Number 02-602658

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.