Application Notes for 911 Secure LLC NG911 Emergency Location Management Solution with Avaya Aura® Application Enablement Services, Avaya Aura® Communication Manager and Avaya Aura® Session Manager - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring the 911 Secure LLC NG911 Emergency Location Management Solution to interoperate with Avaya Aura® Application Enablement Services, Avaya Aura® Session Manager and Avaya Aura® Communication Manager. The 911 Secure solution contains functionality for both E911 (Enhanced 911) and NG911 (Next Gen 911) implementations.

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 procedures for configuring the 911 Secure LLC NG911 Emergency Location Management Solution (hereafter, also referred to as “Sentry”) to interoperate with Avaya Aura® Application Enablement Services (AES), Avaya Aura® Session Manager (Session Manager) and Avaya Aura® Communication Manager (Communication Manager).

When an emergency call (e.g. 911) is placed, an organization’s ability to provide assistance to the first responders is a crucial component in keeping employees, customers, patients, guests, and others safe. Some of the immediate responsibilities of the organization include identifying the caller’s exact location and notifying on-site personnel that an emergency call has been made.

Sentry is a tool to assist enterprises in protecting themselves and their customers in an emergency. By providing on-site notification to key personnel, via screen pops or e-mail, first responders may quickly be directed to the emergency. In addition, database management facilities ensure that the right information is sent to the Public Safety Answering Point (PSAP), and that the call is directed to the right place.

Sentry integrates via the use of Sentry Scouts. Sentry Scouts are services that run on the Sentry Server.

- Sentry Scout for Avaya Aura®: Used for H.323, Analog and Digital Phones
- Sentry Scout for Avaya Aura® Session Manager: Used for SIP Phones

When an IP phone’s location is detected on the network, the Sentry Scout for Avaya Aura® will push the phone’s Emergency Location Extension (ELE), Building, Floor and Room to Communication Manager via the System Management Service (SMS) interface of Application Enablement Services. Additionally, the Sentry Scout for Avaya Aura® utilizes the Device, Media, and Call Control (DMCC) interface of AES to receive an event when an emergency call has been placed. This mode is used for all H.323, Digital and Analog stations.

For SIP endpoints, the Sentry Scout for Avaya Aura® Session Manager subscribes to Session Manager as a listener to send and receive PUBLISH messages for SIP endpoints, but does not receive emergency-alerts from Session Manager. Instead, it relies upon a crisis alert softphone being defined in Communication Manager and a DMCC connection through AES web services to receive crisis alerts which in turn will create the emergency alerts in Sentry. The Sentry Scout for Avaya Aura® Session Manager also allows for tracking the ELE of multiple registrations of a SIP User from different locations.

During the compliance testing, integration of Sentry with Sentry Gatekeeper and Sentry Dispatcher was also successfully performed. However, that configuration is out of scope for this document. For more information, please refer to documentation in Section 11.
2. General Test Approach and Test Results

This section describes the general test approach used to verify the interoperability of the Sentry NG911 Solution with an Avaya infrastructure (consisting of Avaya Aura® Application Enablement Services, Avaya Aura® Session Manager and Avaya Aura® Communication Manager). This section also covers the test results.

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 this Application Note, the interface between Avaya systems and the 911 Secure LLC NG911 Emergency Location Management Solution utilized TLS.

2.1. Interoperability Compliance Testing

The general test approach was to verify the integration of Sentry with AES, Session Manager and Communication Manager. Various emergency calls were placed from Avaya non-SIP endpoints (i.e. analog, digital, and H.323 endpoints) and SIP end points to an emergency number to verify the events were properly logged by the Sentry NG911 in a timely manner. Sentry was also verified to ensure they update the correct ELE, Building, Room and Floor information on the endpoints.

2.2. Test Results

The 911 Secure LLC NG911 Emergency Location Management Solution successfully passed compliance testing.

2.3. Support

For technical support on the 911 Secure LLC NG911 Emergency Location Management Solution, contact 911 Secure LLC at:
- Web: http://www.911secure.com/
- Phone: (213) 425-2050
Email: support@911secure.com
3. Reference Configuration

Figure 1 below illustrates the reference configuration used during compliance testing. The 911 Secure LLC Sentry Sentinel Server was installed on a Windows Server 2016 Standard operating system running on a virtualized environment. Sentry Gatekeeper client was installed on a Windows 10 Enterprise workstation. Sentry Sentinel Server communication with Sentry Dispatcher was via the internet.

![Diagram of Reference Configuration](image-url)

Figure 1: Sentry NG911 Emergency Location Management Solution with AES, Session Manager and Communication Manager
4. Equipment and Software Validated

The following equipment and version were used in the reference configuration described above:

<table>
<thead>
<tr>
<th>Equipment/Software</th>
<th>Release/Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Aura® Communication Manager running on virtualized environment</td>
<td>8.1.1</td>
</tr>
<tr>
<td>Avaya Aura® Session Manager running on virtualized environment</td>
<td>8.1.1</td>
</tr>
<tr>
<td>Avaya Aura® Application Enablement Services running on virtualized environment</td>
<td>8.1.1</td>
</tr>
<tr>
<td>Avaya Aura® System Manager running on virtualized environment</td>
<td>8.1.1</td>
</tr>
<tr>
<td>Avaya Aura® Media Server running on virtualized environment</td>
<td>8.0.2</td>
</tr>
<tr>
<td>Avaya G450 Media Gateway</td>
<td>FW 41.9.1</td>
</tr>
<tr>
<td>Avaya Endpoints:</td>
<td></td>
</tr>
<tr>
<td>• 9641 (SIP)</td>
<td>7.1.7</td>
</tr>
<tr>
<td>• 9611 (H323)</td>
<td>6.8.3</td>
</tr>
<tr>
<td>• J159 (H323)</td>
<td>6.8.3</td>
</tr>
<tr>
<td>• J169 (SIP)</td>
<td>4.0.3</td>
</tr>
<tr>
<td>Avaya one-X® Communicator</td>
<td>2.6.10</td>
</tr>
<tr>
<td>Avaya 9404 Digital station</td>
<td>FW 18</td>
</tr>
<tr>
<td>Avaya Analog station</td>
<td>N/A</td>
</tr>
<tr>
<td>911 Secure LLC Sentinel Sentry server (Windows Server 2016 Standard)</td>
<td>1.11.316.1</td>
</tr>
<tr>
<td>Sentry External Tracker</td>
<td>v20200305.1</td>
</tr>
<tr>
<td>Sentry Dispatcher</td>
<td>-</td>
</tr>
<tr>
<td>Sentry Gatekeeper</td>
<td>1.2.42</td>
</tr>
</tbody>
</table>
5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Avaya Aura® Communication Manager as provisioned in the reference configuration (Figure 1). The assumption has been made that the basic configuration for connectivity between Communication Manager and AES has already been completed.

The configuration of Communication Manager was performed using the System Access Terminal (SAT) and web interface. After the completion of the configuration in SAT, perform a save translation command to make the changes permanent. The procedures include the following areas:

- Create User account on Communication Manager
- Create an IP Softphone with a Crisis Alert Button
- Configure Crisis Alert
- Configure an Emergency Number

**Note:** This section is only required if there are H.323, Digital and/or Analog endpoints in the environment. If the environment only has SIP endpoints, then a Communication Manager-based user account and crisis alert extension are not required.

5.1. Create User Account on Communication Manager

Access the Communication Manager System Management Interface by using the URL https://<ip-address> in an Internet browser window, where <ip-address> is the IP address of Communication Manager. Click the “Continue” link (not shown). The Login screen is displayed (not shown). Log in using appropriate credentials. The main screen of the System Management Interface is seen as shown below. Navigate to Administration → Server (Maintenance).
Navigate to Security ➔ Administrator Accounts as shown below. Select the Privileged Administrator radio button and click on Submit.
Configure the following fields:

- **Login name**: A descriptive name
- **Enter password or key**: Enter a valid password
- **Re-enter password or key**: Confirm the above entered password

Retain default values for all other fields and click on **Submit** (not shown).

Note the **Login name** and **Password** for it is required in the configuration to be shown in Section 8.1.
5.2. Create an IP Softphone with a Crisis Alert Button

Use the add station command to create a soft phone with a crisis alert button. This information is required in the configuration to be shown in Section 8.1.

- A valid Extension must be entered as part of the add station <extension> command
- Set Type to 9641
- Enter a descriptive Name (optional)
- Set the Security Code
- Set IP Softphone to y

```
add station 77771

STATION

Extension: 77771
Type: 9641
Port: IP
Name: Sentry CRSS Alert
Unicode Name? n

STATION OPTIONS

Lock Messages? n
BCC: 0
Security Code: *
TN: 1
Coverage Path 1: COR: 1
Coverage Path 2: COS: 1
Hunt-to Station:
Tests? y

Time of Day Lock Table:
Loss Group: 19
Personalized Ringing Pattern: 1
Message Lamp Ext: 77771
Display Language: english
Speakerphone: 2-way
Mute Button Enabled? y
Button Modules: 0
Survivable GK Node Name:
Survivable COR: internal
Survivable Trunk Dest? y
Media Complex Ext:
IP SoftPhone? y
IP Video Softphone? n
Short/Prefixed Registration Allowed: default
Customizable Labels? y
```

On Page 4, add a crisis alert button (**crss-alert**). As a result of adding this button, the station will receive an alert when an emergency number has been dialed. The Sentry NG911 Solution uses DMCC to monitor this station in order to receive an event when an emergency number has been dialed. Sentry logs the event and can take additional action such as notifying key personnel on-site via screen pops or e-mail. During compliance testing, only the logged events were verified (via their Sentinel web interface and Beacon Alert Tool) to ensure their timely delivery and accuracy. Additional actions that 911 Secure LLC may take to relay the data (e.g. generating a screen-pop or email) were beyond the scope of compliance testing.
5.3. Configure Crisis Alert

Use the `change system-parameters crisis-alert` command and change `Every User Responds` to `y`. This ensures that other endpoints with crisis alert buttons will keep ringing even after Sentry acknowledges an alert and generates a Sentry Beacon alert or email notification.

If multi tenants are configured on Communication Manager, use the `change system parameters features` command and set `Allow Crisis Alert Across Tenants` to `y` on Page 10 (not shown). This ensures that extensions in tenants other than the Sentry crisis alert station will not trigger a crisis alert. If this parameter is not changed to `y` then users will need to set up crisis alerts stations (requiring a DMCC license and basic TSAPI license) for each tenant.
5.4. Configure an Emergency Number

During compliance testing, the Communication Manager was connected to a simulated PSAP.

To create an emergency number, use the `change ars analysis` command to enter a Dialed String that has a Call Type of **alrt**. 211 digits were used to generate crisis alerts.

<table>
<thead>
<tr>
<th>Dialed String</th>
<th>Total</th>
<th>Route</th>
<th>Call Type</th>
<th>Node</th>
<th>ANI Reqd</th>
</tr>
</thead>
<tbody>
<tr>
<td>211</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>alrt</td>
<td>n</td>
</tr>
</tbody>
</table>
6. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Avaya Aura® Application Enablement Services as provisioned in the reference configuration (Figure 1). The assumption has been made that the basic configuration for connectivity between Communication Manager and AES has already been completed. The procedures include the following areas:

- Login
- Enable DMCC Unencrypted Port
- Add User
- Edit User
- Switch Connection Name and PROCR IP Address

Note: This section is only required if there are H.323, Digital and/or Analog endpoints in the environment. If the environment only has SIP endpoints, then AES is not required.

6.1. Login

Access the AES OAM web-based interface by using the URL https://<ip-address> in an Internet browser window, where <ip-address> is the IP address of the AES server. Click the “Continue to Login” link (not shown). The Login screen is displayed as shown below. Log in using appropriate credentials.
The Welcome to OAM screen is displayed, as shown below.

![OAM Welcome Screen](image)

Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- **AE Services** - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- **Communication Manager Interface** - Use Communication Manager Interface to manage switch connection and deletion.
- **High Availability** - Use High Availability to manage AE Services HA.
- **Licensing** - Use Licensing to manage the license servers.
- **Maintenance** - Use Maintenance to manage the routine maintenance tasks.
- **Networking** - Use Networking to manage the network interfaces and ports.
- **Security** - Use Security to manage Linux user accounts, certificates, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- **Status** - Use Status to obtain server status information.
- **User Management** - Use User Management to manage AE Services users and AE Services user-related resources.
- **Utilities** - Use Utilities to carry out basic connectivity tests.
- **Help** - Use Help to obtain a few tips for using the OAM Help system.

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.
6.2. Enable DMCC Unencrypted Port

Navigate to Networking → Ports to enable DMCC Encrypted Port “4722”. Click the Apply Changes button (not shown).
6.3. Add User

Navigate to User Management → User Admin → Add User to create a DMCC user login and password. Enter appropriate values for User Id, Common Name, Surname, User Password, and Confirm Password. Set the CT User to “Yes”. Click the Apply button (not shown).
6.4. Edit User

Navigate to Security → Security Database → CTI Users → List All Users. Select the User ID (i.e. sentry) created in the previous step and click the Edit button.

![CTI Users table](image)

- **Calabrio**
  - User ID: Calabrio
  - Common Name: calabrio
  - Workgroup Name: NONE
  - Device ID: NONE
- **esuser**
  - User ID: esuser
  - Common Name: esuser
  - Workgroup Name: NONE
  - Device ID: NONE
- **interop**
  - User ID: interop
  - Common Name: interop
  - Workgroup Name: NONE
  - Device ID: NONE
- **intradiem**
  - User ID: intradiem
  - Common Name: intradiem
  - Workgroup Name: NONE
  - Device ID: NONE
- **intranext**
  - User ID: intranext
  - Common Name: intranext
  - Workgroup Name: NONE
  - Device ID: NONE
- **mierec**
  - User ID: mierec
  - Common Name: mierec
  - Workgroup Name: NONE
  - Device ID: NONE
- **mindrouter1**
  - User ID: mindrouter1
  - Common Name: mindrouter1
  - Workgroup Name: NONE
  - Device ID: NONE
- **ntrouter1**
  - User ID: ntrouter1
  - Common Name: ntrouter1
  - Workgroup Name: NONE
  - Device ID: NONE
- **ntrole1**
  - User ID: ntrole1
  - Common Name: ntrole1
  - Workgroup Name: NONE
  - Device ID: NONE
- **sentry**
  - User ID: sentry
  - Common Name: sentry
  - Workgroup Name: NONE
  - Device ID: NONE
- **trio**
  - User ID: trio
  - Common Name: trio
  - Workgroup Name: NONE
  - Device ID: NONE
Check the box for **Unrestricted Access** to give the user the ability to monitor the station added in **Section 5, Step 1**. Click the **Apply Changes** button.
6.5. Switch Connection Name and PROCR IP Address

As mentioned in the beginning of Section 6, assumption has been made that the basic configuration for connectivity between Communication Manager and AES has already been completed. This section is shown here only for reference to obtain the Switch Connection Name and PROCR IP Address that is required in the configuration to be shown in Section 8.1.

Navigate to Communication Manager Interface → Switch Connections. Note down the Connection Name configured, in this case “cm81”. Click on the Edit PE/CLAN IPs (not shown) button to note down the IP Address of the PROCR, in this case “10.64.110.213”.

![Communication Manager Interface Switch Connections](image-url)
7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The assumption has been made that the basic configuration for connectivity between Communication Manager and Session Manager has already been completed as mentioned in Section 5. The procedures include the following areas:

- Launch System Manager
- Administer Domain
- Administer locations
- Administer SIP entity
- Obtain Session Manager SIP Entity IP Address
- Link the ELIN entity
- Configure Emergency Dial Pattern
- Import Sentry TLS Certificate

Note: This section is only required if there are SIP endpoints in the environment. If the environment only has H.323, Digital and Analog endpoints and no SIP endpoints, then this section is not required.

7.1. Launch System Manager

Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.
7.2. Administer Domain

In the subsequent screen (not shown), select **Elements → Routing** to display the **Introduction to Network Routing Policy** screen below. Select **Routing → Domains** from the left pane, and click **New** in the subsequent screen (not shown) to add a new domain.

The **Domain Management** screen is displayed. In the **Name** field enter the domain name, select **sip** from the **Type** drop down menu and provide any optional **Notes**.

![Domain Management Screen](image)
7.3. Administer Locations

Select **Routing → Locations** from the left pane, and click **New** in the subsequent screen (not shown) to add a new location for Trio Enterprise.

The **Location Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name** and optional **Notes**. Retain the default values in the remaining fields.

Scroll down to the **Location Pattern** sub-section, click **Add** and enter the IP address of all devices involved in the compliance testing in **IP Address Pattern**, as shown below. Retain the default values in the remaining fields.
7.4. Administer SIP Entity

Add a new SIP entity for the 911 Secure LLC Sentinel Server.

Select Routing → SIP Entities from the left pane, and click New in the subsequent screen (not shown) to add a new SIP entity for Sentinel Server.

The SIP Entity Details screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of the Sentinel Server.
- **Type:** “ELIN server”
- **Notes:** Any desired notes.
- **Location:** Select the location name from Section 7.3.
- **Time Zone:** Select the applicable time zone.
Scroll down to the **Entity Links** sub-section, and click **Add** to add an entity link. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case “sm81”.
- **Protocol:** “TLS”
- **Port:** “5061”
- **SIP Entity 2:** The Sentinel Server entity name from this section.
- **Port:** “5061”

Note that only TLS protocol is supported by Sentry. Click on **Commit** button to complete the configuration.

### 7.5. Obtain Session Manager SIP Entity IP Address

On the left, select **SIP Entities** and note the IP Address of Session Manager. It will be used in **Section 8.1** when adding a Call Server for Session Manager.
7.6. Link the ELIN Entity

This section explains the linking of the ELIN entity as the ELIN server for the Session Manager instance.

From the System Manager home screen (not shown), select **Elements → Session Manager** to display the **Session Manager Dashboard** screen shown below. Select **Session Manager → Session Manager Administration** from the left pane, and under the **Global Settings tab** for the **ELIN SIP Entity** field, select the Sentry SIP entity configured in **Section 7.4**. Retain default values for all other fields and click on the **Commit** button to save the configuration.

Note: with **Enable Application Sequence for Emergency Calls** checked, Session Manager skips origination processing and uses application sequencing for emergency calling. As a result, the SIP phone dialing "911" uses the 911 dial pattern with the "emergency call" option enabled and skips CM features such as the public-unknown-numbering CPN prefix.
7.7. Configure Emergency Dial Pattern

Configure an Emergency dial pattern for Emergency calls. When a dial pattern is added as an Emergency dial pattern, Session Manager skips the Application Sequences configured for a SIP User. This allows for Session Manager to insert a SIP header call AP-Loc, which contains the ELIN for a SIP user. Navigate to Elements → Routing → Dial Patterns to add a new Dial Pattern. The following Dial pattern was added for call routing to Communication Manager.
7.8. Import Sentry TLS Certificate
This section explains the importing of the TLS certificate for ELIN communications.

From the System Manager home screen (not shown), select Services → Inventory to display the main Inventory screen shown below. Navigate to Manage Elements from the left pane and select the Session Manager Element. Click on the Manage Trusted Certificates from the More Actions drop down menu.

![Manage Trusted Certificates](image)

Click on the Add button on the Manage Trusted Certificate page.
In the **Add Trusted Certificate** screen shown below. Select **Import from File** radio button, and browse to the “SentryRootCA.cer” file which is typically found in the file path “C:\Program Files\911 Secure\Sentry” on the Sentry Sentinel server as shown in the screen below, after Sentry has been installed.

Click the **Retrieve Certificate** button and then the **Commit** button to import the Root certificate (not shown). A restart of the System Manager might be required for all of the above changes to take effect.
The **Trusted Certificates** screen is shown below after the certificates have been installed.
8. Configure 911 Secure LLC NG911 Emergency Location Management Solution

It is assumed that the Sentry server has been installed, configured, and is ready for the integration with Communications Manager or Session Manager. The Sentry Software Users Guide can be obtained by contacting 911 Secure LLC. The sub-sections below only provide the steps required to configure the 911 Secure LLC Sentry NG911 Location Management Solution to interoperate with Avaya Communications Manager or Avaya Session Manager.

8.1. Sentinel Web Interface

Access the Sentinel web interface by logging into the Sentry server, opening a web browser and entering the following URL: [http://localhost/Sentinel](http://localhost/Sentinel). If https support has been enabled and a server certificate using a FQDN has been generated and added to the server, then adjust the URL accordingly.

![Sentinel Web Interface](image1)

8.2. Configure Call Servers

Navigate to Configure → Call Servers as shown below to add a Call Server.

![Configure Call Servers](image2)
Two call servers need to be added, one for H.323, Analog and Digital endpoints (Communication Manager and AES) and another for SIP endpoints (Session Manager). From the Call Servers screen as shown below, select “Avaya Aura CM 7+” from the Select a call server type drop down box and click on the Create button. This Call Server is for integration with Communication Manager and AES for H.323, Analog and Digital endpoints.

In the Add Avaya Aura CM7+ screen as shown below, configure the following fields.

- **AES Version:** Select “AES 8.0.1+”.
- **Call Server Description:** A descriptive name.
- ***CM Username @ CM IP Address:** The Communication Manager username configured in Section 5.1 and IP Address/FQDN.
- ***CM Password:** The password created in Section 5.1.
- **ELIN Prefix:** Enter a prefix if 11 digits DID are not used.
- **CM Switch Connection Name:** The name configured in Section 6.5.
- ***CLAN/PROCR IP Address:** The IP Address or FQDN shown in Section 6.5.
- **AES IP Address:** IP Address or FQDN of AES.
- ***AES Username:** The username created in Section 6.4.
- ***AES Password:** The password created in Section 6.4.
- **AES DMCC Port:** The port configured in Section 6.2.
- **DMCC Secure Mode:** Check box.
- **SMS Service URL:** https://[AES_IP_or_FQDN]/sms/SystemManagementService.php
- **Enable Crisis Alerting:** Check the box.
- **Crisis Alert Extension:** This is the extension where the crisis alert key was configured as in Section 5.2.
- **Crisis Alert Extension Security Code:** The security code as configured in Section 5.2.
- **SM Entity Link TLS:** “Set to TLS 1.2”.

Retain default values for all other fields and click on the Submit button.
On the Call Server page, select Avaya Aura Session Manager 7.x and Create another Call Server. This Call Server is for integration with Session Manager for SIP endpoints.

In the Add Avaya Aura Session Manager 7.x screen, configure the following fields:

- **Call Server Description:** Enter a desired name.
- **Call Server IP Address:** Session Manager IP Address/FQDN from Section 7.5.
- **SIP Domain:** The domain from Section 7.2.
- **SM Entity Link Port:** The port defined from Section 7.4.
- **SM Entity Link TLS:** Set to “TLS 1.2”
- **SM Location Update Port:** The port defined from Section 7.4.
- **SM Location Update TLS:** Set to “TLS 1.2”

Retain default values for rest of the fields and select Submit.
Once added, both Call Servers are displayed.
8.3. Configure IP Range Locations

Navigate to **Configure → IP Range Locations** as shown in the screen below and click on the Create button to configure an IP Range.

From the **Create** screen as shown below, configure the following values.

- **From IP Address:** Starting IP Address range of endpoints.
- **To IP Address:** Ending IP Address range of endpoints.
- **ERL/ELE:** An associated ERL/ELE value for call back to the endpoints in this range.

Click on the **Submit** button to complete the configuration.
Screen below shows an example of the **IP Range Locations** created during compliance testing.

<table>
<thead>
<tr>
<th>From Address</th>
<th>To Address</th>
<th>FRL / DLE</th>
<th>Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.64.10.47</td>
<td>10.64.10.47</td>
<td>70000</td>
<td>False</td>
</tr>
<tr>
<td>10.64.10.200</td>
<td>10.64.10.209</td>
<td>80000</td>
<td>False</td>
</tr>
</tbody>
</table>
8.4. Configure Locations

To configure a Location for an ERL/ELE, navigate to Configure → Locations as shown in the screen below and click on the Create button.

In the Create Location screen shown below, configure the required fields for a particular ERL/ELE. During compliance testing only the Address Description, Building and Floor fields were configured for the ERL/ELE “80000”. 
Screen below shows an example of the **Locations** created during compliance testing.

![Locations](image)

### 8.5. Configure External Tracker

Along with IP Range Locations, External Tracker was also tested during the compliance test. External tracker gathers SNMP data from a network switch. Specific ERL/ELE can be associated with a particular port on the switch.

External Tracker used during the compliance test was a Virtual Machine. Installation instructions of the Virtual Machine is outside of scope for this document and as such, is not provided in this document. Installation instructions can be obtained from 911 Secure LLC.

A Site needs to be added for the External Tracker. Navigate to **External Tracker → Sites → Create** to add a site. The following site was configured during the compliance test.

![Edit Site](image)
Once the site has been added, navigate to **External Tracker → Appliances**. Select **Create** to add a new External Tracker.

Screen capture below displays the External Tracker configured during the compliance test. Configure the External Tracker as follows:

- **Appliance Host / IP Address:** IP Address of External Tracker
- **Use SSL:** Check box
- **Site where...is deployed:** Select the Site added in this section
- **Polling Frequency:** Entry to poll the network switch, in cron format

Select **Submit** once done.
Once the External Tracker has been added, add a network switch that can be used by External Tracker to gather the SNMP data. Navigate to **External Tracker → Network Data Switches** and select **Create**.

Screen capture below shows the network switch configured during the compliance test. Configure the Network Data Switch as follows:

- **Site:** Select Site added in this section
- **IP Address:** IP Address of network switch
- **Default ERL/ELE:** An ERL/ELE for the network switch ports
- **Type:** Supported SNMP version of the network switch

Depending on the SNMP version, fill the remaining fields as per the network switch configuration. SNMPv2c was used during the compliance test. Select **Submit** once done.
Once the Network Data Switch has been added, navigate to View ➔ IP Phones. H.323 and SIP Phones connected to the network switch should display the ports these phones are connected to. Note that this can take a few minutes depending on the Polling frequency.

Phone connected to the ports above can be configured with a specific ERL/ELE. To change the ERL/ELE for the connected phones, navigate to External Tracker ➔ Network Data Switches and select the port map icon.
Update the **ERL/ELE** for the phones connected to the port and select **Save Changes** (not shown) once done.

![Switch Ports]

**Port Information for Network Data Switch: DevConnect (10.64.10.5)**

<table>
<thead>
<tr>
<th>Port</th>
<th>Port Description</th>
<th>Location Description</th>
<th>ERL / ELE</th>
<th>Ignore</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>MainRouter</td>
<td></td>
<td>70090</td>
<td>√</td>
</tr>
<tr>
<td>1.10</td>
<td>1/10</td>
<td></td>
<td>70090</td>
<td></td>
</tr>
<tr>
<td>1.11</td>
<td>1/11</td>
<td></td>
<td>70090</td>
<td></td>
</tr>
<tr>
<td>1.12</td>
<td>1/12</td>
<td></td>
<td>70090</td>
<td></td>
</tr>
<tr>
<td>1.13</td>
<td>1/13</td>
<td></td>
<td>70090</td>
<td></td>
</tr>
<tr>
<td>1.14</td>
<td>1/14</td>
<td>Phone 1</td>
<td>80090</td>
<td></td>
</tr>
<tr>
<td>1.15</td>
<td>1/15</td>
<td></td>
<td>70090</td>
<td></td>
</tr>
</tbody>
</table>
9. Verification Steps

The following steps may be used to verify the configuration:

On Avaya Aura® System Manager, navigate to **Elements ➔ Session Manager ➔ System Status ➔ SIP Entity Monitoring**. Value in the **Conn. Status** column, should be **UP**. This verifies that the SIP connectivity between Avaya Aura® Session Manager and Sentinel Server is established successfully.

![SIP Entity, Entity Link Connection Status](image)
From the Sentry Sentinel application’s web interface, verify if all the registered IP endpoints have been discovered by navigating to View → IP Phones as shown in the screen below. Example below shows the IP endpoints registered to Communication Manager and Session Manager during compliance testing.
From the Communication Manager SAT console, display a particular endpoint and note if the ELE, Building and Floor fields are updated as shown in the screen below.

<table>
<thead>
<tr>
<th>FEATURE OPTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>LWC Reception: spe</td>
</tr>
<tr>
<td>LWC Activation? y</td>
</tr>
<tr>
<td>LWC Log External Calls? n</td>
</tr>
<tr>
<td>CDR Privacy? n</td>
</tr>
<tr>
<td>Redirect Notification? y</td>
</tr>
<tr>
<td>Per Button Ring Control? n</td>
</tr>
<tr>
<td>Bridged Call Alerting? n</td>
</tr>
<tr>
<td>Active Station Ringing: single</td>
</tr>
<tr>
<td>H.320 Conversion? n</td>
</tr>
<tr>
<td>Service Link Mode: as-needed</td>
</tr>
<tr>
<td>Multimedia Mode: enhanced</td>
</tr>
<tr>
<td>MWI Served User Type:</td>
</tr>
<tr>
<td>AUDIX Name:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? y</td>
</tr>
<tr>
<td><strong>Emergency Location Ext: 70000</strong></td>
</tr>
<tr>
<td>Precedence Call Waiting? n</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SITE DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Room: 101</td>
</tr>
<tr>
<td>Jack:</td>
</tr>
<tr>
<td>Cable:</td>
</tr>
<tr>
<td>Floor: 2</td>
</tr>
<tr>
<td>Building: 100</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ABBREVIATED DIALING</th>
</tr>
</thead>
<tbody>
<tr>
<td>List1:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BUTTON ASSIGNMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: call-appr</td>
</tr>
<tr>
<td>2: call-appr</td>
</tr>
<tr>
<td>3: call-appr</td>
</tr>
<tr>
<td>4:</td>
</tr>
<tr>
<td>5:</td>
</tr>
<tr>
<td>6:</td>
</tr>
<tr>
<td>7:</td>
</tr>
<tr>
<td>8:</td>
</tr>
<tr>
<td>voice-mail</td>
</tr>
</tbody>
</table>
Verify that 911 calls can be placed from different endpoints and verify these alerts are seen in the Sentry Beacon application.
10. Conclusion
The 911 Secure LLC NG911 Emergency Location Management Solution passed compliance testing. These Application Notes describe the procedures required for the 911 Secure LLC NG911 Emergency Location Management Solution to interoperate with Avaya Aura® Application Enablement Services, Avaya Aura® Session Manager and Avaya Aura® Communication Manager. All feature and serviceability tests were completed successfully with observation(s), if any, noted in Section Error! Reference source not found.

11. Additional References
These documents form part of the Avaya official technical reference documentation suite. Further information may be had from http://support.avaya.com or from the local Avaya representative.

2. Administering Avaya Aura® Application Enablement Services, Release 8.1.x, Issue 3, October 2019
3. Administering Avaya Aura® Session Manager, Release 8.1.1, Issue 2, October 2019

Product documentation for the 911 Secure LLC NG911 Emergency Location Management Solution may be obtained by contacting 911 Secure LLC.

1. Avaya Aura® 8 and Sentry™ v1.10 Configuration Guidelines – Revision 12/31/19
3. Sentry Dispatcher and Sentry Gatekeeper Accounts Setup – Revision 02/26/20
4. Sentry Gatekeeper v1.2 Installation And Users Guide – Revision 5/24/19