Avaya Solution & Interoperability Test Lab

Application Notes for Mobile Heartbeat MH-CURE Dynamic Calling with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the steps required to integrate Mobile Heartbeat MH-CURE Dynamic Calling 20.2 with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1. MH-CURE Dynamic Calling provides to two main features: Dynamic Roles and Privacy/Proxy Numbers. Dynamic Roles allow a user to self-assign a floating role and receive calls for that specific role in addition to their own permanent role. Privacy/Proxy Numbers allow users to hide their personal phone number when they are called from the PSTN. MH-CURE Dynamic Calling integrates with Avaya Aura® Application Enablement Services using the Telephony Server Application Programming Interface (TSAPI) interface.

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

These Application Notes describe the steps required to integrate Mobile Heartbeat MH-CURE Dynamic Calling 20.2 with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1. MH-CURE Dynamic Calling provides to two main features: Dynamic Roles and Privacy/Proxy Numbers. Dynamic Roles allow a user to self-assign a floating role and receive calls for that specific role in addition to their own permanent role. Privacy/Proxy Numbers allow users to hide their personal phone number when they are called from the PSTN. MH-CURE Dynamic Calling integrates with Avaya Aura® Application Enablement Services (AES) using the Telephony Server Application Programming Interface (TSAPI) interface.

MH-CURE consists of an MH-CURE Application Server and MH-CURE SIP clients. MH-CURE Dynamic Calling allows a call to be routed to a Dynamic Role or Proxy Number rather than a specific user. This is achieved by routing calls to MH-CURE using adjunct routing via AES. When enabled, MH-CURE delivers a destination to Communication Manager to which the call is routed. The destination returned by MH-CURE can be an extension used by MH-CURE SIP client, an Avaya H.323/SIP Deskphone, or PSTN. These Application Notes will cover the connectivity between MH-CURE and AES using the TSAPI interface. Configuration of MH-CURE SIP clients is outside the scope of this document. Refer to the following Application Notes for details on how to integrate MH-CURE SIP clients with Avaya Aura® Communication Manager and Avaya® Session Manager.

Application Notes for Mobile Heartbeat MH-CURE with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on placing calls to VDNs/Vectors associated with a Dynamic Role or a Privacy/Proxy Number on MH-CURE. The VDNs used adjunct routing via AES to route call to MH-CURE. MH-CURE would then route call to the appropriate user.

The serviceability testing focused on verifying that MH-CURE returned to service after re-connecting the network or rebooting the application server.

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 MH-CURE did not utilize encryption capabilities as requested by Mobile Heartbeat.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Calls from PSTN and internal users to MH-CURE VDNs, including Dynamic Role and Privacy/Proxy Number VDNs.
- Use of TSAPI routing services to properly route incoming calls using adjunct routing via a TSAPI link to AES. MH-CURE returns the correct destinations as configured in MH-CURE.
- Assigning Dynamic Role to MH-CURE SIP clients, Avaya H.323 / SIP Deskphones, and PSTN phones.
- Assigning Privacy/Proxy Number to MH-CURE users to hide the user's personal phone number.
- Proper system recovery after a restart of MH-CURE application server and loss of network connectivity.

2.2. Test Results

All test cases passed with the following observations:

- Calls from a cell phone to a Privacy/Proxy Number displayed the dialed number on the cell phone's display. The caller does not see the called party's personal phone number.
- Calls from a telephone on the PSTN to a Privacy/Proxy number displayed the called party's name only on the telephone's display. The caller does not see the called party's personal phone number.
- Calls from an internal Avaya deskphone to a Privacy/Proxy Number could see the connected party's number.

2.3. Support

For MH-CURE technical support, contact Mobile Heartbeat technical support via phone or website.

- **Phone:** +1 (781) 238-0000
- **Web:** https://www.mobileheartbeat.com/contact-us/

3. Reference Configuration

Figure 1 illustrates a sample configuration with an Avaya Aura® Environment that includes the following products:

- Communication Manager with a G450 Media Gateway and Avaya Aura® Media Server providing media resources.
- Session Manager connected to Communication Manager via a SIP trunk.
- Session Manager connected to the PSTN via Avaya Session Border Controller for Enterprise (SBCE).
- Avaya Aura® System Manager used to configure Session Manager and SIP stations on Communication Manager.
- Application Services configured to communicate with Avaya Aura® Communication Manager via TSAPI.
- Avaya Messaging serving as the voicemail system.
- Avaya H.323 and SIP Deskphones.
- MH-CURE Clients running on iOS smartphones with wireless LAN device providing network access (not shown).
- MH-CURE Application Server providing SIP configuration to MH-CURE clients and TSAPI connectivity to Application Enablement Services.

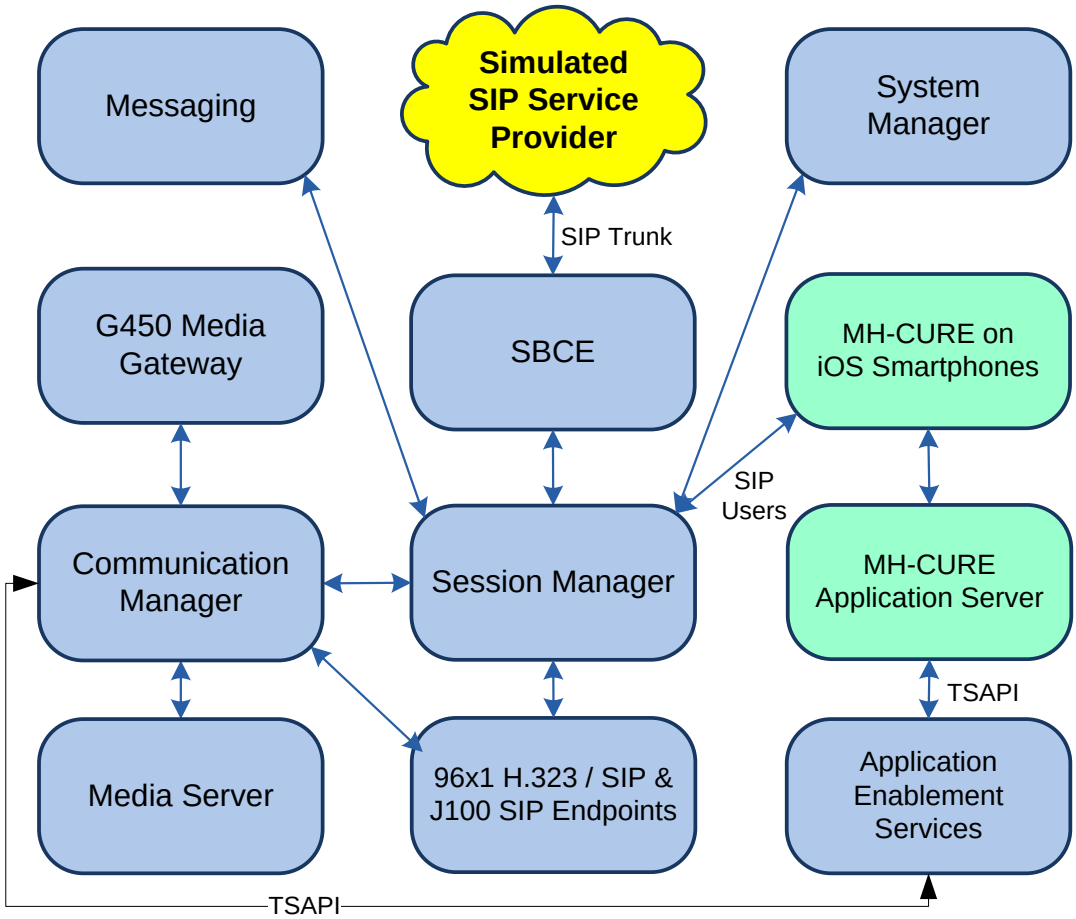


Figure 1: Avaya Aura® with MH-CURE

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	8.1.3.0.1-FP3P1
Avaya G450 Media Gateway	FW 41.24.0
Avaya Aura® Media Server	v.8.0.2.138
Avaya Messaging	10.8.2 SP1
Avaya Aura® System Manager	8.1.3.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.3.0.1012091 Feature Pack 3
Avaya Aura® Session Manager	8.1.3.0.813014
Avaya Aura® Application Enablement Services	8.1.3.0.0.25-0
Avaya 96x1 Series IP Deskphone	6.8502 (H.323) 7.1.11.0.8 (SIP)
Avaya J100 Series SIP Deskphone	4.0.7.1.5
MH-CURE Client running on iOS 14.3 Smartphone	20.2.3.5
MH-CURE Application Server running on Windows Server 2016	20.2.3.109

5. Configure Avaya Aura® Communication Manager

This section provides the steps for configuring Communication Manager. Administration of Communication Manager was performed using the System Access Terminal (SAT). This covers the following areas:

- Verify License
- Administer AES Connection
- Administer CTI Link
- Administer Vectors and VDNs

5.1. Verify License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has appropriate permissions for features illustrated in these Application Notes. Use the **display system-parameters customer-options** command. Navigate to **Page 4** and verify that the **Computer Telephony Adjunct Links** customer option is set to "y".

The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.

```
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? n                       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

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

Navigate to **Page 7** and verify that the **Vectoring (Basic)** customer option is set to "y".

```
display system-parameters customer-options                      Page   7 of  12
                        CALL CENTER OPTIONAL FEATURES

                         Call Center Release: 8.0

                               ACD? y                          Reason Codes? y
                     BCMS (Basic)? y                 Service Level Maximizer? n
        BCMS/VuStats Service Level? y                Service Observing (Basic)? y
 BSR Local Treatment for IP & ISDN? y     Service Observing (Remote/By FAC)? y
                  Business Advocate? n                Service Observing (VDNs)? y
                    Call Work Codes? y                                Timed ACW? y
     DTMF Feedback Signals For VRU? y                      Vectoring (Basic)? y
                  Dynamic Advocate? n                   Vectoring (Prompting)? y
      Expert Agent Selection (EAS)? y                Vectoring (G3V4 Enhanced)? y
                          EAS-PHD? y                 Vectoring (3.0 Enhanced)? y
                  Forced ACD Calls? n     Vectoring (ANI/II-Digits Routing)? y
              Least Occupied Agent? y     Vectoring (G3V4 Advanced Routing)? y
         Lookahead Interflow (LAI)? y                      Vectoring (CINFO)? y
Multiple Call Handling (On Request)? y      Vectoring (Best Service Routing)? y
    Multiple Call Handling (Forced)? y                   Vectoring (Holidays)? y
  PASTE (Display PBX Data on Phone)? y                   Vectoring (Variables)? y
       (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. Administer AES Connection

In the **IP Services** form, add an entry for AES. On Page 1, configure the following fields:

- **Service Type:** Set to *AESVCS*.
- **Enabled:** Set to *y***.**
- **Local Node:** Set to *procr* for the Processor Ethernet interface.
- **Local Port:** **U**se the default of *8765*.

```
change ip-services                                              Page   1 of   3

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

On Page 4 of the **IP Services** form, configure the following fields:

- **AE Services Server:** Set to the AES server hostname from the **IP Node Names** form (not shown).
- **Password:** Set to a password to be administered on AES in **Section 6.3**.
- **Enabled:** Set to *y*.

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

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:      devcon-aes        *                     y        in use
```

5.3. Administer CTI Link

Add a CTI link using the **add cti-link** command. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter *ADJ-IP* in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

```
CTI Link: 1
Extension: 77700
     Type: ADJ-IP
                                                                  COR: 1
     Name: AES TSAPI Link
Unicode Name? n
```

5.4. Configure Vectors and VDNs

Administer two sets of vectors and VDNs shown below, one for a Dynamic Role and another one for a Privacy/Proxy Number. Note that the VDN extensions and vector numbers can vary.

VDN	Vector	Purpose
77300	77	Vector & VDN for the Dynamic Role assigned to "Charge Nurse."
77310	78	Vector & VDN for a Privacy/Proxy Number used by a doctor.

5.4.1. Dynamic Role Vector and VDN

A vector needs to be configured for MH-CURE to perform adjunct routing. Use the **change vector *n*** command to configure a vector, where ***n*** is an available Vector number. The following Vector was used during the compliance test for MH-CURE to route calls to the user assigned to the Dynamic Role associated with "Charge Nurse." This is a simple example that routes calls to AES using the *adjunct route* command. Customers can configure a more robust Vector that handles error conditions, such as the CTI link being down.

```
change vector 77                                          Page   1 of   6
                                CALL VECTOR

    Number: 77               Name: MH-CURE Dynamic Role
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    1   secs hearing silence
02
03 adjunct      routing link 1
04 wait-time    30  secs hearing silence
05
06 busy
07 disconnect   after announcement none
```

Add a VDN using the **add vdn** command. Enter a descriptive **Name** and the vector number specified above for **Vector Number**. Retain the default values for all remaining fields.

```
change vdn 77300                                          Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 77300                  Unicode Name? n
                                 Name*: MH-CURE Dynamic Role
                           Destination: Vector Number        77
                     Attendant Vectoring? n
                   Meet-me Conferencing? n
                     Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none     Report Adjunct Calls as ACD*? n


          VDN of Origin Annc. Extension*:
                              1st Skill*:
                              2nd Skill*:
                              3rd Skill*:

SIP URI:

* Follows VDN Override Rules
```

5.4.2. Privacy/Proxy Number Vector and VDN

Use the **change vector *n*** command to configure a vector, where ***n*** is an available Vector number. The following Vector was used during the compliance test for MH-CURE to route calls to a doctor using the VDN number. This allows the doctor's personal phone number to be hidden from the PSTN caller. This is a simple example that routes calls to AES using the *adjunct route* command. Customers can configure a more robust Vector that handles error conditions, such as the CTI link being down.

```
change vector 78                                          Page   1 of   6
                                  CALL VECTOR

    Number: 78               Name: MH-CURE Proxy Number
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    1   secs hearing silence
02
03 adjunct      routing link 1
04 wait-time    30  secs hearing silence
05
06 busy
07 disconnect   after announcement none
```

Add a VDN using the **add vdn** command. Enter a descriptive **Name** and the vector number specified above for **Vector Number**. Retain the default values for all remaining fields.

```
change vdn 77300                                          Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 77300                  Unicode Name? n
                                 Name*: MH-CURE Proxy Number
                           Destination: Vector Number        78
                     Attendant Vectoring? n
                   Meet-me Conferencing? n
                     Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none     Report Adjunct Calls as ACD*? n


        VDN of Origin Annc. Extension*:
                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:

SIP URI:

* Follows VDN Override Rules
```

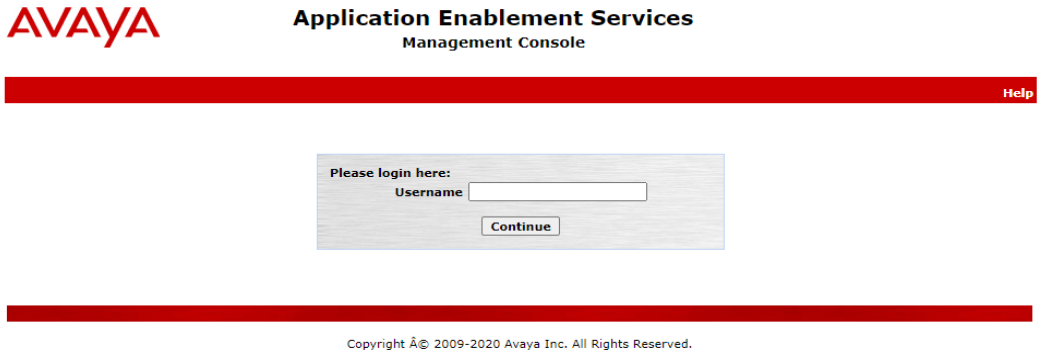
6. Configure Avaya Aura® Application Enablement Services

This section provides the steps for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM Interface
- Verify License
- Administer Switch Connection
- Administer TSAPI Link
- Restart Service
- Obtain Tlink Name
- Administer User
- Verify Security Database

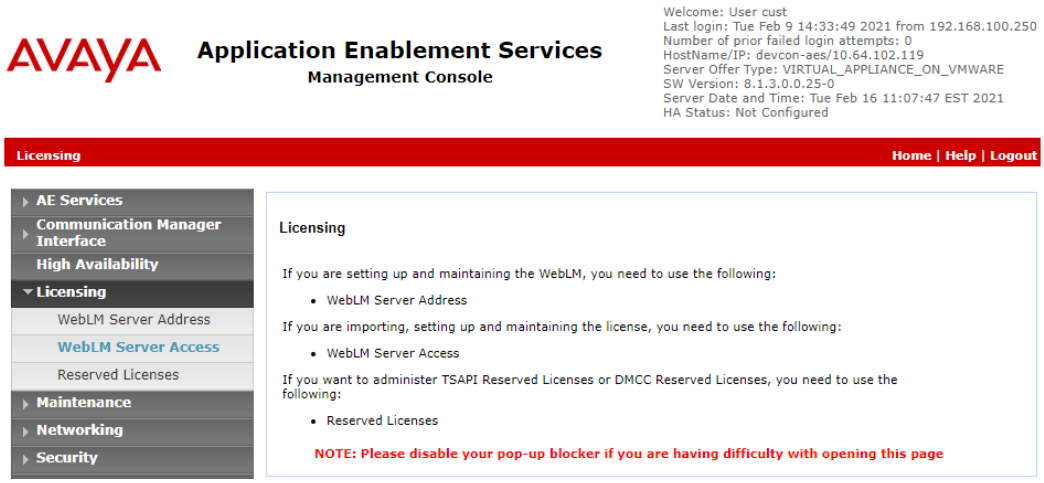
6.1. Launch OAM Interface

Access the OAM web-based interface by using the URL "https://<*ip-address*>" in an Internet browser window, where <*ip-address*> is the IP address of the Application Enablement Services server. The login screen is displayed. Log in using the appropriate credentials.



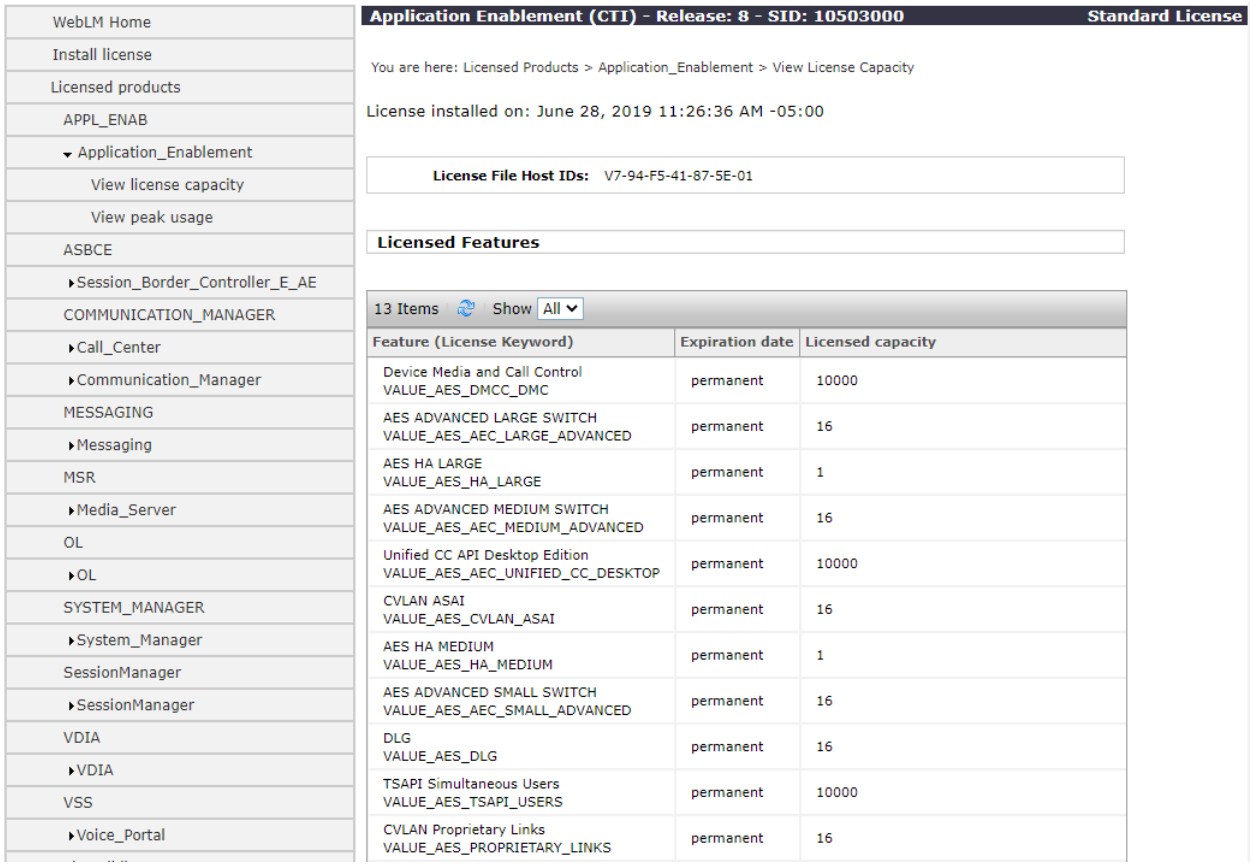
6.2. Verify License

Select **Licensing → WebLM Server Access** in the left pane to display the **Web License Manager** pop-up screen (not shown). Log in using the appropriate credentials.



The **Web License Manager** screen below is displayed. Select **Licensed Products → APPL_ENAB → Application_Enablement** in the left pane to display the **Application Enablement (CTI)** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users** as shown below. Also, verify that there is an applicable advanced switch license, in this case **AES ADVANCED MEDIUM SWITCH** for the virtual server.



Scroll down to see the rest of the licenses. Note that the MH-CURE solution only uses an **AES ADVANCED MEDIUM SWITCH** license as shown in the **Acquired Licenses** section below. No TSAPI user licensing is required for this solution.

Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiS MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_ LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;u TrustedApplications: IPS_001, BasicUnrestricte DMCUnrestricted; 1XP_001, BasicUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted DMCUnrestricted; PC_001, BasicUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricte DMCUnrestricted; VP_001, BasicUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AEC CCE_001, BasicUnrestricted, AdvancedUnrestri CSI_T1_001, BasicUnrestricted, AdvancedUnre CSI_T2_001, BasicUnrestricted, AdvancedUnre AVAYAVERINT_001, BasicUnrestricted, Advanc DMCUnrestricted; CCT_ELITE_CALL_CTRL_001 AdvancedUnrestricted, DMCUnrestricted, Agen BasicUnrestricted, AdvancedUnrestricted, DMC UNIFIED_DESKTOP_001, BasicUnrestricted, Ac DMCUnrestricted, AgentEvents; AACC_001, Ba AdvancedUnrestricted, DMCUnrestricted; CE_A BasicUnrestricted, AdvancedUnrestricted, DMC TP_CLIENT_001, BasicUnrestricted, , , AgentEv , AgentEvents; EXT_CLIENT_002, , , , AgentEv , AgentEvents; EXT_CLIENT_004, , , , AgentEv , AgentEvents; EXT_CLIENT_006, , , , AgentEv , AgentEvents; EXT_CLIENT_008, , , , AgentEv , AgentEvents; EXT_CLIENT_010, , , , AgentEv AAWFO_SELECT_001, BasicUnrestricted, Adva DMCUnrestricted, AgentEvents;OFFICELINX_0 AdvancedUnrestricted, DMCUnrestricted, Agen BasicUnrestricted, , DMCUnrestricted, AgentEv BasicUnrestricted, AdvancedUnrestricted, DMC ECD_001, , AdvancedUnrestricted, , AgentEver VERINT_ESSENTIAL_001, BasicUnrestricted, A DMCUnrestricted;
AES HA SMALL VALUE_AES_HA_SMALL	permanent	1

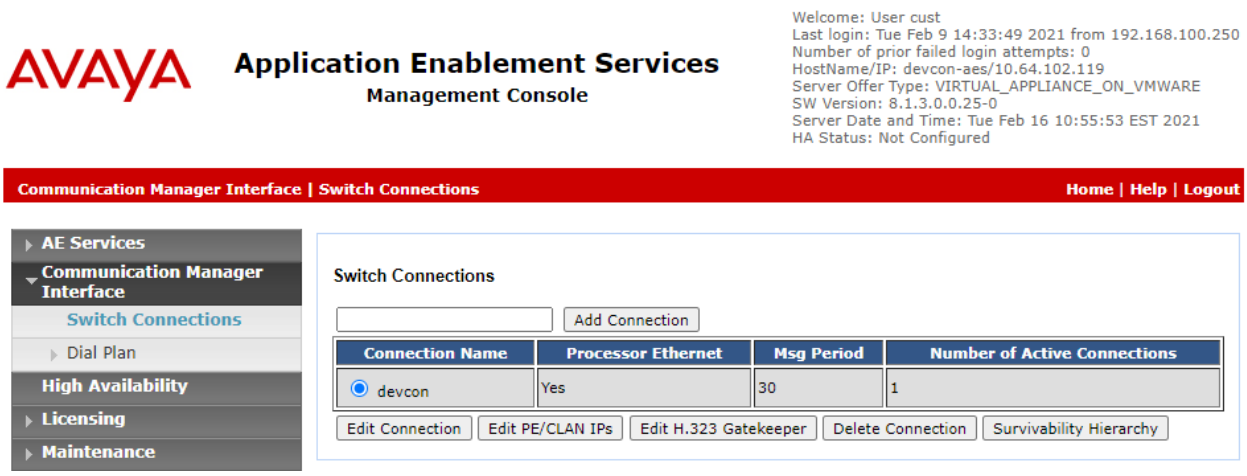
Acquired Licenses

1 Item | Show All

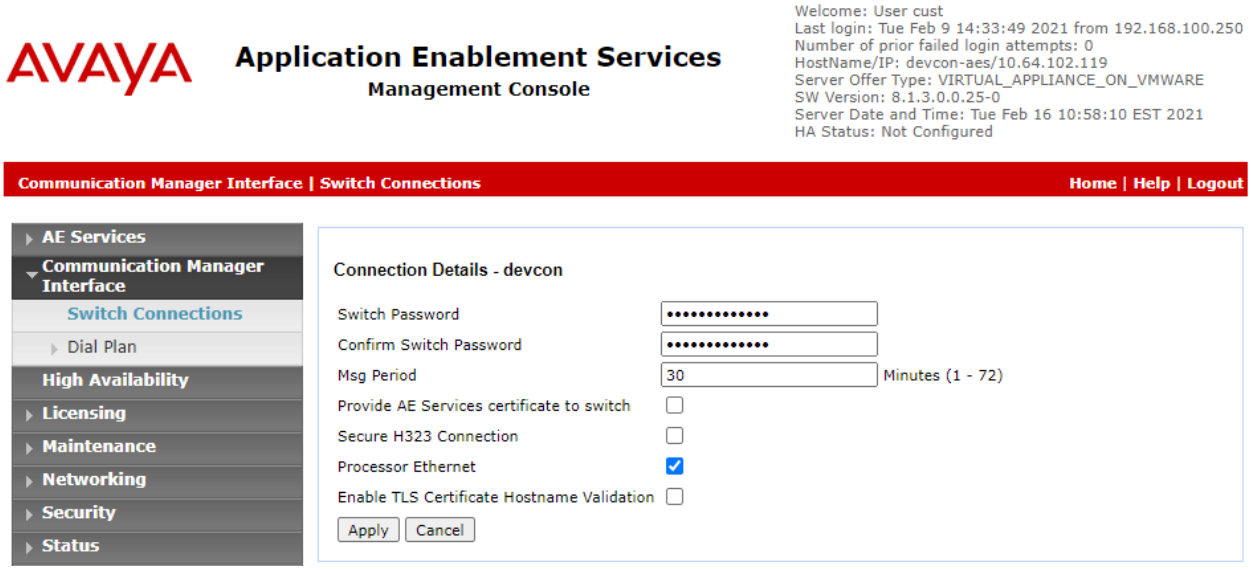
Feature	Acquired by	Acquirer ID	Count
VALUE_AES_AEC_MEDIUM_ADVANCED	TSAPI (devcon-aes)	devcon-aes:1612892496:8549:-164894784:0000	1

6.3. Administer Switch Connection

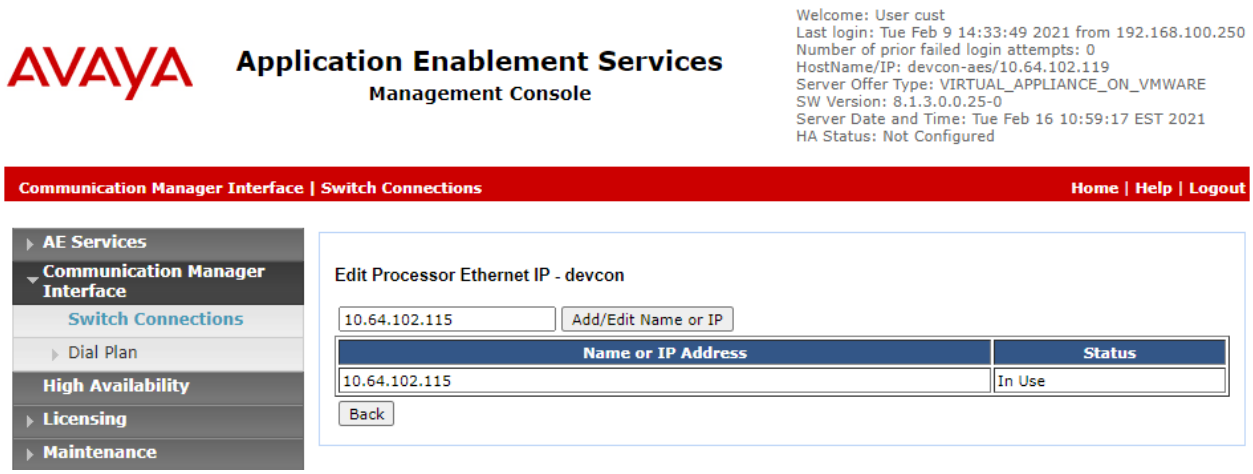
To administer a **Switch Connection** for Communication Manager, navigate to **Communication Manager Interface → Switch Connections** and enter a name for the new switch connection and click the **Add Connection** button. This was previously configured as *devcon* as shown below.



Click **Edit Connection** button to configure the connection details. Enter the **Switch Password** and check the **Processor Ethernet** box, if using the **procr** interface, as shown below. The password must match the one configured when adding AESVCS connection in Communication Manager in **Section 5.2**.

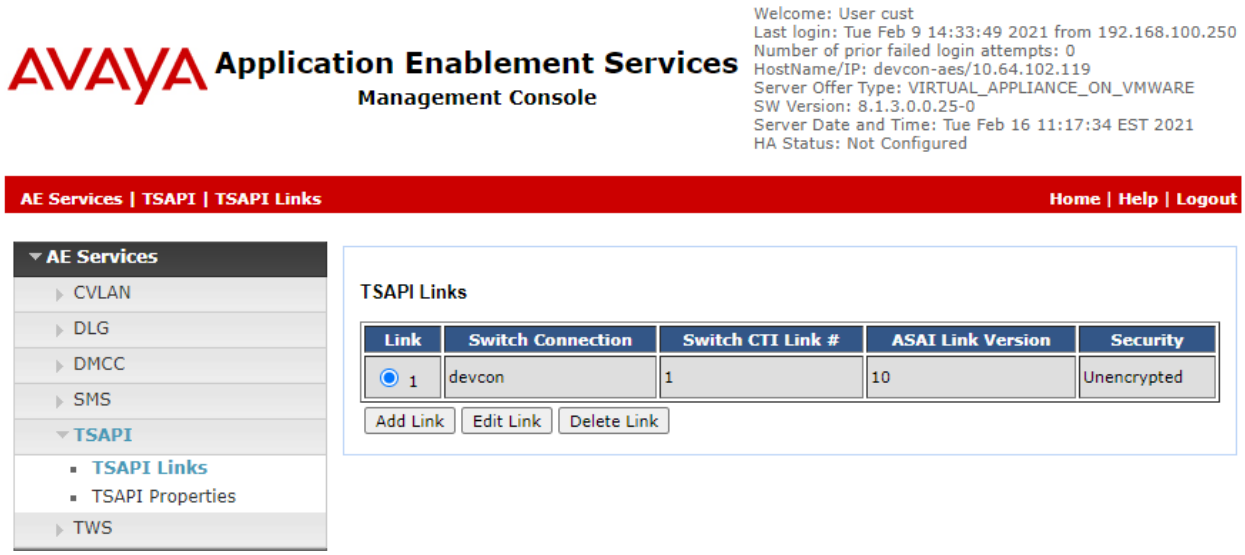


Click **Edit PE/CLAN IPs** on the **Switch Connection** page and configure the **procr** or **CLAN** IP address of Communication Manager and click **Add/Edit Name or IP**.

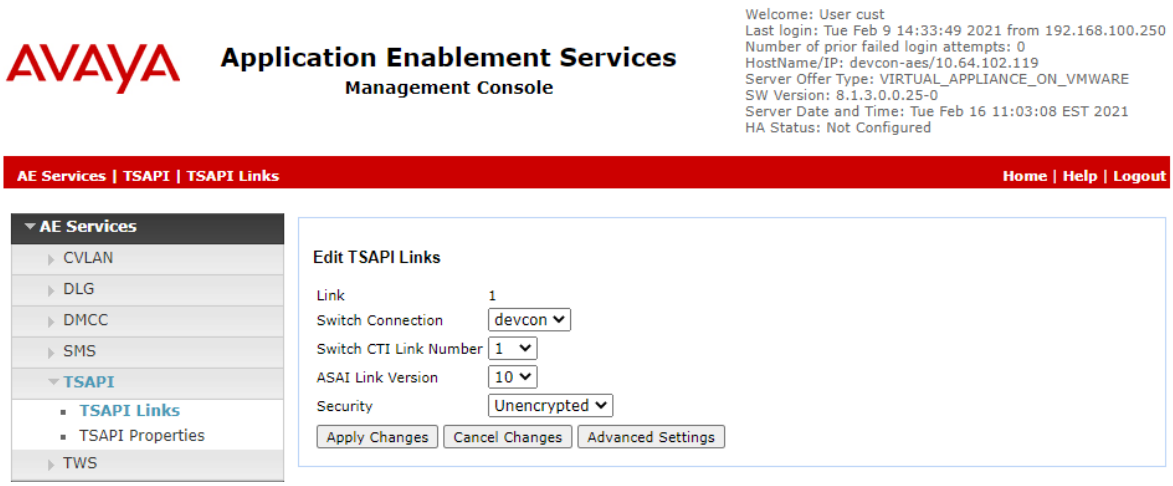


6.4. Administer TSAPI Link

Select **AE Services → TSAPI → TSAPI Links** from the left pane of the **Management Console** to administer a TSAPI link. The **TSAPI Links** screen is displayed as shown below. Click **Add Link**.

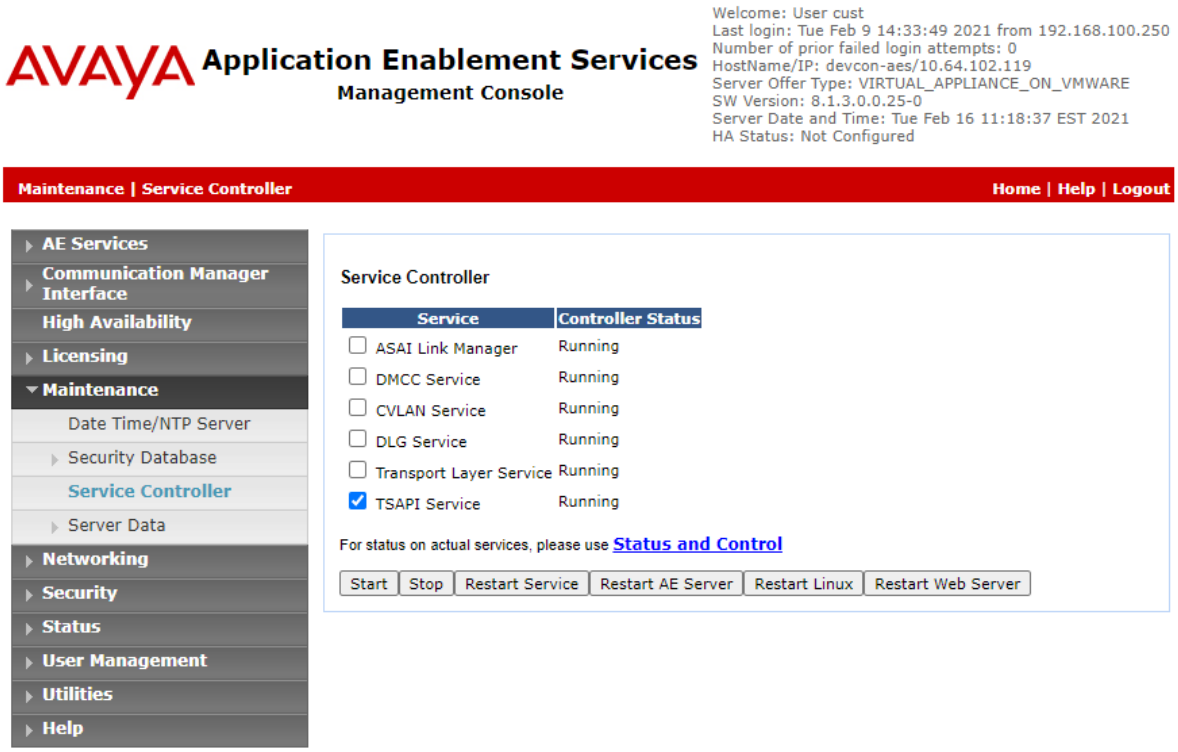


The **Add TSAPI Links** screen is displayed next. The **Link** field is only local to the Application Enablement Services server and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection *devcon* is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.3**. Retain the default values in the remaining fields.



6.5. Restart Service

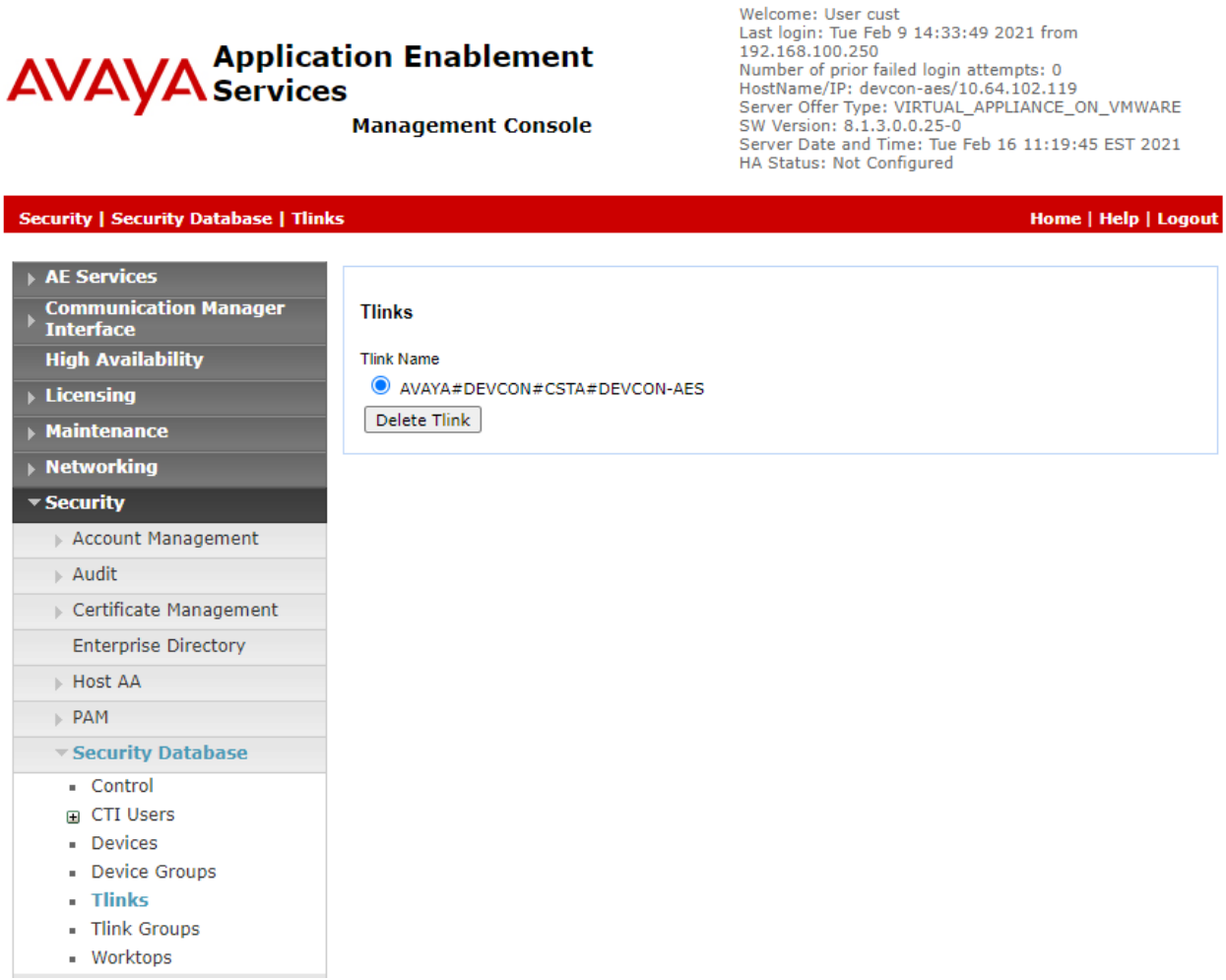
Select **Maintenance → Service Controller** from the left pane to display the **Service Controller** screen in the right pane. Check **TSAPI Service**, as shown below, and click **Restart Service**.



6.6. Obtain Tlink Name

Select **Security → Security Database → Tlinks** from the left pane. The **Tlinks** screen shows a listing of Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name to be used later for configuring Callback.

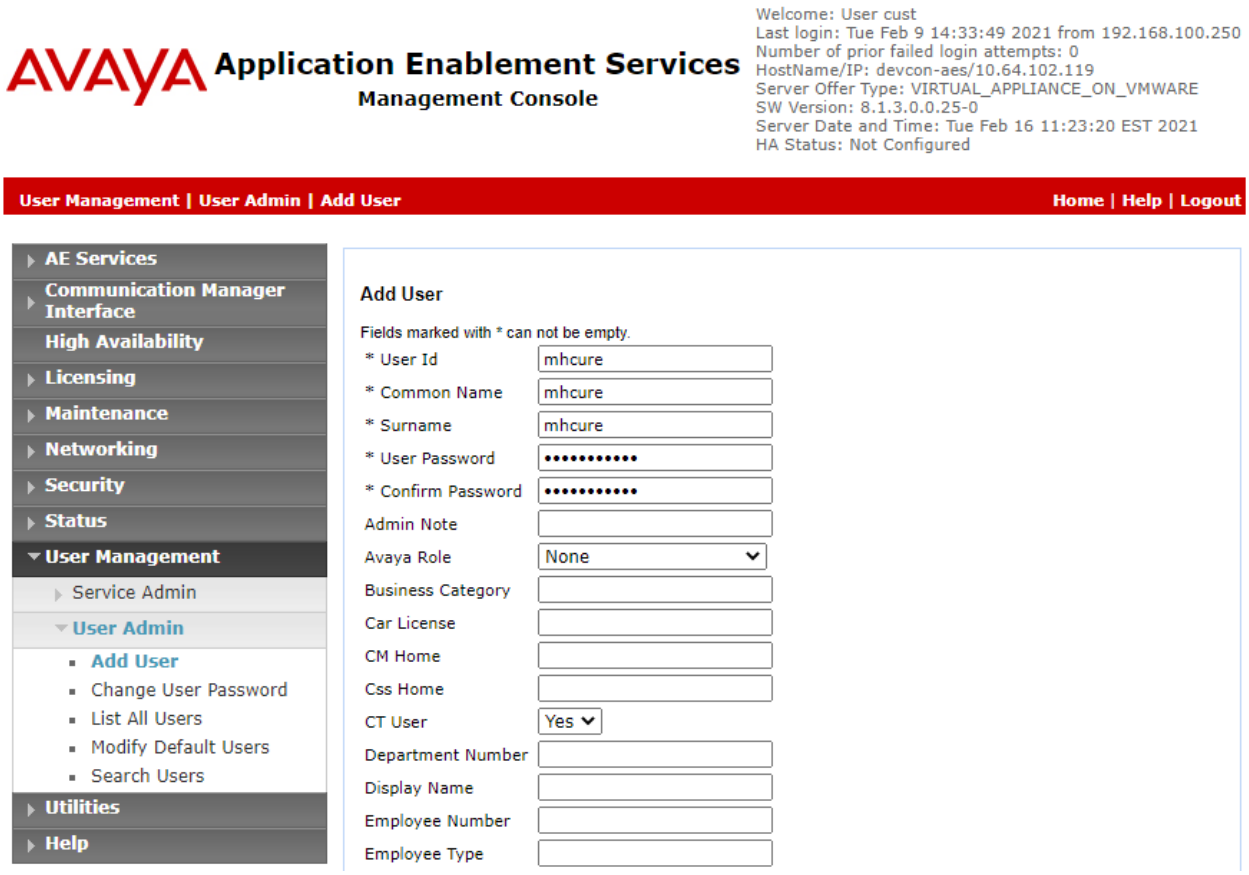
In this case, the associated Tlink name is "AVAYA#DEVCON#CSTA#DEVCON-AES." Note the use of the switch connection "DEVCON" from **Section 6.3** as part of the Tlink name.



6.7. Administer User

Select **User Management → User Admin → Add User** from the left pane to display the **Add User** screen in the right pane.

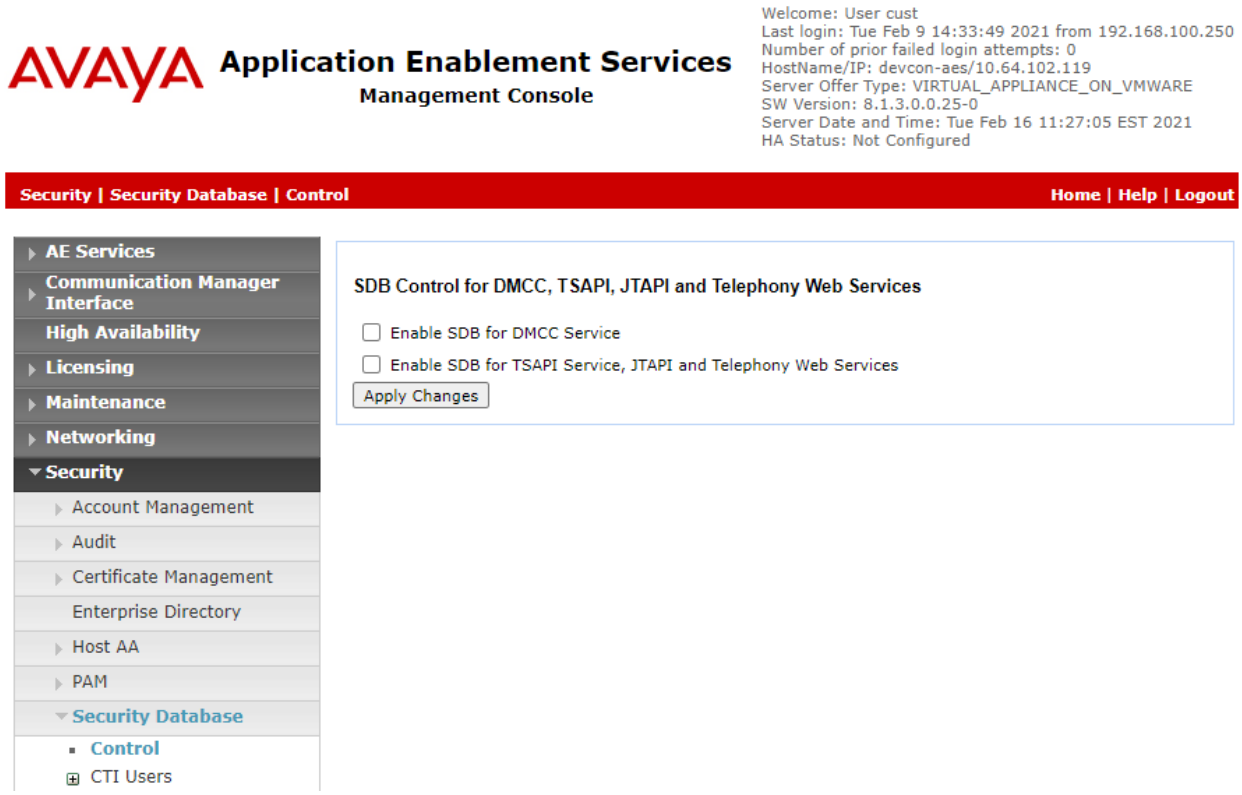
Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select "Yes" from the drop-down list. Retain the default value in the remaining fields.



6.8. Verify Security Database

Select **Security → Security Database → Control** from the left pane to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane.

Verify that **Enable SDB for TSAPI Service, JTAPI and Telephony Web Services** is unchecked. In the event that security database is used by the customer with this parameter already enabled, then follow **[2]** to configure access privileges for the user from **Section 6.7**.



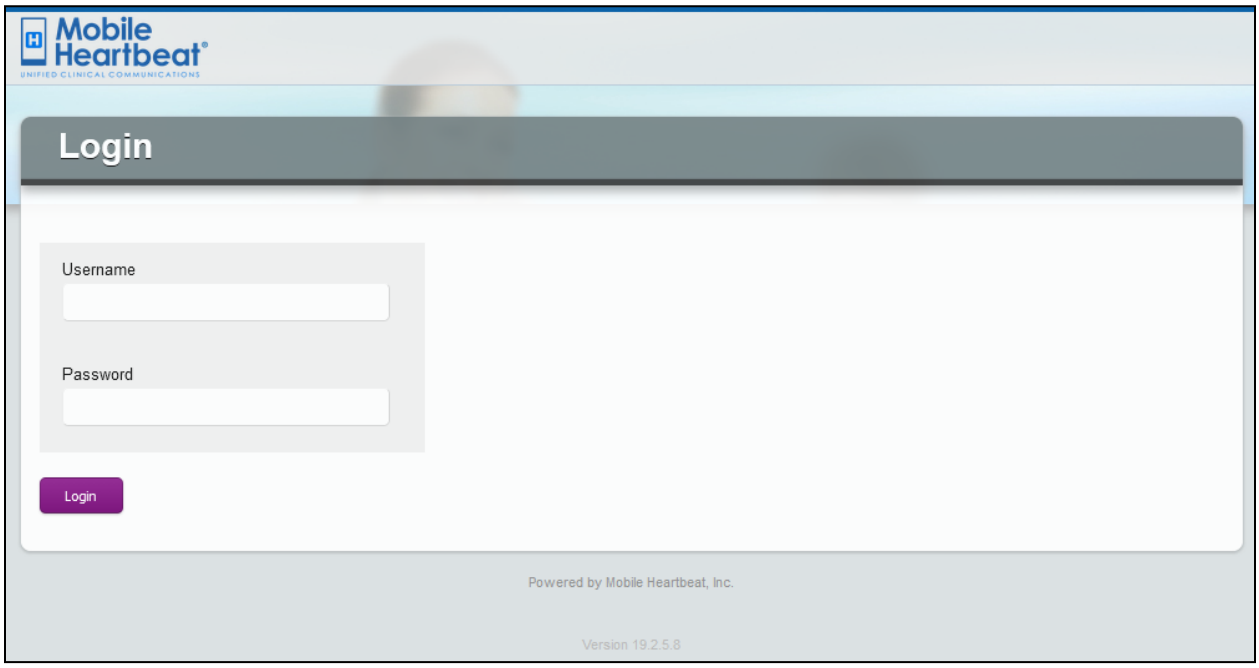
7. Configure Mobile Heartbeat MH-CURE

Configuration for MH-CURE is performed via MH-CURE Administrative Web User Interface.

- Log onto MH-CURE Web Admin Tool
- Administer MH-CURE for AES/TSAPI Connectivity
- Administer Dynamic Role
- Administer Privacy/Proxy Number
- Administer MH-CURE SIP Clients

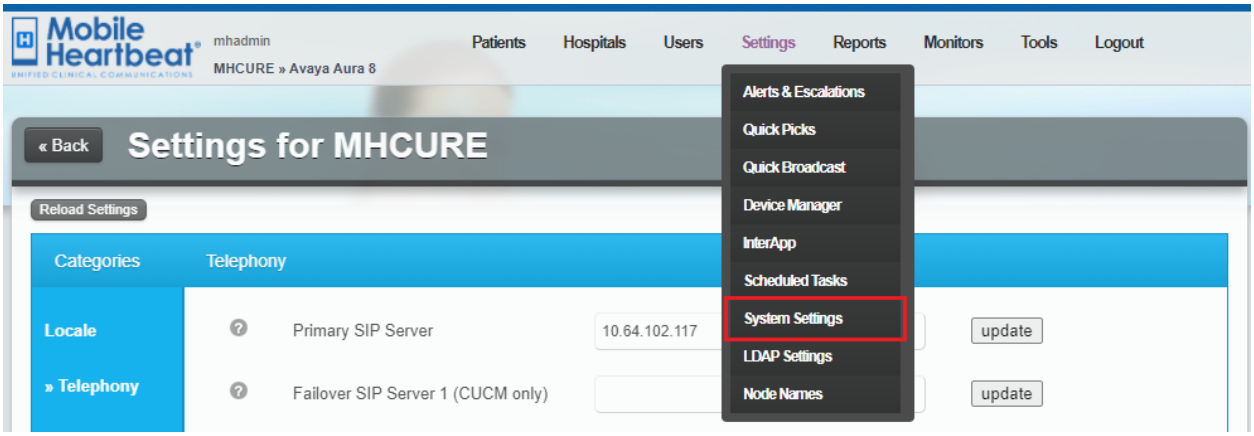
7.1. Log onto MH-CURE Web Admin Tool

Access the MH-CURE Web interface by using the URL "https://<*FQDN*>:8443/heartbeat" in an internet browser, where <*FQDN*> is the FQDN of the MH-CURE Application Server. Log in using appropriate credentials.

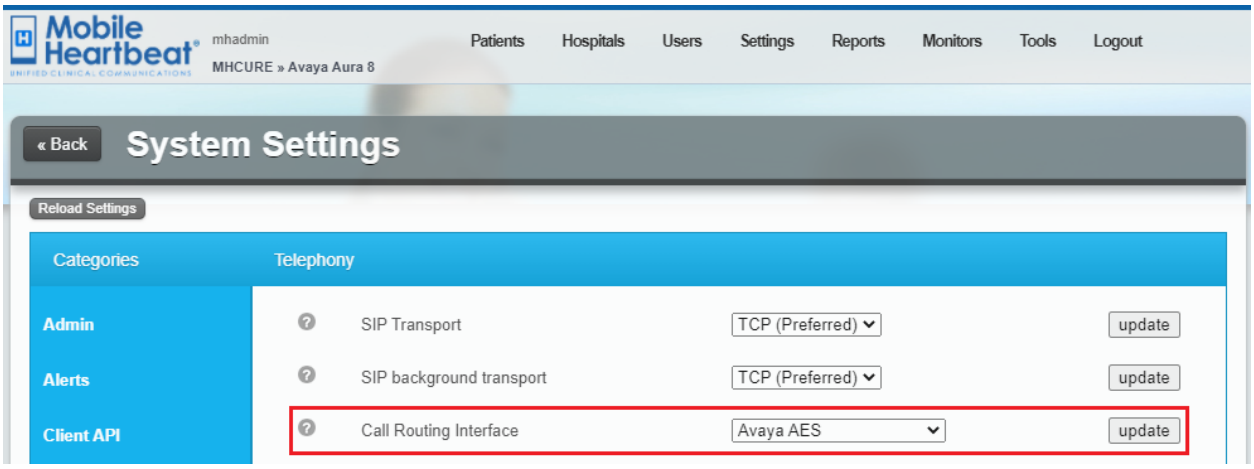


7.2. Administer MH-CURE for AES/TSAPI Connectivity

From the top menu, navigate to **Settings → System Settings**.



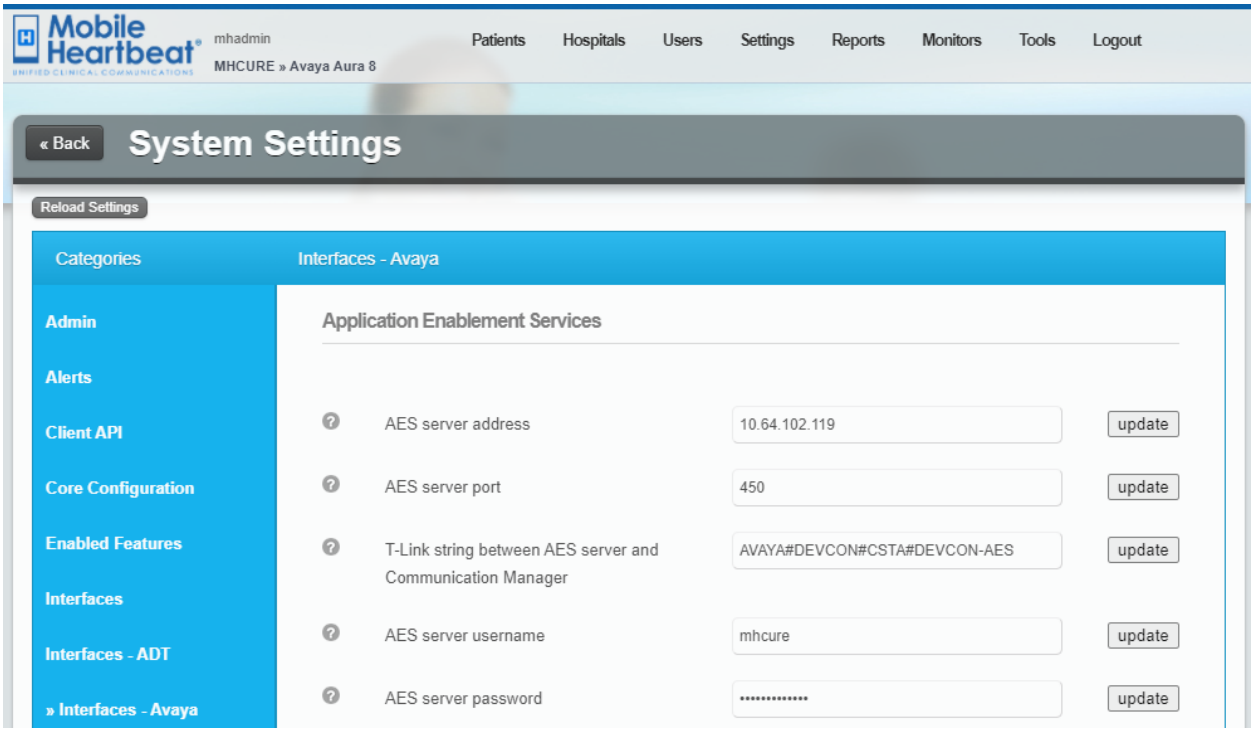
In the left pane, click **Telephony** (not shown). For **Call Routing Interface,** select **Avaya AES** and click **update**.



In the left side, click **Interfaces – Avaya**. Configure the fields as shown below:

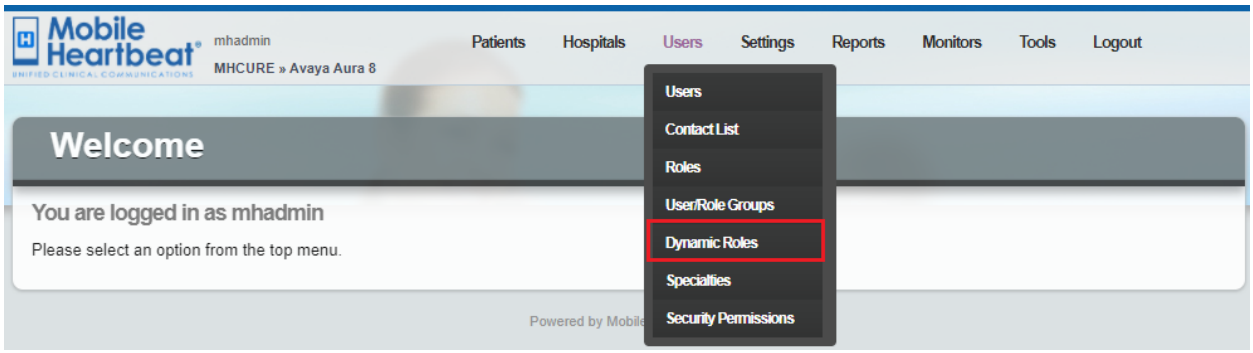
- **AES server address:** Set to AES IP address.
- **AES server port:** Set to port for AES TSAPI services. Default port *450* is used.
- **T-Link string between AES server and Communication Manager:** Set to **Tlink** obtained from **Section 6.6**.
- **AES server username** Set to **User ID** from **Section 6.7**.
- **AES server password** Set to **User Password** from **Section 6.7**.

It is recommended to restart Tomcat Services on the MH-CURE application server.

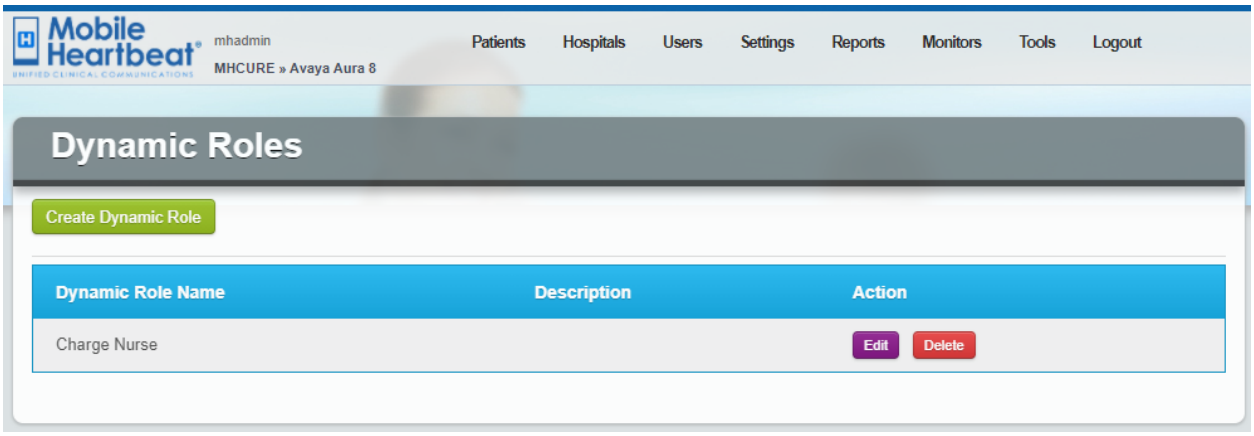


7.3. Administer Dynamic Role

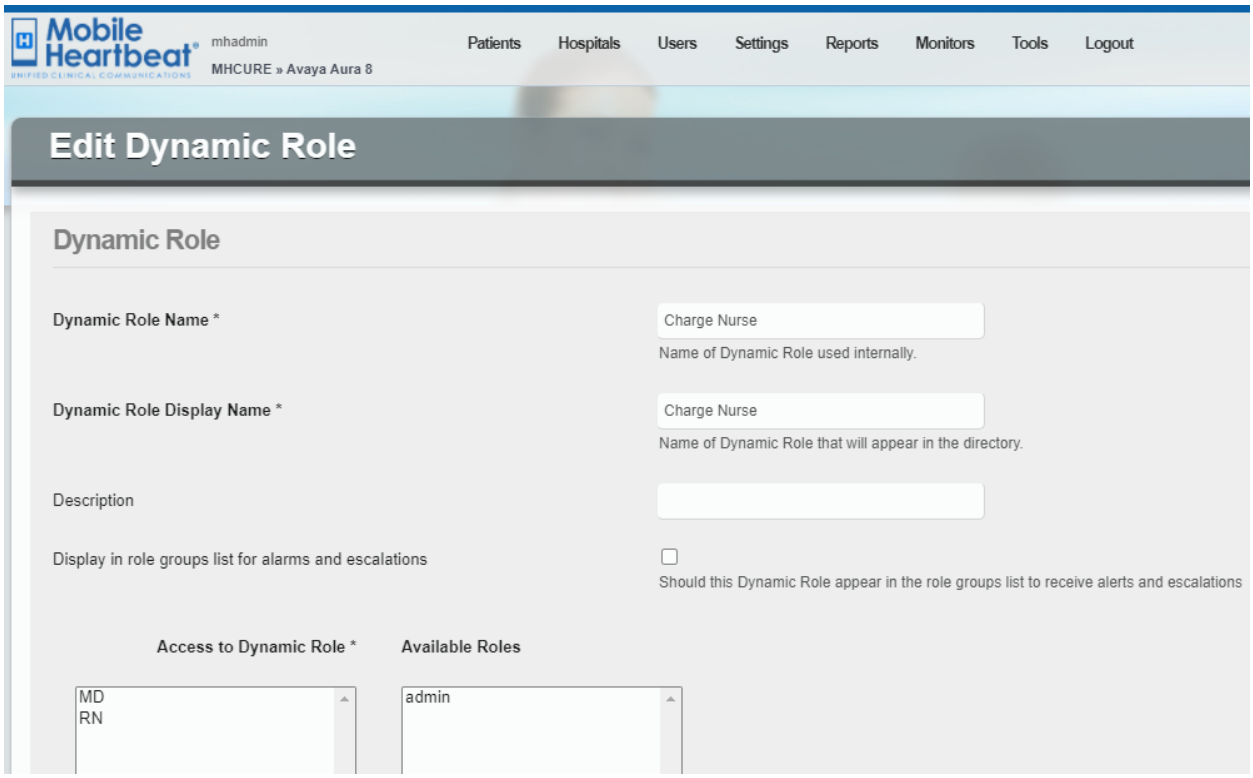
The extension of a Dynamic Roles must match the VDN extension configured for Vector/Adjunct routing in Communication Manager in **Section 5.4.1**. An example Dynamic Role was configured for "Charge Nurse." The VDN extension for this Dynamic Role is 77300. From the top menu, navigate to **Users → Dynamic Roles**.



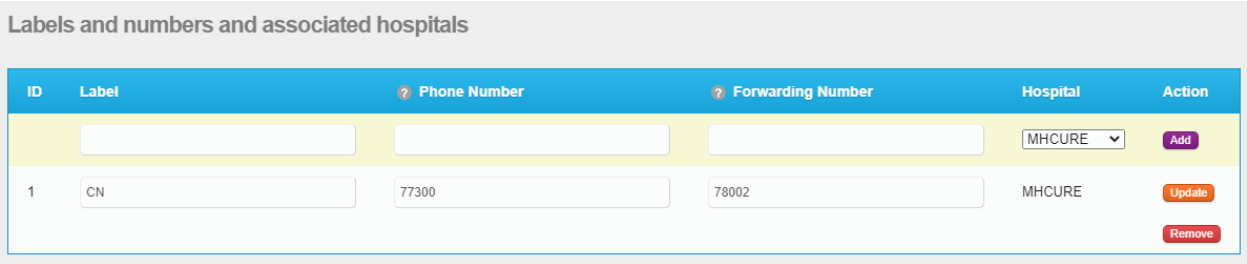
Click **Edit** associated with the "Charge Nurse" Dynamic Role Name to assign the VDN extension.



In the **Dynamic Role** page, the Dynamic Role Name is specified as "Charge Nurse." Also, note that users assigned to the *RN* role are allowed to assign themselves to this Dynamic Role.



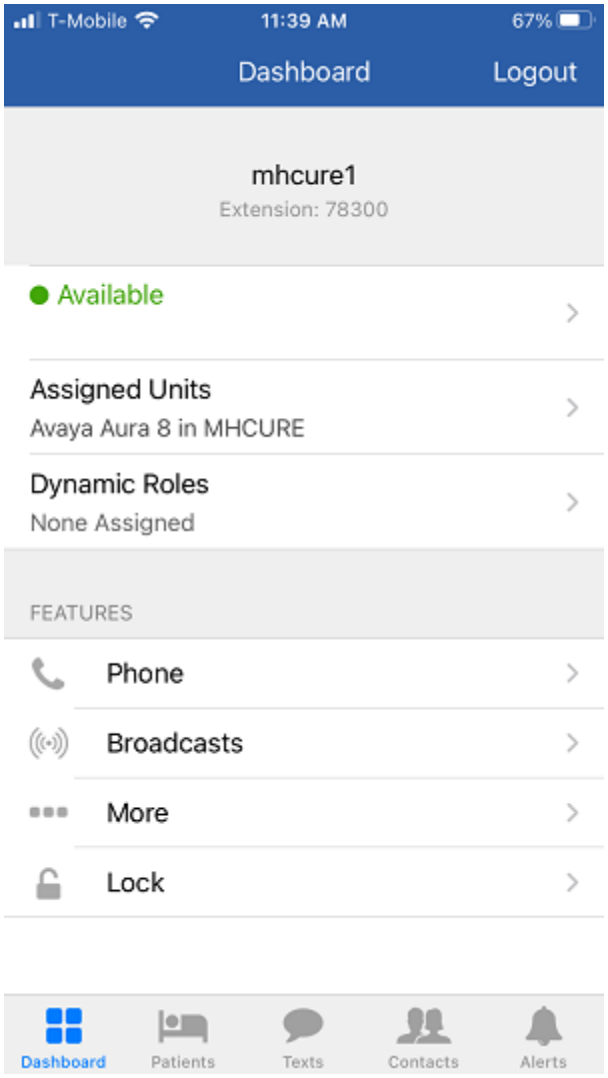
Scroll down to the **Labels and numbers and associated hospitals** section. Enter the VDN extension (e.g., *77300*) in the **Phone Number** field. If MH-CURE SIP clients are used, the Dynamic Role can be assigned (enabled) within the MH-CURE SIP client application. When assigned, MH-CURE returns the MH-CURE SIP client extension as destination to Communication Manager. If no MH-CURE user is assigned to the dynamic role, and the number in the **Forwarding Number** field is configured, then the call will be routed to that number. Click **Update**.

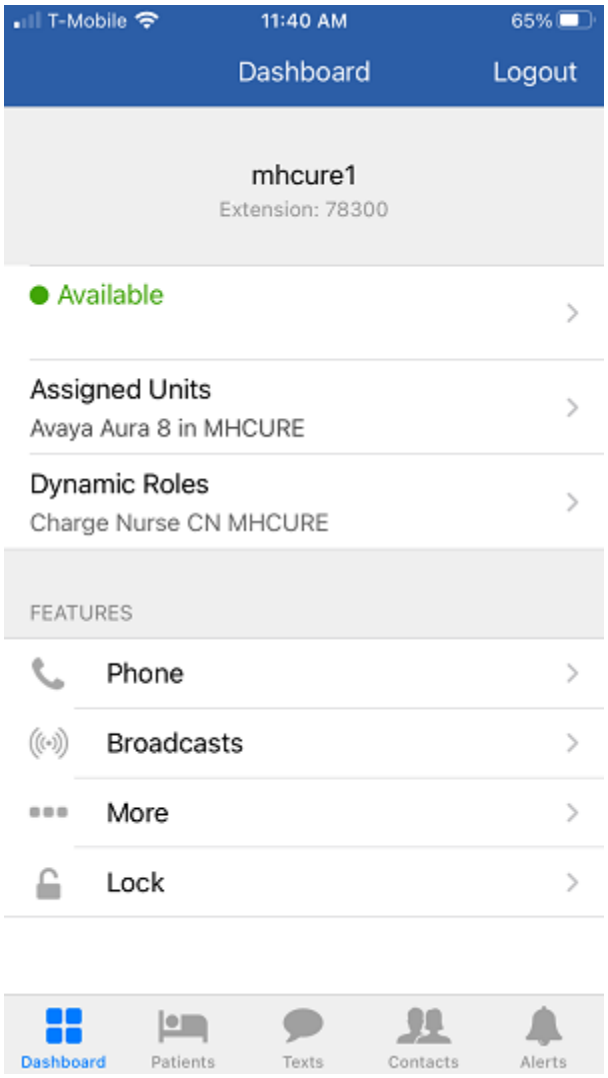


7.4. Administer MH-CURE SIP Clients

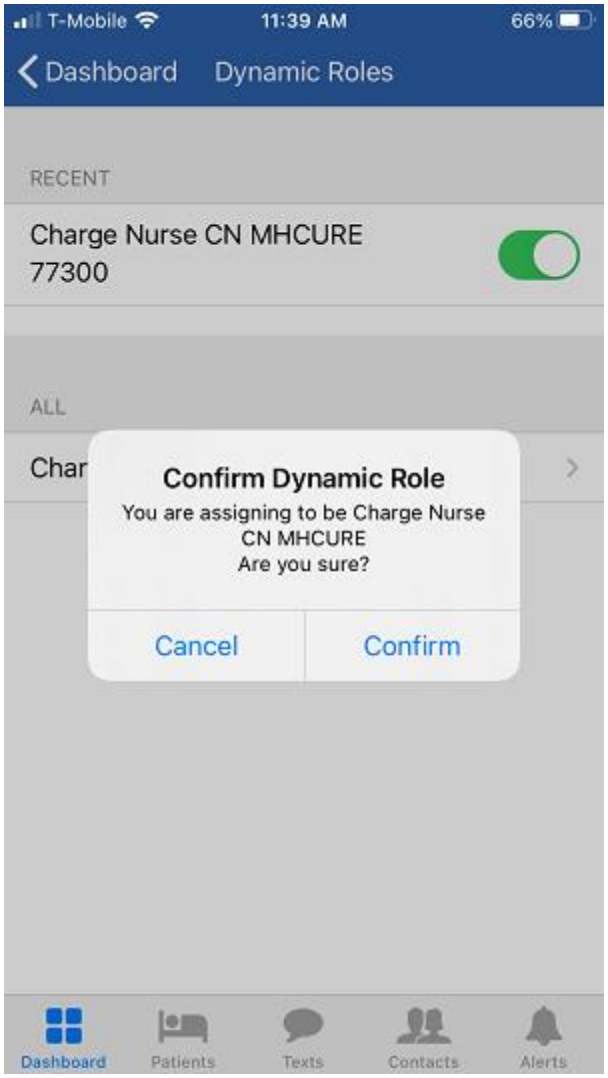
If MH-CURE SIP clients are used, a user may assign themselves to a Dynamic Role from the MH-CURE app on a mobile device. Log into the MH-CURE app and select **Dynamic Roles**.

Note: Avaya H.323 / SIP Deskphones and PSTN users can also be assigned to Dynamic Roles.

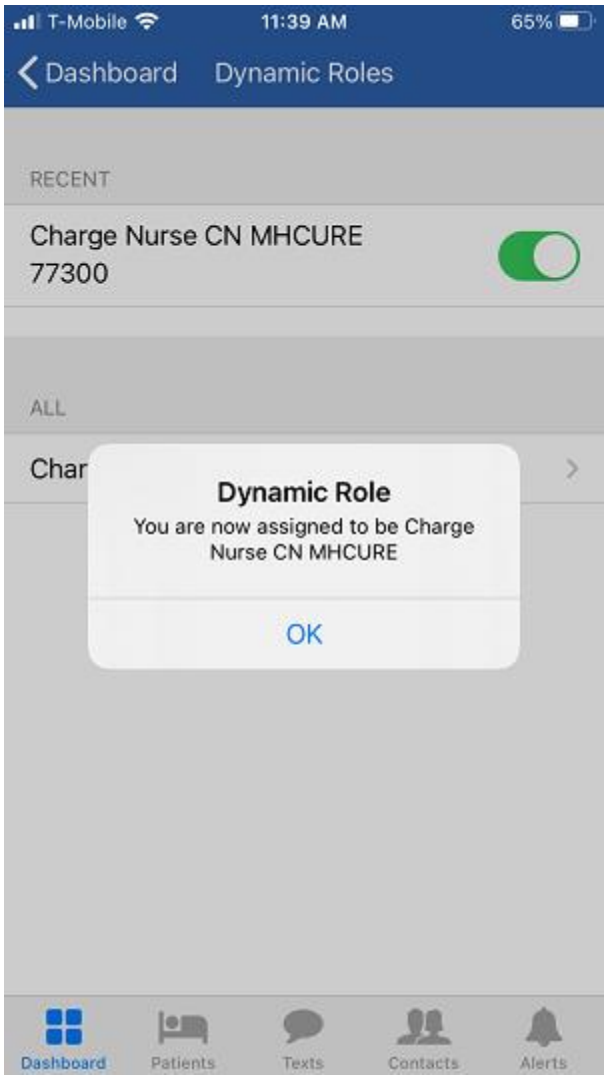




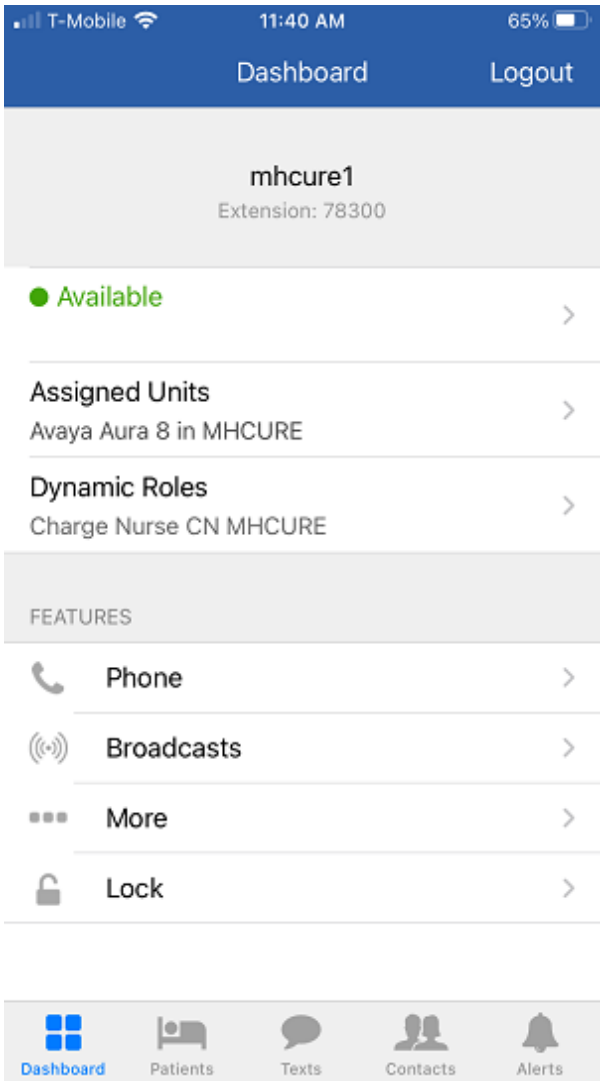
Toggle the Dynamic Role button and confirm the assignment.



The MH-CURE app notifies the user that the user has been assigned to the Dynamic Role. Click **OK**.



The **Dashboard** on the MH-CURE app displays the successful assignment of the Dynamic Role to the user. When a call is placed to the VDN 77300, MH-CURE returns the current user as a destination and Communication Manager delivers the call to the MH-CURE SIP client.



8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services, and MH-CURE.

8.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the status of the AES connection using the status aesvcs command.

```
status aesvcs interface

                          AE SERVICES INTERFACE STATUS

Local Node         Enabled?  Number of     Status
                             Connections

procr              yes       1             listening
```

Verify communication between Communication Manager and AES using the **status aesvcs link** command.

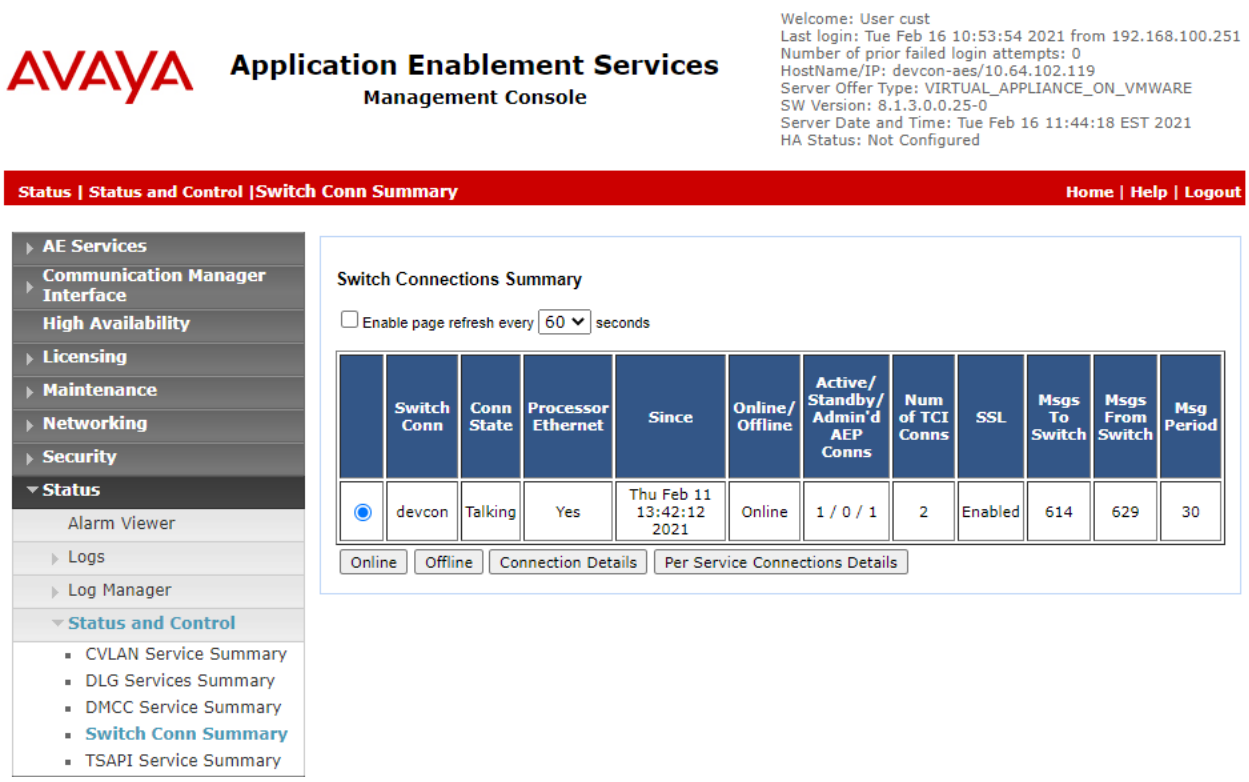
```
status aesvcs link

                             AE SERVICES LINK STATUS

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

01/01  devcon-aes                       49786   procr           628     614
                       10.64.102.119
```

Verify the status of the CTI link between Communication Manager and AES using the **status aesvcs cti-link** command. Verify the **Service State** is *established.*

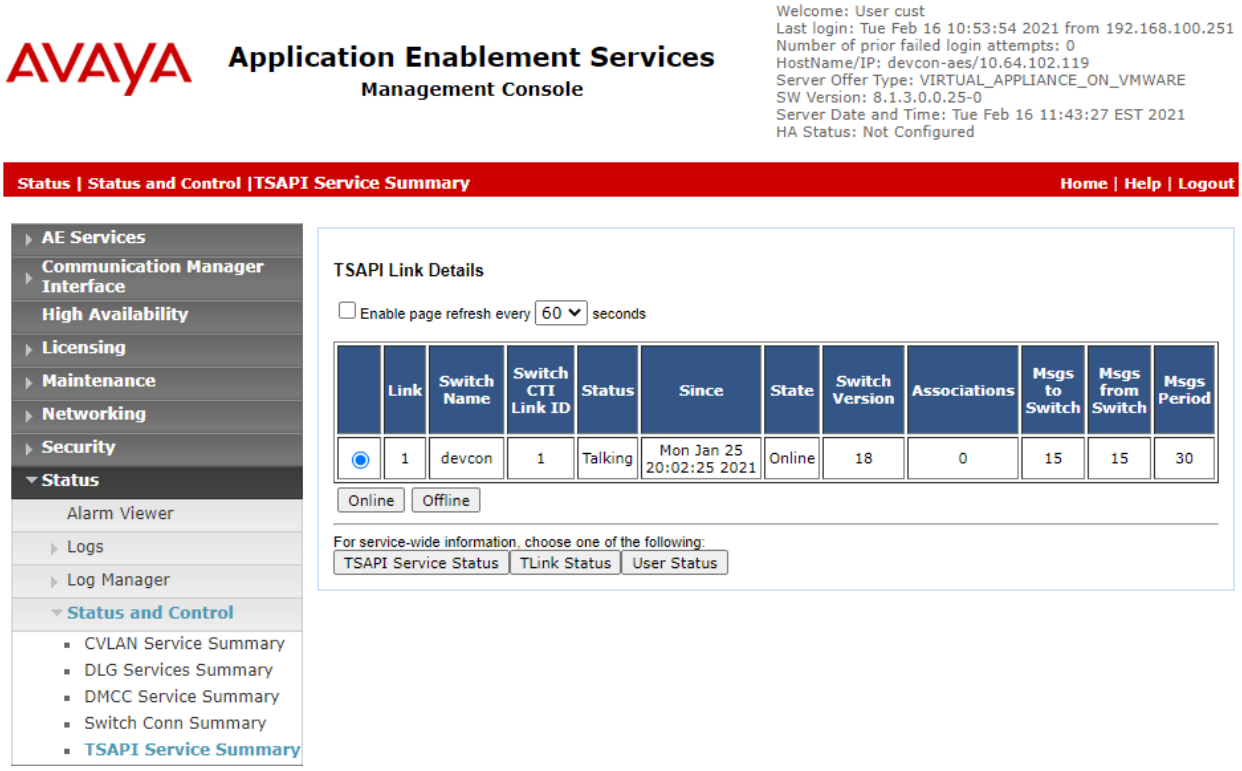
```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

1     10       no    devcon-aes       established   15       15
```

8.2. Verify Avaya Aura® Application Enablement Services

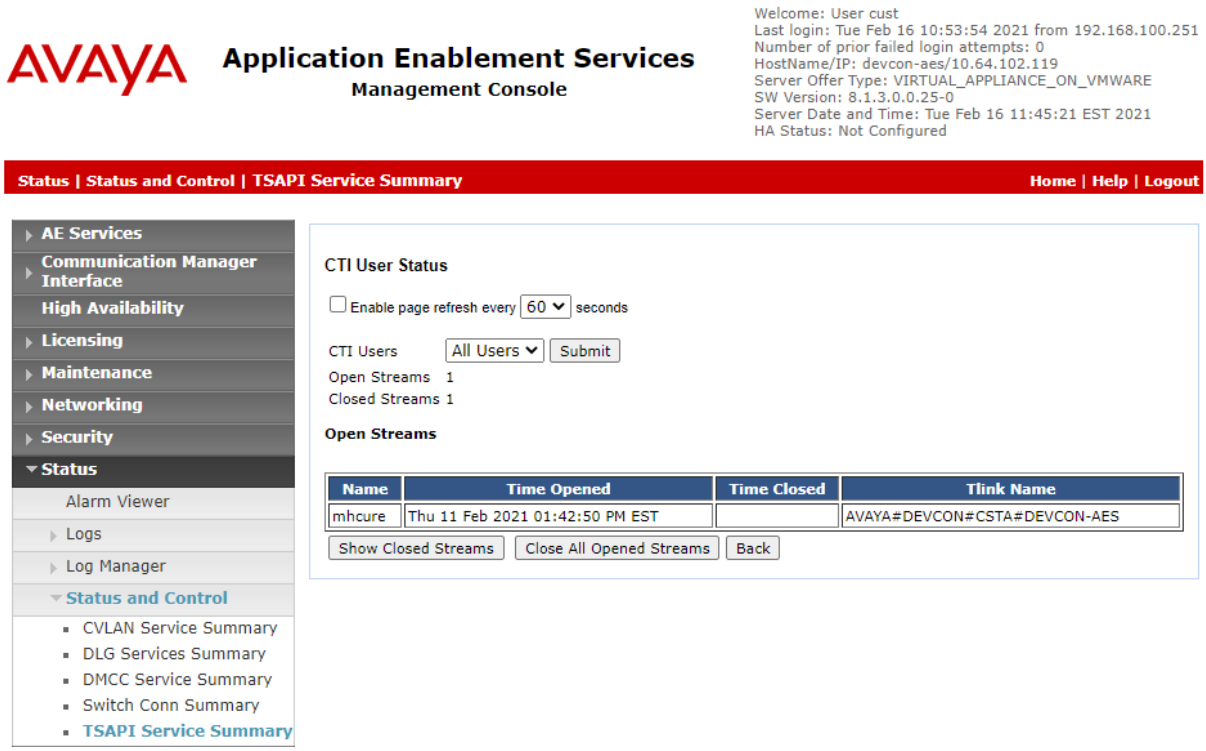
On Application Enablement Services, navigate to **Status → Status and Control → Switch Conn Summary.** Verify the Switch Connection to Communication Manager is **Talking** and **Online**.



Select **TSAPI Service Summary** in the left pane. Verify the TSAPI link is **Talking** and **Online**.



Continuing from above, select **User Status**. Verify the MH-CURE user is connected to AES.



9. Conclusion

These Application Notes describe the steps required to integrate Mobile Heartbeat MH-CURE Dynamic Calling with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. Calls to the Dynamic Role VDN were routed to the user assigned to the Dynamic Role and calls to Proxy Number VDN was routed to the user assigned to that proxy number. All tests passed with observations noted in **Section 2.2**.

10. Additional References

This section references the product documentation relevant for these Application Notes.

[1] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 2, July 2019, available at http://support.avaya.com.

[2] *Administering and Maintaining Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 2, August 2019, available at http://support.avaya.com.

[3] *Application Notes for Mobile Heartbeat MH-CURE with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.*

[4] *MH-CURE 20.2 Web Admin Guide*, MH00333, Revision 1.0.

[5] *MH-CURE 20.2 iOS Shared User Guide*, MH00324, Revision 1.0.

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.