Avaya Solution & Interoperability Test Lab

Application Notes for Resource Software International Shadow Onsite Notification Version 5.3 with Avaya Aura® Communication Manager Release 8.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Resource Software International Shadow Onsite Notification to interoperate with Avaya Aura Communication Manager.

Resource Software International Shadow Onsite Notification is an E911 notification solution that uses Properties Management System and System Access Terminal interfaces from Avaya Aura® Communication Manager, to provide monitoring and notification of emergency calls.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required for Resource Software International (RSI) Shadow Onsite Notification (OSN) 5.3.5 to interoperate with Avaya Aura® Communication Manager 8.1.3.

Shadow OSN is an E911 notification solution that uses the Properties Management System (PMS) interface from Communication Manager to monitor Crisis Alert emergency calls via the PMS journal printer, and uses the RSI Winlink Remote BCMS application that interfaces with Communication Manager via System Access Terminal (SAT) to obtain station location information such as building, floor, and room associated with the emergency caller.

In the compliance test, simulated 911 emergency was configured via SIP trunk through Avaya Session Border Controller for Enterprise.

The Shadow OSN software is for use with Communication Manager telephone system with the Crisis Alert feature to be configured. The Shadow OSN product adds Onsite Notification event generation to the telephone system. This feature when active will generate and deliver notification messages for emergency call events. The notification messages can be delivered via email, email to SMS, or to a network computer utilizing Windows popup/network messages. Note that only email method was used during the testing.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Shadow OSN application, the application automatically connects to an assigned port of PMS and obtains list of station in Communication Manager through SAT.

For the manual part of the testing, emergency calls were placed manually from the enterprise station to the emulated PSTN.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet connection to the Shadow OSN server.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya

products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between Avaya systems and the Shadow OSN did not include use of any specific encryption features as requested by RSI.

This solution uses the System Access Terminal (SAT) interface to interact with Avaya Aura® Communication Manager or the Telnet/SSH interface to interact with other Avaya products. While this solution has successfully completed Compliance Testing for the specific release levels as described in these Application Notes, Avaya does not generally recommend use of these interfaces as a programmatic approach to integration of 3rd party applications. Avaya may make changes or enhancements to the interfaces in any subsequent release, feature pack, service pack, or patch that may impact the interoperability of 3rd party applications using these interfaces. Using these interfaces in a programmatic manner may also result in a variety of operational issues, including performance impacts to the Avaya solution. If there are no other programmatic options available to obtain the required data or functionality, Avaya recommends that 3rd party applications only be executed during low call volume periods, and that real-time delays be inserted between each command execution. NOTE: The scope of the compliance testing activities reflected in these Application Notes explicitly did not include load or performance evaluation criteria, and no guarantees or assurances are made by Avaya that the 3rd party application has implemented these recommendations. The vendor of the 3rd party application using this interface remains solely responsible for verifying interoperability with all later Avaya Product Releases, including feature packs, service packs, and patches as issued by Avaya. For additional details see Avaya Product Support Notices PSN002884u, PSN005085u, and PSN020295u, available at www.avaya.com/support.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing focused on verifying the following on Shadow OSN:

- Proper handling of Crisis Alert emergency call log record via PMS journal printer
- Proper obtainment of emergency callers' location related information via SAT
- Proper delivering of emergency call notification to desired mailboxes via email

The serviceability testing focused on verifying the ability of Shadow OSN to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to the Shadow OSN server.

2.2. Test Results

All test cases were executed and completed successfully.

2.3. Support

Technical support on Shadow OSN can be obtained through the following:

- **Phone:** (800) 891-6014
- **Email:** support@telecost.com
- **Web:** www.telecost.com

3. Reference Configuration

As shown in **Figure 1**, RSI Shadow OSN server connects to Communication Manager through Properties Management System (PMS). The testing utilizes simulated 911 emergency configured via SIP trunk through Avaya Session Border Controller for Enterprise.

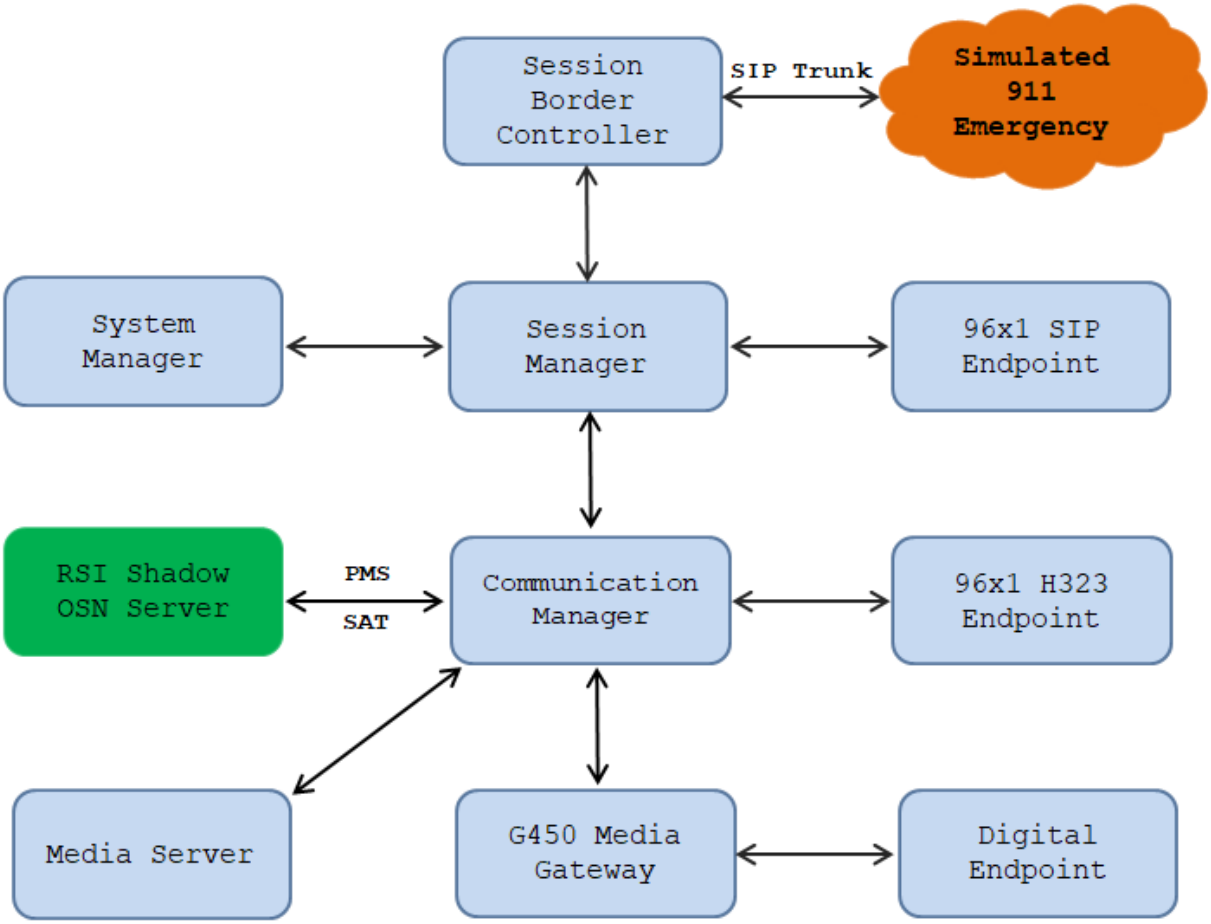


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Communication Manager running on Virtual Environment	8.1.3 (8.1.3.0.0.890.26568)
Avaya G450 Media Gateway	41.34.0
Avaya Aura® Media Server running on Virtual Environment	8.0.1
Avaya Aura® Session Manager running on Virtual Environment	8.1.3 (8.1.3.0.813014)
Avaya Aura® System Manager running on Virtual Environment	8.1.3 (8.1.3.0.1011784)
Avaya Aura® Session Border Controller for Enterprise running on Virtual Environment	8.1.1 (8.1.1.0-26-19214)
Avaya 9611G IP Deskphone (H.323)	6.8304
Avaya J189 IP Deskphone (SIP)	4.0.7.1.5
Avaya 9408 Digital Deskphone	20.6
RSI Shadow OSN/CMS	5.3.5.0
RSI Winlink Remote BCMS application	1.1.1.0

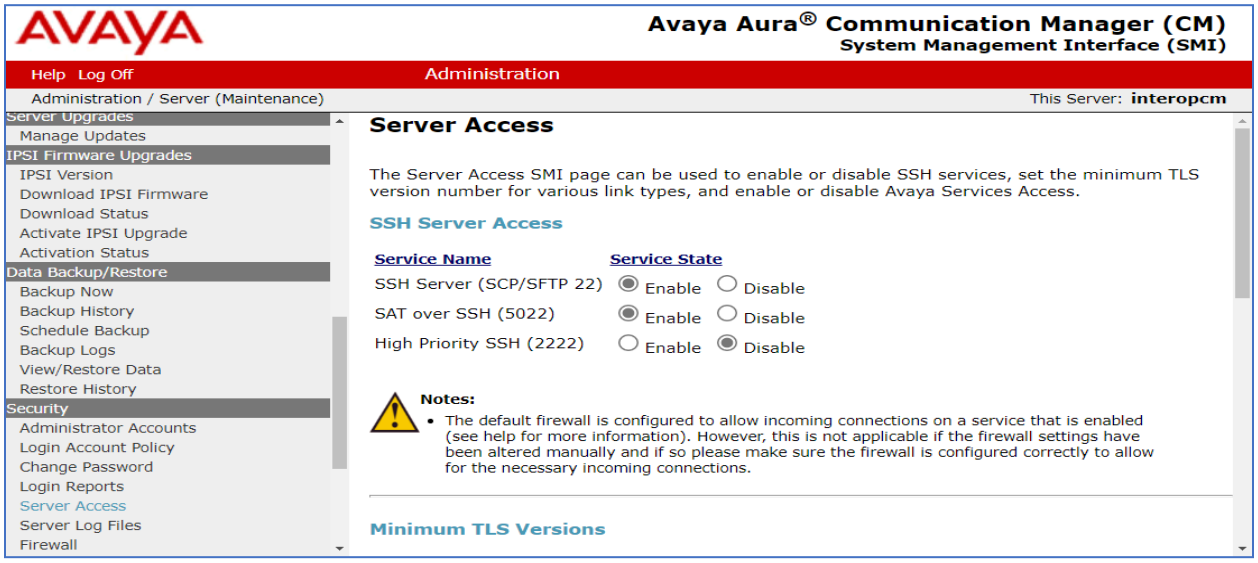
5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager.

5.1. Configure Server Access

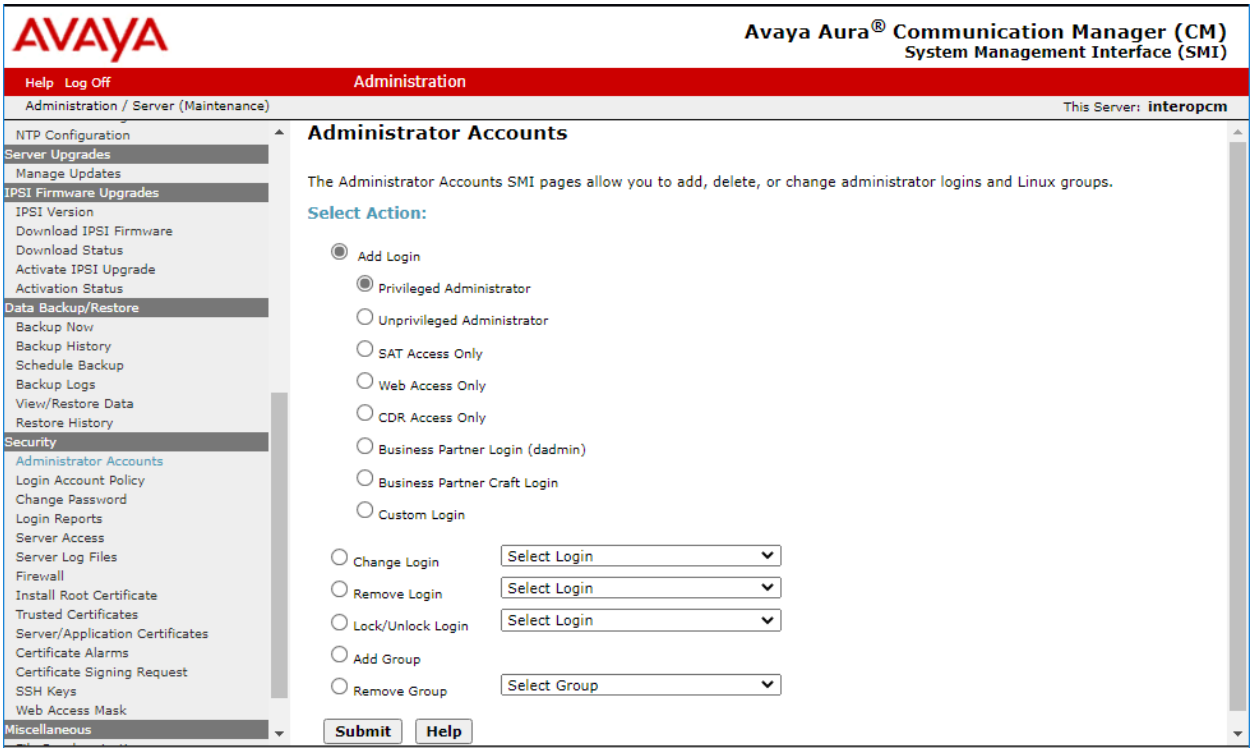
From a web browser, use the http://<ip-address>, where ip-address is the IP address of Communication Manager URL to access System Management Interface for Communication Manager. Log in using appropriate credentials.

Navigate to **Administration / Server (Maintenance) → Security → Server Access** and ensure that the **SAT over SSH (5022)** is enabled. This is the port that Shadow OSN will connect to Communication Manager to collect the required station information.

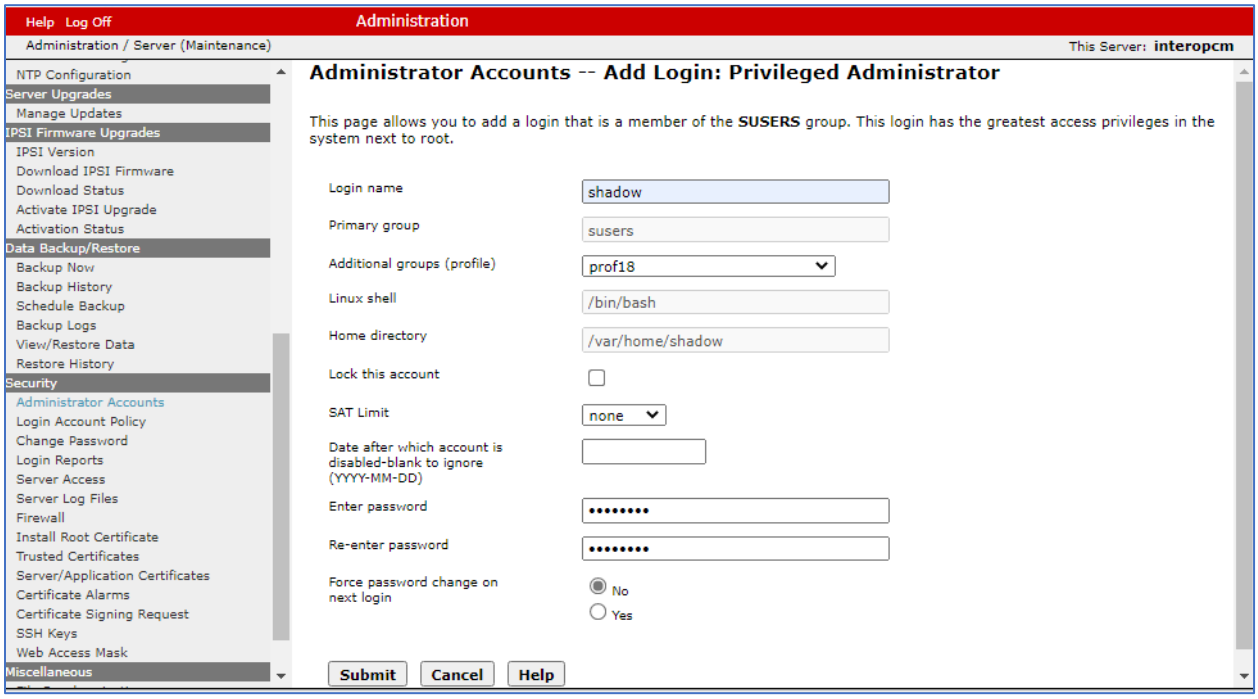


Add a username for the Shadow OSN to connect to Communication Manager via SAT to obtain the station location information.

Create a user account on Communication Manager by navigating to the **Administer Accounts** page under **Security** from the left-hand pane and selecting the radio button **Add Login** and **Privileged Administrator**. Click **Submit** to continue.



The Administrator Accounts -- Add Login screen is displayed. Enter a name to the Login name field and enter desired password. Select **Submit** to save the change.



5.2. Verify License

The following configuration in Communication Manager was performed using the System Access Terminal (SAT).

Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the "display system-parameters customer-options" command to verify that the **Hospitality (Basic)** and **Hospitality (G3V3 Enhancements)** customer option is set to "y" on **Page 5**. If this option is not set to "y", then contact the Avaya sales team or business partner for a proper license file.

```
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? n
                  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? y
  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

           IP Attendant Consoles? y
        (NOTE: You must logoff & login to effect the permission changes.)
```

5.3. Configure Site Data

The following configuration in Communication Manager was performed using the System Access Terminal (SAT).

To configure specific building codes and floor information for a site, use **change site-data** command. On **Page 1**, add entries for building fields. For example, two entries of **AA1** and **AA2** were added. On **Page 3**, add entries for floor fields. For example, one entry of **AA1-F1** and **AA2-F1** were added.

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

  AA1
  AA2
```

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


  AA1-F1
  AA2-F1
```

5.4. Configure Station

Use **add station n** command to add a station, where **n** is an available station extension. This station is a sample station that was used during compliance testing to dial emergency calls. 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**.

```
add station 3301                                                Page   1 of   6
                                     STATION

Extension: 3301                          Lock Messages? n               BCC: 0
     Type: 9641                          Security Code: *                TN: 1
     Port: S000011                     Coverage Path 1:                COR: 1
     Name: H323-3301                   Coverage Path 2:                 COS: 15
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: 3301
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                  Button Modules: 1
 Survivable GK Node Name: lsp
          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, enter the site data information, as shown below. The floor and building information are configured based on the information configured previously.

```
add station 3301                                                Page   4 of   6
                                     STATION
 SITE DATA
       Room: Ottawa                                       Headset? n
       Jack: J3301                                        Speaker? n
      Cable: C-H32                                       Mounting: d
      Floor: AA1-F1                                   Cord Length: 0
   Building: AA1                                        Set Color:

ABBREVIATED DIALING
     List1:                     List2:                     List3:




BUTTON ASSIGNMENTS
 1:call-appr                             5:manual-in           Grp:
 2:call-appr                             6:after-call          Grp:
```

5.5. Configure Crisis Alert

Use change **system-parameters crisis-alert** command and set **Every User Responds** to **y**. Note that the parameter "**Every User Responds?**" is enabled or not, the crisis alert is still sent out as user places an emergency call, during the testing the configuration was enabled.

```
change system-parameters crisis-alert                          Page   1 of   1
                         CRISIS ALERT SYSTEM PARAMETERS
ALERT STATION
    Every User Responds? y

ALERT PAGER
            Alert Pager? n
```

5.6. Administer IP Node Names

Use the **change node-names ip** command to create a new node name for the server running **Shadow OSN**. This node name is associated with the IP address of the server. In the sample configuration **ShadowOSN** was used for the name and **10.33.100.51** was used for the IP address. Also, take note of the node name **procr**. It will be used in the next step. The **procr** entry on this form was previously administered.

```
change node-names ip                                           Page   1 of   2
                                   IP NODE NAMES
    Name               IP Address
AMS1                10.33.1.30
CMS19               10.33.1.18
procr               10.33.1.6
ShadowOSN           10.33.100.51
```

5.7. Configure PMS_JOURNAL Port

Use the **change ip-services command** to define the **PMS_JOURNAL** service on Communication Manager. Shadow OSN will listen on this port to capture any emergency alerts that will be generated by Communication Manager. To define a PMS_JOURNAL service, provide the following information:

- **Service Type**: **PMS_JOURNAL**
- **Local Node**: **procr**, that is the processor Ethernet of Communication Manager.
- **Local Port**: 0
- **Remote Node**: **ShadowOSN**
- **Remote Port**: **8901**, the remote port may be set to a value between 5000 and 64500 inclusive, and must match the port configured in Shadow OSN.

```
change ip-services                                             Page   1 of   4

                                   IP SERVICES
 Service     Enabled     Local        Local       Remote      Remote    TLS
```

```
  Type                    Node          Port        Node         Port
Encryption
PMS_JOURNAL           procr             0        ShadowOSN       8901
```

For this solution the Reliable Session Protocol (RSP) is not used. On **Page 3** of the ip-services form, set the **Reliable Protocol** field to **n**.

```
change ip-services                                            Page   3 of   4

                              SESSION LAYER TIMERS
  Service     Reliable  Packet Resp   Session Connect  SPDU  Connectivity
   Type       Protocol     Timer       Message Cntr    Cntr     Timer

 PMS_JOURNAL      n         30                 3          3         60
```

5.8. Configure Hospitality

Use change system-parameters hospitality command to assign the PMS_JOURNAL configured in **Section 5.6** to **Journal/Schedule Endpoint** field as shown below.

```
change system-parameters hospitality                          Page   1 of   3
                              HOSPITALITY

                      Message Waiting Configuration: act-nopms
               Controlled Restrictions Configuration: act-nopms
               Housekeeper Information Configuration: act-nopms
                     Number of Housekeeper ID Digits: 2
                                   PMS Log Endpoint:
                          Journal/Schedule Endpoint: PMS_JOURNAL
             Client Room Coverage Path Configuration: act-nopms
              Default Coverage Path for Client Rooms:
             Forward PMS Messages to Intuity Lodging? n
```

5.9. Configure ARS Routing

Use the **change ars analysis 911** command to configure 911 calls to route them appropriately and enable crisis alerts. The following configuration shows that when 911 is dialed, the call is routed over route pattern 3 and a crisis alert is generated by Communication Manager.

- Set **Dialed String** to **911**.
- Set **Total Min** and **Max** to **3**.
- Set **Route Pattern** to a valid pattern that is already configured in Communication Manager to route correctly to PSTN.
- 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     3        alrt         n
    *08                   10   15    8        pubu         n
```

6. Configure RSI Shadow Onsite Notification

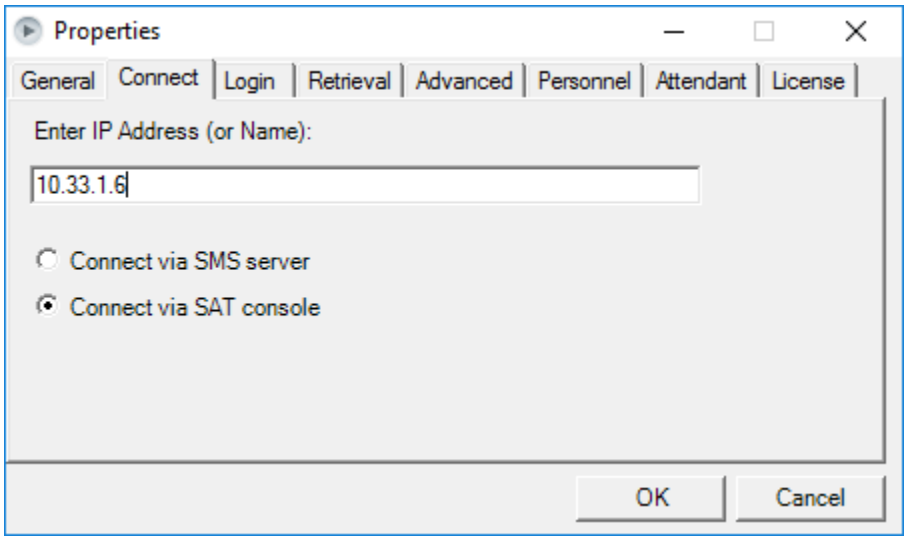
This section provides the procedures for configuring and testing the Shadow OSN software to capture Avaya Crisis Alert data and generate the user specified alert notifications. The procedures include the following areas:

- Configure Winlink Remote BCMS
- Configure Shadow WinLink to capture crisis alerts
- Configure Shadow OSN to generate 911 Alert Notifications

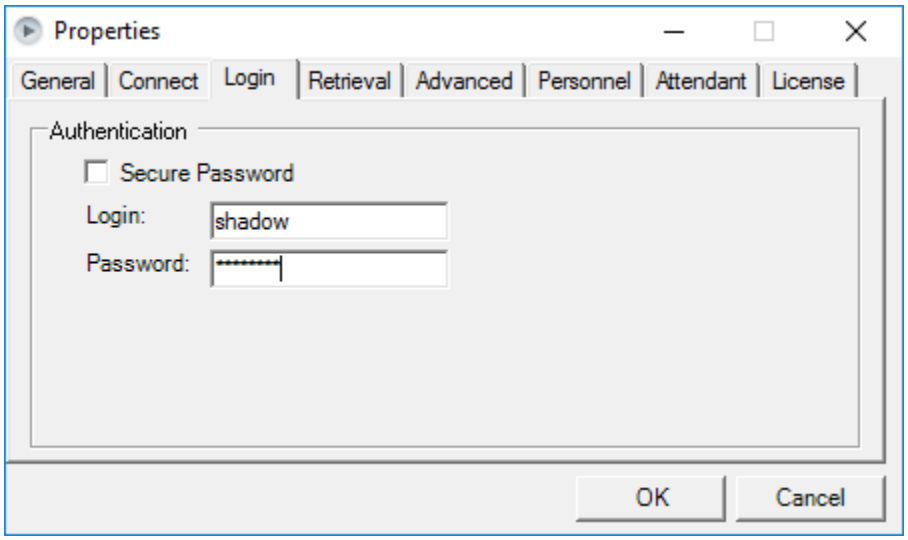
6.1. Configure Winlink Remote BCMS

Using the Winlink Remote BCMS application to establish a SSH connection to Communication Manager to obtain station's location information.

Launch the Winlink Remote BCMS application from the menu **Start** (not shown), the **Winlink Remote BCMS** application displays. Select the **Properties** button (not shown), the **Properties** window displays. Select **Connect** tab, enter the IP address of Communication Manager in the **Enter IP Address (or Name)** field and select option **Connect via SAT console**.

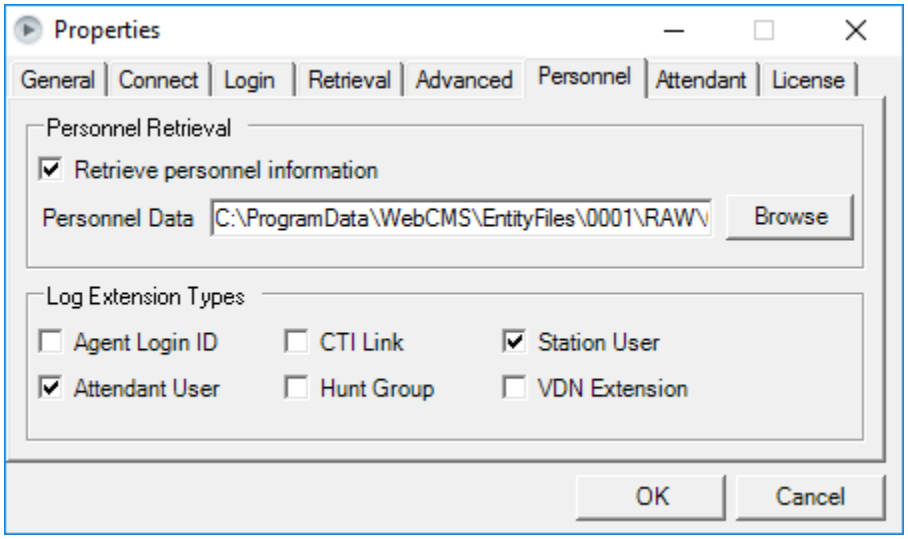


Continue to select the **Login** tab, enter the username configured in **Section 5.1** and its password in the **Login** and **Password** fields and leave other tabs at default.

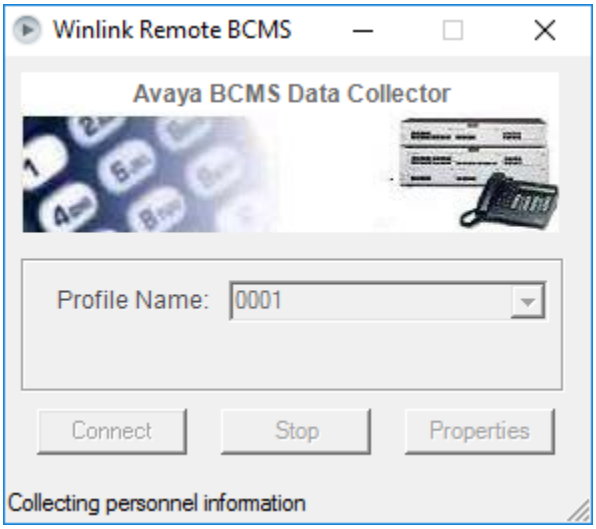


Select the **Personnel** tab, in the **Personnel Retrieval** section select the **Retrieve personnel information** check box and point to a text file by selecting the **Browse** button, the original text file is a blank file and, the station location will be saved later as the Winlink application makes a connection to Communication Manager via SAT and pull out all station location s and save it to the text file and then will be used for the crisis alert. In the **Log Extension Types** section, select **Station User** and **Attendant User** check boxes. Note that the **Attendant User** check box is selected during the testing, depends on customer's system the other check boxes can be selected.

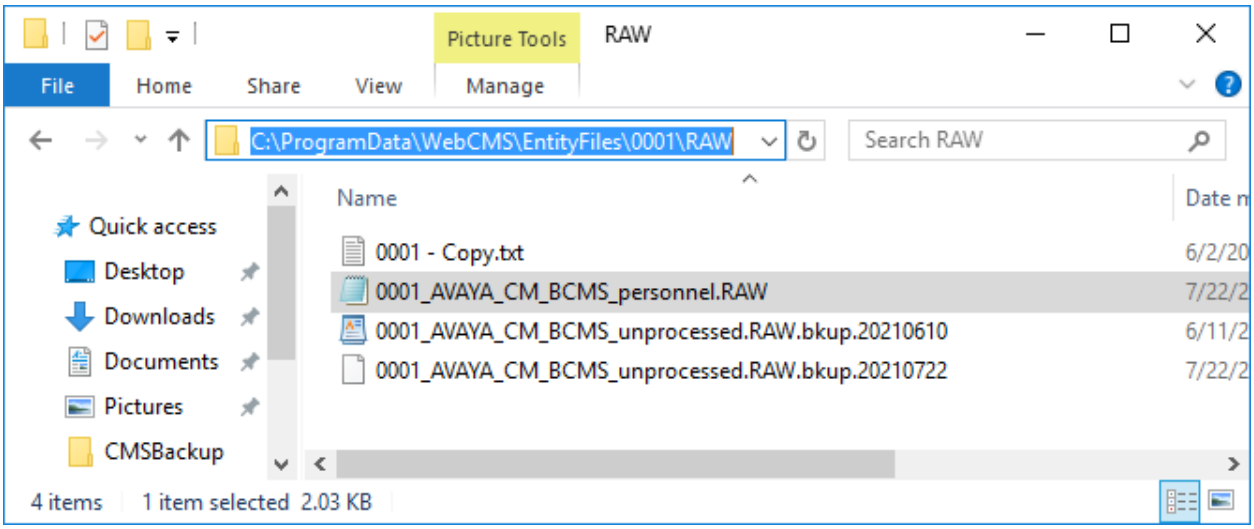
Select **OK** to save changes.



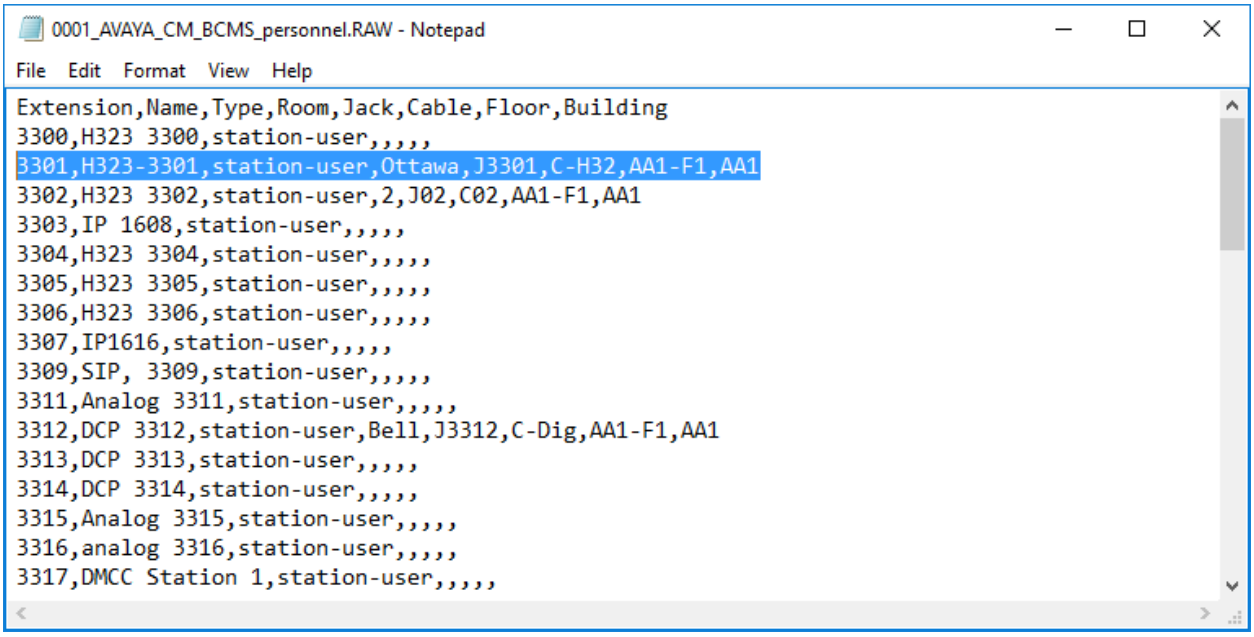
Select **Connect** to start connecting to Communication Manager to obtain the station location information. Note that the Winlink application is configured to pull out the location based on schedule and manually depending on the customer need.



The station location information is saved under filename "0001_AVAYA_CM_BCMS_personnel.RAW" and in the path below.



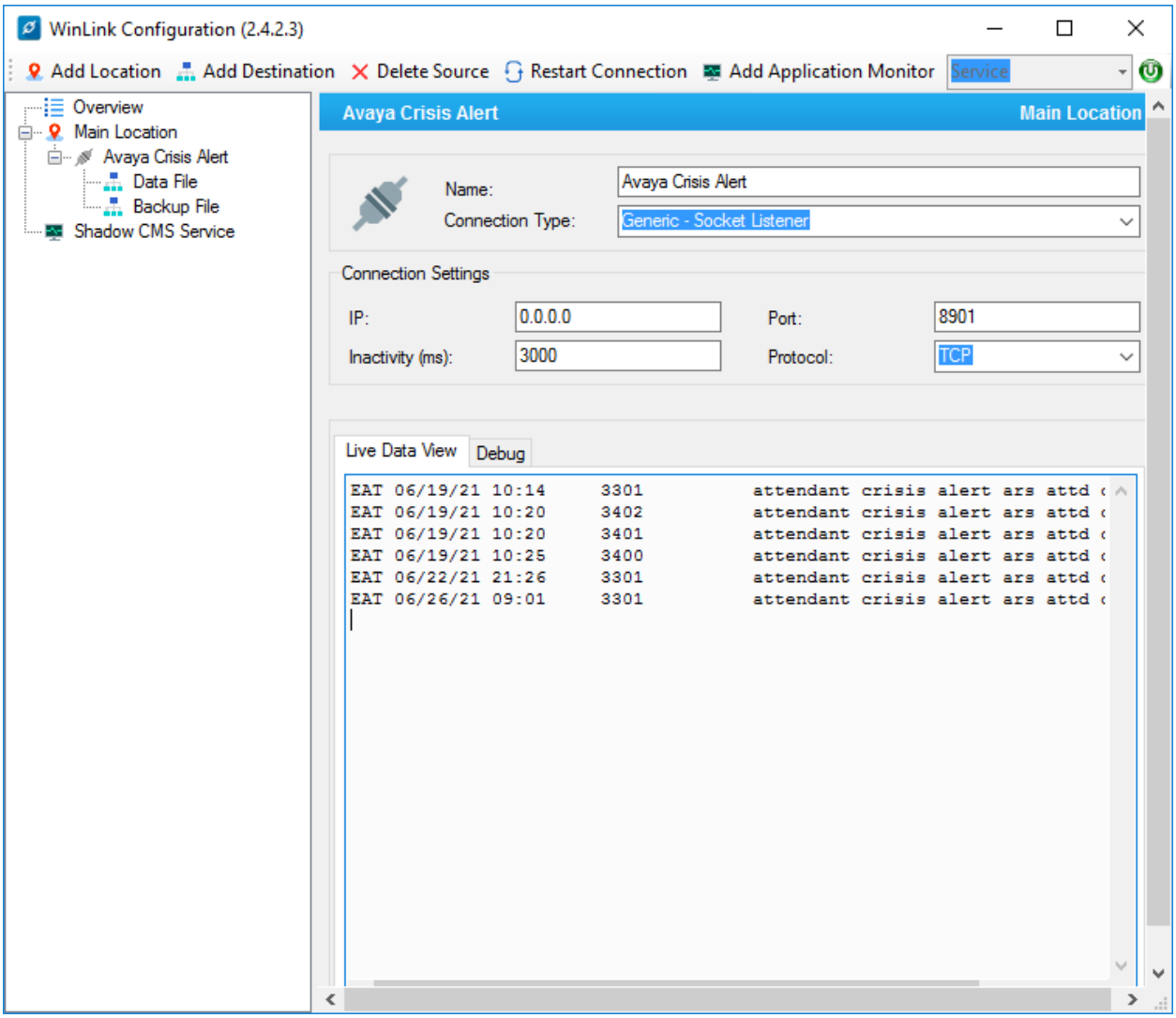
Open the filename “0001_AVAYA_CM_BCMS_personnel.RAW”, the station location information of all stations is successfully obtained as highlighted and shown in the screenshot below.




```
Extension,Name,Type,Room,Jack,Cable,Floor,Building
3300,H323 3300,station-user,,,,,
3301,H323-3301,station-user,Ottawa,J3301,C-H32,AA1-F1,AA1
3302,H323 3302,station-user,2,J02,C02,AA1-F1,AA1
3303,IP 1608,station-user,,,,,
3304,H323 3304,station-user,,,,,
3305,H323 3305,station-user,,,,,
3306,H323 3306,station-user,,,,,
3307,IP1616,station-user,,,,,
3309,SIP, 3309,station-user,,,,,
3311,Analog 3311,station-user,,,,,
3312,DCP 3312,station-user,Bell,J3312,C-Dig,AA1-F1,AA1
3313,DCP 3313,station-user,,,,,
3314,DCP 3314,station-user,,,,,
3315,Analog 3315,station-user,,,,,
3316,analog 3316,station-user,,,,,
3317,DMCC Station 1,station-user,,,,,
```

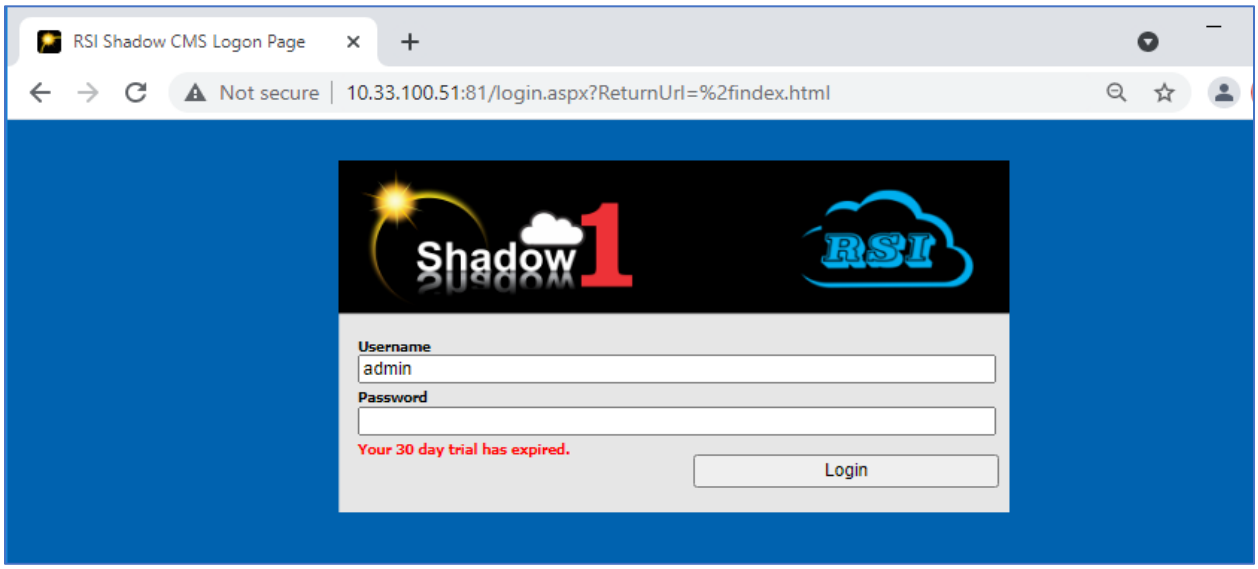
6.2. Configure WinLink to Capture Crisis Alerts

Launch Winlink and configure it to be socket listener on PMS_JOURNAL port configured previously (port 8901 in this example in **Section 5.7**.

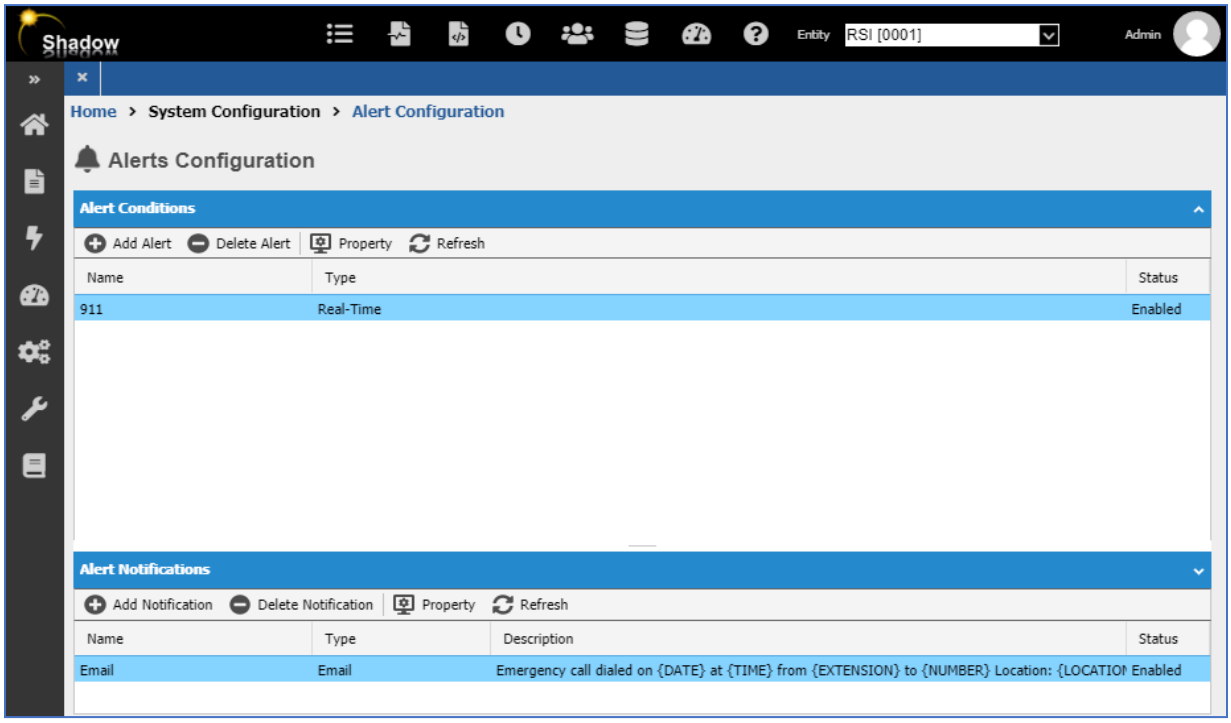


6.3. Configure Shadow OSN to Generate 911 Alert Notifications

Access to the Shadow OSN web interface by entering the IP address of Shadow OSN in the internet browser. Enter credentials to login.

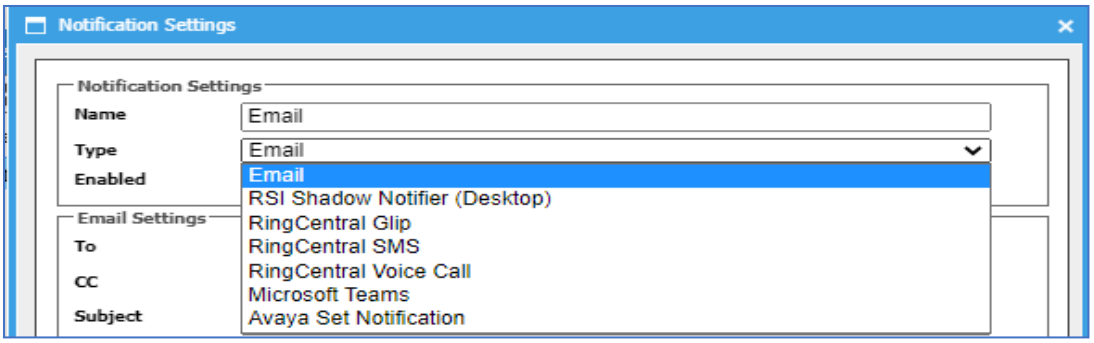


From the homepage, navigate to **Home → System Configuration → Alert Configuration** and press the **Add Alert** button and create an alert for Crisis Alert emergency calls. The name of the alert can be anything. It strongly recommends a descriptive name that clearly identifies the type of alert. The example below depicts this alert defined as "911".



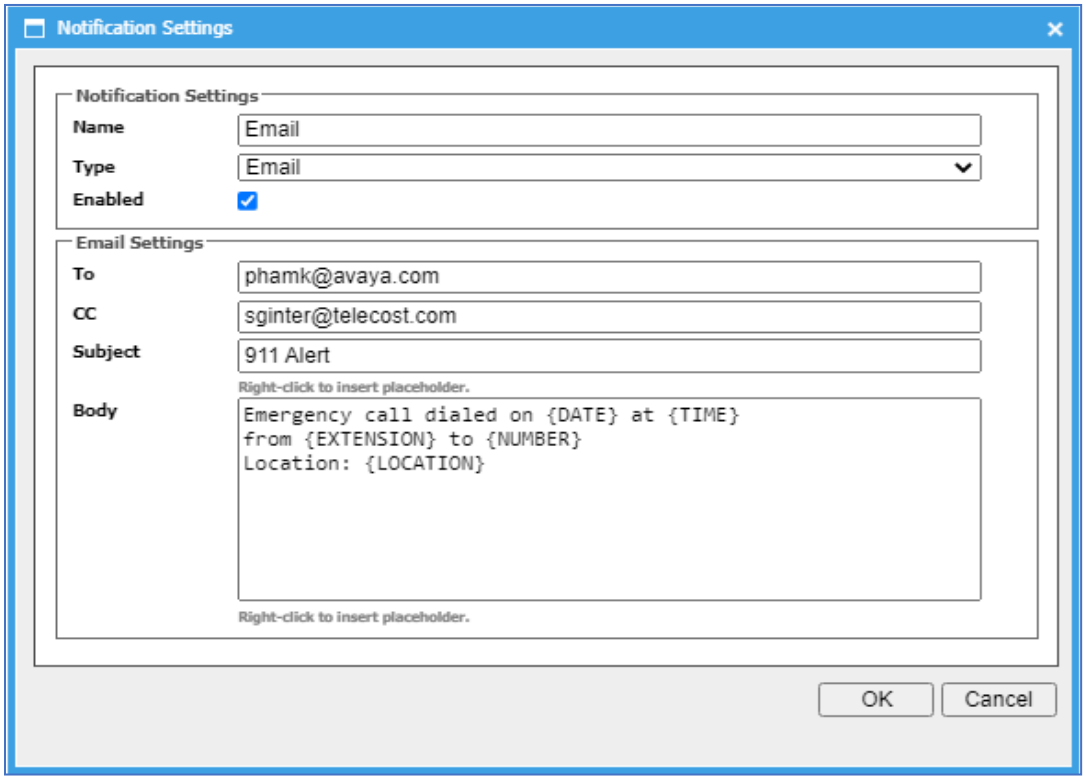
Press the **Add Notification** button to specify the type of alerts to be generated and the corresponding alert recipients. Possible Alert types are as follows:

1. Email
2. RSI Shadow Notifier (Desktop) – popup message to Windows based computer
3. Ring Central Slip
4. Ring Central SMS
5. Ring Central Voice Call
6. Microsoft Teams Meeting Room
7. Avaya Set Notification



During the testing, the **Email** type was used as the notification alert.

Repeat the above steps to create as many alert notification methods and recipients as required.



7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager and Shadow OSN.

7.1. Verify Emergency Alerts via SAT

Use the list emergency command to verify the alerts that were generated by Communication Manager as shown below:

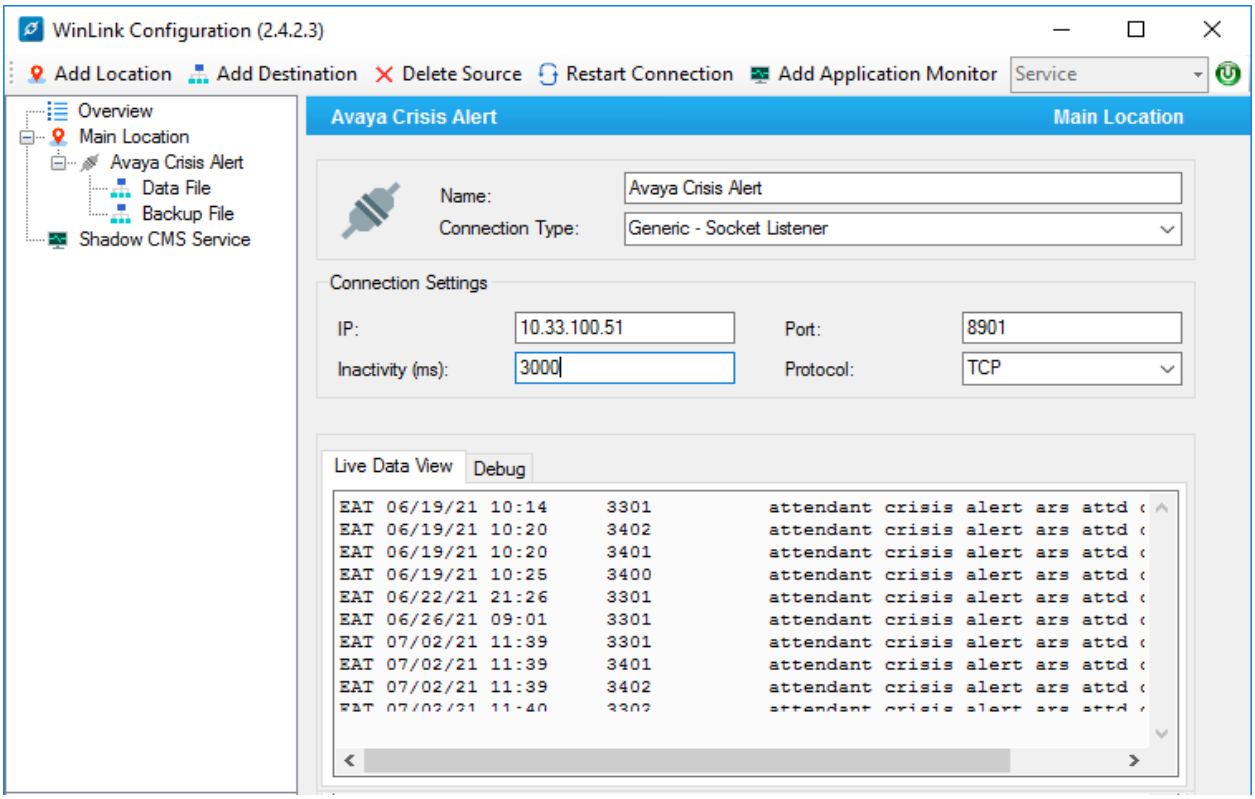
```
list emergency

                        EMERGENCY ACCESS CALLS

Caller                     Event            Type of Call          Date     Time
                                                                mm/dd/yy
3301                attd crisis alert    ars alrt call type     07/02/21 11:39 A
3401                attd crisis alert    ars alrt call type     07/02/21 11:39 A
3402                attd crisis alert    ars alrt call type     07/02/21 11:39 A
3302                attd crisis alert    ars alrt call type     07/02/21 11:40 A
```

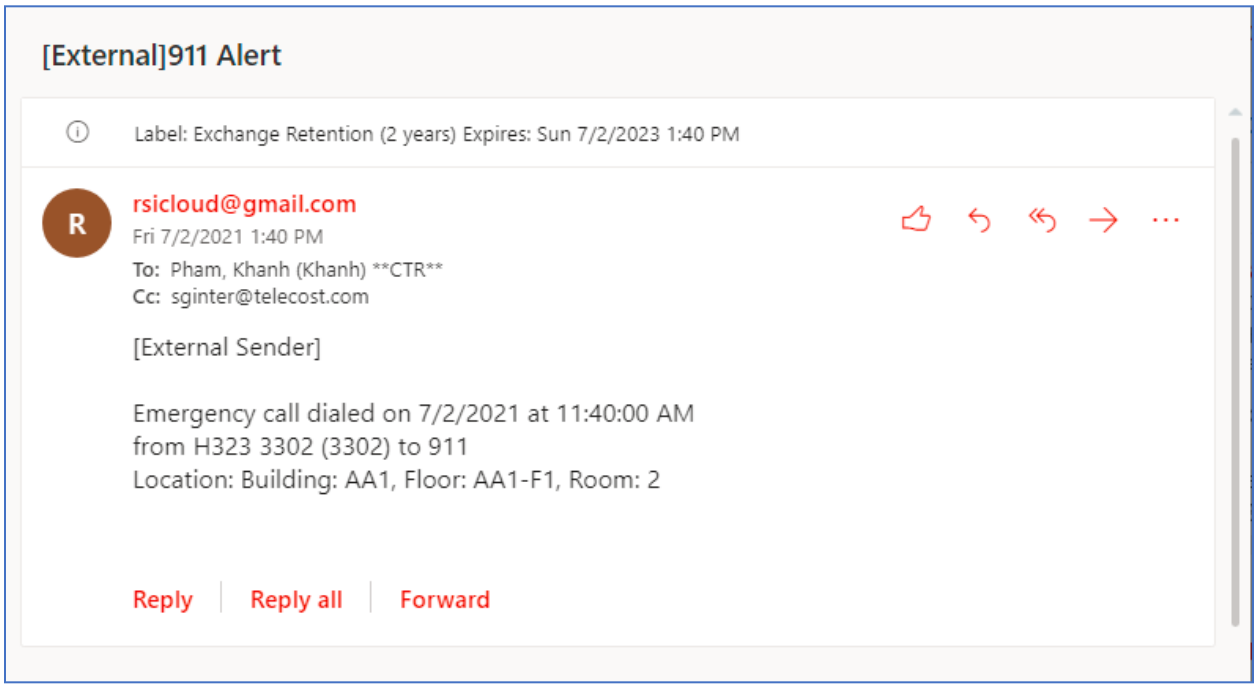
7.2. Test Shadow WinLink

View the WinLink user interface to confirm the WinLink application captured the Crisis Alert data generated by Communication Manger for the Crisis Alert emergency test call. The WinLink screen should display information similar to the text shown below.



7.3. Confirm the Alert Notifications were delivered to the Recipients

If the email notification is configured, the alert message will be delivered to the inbox and it looks similar to the following.



8. Conclusion

These Application Notes describe the configuration steps required for RSI Shadow OSN 5.3.5 to successfully interoperate with Avaya Aura® Communication Manager 8.1.3. All feature and serviceability test cases were completed in **Section 2.2**.

9. Additional References

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

This section references the documentation relevant to these Application Notes. Product documentation for Avaya, including the following, is available at: http://support.avaya.com/

[1] Administering Avaya Aura® Communication Manager (Release 8.1.3, Issue 5, February 2020)

[2] Administering Network Connectivity on Avaya Aura® Communication Manager (Release 8.1.3, Issue 2, August 2020), 555-233-504

[3] Avaya Aura® Communication Manager Feature Description and Implementation (Release 8.1.3, Issue 4, January 2020)

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.