Avaya Solution & Interoperability Test Lab

Application Notes for the Spok PC/PSAP, utilizing Spok CTI Layer, with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe a compliance-tested configuration comprised of Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services, Avaya H.323 and Digital Telephones, and Spok PC/PSAP desktop applications.

Spok PC/PSAP is a Windows-based intelligent E911 workstation solution for a campus or municipality. Using the existing PBX telephone system as an "Automatic Number Identification (ANI)/Automatic Location Information (ALI) controller", Spok PC/PSAP eliminates the need for external proprietary switching solutions and is able to perform all necessary telephony functions from the call taker's PC keyboard. Spok PC/PSAP integrates with Spok CTI Layer, which is a middleware between Spok PC/PSAP and Avaya Aura® Application Enablement Services, to control and monitor phone states.

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.

©2019 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe a compliance-tested configuration comprised of Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services, Avaya H.323 and Digital telephones, and Spok PC/PSAP applications.

Spok PC/PSAP is a PC and LAN based system used in a PSAP (Public Safety Answering Position – a physical location where 911 emergency telephone calls are received and then routed to the proper emergency services by the security agent or "911 operator" at the PSAP). Campuses or municipalities can set up a public or private PSAP using Spok PC/PSAP, which has the capabilities to extract ANI (Automatic Number Identification – phone number of the caller) from Emergency 911 trunks and retrieve corresponding ALI (Automatic Location Information – information about the call based on the ANI such as name, phone number, address, nearest cross street, etc.). Spok PC/PSAP integrates with Spok CTI Layer, which is a middleware between Spok PC/PSAP and Avaya Aura® Application Enablement Services, to control and monitor phone states.

It is the Spok CTI Layer service that actually uses the Avaya Aura® Application Enablement Services Device and Media Call Control (DMCC) Application Programming Interface (API) to share control of and monitor a physical telephone and receive the same terminal and first party call information received by the physical telephone. Spok PC/PSAP in turn uses the Spok CTI Layer service to control and monitor a physical telephone. Spok PC/PSAP registers as a DMCC station for Avaya H.323 or Avaya Digital endpoint configured on Communication Manager. The PC/PSAP applications regularly provide the database server with call and lamp state information concerning the controlled telephones.

2. General Test Approach and Test Results

The general approach was to exercise basic telephone and call operations on Avaya H.323 and Digital telephones using the aforementioned Spok desktop application.

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.

©2019 Avaya Inc. All Rights Reserved.

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 Spok made use of secure DMCC.

2.1. Interoperability Compliance Testing

The interoperability compliance test included features and serviceability. The focus of the compliance test was primarily on verifying the interoperability between Spok PC/PSAP, Application Enablement Services, and Communication Manager. The main objectives were to verify that:

- The user may successfully use PC/PSAP to perform off-hook, on-hook, dial, answer, hold, retrieve, transfer, conference, and release operations on the physical telephone.
- Call from PC/PSAP to/from Avaya Endpoints (SIP, H.323 and Digital) and PSTN.
- The agent user may successfully use PC/PSAP to log into and out of an ACD, and move between agent work modes.
- Manual operations performed on the physical telephone are correctly reflected in the PC/PSAP GUI.
- PC/PSAP and manual telephone operations may be used interchangeably; for example, go off-hook using PC/PSAP and manually dial digits.
- Display and call information on the physical telephone is accurately reflected in the PC/PSAP GUI.
- Call states are consistent between PC/PSAP and the physical telephone.

Serviceability testing such as network failure and server reset for Spok PC/PSAP was also performed.

2.2. Test Results

All test cases were executed and passed with the exception of the observations below:

- During a scenario where the network connection from Spok PC/PSAP is lost, the CTI service on Spok PC/PSAP needed to be manually restarted to register the DMCC station again.
- Spok PC/PSAP does not support SIP endpoints configured on Communication Manager because it uses DMCC "Dependent" mode for device registrations, which is not supported for SIP telephones through the DMCC API.

2.3. Support

Technical support for the Spok PC/PSAP solution can be obtained by contacting Spok:

- URL – http://www.spok.com
- Phone – +1 (888) 797-7487

©2019 Avaya Inc. All Rights Reserved.

3. Reference Configuration

Figure 1 illustrates the configuration used in these Application Notes. The sample configuration shows an enterprise with an Application Enablement Services, Communication Manager, Media Server with an Avaya G450 Media Gateway. The PC/PSAP is configured to be in the same network as the enterprise. Endpoints include Avaya 9600 Series SIP, H.323 and Digital Telephones.

Note: Basic administration of Communication Manager and Application Enablement Services server is assumed. For details, see [1] and [2].

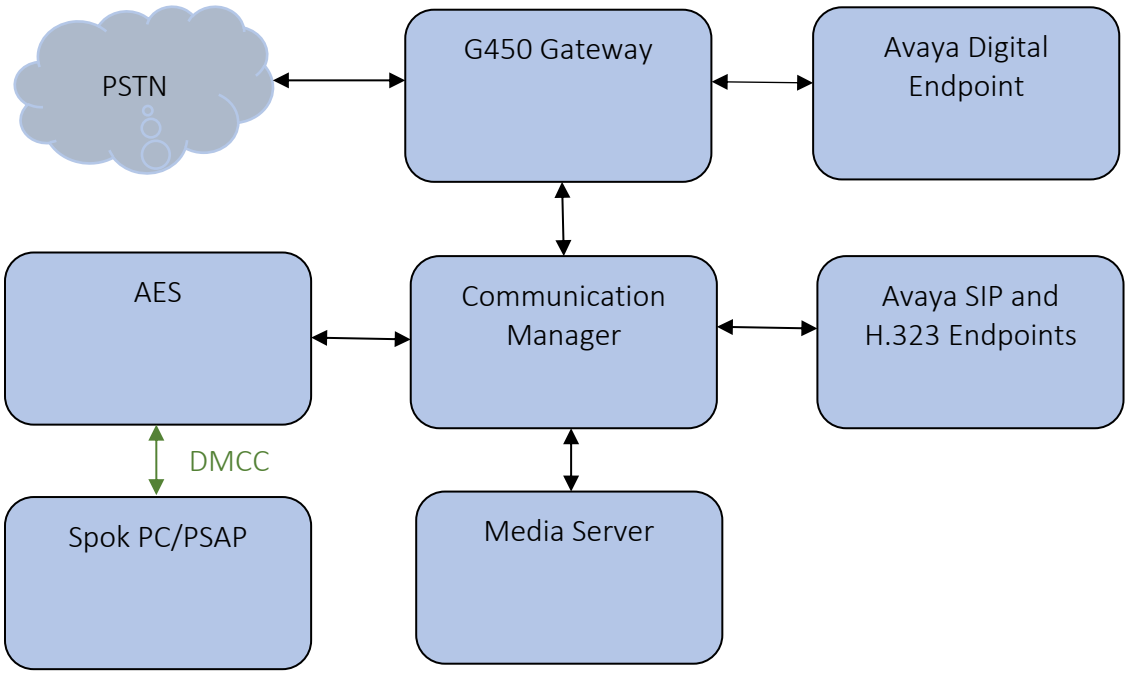


Figure 1: Spok PC/PSAP Test Configuration.

©2019 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya Aura® Communication Manager	8.0.1.1.0.822.25183
Avaya Aura® Application Enablement Services	8.0.1.0.2.5-0
Avaya Aura® Media Server	8.0.0.183
Avaya G450 Media Gateway	40.20.1
Avaya 9600 Series IP Telephones (H.323) • 96x1 H.323 • 96x1 SIP	 • 6.8102 • 7.1.5.0
Avaya 9404 Digital Endpoint	2.0 SP8
Spok CTI Layer	7.x (7.0.0.6)
Spok PC/PSAP	11.x (11.11.0.404)

©2019 Avaya Inc. All Rights Reserved.

5. Configure Avaya Aura® Communication Manager

This section describes the procedures for configuring IP Services, Feature Access Codes, Abbreviated Dialing, and controlled telephones.

5.1. Configure IP Services

Enter the **change node-names ip** command. In the compliance-tested configuration, the procr IP address was used for registering H.323 endpoints, and for connectivity to Application Enablement Services.

```
change node-names ip
                                IP NODE NAMES
    Name                  IP Address
aes15019                10.64.150.19
aes8                    10.64.110.132
ams8                    10.64.110.136
cms18                   10.64.110.20
default                 0.0.0.0
egw1                    10.64.110.200
egw2                    10.64.110.201
procr                   10.64.110.131
procr6                  ::
sm8                     10.64.110.135
```

Enter the **change ip-services** command. On **Page 1**, configure the Service Type field to **AESVCS** and the Enabled field to **y**. The Local Node field should be pointed to the **procr** that was configured previously in the IP NODE NAMES form in this section. During the compliance test, the default port was used for the Local Port field.

```
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**, enter the hostname of the Application Enablement Services server for the AE Services Server field. The server name may be obtained by logging in to the Application Enablement Services server using ssh, and running the command **uname –a**. Enter an alphanumeric password for the Password field. Set the Enabled field to **y**. The same password will be configured on the Application Enablement Services server in **Section 6.2**.

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

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:       aes8               *                   y        in use
      2:
```


©2019 Avaya Inc. All Rights Reserved.

5.2. Configure Feature Access Codes (FAC)

Enter the **change feature-access-codes** command. On **Page 1** of the FEATURE ACCESS CODE (FAC) form, verify the **Auto Route Selection (ARS) – Access Code 1** field is set to **9**.

```
change feature-access-codes                                    Page   1 of  11
                            FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                       Answer Back Access Code: #25
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA: *97    All: *99    Deactivation: *98
```

5.3. Configure Dialplan

Enter the **change dialplan analysis** command. Create a single digit dial string with **9** and associate it with **Feature Access Code (fac)**.

```
change dialplan analysis                                       Page   1 of  12
                           DIAL PLAN ANALYSIS TABLE
                                 Location: all            Percent Full: 1

    Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
    String   Length Type     String   Length Type     String   Length Type
   1           3   dac
   1           4   ext
   1           5   ext
   3           10  ext
   8           1   fac
   9           1   fac
   *           3   dac
   #           3   dac
```


©2019 Avaya Inc. All Rights Reserved.

5.4. Configure Hunt Group

Enter the **add hunt-group n** command, where **n** is an unused hunt group number. On **Page 1** of the HUNT GROUP form, assign a descriptive Group Name and Group Extension valid in the provisioned dial plan. Set **ACD**, **Queue** and **Vector** to **y**.

```
add hunt-group 1                                              Page   1 of   4
                                  HUNT GROUP

            Group Number: 1                                 ACD? y
              Group Name: Skill 1                         Queue? y
         Group Extension: 59001                          Vector? y
              Group Type: ucd-mia
                      TN: 1
                     COR: 1                    MM Early Answer? n
           Security Code:                Local Agent Preference? n
 ISDN/SIP Caller Display:

             Queue Limit: unlimited
 Calls Warning Threshold:      Port:
  Time Warning Threshold:      Port:
```

5.5. Configure Abbreviated Dialing

Enter the **add abbreviated-dialing system** command. In the **DIAL CODE** list, enter the Feature Access Codes for ACD Login and Logout.

```
change abbreviated-dialing system                              Page   1 of   1
                         ABBREVIATED DIALING LIST
                                 SYSTEM LIST

Size (multiple of 5): 5       Privileged? n     Label Language:english
DIAL CODE                              LABELS (FOR STATIONS THAT DOWNLOAD LABELS)
     01: *01                                 01: Log-in
     02: *06                                 02: Log-out
     03:                                     03: *************
     04:                                     04: *************
     05:                                     05: *************
```


©2019 Avaya Inc. All Rights Reserved.

5.6. Configure Controlled Telephones

Enter the **change station r** command, where **r** is the extension of a registered, physical Avaya H.323 or Digital telephone. On **Page 1** of the **station** form, enter a phone Type, descriptive name, Security Code and set **IP SoftPhone** field to **y** to allow the physical station to be controlled by a softphone such as the Spok PC/PSAP application.

```
change station 57001                                          Page   1 of   5
                                    STATION

Extension: 57001                        Lock Messages? n               BCC: 0
     Type: 9641                         Security Code: *                TN: 1
     Port: S00039                     Coverage Path 1:                 COR: 1
     Name: Spok PCPSAP 1              Coverage Path 2:                 COS: 1
Unicode Name? n                     Hunt-to Station:                Tests? y
STATION OPTIONS
                                          Time of Day Lock Table:
             Loss Group: 19          Personalized Ringing Pattern: 1
                                       Message Lamp Ext: 57001
           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
```


©2019 Avaya Inc. All Rights Reserved.

On **Page 4** of the station form, for **ABBREVIATED DIALING List 1**, enter the abbreviated dialing group configured in previous section. On **Pages 4**, **5**, and **6** of the station forms, configure the following BUTTON ASSIGNMENTS in addition to the call-appr (call appearance) buttons as shown below:

```
change station 57001                                          Page   4 of   5
                                    STATION
 SITE DATA
      Room:                                            Headset? n
      Jack:                                            Speaker? n
     Cable:                                           Mounting: d
     Floor:                                       Cord Length: 0
   Building:                                        Set Color:

ABBREVIATED DIALING
     List1: system              List2:                    List3:




BUTTON ASSIGNMENTS
 1: call-appr                           5: call-pkup
 2: call-appr                           6: next
 3: brdg-appr  B:1 E:57002              7: aux-work    RC:    Grp:
 4: brdg-appr  B:1 E:57003              8: auto-in             Grp:

change station 11054                                           Page   5 of   7
                                    STATION

BUTTON ASSIGNMENTS

 9: abrv-dial  List: 1 DC: 01    HL? n
10: abrv-dial  List: 1 DC: 02    HL? n
11: release
12: togle-swap

change station 57001                                          Page   5 of   5
                                    STATION

BUTTON ASSIGNMENTS

 9: abrv-dial  List: 1 DC: 01
10: abrv-dial  List: 1 DC: 02
11: release
12: togle-swap
13:
14:
15:
16:
17: q-calls    Grp: 2
```

Repeat the instructions provided in this section for each physical station that is to be controlled / monitored by the Spok CTI Layer.

©2019 Avaya Inc. All Rights Reserved.

6. Configure Application Enablement Services

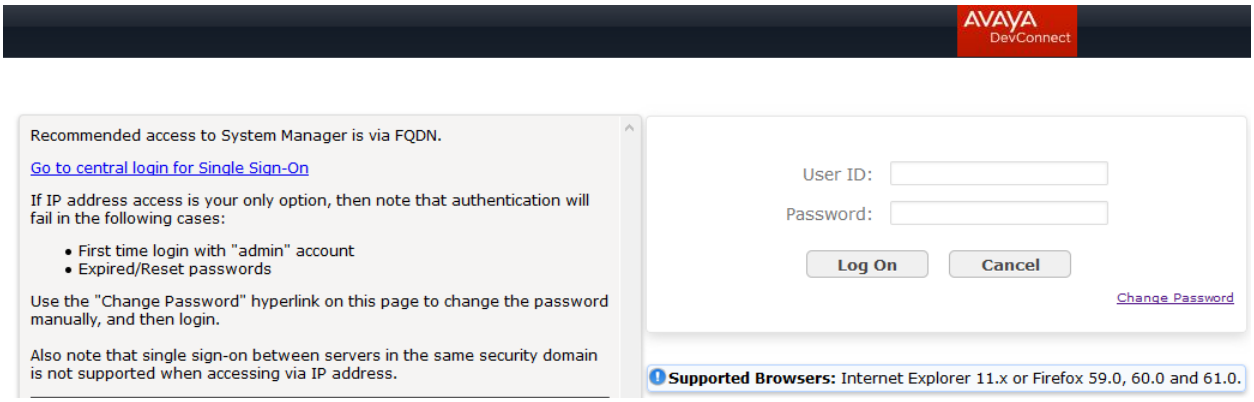
The Application Enablement Services server enables Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Communication Manager.

This section assumes that installation and basic administration of the Application Enablement Services server has been performed. The steps in this section describe the configuration of a Switch Connection, a CTI user, a DMCC port.

6.1. Device and Media Call Control API Station Licenses

The Spok PC/PSAP Service instances appear as "virtual" stations/softphones to Communication Manager. Each of these virtual stations, hereafter called Device and Media Call Control API station, requires a license. Note that this is separate and independent of Avaya IP Softphone licenses, which are required for Avaya IP Softphones but not required for Device and Media Call Control API stations. To check and verify that there are sufficient DMCC licenses, log in to https://<IP address of the Application Enablement Services server>/index.jsp, and enter appropriate login credentials to access the Application Enablement Services Management Console page.
Select the **Licensing → WebLM Server Access** link from the left pane of the window (not shown). During the compliance testing, Avaya Aura System Manager was used as a license server.

Provide appropriate login credentials and log in.

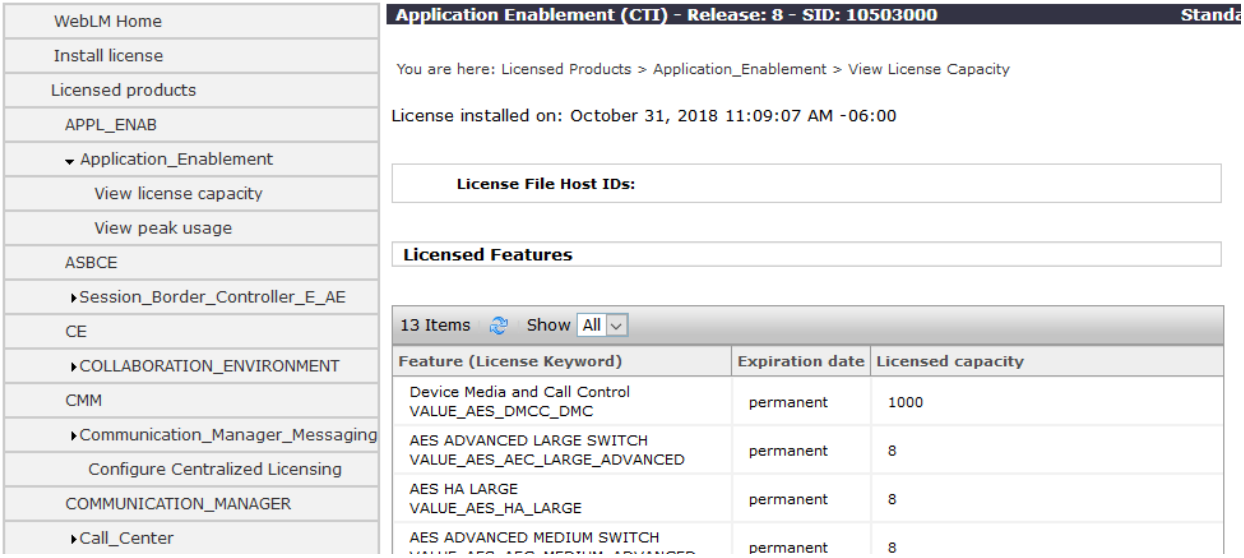


©2019 Avaya Inc. All Rights Reserved.

Navigate to **Home → Services → Licenses.** On the WebLM Home page, select **License Products → Application_Enablement** link from the left pane of the window.

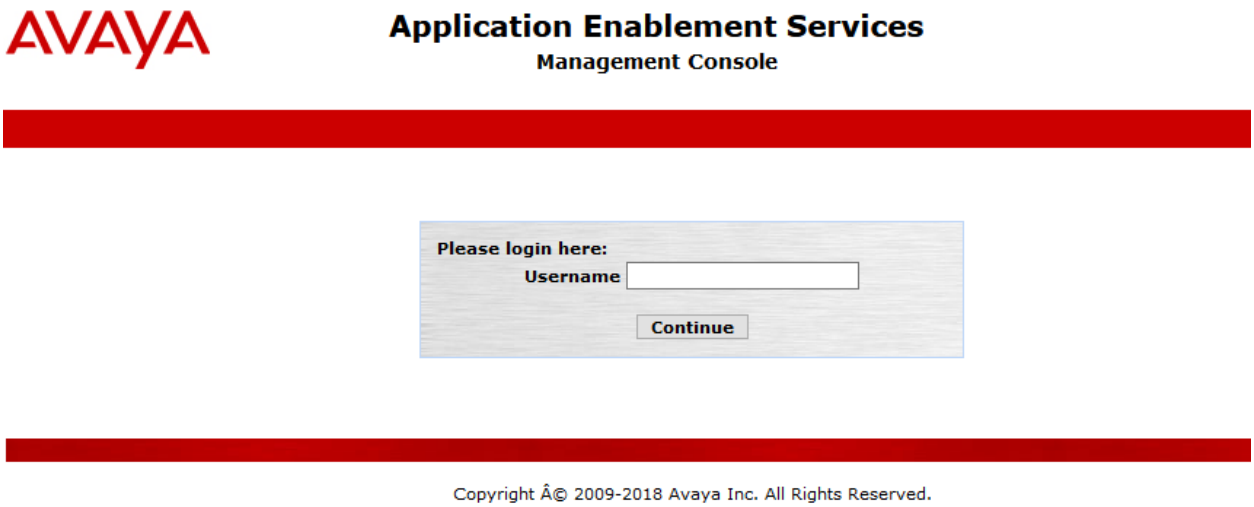
On the Licensed Features page, verify that there are sufficient DMCC licenses.

Note: TSAPI licenses (1 per agent station) are also required if calls routed to agent stations via ACD. Without TSAPI licenses, the agents will not see the First Party Call Control (1PCC) calling party information. i.e., Calling Party Number.



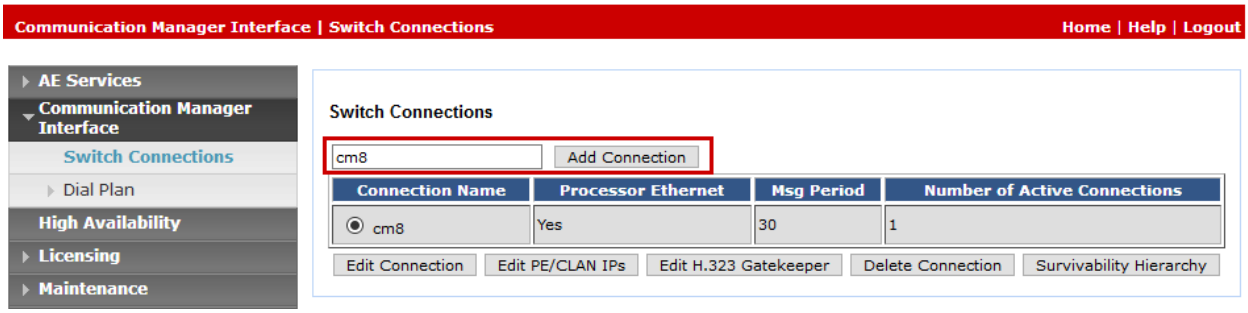
6.2. Configure Switch Connection

Launch a web browser, enter https://<IP address of the Application Enablement Services server> in the address field, and log in with the appropriate credentials for accessing the Application Enablement Services Management Console pages.

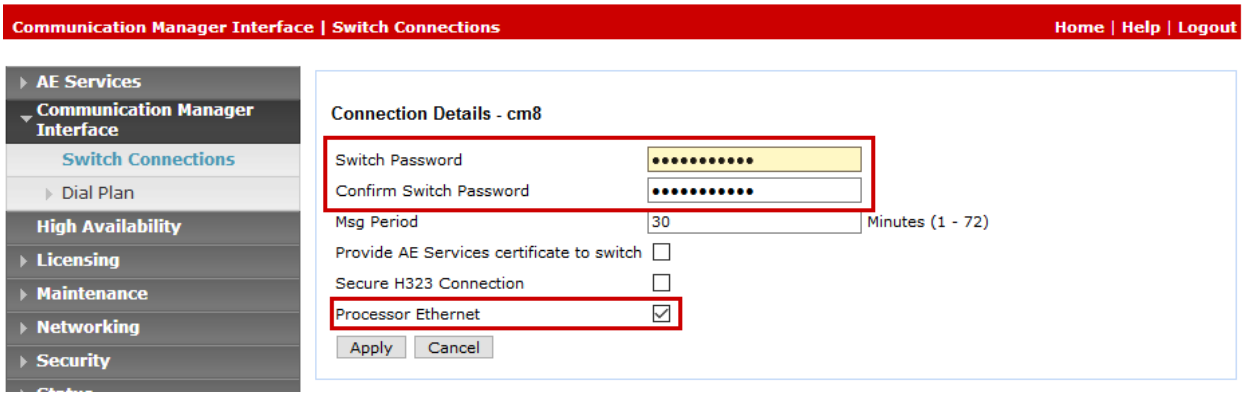


©2019 Avaya Inc. All Rights Reserved.

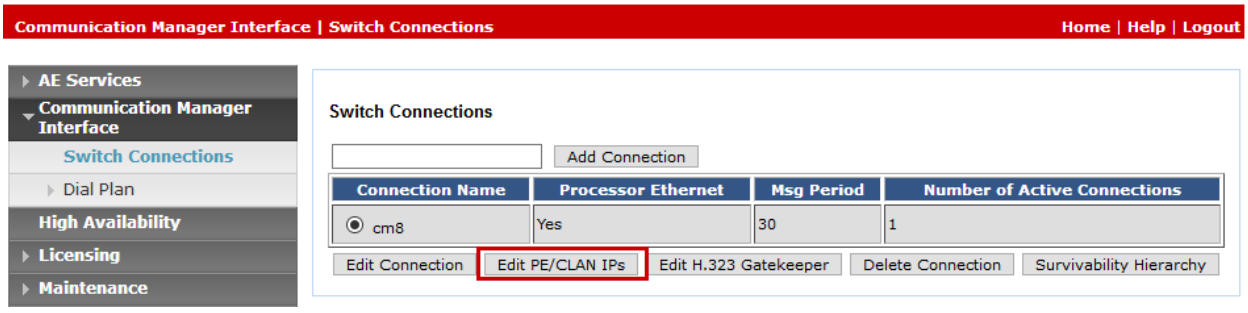
Click on **Communication Manager Interface → Switch Connection** in the left pane to invoke the Switch Connections page. A Switch Connection defines a connection between the Application Enablement Services and Communication Manager. Enter a descriptive name for the switch connection and click on **Add Connection**.



The next window that appears prompts for the **Switch Password**. Enter the same password that was administered in Communication Manager in **Section 5.1**. Check box for **Processor Ethernet**. Click on **Apply**.



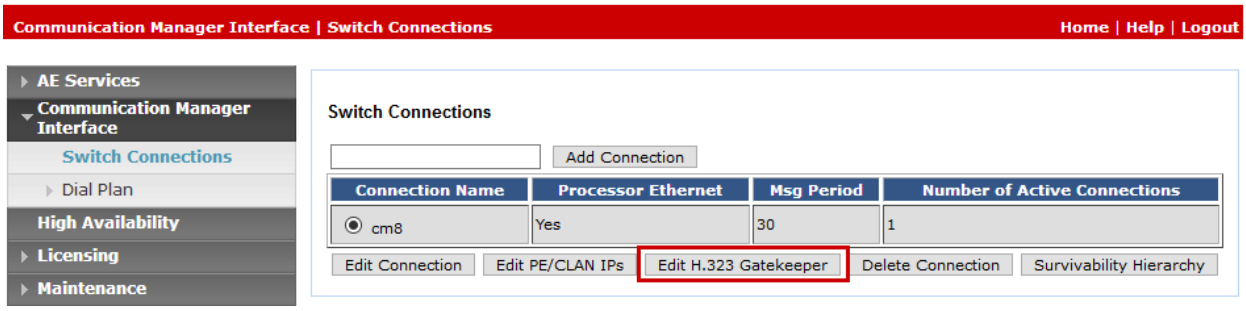
After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on **Edit PE/CLAN IPs**.



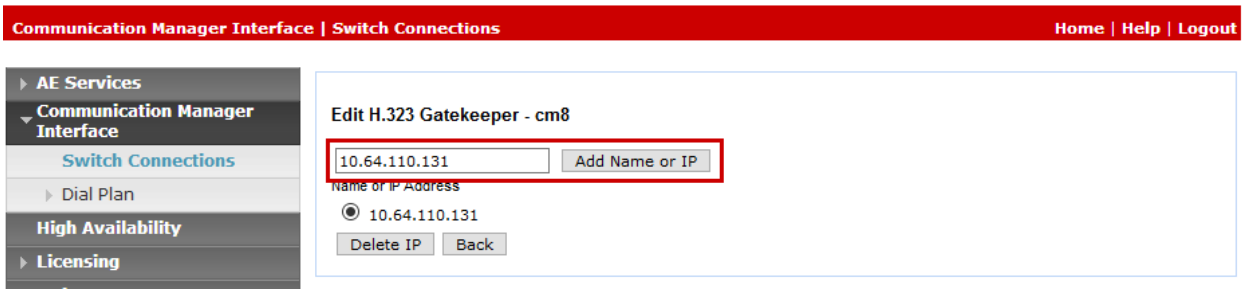
©2019 Avaya Inc. All Rights Reserved.

Enter the IP address of Procr used for Application Enablement Services connectivity from **Section 5.1**, and click on **Add Name or IP**.

After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on the **Edit H.323 Gatekeeper** button.



On the **Edit H.323 Gatekeeper – acm** page, enter the procr IP address which will be used for the DMCC service. Click on **Add Name or IP**.



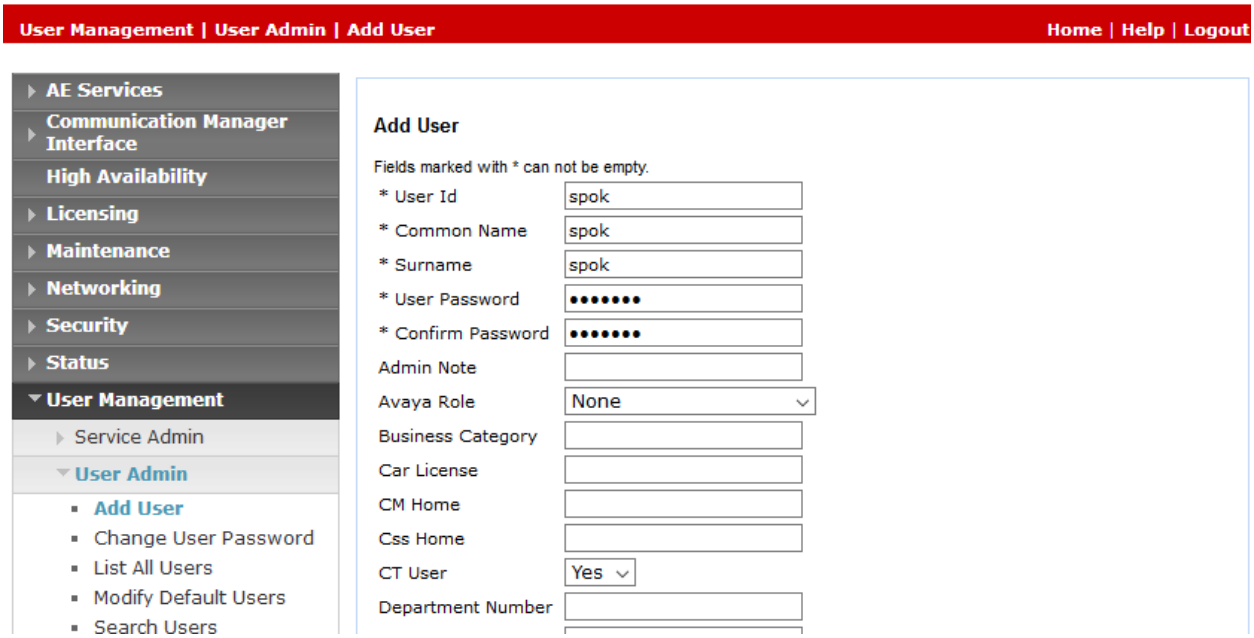
©2019 Avaya Inc. All Rights Reserved.

6.3. Configure the CTI Users

Navigate to **User Management → User Admin → Add User** link from the left pane of the window. On the Add User page, provide the following information:

- User Id
- Common Name
- Surname
- User Password
- Confirm Password

Select **Yes** using the drop-down menu on the CT User field. This enables the user as a CTI user. Default values may be used in the remaining fields. Click the **Apply** button (not shown) at the bottom of the screen to complete the process.

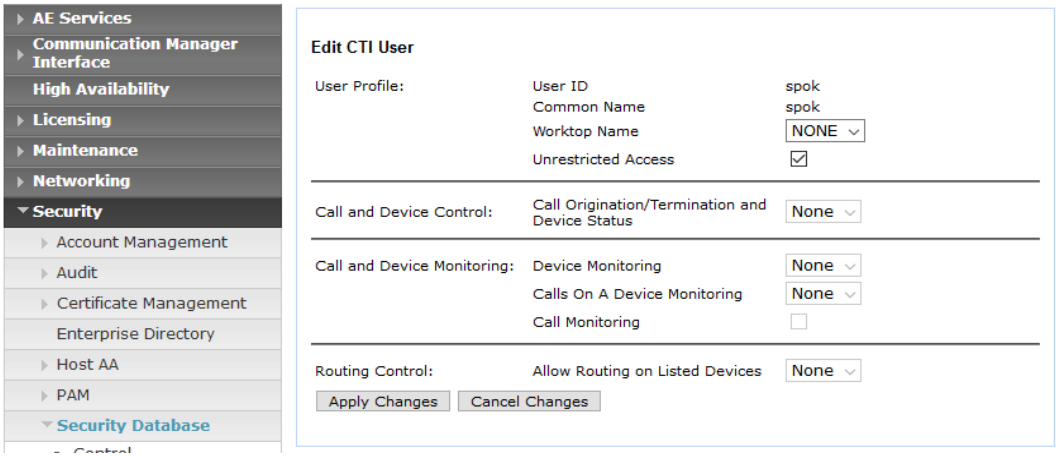


The above information (User ID and User Password) must match with the information configured in the Spok PC/PSAP Configuration page in **Section 7**.

©2019 Avaya Inc. All Rights Reserved.

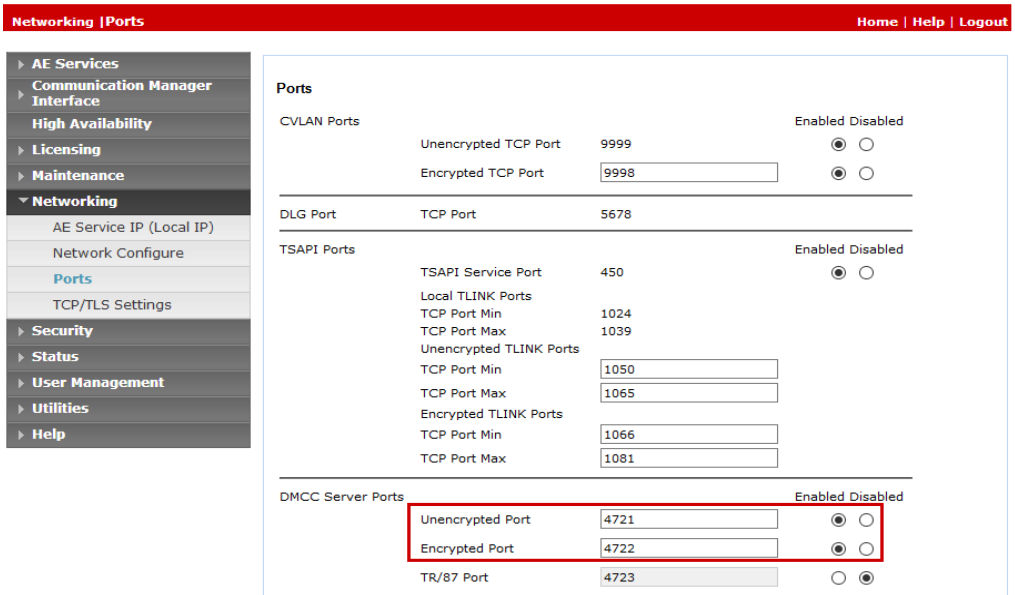
Once the user is created, navigate to the **Security → Security Database → CTI Users → List All Users** link from the left pane of the window. Select the User ID created previously, and click the **Edit** button to set the permission of the user (not shown).

Provide the user with unrestricted access privileges by checking the **Unrestricted Access** checkbox. Click on the **Apply Changes** button.



6.4. Configure the DMCC Port

Navigate to the **Networking → Ports** link, from the left pane of the window, to set the DMCC server port. During the compliance test, the default port values were utilized. The following screen displays the default port values. Since the unencrypted port was utilized during the compliance test, set the Unencrypted Port field to **Enabled**. Default values may be used in the remaining fields. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process.



©2019 Avaya Inc. All Rights Reserved.

7. Configure Spok PC/PSAP

Spok installs, configures, and customizes the PC/PSAP applications for their end customers. Spok PC/PSAP integrates with Spok CTI Layer, which is a middleware between Spok PC/PSAP and Application Enablement Services, to control and monitor the phone states. Thus, only the Spok CTI layer will be discussed in these Application Notes.

Note: Avaya phones as the network supplier for the agent workstations is not supported by Spok. Agent workstations should have their own network connection, separate from Avaya phones.

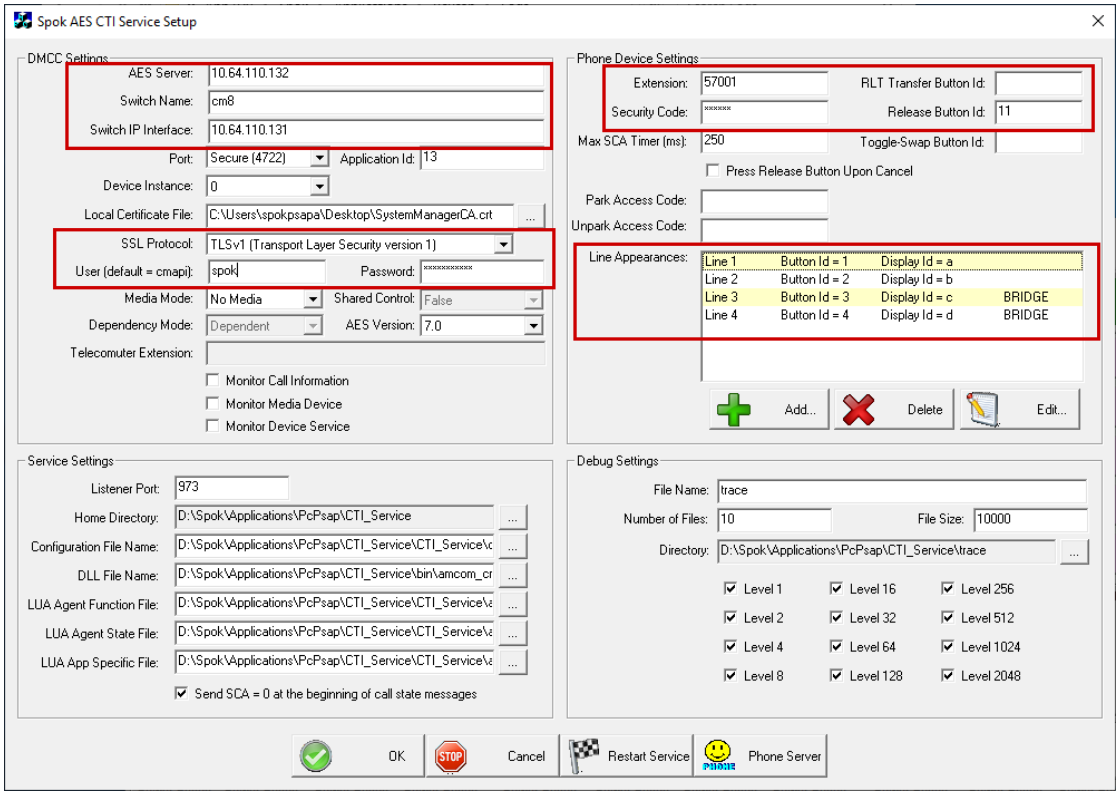
The following shows the **Spok AES CTI Services Setup** page. Provide the following information:

Under DMCC Settings

- **AES Server** – Enter the IP address of the Application Enablement Service.
- **Switch IP Address** – Enter the procr IP address of Communication Manager.
- **Port** – Enter the DMCC port (4721).
- **User** – Enter the user name created for Spok PC/PSAP in **Section 6.3**.
- **Password** – Enter the password created for Spok PC/PSAP in **Section 6.3**.

Under Phone Device Settings

- **Extension** –Enter the extension that will be controlled by the Spok PC/PSAP.
- **Security Code** – Enter the security code for the controlled station.
- **Release Button** – Enter the Release button assigned for the controlled station.
- **Line Appearances** – Enter the line appearances used for the controlled station.



©2019 Avaya Inc. All Rights Reserved.

8. Verification Steps

The following steps may be used to verify the configuration:

- From the Spok client computers, ping IP interfaces, in particular the Application Enablement Services server, and verify connectivity.
- For the physical IP telephones, verify that the physical telephones are registered by using the **list registered-ip-stations** command on the Communication Manager System Access Terminal (SAT). For the physical Digital telephones, verify that the telephones are attached to the correct ports.
- Go off-hook and on-hook on the controlled telephones manually and use PC/PSAP to verify consistency.
- Place and answer calls from the controlled telephones manually and use PC/PSAP to verify consistency.

9. Conclusion

These Application Notes described a compliance-tested configuration comprised of Communication Manager, Application Enablement Services, Avaya H.323 and Digital telephones, and the Spok PC/PSAP application. Spok PC/PSAP allows a user to operate a physical telephone and view call and telephone display information through a graphical user interface (GUI). During compliance testing, calls were successfully placed to and from Avaya H.323 and Digital telephones that were controlled and monitored by the Spok PC/PSAP application.

10. Additional References

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

[1] *Administering Avaya Aura® Communication Manager, Release 8.0.1*
[2] *Administering Avaya Aura® Avaya Aura® Application Enablement Services, Release 8.0.1,*

Product information for Spok products may be found at http://www.spok.com.

©2019 Avaya Inc. All Rights Reserved.

©2019 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.

©2019 Avaya Inc. All Rights Reserved.