Avaya Solution & Interoperability Test Lab

Application Notes for Mobile Heartbeat MH-CURE with Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager – Issue 1.1

Abstract

These Application Notes contain interoperability instructions for Mobile Heartbeat MH-CURE with Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager to successfully interoperate. Mobile Heartbeat MH-CURE 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 configuration steps required to integrate Mobile Heartbeat MH-CURE (MH-CURE) with Avaya Aura® Application Enablement Services (AES) and Avaya Aura® Communication Manager (Communication Manager).

These Application Notes describe the MH-CURE connectivity to AES using the TSAPI interface. MH-CURE solution consists of MH-CURE Application Server and MH-CURE SIP clients. MH-CURE provides Dynamic Role calling feature that allows a call to be routed to a Dynamic Role rather than a specific user. This is achieved via adjunct routing a call to MH-CURE via AES. When enabled, MH-CURE delivers a destination to Communication Manager to route a call to. The destination returned by MH-CURE can be an extension used by MH-CURE SIP client or an Avaya endpoint. Configuration of MH-CURE SIP clients is out of scope for this document. Please refer to the application notes below for MH-CURE SIP clients:

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

2. General Test Approach and Test Results

The general test approach was to validate successful integration of MH-CURE with AES. The feature test cases were performed manually. Incoming calls were placed to the VDNs/Vectors that adjunct routed the calls to MH-CURE via AES.

The serviceability testing focused on verifying that MH-CURE returned to service after re-connecting the network or rebooting the MH-CURE 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 this DevConnect Application Note 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.

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 interoperability compliance test included feature and serviceability testing.

- Calls from PSTN and internal users to MH-CURE VDNs
- Use of TSAPI routing services to properly route incoming calls.
    - Adjunct routing calls to MH-CURE
    - MH-CURE returning correct destinations as configured in MH-CURE
- Destinations include Avaya SIP and H.323 endpoints, and MH-CURE SIP clients
- Dynamic Role via MH-CURE SIP clients

Serviceability tests included network unavailability and reboot of MH-CURE server. In such cases, calls routed as per the vector configurations.

2.2. Test Results

All planned test cases were executed successfully.

2.3. Support

For technical related to MH-CURE, contact Mobile Heartbeat Support via the Mobile Heartbeat website.

3. Reference Configuration

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

- Avaya Aura® Communication Manager running in a virtual environment with an Avaya G450 Gateway. Avaya G450 Gateway was connected to the PSTN via an ISDN-PRI trunk.
- Media resources in the Avaya G450 Media Gateway and Avaya Aura® Media Server.
- Avaya Aura® Session Manager connected to Avaya Aura® Communication Manager via a SIP trunk and acting as a Registrar/Proxy for SIP Endpoints.
- Avaya Aura® Application Services configured to communicate with Avaya Aura® Communication Manager via TSAPI.
- Avaya 96x1 and J Series H.323 and SIP Deskphones.
- MH-CURE Application Server running on a Windows Server 2016 and MH-CURE SIP clients running on iOS devices.

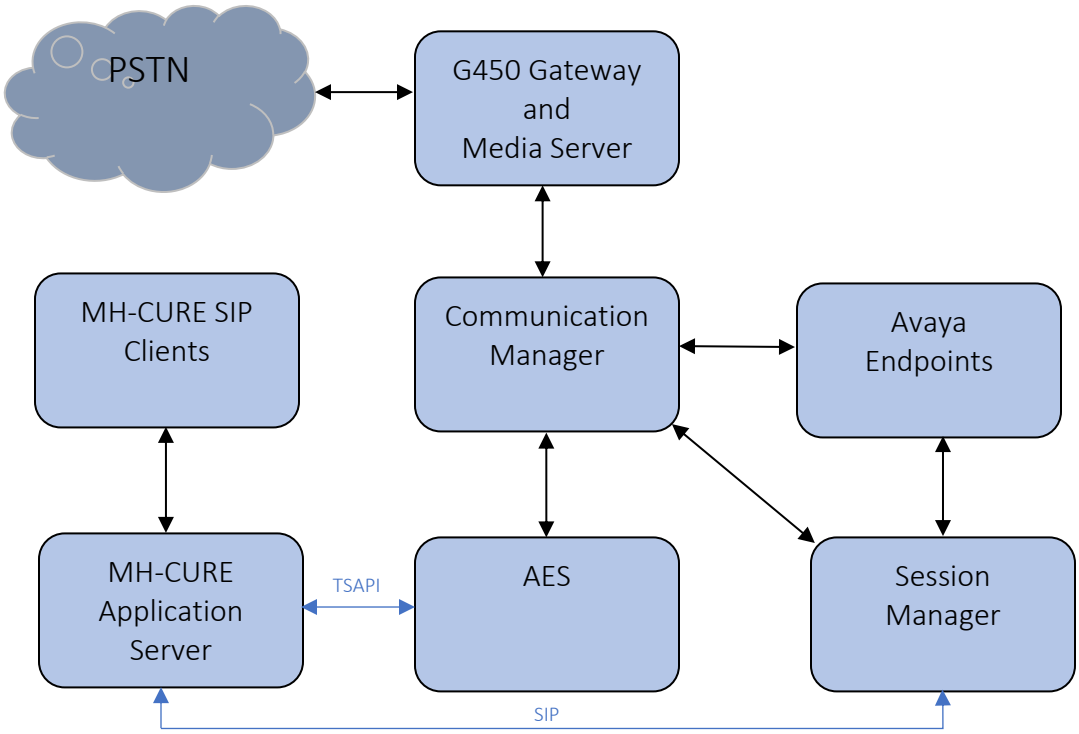


Figure 1: Avaya Aura® with MH-CURE

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	7.1.3.3.0-FP3SP3
Avaya G450 Media Gateway	FW 40.19.1
Avaya Aura® Media Server	8.0.0.205
Avaya Aura® Session Manager	7.1.3.3.713307
Avaya Aura® Application Enablement Services	7.1.3.3.0.2-0
Avaya Aura® Communication Manager Messaging	7.1.3.1.0-FP3SP1
Avaya 9600 Series IP Deskphones	6.8.2 (H.323) 7.1.6.1 (SIP)
Avaya J100 Series IP Phones	6.8.2 (H.323) 4.0.2.1 (SIP)
Mobile Heartbeat MH-CURE Application Server running on Windows server 2016 Mobile Heartbeat MH-CURE SIP client running on iOS mobile devices v12.1.3	R19.2.5

5. Configure Avaya Aura® Communication Manager

This section contains steps necessary to configure MH-CURE successfully with Avaya Aura® Communication Manager.

All configurations in Communication Manager were performed via SAT terminal.

5.1. Configure AES connection

An AE Services link must be established between Communication Manager and AES. Use the **change node-names ip**. Take a note of the **procr** node **IP Address**, which will be used when configuring AES.

```
change node-names ip                                          Page   1 of   2
                                  IP NODE NAMES
    Name                 IP Address
procr                  10.64.150.14
procr6                 ::
```

Use the **change ip-services** command to add an entry for AES. On Page 1,

- 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**.

```
change ip-services                                            Page   1 of   4

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

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

- In the **AE Services Server** field, type the name obtained from the AES server (hostname).
- In the **Password** field, type a password to be administered on the AES server.
- 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:      aes15019          *                     y        in use
```

5.2. Configure CTI Link

In order for Communication Manager to establish a connection to AES, a CTI link needs to be configured. Use **add cti-link *n*** command, where ***n*** is an available CTI link number.

- In the **Extension** field, type in an available extension number
- 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: 58001
     Type: ADJ-IP
                                                                      COR: 1
     Name: AES 7.1.3
```

5.3. Configure Vector

A vector needs to be configured for MH-CURE to perform adjunct routing. Use **change vector *n*** to configure a Vector, where ***n*** is an available Vector number. The following vector was used during the compliance test. Note that, in a case where the cti link 1 returns an error or is not available, call is routed to the extension configured in step 3.

```
change vector 2                                              Page   1 of   6
                                CALL VECTOR

    Number: 2                Name: Hunt 1
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    3   secs hearing ringback
02 adjunct      routing link 1
03 route-to     number 53101            with cov n if unconditionally
04 wait-time    30  secs hearing ringback
05 goto step    2             if unconditionally
```

5.4. Configure VDN

Use **add vdn *n*** to add a vdn, where ***n*** is an available vdn extension**.** On Page 1:

- In the **Name** field, enter a descriptive name
- In the **Destination** field, set **Vector Number** to the vector configured in previous section. i.e., Vector Number 2.

Two VDNs, 50001 and 50002 were used during the compliance test that used the same vector.

```
add vdn 50001                                                Page   1 of   3
                           VECTOR DIRECTORY NUMBER

                             Extension: 50001
                                 Name*: MH-CURE VDN
                           Destination: Vector Number        2
                 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:
```

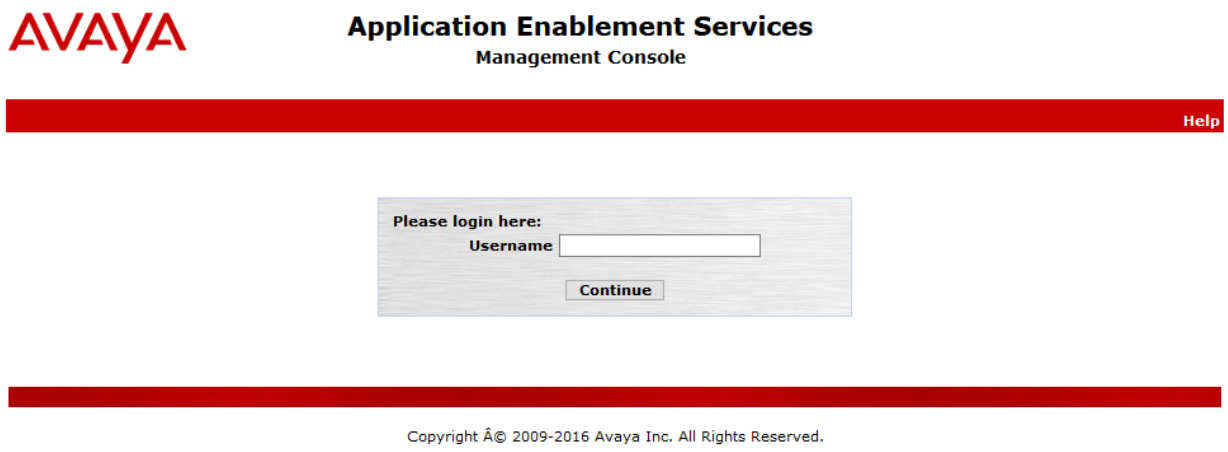
6. Configure Avaya Aura® Application Enablement Services

This section provides the procedure for configuring AES. The procedures include the following areas:

- Launch OAM interface
- Administer the Switch Connection
- Administer TSAPI Link
- Administer User
- Obtain Tlink

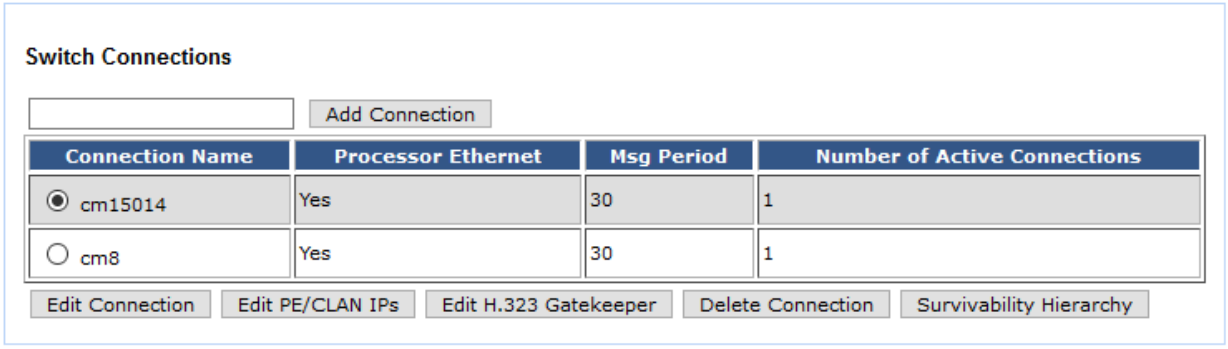
6.1. Launch OAM interface

Access the AES OAM web interface using the URL https://<AES_IP_Address> and log on using appropriate credentials.

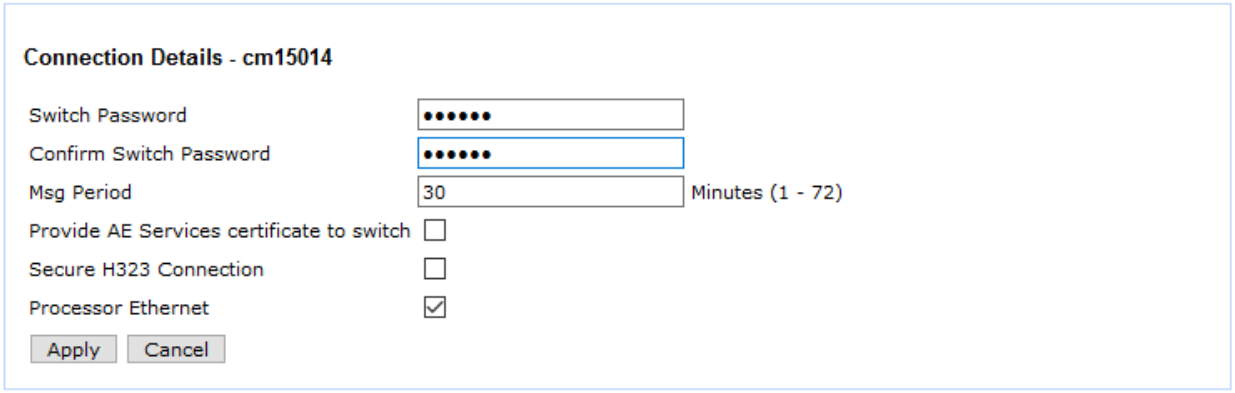


6.2. Administer Switch Connection

To administer a Switch Connection for Communication Manager, navigate to the **Communication Manager Interface → Switch Connections** page and enter a name for the new switch connection and click the **Add Connection** button. This was previously configured as **cm15014** for this test environment:



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



Use the **Edit PE/CLAN IPs** button (shown in this section's first screen shot above) to configure the **procr** or **CLAN** IP Address (es) of Communication Manager from **Section 5.1**.

6.3. Administer TSAPI Link

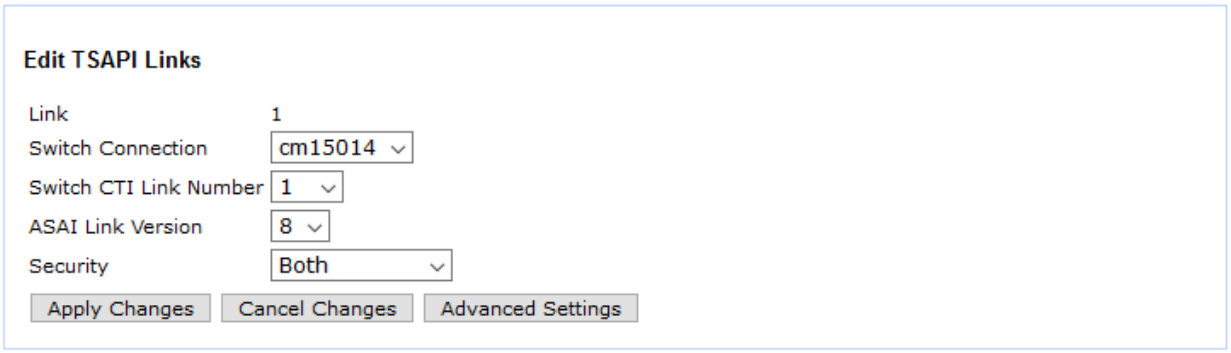
Navigate to the **AE Services → TSAPI → TSAPI Links** page to add the TSAPI CTI Link. Click **Add Link** (not shown).

Select a **Switch Connection** using the drop down menu. Select the **Switch CTI Link Number** using the drop down menu. The **Switch CTI Link Number** must match the number configured in the **cti-link** form for Communication Manager.

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

Click **Apply Changes**.

Configuration shown below was previously configured.



6.4. Administer User

A user needs to be created for MH-CURE to communicate with AES. Navigate to **User Management → User Admin → Add User**.

Fill in **User Id, Common Name, Surname, User Password** and **Confirm Password** and set the **CT User** to **Yes,** and click **Apply** (not shown).

Add User

Fields marked with * can not be empty.

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

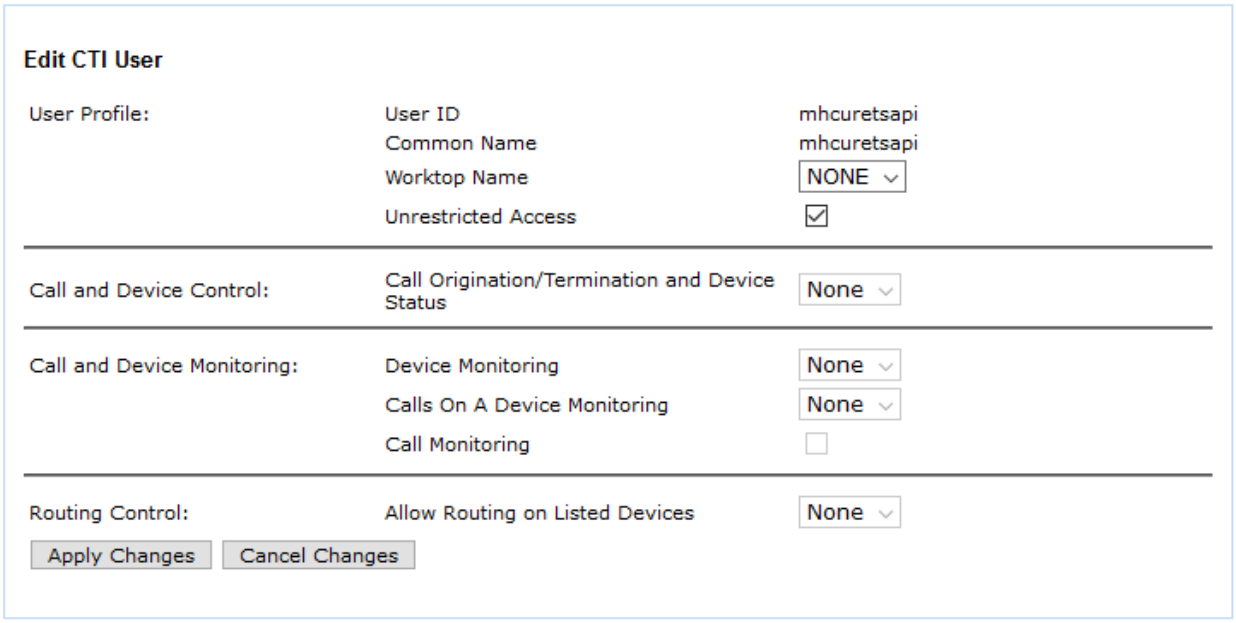
Navigate to **Security → Security Database → CTI Users → List All Users**.

CTI Users

User ID	Common Name	Worktop Name	Device ID
○ interop	interop	NONE	NONE
◉ mhcuretsapi	mhcuretsapi	NONE	NONE
○ tailitu	tailitu	NONE	NONE

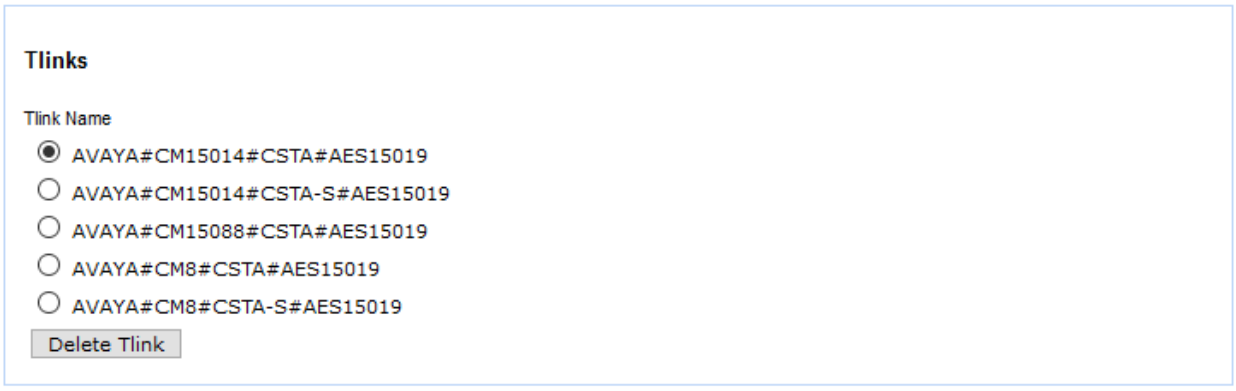
Edit List All

Select the recently added user and click **Edit**. Check the box for **Unrestricted Access** and click **Apply Changes**.



6.5. Obtain Tlink

Obtain the Tlink that will be used by MH-CURE to connect to AES. Continuing from above, select **Tlinks** on the left pane and note that Tlink that will be used by MH-CURE.



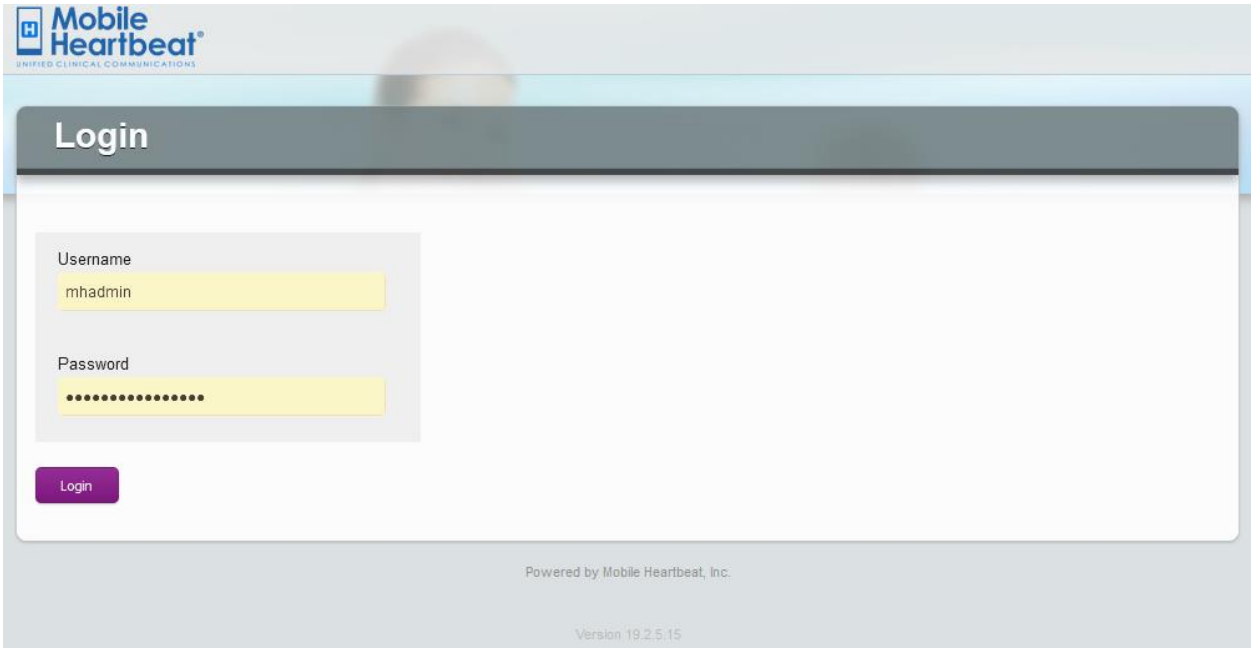
7. Configure Mobile Heartbeat MH-CURE

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

- Log onto MH-CURE web UI
- Administer MH-CURE for AES/TSAPI
- Administer Dynamic Role Numbers
- Administer MH-CURE SIP Clients

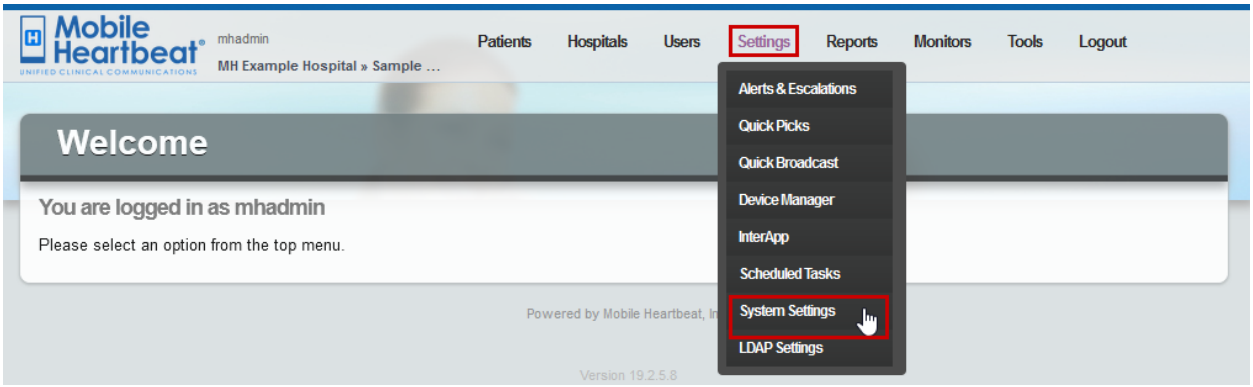
7.1. Log onto MH-CURE web UI

Via a browser, navigate to https://<MH-CURE>/heartbeat/ where MH-CURE is the IP-Address/FQDN and port of the MH-CURE Administrative web UI. Log on using appropriate credentials.

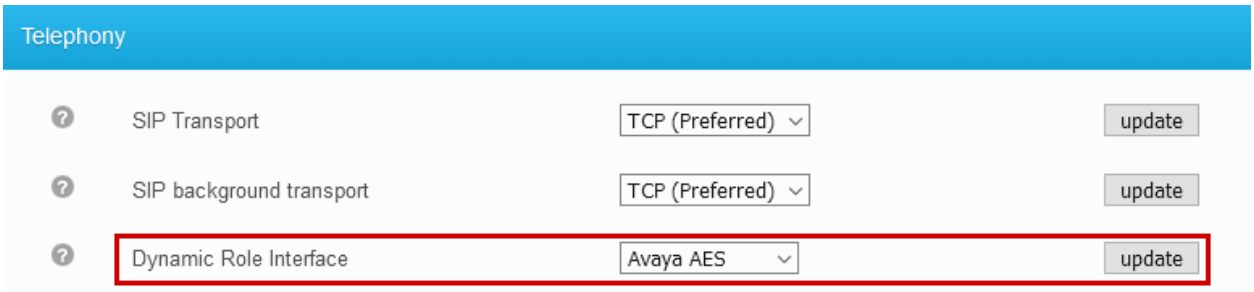


7.2. Administer MH-CURE for AES/TSAPI

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



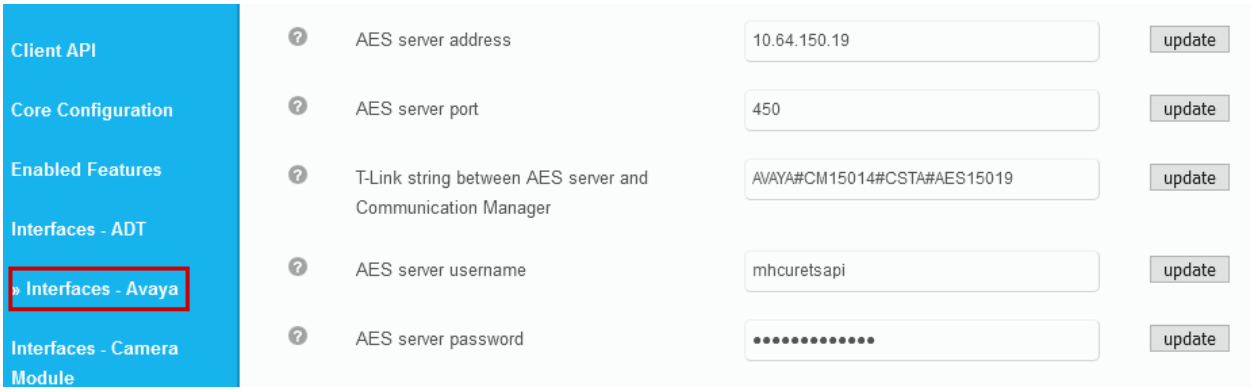
On left side, click **Telephony** (not shown). For **Dynamic Role Interface,** select **Avaya AES** and click **update.**



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

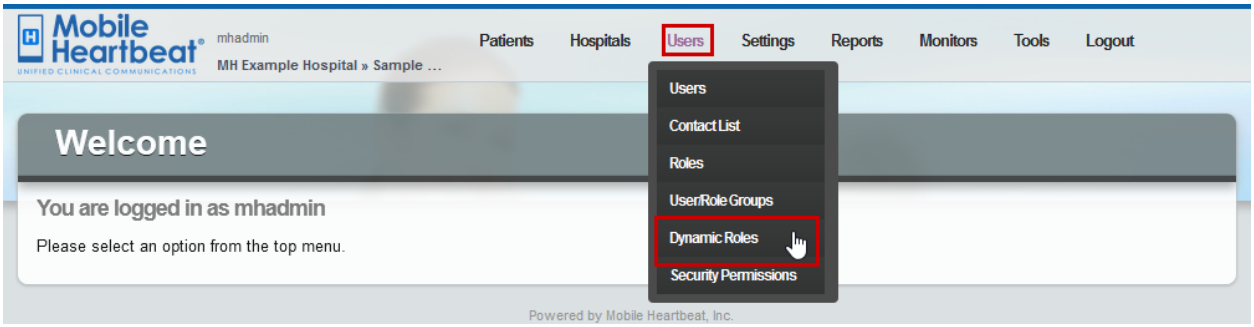
- **AES server address** IP Address of AES.
- **AES server port** Port for AES TSAPI services. Default port 450 is used.
- **T-Link string…Manager** Tlink obtained from **Section 6.5.**
- **AES server username** Username from **Section 6.4.**
- **AES server password** Password from **Section 6.4.**

Though not needed, it is recommended to restart the Tomcat Services on the MH-CURE server.

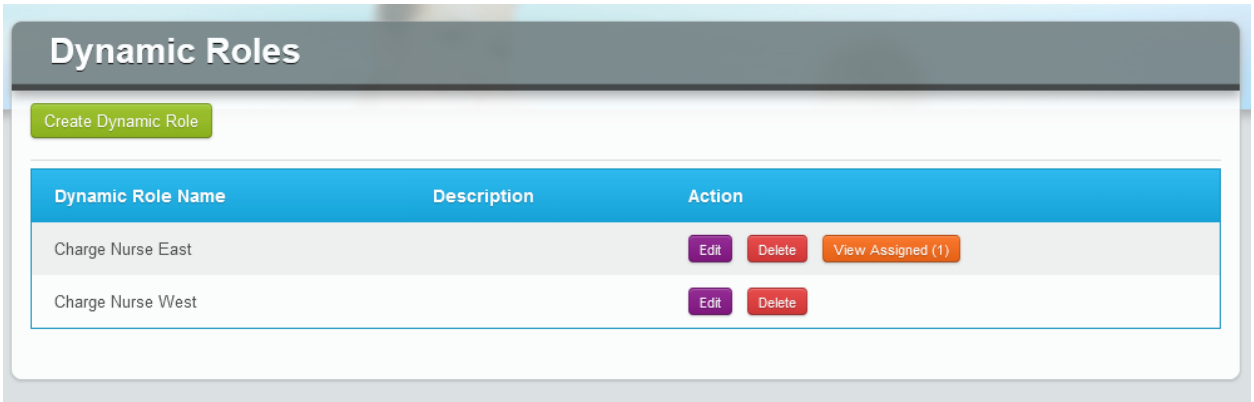


7.3. Administer Dynamic Role Numbers in MH-CURE

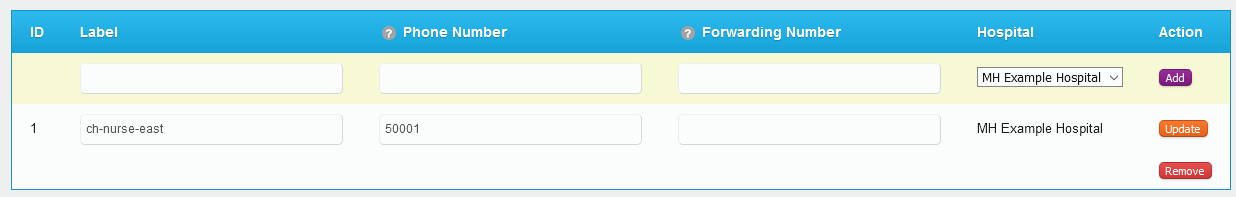
Dynamic Roles with an Extension in MH-CURE needs to match VDN's configured for Vector/Adjunct routing in Communication Manager (**Section 5.4**). Two example roles have been created, "East" and "West", each needs a VDNs configured in **Section 5.4.** From the top, navigate to **Users → Dynamic Roles.**



Select **Edit** to configure a role with a specific VDN.

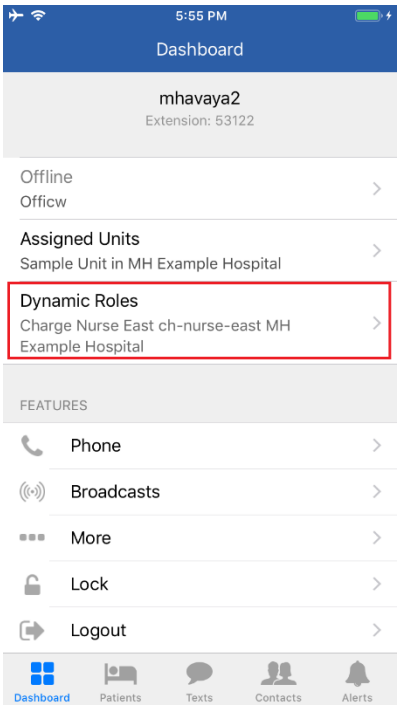


At the bottom of the page, under the **Labels and numbers and associated hospitals** section, type in the VDN in **Phone Number** field. If MH-CURE SIP clients are used, the Dynamic Role can be assigned (enabled) within the MH-CURE SIP client application. When assigned, MH-CURE returns the MH-CURE SIP 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 left blank, no destination number will be returned. If MH-CURE SIP clients are used, Dynamic Role can be enabled as shown in **Section 7.4.** Optionally, any Avaya Endpoint extension can be defined in the **Forwarding Number**, MH-CURE will return the **Forwarding Number** as destination to Communication Manager if no MH-CURE user have been assigned to the role.

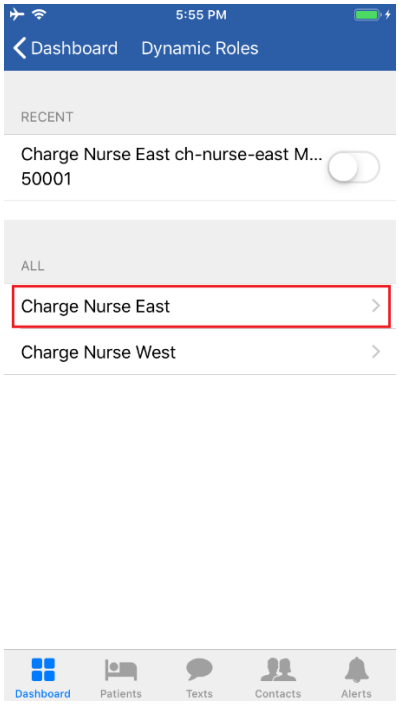


7.4. Administer MH-CURE SIP Clients

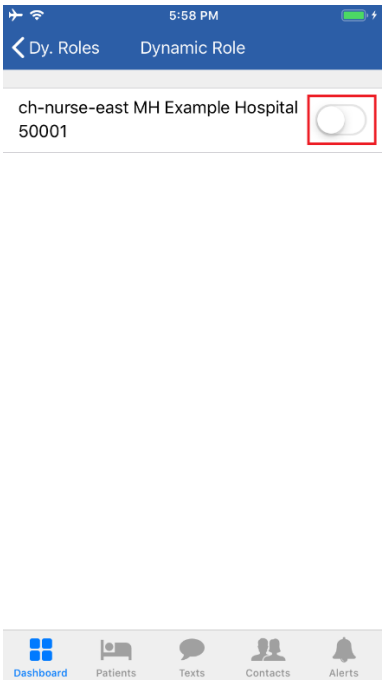
If MH-CURE SIP clients are used, Dynamic Role can be enabled from within the MH-CURE app on a mobile device. Open the MH-CURE app and select **Dynamic Roles.**



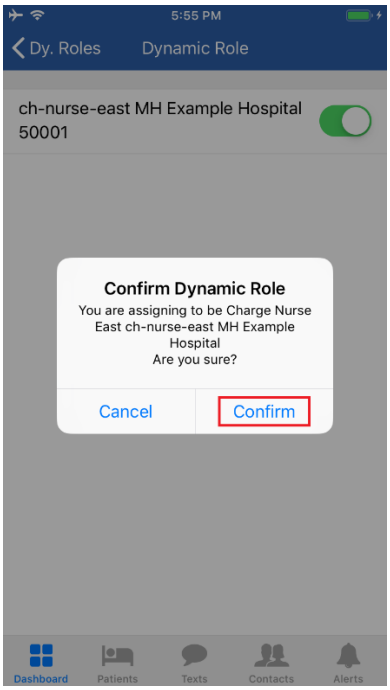
Select a Role that needs to be enabled for the user.

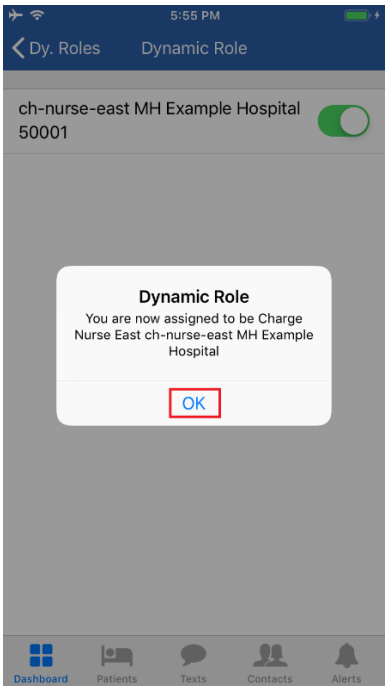


Toggle the switch to enable the role.

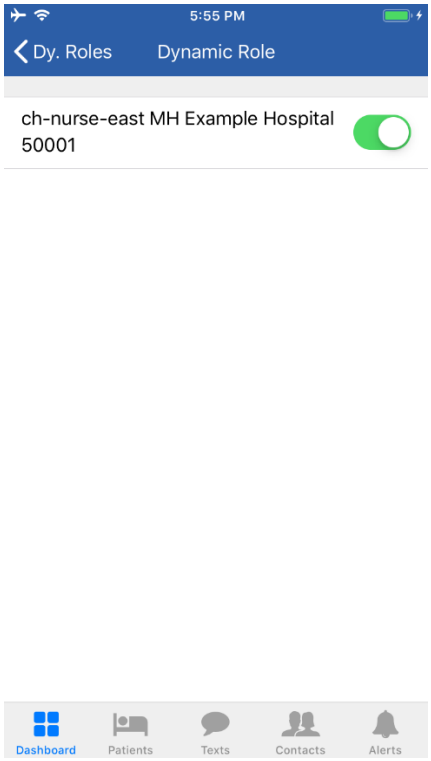


Select **Confirm** followed by **OK.**





Following screen capture displays successful Dynamic Role assignment to the user. When a call is placed to the VDN 50001, MH-CURE returns the current user as a destination and Communication Manager delivers the call to MH-CURE SIP client.



8. Verification Steps

8.1. Verify Avaya Aura® Communication Manager

Via a SAT terminal, verify that AES is enabled and listening using the **status aesvcs interface** command.

```
status aesvcs interface

                          AE SERVICES INTERFACE STATUS

Local Node         Enabled?  Number of     Status
                             Connections

procr              yes       2             listening
```

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

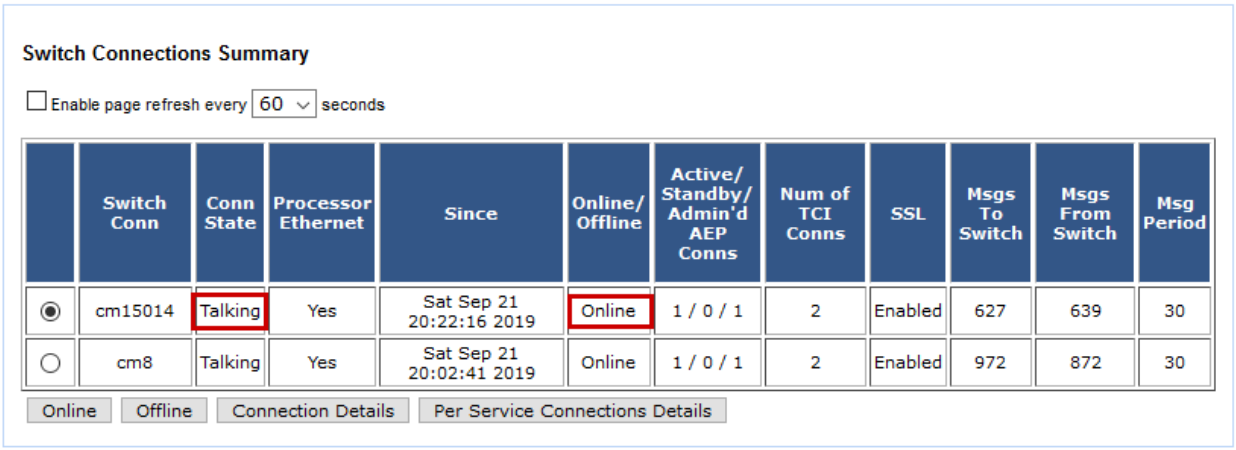
```
status aesvcs link

                           AE SERVICES LINK STATUS

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

01/01  aes15019                          50298   procr           636     626
                       10.64.150.19
```

Verify 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     8        no    aes15019         established   36       31
```

8.2. Verify Avaya Aura® Application Enablement Services

Via AES OAM, navigate to **Status → Status and Control → Switch Conn Summary.** Verify the Switch Connection to Communication Manager is **Talking** and **Online**.



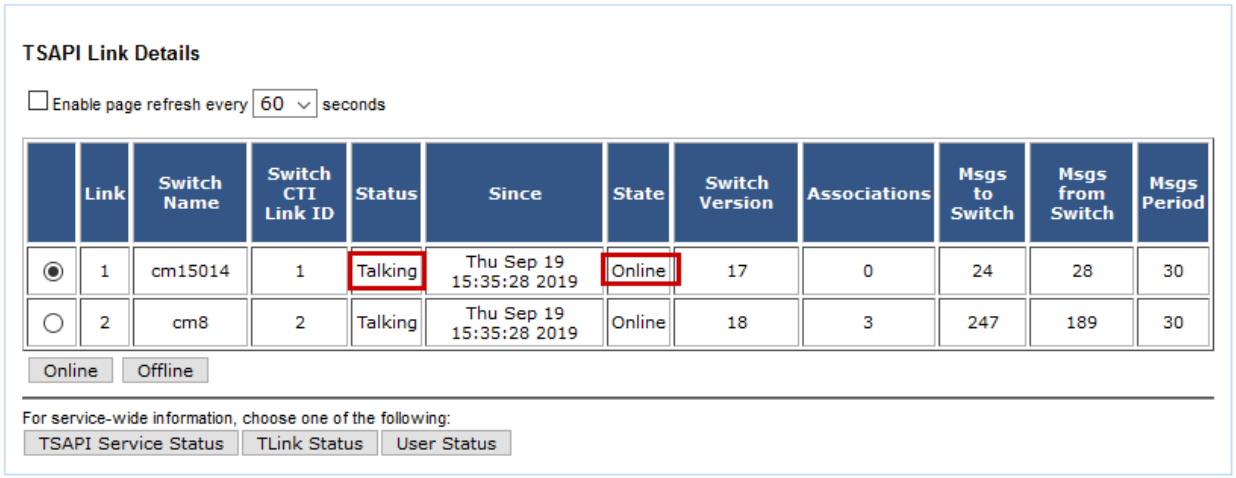
Switch Connections Summary

Enable page refresh every 60 seconds

	Switch Conn	Conn State	Processor Ethernet	Since	Online/ Offline	Active/ Standby/ Admin'd AEP Conns	Num of TCI Conns	SSL	Msgs To Switch	Msgs From Switch	Msg Period
◉	cm15014	Talking	Yes	Sat Sep 21 20:22:16 2019	Online	1 / 0 / 1	2	Enabled	627	639	30
○	cm8	Talking	Yes	Sat Sep 21 20:02:41 2019	Online	1 / 0 / 1	2	Enabled	972	872	30

Online | Offline | Connection Details | Per Service Connections Details

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



TSAPI Link Details

Enable page refresh every 60 seconds

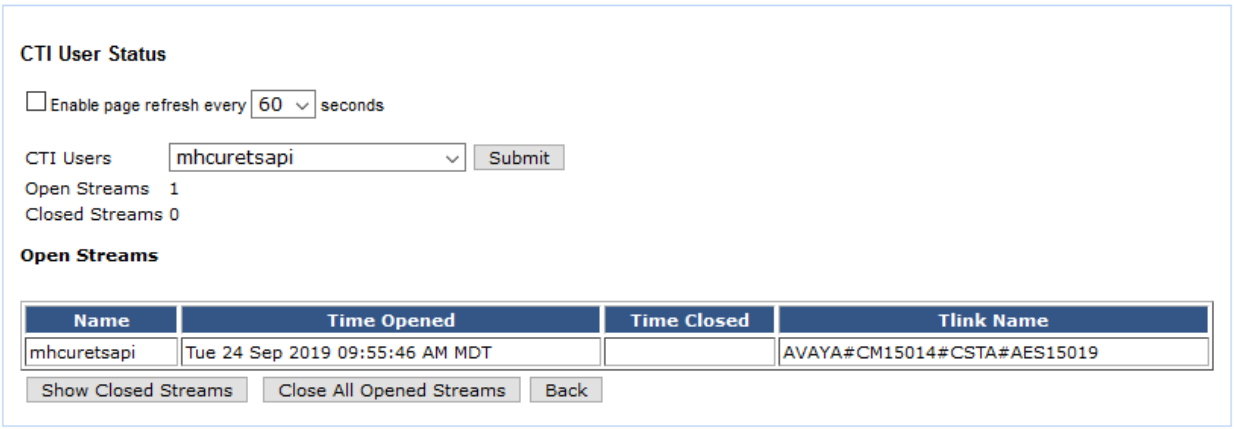
	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
◉	1	cm15014	1	Talking	Thu Sep 19 15:35:28 2019	Online	17	0	24	28	30
○	2	cm8	2	Talking	Thu Sep 19 15:35:28 2019	Online	18	3	247	189	30

Online | Offline

For service-wide information, choose one of the following:

TSAPI Service Status | TLink Status | User Status

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



9. Conclusion

Mobile Heartbeat MH-CURE was able to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All executed test cases were passed with the exception mentioned **Section 2.2**.

10. Additional References

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

[1] Administering Avaya Aura® Communication Manager, Release 7.1.3, Issue 78, August 2019

[2] Administering and Maintaining Avaya Aura® Application Enablement Services, Release 7.1.3, Issue 6, August 2019

Documentation related to MH-CURE can be directly obtained from Mobile Heartbeat.

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.