Avaya Solution & Interoperability Test Lab

Application Notes for 911 Secure LLC Sentry NG911 Emergency Location Management with Avaya IP Office Server Edition using Location API - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate the 911 Secure LLC Sentry NG911 Emergency Location Management Solution with Avaya IP Office Server Edition. The 911 Secure LLC Sentry NG911 Emergency Location Management Solution provides location setting and on-site notification when an emergency call has been placed using Software Development Kit (SDK) for Avaya Location API. 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 the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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

1. Introduction

These Application Notes describe the configuration steps required to integrate the 911 Secure LLC Sentry NG911 Emergency Location Management Solution (hereafter, also referred to as "Sentry") with Avaya IP Office Server Edition (hereafter, also referred to as "IP Office"). Sentry provides location discovery and on-site notification when an emergency call has been placed. Sentry is a software-based solution that utilized the following components for compliance testing: the Sentry Sentinel web server, Sentry database, SDK that is part of the Avaya Location API and the Beacon On-site notification application.

The IP Office Server Edition configuration consisted of two IP Office systems, a primary Linux server and an expansion IP500V2 that were connected via Small Community Network (SCN) trunks. A Location API WebSocket connection was established between Sentry and IP Office (both primary and expansion).

When an emergency call (e.g. 911) has been 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 provides the ability for organizations to provide such locations to first responders.

2. General Test Approach and Test Results

This section includes the general test approach, what was covered, and results of the testing.

Emergency calls were manually made from various endpoints (H.323, SIP, Digital and Analog) of IP Office to a simulated Emergency Services provider via SIP and ISDN-PRI trunks, and the alerts generated by the IP Office were displayed by Sentry and also on the Beacon On-site notification application along with the location information. This information was then verified with the information present in IP Office.

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

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

For the testing associated with these Application Notes, the interface between Avaya systems and 911 Secure LLC utilized enabled capabilities of secure WebSocket requests.

2.1. Interoperability Compliance Testing

The general test approach was to verify the integration of Sentry with Avaya IP Office Server Edition. Various emergency calls were placed from IP Office telephones (both from primary and expansion) to verify that the alerts generated by IP Office were displayed by Sentry using the Location API. The Location API was also used by Sentry to import the locations defined in IP Office (both in primary and expansion), verifying that Sentry imported the correct ELE, Building, Room and Floor information. Sentry then uses it to update IP Office's dynamic location for the extensions that Sentry has discovered so that they are correctly set for emergency calls.

Additionally, basic serviceability testing examined the handling of and recovery from error conditions (such as network disconnects and power failures).

2.2. Test Results

The 911 Secure LLC Sentry NG911 Emergency Location Management Solution successfully passed compliance testing with the following observations:

- The Avaya IP Office Locations feature must be set up in a certain way to allow information to align with Sentry. To do this, IP Office administrator must name the Locations with a certain pattern that will make sense to both IP Office administrator and the Sentry software. The format required is "Name###ERL" (e.g. ServerEdPri###81111). The first part identifies the true Location Name and the last part (after the ### separator) indicates the Emergency Response Location (ERL) that is mapped to Locations in the Sentry database. The ERL value is just an arbitrary number used to identify the Emergency Zone but must be unique across all the IP Office Locations.

- The IP Office administrator can manually configure Locations for extensions using IP Office Manager. If set, these are used to determine various things including the call handling for emergency calls by those extensions.
  The Location API permits extensions to have a dynamic location value that overrides their manual location for emergency calls. The dynamic location is not permanently stored in the IP Office configuration and, as the name implies, it is not preserved through restarts. If the location is set to dynamic location then it is used in preference to the manual location. The dynamic location remains set until it is reset via the Location API or from IP Office System Status Application or when the system is re-booted.
  The Sentry application periodically sets the dynamic location to overcome the above scenario and also when reconnecting to IP Office after a reboot or restart of IP Office.

2.3. Support

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

- **Web**: http://www.911secure.com/
- **Email**: support@911secure.com
- **Phone**: (213) 425-2050

3. Reference Configuration

The IP Office Server Edition configuration used in the compliance testing consisted of a primary Linux server, and an expansion IP500V2, with SCN trunks for connectivity between the two systems. IP Office Server Edition routed Emergency calls via SIP Trunk and the Expansion IP Office 500V2 routed Emergency calls via ISDN-PRI Trunks.

Figure 1 below illustrates the configuration used to compliance test the 911 Secure LLC Sentry NG911 Emergency Location Management Solution with Avaya IP Office. The Sentry Solution (utilizing the Sentinel web server, Sentry database and the Beacon On-site notification application) was installed on a Windows Server 2016 Standard server. Sentry communicated with IP Office (both primary and expansion) using Location API WebSocket. Sentry External Tracker was deployed as a Virtual Machine that was provided by Sentry.

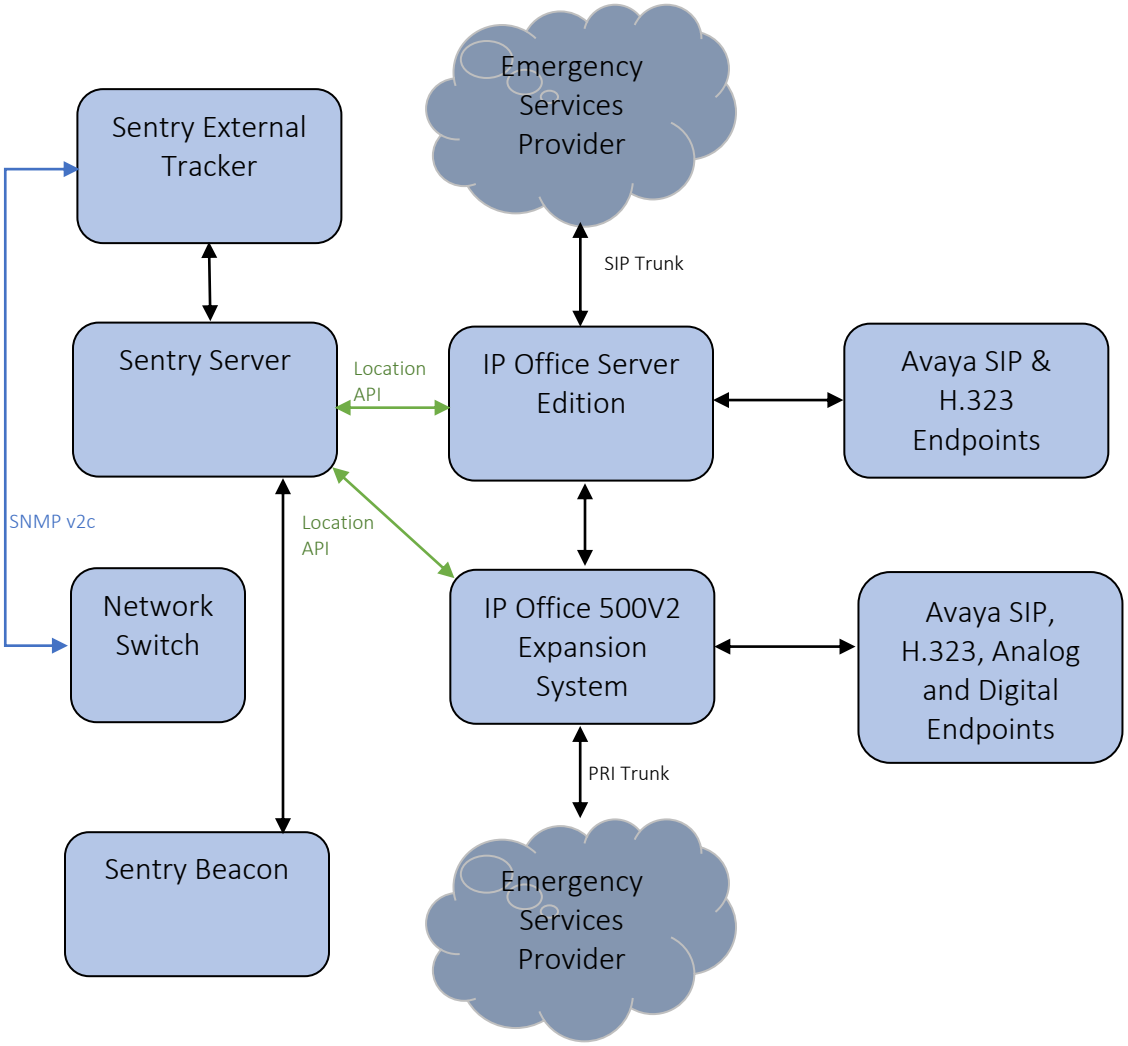


Figure 1: 911 Secure LLC Sentry NG911 Emergency Location Management Solution with Avaya IP Office

4.

5. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya IP Office Server Edition Avaya IP Office 500V2 Expansion System	11.0.4.2.0 Build 58
Avaya Endpoints: 9641G (H323) H175 (SIP) J129 (SIP) J169 (SIP) One-X® Communicator (SIP)	 6.8.2 1.0.2.3 4.0.3 4.0.3 6.2.10
Avaya 9504 Digital Deskphone	1.1
Avaya Analog Deskphone	N/A
911 Secure Sentry server (Windows Server 2016 Standard) 911 Secure External Tracker Location API	1.11.316.1 v20200305.1 10.0

Note: *Testing was performed with IP Office Server Edition and an Expansion IP Office 500 V2. Testing also applies to an IP Office 500 V2 standalone system, and all IP Office Server Edition configurations.*

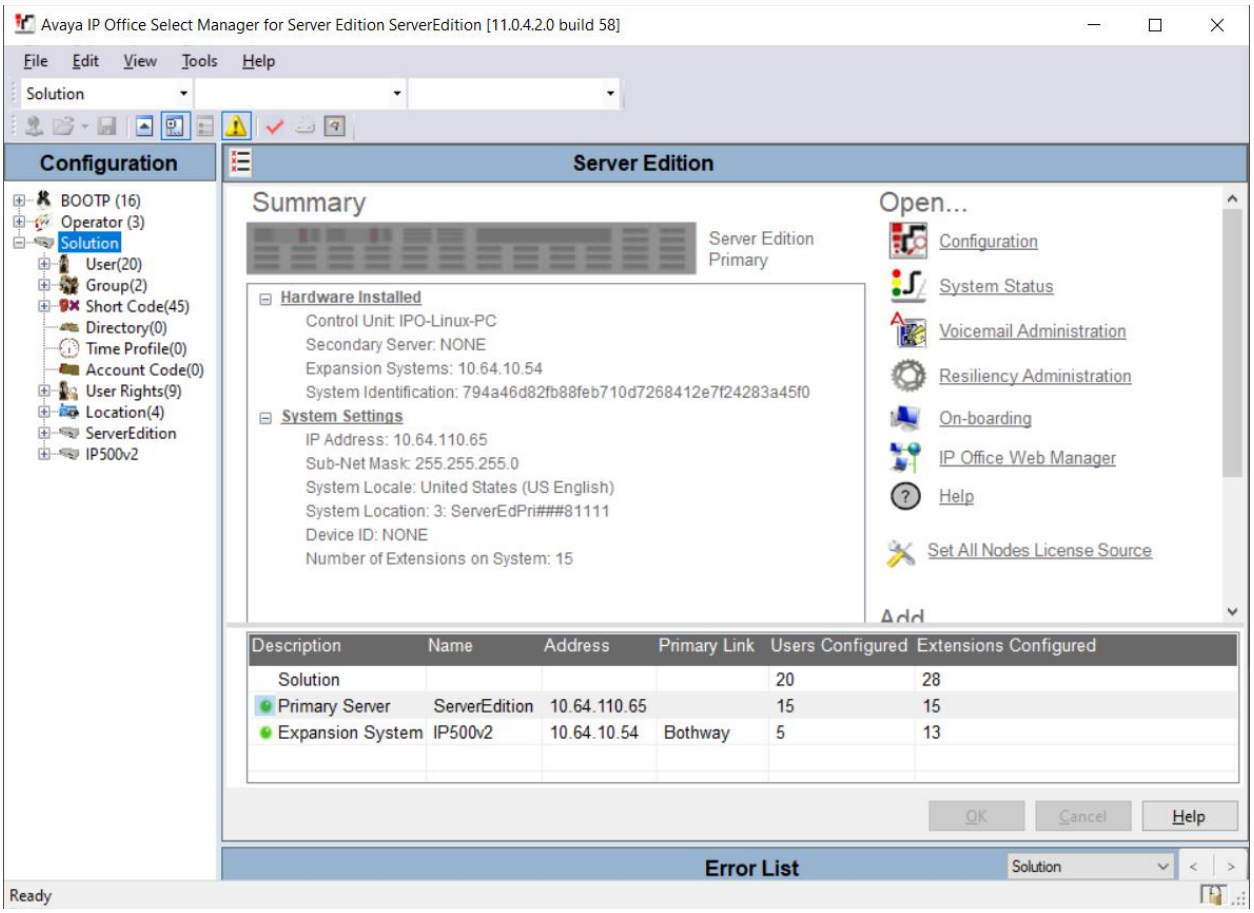
6. Configure Avaya IP Office

Configuration and verification operations on the Avaya IP Office illustrated in this section were all performed using Avaya IP Office Manager. The information provided in this section describes the configuration done on the Primary (Linux server) system. The configuration described below needs to be implemented on the Expansion system also. It is implied a working system is already in place with the necessary licensing. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section** 10 **Additional Resources**.

The configuration operations described in this section can be summarized as follows:

- Configure System
- Configure Security Settings for Location API
- Configure Emergency Calls
- Create ARS
- Create Short Codes
- Create Locations
- Configure IP Office System Location
- Configure Lines
- Save Configuration

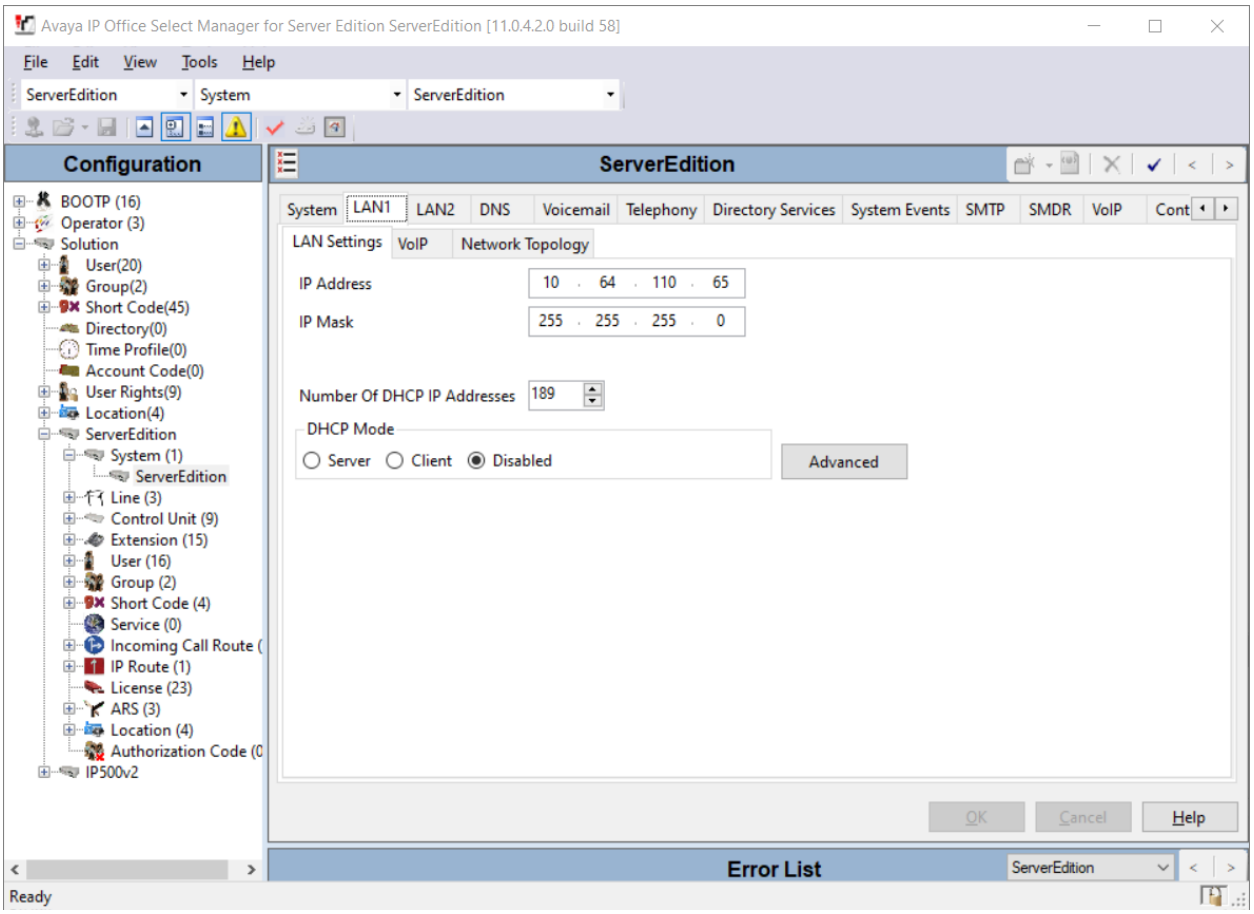
From a PC running the IP Office Manager application, select **Start → Programs →IP Office → Manager** to launch the Manager application. Select the proper IP Office system, and log in using the appropriate credentials (not shown). The **Avaya IP Office Manager for Server Edition** screen is displayed as shown below.



6.1. Configure System

From the configuration tree in the left pane, select **Solution → ServerEdition → System → ServerEdition** to display the screen in the right pane, where **ServerEdition** is the name of the IP Office system.

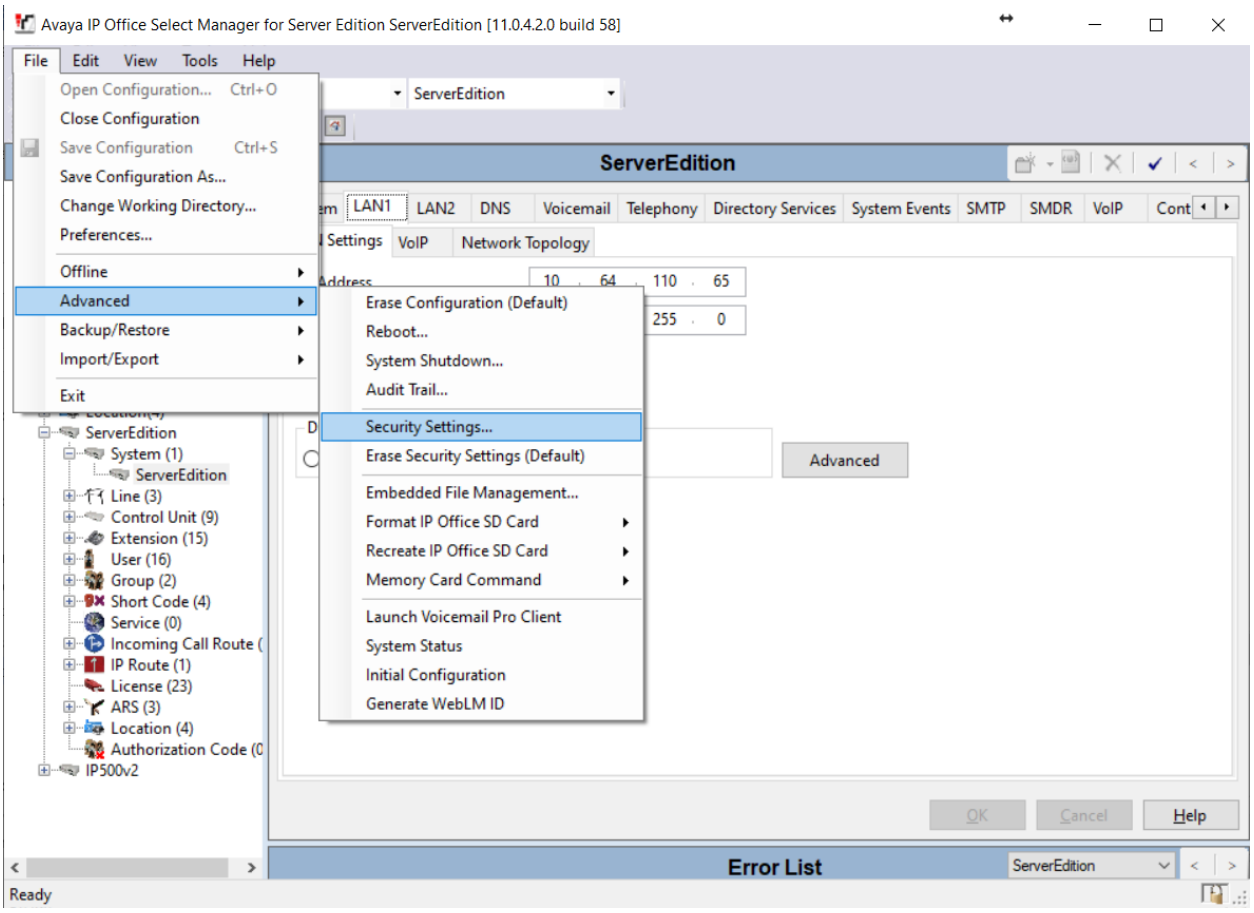
Select the **LAN1** tab, IP Office can support LAN1 and/or LAN2 interfaces, however during compliance testing the LAN1 interface was used. From the **LAN Settings** sub-tab, note the **IP Address** configured, which is **10.64.110.65**. This IP Address is required by 911 Secure while configuring Call Servers in Sentinel web server as described in **Section 7.2**.



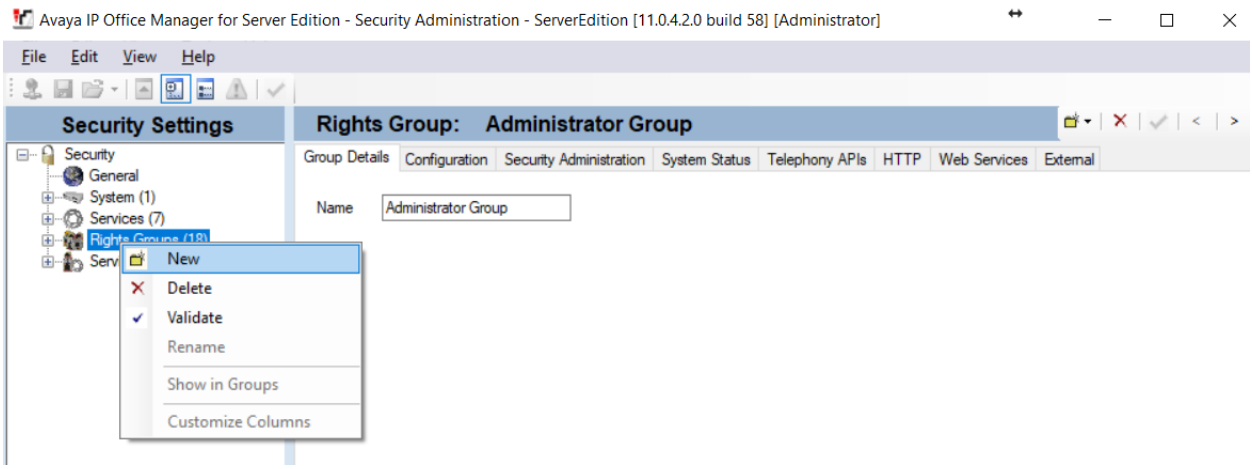
6.2. Configure Security Settings for Location API

In order for the Sentry Server to communicate with IP Office Location API, a Rights Group and User must be created in IP Office. Afterwards, the location information provided in IP Office can be used by the Sentry Server to provide location-specific information when a 911 call is made. These required security steps allow the Sentry Server to get the information from IP Office and set the dynamic location in IP Office.

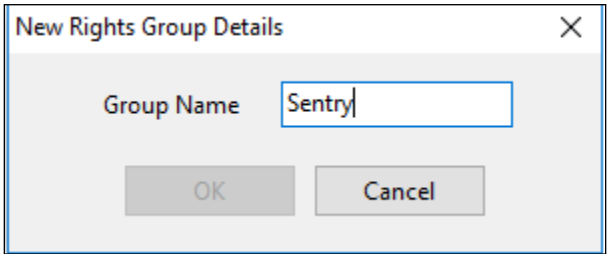
From **Avaya IP Office Manager for Server Edition**, navigate to **File → Advanced → Security Settings** as shown in the screen below.



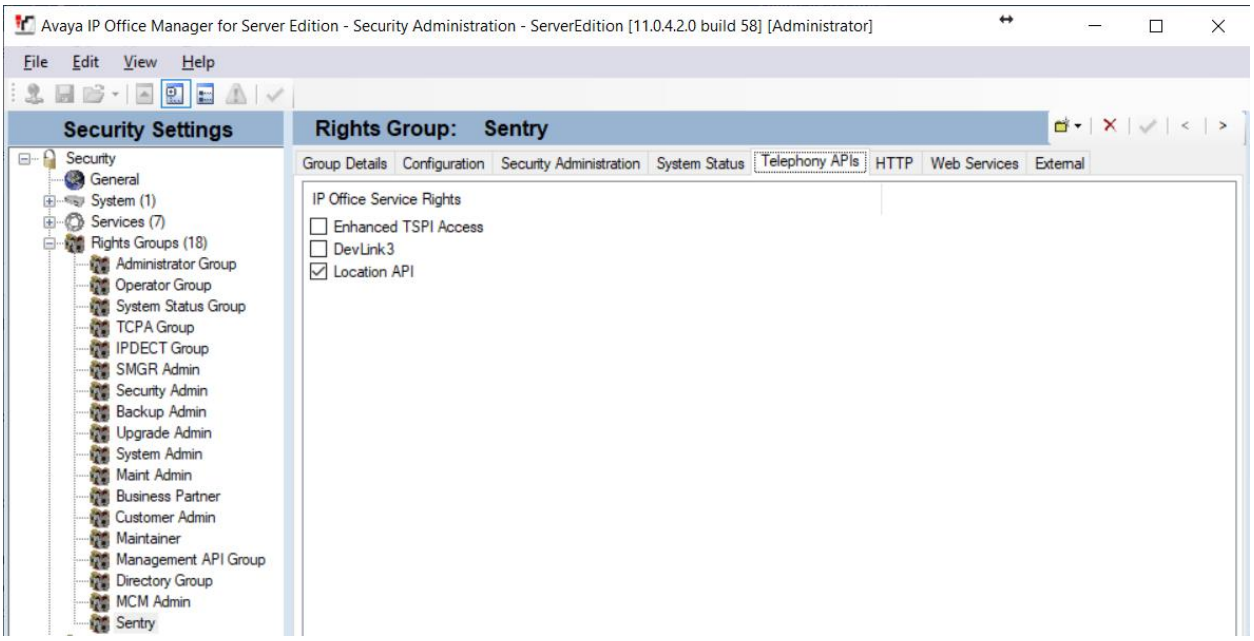
Select **Right Groups** from the left pane and then right click to select **New** as shown in the screen below.



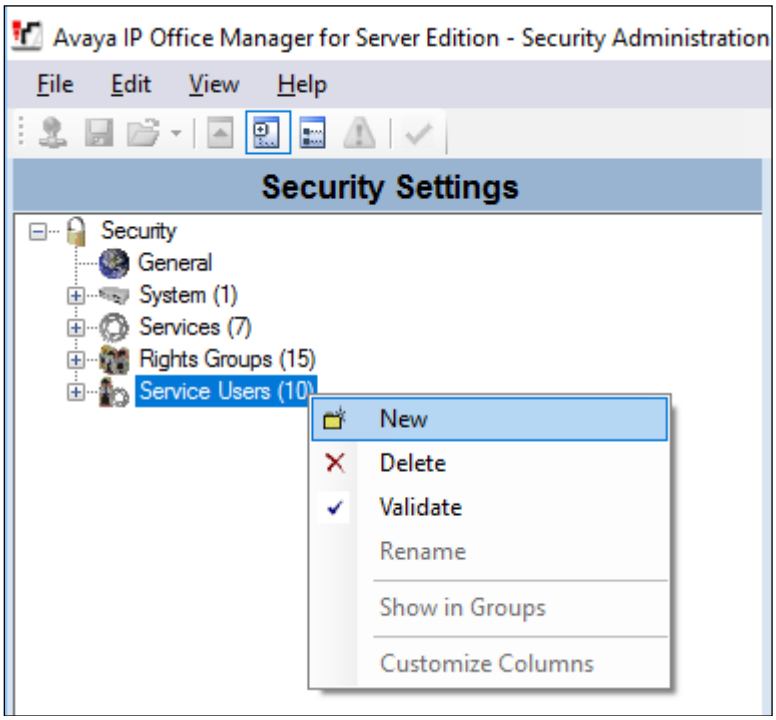
In the following **New Rights Group Details** window, provide a descriptive **Group Name**. During compliance testing, **Sentry** was configured.



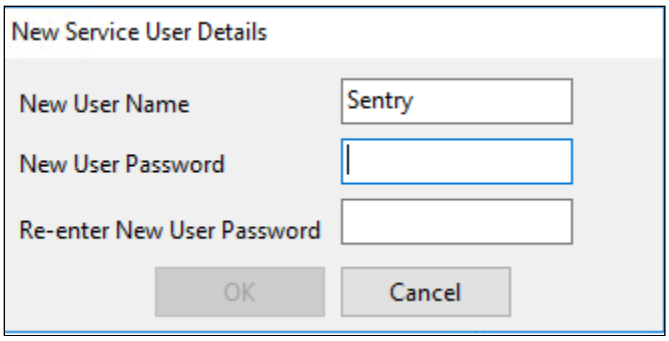
In the **Rights Group: Sentry** window shown below, navigate to the **Telephony APIs** tab and select the **Location API** box.



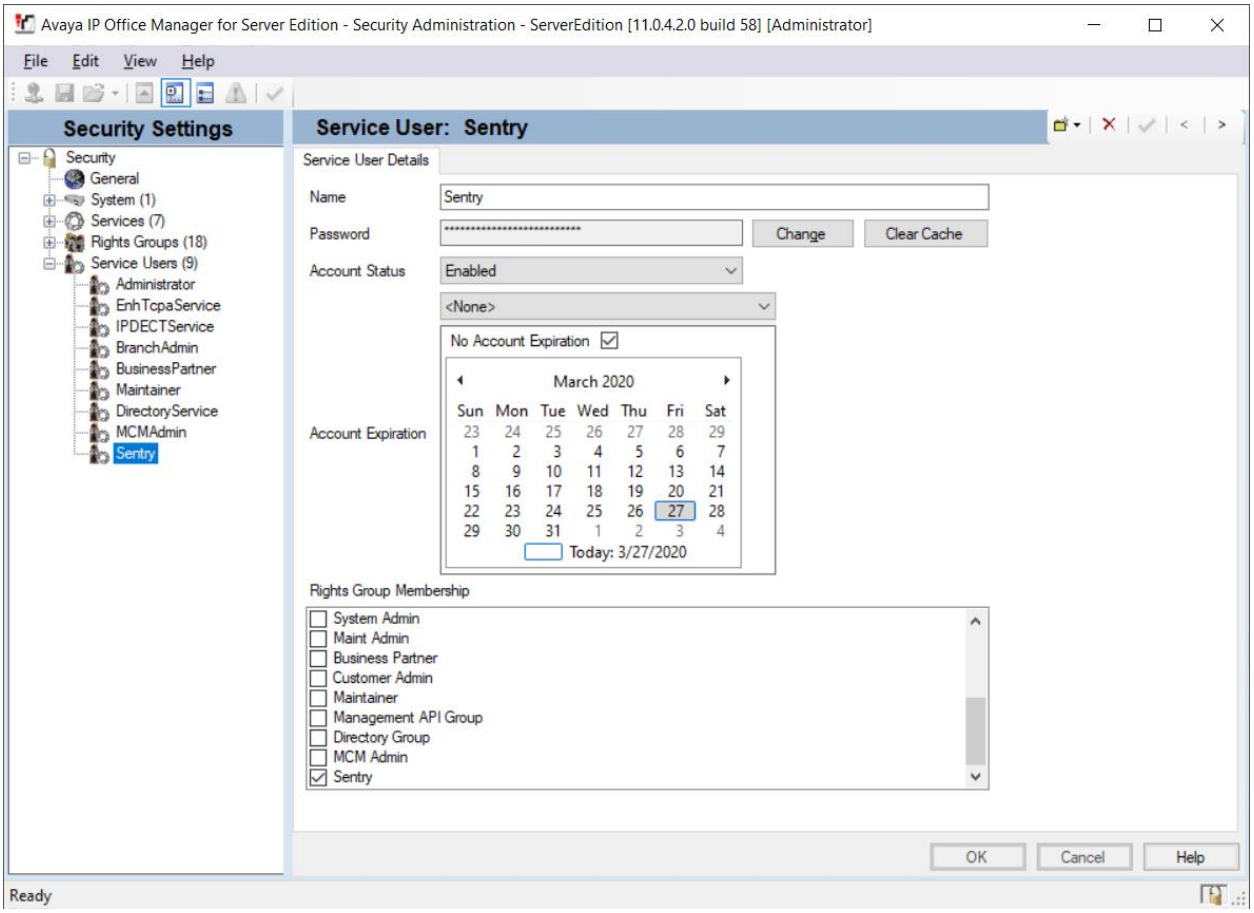
Select **Service Users** from the left pane and then right click to select **New** as shown in the screen below.



In the following **New Service User Details** window, provide a descriptive **New User Name**. During compliance testing, **Sentry** was configured. Configure password for this new service user created. Sentry server will connecte to IP Office Location API using this user name and password.



In the **Service User: Sentry** window shown below, under **Rights Group Membership** window select the **Sentry** Rights Groups Membership box.



6.3. Configure Emergency Calls

IP Office Manager expects that the configuration of each system to contain at least one short code that is set to use the Dial Emergency feature. If no such short code is present in the configuration, then Manager will display an error warning. The importance of the Dial Emergency feature is that it overrides all external call barring that may have been applied to the user whose dialing has been matched to the short code. Also, ensure that no other short code or extension match occurs that would prevent the dialing of an emergency number being matched to the short code.

The short code (or codes) can be added as a system short code or as an ARS record short code. If the Dial Emergency short code is added at the solution level, that short code is automatically replicated into the configuration of all servers in the network and must be suitable for dialing by users on all systems. Separate Dial Emergency short codes can be added to the configuration of an individual system. Those short codes will only be useable by users currently hosted on the system including users who have hot-desked onto an extension supported by the system. For compliance testing, short codes were configured for the individual systems.

It is the installer's/administrator's responsibility to ensure that a Dial Emergency short code or codes are useable by all users. It is also their responsibility to ensure that either:

- The trunks via which the resulting call may be routed are matched to the physical location to which emergency service will be dispatched.

  or

- The outgoing calling line ID number sent with the call matches the physical location from which the user is dialing.

When configuring locations, consult local guidelines. For example, regions may require identification based on building or building floor. Floors may be subdivided based on number of staff or the location of hazardous materials. Typically, fire alarm planning will have defined zones based on these or similar requirements.

Routing of emergency calls is based on a call resolving to a Dial Emergency short code. Based on the location value for the extension making the call, routing is performed as configured in the Emergency ARS.

Following steps were performed to configure routing of Emergency calls during the compliance testing:

1. Create an Emergency ARS containing a Dial Emergency short code.

2. Create a Short Code to use the ARS added in **Step 1**.

3. Create a Location and set the Emergency ARS to the ARS created in **Step 1**.

4. Open the Extn tab for an extension that will use the location defined in **Step 3** and set the Location value to the location defined in **Step 3**.

   Note that once you define a location, you must set a system Location value by navigating to each IP Office system. E.g., **Solution → ServerEdition → System → ServerEdition**.

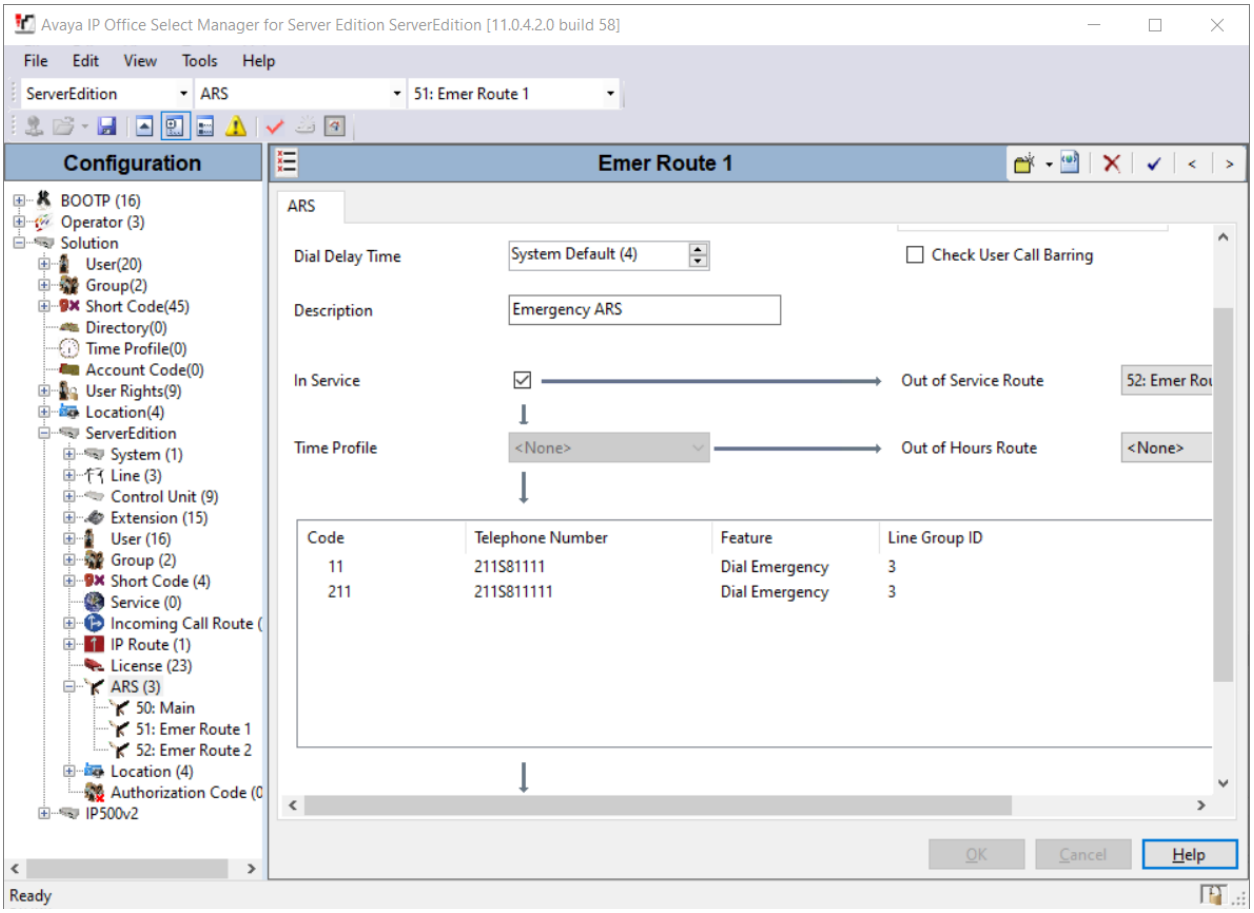
   For non-IP based extensions, the system location value is used as the default if no location is assigned to them. For IP based extensions, the location value is set to Automatic.

5. To test an emergency call, from the extension used in **Step 3**, dial the Dial Emergency short code. Avaya IP Office checks the location value and determines the emergency ARS set for the location. Once the emergency ARS is found, Avaya IP Office will try to match the Telephone Number in the Dial Emergency short code to a short code in the ARS and use it to make the emergency call.

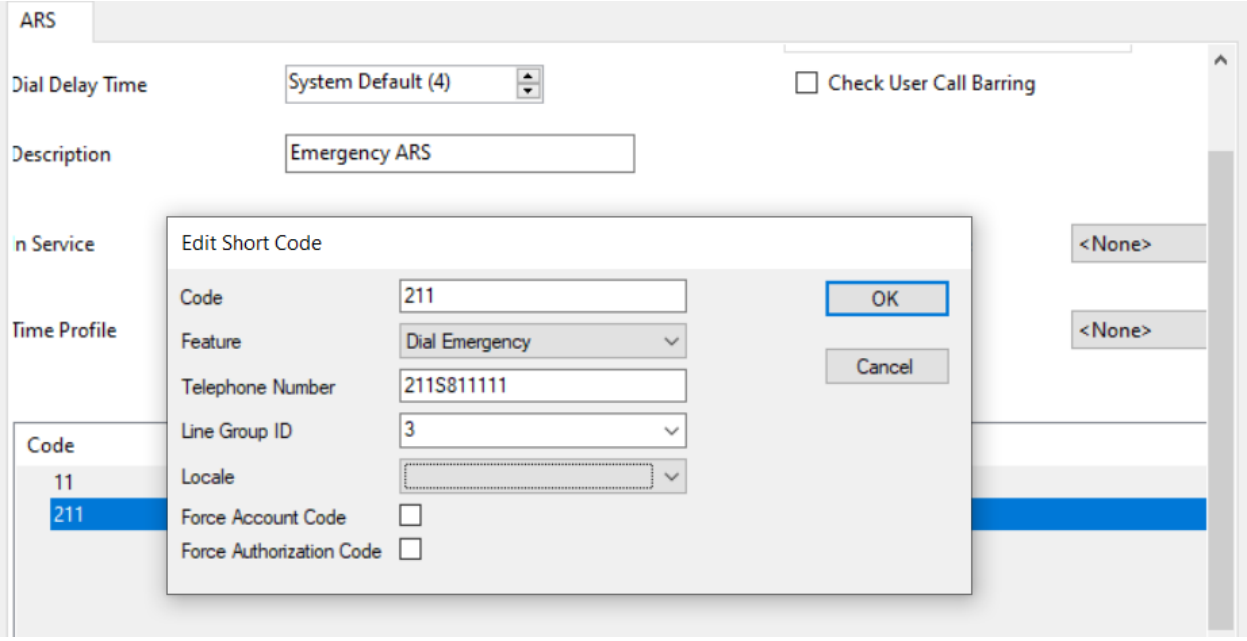
The sections below show the configuration used during compliance testing.

6.4. Create ARS

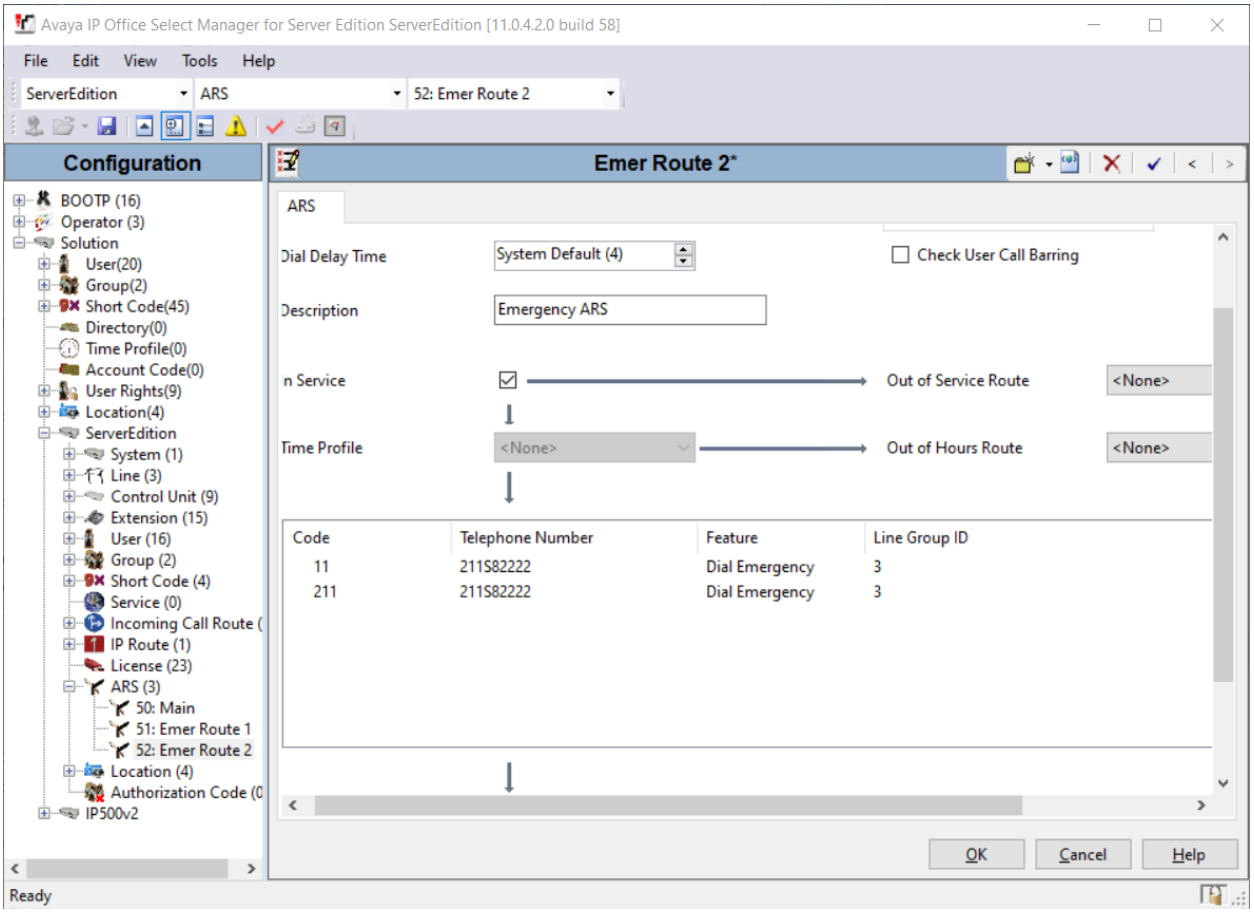
Navigate to **ServerEdition → ARS**, and then right click and select **New** (not shown). Provide a descriptive **Route Name** and ensure **In Service** box is selected. Click the **Add…** button on the right to add an ARS short code. Perform this step on each IP Office system. During the compliance test, two ARS were added on each IP Office system.



The screen below shows short code **211** was created. For compliance testing, calls to 211 was used to test emergency calls rather than placing actual 911 calls. Set the **Feature** to **Dial Emergency**. The **Telephone Number** was set to "211S81111" during compliance testing. Set the **Line Group ID** value to the line to be used to route emergency calls. When an Emergency call is placed via this short code, the calling party number of an extension on IP Office will be replaced with the digits following S in the **Telephone Number** field. In this case, the calling party number (caller ID) will set to 81111 when an emergency call is placed.

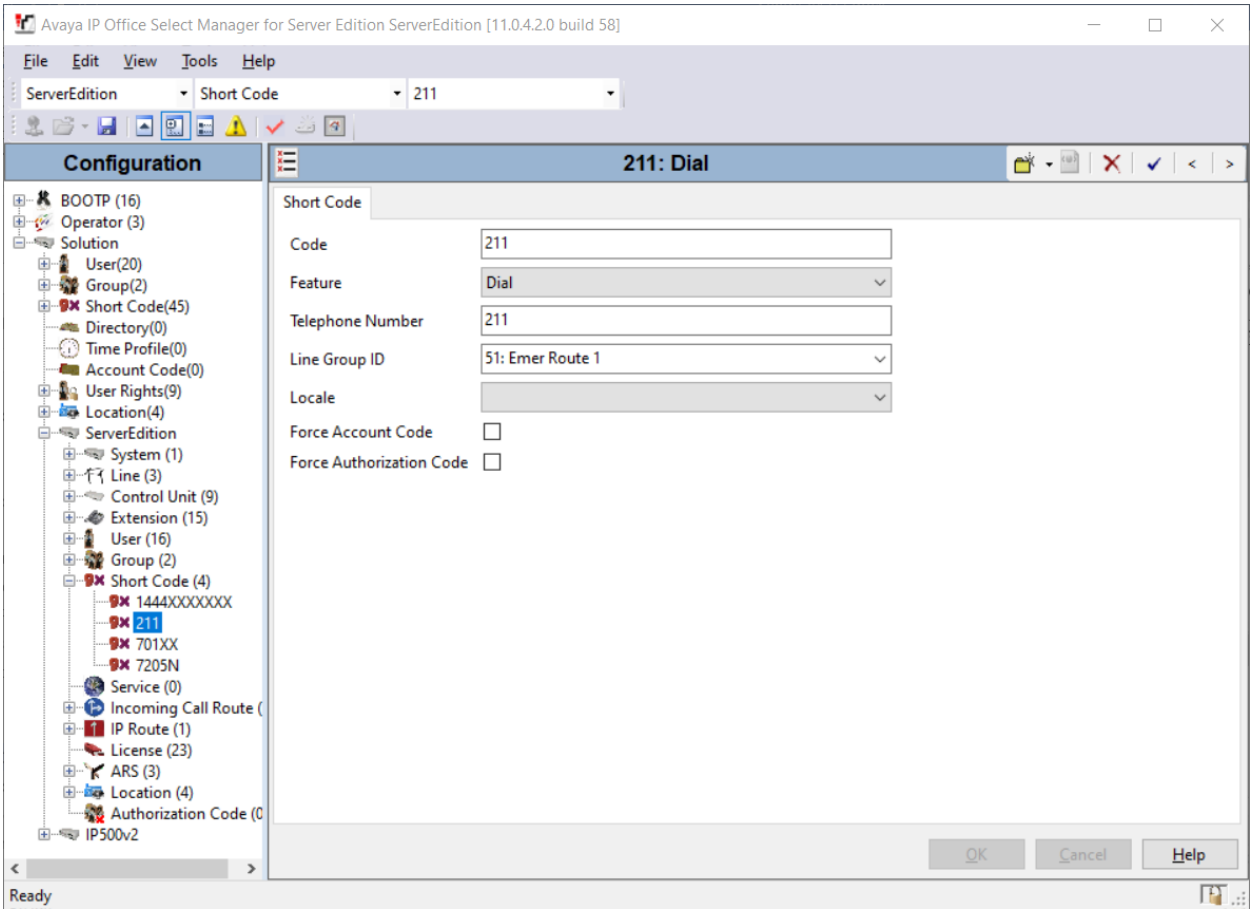


Following screen capture displays the 2nd ARS added on the Server Edition IP Office system. Note that when this ARS is used for routing the Emergency calls, the calling party number will be set to 82222.



6.5. Create Short Code

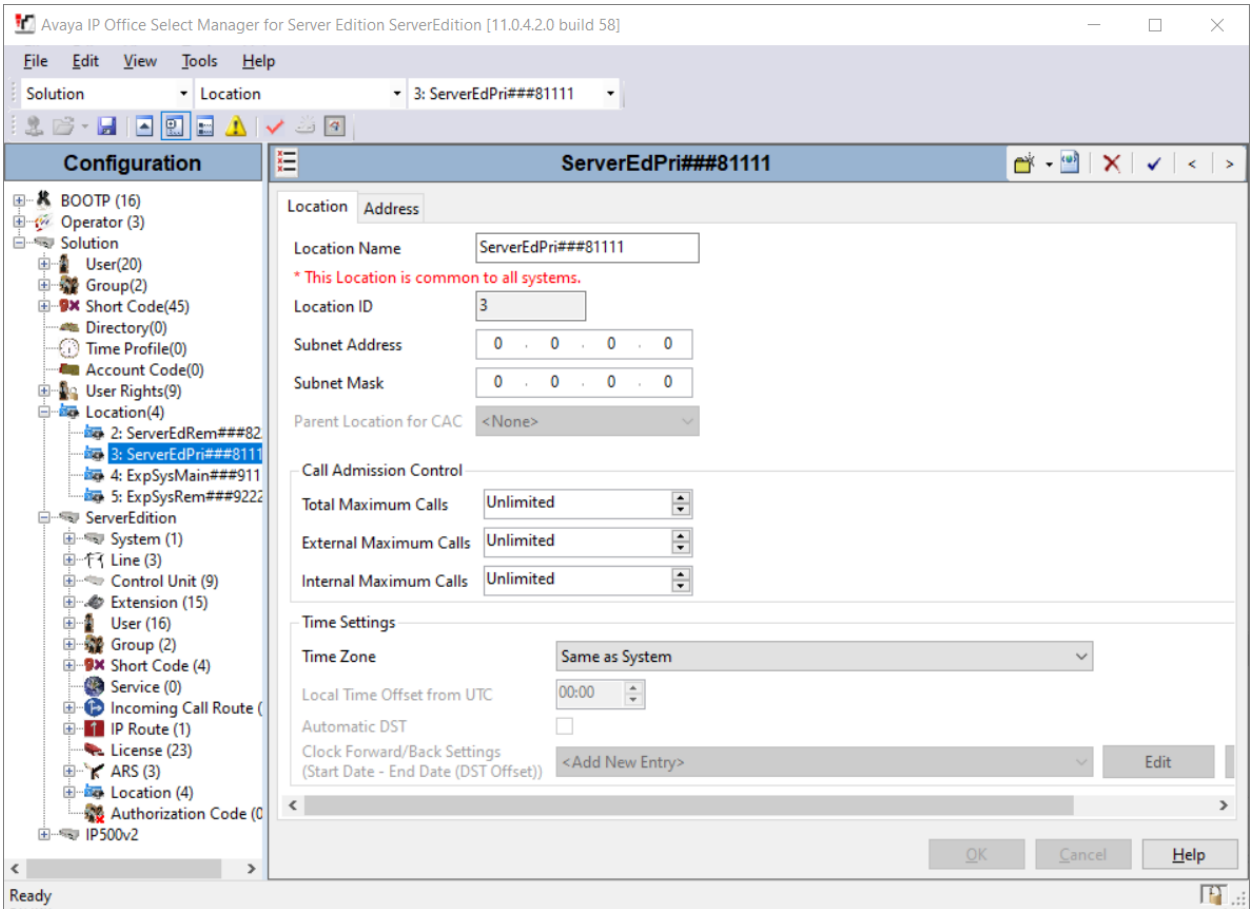
Navigate to **ServerEdition → Short Code**, and then right-click and select **New** (not shown). The screen below shows short code **211** was created. For compliance testing, calls to 211 were used to test emergency calls rather than placing actual 911 calls. Set the **Feature** to **Dial**. The **Telephone Number** was set to **211**. Line Group ID is set to ARS configured in previous section.



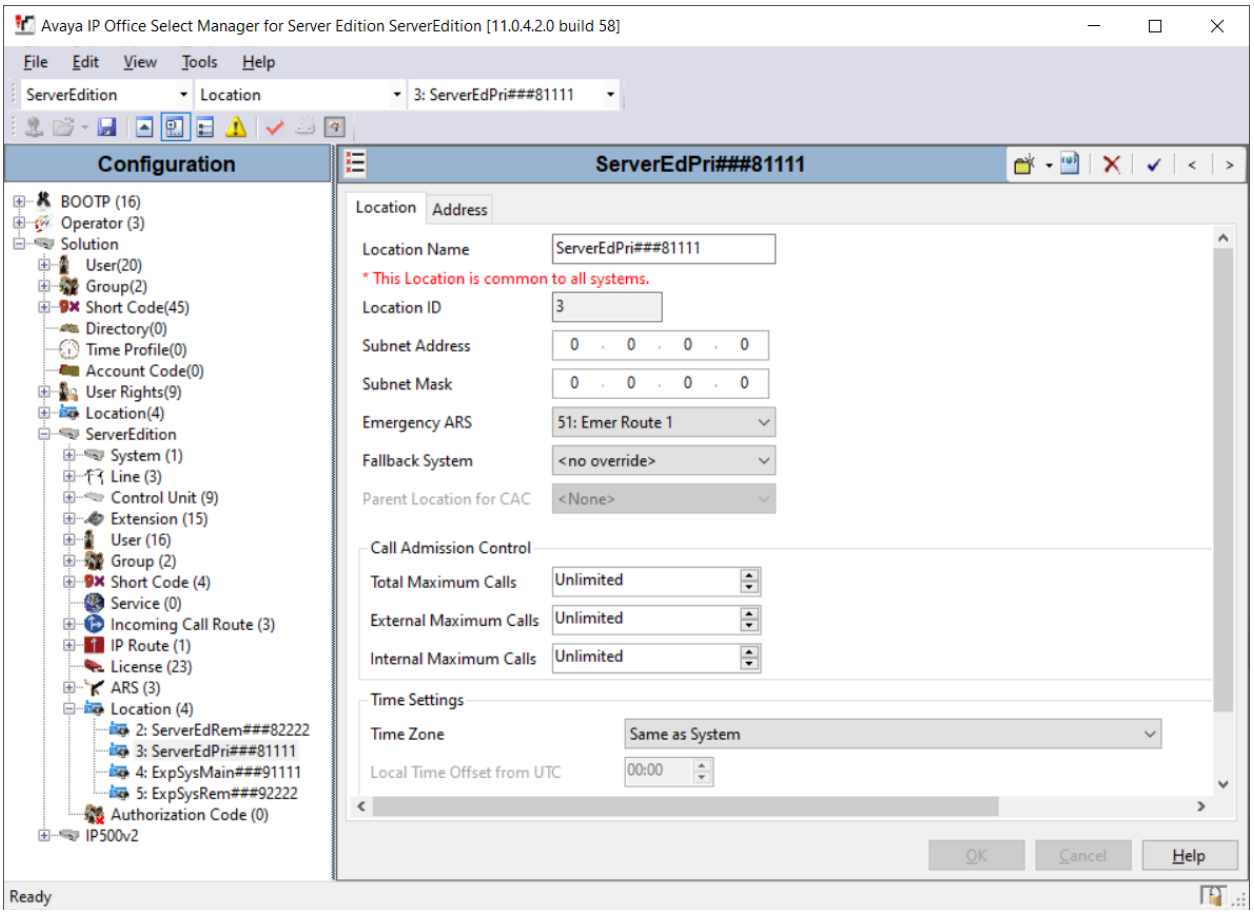
6.6. Create Locations

In a Primary/Expansion environment of IP Office, **Location** can be set at the **Solution** level; however, the **Emergency ARS** needs to be set at the individual system level. During compliance testing, the Locations were configured at the Solution level and Emergency ARS was configured at individual system as mentioned below. There were four Locations configured during the compliance test, two for Server Edition and the rest for 500V2.

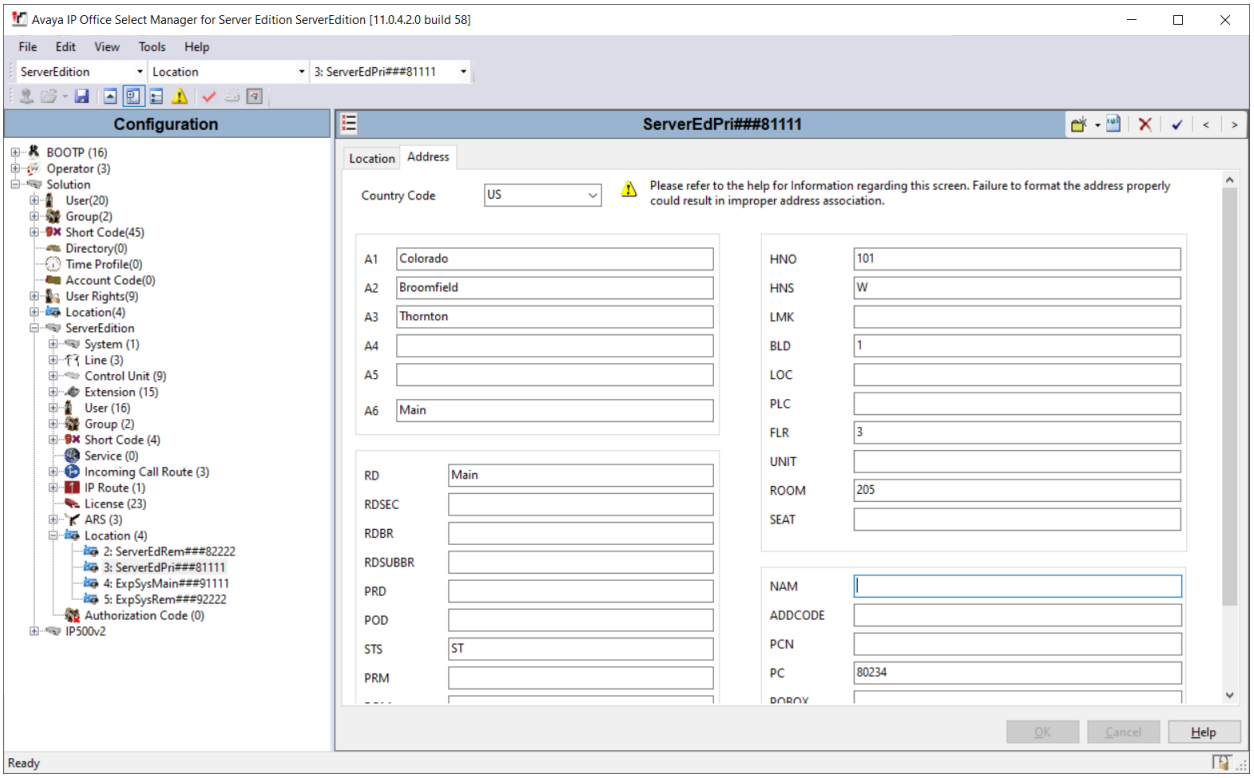
Navigate to **Solution → Location**, and then right click and select **New**. Configure the **Location Name** by following the specifications as explained in **Section 2.2**.



Now, from the individual IP Office system, navigate to **ServerEdition → Location** and select the newly configured location, in this case **ServerEdPri###81111**. Set **Emergency ARS** to the ARS entry created in **Section 6.4**. Retain default values for all other fields. It is very important to associate an Emergency ARS with the location; without it the correct Emergency ARS will not be invoked.

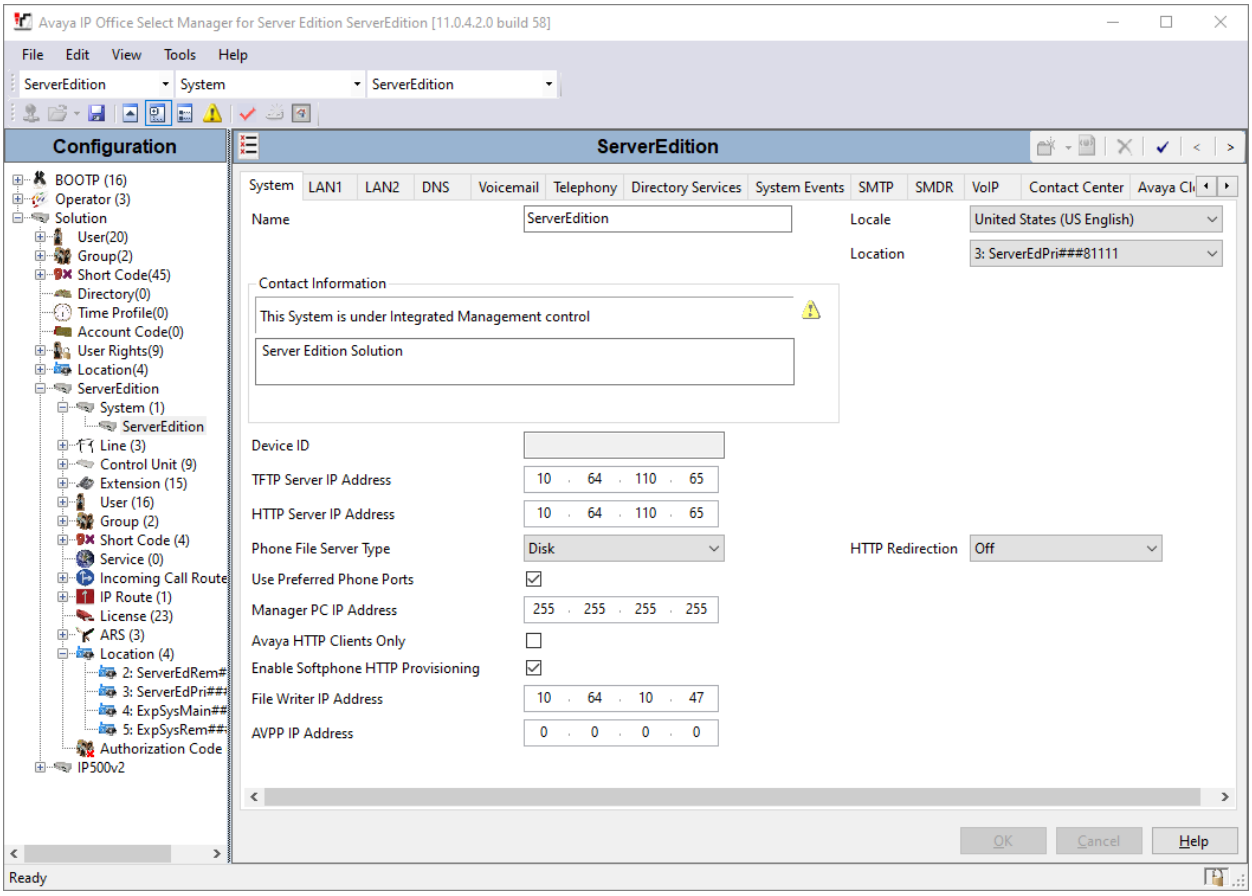


In the **Address** tab, additional information can be provided for the location by configuring the various fields. During compliance testing, the following information was configured. It is very important to work with 911 Secure Engineers to configure these fields.



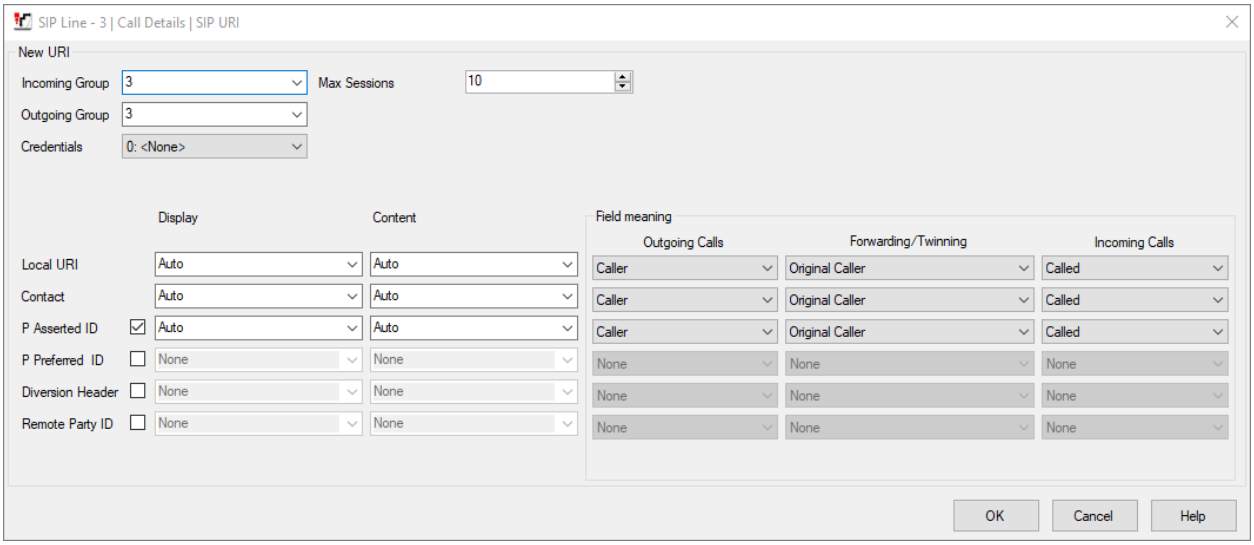
6.7. Configure IP Office System Location

Associate each IP Office system with a Location. On the left Navigation pane, click **ServerEdition → System** for the Primary Server and select a **Location** from **Section 5.6**. Again, please note that the Location being selected should have the correct Emergency ARS associated. Similarly, assign a location for the expansion IP Office system (not shown).

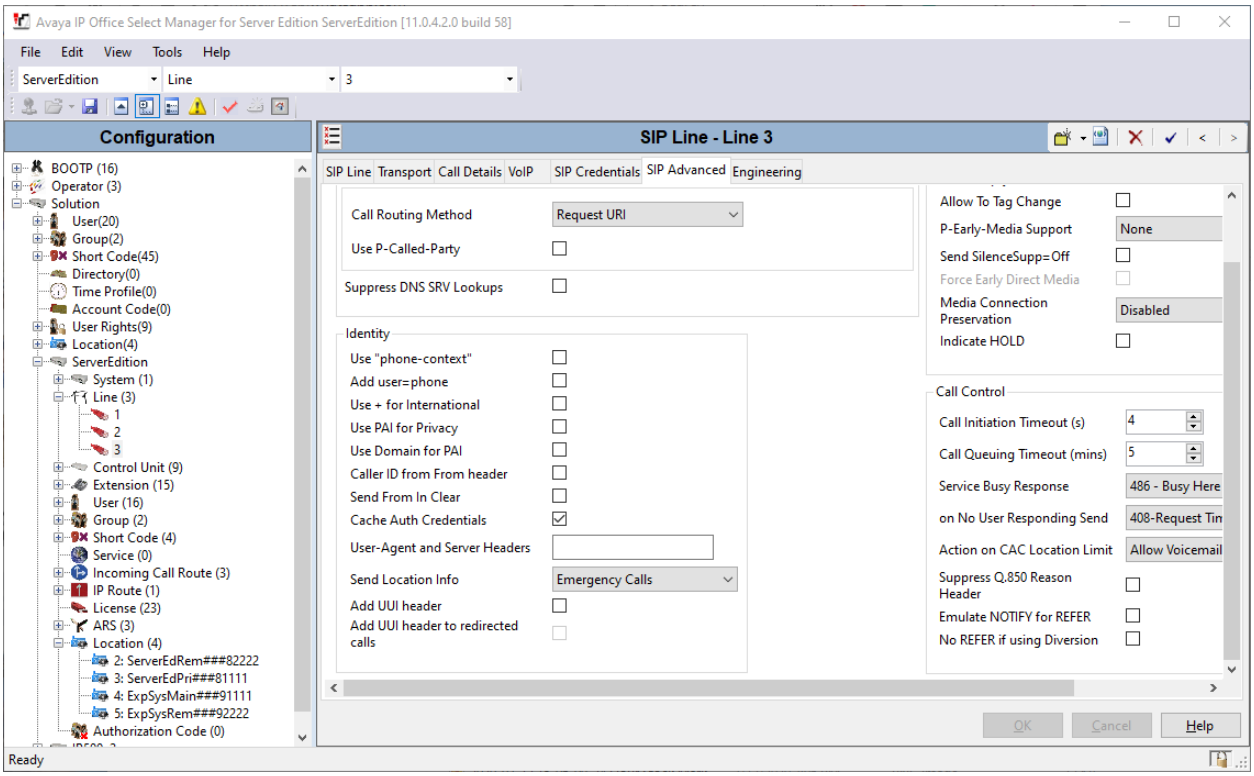


6.8. Configure Lines

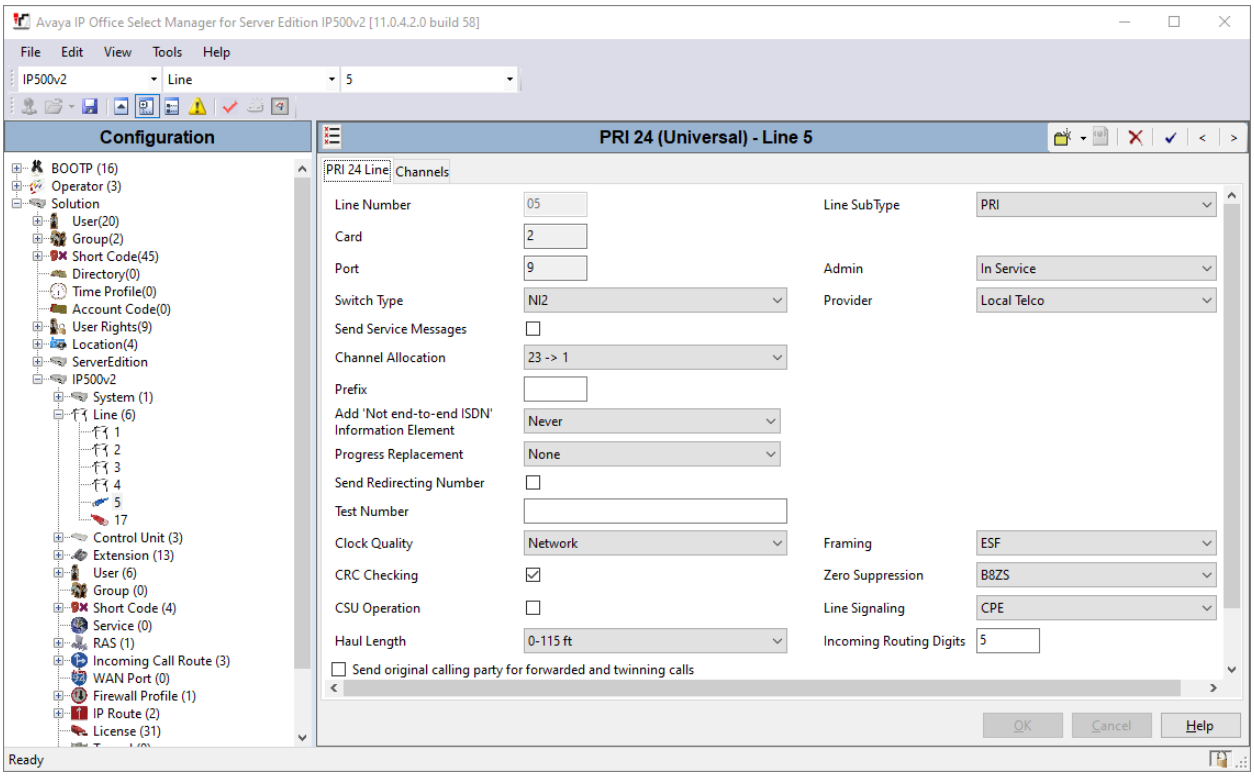
Emergency calls were routed via SIP Trunks from the Server Edition. Configuration for a SIP line is standard in nature, but the following screen capture displays the configuration used during the compliance test. SIP Line 3 was configured as shown below.



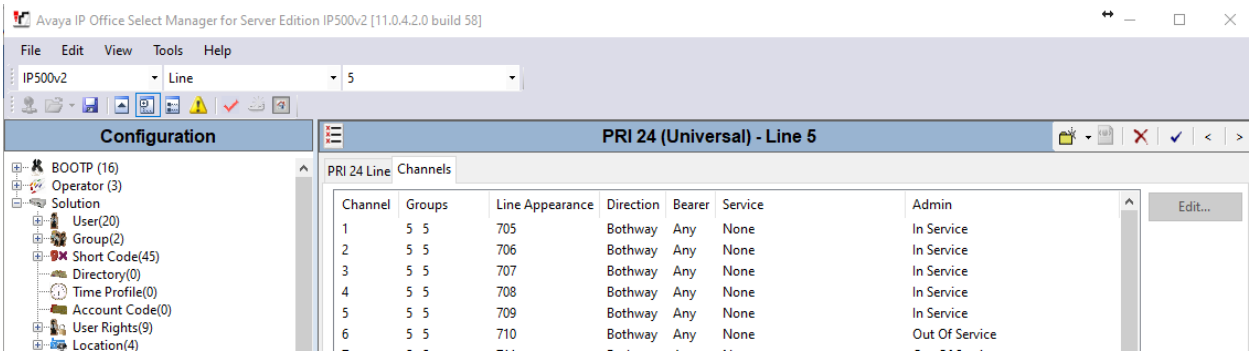
If Location data needs to be sent to the Emergency services provider (via pdf), set the **Send Location Info** to **Emergency Calls** under the **SIP Advanced** tab.



Emergency calls were also routed via an ISDN-PRI trunk from the IP Office 500V2 system. The ISDN-PRI Line was configured as shown below:

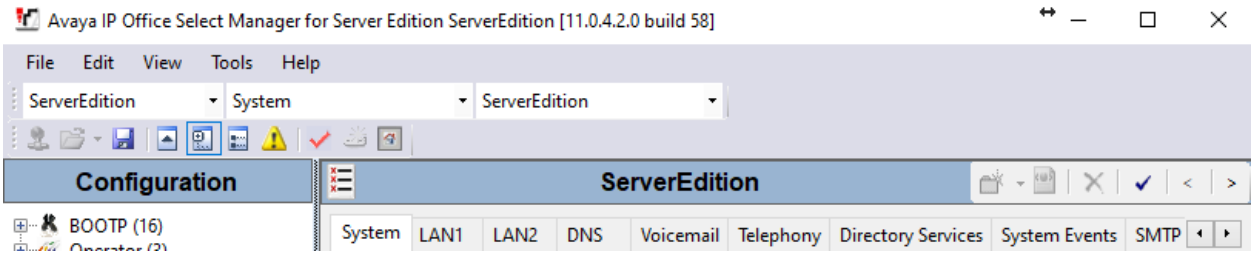


Five channels were enabled during the compliance test.



6.9. Save Configuration

Once all the configurations are complete, the changes need to be saved on the IP Office System. Click on the **Save** icon as shown in the screen below to save the changes, a subsequent window will appear (not shown) asking the user to proceed with the changes made to the IP Office system/s or not. Click on the **OK** button to confirm (not shown).

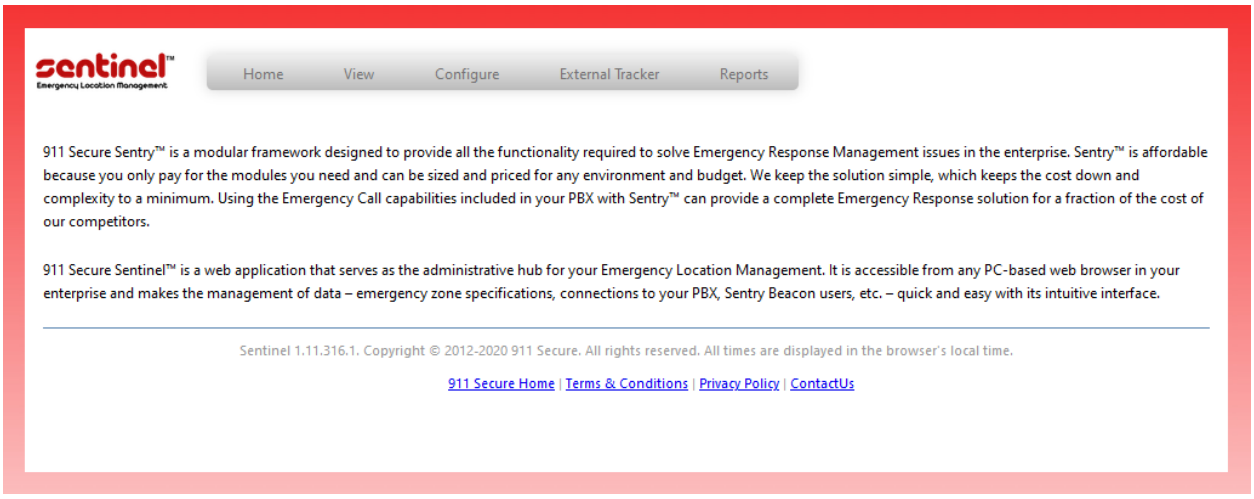


7. Configure 911 Secure LLC Sentry NG911 Emergency Location Management Solution

It is assumed that the Sentry server has been installed, configured, and is ready for the integration with Avaya IP Office. 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 IP Office.

7.1. Sentinel Web Interface

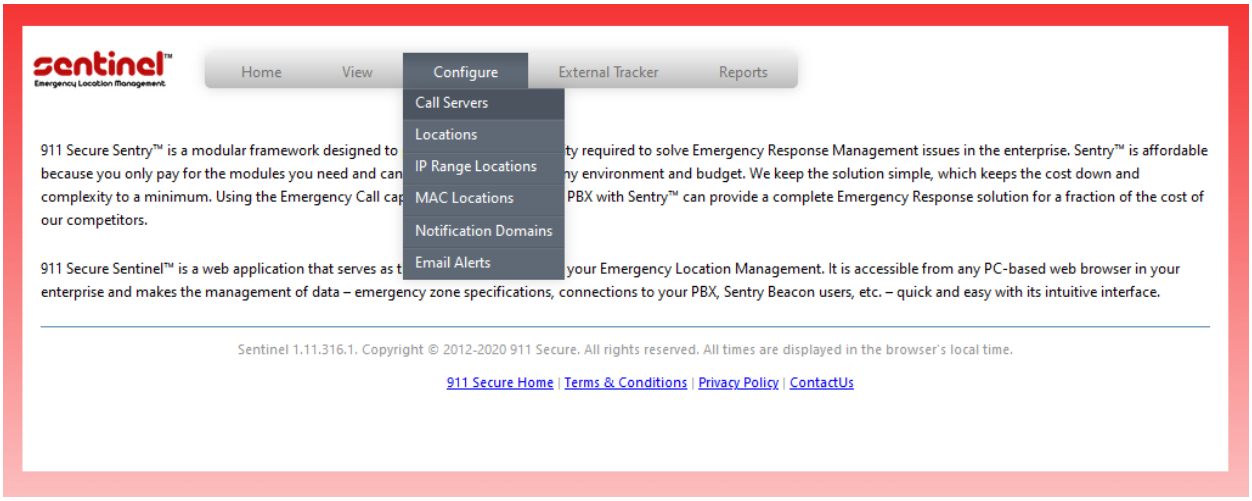
Access the Sentinel web interface by logging into the Sentry server, opening a web browser and entering the following URL: ***http://localhost/Sentinel***. If https support has been enabled and a server certificate using a FQDN has been generated and added to the server, then adjust the URL accordingly.



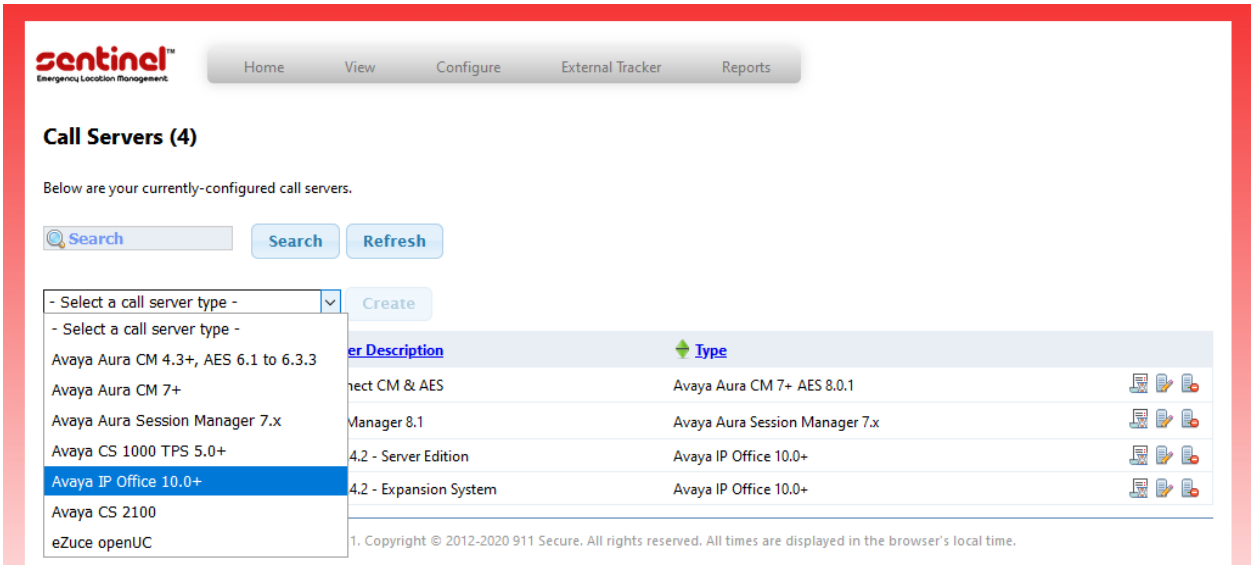
7.2. Configure Call Servers

This section explains the configuration required for Sentry to connect to IP Office Call Server. In this compliance testing, Sentry connected to both the primary and expansion systems of IP Office. Thus, two Call Servers were added.

From the main screen of Sentinel web page, navigate to **Configure → Call Servers** as shown below.



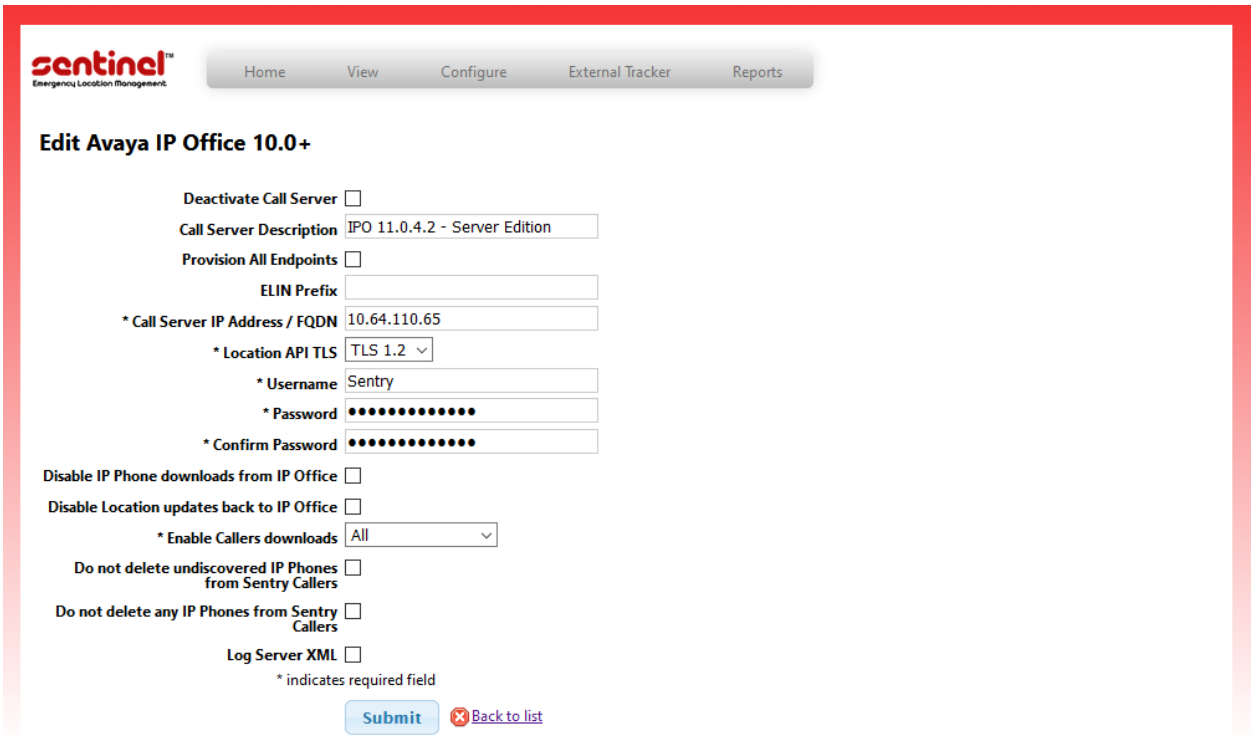
From the **Call Servers** screen, select **Avaya IPOffice 10.0+** from the **Select a call server type** drop down menu as shown below and click the **Create** button (not shown).



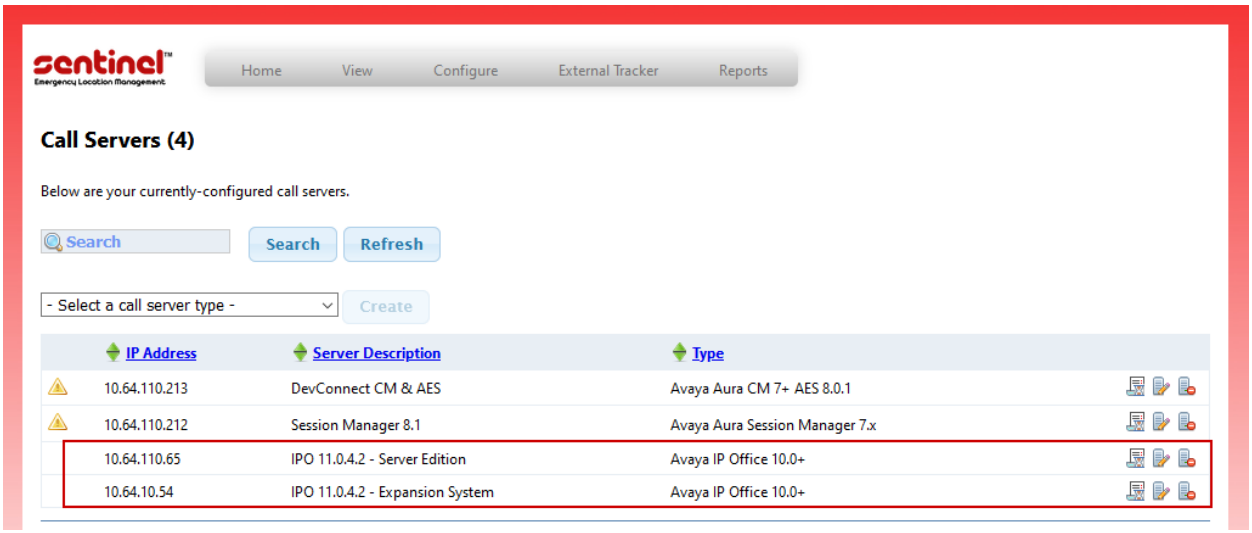
In the **Create Avaya IPOffice 10.0+** screen shown below, configure the following values:

- **Call Server Description:** A descriptive name
- **Call Server IP Address:** IP address of the primary IP Office
- **Location API TLS:** Set to **TLS 1.2**
- **Username:** Username created in **Section 6.2**
- **Password:** Password configured in **Section 6.2**

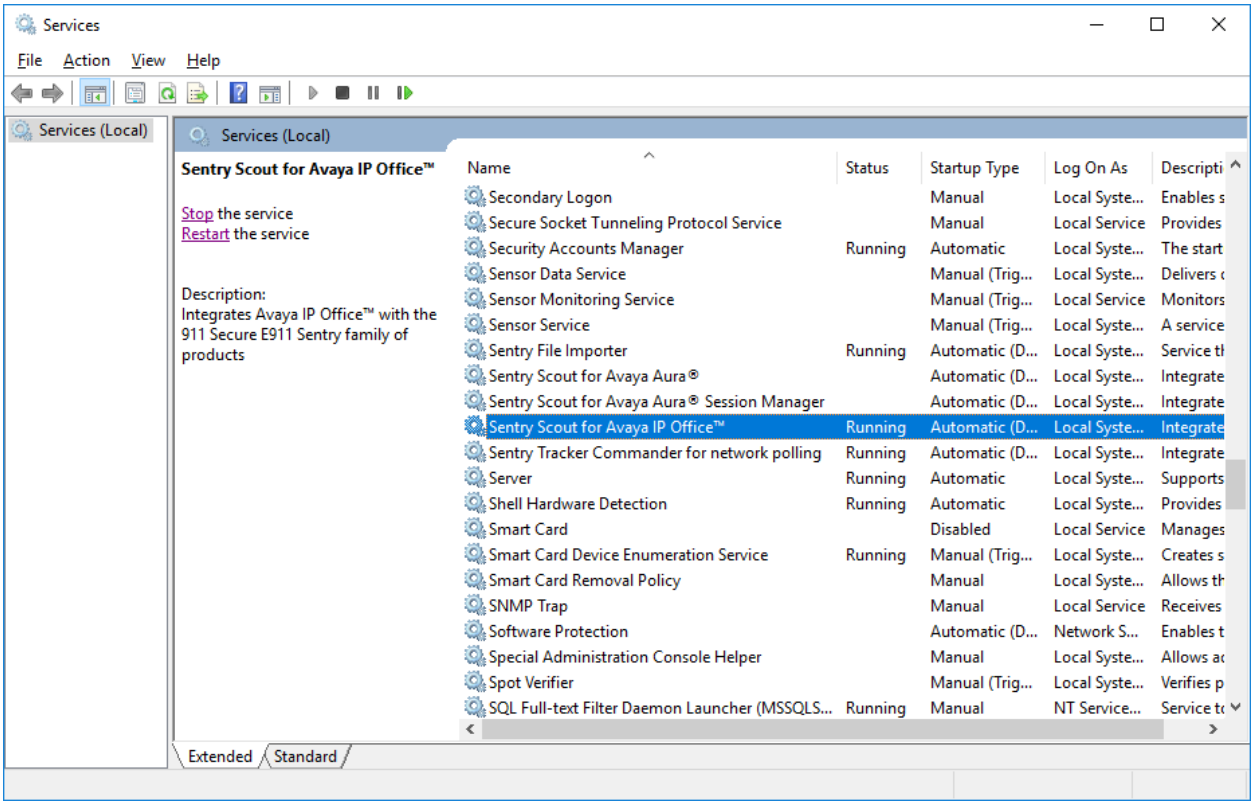
Retain default values for the rest and click on the **Submit** button.



Screen below shows the Call Servers configured during compliance testing, which is the primary and expansion systems of IP Office.



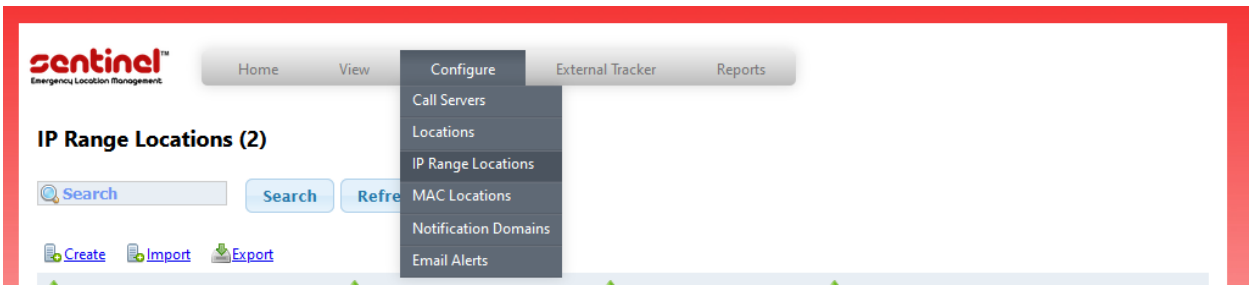
From the **Services** window, restart the **Sentry Scout for Avaya IP Office™** service after adding all the required Call Servers.



7.3. Configure Discovery of IP Phones

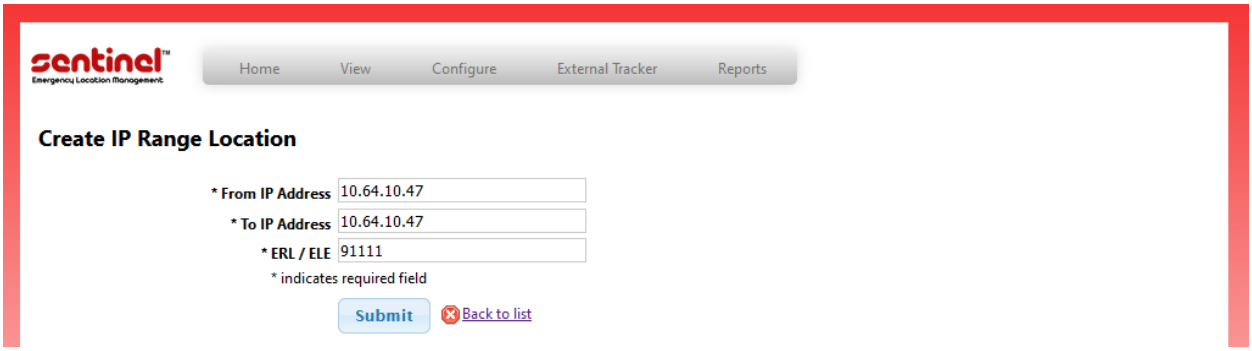
Once the information of locations, H.323, SIP, Digital and Analog phones has been collected by Sentry (refer to **Section 0**), the Emergency Response Location/Emergency Location Extension (ERL/ELE) for the phones need to be configured for use with IP Discovery in Sentry. This section only explains using Sentry's IP Ranges for the discovery of IP phones.

From the main Sentinel web page, navigate to **Configure → IP Range Locations** as shown below.



In the **IP Range Locations** window shown below, click on the **Create** button (not shown).

In the **Create** window, provide an **IP Address** range that the IP phones belong to and configure an **ERL/ELE** for this IP address range as shown below. Click on the **Submit** button.



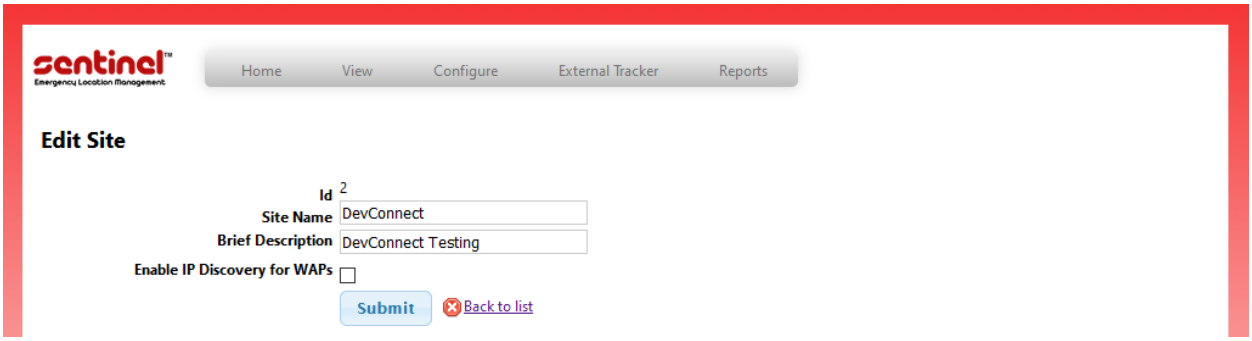
Screen below shows the IP Range Locations configured during compliance testing and their corressponding ERL/ELE values.

7.4. Configure External Tracker

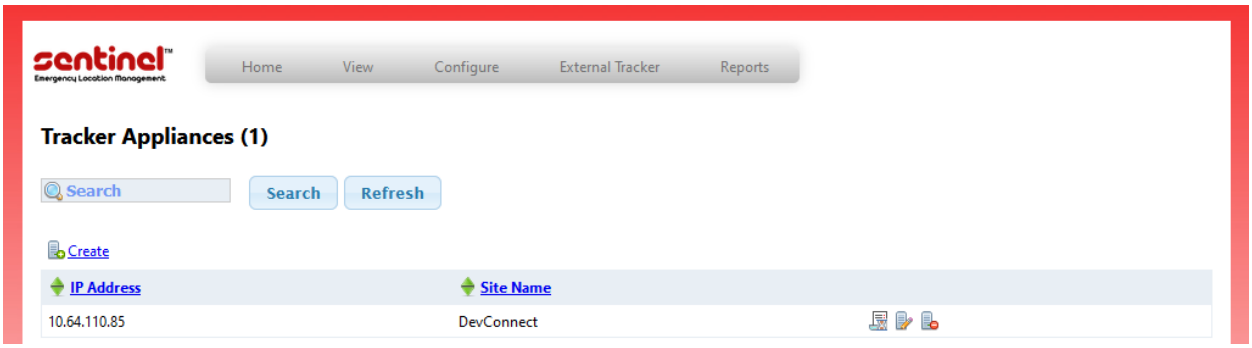
Along with IP Range Locations, the Sentry External Tracker was also tested during the compliance test. External tracker gathers SNMP data from a network switch. Specific ERL/ELE can be associated with a particular port on the switch.

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.

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.



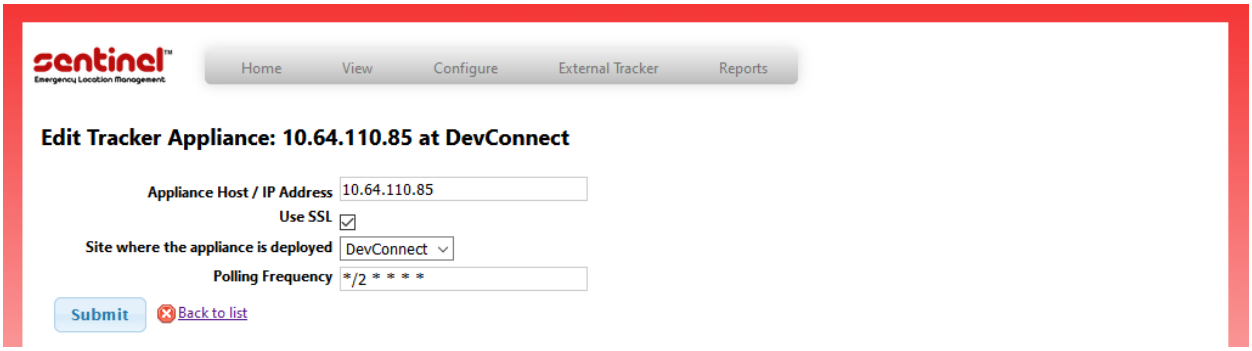
Once the site has been added, navigate to **External Tracker → Appliances.** Select **Create** to add a new External Tracker.



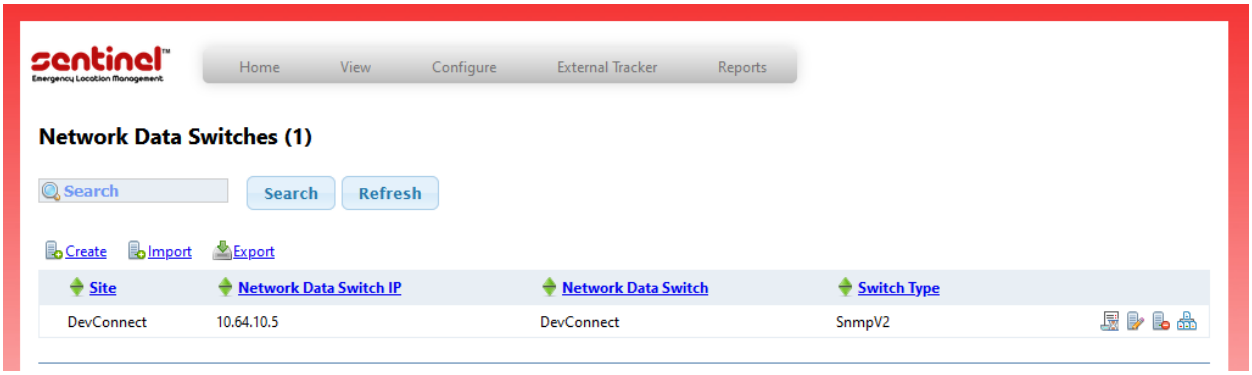
Screen capture below displays the External Tracker configured during the compliance test. Configure the External Tracker as follows:

- **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.



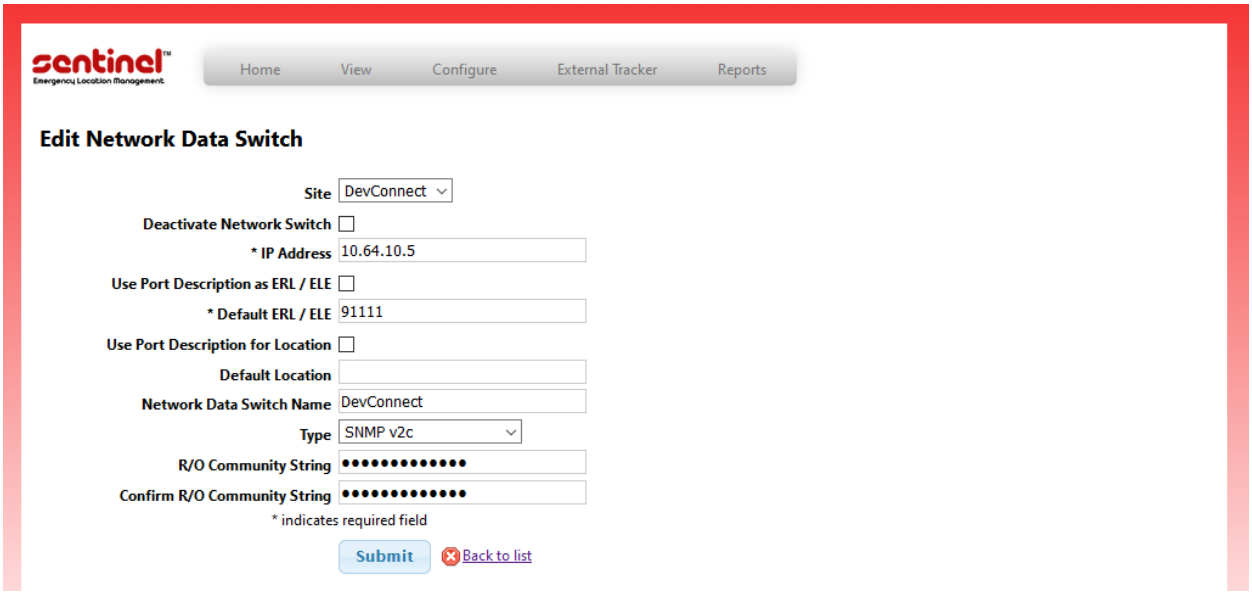
Once the External Tracker has been added, add a network switch that can be used by External Tracker to gather the SNMP data. Navigate to **External Tracker → Network Data Switches** and select **Create.**



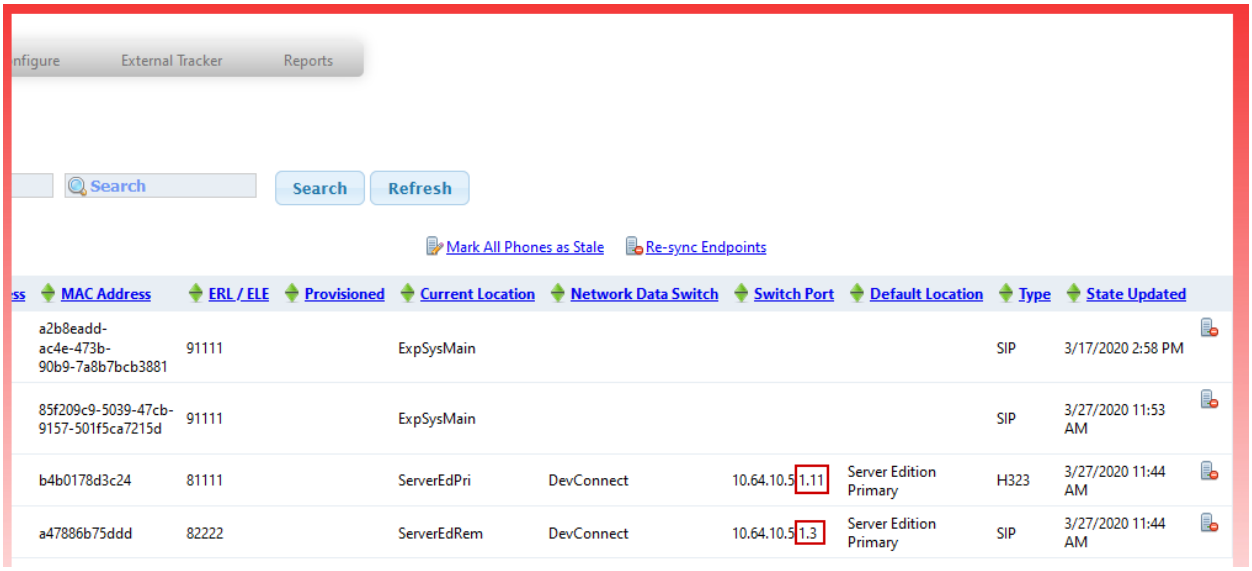
Screen capture below shows the network switch configured during the compliance test. Configure the Network Data Switch as follows:

- **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

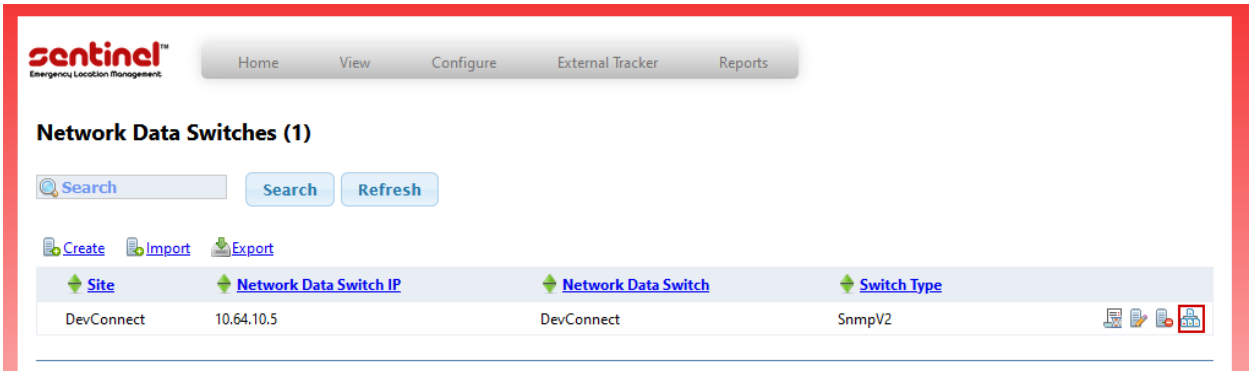
Depending on the SNMP version, fill the remaining fields as per the network switch configuration. SNMPv2c was used during the compliance test. Select **Submit** once done.



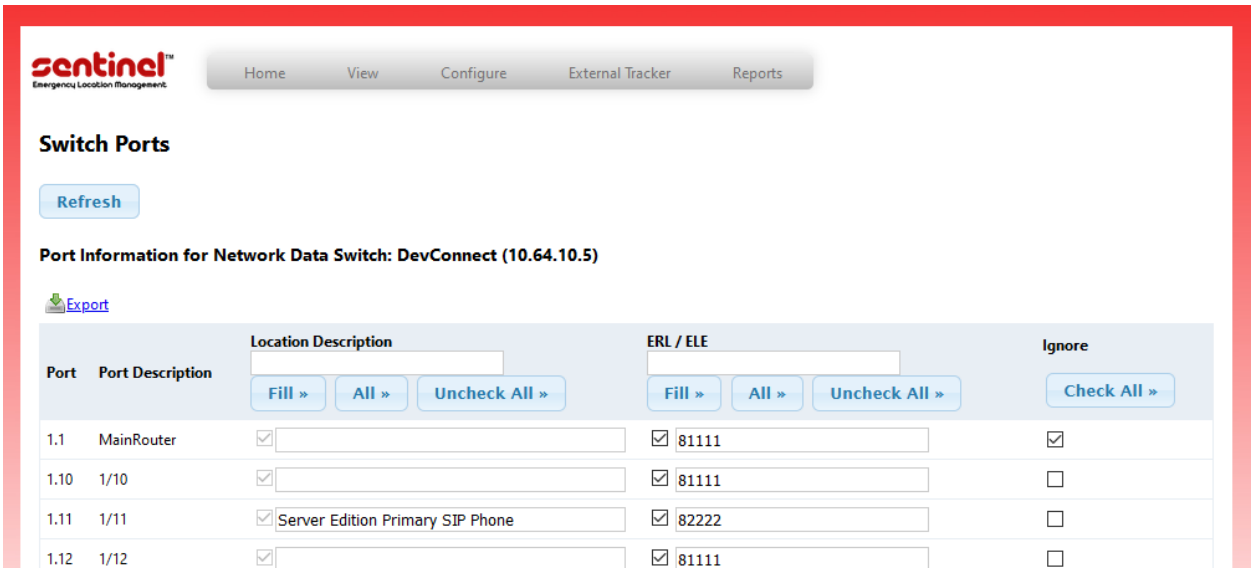
Once the Network Data Switch has been added, navigate to **View → IP Phones.** H.323 and SIP Phones connected to the network switch should display the ports these phones are connected to. Note that this can take a few minutes depending on the Polling frequency.



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.

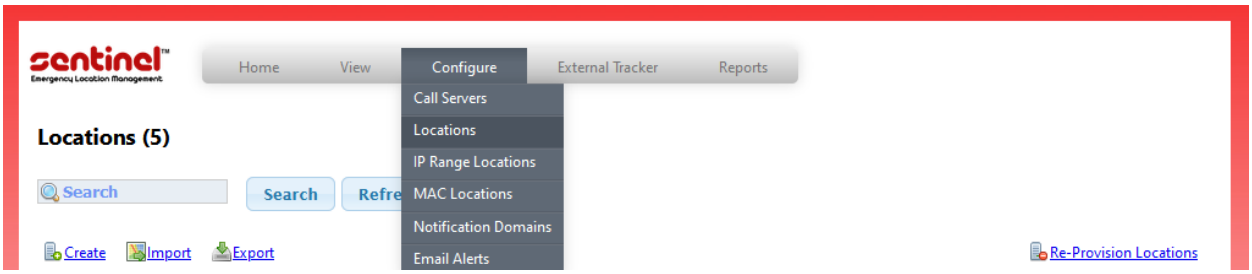


8. Verification Steps

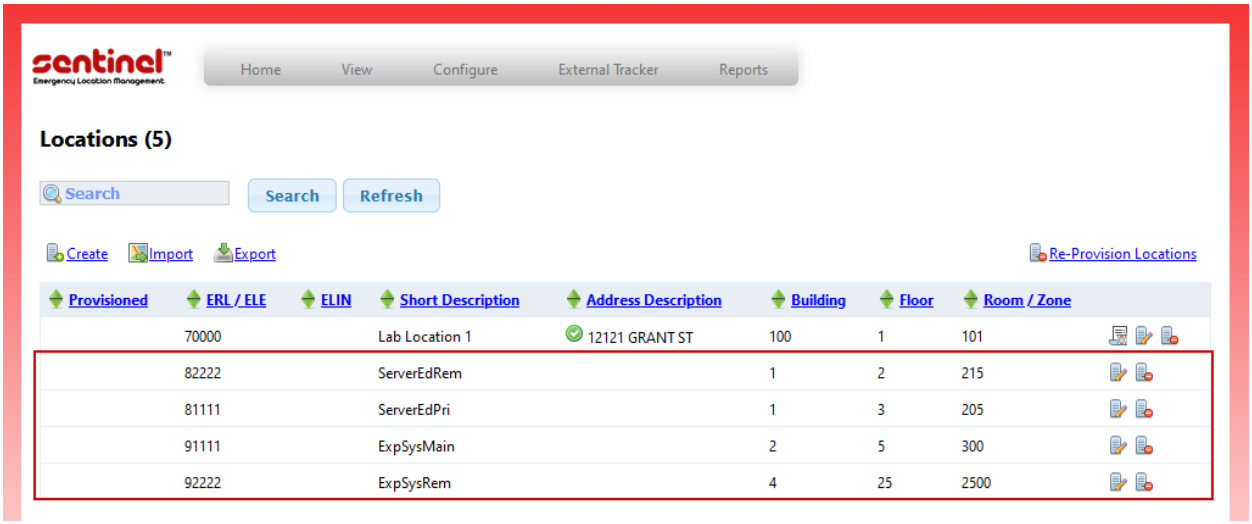
This section includes some steps that can be followed to verify the configuration.

8.1. Verify Locations

Once the Sentry server connects to IP Office via the Location API, verify if all the locations configured in IP Office using the required format of **"**Name###ERL" (e.g. ServerEdPri###81111) are seen in the Sentry server. To verify locations, from the main window of Sentinel web page, navigate to **Configure → Locations** as shown below.

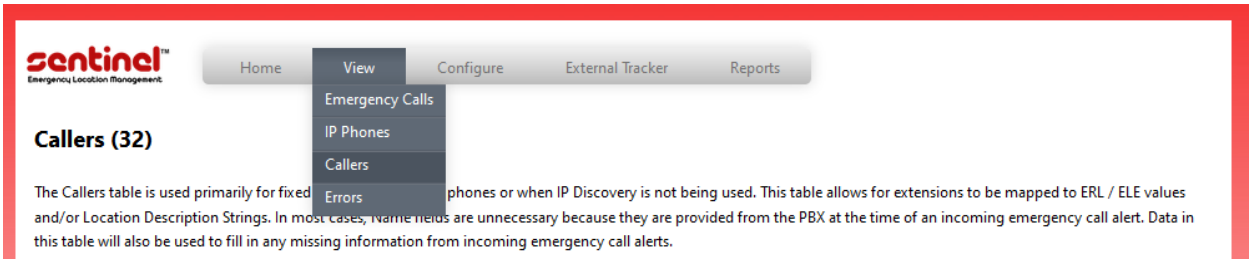


The **Locations** window shows all the locations that were configured in IP Office and now present in Sentry server as seen below.

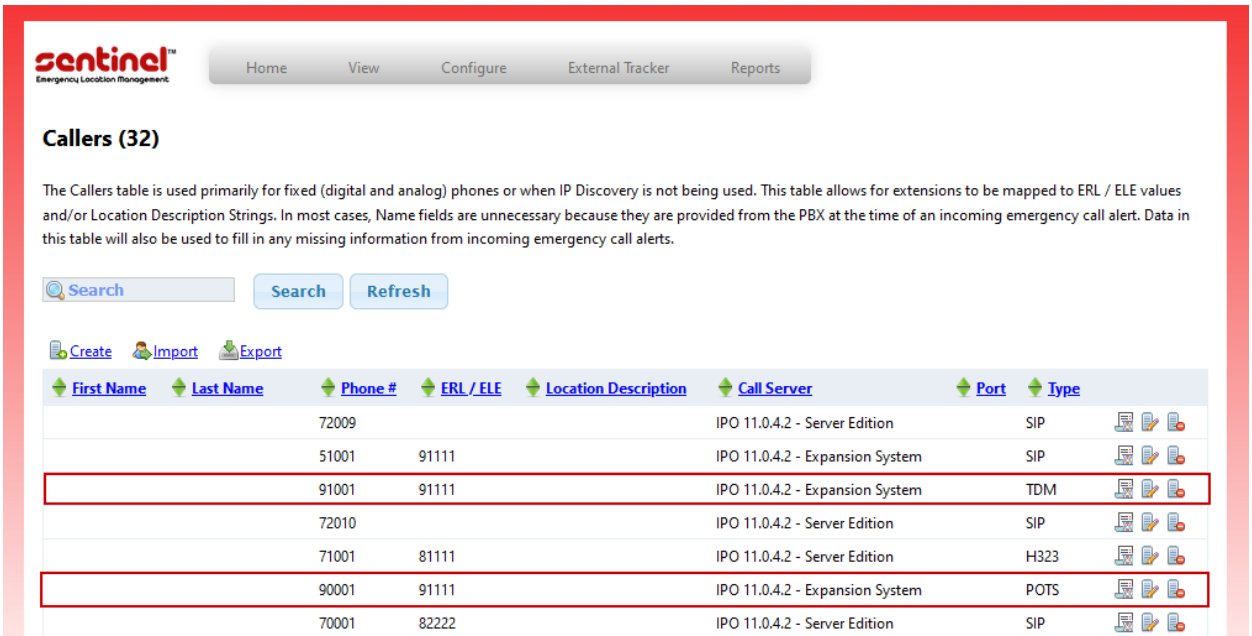


8.2. Verify Digital and Analog Extensions

Once the Sentry server connects to IP Office via the Location API, verify if all the digital and analog extensions connected on the IP Office are seen in the Sentry server. To verify these extensions, from the main window of Sentinel web page, navigate to **View → Callers** as shown below.

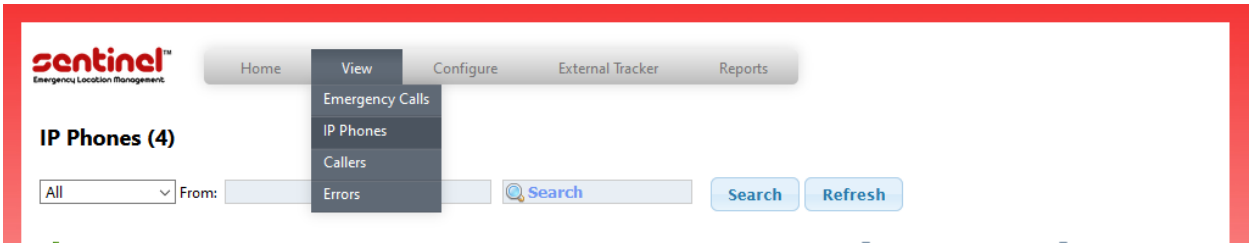


The **Callers** window shows all the digital and analog extensions that are connected on the IP Office and now present in Sentry server as seen below.

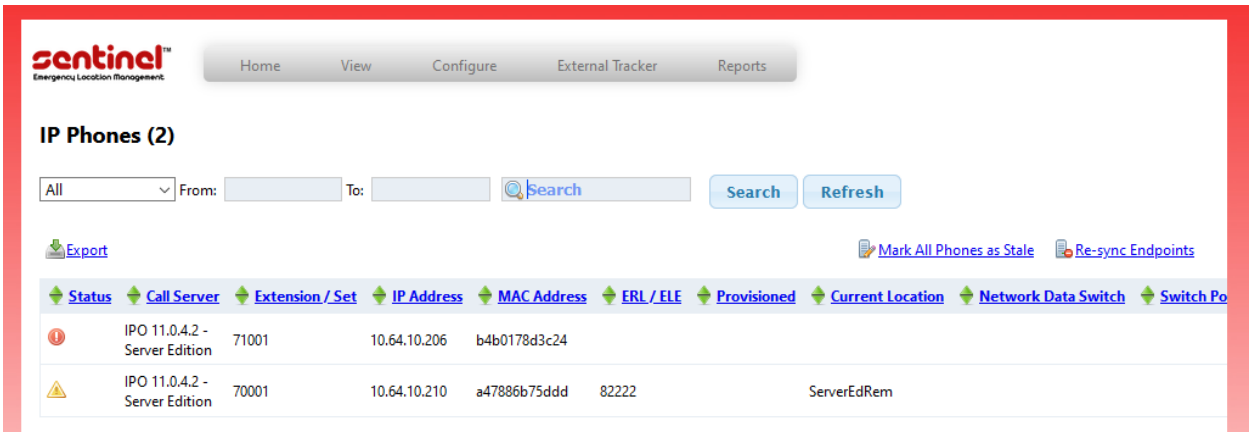


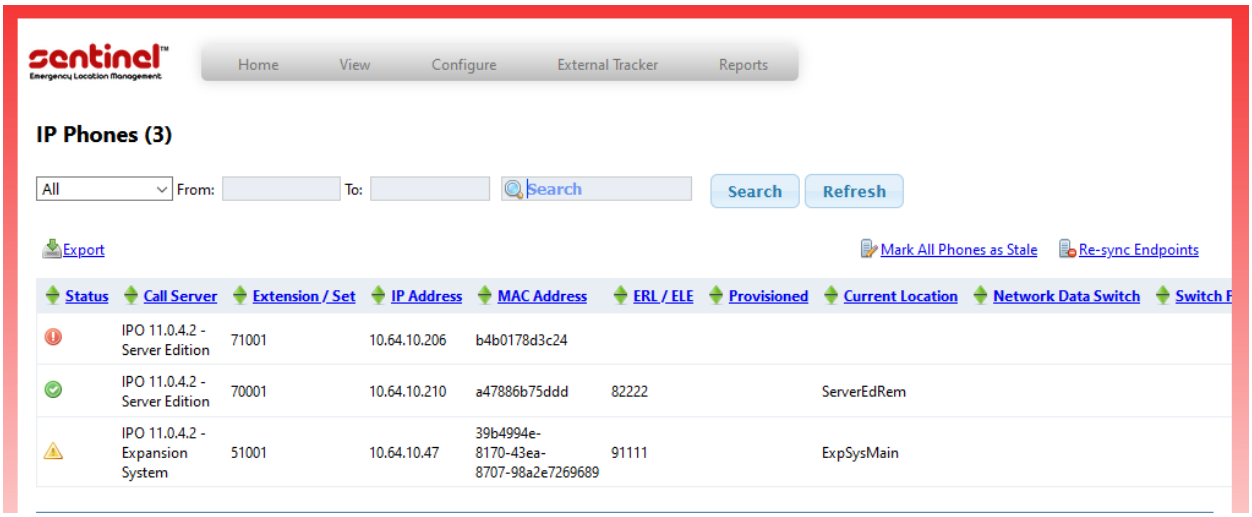
8.3. Verify IP Phone Extensions

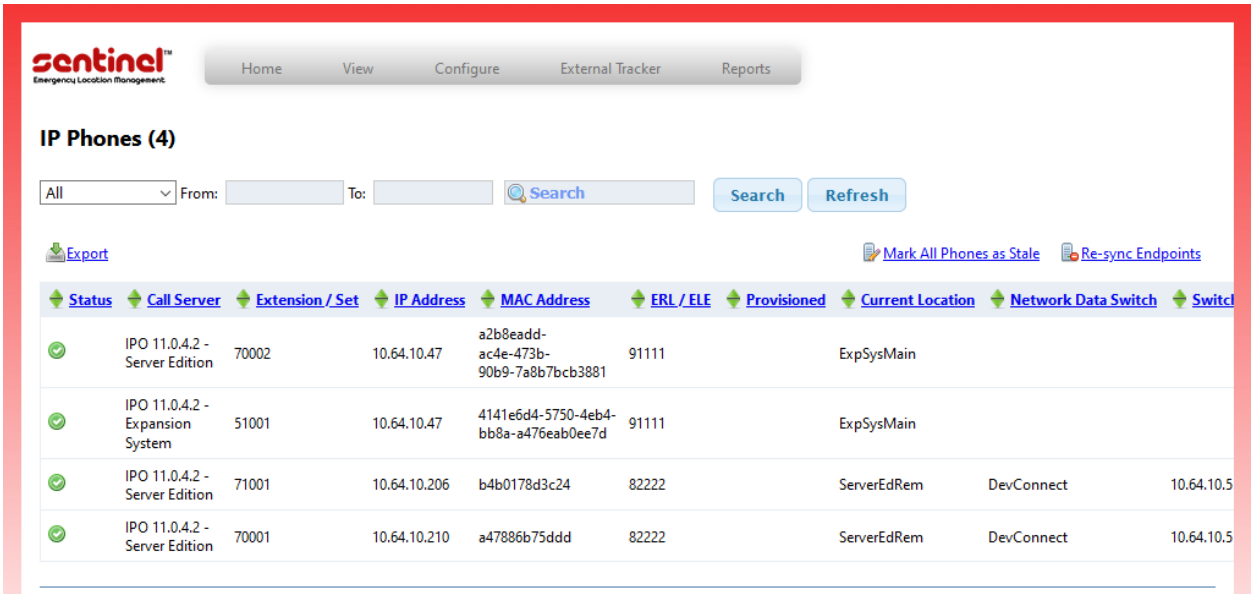
Once the Sentry server connects to IP Office via the Location API, verify if all the IP Phones extensions registered to the IP Office are seen in the Sentry server. To verify these extensions, from the main window of Sentinel web page, navigate to **View → IP Phones** as shown below.



The **IP Phones** window shows the IP phones that are currently registered to IP Office or that were registered at some point. A registered IP phone status changes from " Not Found" (red icon) to "Stale" (amber icon) to "Located" (green icon) as shown in the three screens below when it has been discovered. As the phones are discovered, the phones are shown and Status is updated.

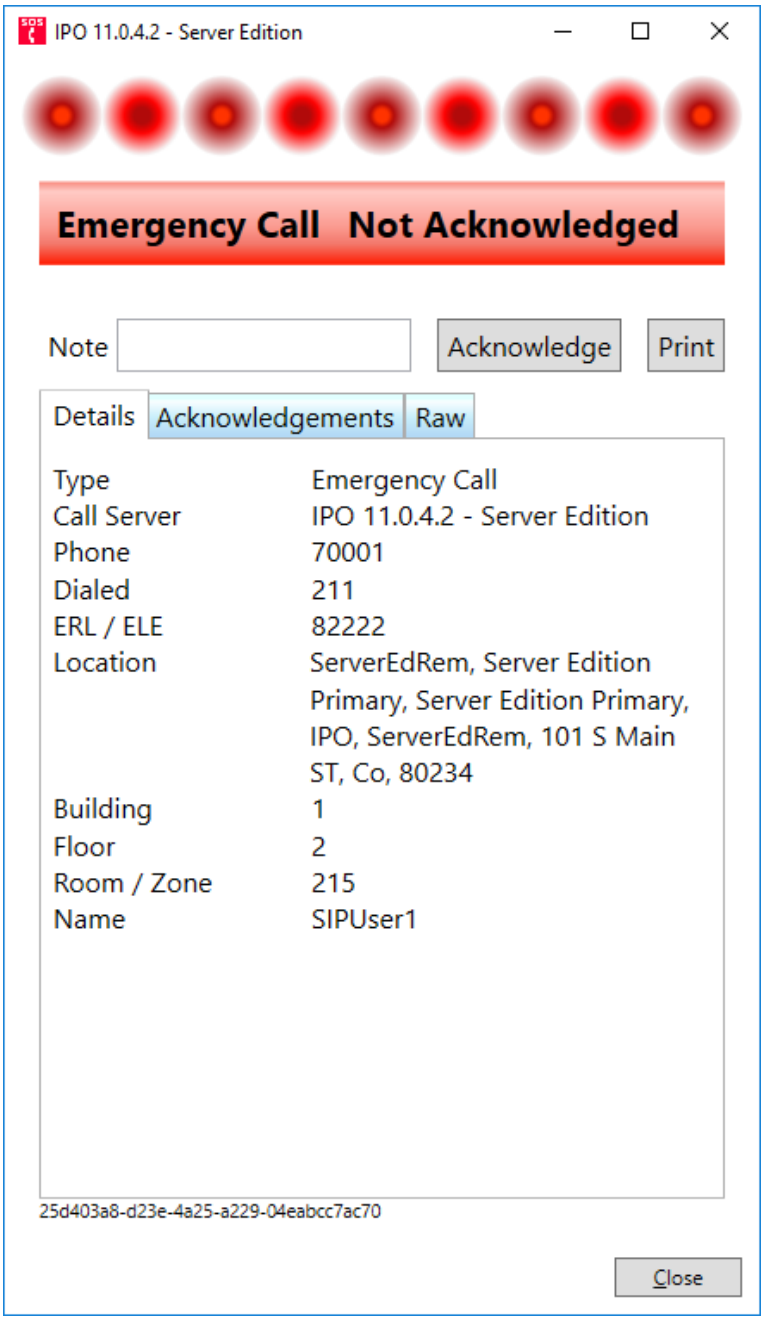






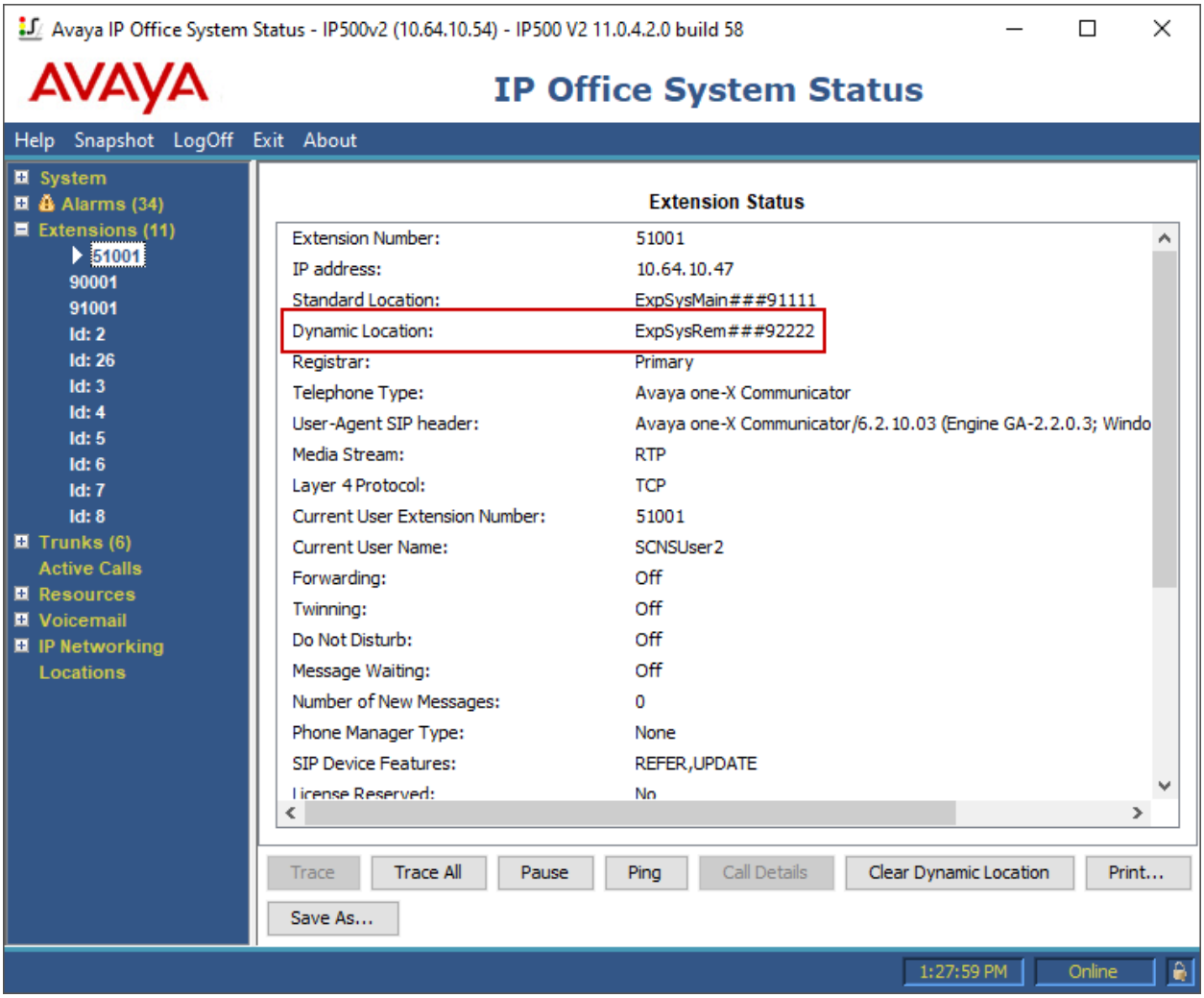
8.4. Verify On-site Alert Notification

Place an emergency call. Verify the Sentry Beacon pops an Alert window such as the one shown below. Verify the data in each of the tabs.



8.5. Verify Dynamic Locations

Each extension configured on IP Office can be assigned a dynamic location, regardless of what is configured on IP Office. Dynamic Location is a location that is other than what is configured in IP Office and is updated by Sentry using the Location API. ERL/ELE associated with IP Range Location or External Tracker Network Data Switches configuration. Using the **System Status** application of IP Office, this can be verified by expanding **Extensions** and selecting an extension.



To verify that IP Office is using this Location when an Emergency calls is placed, place an emergency call from this extension. The Emergency ARS assigned to the Location should get invoked and the calling party number assigned to the Emergency ARS short code should replace the caller's extension number. This can be verified via the IP Office **System Monitor** application. The log below shows the call placed for the extension above.

```
2020-03-27T13:33:32  333660279mS PRN: EMERGENCY CALL from originator with dynamic
location id 5
2020-03-27T13:33:32  333660283mS PRN: EMERGENCY CALL from originator with dynamic
location id 5
2020-03-27T13:33:32  333660285mS SNMPTrapGen: Emergency call!
Location:"ExpSysRem###92222" Dialled:211 Called:211 CallerID:92222
Usr:51001:"SCNSUser2" Extn:51001:8001:SIP:0A400A2F:000000000000
2020-03-27T13:33:32  333660286mS PRN: Setting configured voice gain for ch 5.
2020-03-27T13:33:32  333660286mS T1DSP:     PRIU DSP 2: channel 5 (timeslot 10),
restore gains tx 10, rx 10
```

9. Conclusion

The 911 Secure LLC Sentry NG911 Emergency Location Management Solution passed compliance testing. These Application Notes describe the procedures required for the 911 Secure LLC Sentry NG911 Emergency Location Management Solution to interoperate with Avaya IP Office Server Edition to support the reference configuration shown in **Figure 1**. Refer to **Section 2.2** for testing result details and any observations noted during testing.

10. Additional References

This section references the Avaya documentation relevant to these Application Notes. The following Avaya product documentation is available at http://support.avaya.com.

1. *Deploying Avaya IP Office Servers as Virtual Machines - 15-601011 Issue 06i - (Thursday, April 25, 2019)*
2. *Administering Avaya IP Office™ Platform with Manager,* Release 11.0, February 2019.
3. *Deploying IP Office Essential Edition (IP500 V2) - 15-601042 Issue 35f - (Monday, January 6, 2020)*

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

4. *Sentry and Avaya IP Office 10+: Setting up Notification Only and IP Discovery-Based Solutions for NG911 Revision 01/08/20*

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.