



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 1.1

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 Aura® Communication Manager and Avaya 9600 Series IP Deskphones – SNMP interface
- 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 via HTTPS.

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
- Bridging on a phone to an active emergency call via a listen only bridge
- 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).

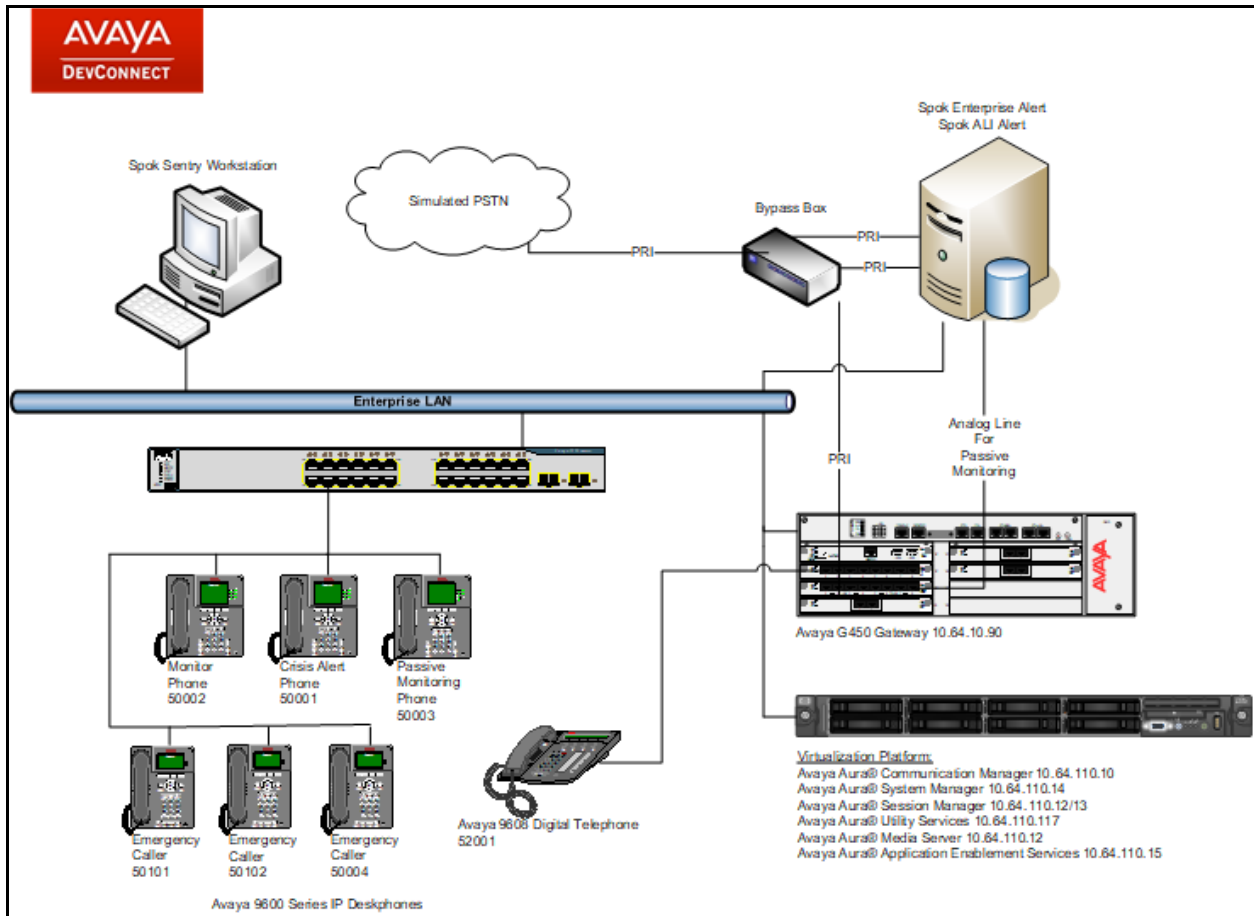


Figure 1: Test Configuration for Spok

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	7.1.1.0.0.532.23985
Avaya Aura [®] Session Manager	7.1.1.0.711008
Avaya Aura [®] System Manager	7.1.1.0.046931
Avaya G450 Media Gateway	38.20.1
Avaya Aura [®] Media Server	7.8.0.333
Avaya Aura [®] Application Enablement Services	7.1.1.0.0.5
Avaya 9600 Series Deskphones <ul style="list-style-type: none">• 96x1 SIP• 96x1 H.323• 96xx SIP• 96xx H.323	<ul style="list-style-type: none">• 7.1.1.0.91817• 6.6.5.06• 2.6.17• 3.2.8.091517
Spok Enterprise Alert/ALI Alert running Windows Server 2016 (x64)	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.

One **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 50001                                     Page 1 of 5
                                                    STATION
Extension: 50001                                     Lock Messages? n          BCC: 0
  Type: 9630                                         Security Code: *          TN: 1
  Port: S00002                                       Coverage Path 1:         COR: 1
  Name: H.323 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: 50001
Survivable GK Node Name:                               Mute Button Enabled? y
  Survivable COR: internal                             Button Modules: 0
Survivable Trunk Dest? y                             Media Complex Ext:
                                                    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 50001                                 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 **9630**
- Enter a **Security Code**

```

add station 72872                                     Page 1 of 5
                                                    STATION
Extension: 72872                                     Lock Messages? n          BCC: 0
  Type: 9630                                         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 G540 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 10                               Page 1 of 1
                                           SIGNALING GROUP
Group Number: 10                                Group Type: isdn-pri
Associated Signaling? y                        Max number of NCA TSC: 0
Primary D-Channel: 001V124                    Max number of CA TSC: 0
Trunk Group for NCA TSC:
Trunk Group for Channel Selection:             X-Mobility/Wireless Type: NONE
TSC Supplementary Service Protocol: b         Network Call Transfer? n
```

5.6. Configure Trunk Group

Use **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 10                               Page 1 of 21
                                           TRUNK GROUP
Group Number: 2                                Group Type: isdn          CDR Reports: r
Group Name: to_SPOK                           COR: 1                   TN: 1           TAC: *002
Direction: two-way                            Outgoing Display? y      Carrier Medium: PRI/BRI
Dial Access? y                               Busy Threshold: 255     Night Service:
Queue Length: 0                               Auth Code? n            TestCall ITC: rest
Service Type: tie                             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**

```

TRUNK FEATURES
ACA Assignment? n          Measured: none          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              Send EMU Visitor CPN? n
                          Suppress # Outpulsing? n    Format: private
Outgoing Channel ID Encoding: preferred    UII IE Treatment: service-provider

                          Replace Restricted Numbers? n
                          Replace Unavailable Numbers? n
                          Send Connected Number: n
Network Call Redirection: none             Hold/Unhold Notifications? n
                          Send UII IE? y              Modify Tandem Calling Number: no
                          Send UCID? n
Send Codeset 6/7 LAI IE? y                Dsl Echo Cancellation? n

```

On **Page 5 and 6**, add the **Port 1-23** according to the location of the T1 board on Avaya Media Gateway.

```

add trunk-group 10
Page 5 of 21
TRUNK GROUP
Administered Members (min/max): 1/23
GROUP MEMBER ASSIGNMENTS          Total Administered Members: 23

Port   Code Sfx Name      Night      Sig Grp
1: 001V101 MM710
2: 001V102 MM710
3: 001V103 MM710
4: 001V104 MM710
5: 001V105 MM710
6: 001V106 MM710
7: 001V107 MM710
8: 001V108 MM710
9: 001V109 MM710
10: 001V110 MM710
11: 001V111 MM710
12: 001V112 MM710
13: 001V113 MM710
14: 001V114 MM710
15: 001V115 MM710

```

5.7. Configure Route Pattern

Configure route pattern to use the trunk group configured in the previous section. Use the **change route-pattern 10** 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 10                                     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: 10  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
  11 1
  5 5      Total Administered: 2
      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**

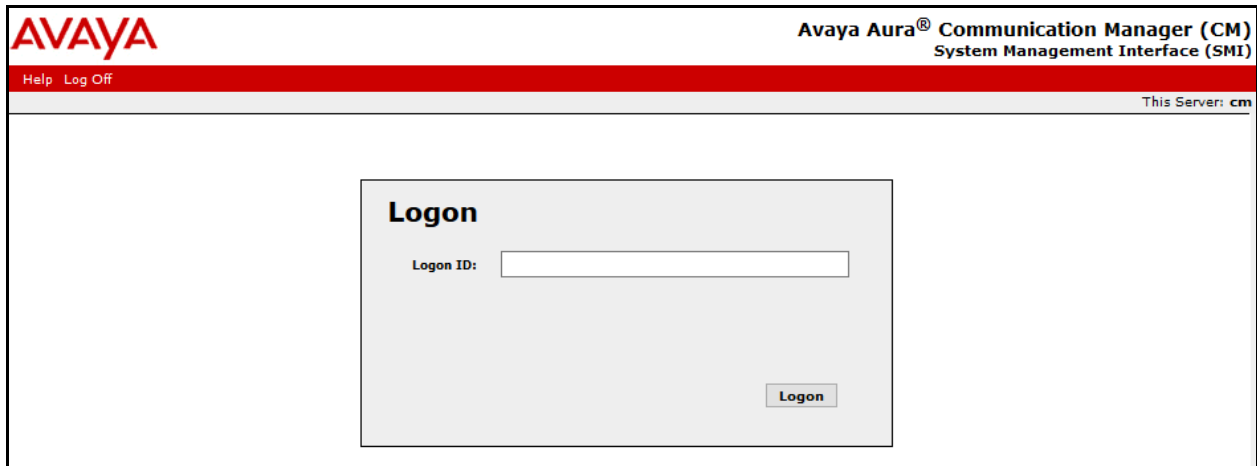
```
change ars analysis 911                                           Page 1 of 2
                        ARS DIGIT ANALYSIS TABLE
                        Location: all                               Percent Full: 1

   Dialed      Total      Route      Call      Node      ANI
   String      Min      Max      Pattern   Type      Num      Reqd
911           3       3       10       alrt      n
```

5.11.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.



The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) login page. The page has a red header with the Avaya logo on the left and the text "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)" on the right. Below the header, there are links for "Help" and "Log Off" on the left, and "This Server: cm" on the right. The main content area is a light gray box with the title "Logon". Inside this box, there is a label "Logon ID:" followed by a text input field. Below the input field is a "Logon" button.

Navigate to **Administration → Server Maintenance**.



The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) Administration page. The page has a red header with the Avaya logo on the left and the text "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)" on the right. Below the header, there are links for "Help" and "Log Off" on the left, and "This Server: cm" on the right. A navigation menu is visible, with "Administration" selected, showing sub-items: "Administration", "Licensing", and "Server (Maintenance)". The main content area is titled "System" and contains a text box with the description: "The Server (Maintenance) Interface allows you to maintain, troubleshoot, and configure the server." Below this, there is a copyright notice: "© 2001-2017 Avaya Inc. All Rights Reserved." and a section titled "Copyright" with the text: "Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights." and "Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law."

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

The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) Administration page. The left navigation pane is expanded to the **Security** section, with **Administrator Accounts** selected. The main content area is titled **Administrator Accounts** and contains the following elements:

- Navigation:** Help, Log Off, Administration, Administration / Server (Maintenance), This Server: cm
- Section Header:** Administrator Accounts
- Description:** The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups.
- Select Action:**
 - Add Login
 - Privileged Administrator
 - Unprivileged Administrator
 - SAT Access Only
 - Web Access Only
 - CDR Access Only
 - Business Partner Login (dadmin)
 - Business Partner Craft Login
 - Custom Login
- Form Fields:**
 - Change Login: Select Login (dropdown)
 - Remove Login: Select Login (dropdown)
 - Lock/Unlock Login: Select Login (dropdown)
 - Add Group: Add Group (dropdown)
 - Remove Group: Select Group (dropdown)
- Buttons:** Submit, Help

- 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.

AVAYA Avaya Aura® Communication Manager (CM) System Management Interface (SMI)

Help Log Off Administration This Server: cm

Administration / Server (Maintenance)

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 privileges 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:

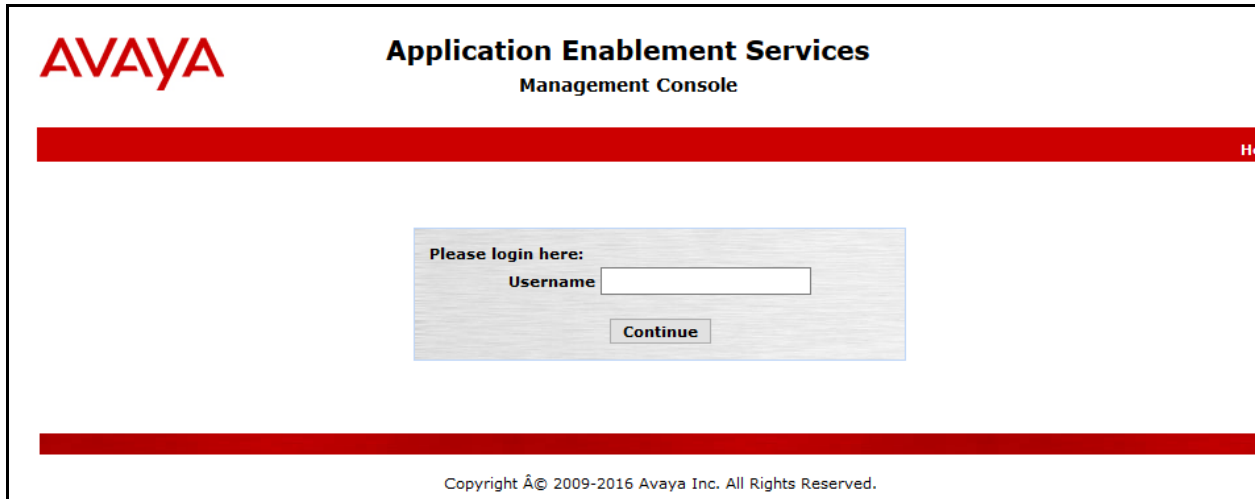
Force password change on next login: No Yes

6. Configure Avaya Aura® Application Enablement Services

Configuration of Application Enablement Services requires a user account to be configured for Spok Enterprise Alert.

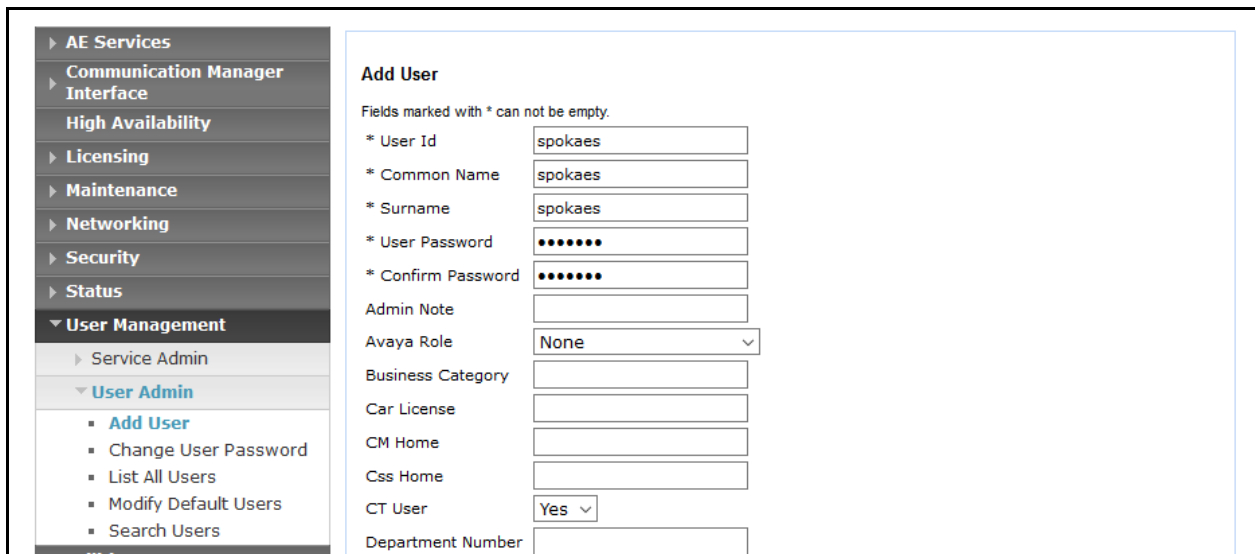
6.1. Configure User

All administration is performed by web browser, <https://<aes-ip-address>/>. Log on using appropriate credentials



The screenshot shows the Avaya Application Enablement Services Management Console login page. At the top left is the Avaya logo. The title is "Application Enablement Services Management Console". Below the title is a red horizontal bar. In the center, there is a login box with the text "Please login here:" and a "Username" label followed by a text input field. Below the input field is a "Continue" button. At the bottom of the page, there is a red horizontal bar and the copyright notice: "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

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**.



The screenshot shows the Avaya User Management console. On the left is a navigation menu with the following items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management (expanded), Service Admin, and User Admin (expanded). Under User Admin, the following options are listed: Add User, Change User Password, List All Users, Modify Default Users, and Search Users. The main content area is titled "Add User" and contains the following fields: * User Id (spokaes), * Common Name (spokaes), * Surname (spokaes), * User Password (masked with dots), * Confirm Password (masked with dots), Admin Note (empty), Avaya Role (None), Business Category (empty), Car License (empty), CM Home (empty), Css Home (empty), CT User (Yes), and Department Number (empty). A note at the top of the form states: "Fields marked with * can not be empty."

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

CTI Users

User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> oceana	oceana	NONE	NONE
<input checked="" type="radio"/> spokaes	spok	NONE	NONE

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

Edit CTI User

User Profile: User ID: spokaes
 Common Name: spok
 Worktop Name: NONE ▾
 Unrestricted Access:

Call and Device Control: Call Origination/Termination and Device Status: None ▾

Call and Device Monitoring: Device Monitoring: None ▾
 Calls On A Device Monitoring: None ▾
 Call Monitoring:

Routing Control: Allow Routing on Listed Devices: None ▾

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 SNMP SETTINGS section in the 46xxsettings.txt file:

```
##### SNMP SETTINGS #####  
SET SNMPADD <ip-address>  
SET SNMPSTRING spok
```

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/asp/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 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.

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 7.1, August 2017, Document Number 03-300509, Issue 1.*
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation, Release 7.1, August 2017, Document Number 555-245-205, Issue 1.*
- [3] *Administering Avaya Aura® Session Manager, Release 7.1, Issue 1 August 2017*
- [4] *Administering Avaya Aura® System Manager, Release 7.1, Issue 1, August, 2017*

©2018 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.