



## **Avaya Solution & Interoperability Test Lab**

---

# **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

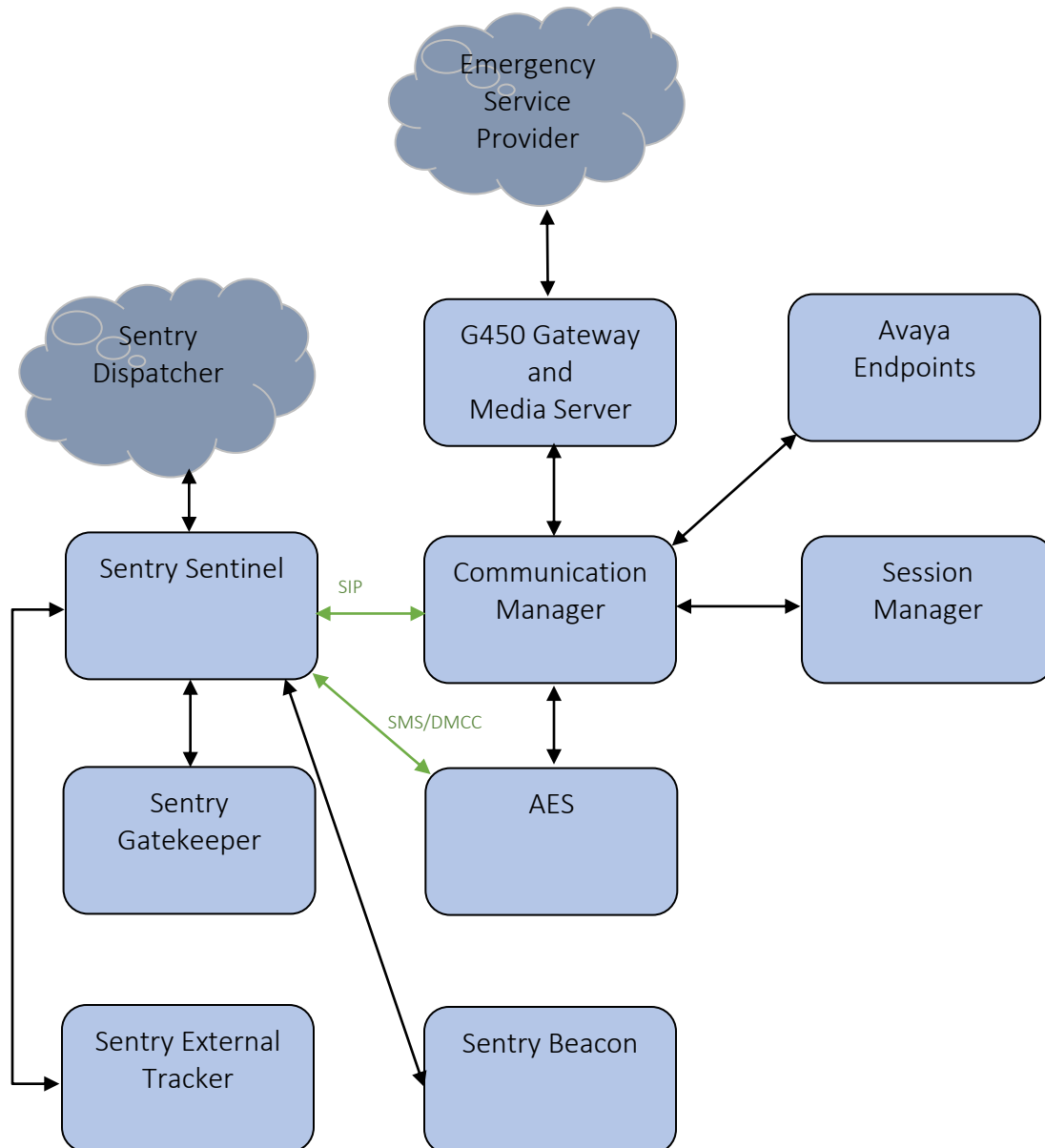
For technical support on the 911 Secure LLC NG911 Emergency Location Management Solution, contact 911 Secure LLC at:

- Web: <http://www.911secure.com/>
- Phone: (213) 425-2050

- Email: [support@911secure.com](mailto: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.



**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:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on virtualized environment	8.1.1
Avaya Aura® Session Manager running on virtualized environment	8.1.1
Avaya Aura® Application Enablement Services running on virtualized environment	8.1.1
Avaya Aura® System Manager running on virtualized environment	8.1.1
Avaya Aura® Media Server running on virtualized environment	8.0.2
Avaya G450 Media Gateway	FW 41.9.1
Avaya Endpoints: <ul style="list-style-type: none"><li>• 9641 (SIP)</li><li>• 9611 (H323)</li><li>• J159 (H323)</li><li>• J169 (SIP)</li></ul>	7.1.7 6.8.3 6.8.3 4.0.3
Avaya one-X® Communicator	2.6.10
Avaya 9404 Digital station	FW 18
Avaya Analog station	N/A
911 Secure LLC Sentinel Sentry server (Windows Server 2016 Standard)	1.11.316.1
Sentry External Tracker	v20200305.1
Sentry Dispatcher	-
Sentry Gatekeeper	1.2.42

## 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.

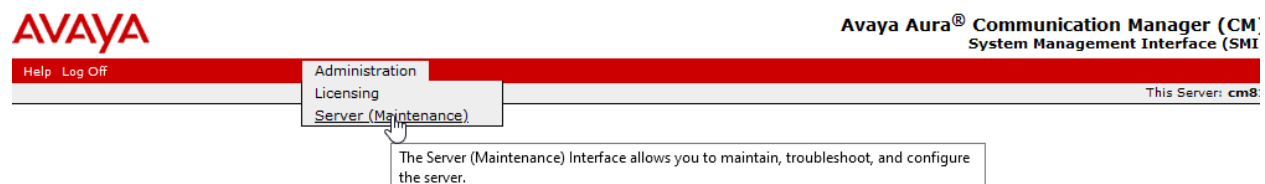
The configuration of Communication Manager was performed using the System Access Terminal (SAT) and web interface. After the completion of the configuration in SAT, perform a **save translation** command to make the changes permanent. The procedures include the following areas:

- 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)**.



© 2001-2019 Avaya Inc. All Rights Reserved.

#### Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

#### Third-party Components

Navigate to **Security** → **Administrator** Accounts as shown below. Select the **Privileged Administrator** radio button and click on **Submit**.

The screenshot displays the Avaya Aura® Communication Manager (CM) System Management Interface (SMI). The top navigation bar includes 'Help', 'Log Off', and 'Administration'. The left sidebar lists various system management categories, with 'Security' expanded to show 'Administrator Accounts'. The main content area, titled 'Administrator Accounts', provides instructions and a 'Select Action:' section. In this section, the 'Add Login' and 'Privileged Administrator' radio buttons are selected and enclosed in a red rectangular box. Other options include 'Unprivileged Administrator', 'SAT Access Only', 'Web Access Only', 'CDR Access Only', 'Business Partner Login (dadmin)', 'Business Partner Craft Login', and 'Custom Login'. Below these are fields for 'Change Login', 'Remove Login', 'Lock/Unlock Login', 'Add Group', and 'Remove Group', each with a dropdown menu. At the bottom of the form are 'Submit' and 'Help' buttons.



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**.

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

Help Log Off Administration This Server: cm81

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 privilege: in the system next to root.

Login name	sentry
Primary group	susers
Additional groups (profile)	prof18
Linux shell	/bin/bash
Home directory	/var/home/sentry
Lock this account	<input type="checkbox"/>
SAT Limit	none
Date after which account is disabled-blank to ignore (YYYY-MM-DD)	
Enter password	*****
Re-enter password	*****
Force password change on next login	<input checked="" type="radio"/> No <input type="radio"/> Yes

**Submit** **Cancel** **Help**

## 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                                     Page 1 of 5
                                                    STATION
Extension: 77771                                     Lock Messages? n          BCC: 0
  Type: 9641                                           Security Code: *          TN: 1
  Port: IP                                           Coverage Path 1:          COR: 1
  Name: Sentry CRSS Alert                           Coverage Path 2:          COS: 1
Unicode Name? n                                     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: 77771
    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
                                                    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.

add station 77771		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:	
2:call-appr	6:	
3:call-appr	7:	
4:crss-alert	8:	

### 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.

change system-parameters crisis-alert		Page 1 of 1
CRISIS ALERT SYSTEM PARAMETERS		
ALERT STATION		
<b>Every User Responds? y</b>		
ALERT PAGER		
Alert Pager? n		

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.

change ars analysis 211							Page 1 of 2	
ARS DIGIT ANALYSIS TABLE								
Location: all							Percent Full: 0	
	Dialed	Total		Route	Call	Node	ANI	
	String	Min	Max	Pattern	Type	Num	Reqd	
211		3	3	1	alrt		n	

## 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 screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text 'Application Enablement Services' and 'Management Console' is displayed. A red horizontal bar spans the width of the page, with a 'Help' link on the right. Below this bar is a login form with the text 'Please login here:' followed by a 'Username' label and a text input field. A 'Continue' button is located below the input field. At the bottom of the page, another red horizontal bar contains the copyright notice: 'Copyright © 2009-2019 Avaya Inc. All Rights Reserved.'

The **Welcome to OAM** screen is displayed, as shown below.



## Application Enablement Services Management Console

Welcome: User cust  
Last login: Fri Mar 27 14:33:21 2020 from 10.64.10.47  
Number of prior failed login attempts: 3  
HostName/IP: aes81/10.64.110.215  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.1.1.0.0.8-0  
Server Date and Time: Fri Mar 27 14:33:27 MDT 2020  
HA Status: Not Configured

Home

Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

### 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 dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- 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, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- 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).

**Networking | Ports**Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

AE Service IP (Local IP)

Network Configure

Ports

TCP/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

**Ports**

CVLAN Ports

Unencrypted TCP Port9999Enabled Disabled

Encrypted TCP Port9998Enabled Disabled

DLG Port

TCP Port5678

TSAPI Ports

TSAPI Service Port450Enabled Disabled

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721Enabled Disabled

Encrypted Port4722Enabled Disabled

TR/87 Port4723Enabled Disabled

## 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).

User Management | User Admin | Add User

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with \* can not be empty.

\* User Id

sentry

\* Common Name

sentry

\* Surname

sentry

\* User Password

•••••

\* Confirm Password

•••••

Admin Note

Avaya Role

None

Business Category

Car License

CM Home

Css Home

CT User

Yes

Department Number

Display Name

Employee Number

Employee Type



## 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.

Security | Security Database | CTI Users | List All Users

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▶ Certificate Management

Enterprise Directory

▶ Host AA

▶ PAM

▼ Security Database

▪ Control

▣ CTI Users

▪ List All Users

▪ Search Users

▪ Devices

▪ Device Groups

▪ Trunks

CTI Users

User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> calabrio	calabrio	NONE	NONE
<input type="radio"/> cscuser	cscuser	NONE	NONE
<input type="radio"/> interop	interop	NONE	NONE
<input type="radio"/> intradiem	intradiem	NONE	NONE
<input type="radio"/> intranext	intranext	NONE	NONE
<input type="radio"/> miarec	miarec	NONE	NONE
<input type="radio"/> rtirdrouter1	rtirdrouter1	NONE	NONE
<input type="radio"/> rtirouter1	rtirouter1	NONE	NONE
<input type="radio"/> rtitele1	rtitele1	NONE	NONE
<input checked="" type="radio"/> sentry	sentry	NONE	NONE
<input type="radio"/> trio	trio	NONE	NONE

EditList All

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.

[Security](#) | [Security Database](#) | [CTI Users](#) | [List All Users](#)[Home](#) | [Help](#) | [Logout](#)

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▶ Certificate Management

Enterprise Directory

▶ Host AA

▶ PAM

▼ Security Database

▪ Control

Edit CTI User

User Profile:

User ID

Common Name

Worktop Name

Unrestricted Access

sentry

sentry

NONE ▼

☒

Call and Device Control:

Call Origination/Termination and Device Status

None ▼

Call and Device Monitoring:

Device Monitoring

Calls On A Device Monitoring

Call Monitoring

None ▼

None ▼

☐

Routing Control:

Allow Routing on Listed Devices

None ▼

Apply Changes

Cancel Changes

## 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

Home | Help | Logout

▶ AE Services

▼ Communication Manager Interface

Switch Connections

▶ Dial Plan

High Availability

▶ Licensing

▶ Maintenance

Edit Processor Ethernet IP - cm81

10.64.110.213

Add/Edit Name or IP

Name or IP Address	Status
10.64.110.213	In Use

Back

## 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.



Recommended access to System Manager is via FQDN.  
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or

User ID:

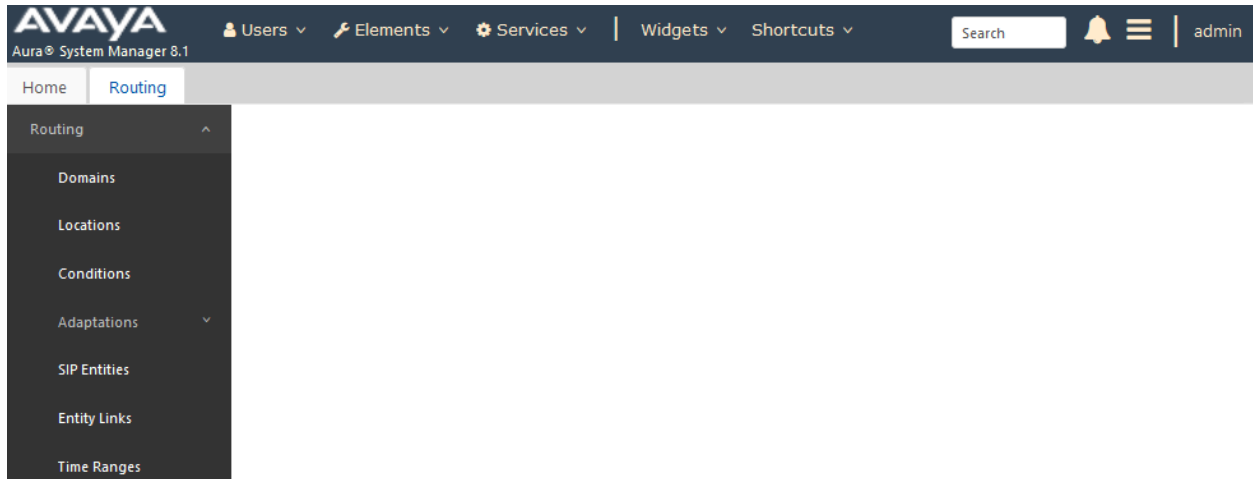
Password:

[Change Password](#)

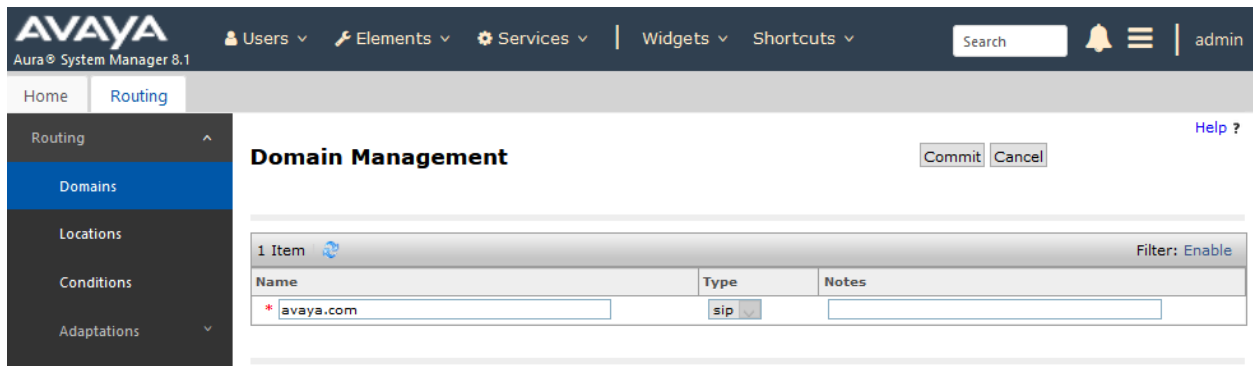
**Supported Browsers:** Internet Explorer 11.x or Firefox 65.0, 66.0 and 67.0.

## 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**.



### 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.

AVAYA  
Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰ | adm

Home Routing

Routing Domains Locations Conditions

**Location Details** Commit Cancel [Help ?](#)

General

\* Name:

Notes:

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.

Location Pattern

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.64.*	

Select : All, None

Commit Cancel

## 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.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 8.1', and various menu items like Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile icon are also present. The left sidebar contains a list of navigation options: Home, Routing, Domains, Locations, Conditions, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, and Routing Policies. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The form contains the following fields:

- Name:** sentry
- FQDN or IP Address:** 10.64.110.84
- Type:** ELIN server
- Notes:**
- Adaptation:**
- Location:** DevConnect
- Time Zone:** America/Denver
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting

Buttons for 'Commit' and 'Cancel' are located at the top right of the form area.

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.

#### Entity Links

Override Port & Transport with DNS SRV: ☐

Add Remove		1 Item <span>Filter: Enable</span>				
<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port
<input type="checkbox"/>	* sm81_sentry_5061_TLS	sm81	TLS	* 5061	sentry	* 5061

Select : All, None

## 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.

Routing	<b>SIP Entities</b>
Domains	New Edit Delete Duplicate More Actions
Locations	17 Items <span>Filter: Enable</span>
Conditions	
Adaptations	
<b>SIP Entities</b>	
Entity Links	
Time Ranges	
Routing Policies	
Dial Patterns	
Regular Expressions	
Defaults	

<input type="checkbox"/>	Name	FQDN or IP Address	Type	Notes
<input type="checkbox"/>	audiocodes	10.64.110.82	SIP Trunk	
<input type="checkbox"/>	brz81	10.64.110.219	Avaya Breeze	
<input type="checkbox"/>	brzws1	10.64.110.182	Avaya Breeze	
<input type="checkbox"/>	brzws2	10.64.110.184	Avaya Breeze	
<input type="checkbox"/>	brzws3	10.64.110.186	Avaya Breeze	
<input type="checkbox"/>	cm81	10.64.110.213	CM	
<input type="checkbox"/>	cmm81	10.64.110.216	Messaging	
<input type="checkbox"/>	intranext	10.64.110.87	SIP Trunk	
<input type="checkbox"/>	ipo11	10.64.110.65	SIP Trunk	
<input type="checkbox"/>	mpp722	10.64.110.51	Voice Portal	
<input type="checkbox"/>	mx62	10.64.10.20	Conferencing	
<input type="checkbox"/>	ps81-brz	ps81.avaya.com	Presence Services	
<input type="checkbox"/>	sbce81	10.64.110.222	SIP Trunk	
<input type="checkbox"/>	sentry	10.64.110.84	ELIN server	
<input type="checkbox"/>	sm81	10.64.110.212	Session Manager	

Select : All, None Page 1 of 2



## 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.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile 'admin' are also present. The left sidebar shows the navigation menu with 'Session Manager' selected. The main content area is titled 'Global Settings' and contains a list of configuration options. The 'ELIN SIP Entity' dropdown is highlighted with a red box and set to 'sentry'. Other settings include 'Failback Policy' (Auto), 'Allow Unauthenticated Emergency Calls' (unchecked), 'Ignore SDP for Call Admission Control' (unchecked), 'Disable Call Admission Control Threshold Alarms' (unchecked), 'Disable Loop Detection Alarms' (unchecked), '\*Loop Detection Alarms Threshold (hours)' (24), 'Enable Dial Plan Ranges' (unchecked), 'Enable Regular Expression Adaptations' (unchecked), 'Enable Flexible Routing' (unchecked), 'Better Matching Dial Pattern or Range in Location ALL Overrides Match in Originator's Location' (checked), 'Enable Load Balancer' (unchecked), 'Enable IPv6' (unchecked), 'Allow Unsecured PPM Traffic' (checked), 'Minimum SIP Entity TLS Version' (1.2), 'Minimum Endpoint TLS Version' (1.2), 'TLS Endpoint Certificate Validation' (None), 'Enable End to End Secure Call Indication' (unchecked), 'Enable Military Support' (unchecked), 'Enable Application Sequence for Emergency Calls' (unchecked), 'Emergency Call Resource-Priority Headers' (empty), 'Enable Implicit Users Applications for SIP users' (unchecked), and 'Enable SIP Resiliency' (unchecked). Buttons for 'Commit', 'Cancel', and 'View Defaults' are at the top right of the settings area.

Global Settings	
Administer settings that apply to all Session Managers	
Failback Policy	Auto
Allow Unauthenticated Emergency Calls	<input type="checkbox"/>
ELIN SIP Entity	sentry
Ignore SDP for Call Admission Control	<input type="checkbox"/>
Disable Call Admission Control Threshold Alarms	<input type="checkbox"/>
Disable Loop Detection Alarms	<input type="checkbox"/>
*Loop Detection Alarms Threshold (hours)	24
Enable Dial Plan Ranges	<input type="checkbox"/>
Enable Regular Expression Adaptations	<input type="checkbox"/>
Enable Flexible Routing	<input type="checkbox"/>
Better Matching Dial Pattern or Range in Location ALL Overrides Match in Originator's Location	<input checked="" type="checkbox"/>
Enable Load Balancer	<input type="checkbox"/>
Enable IPv6	<input type="checkbox"/>
Allow Unsecured PPM Traffic	<input checked="" type="checkbox"/>
Minimum SIP Entity TLS Version	1.2
Minimum Endpoint TLS Version	1.2
TLS Endpoint Certificate Validation	None
Enable End to End Secure Call Indication	<input type="checkbox"/>
Enable Military Support	<input type="checkbox"/>
Enable Application Sequence for Emergency Calls	<input type="checkbox"/>
Emergency Call Resource-Priority Headers	
Enable Implicit Users Applications for SIP users	<input type="checkbox"/>
Enable SIP Resiliency	<input type="checkbox"/>

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.

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.

KJA; Reviewed:  
SPOC 4/10/2020



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 screenshot shows the 'Add Trusted Certificate' window in the Sentry Sentinel interface. The window has a title bar with 'Manage Elements' and 'Discovery' tabs. The main title is 'Add Trusted Certificate'. There are 'Commit' and 'Cancel' buttons in the top right corner. Below the title, there is a section for 'Select Store Type to add trusted certificate' with a dropdown menu set to 'All'. Underneath, there are four radio button options: 'Import from file' (which is selected and highlighted with a red box), 'Import as PEM certificate', 'Import from existing certificates', and 'Import using TLS'. Below these options, there is a table with two columns: 'Filename' and 'Action'. The table contains one row with 'SentryRootCA.cer' in the 'Filename' column and 'Remove' in the 'Action' column. To the left of the table, there is a red asterisk and the text '\* Please select a file'. Below the table, there is a 'Browse...' button and the text 'No file selected.'. At the bottom of the window, there is a message: 'You must click the Retrieve certificate button and review the certificate details before you can continue'. To the right of this message is a 'Retrieve Certificate' button, which is highlighted with a red box. At the very bottom of the window, there are 'Commit' and 'Cancel' buttons.

Filename	Action
SentryRootCA.cer	Remove

The **Trusted Certificates** screen is shown below after the certificates have been installed.

## Manage Trusted Certificates

Done

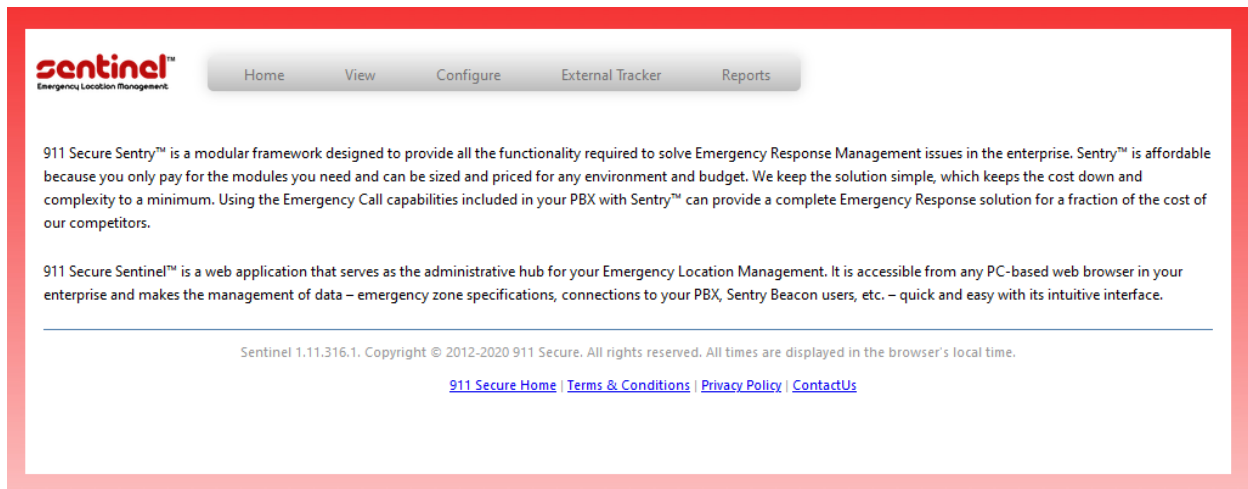
Manage Trusted Certificates		
View Add Export Remove		
23 Items		Filter: Enable
<input type="checkbox"/>	Store Description	Subject Name
<input type="checkbox"/>	Used for validating TLS client identity certificates	CN=SentryRootCA, O=Default Company Ltd, L=Default City, C=XX
<input type="checkbox"/>	Used for validating TLS client identity certificates	CN=epms.avaya.com, OU=SIP CA, O=Avaya
<input type="checkbox"/>	Used for validating TLS client identity certificates	CN=Avaya Product Root CA, OU=Avaya Product PKI, O=Avaya Inc., C=US
<input type="checkbox"/>	Used for validating TLS client identity certificates	O=AVAYA, OU=MGMT, CN=System Manager CA
<input type="checkbox"/>	Used for validating TLS client identity certificates	CN=Avaya Call Server, OU=Media Server, O=Avaya Inc., C=US
<input type="checkbox"/>	Used for validating TLS client identity certificates	O=AVAYA, OU=MGMT, CN=System Manager CA
<input type="checkbox"/>	Used for validating TLS client identity certificates	CN=SentryRootCA, O=Default Company Ltd, L=Default City, C=XX
<input type="checkbox"/>	Used for validating TLS client identity certificates	CN=epms.avaya.com, OU=SIP CA, O=Avaya
Select : All, None		
Page 2 of 2		

## 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.

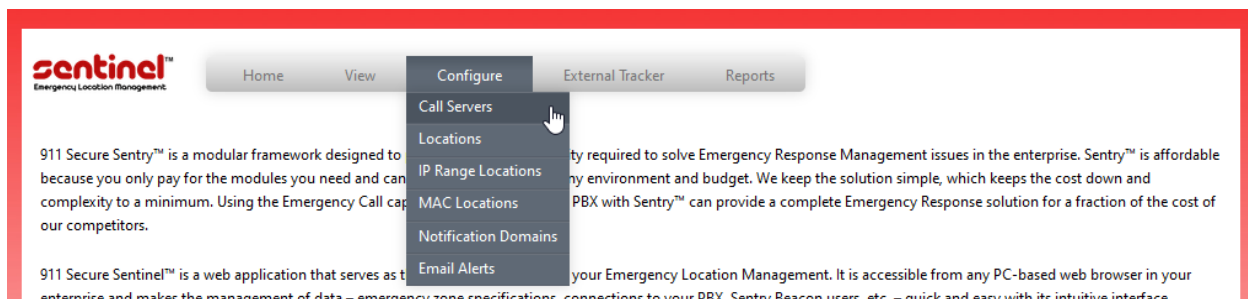
### 8.1. Sentinel Web Interface

Access the Sentinel web interface by logging into the Sentry server, opening a web browser and entering the following URL: ***http://localhost/Sentinel***. 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.



### 8.2. Configure Call Servers

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



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](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.

Deactivate Call Server ☐

\* AES Version

Call Server Description

\* CM Username @ CM IP Address / FQDN

\* CM Password

\* Confirm CM Password

Provision All Endpoints ☒

ELIN Prefix

\* CM Switch Connection Name

\* CLAN / PROCR IP Address / FQDN

Enable Crisis Alerting ☒

Crisis Alert Extension

Crisis Alert Extension Security Code

\* AES IP Address / FQDN

\* AES Username

\* AES Password

\* Confirm AES Password

\* AES DMCC Port

DMCC Secure Mode ☒

\* SMS Service URL

SIP Domain

SM Entity Link Port

\* SM Entity Link TLS

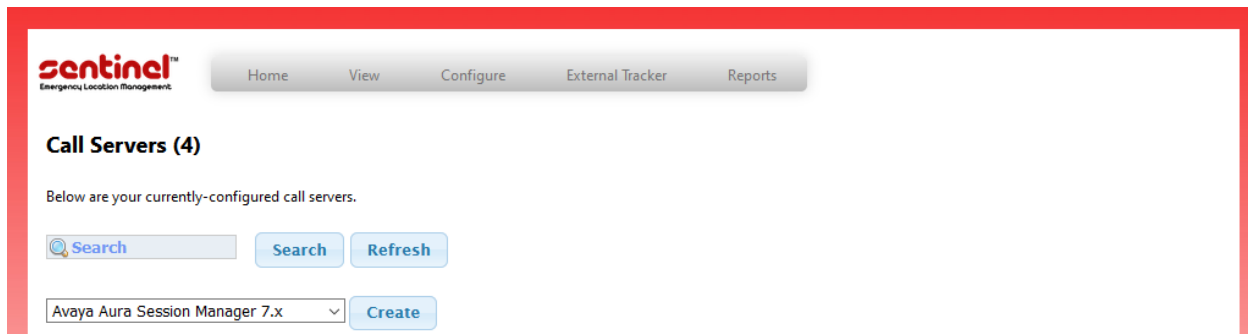
Disable IP Phone downloads from CM ☐

Disable Location updates back to CM ☐

\* Enable Callers downloads



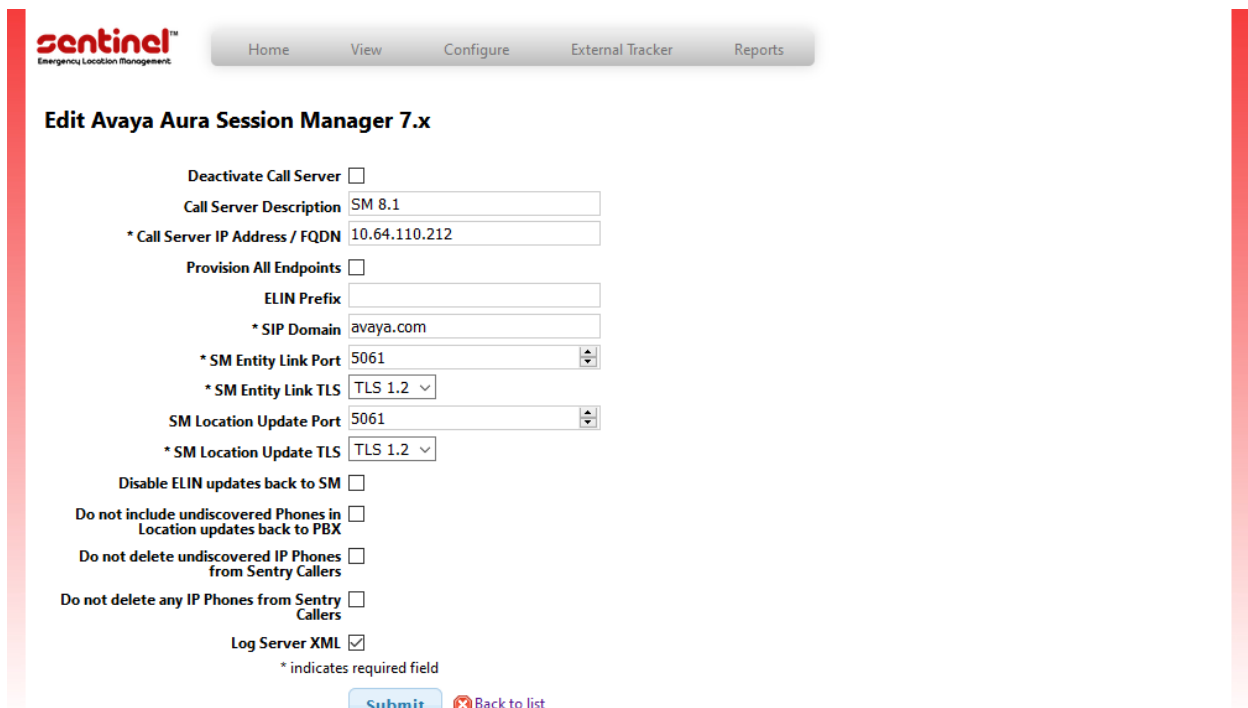
On the **Call Server** page, select **Avaya Aura Session Manager 7.x** and **Create** another Call Server. This Call Server is for integration with Session Manager for SIP endpoints.



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**.



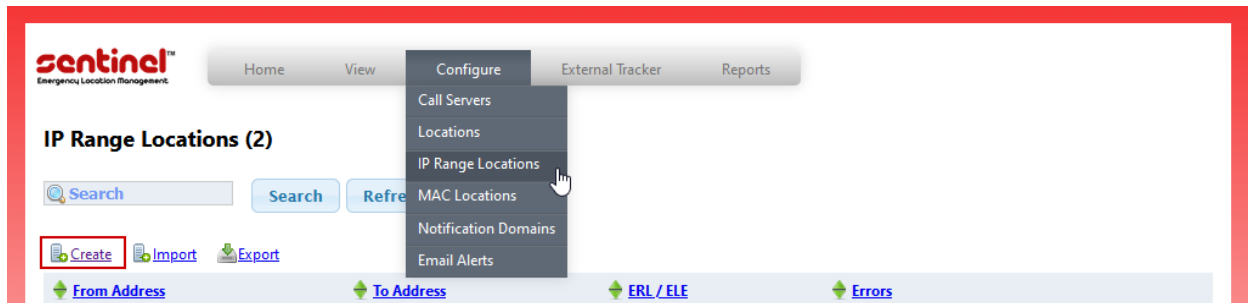
Once added, both Call Servers are displayed.

The screenshot displays the Sentinel Emergency Location Management web application. At the top, there is a navigation bar with the Sentinel logo and tabs for Home, View, Configure, External Tracker, and Reports. The main heading is "Call Servers (4)". Below this, a message states "Below are your currently-configured call servers." There are three buttons: "Search" (with a magnifying glass icon), "Refresh", and a "Create" button next to a dropdown menu labeled "- Select a call server type -".

IP Address	Server Description	Type	
10.64.110.213	CM & AES 8.1	Avaya Aura CM 7+ AES 8.0.1	
10.64.110.212	SM 8.1	Avaya Aura Session Manager 7.x	
10.64.110.65	IPO 11.0.4.2 - Server Edition	Avaya IP Office 10.0+	
10.64.10.54	IPO 11.0.4.2 - Expansion System	Avaya IP Office 10.0+	

### 8.3. Configure IP Range Locations

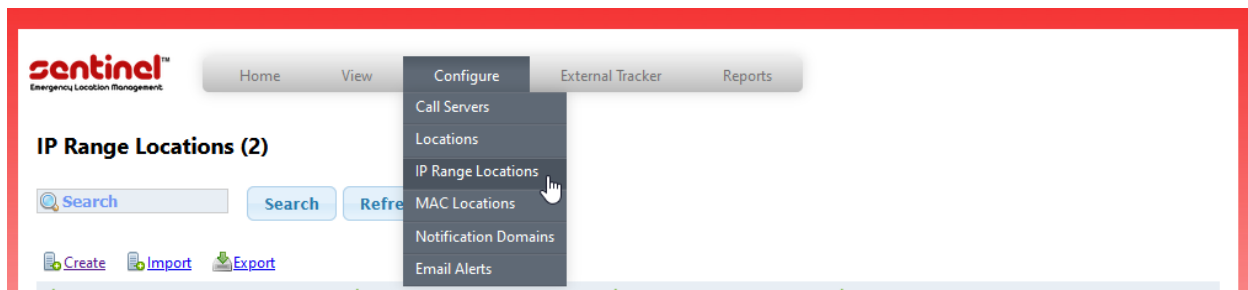
Navigate to **Configure → IP Range Locations** as shown in the screen below and click on the Create button to configure an IP Range.



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.



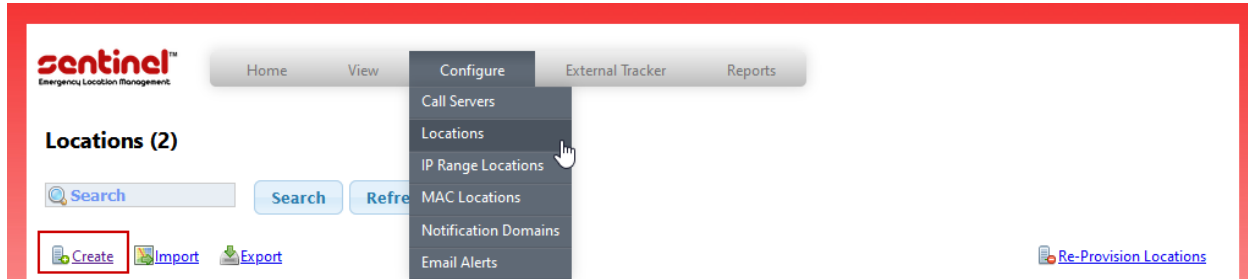
Screen below shows an example of the **IP Range Locations** created during compliance testing.

The screenshot displays the Sentinel Emergency Location Management web application. At the top, there is a navigation bar with the Sentinel logo and tabs for Home, View, Configure, External Tracker, and Reports. The main heading is "IP Range Locations (2)". Below this, there is a search bar with a "Search" button and a "Refresh" button. To the left of the table are links for "Create", "Import", and "Export". The table has four columns: "From Address", "To Address", "ERL / ELE", and "Errors". It contains two rows of data. At the bottom, there is a footer with the version "Sentinel 1.11.316.1", copyright information, and links to "911 Secure Home", "Terms & Conditions", "Privacy Policy", and "ContactUs".

From Address	To Address	ERL / ELE	Errors
10.64.10.47	10.64.10.47	70000	False
10.64.10.200	10.64.10.200	80000	False

## 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”.

Standard Fields

ERL / ELE

80000

ELIN

Short Description

Lab Location 2

Address Description

12121 GRANT ST

Building

100

(for Avaya CM, must be predefined in CM's site-data)

Floor

2

(for Avaya CM, must be predefined in CM's site-data)

Room / Zone

101

(for Avaya CM, must be 10 characters or less)

External Data Portal URL

Floor Plan URL

Fixed Video Feed URL

Video Format

MP4

Location Details

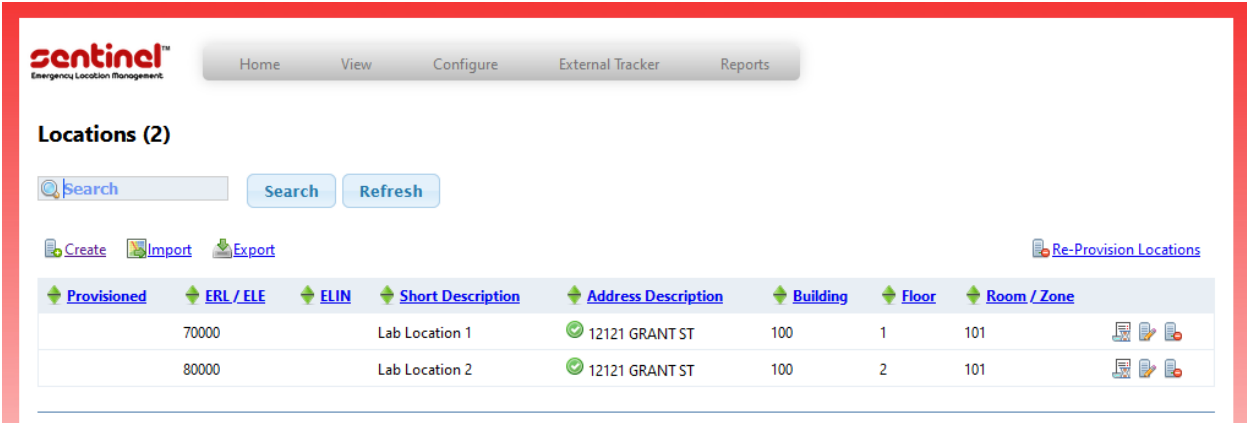
Contact Information (optional)

NENA Specific Fields (optional)

Submit

Back to list

Screen below shows an example of the **Locations** created during compliance testing.



The screenshot shows the Sentinel Emergency Location Management interface. At the top, there is a navigation bar with links: Home, View, Configure, External Tracker, and Reports. Below the navigation bar, the title "Locations (2)" is displayed. There is a search bar with a magnifying glass icon and a "Search" button, and a "Refresh" button. Below the search bar, there are links for "Create", "Import", "Export", and "Re-Provision Locations". The main content is a table with the following columns: Provisioned, ERL / ELE, ELIN, Short Description, Address Description, Building, Floor, and Room / Zone. The table contains two rows of data.

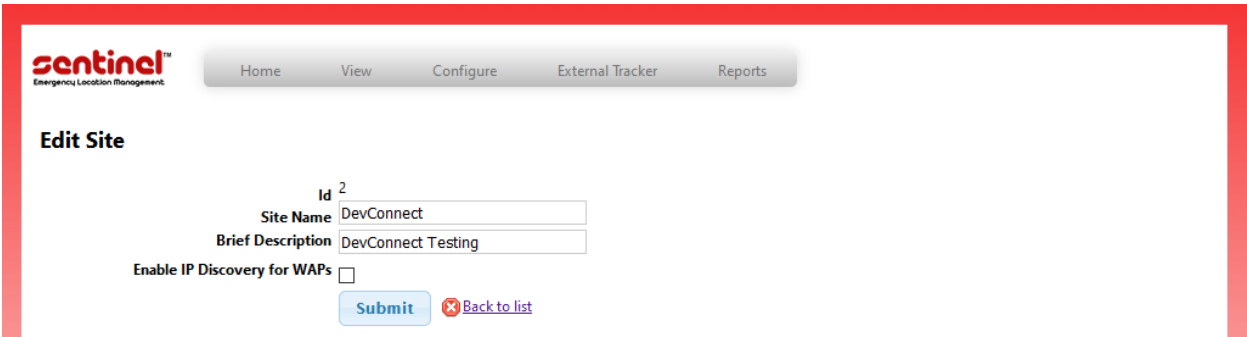
Provisioned	ERL / ELE	ELIN	Short Description	Address Description	Building	Floor	Room / Zone
	70000		Lab Location 1	12121 GRANT ST	100	1	101
	80000		Lab Location 2	12121 GRANT ST	100	2	101

## 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.



The screenshot shows the Sentinel Emergency Location Management interface with the "Edit Site" form. The form has the following fields: "Id" (with a superscript 2), "Site Name" (with the value "DevConnect"), "Brief Description" (with the value "DevConnect Testing"), and "Enable IP Discovery for WAPs" (with a checkbox). There is a "Submit" button and a "Back to list" link.

Id<sup>2</sup>

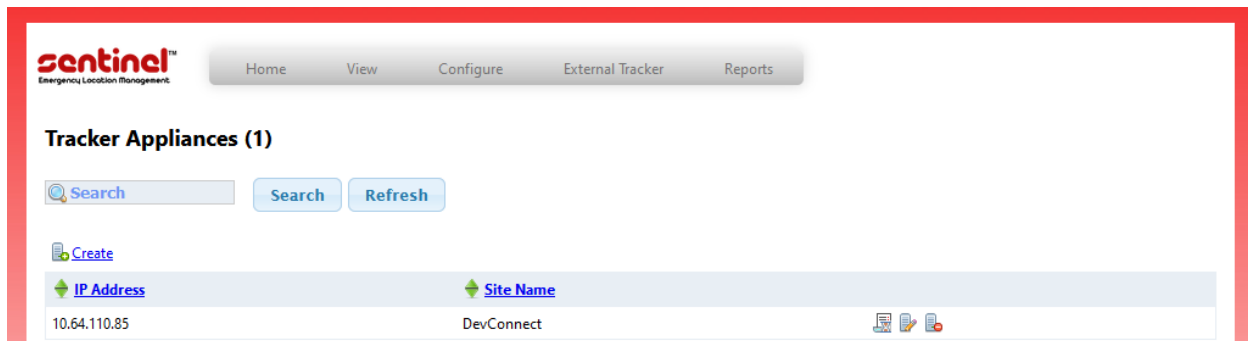
Site Name DevConnect

Brief Description DevConnect Testing

Enable IP Discovery for WAPs ☐

Submit Back to list

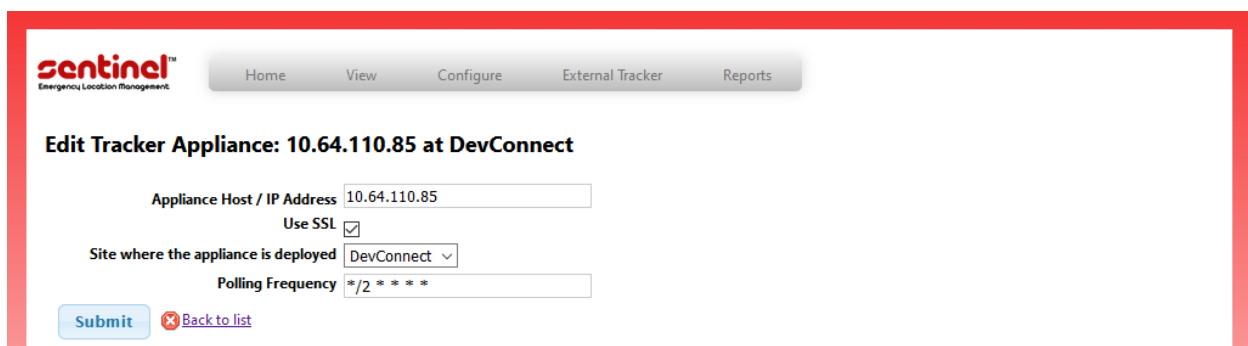
Once the site has been added, navigate to **External Tracker** → **Appliances**. Select **Create** to add a new External Tracker.



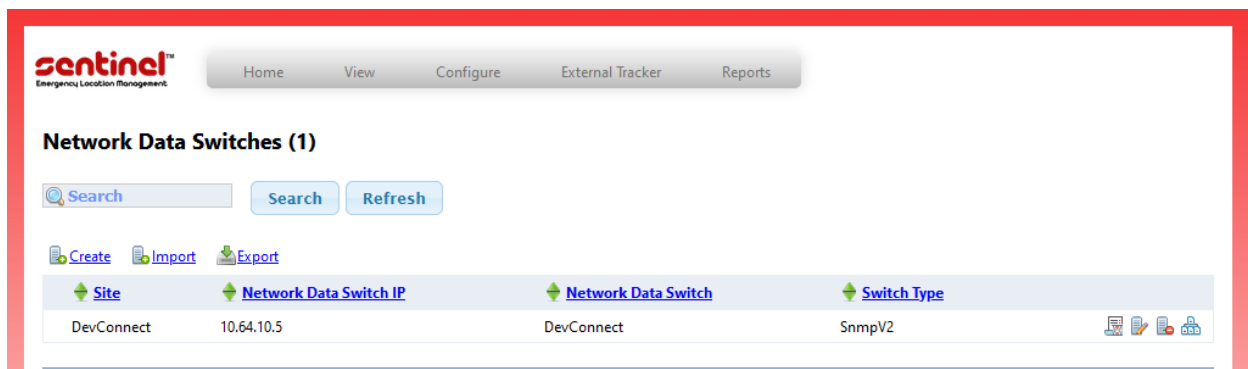
Screen capture below displays the External Tracker configured during the compliance test. Configure the External Tracker as follows:

- **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.

The screenshot shows the 'Edit Network Data Switch' form. The fields are as follows:

- Site: DevConnect (dropdown)
- Deactivate Network Switch: ☐
- \* IP Address: 10.64.10.5
- Use Port Description as ERL / ELE: ☐
- \* Default ERL / ELE: 70000
- Use Port Description for Location: ☐
- Default Location: (empty)
- Network Data Switch Name: DevConnect
- Type: SNMP v2c (dropdown)
- R/O Community String: (masked with dots)
- Confirm R/O Community String: (masked with dots)

\* indicates required field

Buttons: Submit, Back to list




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.

/Set	IP Address	MAC Address	ERL / ELE	Provisioned	Current Location	Network Data Switch	Switch Port	Default Location	Type	Stat
	10.64.110.215	cbe283ad-a61a-4254-b408-04a65ac8ca8c						9641		3/27/20
	10.64.10.202	b4b017893c80	70000	✓	Lab Location 1	DevConnect	10.64.10.5 1.14	9608		3/27/20
	10.64.10.200	a009ede7f7a3	70000	✓	Lab Location 1	DevConnect	10.64.10.5 1.5	9641		3/27/20

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.

Site	Network Data Switch IP	Network Data Switch	Switch Type
DevConnect	10.64.10.5	DevConnect	SnmpV2

Update the **ERL/ELE** for the phones connected to the port and select **Save Changes** (not shown) once done.




[Home](#)
[View](#)
[Configure](#)
[External Tracker](#)
[Reports](#)

### Switch Ports

Refresh

Port Information for Network Data Switch: DevConnect (10.64.10.5)


[Export](#)

Port	Port Description	Location Description			ERL / ELE			Ignore
		<input type="checkbox"/>	<input type="text"/>		<input type="checkbox"/>	<input type="text"/>		
		<input type="checkbox"/>			<input type="checkbox"/>			
1.1	MainRouter	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	70000		<input checked="" type="checkbox"/>
1.10	1/10	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	70000		<input type="checkbox"/>
1.11	1/11	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	70000		<input type="checkbox"/>
1.12	1/12	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	70000		<input type="checkbox"/>
1.13	1/13	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	70000		<input type="checkbox"/>
1.14	1/14	<input checked="" type="checkbox"/>	Phone 1		<input checked="" type="checkbox"/>	80000		<input type="checkbox"/>
1.15	1/15	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	70000		<input type="checkbox"/>


## 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

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

Status Details for the selected Session Manager:									
All Entity Links to SIP Entity: sentry									
Summary View									
1 Item  Filter: Enable									
	Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	<a href="#">sm81</a>	IPv4	10.64.110.84	5061	TLS	FALSE	UP	200 Ok	UP
Select : None									

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.

**IP Phones (6)**

All From: To: Search Search Refresh

Export Mark All Phones as Stale Re-sync Endpoints

Status	Call Server	Extension / Set	IP Address	MAC Address	ERL / ELE	Provisioned	Current Location	Network Data Switch	Switch Po
⚠	CM & AES 8.1	70003	10.64.10.202	b4b017893c80	80000	✓	Lab Location 2	DevConnect	10.64.10.5 1.14
✓	CM & AES 8.1	70001	10.64.10.200	a009ede7f7a3	70000	✓	Lab Location 1	DevConnect	10.64.10.5 1.5
✓	SM 8.1	70103	10.64.10.205	b4b0178996ce	70000		Lab Location 1	DevConnect	10.64.10.5 1.6
✓	SM 8.1	70101	10.64.10.201	c81fea823aca	70000		Lab Location 1	DevConnect	10.64.10.5 1.8
✓	SM 8.1	70103	10.64.10.47	4bc5c247f2ea	80000		Lab Location 2		
⚠	CM & AES 8.1	77771	10.64.110.215	60e5031e- ee8c-4f88-8919- c6ec2b4df0b8					

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.

```
display station 70003                                     Page 2 of 5
STATION
FEATURE OPTIONS
    LWC Reception: spe                                     Auto Select Any Idle Appearance? n
    LWC Activation? y                                     Coverage Msg Retrieval? y
    LWC Log External Calls? n                             Auto Answer: none
    CDR Privacy? n                                       Data Restriction? n
    Redirect Notification? y                             Idle Appearance Preference? n
    Per Button Ring Control? n                           Bridged Idle Line Preference? n
    Bridged Call Alerting? n                             Restrict Last Appearance? y
    Active Station Ringing: single
                                                         EMU Login Allowed? n
    H.320 Conversion? n                                 Per Station CPN - Send Calling Number?
    Service Link Mode: as-needed                         EC500 State: enabled
    Multimedia Mode: enhanced                           Audible Message Waiting? n
    MWI Served User Type:                               Display Client Redirection? n
    AUDIX Name:                                         Select Last Used Appearance? n
                                                         Coverage After Forwarding? s
                                                         Multimedia Early Answer? n
Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? y
Emergency Location Ext: 70000                         Always Use? n IP Audio Hairpinning? n
    Precedence Call Waiting? n

display station 70003                                     Page 4 of 5
STATION
SITE DATA
    Room: 101                                           Headset? n
    Jack:                                               Speaker? n
    Cable:                                              Mounting: d
    Floor: 2                                           Cord Length: 0
    Building: 100                                       Set Color:

ABBREVIATED DIALING
    List1:                                             List2:
                                                         List3:

BUTTON ASSIGNMENTS
    1:call-appr                                         5:
    2:call-appr                                         6:
    3:call-appr                                         7:
    4:                                                  8:

voice-mail
```

Verify that 911 calls can be placed from different endpoints and verify these alerts are seen in the Sentry Beacon application.

The screenshot displays the Sentry Beacon by 911 Secure application. The interface is divided into two main sections: a list of emergency calls on the left and a detailed view of a selected call on the right.

**Emergency Calls List:**

- Mar 27, 2020 15:44:25 GMT-07:00**  
72001 911  
BLDG 200, FL 3, RM 103  
*Digital Station 1 Emergency Call*
- Mar 27, 2020 15:44:13 GMT-07:00**  
70003 911  
Phone 1, Lab 1, Lab Location 2, 12121 GRANT ST, THORNTON, CO, 80241-3129  
100 2 101  
*H.323 Station 3 Emergency Call*
- Mar 27, 2020 15:43:31 GMT-07:00**  
70101 9211  
Lab Location 1, 12121 GRANT ST, THORNTON, CO, 80241-3129  
100 1 101  
*Emergency Call*
- Mar 27, 2020 15:42:53 GMT-07:00**  
70103 9211  
Lab Location 1, 12121 GRANT ST, THORNTON, CO, 80241-3129  
100 1 101  
*Emergency Call*
- Mar 27, 2020 15:42:42 GMT-07:00**  
70103 9211  
Lab Location 2, 12121 GRANT ST, THORNTON, CO, 80241-3129  
100 2 101  
*Emergency Call*
- Mar 27, 2020 15:38:02 GMT-07:00**

**Emergency Call Details:**

Note

Details Acknowledgements Raw

Type Emergency Call  
Call Server CM & AES 8.1  
Phone 70103  
Dialed 911  
ERL / ELE 70103  
Name Station 3, SIP

515026c2-fe50-428b-9cf4-01c69bb96b22

Connected to <https://sentry.avaya.com/Sentinel>. Client Connected with Filtering Version 1.11.316.1

## 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.

1. *Administering Avaya Aura® Communication Manager, Release 8.1.x, Issue 5, November 2019*
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*
2. *Sentry™ Sentinel v1.10 User's Guide – 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*
5. *Sentry Dispatcher v1.2 Users Guide – Revision 4/23/18*

---

**©2020 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](mailto:devconnect@avaya.com).