



Avaya Solution & Interoperability Test Lab

Application Notes for Spok Enterprise Alert and Spok ALI Alert with Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager – Issue 1.0

Abstract

These Application Notes contain instructions for Spok Enterprise Alert and Spok ALI Alert with Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager to successfully interoperate.

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

Spok Enterprise Alert (Enterprise Alert) and Spok ALI (Automatic Location Identification) Alert (ALI Alert) are Enhanced E911 solutions. Enterprise Alert interoperates with the Avaya Aura® Communications Manager by integrating via a PRI trunk which routes emergency (911) calls. By monitoring the D channel, Enterprise Alert captures emergency call events, performs ANI (Automatic Number Identification) substitution, records the call and provides passive monitoring that bridges one or more phones on the call so that internal resources can listen to the call. ALI Alert monitors a configured crises alert Avaya 9600 Series IP Deskphone to capture emergency call events. It provides the same features as Enterprise Alert except Passive monitoring and call recording. Both solutions rely on Avaya Site Administration to automatically obtain the extension and extension location of non-IP phones. Both solutions rely on the Spok Avaya inventory function to automatically obtain extension and MAC address of Avaya IP phones (SIP and H.323). Both solutions rely on Spok's IP phone tracking function and Avaya's Push interface to automatically obtain the location of each IP phone extension. Link layer discovery is used to track the location of the IP phones' MAC address.

To achieve the above functionality Spok Enterprise Alerts uses the following Avaya Interfaces:

- Avaya Aura® Communication Manager – PRI Interface (Enterprise Alert)
- Avaya Aura® Communications Manager – Crises Alert (ALI Alert)
- Avaya Aura® Application Enablement Services – SMS Interface
- Avaya Aura® Communications Manager – H.323 phone inventory
- Avaya Aura® Session manager – SIP phone inventory
- Avaya Site Administration
- Avaya 9600 Series IP Deskphones – Push Interface

2. General Test Approach and Test Results

General test approach was to verify that Spok Enterprise Alert and ALI Alert are able to successfully integrate with various Avaya Interfaces. Functional test scenarios are mentioned in **Section 2.1**.

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 AES and Spok utilized capabilities of SSL. All other interfaces did not make use of secure capabilities.

2.1. Interoperability Compliance Testing

Interoperability testing contained functional test scenarios:

- Location information retrieval using Avaya Site Administration and upload to Spok ALI Database table
- Avaya IP Endpoint extensions and MAC address upload to Spok ALI database table
- Avaya 9600 Deskphone registration to Spok Push Application
- Update Emergency Location Extension for Avaya IP Endpoints
- Obtain Emergency Location Extension for Avaya IP Endpoints
- Tracking Avaya IP Endpoints
- Display of emergency caller extension and location on a networked PC via the Spok Sentry notification feature.
- Emergency calls notifications and recordings via Email

2.2. Test Results

All planned test cases passed.

2.3. Support

Technical support for the Spok Enterprise Alert and ALI Alert solution can be obtained by contacting Spok:

- **Web:** <http://www.spok.com>
- **Phone:** +1-888-797-7487

3. Reference Configuration

Figure 1 illustrates a sample configuration that consists of Avaya Products, Spok Enterprise Alert and Spok ALI Alert. Enterprise Alert uses a configuration that enables the emergency event determination, Passive Monitoring and ANI insertion on the PRI. ALI Alert uses a configuration that uses the Crises Alert phone for emergency call event determination and SMS for ANI insertion (i.e. setting the emergency location extension in the station record).

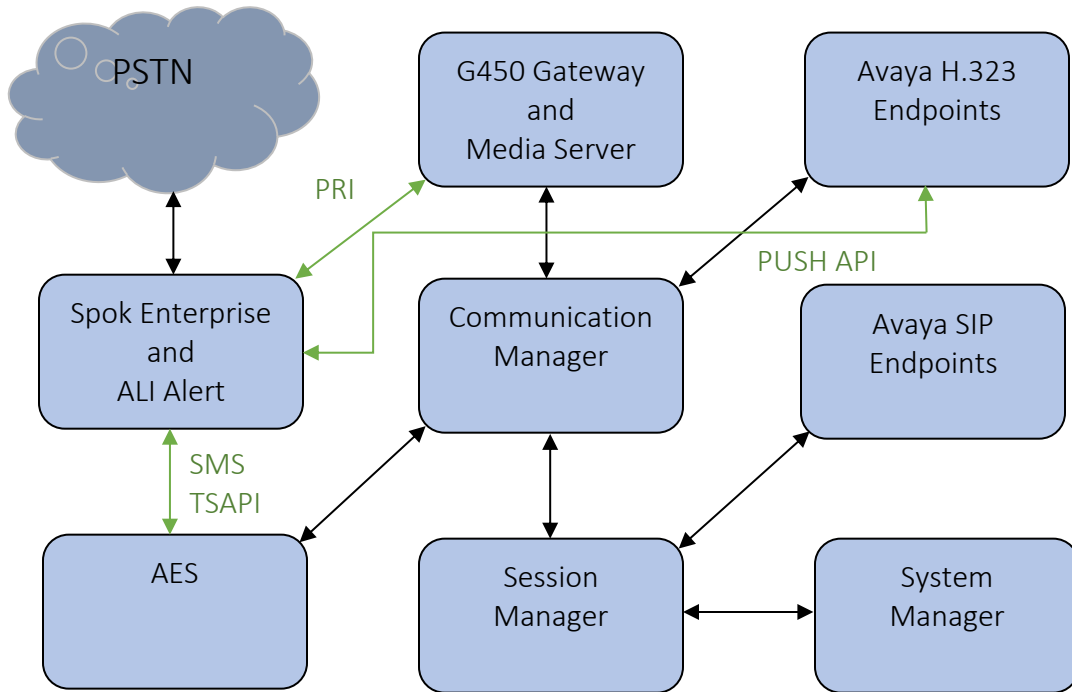


Figure 1: Test Configuration for Spok

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 | 8.0.1.1.0.822.25183 |
| Avaya Aura® Session Manager | 8.0.1.1.801103 |
| Avaya Aura® System Manager | 8.0.1.1.039340 |
| Avaya G450 Media Gateway | 40.20.0 |
| Avaya Aura® Media Server | 8.0.0.183 |
| Avaya Aura® Application Enablement Services | 8.0.1.0.2.5-0 |
| Avaya 9600 Series Deskphones <ul style="list-style-type: none">• 96x1 SIP• 96x1 H.323 | <ul style="list-style-type: none">• 7.1.5• 6.8102 |
| Spok Enterprise Alert/ALI Alert running Windows Server 2016 Standard | 11.11.0.417 |

5. Configure Avaya Aura® Communication Manager

This section contains steps necessary to configure Spok Enterprise Alert and Spok ALI Alert successfully with Communication Manager.

All configurations in Communication Manager were performed via the SAT terminal.

5.1. Verify Feature and License

Enter the **display system-parameters customer-options** command and ensure that the following features are enabled.

One Page 4, verify **Computer Telephony Adjunct Links**, **ASAI Link Core Capabilities** and **ASAI Link Plus Capabilities** are set to **y**.

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

Abbreviated Dialing Enhanced List? y      Audible Message Waiting? y
Access Security Gateway (ASG)? n          Authorization Codes? y
Analog Trunk Incoming Call ID? y         CAS Branch? n
A/D Grp/Sys List Dialing Start at 01? y  CAS Main? n
Answer Supervision by Call Classifier? y   Change COR by FAC? n
ARS? y      Computer Telephony Adjunct Links? y
ARS/AAR Partitioning? y                  Cvg Of Calls Redirected Off-net? y
ARS/AAR Dialing without FAC? y           DCS (Basic)? y
ASAI Link Core Capabilities? 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
```

On Page 5, verify **ISDN Feature Plus**, **ISDN-PRI**, **IP Trunks** and **Multimedia IP SIP Trunking** are set to **y**.

```

display system-parameters customer-options                               Page 5 of 12
                                OPTIONAL FEATURES

Emergency Access to Attendant? y                                     IP Stations? y
  Enable 'dadmin' Login? y
  Enhanced Conferencing? y                                         ISDN Feature Plus? y
    Enhanced EC500? y                                             ISDN/SIP Network Call Redirection? y
Enterprise Survivable Server? n                                     ISDN-BRI Trunks? y
  Enterprise Wide Licensing? n                                     ISDN-PRI? y
    ESS Administration? y                                         Local Survivable Processor? n
  Extended Cvg/Fwd Admin? y                                       Malicious Call Trace? y
  External Device Alarm Admin? y                                   Media Encryption Over IP? n
Five Port Networks Max Per MCC? n                                  Mode Code for Centralized Voice Mail? n
  Flexible Billing? n
  Forced Entry of Account Codes? y                                  Multifrequency Signaling? y
  Global Call Classification? y                                    Multimedia Call Handling (Basic)? y
  Hospitality (Basic)? y                                          Multimedia Call Handling (Enhanced)? y
Hospitality (G3V3 Enhancements)? y                                Multimedia IP SIP Trunking? y
  IP Trunks? y

```

On Page 11, verify **IP_API_A** has a sufficient limit.

```

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

Product ID  Rel. Limit      Used
AgentSC    * : 2400        0
IP_API_A  * : 2400        6
IP_Agent   * : 2400        0
IP_NonAgt  * : 2400        0
IP_Phone   * : 2400        1
IP_ROMax   * : 2400        0
IP_Soft    * : 2400        0
IP_Supv    * : 2400        0
IP_eCons   * : 68         0
oneX_Comm  * : 2400        0
           : 0           0
IP Attendant Consoles? y

```

5.2. Configure Site Data

To configure specific building codes for a site, use **change site-data** command. On Page 1, add entries for building codes. For compliance test, two entries of **MADISON** and **PARK** were added.

```
change site-data                                     Page 1 of 4
                                                    SITE DATA USER DEFINITION
                                                    VALID BUILDING FIELDS

MADISON
PARK
```

On Page 3, two entries of **10** and **8** for Floors were configured.

```
change site-data                                     Page 3 of 4
                                                    SITE DATA USER DEFINITION
                                                    VALID FLOOR FIELDS

10
8
```

Ensure to configure user extensions with the site data. When Spok runs SMS queries, this data is used for location information.

5.3. Configure Stations

Use **add station *n*** command to add a station, where *n* is an available station extension. This station will be used by Spok Enterprise Alert as a monitoring station for Crisis Alert. Configure the station as follows, on Page 1:

- In **Name** field, enter a descriptive name
- Set **Type** to the type of the telephones
- Enter a **Security Code**
- Set **IP SoftPhone** to **y**

```
add station 53001                                     Page 1 of 5
                                                    STATION
Extension: 53001                                     Lock Messages? n          BCC: 0
  Type: 9641                                         Security Code: *         TN: 1
  Port: S00068                                       Coverage Path 1:         COR: 1
  Name: Amcom Crisis Alert Station                   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: 53001
  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
```

One Page 4, under **BUTTON ASSIGNMENTS**, add **crss-alert** and **release**, as shown below:

```
change station 53001                                 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:                                             List2:
                                                    List3:
BUTTON ASSIGNMENTS
  1: call-appr                                     5: crss-alert
  2: call-appr                                     6: release
  3: call-appr                                     7:
  4:                                               8:
```

Add another station for an Incoming DID. For example, if the incoming DID is 732-277-2872, use the last five digits as a station extension. This station is a virtual station that will be used by Spok Enterprise alert to remotely perform call forwarding for callbacks from Public Safety Answering Point (PSAP).

- In **Name** field, enter a descriptive name
- Set **Type** to **9641**
- Enter a **Security Code**

```

add station 72872                                     Page 1 of 5
                                                    STATION
Extension: 72872                                     Lock Messages? n          BCC: 0
  Type: 9641                                         Security Code: 123456     TN: 1
  Port: IP                                           Coverage Path 1:         COR: 1
  Name: DID Station 1                               Coverage Path 2:         COS: 1
                                                    Hunt-to Station:        Tests? y

STATION OPTIONS
  Loss Group: 19                                     Time of Day Lock Table:
  Speakerphone: 2-way                               Personalized Ringing Pattern: 1
  Display Language: english                         Message Lamp Ext: 72872
  Survivable GK Node Name:                          Mute Button Enabled? y
  Survivable COR: internal                           Button Modules: 0
  Survivable Trunk Dest? y                           Media Complex Ext:
                                                    IP SoftPhone? n
                                                    IP Video? n
Short/Prefixed Registration Allowed: default
  
```

5.4. Configure DS1

For an available T1 card on the Avaya G450 gateway, use **add ds1 n**, where *n* is the location of the T1 card. The PRI trunk from this T1 card will be connected to the PRI Bypass box on a PBX port. Configure as follows:

- Type in a descriptive name in **Name** field
- Set **Bit Rate** to **1.544**
- Set **Line Coding** to **b8zs**
- Set **Framing Mode** to **esf**
- Set **Signaling Mode** to **isdn-pri**
- Set **Connect** to **network**
- Set **Protocol Version** to **b**

```
add ds1 1v1                                     Page 1 of 2
                                               DS1 CIRCUIT PACK
      Location: 001V1                               Name: to_SPOK
      Bit Rate: 1.544                               Line Coding: b8zs
Line Compensation: 1                               Framing Mode: esf
      Signaling Mode: isdn-pri
      Connect: network
      TN-C7 Long Timers? n                           Country Protocol: 1
Interworking Message: PROgress                     Protocol Version: b
Interface Companding: mulaw                         CRC? n
      Idle Code: 11111111
                                               DCP/Analog Bearer Capability: 3.1kHz
                                               T303 Timer(sec): 4
      Slip Detection? n                               Near-end CSU Type: other
      Echo Cancellation? n                           Block Progress Indicator? n
```

5.5. Configure Signaling Group

User **add signaling-group *n***, where *n* is an available signaling group number, to add a signaling group. Configure as follows:

- Set **Group Type** to **isdn-pri**
- Set the **Primary D-Channel** according to the DS1 configured. Use channel number 24 as a D-Channel
- Set **TSC Supplementary Service Protocol** to **b**
- Once the trunk group has been configured return to this form and set the **Trunk Group for Channel Selection**

```
add signaling-group 97                               Page 1 of 1
                                           SIGNALING GROUP

Group Number: 97          Group Type: isdn-pri
Associated Signaling? y   Max number of NCA TSC: 0
Primary D-Channel: 001V624   Max number of CA TSC: 0
Trunk Group for NCA TSC:
Trunk Group for Channel Selection: 97   X-Mobility/Wireless Type: NONE
TSC Supplementary Service Protocol: b   Network Call Transfer? n
```

5.6. Configure Trunk Group

User **add trunk-group *n***, where *n* is an available trunk group number, to add a trunk group. On Page 1, configure as follows:

- Set **Group Type** to **isdn**
- Provide a descriptive name in **Group Name**
- Set **TAC** according to the dial plan
- Set **Carrier Medium** to **PRI/BRI**
- Set **Outgoing Display** to **y**
- Set **Service Type** to **tie**

```
add trunk-group 97                               Page 1 of 22
                                           TRUNK GROUP

Group Number: 97          Group Type: isdn          CDR Reports: y
Group Name: Avaya DevConnect   COR: 1          TN: 1          TAC: 197
Direction: two-way          Outgoing Display? y   Carrier Medium: PRI/BRI
Dial Access? n          Busy Threshold: 255   Night Service:
Queue Length: 0
Service Type: tie          Auth Code? n          TestCall ITC: rest
Far End Test Line No:
TestCall BCC: 4
```

On Page 3, configure as follows:

- Set **Send Name** and **Send Calling Number** to **y**
- Set **Format** to **private**

```

change trunk-group 97                                     Page 3 of 22
TRUNK FEATURES
  ACA Assignment? n                                     Measured: both      Wideband Support? n
                                                    Internal Alert? n    Maintenance Tests? y
  Data Restriction? n                               NCA-TSC Trunk Member:
                                                    Send Name: y       Send Calling Number: y
  Used for DCS? n                                     Format: private
  Suppress # Outpulsing? n
  Outgoing Channel ID Encoding: preferred           UII IE Treatment: shared
                                                    Maximum Size of UII IE Contents: 128
                                                    Replace Restricted Numbers? n
                                                    Replace Unavailable Numbers? n
                                                    Send Connected Number: y
  Network Call Redirection: none                   Hold/Unhold Notifications? n
  Send UII IE? y                                   Modify Tandem Calling Number: no
  Send UCID? y                                     BSR Reply-best DISC Cause Value: 31
  Send Codeset 6/7 LAI IE? y                       Dsl Echo Cancellation? n
  
```

On Page 5 and 6, add ports according to the location of the T1 board on Avaya Media Gateway.

```

change trunk-group 97                                     Page 6 of 22
                                                    TRUNK GROUP
                                                    Administered Members (min/max): 1/5
GROUP MEMBER ASSIGNMENTS                               Total Administered Members: 5

  Port      Code Sfx Name      Night      Sig Grp
  1: 001V601 MM710
  2: 001V602 MM710
  3: 001V603 MM710
  4: 001V604 MM710
  5: 001V605 MM710
  
```

5.7. Configure Route Pattern

Configure route pattern to use the trunk group configured in the previous section. Use the **change route-pattern 97** command to configure the following:

- Set **Grp No** for Line 1 to the trunk group configured in the previous section
- Set **FRL** to **0**
- Set **Numbering Format** to **lev0-pvt** as configured in the screen capture below

```

change route-pattern 97                                     Page 1 of 3
      Pattern Number: 10      Pattern Name:
  SCCAN? n      Secure SIP? n      Used for SIP stations? n

  Grp FRL NPA Pfx Hop Toll No.  Inserted      DCS/ IXC
  No      Mrk Lmt List Del  Digits      QSIG
                                     Dgts      Intw
1: 97  0
2:
3:
4:
5:
6:

      BCC VALUE  TSC CA-TSC      ITC BCIE Service/Feature PARM Sub  Numbering LAR
      0 1 2 M 4 W      Request      Dgts  Format
1: y y y y y n  n      rest      lev0-pvt none
2: y y y y y n  n      rest      none
3: y y y y y n  n      rest      none
4: y y y y y n  n      rest      none
5: y y y y y n  n      rest      none
6: y y y y y n  n      rest      none
  
```

5.8. Configure Private Numbering

Use **change private-number 0** command to configure the private numbering. This will ensure that the calling party number is sent to Spok Enterprise Alerts when a call is placed from any of the Avaya Endpoints. For the test configuration, extensions starting with **5** and **5** digits long were used.

```

change private-numbering 0                                 Page 1 of 2
      NUMBERING - PRIVATE FORMAT

  Ext  Ext      Trk      Private      Total
  Len  Code      Grp(s)      Prefix      Len
  5  1
  5  5
      5  Total Administered: 2
      5  Maximum Entries: 540
  
```

5.9. Configure Crisis Alert

Use **change system-parameters crisis-alert** command and set **Every User Respond** to **n**.

```
change system-parameters crisis-alert                               Page 1 of 1
                               CRISIS ALERT SYSTEM PARAMETERS

ALERT STATION
  Every User Responds? n

ALERT PAGER
  Alert Pager? n
```

5.10. Configure ARS Routing

Due to the nature of emergency calls, 933 was used instead of 911, but steps here show how 911 routing can be configured. Use the **change ars analysis 911** command to configure 911 calls to route to Spok Emergency Alerts and enable crisis alerts. The following configuration shows that when 911 is called, the call is routed to Spok Emergency Alerts and a crisis alert is sent to all the phones that are configured with crss-alert buttons.

- Set **Dialed String** to **911**
- Set **Total Min** and **Max** to **3**
- Set **Route Pattern** to the pattern configured in **Section 5.7**
- Set **Call Type** to **alrt**

```
change ars analysis 911                                           Page 1 of 2
                               ARS DIGIT ANALYSIS TABLE
                               Location: all                       Percent Full: 1

   Dialed      Total      Route      Call      Node      ANI
   String      Min      Max      Pattern   Type      Num      Reqd
911           3       3       97       alrt      n
```

5.11. 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 AES.

| change node-names ip | | Page 1 of 2 |
|----------------------|----------------------|-------------|
| IP NODE NAMES | | |
| Name | IP Address | |
| 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 Type | Enabled | Local Node | Local Port | Remote Node | Remote Port | |
| AESVCS | y | procr | 8765 | | | |

On **Page 4**, enter the hostname of the AES server for the AE Services Server field. The server name may be obtained by logging in to the AES 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 AES server in **Section 6.1**.

| change ip-services | | | | | Page 3 of 3 |
|----------------------------|--------------------|----------|----------|-------------|-------------|
| AE Services Administration | | | | | |
| Server ID | AE Services Server | Password | Enabled | Status | |
| 1: | aes8 | * | y | idle | |
| 2: | | | | | |

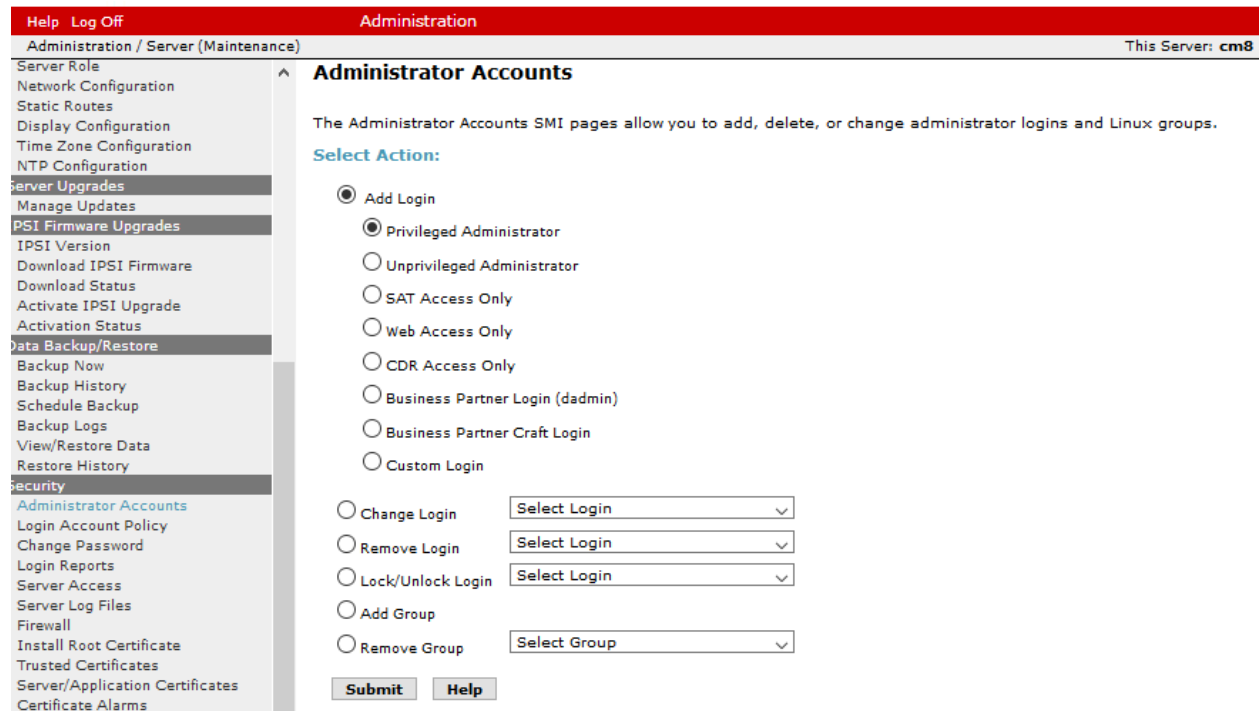
5.12.Add an Administrative User

Add a user for Spok Enterprise Alert to provide access for Avaya Site Administration and the SMS interface.

Navigate to <https://<ip-address>> where ip-address is the ip-address of Communication Manager and log in using appropriate credentials.



Navigate to **Administration** → **Server Maintenance**. On the left pane, navigate to **Security** → **Administrator Accounts**, and select **Add Login** → **Privileged Administrator**; click **Submit**.



- Type in a **Login Name**.
- Set **Additional Groups** to a profile configured in Communication Manager. Please note that this profile was pre-configured in Communication Manager and is not shown in this document. To add a profile in Communication Manager via SAT, use the **add user-profile** command.
- Type in a password in **Enter Password** and **Re-enter password**.
- Click **Submit** when done.

Help Log Off Administration Administration / Server (Maintenance) This Server: cm8

Administrator Accounts -- Add Login: Privileged Administrator

This page allows you to add a login that is a member of the **SUSERS** group. This login has the greatest access privileg in the system next to root.

Login name:

Primary group:

Additional groups (profile):

Linux shell:

Home directory:

Lock this account:

SAT Limit:

Date after which account is disabled-blank to ignore (YYYY-MM-DD):

Enter password:

Re-enter password:

Force password change on next login: No Yes

6. Configure Avaya Aura® 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 and a CTI user for Spok Enterprise Alert.

6.1. 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.



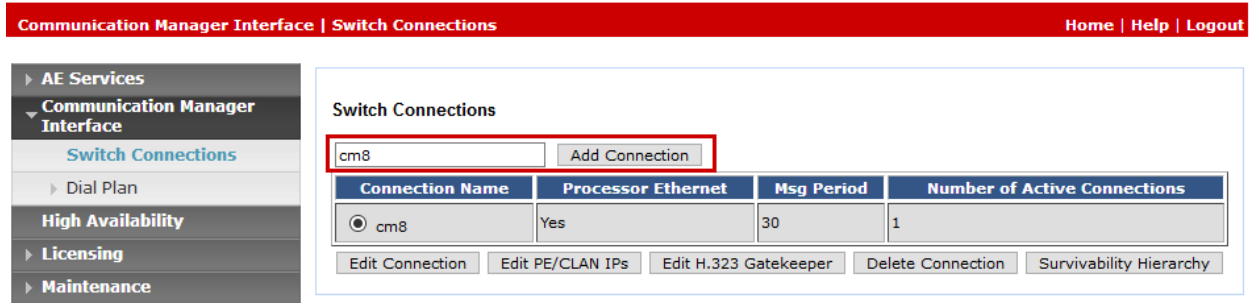
Application Enablement Services Management Console

A screenshot of a login page with a light gray background. The text "Please login here:" is at the top left. Below it, the label "Username" is followed by a white text input field. At the bottom center, there is a "Continue" button with a gray border and a light gray background.

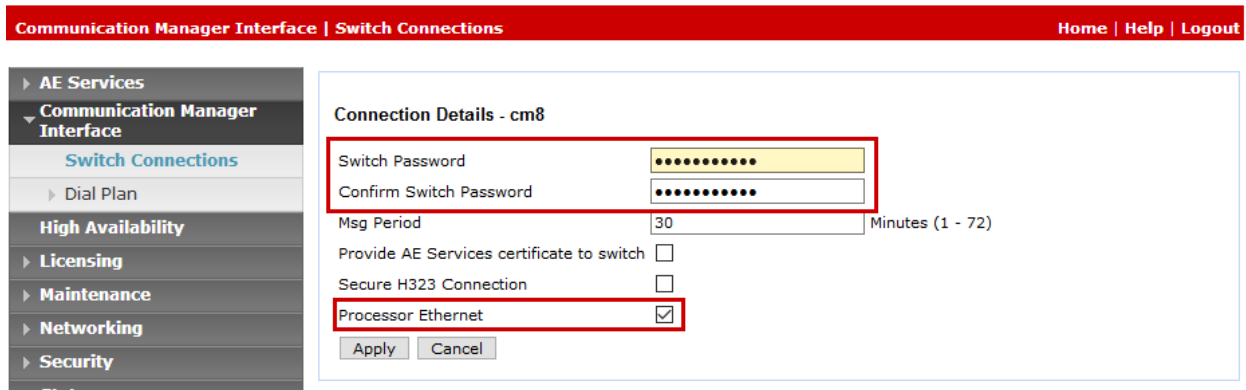
Please login here:
Username

Copyright © 2009-2018 Avaya Inc. All Rights Reserved.

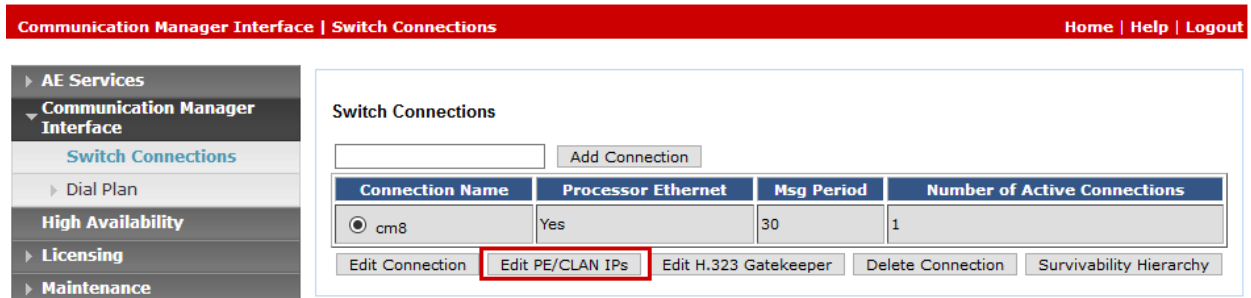
Click on **Communication Manager Interface** → **Switch Connection** in the left pane to invoke the Switch Connections page. A Switch Connection defines a connection between the Application Enablement Services and Communication Manager. Enter a descriptive name for the switch connection and click on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



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

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
 Communication Manager Interface
 Switch Connections
 Dial Plan
 High Availability
 Licensing
 Maintenance

Edit Processor Ethernet IP - cm8

10.64.110.131

| Name or IP Address | Status |
|--------------------|--------|
| 10.64.110.131 | In Use |

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.

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
 Communication Manager Interface
 Switch Connections
 Dial Plan
 High Availability
 Licensing
 Maintenance

Switch Connections

| Connection Name | Processor Ethernet | Msg Period | Number of Active Connections |
|--------------------------------------|--------------------|------------|------------------------------|
| <input checked="" type="radio"/> cm8 | Yes | 30 | 1 |

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**.

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
 Communication Manager Interface
 Switch Connections
 Dial Plan
 High Availability
 Licensing

Edit H.323 Gatekeeper - cm8

10.64.110.131

Name or IP Address

10.64.110.131

6.2. Configure User

A user needs to be created for Spok Enterprise Alert to communicate with AES. Navigate to **User Management** → **User Admin** → **Add User**. Populate the **User Id**, **Common Name**, **Surname**, **User Password** and **Confirm Password** fields. Set the **CT User** to **Yes** and click **Apply**.

User Management | User Admin | Add User Home | Help | Logout

Add User

Fields marked with * can not be empty.

* User Id

* Common Name

* Surname

* User Password

* Confirm Password

Admin Note

Avaya Role

Business Category

Car License

CM Home

Cms Home

CT User

Department Number

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

| User ID | Common Name | Worktop Name | Device ID |
|---------------------------------------|-------------|--------------|-----------|
| <input type="radio"/> aessim | aessim | NONE | NONE |
| <input type="radio"/> ctinteg | ctinteg | NONE | NONE |
| <input type="radio"/> ctuser | ctuser | NONE | NONE |
| <input type="radio"/> interop | interop | NONE | NONE |
| <input type="radio"/> redsky | redsky | NONE | NONE |
| <input checked="" type="radio"/> spok | spok | NONE | NONE |
| <input type="radio"/> spokmcs | spokmcs | NONE | NONE |
| <input type="radio"/> spokscs | spokscs | NONE | NONE |
| <input type="radio"/> spokss | spokss | NONE | NONE |
| <input type="radio"/> sureconnect | sureconnect | NONE | NONE |
| <input type="radio"/> tenfold | tenfold | NONE | NONE |

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

| | | |
|-----------------------------------|--|--|
| ▶ AE Services | Edit CTI User | |
| ▶ Communication Manager Interface | User Profile: | User ID: spok |
| High Availability | | Common Name: spok |
| ▶ Licensing | | Worktop Name: NONE ▾ |
| ▶ Maintenance | | Unrestricted Access: <input checked="" type="checkbox"/> |
| ▶ Networking | <hr/> | |
| ▼ Security | Call and Device Control: | Call Origination/Termination and Device Status: None ▾ |
| ▶ Account Management | <hr/> | |
| ▶ Audit | Call and Device Monitoring: | Device Monitoring: None ▾ |
| ▶ Certificate Management | | Calls On A Device Monitoring: None ▾ |
| Enterprise Directory | | Call Monitoring: <input type="checkbox"/> |
| ▶ Host AA | <hr/> | |
| ▶ PAM | Routing Control: | Allow Routing on Listed Devices: None ▾ |
| ▼ Security Database | <input type="button" value="Apply Changes"/> <input type="button" value="Cancel Changes"/> | |
| - Control | | |

7. Configure 46xxSetting.txt

To configure the Push, Subscribe and SNMP settings for Avaya 9600 Series IP Deskphones, configure the 46xxSetting.txt file with the following settings. Once configured, reboot the phones to take the changes.

The following is an example of PUSH INTERFACE SETTINGS section in the 46xxsettings.txt file:

```
##### PUSH INTERFACE SETTINGS #####  
SET TPSLIST <ip-address>  
SET SUBSCRIBELIST http:// <ip-address>/avayapush/aspx/processingpage.aspx  
SET PUSHCAP 2222  
SET PUSHPORT 80
```

<ip-address> is the IP Address of Spok Enterprise Alert.

8. Configure Spok Enterprise Alert

Spok installs, configures, and customizes the Enterprise Alert and ALI Alert applications for their end customers and is outside the scope of this document.

9. Verification

To verify the connectivity to Spok Enterprise Alert, use **status trunk <n>** where n is the trunk number of the PRI trunk connected to Spok Enterprise Alert. Verify **Service State** for all trunk members is **in-service/idle**.

```

status trunk 10
Page 1

TRUNK GROUP STATUS

Member   Port      Service State   Mtce Connected Ports
          Port          Busy

0010/001 001V101  in-service/idle  no
0010/002 001V102  in-service/idle  no
0010/003 001V103  in-service/idle  no
0010/004 001V104  in-service/idle  no
0010/005 001V105  in-service/idle  no
0010/006 001V106  in-service/idle  no
0010/007 001V107  in-service/idle  no
0010/008 001V108  in-service/idle  no
0010/009 001V109  in-service/idle  no
0010/010 001V110  in-service/idle  no
  
```

To verify Spok ALI Alert, generate a test call that will generate a crisis alert. Verify Spok ALI Alert receives the crisis alert.

The screenshot displays the SPOK Enterprise Alert application window. At the top, there are navigation icons for Silence, Ack, Clear, and About, along with an Exit button. Below this is a table with columns: DATE, TIME, LOCATION, ANI, EXTN., ELIN, NAME, and ACK. The table contains three entries:

| DATE | TIME | LOCATION | ANI | EXTN. | ELIN | NAME | ACK. |
|------------|----------|-----------------------|------------|-------|------|----------------|-------|
| 07-02-2019 | 10:08:40 | BLD:190, FLR:2 RM:190 | 6462640900 | 51001 | | Frazier, Clint | 2 |
| 07-02-2019 | 10:05:13 | BLD:220, FLR:2 RM:220 | | | | Romine, Austin | YES 2 |
| 07-02-2019 | 10:04:26 | | | | | | 2 |

An information dialog box titled "SPOK Enterprise Alert" is overlaid on the table. It contains the following details:

- Call Date: 07-02-2019
- Call Time: 10:08:40
- Caller's Location: BLD:190, FLR:2 RM:190
- Caller's ANI: 6462640900
- Caller's Extension: 51001
- Caller's Name: Frazier, Clint
- ELIN:
- Acknowledged: 23
- CAMA Trunk #:
- Called Number:

The dialog box has an "OK" button at the bottom. The status bar at the bottom of the application window shows "2019-07-02_15:21:45 PRI-All Ok!" and "Ctrl+P to print report".

10. Conclusion

Spok Enterprise Alert and ALI Alert were able to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services.

11. References

Documentation related to Avaya products may be obtained via <http://support.avaya.com>.

[1] *Administering Avaya Aura® Communication Manager, Release 8.0.1*

[2] *Avaya Aura® Communication Manager Feature Description and Implementation, Release 8.0.1.*

[3] *Administering Avaya Aura® Session Manager, Release 8.0.1*

[4] *Administering Avaya Aura® System Manager, Release 8.0.1*

©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.