



## **Application Notes for DuVoice Emergency Alert System 7.0 with Avaya IP Office Server Edition 11.1 – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for DuVoice Emergency Alert System 7.0 to interoperate with Avaya IP Office Server Edition 11.1. DuVoice Emergency Alert System is an emergency notification application.

In the compliance testing, DuVoice Emergency Alert System used the SNMP and SIP User interfaces from Avaya IP Office to provide monitoring and notification of emergency calls.

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

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

# 1. Introduction

These Application Notes describe the configuration steps required for DuVoice Emergency Alert System (EAS) 7.0 to interoperate with Avaya IP Office Server Edition 11.1. EAS is an emergency notification application.

In the compliance testing, EAS used the SNMP and SIP User interfaces from IP Office to provide monitoring and notification of emergency calls.

The SNMP interface was used by EAS to monitor initiation of emergency calls by users on IP Office. In the compliance testing, 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) trunk. Both IP Office systems were configured to generate emergency call alarms and send corresponding SNMP traps to EAS when emergency calls are attempted by IP Office users. Upon informed of an emergency call attempt via SNMP trap, EAS sends notifications to configured call, email, and SMS alert destinations. The notifications included the caller ID of the emergency call originator and the dialed emergency number that were obtained from the SNMP trap.

The SIP User interface was used by EAS to notify call alert destinations of emergency calls. Upon connection with a call alert destination, EAS played voice announcement informing of the emergency call. The SIP connection between EAS and IP Office can be with either the primary or the expansion IP Office system. In the compliance testing, two virtual SIP users were configured and registered to the primary IP Office system.

Note that EAS is a standalone application from the DuVoice DV2000 solution, and as such there are references to DV2000 in various sections of these Application Notes.

## 2. General Test Approach and Test Results

The feature test cases were performed manually. Emergency calls were placed manually from various IP Office users on both IP Office systems to the simulated PSTN.

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

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 SIP User interface between IP Office and EAS did not include use of any specific encryption feature as requested by DuVoice.

### 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on EAS:

- Proper SIP exchanges including registration, media shuffling/non-shuffling, G.711, codec negotiation, and transfer with REFER.
- Proper handling of emergency call scenarios involving originators from both IP Office systems, call alert destinations on both IP Office systems, unsuccessful notifications, transfer of call alert destination to emergency call originator, simultaneous emergency calls, and simultaneous notifications.

The serviceability testing focused on verifying the ability of EAS to recover from adverse conditions, such as disconnecting and reconnecting the Ethernet connection to EAS.

## 2.2. Test Results

All test cases were executed and verified. The following were observations on EAS from the compliance testing.

- By design, the EAS report only logs the attempted call, email, and SMS notifications without indication of delivery results.
- By design, EAS does not use the location nor any failure cause from the SNMP trap and therefore not included in the notifications and EAS report.
- By design, EAS reports the name of the emergency call originator from the SNMP trap in the email notification, and not in the call and SMS notifications.
- In the case that a call notification covered to the alert destination's voicemail on IP Office, no voice message was left by EAS. DuVoice shared that this will be addressed in a future EAS release.
- When an emergency call originated from one IP Office system and routed to the PSTN over the other IP Office system, EAS received one SNMP trap with user as type from the originating IP Office system and one SNMP trap with trunk as type from the routing IP Office system. In this case, EAS reported two sets of notifications – one set of notification for each received SNMP trap.

## 2.3. Support

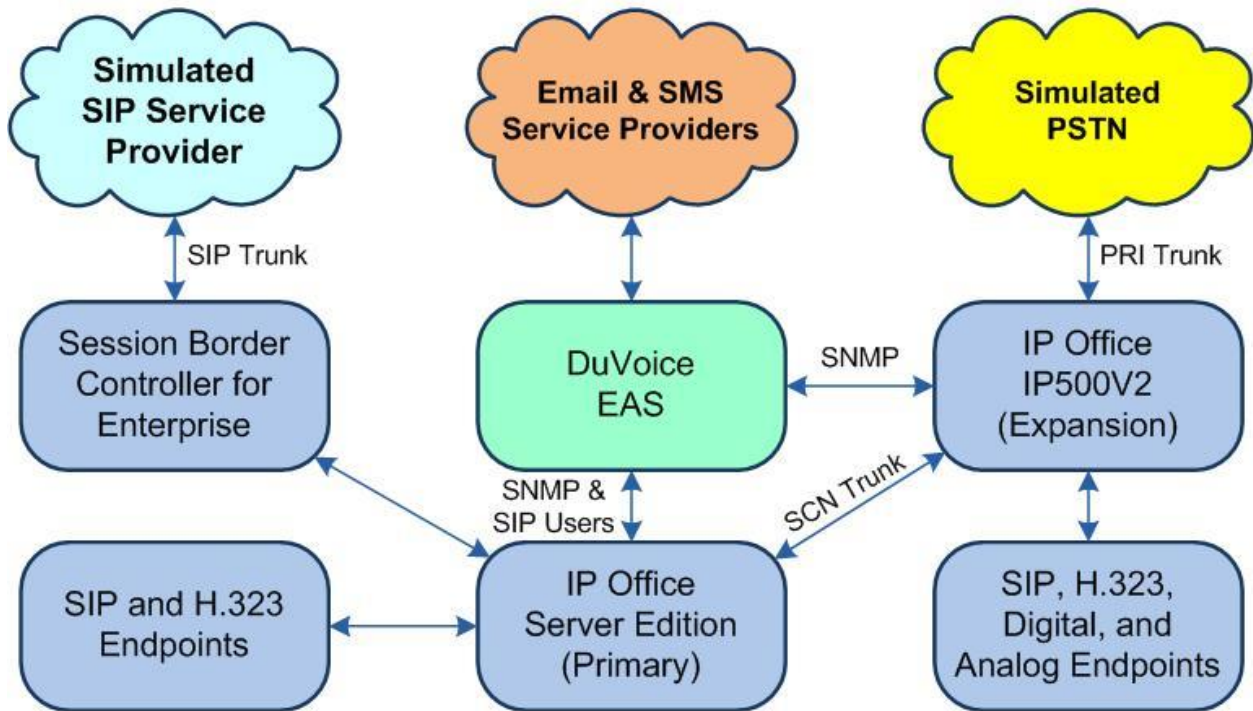
Technical support on EAS can be obtained through the following:

- **Phone:** (425) 250-2393
- **Email:** [support@duvoice.com](mailto:support@duvoice.com)

### 3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. Each IP Office system has connectivity to the simulated PSTN, for testing of cross system PSTN scenarios.

The EAS server used in the testing included the Dialogic Host Media Processing Software for support of the SIP protocol.



**Figure 1: Compliance Testing Configuration**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya IP Office Server Edition (Primary) in Virtual Environment	11.1.0.0.0
Avaya IP Office on IP500V2 (Expansion)	11.1.0.0.0
Avaya 1120E IP Deskphone (SIP)	4.4.23.0
Avaya J129 IP Deskphone (SIP)	4.0.4.0.10
Avaya 1608-I IP Deskphone (H.323)	1.3120
Avaya 9611G IP Deskphone (H.323)	6.8202
Avaya 1408 Deskphone (Digital)	48.02
2500YMGK Analog Phone	NA
DuVoice DV2000 on Microsoft Windows 10 Pro	7.0.10
• Dialogic PowerMedia HMP	3.0.395

*Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with IP Office Server Edition in all configurations.*

## 5. Configure Avaya IP Office

This section provides the procedures for configuring IP Office. The procedures include the following areas:

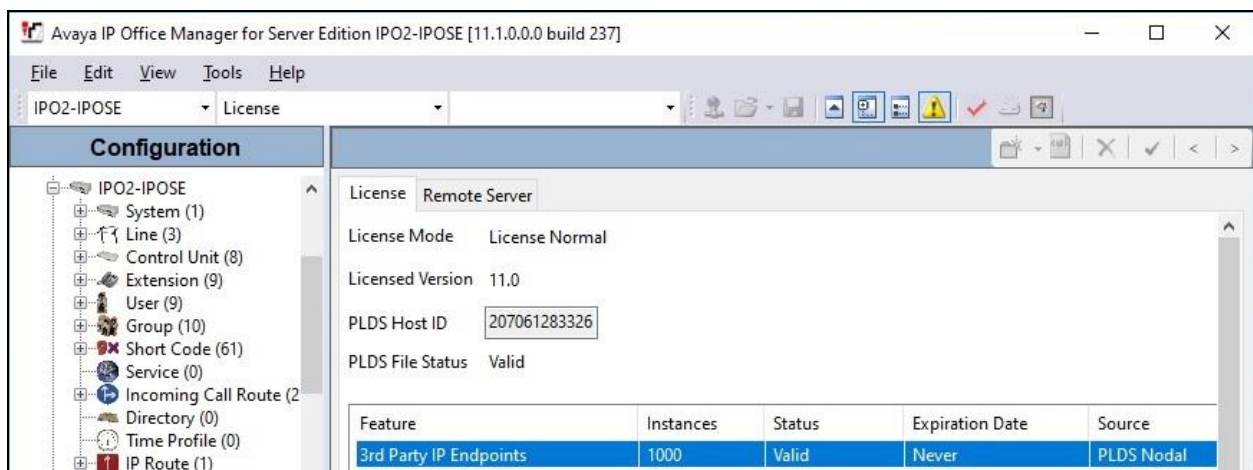
- Verify license
- Obtain LAN IP address
- Administer SIP Registrar
- Administer SNMP system events
- Administer SIP extensions
- Administer SIP users
- Administer common locations
- Administer extensions with location
- Administer emergency ARS
- Administer locations with emergency ARS
- Administer short codes

Note that the emergency call configuration presented in these Application Notes represents the sample used in the compliance test, and that the actual configuration can vary based on customer needs. For more information on emergency call configuration, see reference [2].

### 5.1. Verify License

From a PC running the IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the application. Select the proper primary IP Office system, and log in using the appropriate credentials. The **Avaya IP Office Manager for Server Edition IPO2-IPOSE** screen is displayed, where **IPO2-IPOSE** is the name of the primary IP Office system.

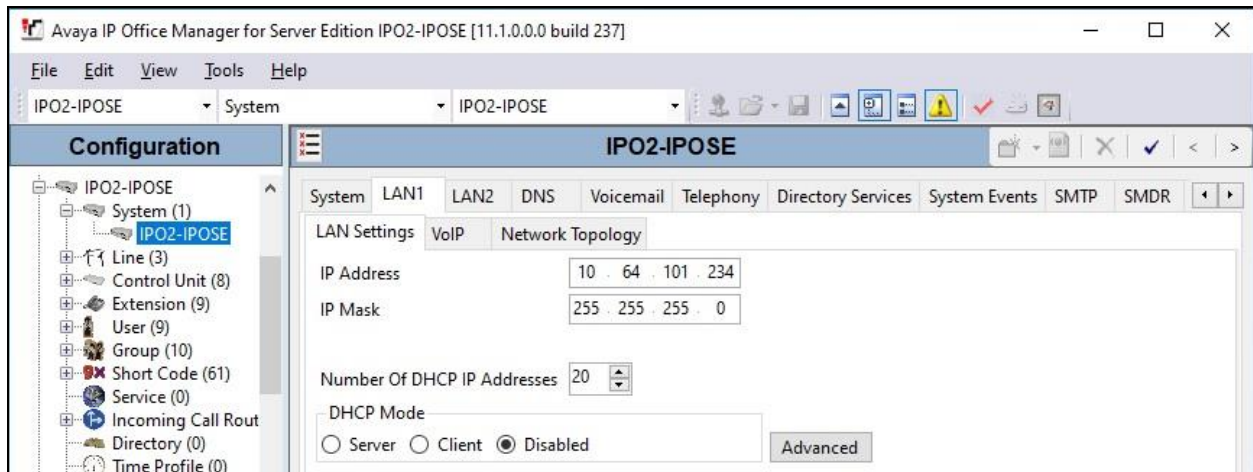
From the configuration tree in the left pane, select **License** (not shown) under the IP Office system that will be used for SIP user integration with EAS, in this case “IPO2-IPOSE”, a list of licenses is displayed in the right pane. Verify that there is sufficient license for **3<sup>rd</sup> Party IP Endpoints**, as shown below.



## 5.2. Obtain LAN IP Address

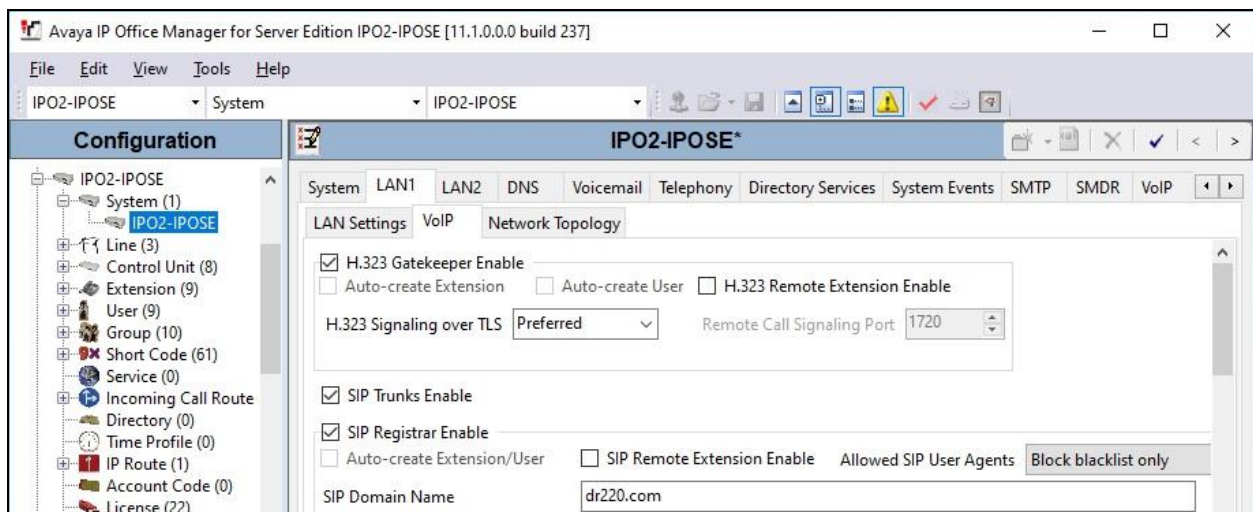
From the configuration tree in the left pane, select **System** under the IP Office system that will be used for SIP user integration with EAS, in this case “IPO2-IPOSE”. Select the **LAN1** tab, followed by the **LAN Settings** sub-tab in the right pane.

Make a note of the **IP Address**, which will be used later to configure EAS. Note that IP Office can support SIP on the LAN1 and/or LAN2 interfaces, and the compliance testing used the LAN1 interface.



## 5.3. Administer SIP Registrar

Select the **VoIP** sub-tab. Make certain that **SIP Registrar Enable** is checked, as shown below. Make a note of the **SIP Domain Name** field value, which will be used later to configure EAS.

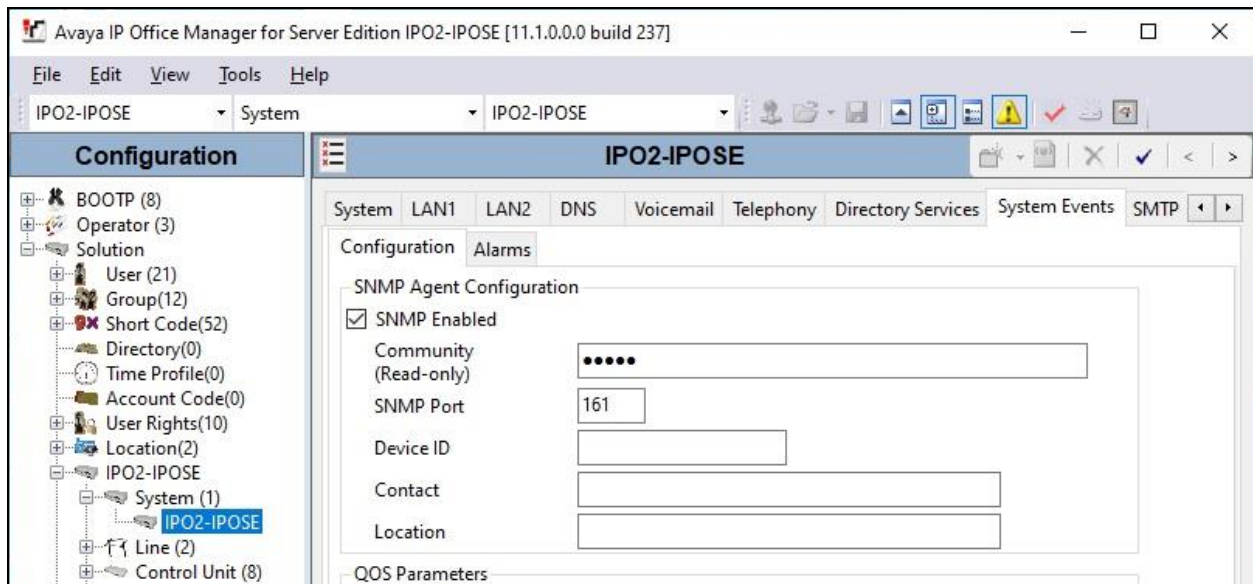




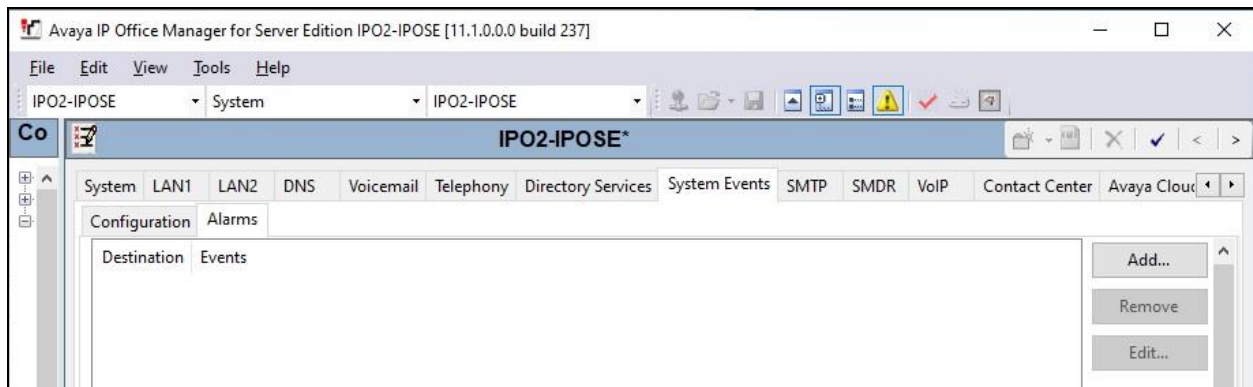
## 5.4. Administer SNMP System Events

Select the **System Events** tab, followed by the **Configuration** sub-tab.

Check **SNMP Enabled**, and enter a desired string for **Community**. Note that the community string is not used by EAS but required to be configured on IP Office for SNMP integration. Retain the default value in the remaining fields.



Select the **Alarms** sub-tab and click **Add**.



The screen is updated with new parameters, as shown below. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Trap:** Select this field.
- **Server Address:** The IP address of the EAS server.
- **Emergency Calls:** Check this field.

Note that the default value of “162” for **Port** must be retained, as required by EAS.

Avaya IP Office Manager for Server Edition IPO2-IPOSE [11.1.0.0.0 build 237]

File Edit View Tools Help

IPO2-IPOSE System IPO2-IPOSE

Co IPO2-IPOSE\*

System LAN1 LAN2 DNS Voicemail Telephony Directory Services System Events SMTP SMDR VoIP Contact Center Avaya Cloud

Configuration Alarms

Destination Events

Add... Remove Edit...

New Alarm

Destination:

☒ Trap ☐ Syslog ☐ Email

Server Address: 10.64.101.202

Port: 162

Community: \*\*\*\*\*

Format: IP Office

Minimum Severity Level: Warnings

OK Cancel

Events

Quality of Service

☐ QOS Monitoring

System

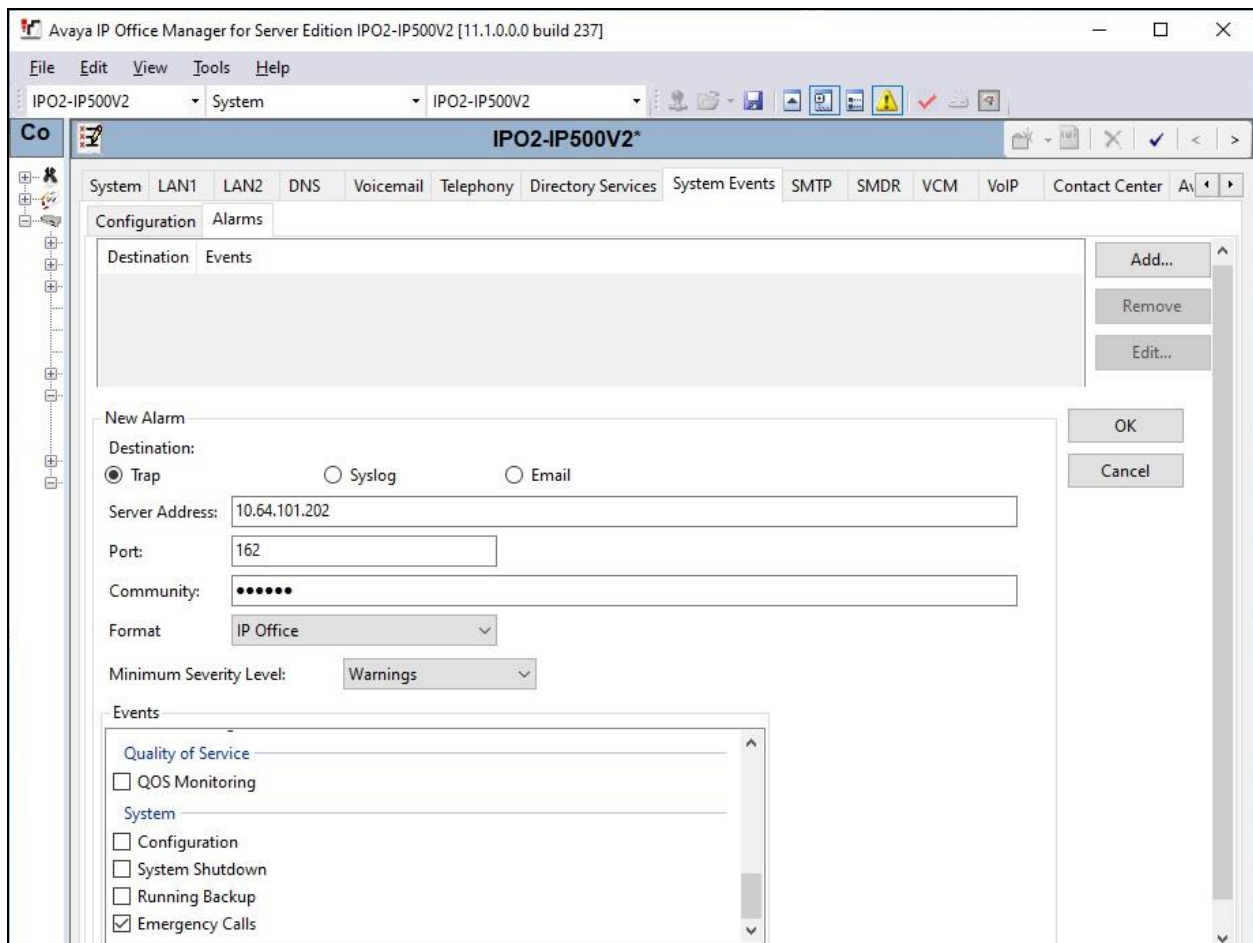
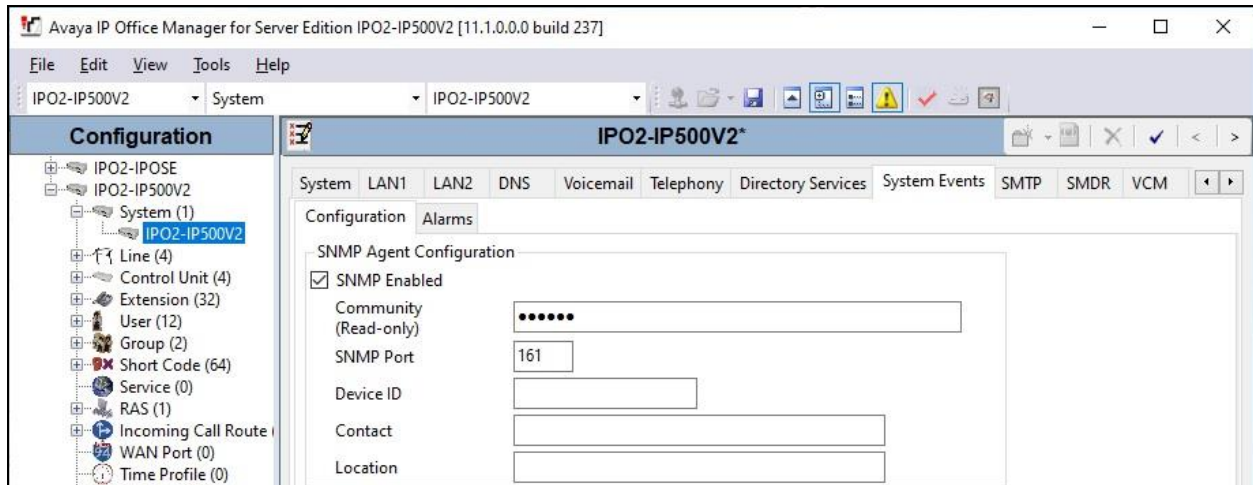
☐ Configuration

☐ System Shutdown

☐ Running Backup

☒ Emergency Calls

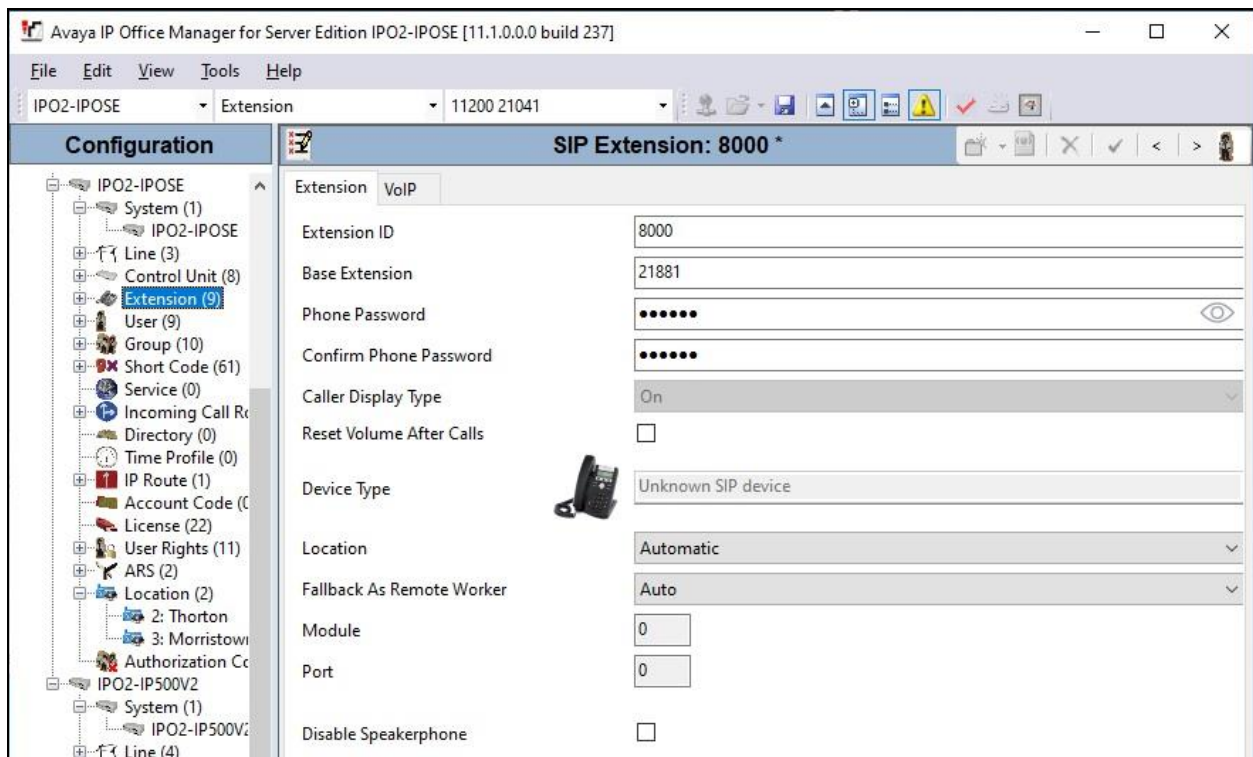
Repeat this section to enable SNMP and emergency calls alarm on the expansion IP Office system, as shown in screenshots below.



## 5.5. Administer SIP Extensions

From the configuration tree in the left pane, right-click on **Extension** under the IP Office system that will be used for SIP user integration with EAS, in this case “IPO2-IPOSE”, and select **New** → **SIP Extension** from the pop-up list to add a new SIP extension. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Base Extension:** Enter an available extension number, in this case “21881”.
- **Phone Password:** Enter a desired password.
- **Confirm Phone Password:** Enter the same desired password.



Avaya IP Office Manager for Server Edition IPO2-IPOSE [11.1.0.0.0 build 237]

File Edit View Tools Help

IPO2-IPOSE Extension 11200 21041

**Configuration** **SIP Extension: 8000 \***

Extension	VolP
Extension ID	8000
Base Extension	21881
Phone Password	.....
Confirm Phone Password	.....
Caller Display Type	On
Reset Volume After Calls	<input type="checkbox"/>
Device Type	Unknown SIP device
Location	Automatic
Fallback As Remote Worker	Auto
Module	0
Port	0
Disable Speakerphone	<input type="checkbox"/>

Select the **VoIP** tab. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Codec Selection:** “Custom”
- **Selected:** Retain only the applicable G.711 codec variant.
- **Reserve License:** “Reserve 3rd party IP endpoint license”
- **Media Security:** “Disabled”

Repeat this section to add the desired number of SIP extensions. In the compliance testing, two SIP extensions with base extensions of 21881-21882 were created.

The screenshot displays the Avaya IP Office Manager for Server Edition (IPO2-IPOSE) interface, version 11.1.0.0.0 build 237. The window title is "Avaya IP Office Manager for Server Edition IPO2-IPOSE [11.1.0.0.0 build 237]". The menu bar includes File, Edit, View, Tools, and Help. The toolbar shows various icons for file operations and system management. The main window is titled "SIP Extension: 8000 \*". The left sidebar shows a tree view with "Extension" and "VoIP" tabs. The "VoIP" tab is selected, showing the configuration for the SIP extension. The configuration fields are as follows:

- IP Address:** 0 . 0 . 0 . 0
- Codec Selection:** Custom
- Unused:** G.711 ALAW 64K, G.722 64K, G.729(a) 8K CS-ACELP
- Selected:** G.711 ULAW 64K
- Reserve License:** Reserve 3rd party IP endpoint license
- Fax Transport Support:** None
- DTMF Support:** RFC2833/RFC4733
- 3rd Party Auto Answer:** None
- Media Security:** Disabled
- Requires DTMF:** ☐
- Local Hold Music:** ☐
- Re-invite Supported:** ☒
- Codec Lockdown:** ☐
- Allow Direct Media Path:** ☒

## 5.6. Administer SIP Users

From the configuration tree in the left pane, right-click on **User** under the IP Office system that will be used for SIP user integration with EAS, in this case “IPO2-IPOSE”, and select **New** from the pop-up list to add a new user.

Enter desired values for **Name** and **Full Name**. For **Extension**, enter the first SIP base extension from **Section 5.5**. Retain the default values in the remaining fields.

The screenshot shows the Avaya IP Office Manager for Server Edition IPO2-IPOSE [11.1.0.0.0 build 237] window. The left pane shows the configuration tree with 'User (11)' selected. The right pane shows the configuration for a new user, '<User:0>: \*'. The 'User' tab is selected, and the following fields are visible:

Field	Value
Name	SIP-21881
Password	
Confirm Password	
Unique Identity	
Conference PIN	
Confirm Audio Conference PIN	
Account Status	Enabled
Full Name	EAS SIP1
Extension	21881

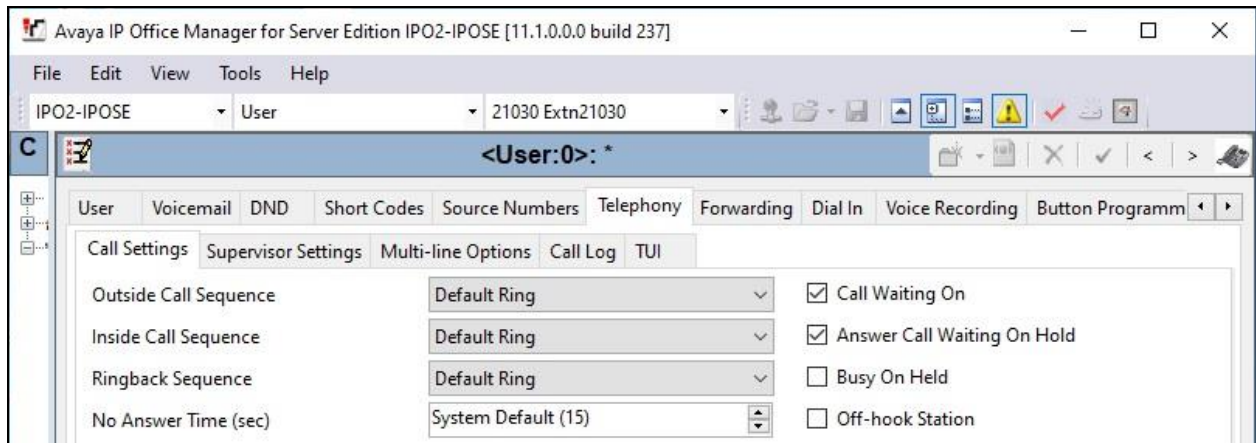
Select the **Voicemail** tab, and uncheck **Voicemail On**, as shown below.

The screenshot shows the Avaya IP Office Manager for Server Edition IPO2-IPOSE [11.1.0.0.0 build 237] window. The left pane shows the configuration tree with 'User (11)' selected. The right pane shows the configuration for a new user, '<User:0>: \*'. The 'Voicemail' tab is selected, and the following fields are visible:

Field	Value
Voicemail Code	
Confirm Voicemail Code	
Voicemail Email	
Voicemail On	<input type="checkbox"/>
Voicemail Help	<input type="checkbox"/>
Voicemail Ringback	<input type="checkbox"/>
Voicemail Email Reading	<input type="checkbox"/>
UMS Web Services	<input type="checkbox"/>
Enable GMAIL API	<input type="checkbox"/>

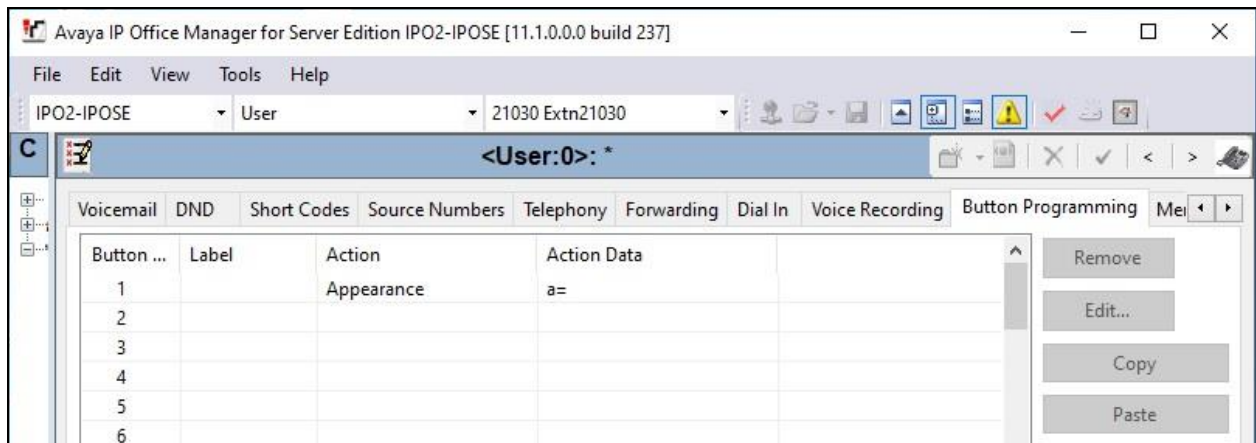


Select the **Telephony** tab, followed by the **Call Settings** sub-tab. Check **Call Waiting On**, as shown below. Retain the default values in the remaining fields.



Select the **Button Programming** tab. Retain only the first **Appearance** button and remove all others as shown below.

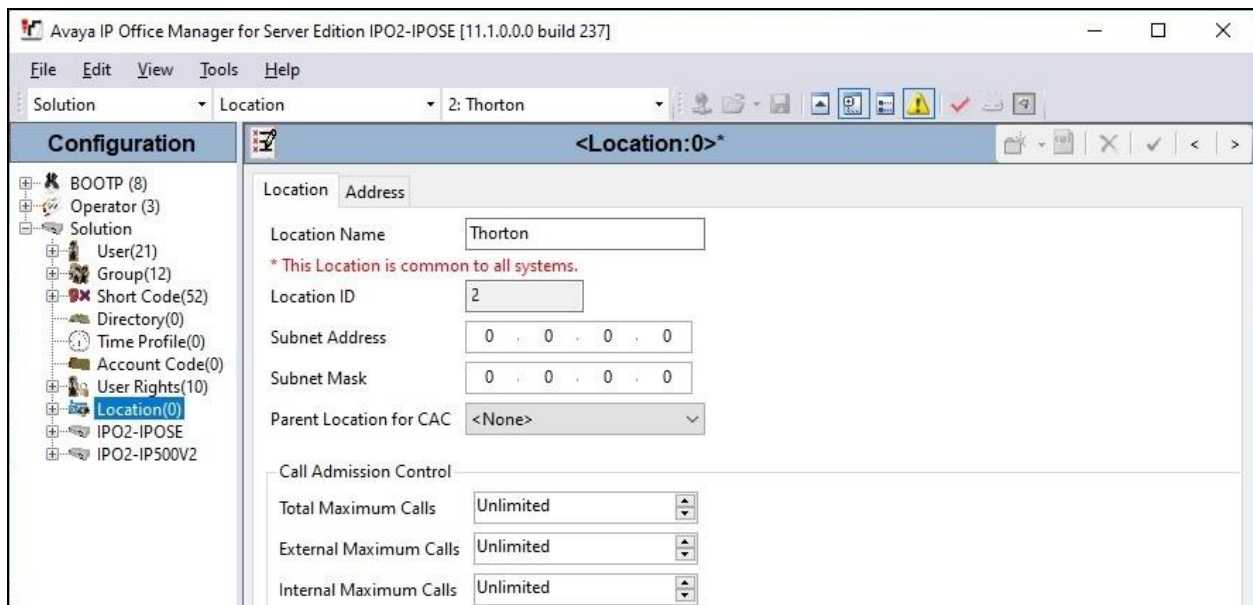
Repeat this section to add a new user for each SIP extension from **Section 5.5**. In the compliance testing, two users with names of “SIP-21881” and “SIP-21882” were created.



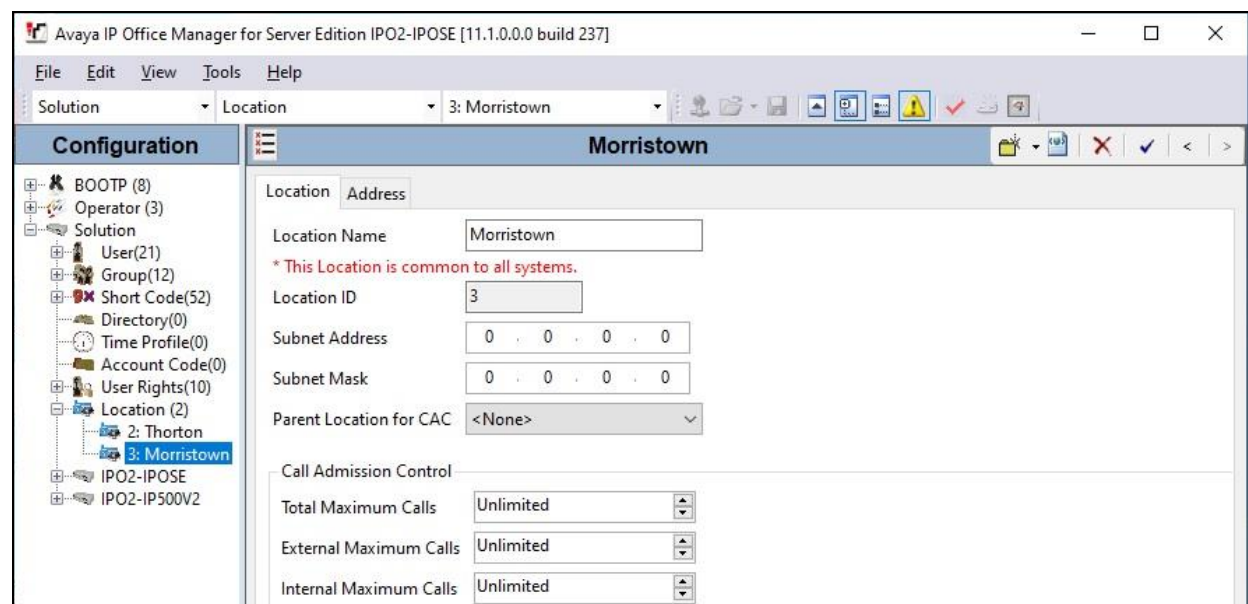
## 5.7. Administer Common Locations

From the configuration tree in the left pane, right-click on **Solution** → **Location**, and select **New** from the pop-up list to add a new common location.

For **Location Name**, enter a desired name for the primary IP Office system, in this case “Thorton”. Retain the default values in the remaining fields.



Repeat this section to add a common location for the expansion IP Office system, in this case “Morristown”. The left pane of the screenshot below shows the two common locations that were created.

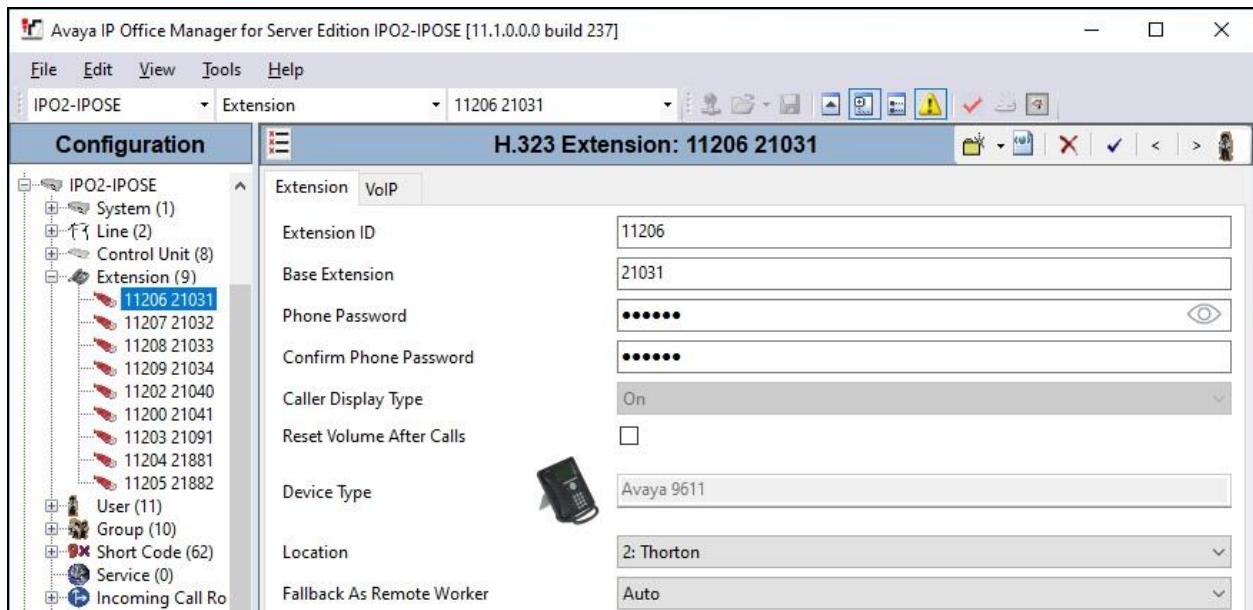




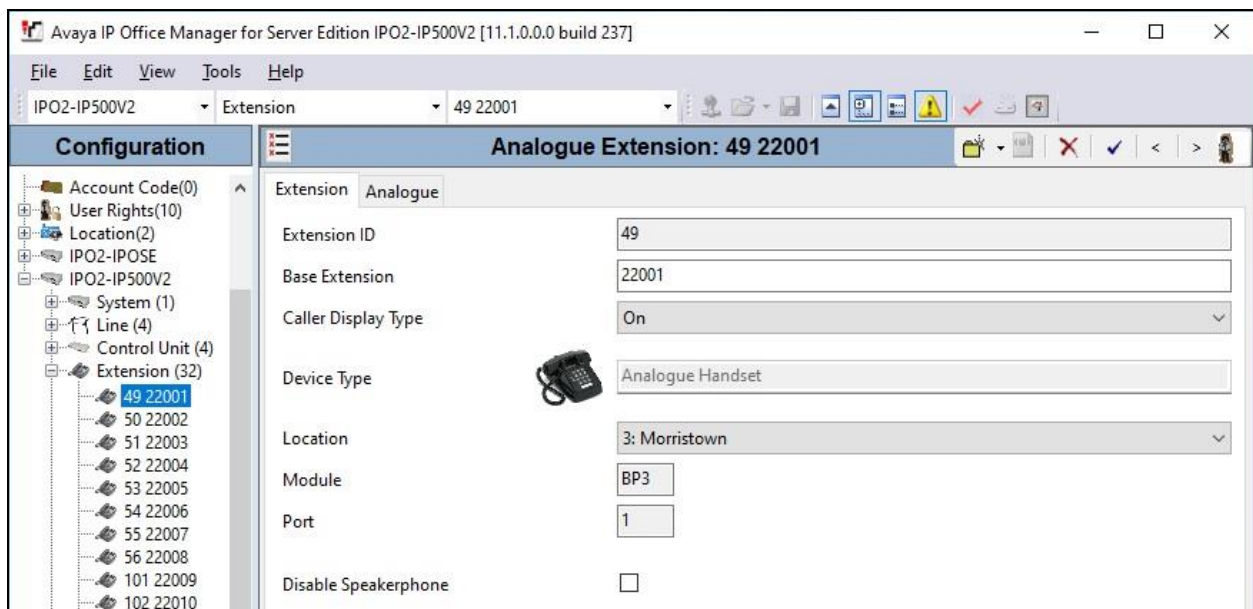
## 5.8. Administer Extensions with Location

From the configuration tree in the left pane, expand and select the first entry under **Solution** → **IPO2-IPOSE** → **Extension**, where **IPO2-IPOSE** is the name of the primary IP Office system.

For **Location**, select the location for the primary IP Office system from **Section 5.7**. Repeat the same location assignment for all extensions on the primary IP Office system.



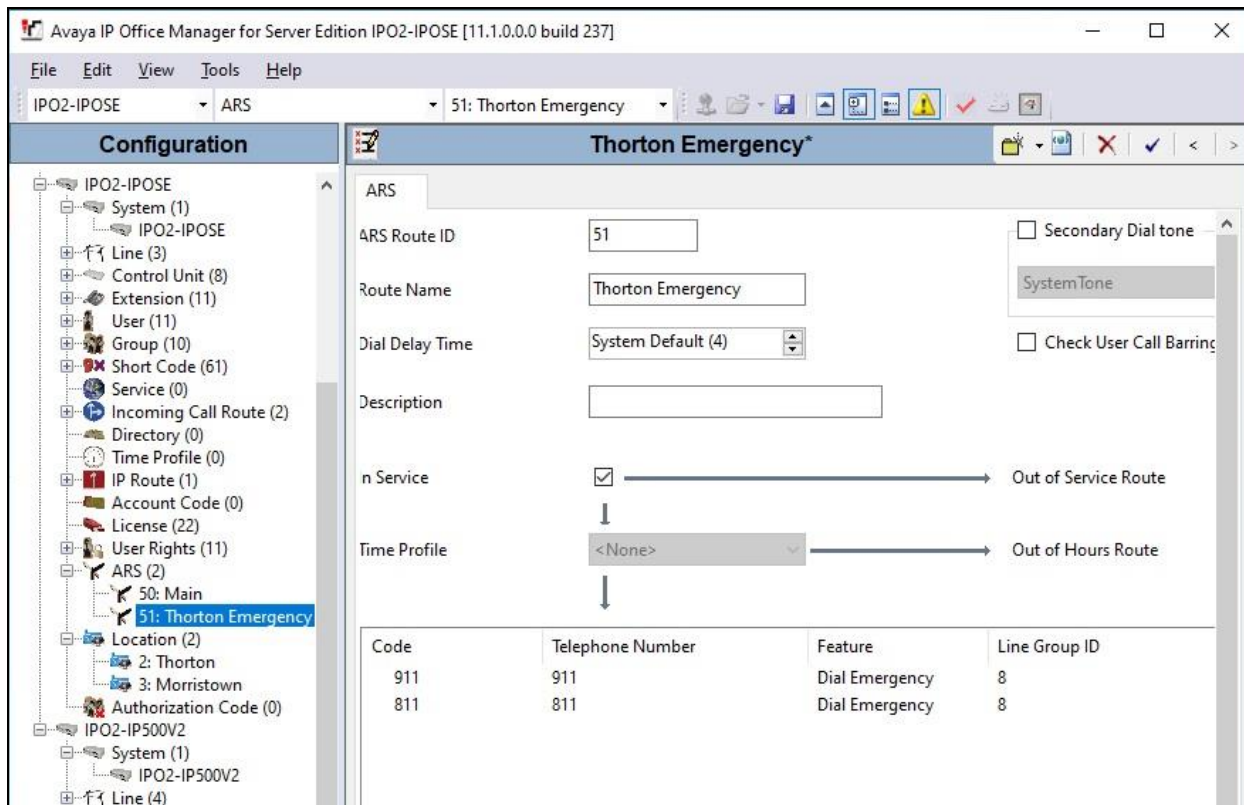
Repeat this section to assign the applicable location to all extensions on the expansion IP Office system, as shown below.



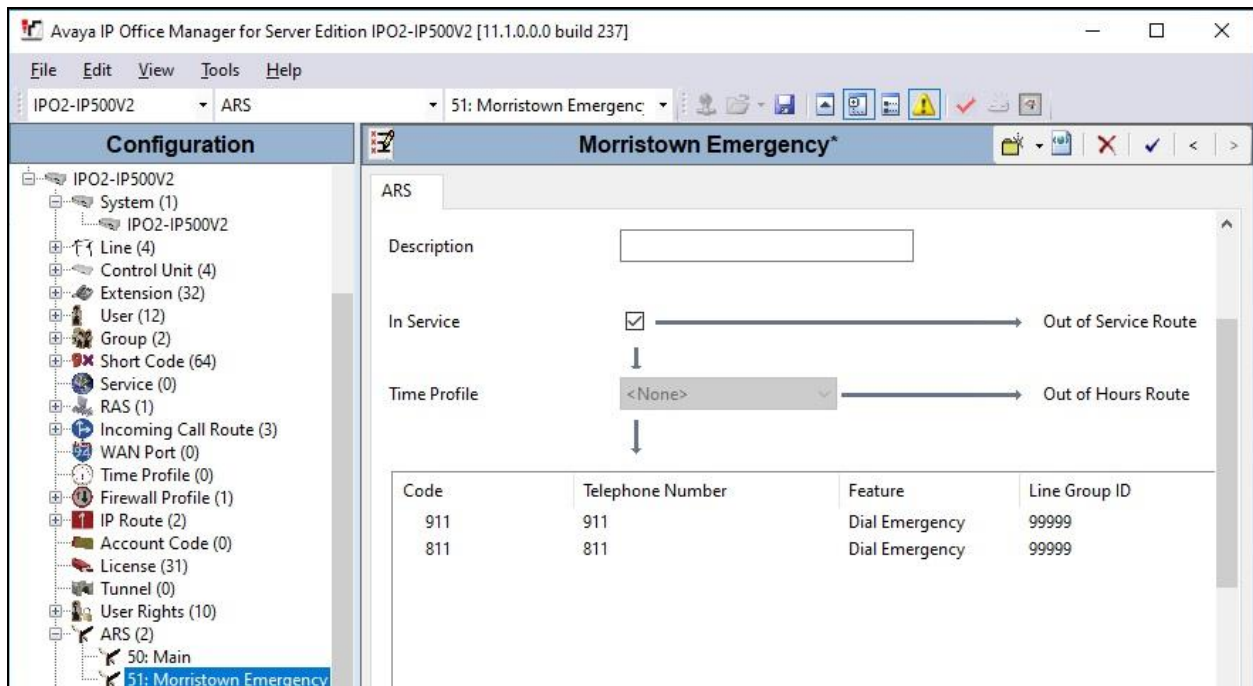
## 5.9. Administer Emergency ARS

From the configuration tree in the left pane, right-click on **Solution → IPO2-IPOSE → ARS**, where **IPO2-IPOSE** is the name of the primary IP Office system, and select **New** from pop-up list to add an ARS for routing of emergency calls, if not already in place.

The screenshot below shows the ARS added to the primary IP Office system for routing of emergency calls, where **Line Group ID 8** is an existing line for connection to the simulated PSTN.

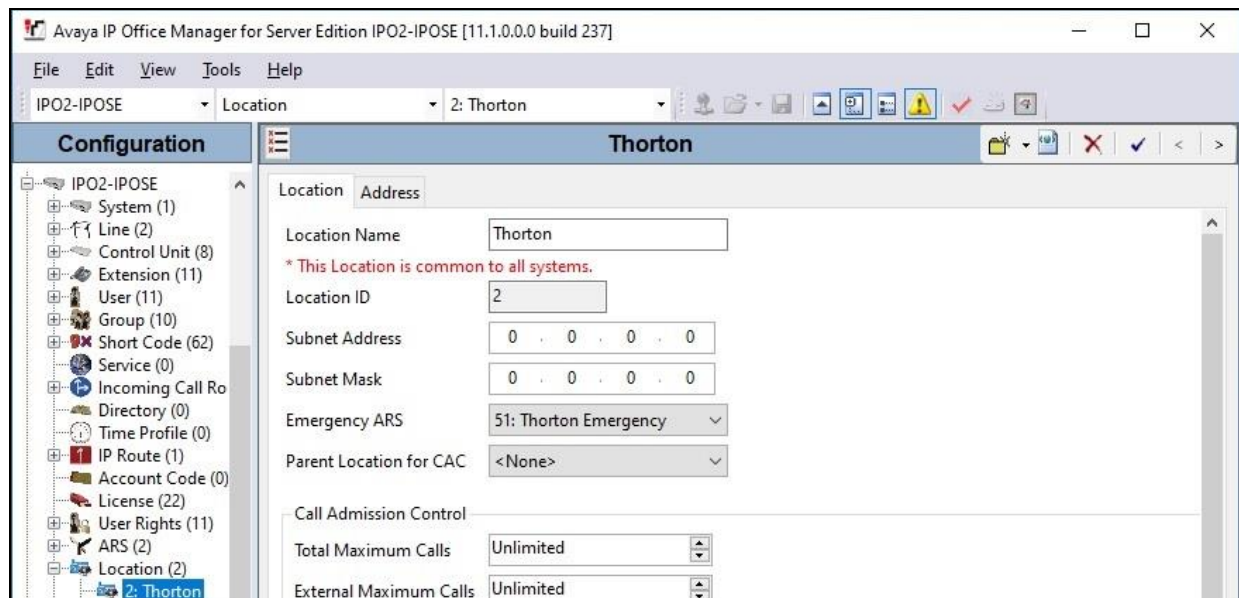


Repeat this section to add an ARS to the expansion IP Office system for routing of emergency calls. In the screenshot below, **Line Group ID 99999** is an existing SCN line to the primary IP Office system.

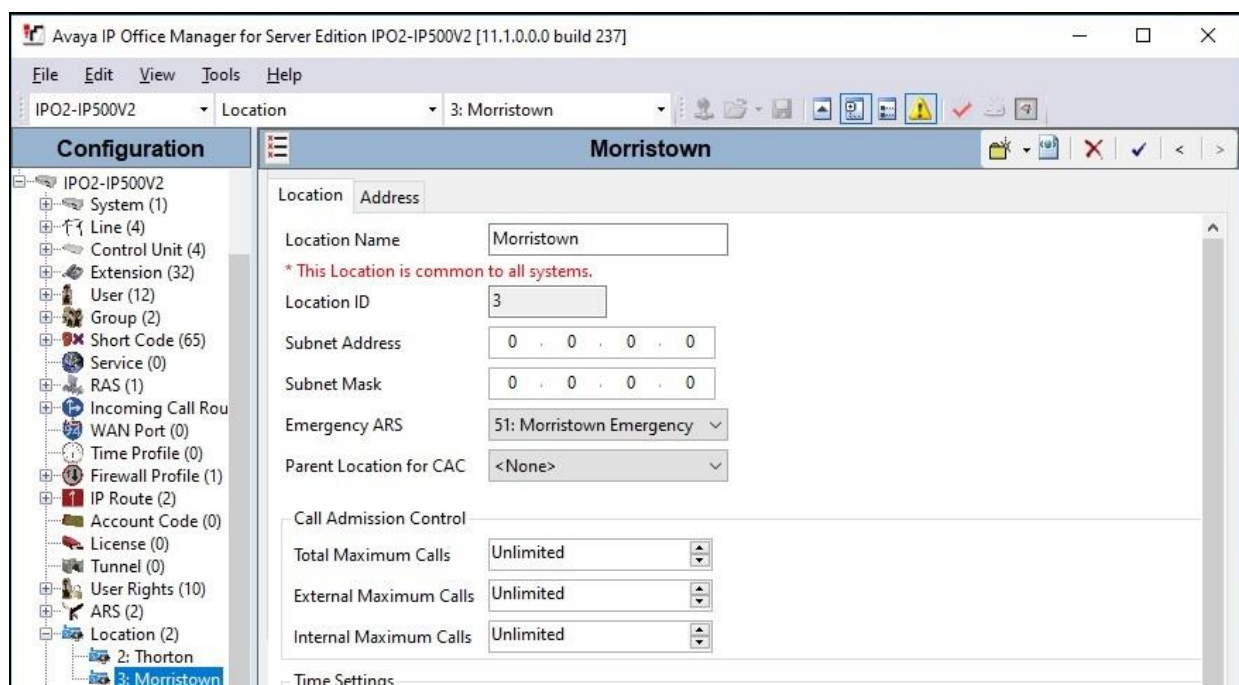


## 5.10. Administer Locations with Emergency ARS

From the configuration tree in the left pane, under **Solution → IPO2-IPOSE → Location**, expand and select the location associated with the primary IP Office system from **Section 5.7**, in this case **Thorton**. For **Emergency ARS**, select the ARS associated with routing of emergency calls for the primary IP Office system from **Section 5.9**, as shown below.



Repeat this section to administer the expansion IP Office system location with the appropriate ARS from **Section 5.9**, as shown below.

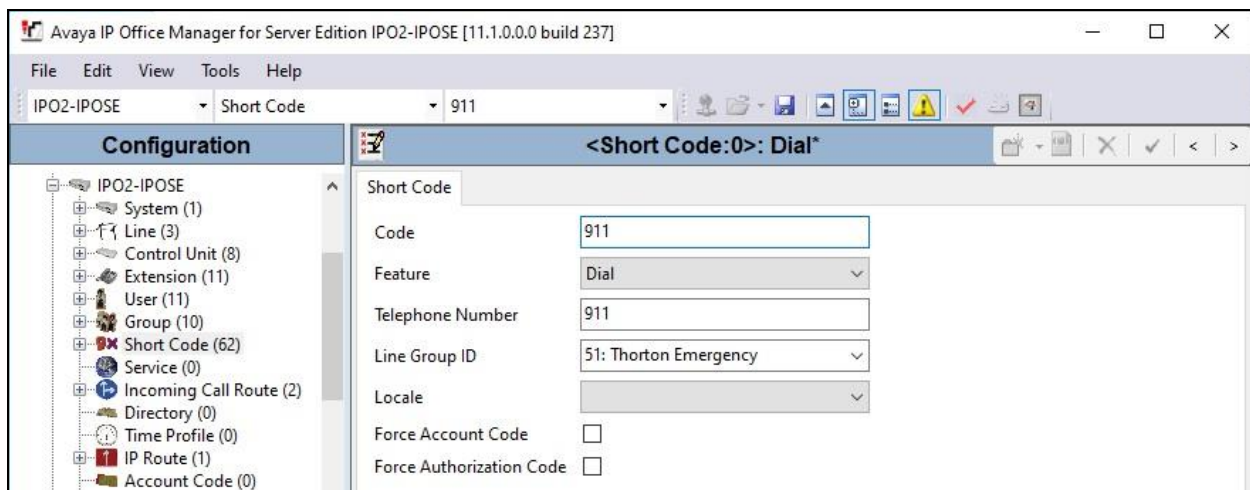


## 5.11. Administer Short Codes

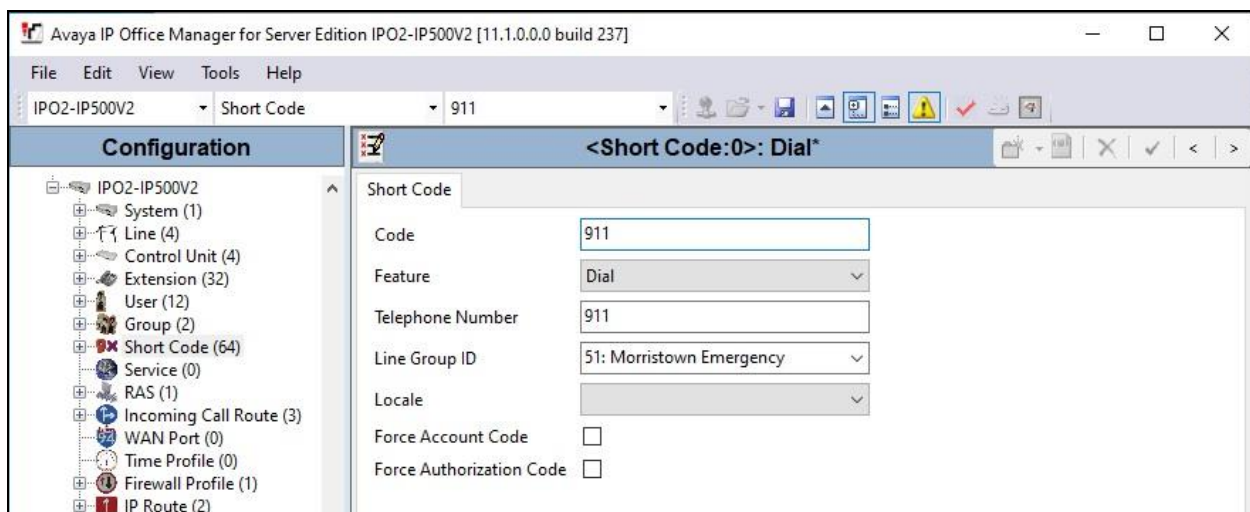
From the configuration tree in the left pane, right-click on **Solution → IPO2-IPOSE → Short Code**, where **IPO2-IPOSE** is the name of the primary IP Office system, and select **New** from pop-up list to add a short code for dialing and routing of emergency calls.

In the case that the short code already exists, then select the short code to make modifications. Enter the following values for the specified fields and retain the default values for the remaining fields. In the compliance testing, two short codes 911 and 811 were created.

- **Code:** Digits that will be dialed for emergency call, in this case “911”.
- **Feature:** “Dial”
- **Telephone Number:** Applicable number for proper routing of emergency call to PSTN.
- **Line Group ID:** The applicable ARS entry from **Section 5.9**.



Repeat this section to add or modify similar short codes for routing of emergency calls for the expansion IP Office system, as shown below.





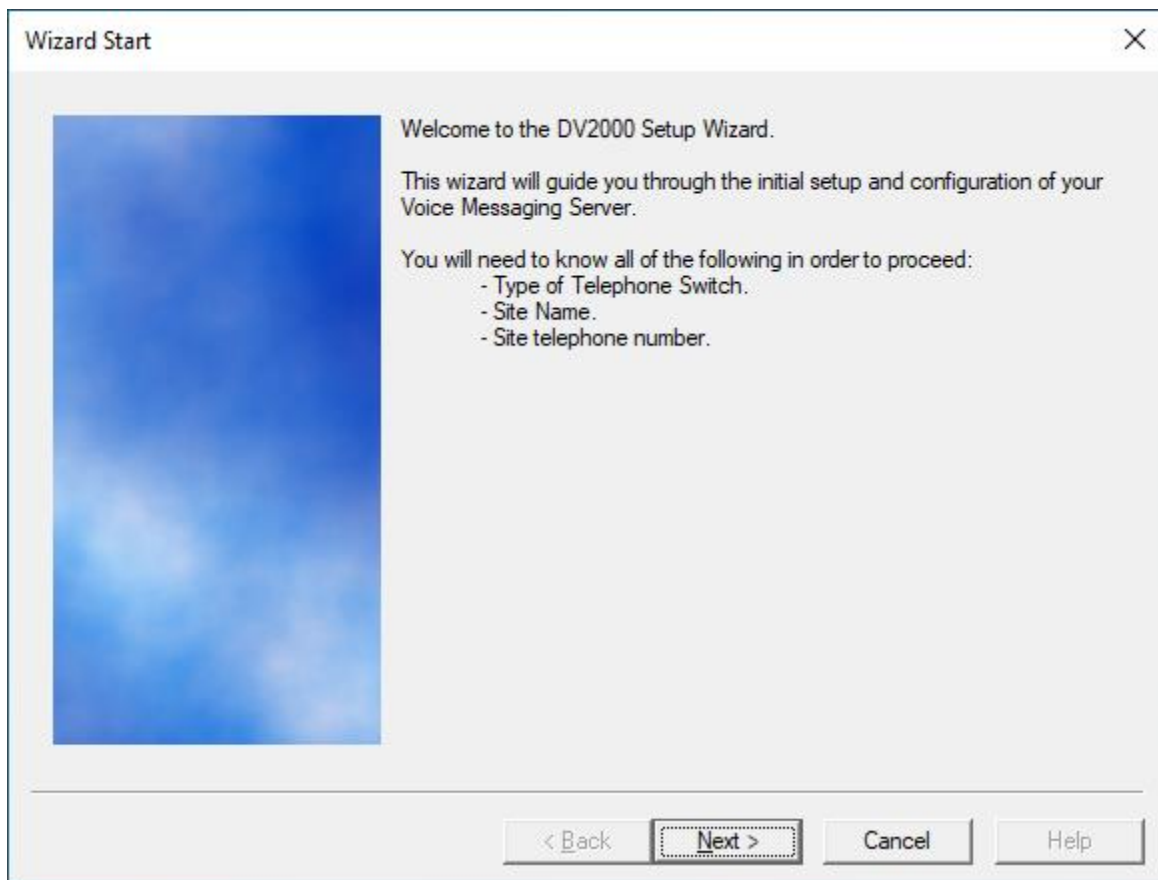
## 6. Configure DuVoice Emergency Alert System

This section provides the procedures for configuring EAS. The procedures include the following areas:

- Administer Setup Wizard
- Administer SIP configuration
- Administer site profile
- Administer EAS configuration
- Administer VeMail configuration
- Administer connector
- Administer mailbox
- Start services

### 6.1. Administer Setup Wizard

From the EAS server, launch the Setup Wizard by selecting **Start → DV2000 → System Configuration**. The **Wizard Start** screen below is displayed upon initial access.



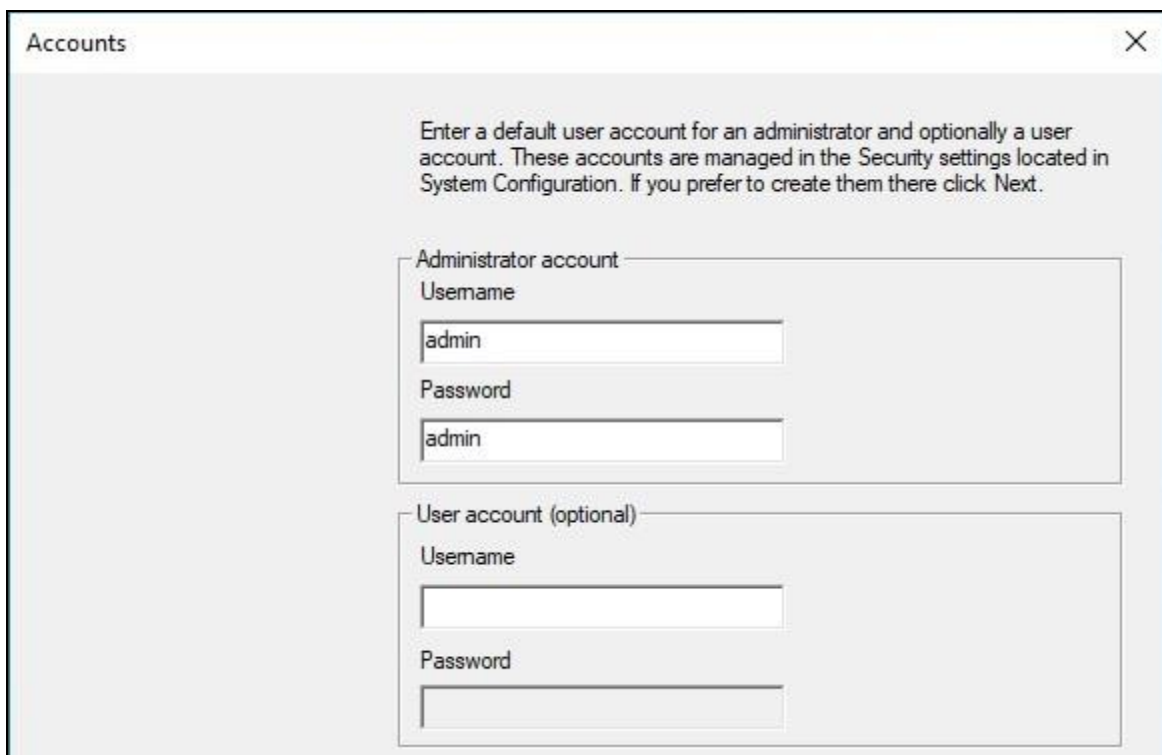
The **Site Information** screen is displayed next. Enter descriptive values for the required fields.



The 'Site Information' window contains a blue placeholder image on the left and a form on the right. The form has a message: 'Site Name is required. All other entries should be filled'. Below this is a 'Site Name' field with the value 'Avaya DevConnect'. A table below contains the following data:

Site Telephone	908-950-2222
Dealer Name	Avaya
Dealer Telephone	908-950-2222
Address	350 Mount Kemble Ave
Address	
State	NJ
Zip	07960
City	Morristown
Country	USA

The **Accounts** screen is displayed. Enter desired credentials for the **Administrator account** shown below. The administrator account will be used to access the EAS report.



The 'Accounts' window contains instructions: 'Enter a default user account for an administrator and optionally a user account. These accounts are managed in the Security settings located in System Configuration. If you prefer to create them there click Next.' Below are two sections:

**Administrator account**

Username:

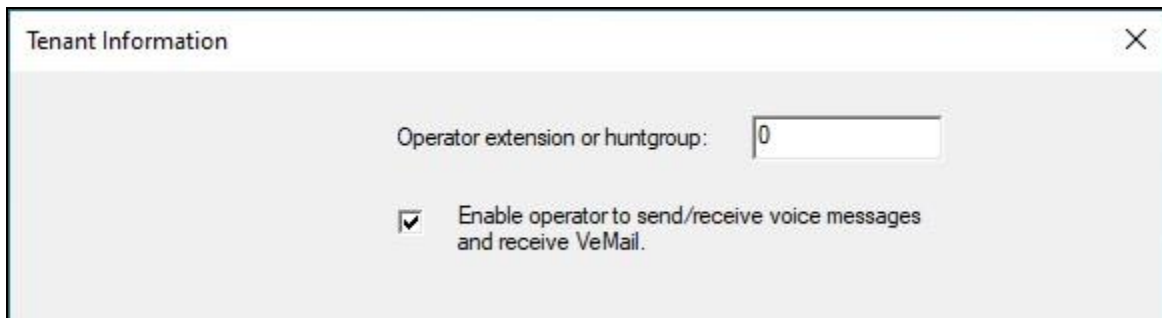
Password:

**User account (optional)**

Username:

Password:

The **Tenant Information** screen is displayed. Retain the default value for **Operator extension or huntgroup**, and check **Enable operator to send/receive voice messages and receive VeMail** as shown below.

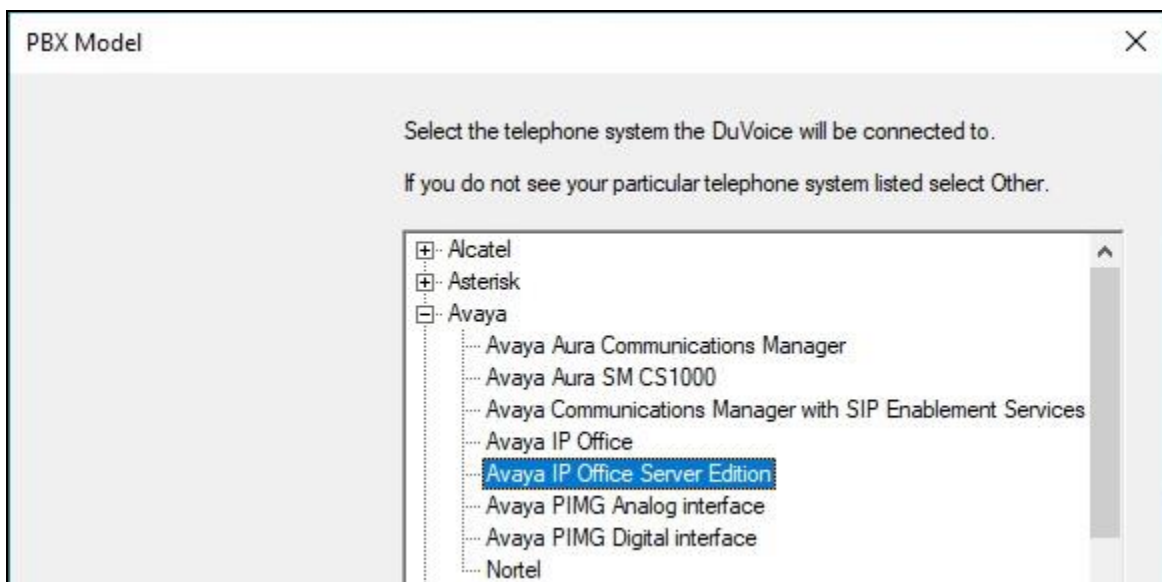


Tenant Information

Operator extension or huntgroup: 0

☒ Enable operator to send/receive voice messages and receive VeMail.

The **PBX Model** screen is displayed next. Expand and select **Avaya → Avaya IP Office Server Edition**. Retain the default values in the remaining screens and complete the Setup Wizard.



PBX Model

Select the telephone system the DuVoice will be connected to.  
If you do not see your particular telephone system listed select Other.

- Alcatel
- Asterisk
- Avaya
  - Avaya Aura Communications Manager
  - Avaya Aura SM CS1000
  - Avaya Communications Manager with SIP Enablement Services
  - Avaya IP Office
  - Avaya IP Office Server Edition**
  - Avaya PIMG Analog interface
  - Avaya PIMG Digital interface
- Nortel



## 6.2. Administer SIP Configuration

From the EAS server, double-click on the **System Configuration** icon shown below, which was created as part of server installation.

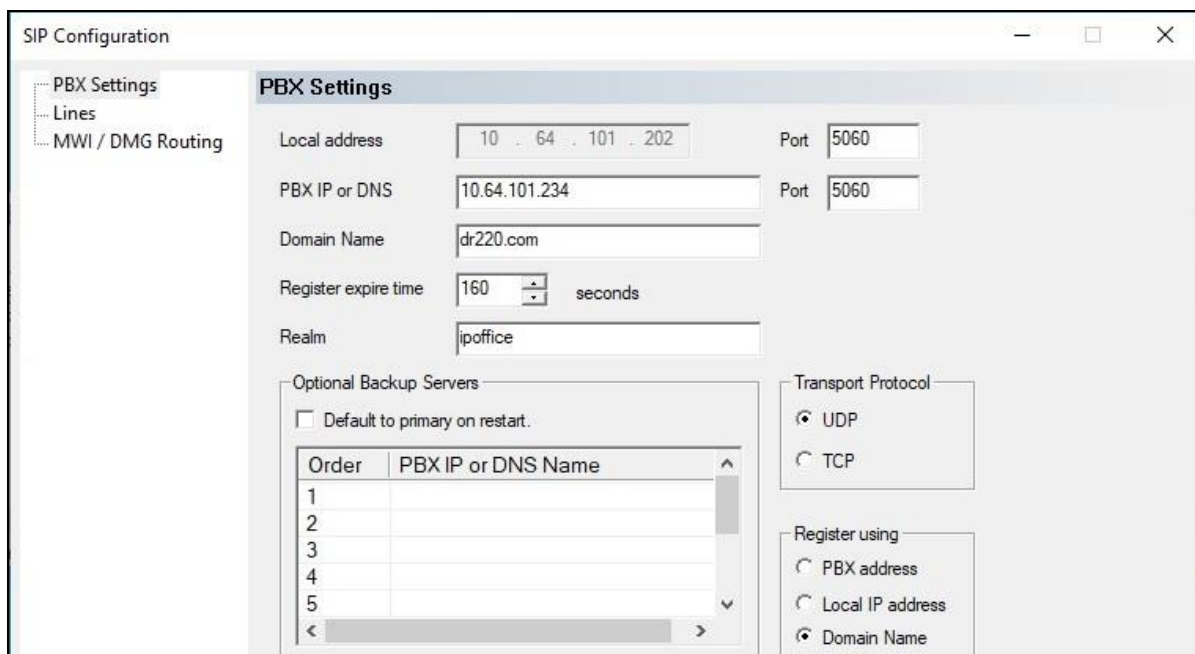


The **System Configuration** screen below is displayed. Select **Telephony → SIP Integration** from the top menu.

System Configuration							
File Site Telephony Features							
Device	Extension	Hunt Group	PBX Template	SIP User	Server	Enable Register	Tenant
SIP Line 1			SIP_IPOFFICE_SRVR			No	Avaya DevConnect
SIP Line 2			SIP_IPOFFICE_SRVR			No	Avaya DevConnect

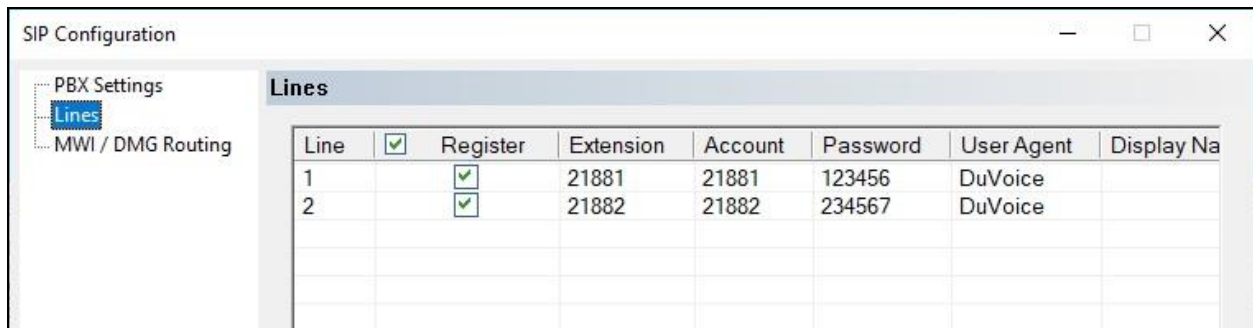
The **SIP Configuration** screen is displayed next. Select **PBX Settings** from the left pane. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **PBX IP or DNS:** IP address of the primary IP Office system.
- **Domain Name:** The IP Office domain name from **Section 5.3**.
- **Realm:** “ipoffice”
- **Register using:** Select **Domain Name**.

A screenshot of the 'SIP Configuration' window. The left sidebar shows a tree view with 'PBX Settings' selected. The main area is titled 'PBX Settings' and contains several input fields: 'Local address' (10.64.101.202), 'Port' (5060), 'PBX IP or DNS' (10.64.101.234), 'Port' (5060), 'Domain Name' (dr220.com), 'Register expire time' (160 seconds), and 'Realm' (ipoffice). There is a section for 'Optional Backup Servers' with a checkbox 'Default to primary on restart.' and a table with columns 'Order' and 'PBX IP or DNS Name'. The table has 5 rows. To the right, there are two sections: 'Transport Protocol' with radio buttons for 'UDP' (selected) and 'TCP', and 'Register using' with radio buttons for 'PBX address', 'Local IP address', and 'Domain Name' (selected).

Select **Lines** from the left pane. For each row, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Register:** Check this field.
- **Extension:** The corresponding SIP base extension from **Section 5.5**.
- **Account:** Same value as the extension number.
- **Password:** The corresponding SIP extension password from **Section 5.5**.

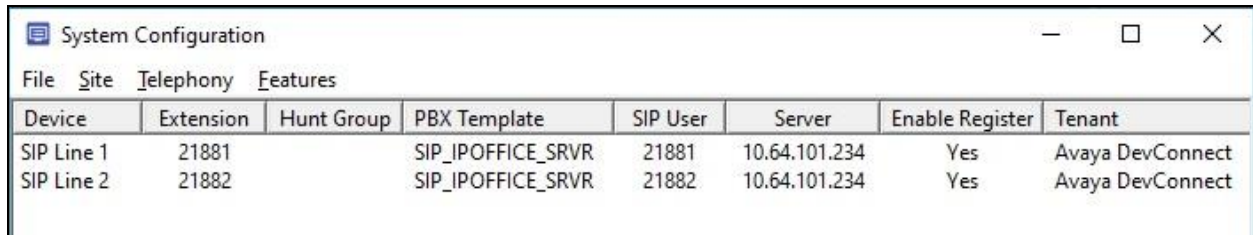


The screenshot shows a window titled "SIP Configuration" with a sidebar on the left containing "PBX Settings", "Lines" (highlighted), and "MWI / DMG Routing". The main area is titled "Lines" and contains a table with the following data:

Line	<input checked="" type="checkbox"/>	Register	Extension	Account	Password	User Agent	Display Na
1	<input checked="" type="checkbox"/>		21881	21881	123456	DuVoice	
2	<input checked="" type="checkbox"/>		21882	21882	234567	DuVoice	

### 6.3. Administer Site Profile

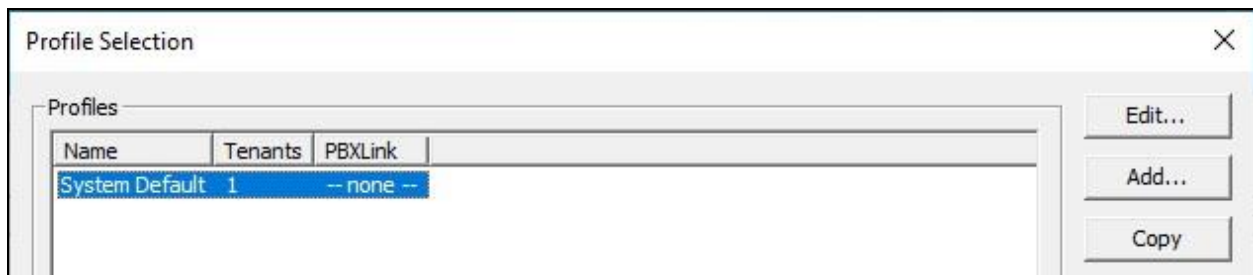
The **System Configuration** screen below is displayed again. Select **Site → Profiles** from the top menu.



The screenshot shows a window titled "System Configuration" with a menu bar (File, Site, Telephony, Features) and a table of SIP lines.

Device	Extension	Hunt Group	PBX Template	SIP User	Server	Enable Register	Tenant
SIP Line 1	21881		SIP_IPOFFICE_SRVR	21881	10.64.101.234	Yes	Avaya DevConnect
SIP Line 2	21882		SIP_IPOFFICE_SRVR	21882	10.64.101.234	Yes	Avaya DevConnect

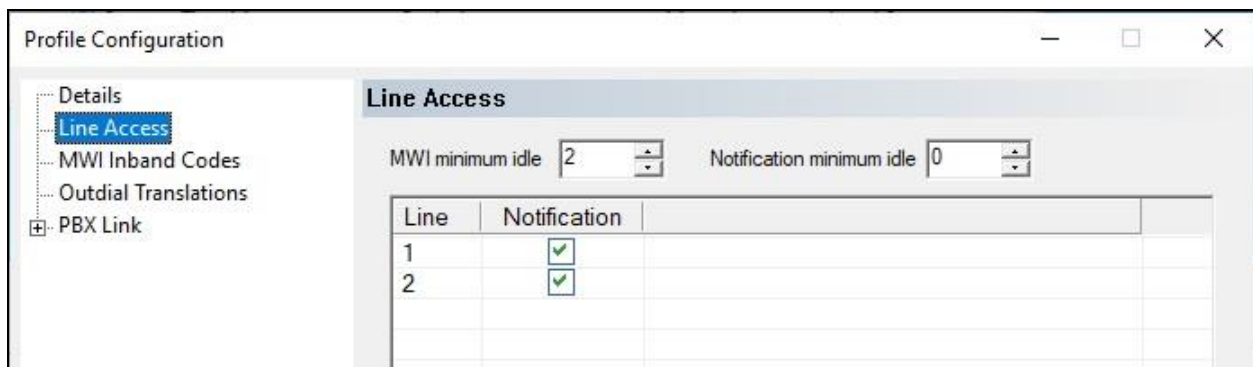
The **Profile Selection** screen is displayed next. Select the default entry and click **Edit**.



The screenshot shows a window titled "Profile Selection" with a table of profiles and buttons for Edit, Add, and Copy.

Name	Tenants	PBXLink
System Default	1	-- none --

The **Profile Configuration** screen is displayed. Select **Line Access** in the left pane to display the **Line Access** screen. For each line access entry, select the **Notification** column as shown below to enable the line to be used for call notifications. Note that by default only the first SIP line is set to be used for call notifications.



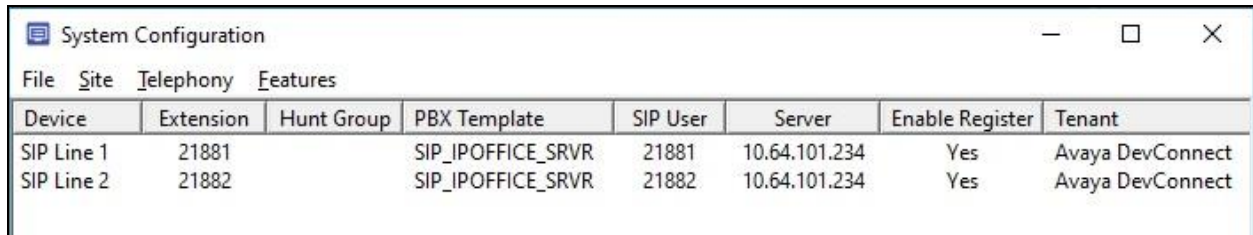
The screenshot shows a window titled "Profile Configuration" with a left pane containing "Details", "Line Access", "MWI Inband Codes", "Outdial Translations", and "PBX Link". The main pane shows "Line Access" settings.

MWI minimum idle: 2      Notification minimum idle: 0

Line	Notification
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>

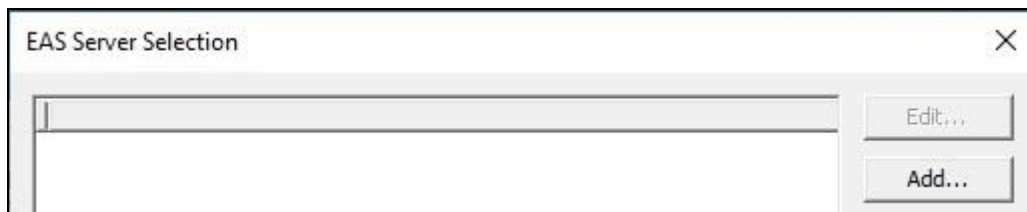
## 6.4. Administer EAS Configuration

The **System Configuration** screen below is displayed again. Select **Features** → **Emergency Alerts** from the top menu.



Device	Extension	Hunt Group	PBX Template	SIP User	Server	Enable Register	Tenant
SIP Line 1	21881		SIP_IPOFFICE_SRVR	21881	10.64.101.234	Yes	Avaya DevConnect
SIP Line 2	21882		SIP_IPOFFICE_SRVR	21882	10.64.101.234	Yes	Avaya DevConnect

The **EAS Server Selection** screen is displayed next. Click **Add**.



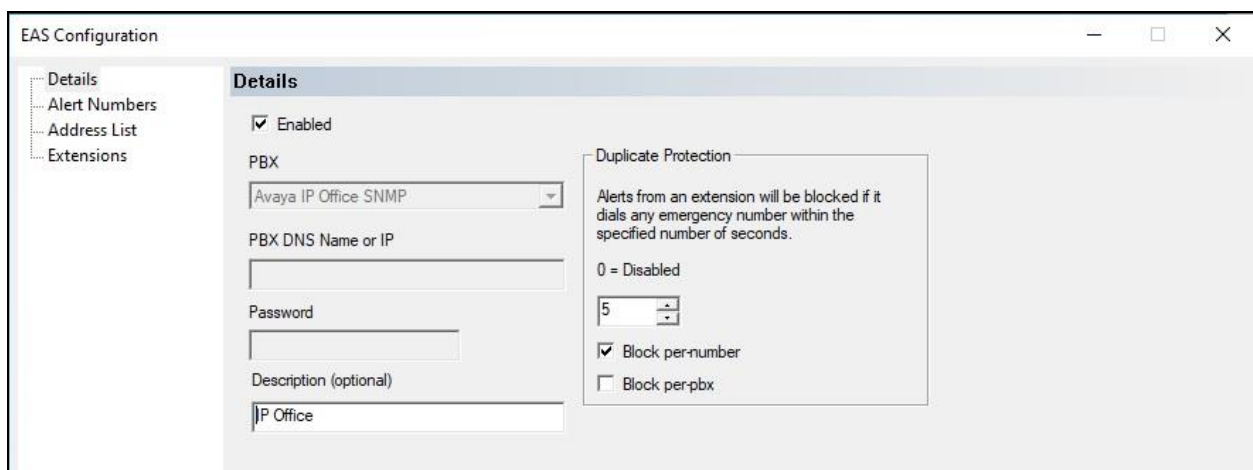
EAS Server Selection

Empty list box with "Edit..." and "Add..." buttons.

The **EAS Configuration** screen is displayed. In the **Details** screen in the right pane, enter the following values for the specified fields and retain the default values for the remaining fields.

- **Enabled:** Check this field.
- **PBX:** “Avaya IP Office SNMP”
- **Description:** An optional description.

In the **Duplicate Protection** sub-section, configure the desired block for multiple emergency calls from the same originator within a specified number of seconds. In the compliance testing, the setting below was configured.



EAS Configuration

**Details**

- ☒ Enabled
- PBX: Avaya IP Office SNMP
- PBX DNS Name or IP:
- Password:
- Description (optional): IP Office

**Duplicate Protection**

Alerts from an extension will be blocked if it dials any emergency number within the specified number of seconds.

0 = Disabled

5

- ☒ Block per-number
- ☐ Block per-pbx

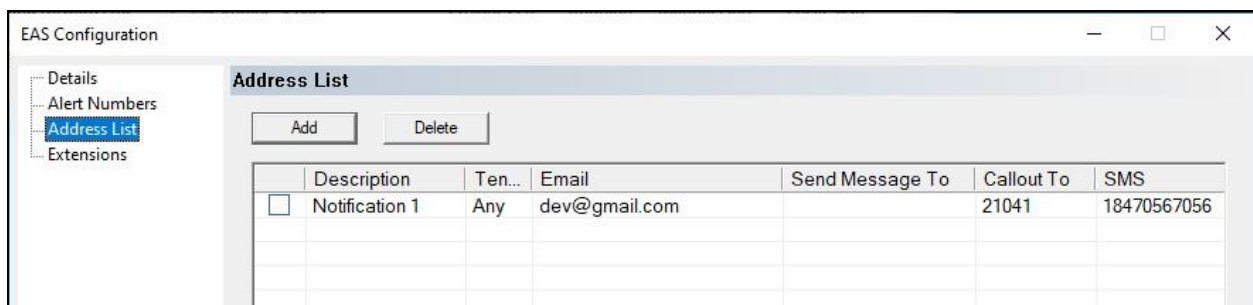
Select **Address List** from the left pane and add the desired notification destinations. Note that all alert destinations are to be provided by the customer and that multiple address list entries can be created. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Description:** A desired description.
- **Email:** A pertinent email address for email alert destination.
- **Callout To:** A pertinent user extension on IP Office for call alert destination.
- **SMS:** A pertinent SMS number for messaging alert destination.

In the compliance testing, one address list entry was created with sample **Email**, **Callout To**, and **SMS** destinations shown below. The **Email** destination below corresponded to a Microsoft Gmail test account, and the **Callout To** destination corresponded to a user extension on IP Office.

For **SMS**, note that EAS supports direct integration with Twilio and Clickatell for SMS notifications. In the compliance testing, a Twilio test account was used as sender of SMS notification messages, and the **SMS** destination below corresponded to a valid SMS number.

For customers that do not use Twilio and Clickatell for SMS notification, EAS will send SMS notifications via the email communication platform. In such case, the **SMS** destination in the screenshot below will need to be suffixed with the appropriate carrier domain name associated with the SMS destination. An example of this would be [14489285920@mms.att.net](mailto:14489285920@mms.att.net).

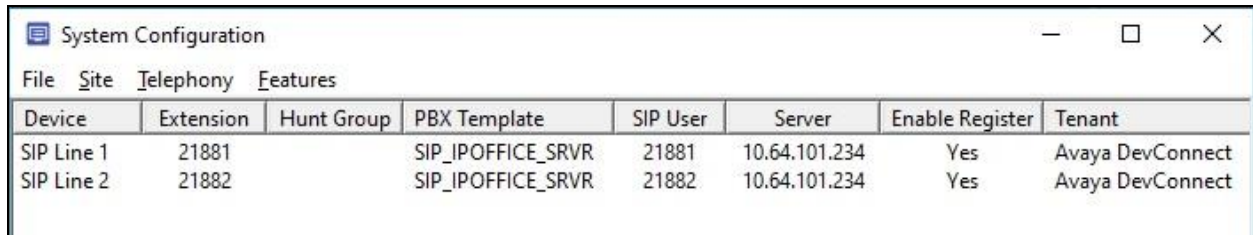


The screenshot shows the 'EAS Configuration' window with the 'Address List' tab selected. The table contains one entry with the following details:

	Description	Ten...	Email	Send Message To	Callout To	SMS
<input type="checkbox"/>	Notification 1	Any	dev@gmail.com		21041	18470567056

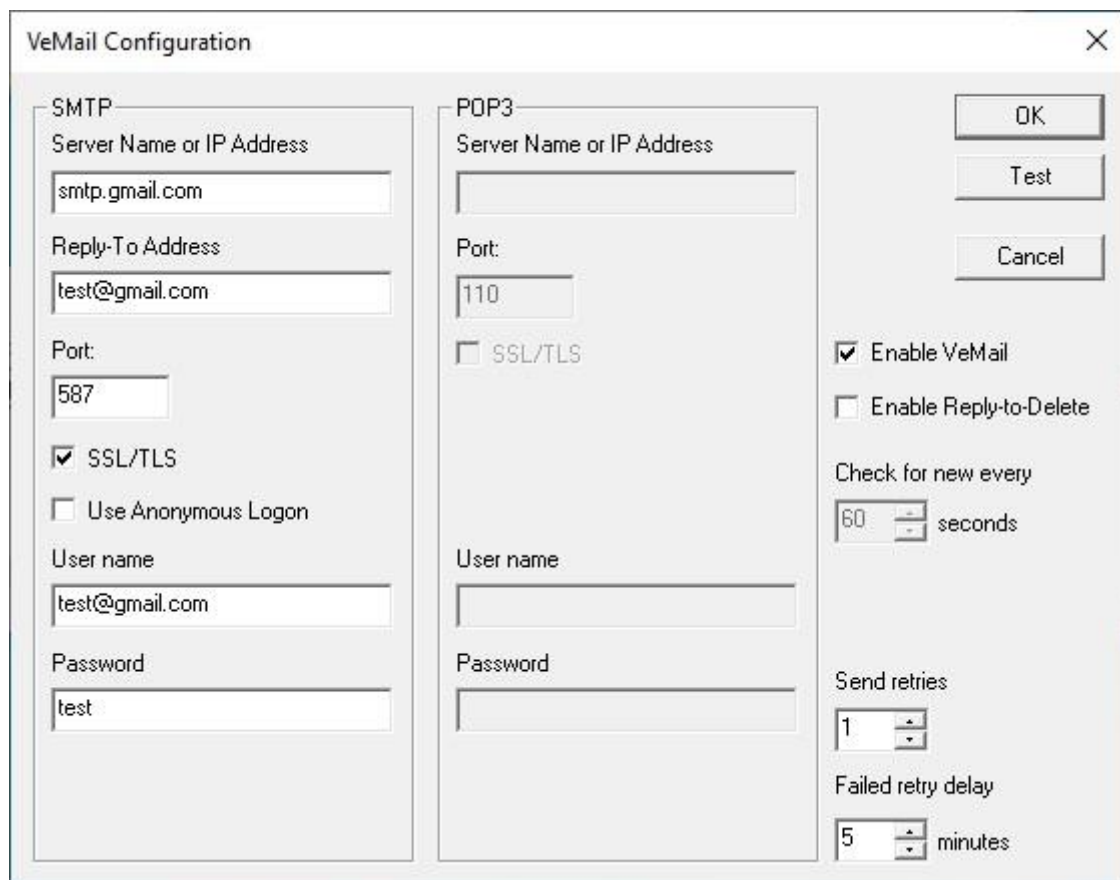
## 6.5. Administer VeMail Configuration

The **System Configuration** screen below is displayed again. Select **Features** → **VeMail** from the top menu.



Device	Extension	Hunt Group	PBX Template	SIP User	Server	Enable Register	Tenant
SIP Line 1	21881		SIP_IPOFFICE_SRVR	21881	10.64.101.234	Yes	Avaya DevConnect
SIP Line 2	21882		SIP_IPOFFICE_SRVR	21882	10.64.101.234	Yes	Avaya DevConnect

The **VeMail Configuration** screen is displayed next. Check **Enable VeMail** on the right side of the screen. Follow reference [3] to configure the appropriate settings using customer provided information for email communication. The screenshot below represents a sample configuration.



**VeMail Configuration**

**SMTP**

Server Name or IP Address: smtp.gmail.com

Reply-To Address: test@gmail.com

Port: 587

☒ SSL/TLS

☐ Use Anonymous Logon

User name: test@gmail.com

Password: test

**POP3**

Server Name or IP Address:

Port: 110

☐ SSL/TLS

User name:

Password:

☒ Enable VeMail

☐ Enable Reply-to-Delete

Check for new every 60 seconds

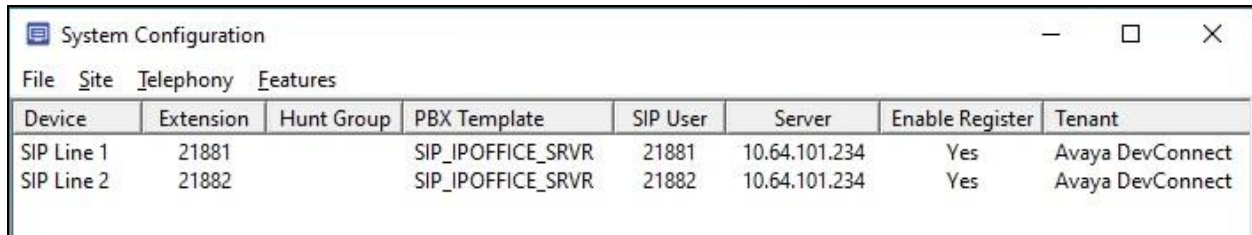
Send retries 1

Failed retry delay 5 minutes

OK, Test, Cancel buttons

## 6.6. Administer Connector

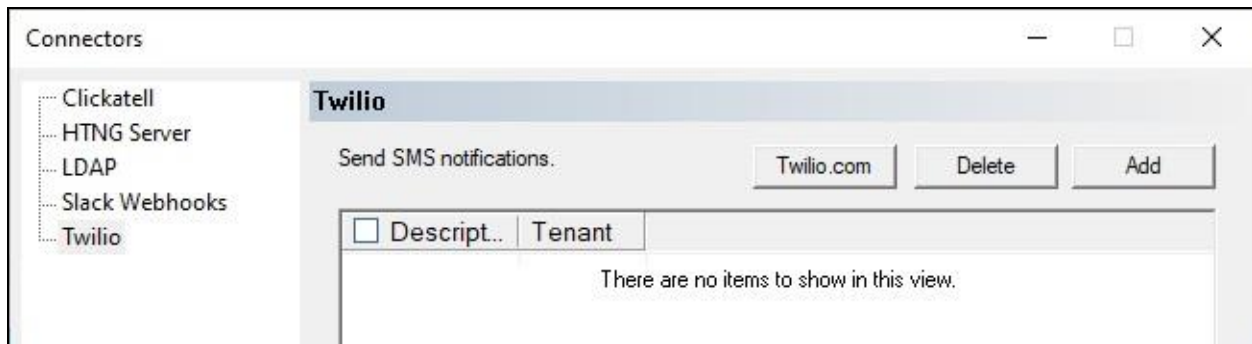
The **System Configuration** screen below is displayed again. For customers that use Twilio or Clickatell for SMS notification, an appropriate connector needs to be configured. Select **Features** → **Connectors** from the top menu.



The screenshot shows a 'System Configuration' window with a menu bar (File, Site, Telephony, Features) and a table of SIP lines. The table has columns for Device, Extension, Hunt Group, PBX Template, SIP User, Server, Enable Register, and Tenant. Two rows are visible: SIP Line 1 and SIP Line 2, both using the SIP\_IPOFFICE\_SRVR template and Avaya DevConnect tenant.

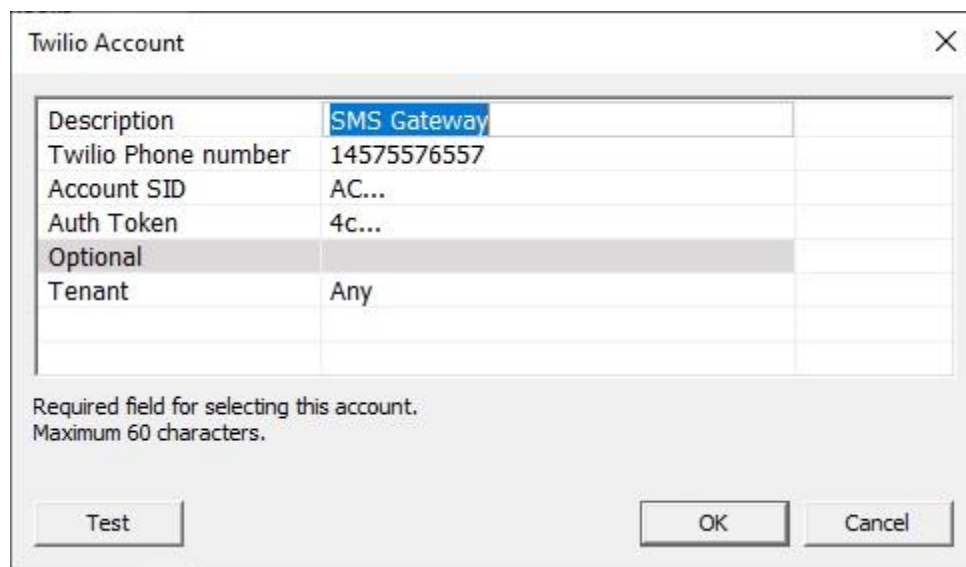
Device	Extension	Hunt Group	PBX Template	SIP User	Server	Enable Register	Tenant
SIP Line 1	21881		SIP_IPOFFICE_SRVR	21881	10.64.101.234	Yes	Avaya DevConnect
SIP Line 2	21882		SIP_IPOFFICE_SRVR	21882	10.64.101.234	Yes	Avaya DevConnect

The **Connectors** screen is displayed next. Select the appropriate connector in the left pane, in this case **Twilio**, followed by **Add** in the updated right pane.



The screenshot shows a 'Connectors' window. On the left, a list of connectors includes Clickatell, HTNG Server, LDAP, Slack Webhooks, and Twilio (which is highlighted). On the right, the 'Twilio' connector details are shown, including a 'Send SMS notifications' checkbox, a 'Twilio.com' button, and 'Delete' and 'Add' buttons. Below these is a table with columns 'Description' and 'Tenant', which is currently empty with the message 'There are no items to show in this view.'

The **Twilio Account** screen is displayed. Enter a desired **Description**, and pertinent values associated with the sender account to use for SMS notifications.



The screenshot shows a 'Twilio Account' configuration window. It contains a table with the following fields: Description (SMS Gateway), Twilio Phone number (14575576557), Account SID (AC...), Auth Token (4c...), Optional (highlighted), and Tenant (Any). Below the table is a note: 'Required field for selecting this account. Maximum 60 characters.' At the bottom are buttons for 'Test', 'OK', and 'Cancel'.

Description	SMS Gateway
Twilio Phone number	14575576557
Account SID	AC...
Auth Token	4c...
Optional	
Tenant	Any



## 6.7. Administer Mailbox

From the EAS server, double-click on the **Mailbox Administration** icon shown below, which was created as part of server installation.



The **Mailbox Administration** screen is displayed. Follow reference [3] to create a mailbox for each call alert destination from **Section 6.4** along with “Standard” as mailbox **Type**, as shown below.

Mailbox Administration									
File Mailbox Templates Reports									
Distribution List	Mailbox	Extension	First name	Type	Description	Tenant	COS	SDA	
Group	0	0	Operator	Standard	Operator	Avaya DevConnect	standard	standard	
Guest	991	991	Auto Attendant	System	Auto Attendant	Avaya DevConnect	system	default	
QA	21041	21041	Standard 21041	Standard	Standard	Avaya DevConnect	standard	standard	
Standard									
System									

Next, select **Templates → Class of Service** from the top menu of the **Mailbox Administration** screen above to display the **Class of Service Templates** screen below. Select the **standard** entry followed by **Edit**.

Class of Service Templates				
Name	Used			
audiotext	0		Edit...	
directvm	0		Copy...	
emergency alert	0		Delete	
extended stay	0			
group	0			
guest	0		New...	
standard	7		Import...	
system	1			
toshiba perception	0		Close	



The **COS - standard** screen is displayed. Select **Recording** to display the **Recording** screen. Uncheck **Allow receiving messages** as shown below. Note that this setting is necessary for EAS standalone deployments that are not using the DV2000 voicemail feature.

The screenshot shows a software window titled "COS - standard" with a close button (X) in the top right corner. On the left is a vertical navigation pane with the following items: General, Recording (highlighted), Playback, Transfers, VeMail, Greetings / Prompts, and Wakeup Calls. The main area of the window is titled "Recording" and contains two primary sections: "Message Settings" and "Minimum / Maximum Settings".

**Message Settings:**

- ☒ Allow sending messages
- ☐ Allow receiving messages (this checkbox is highlighted with a dashed border)
- ☐ Block delivery to checked out rooms
- ☒ Allow private messages
- ☒ Allow urgent messages
- ☐ Reply to creator not sender
- ☐ Limit message retention
- Retention in days: 0

**Minimum / Maximum Settings:**

- Max message size in seconds: 300
- Min message size in seconds: 1
- Max message storage in minutes: 180
- Max greeting size in seconds: 60
- Max call screening name record: 5

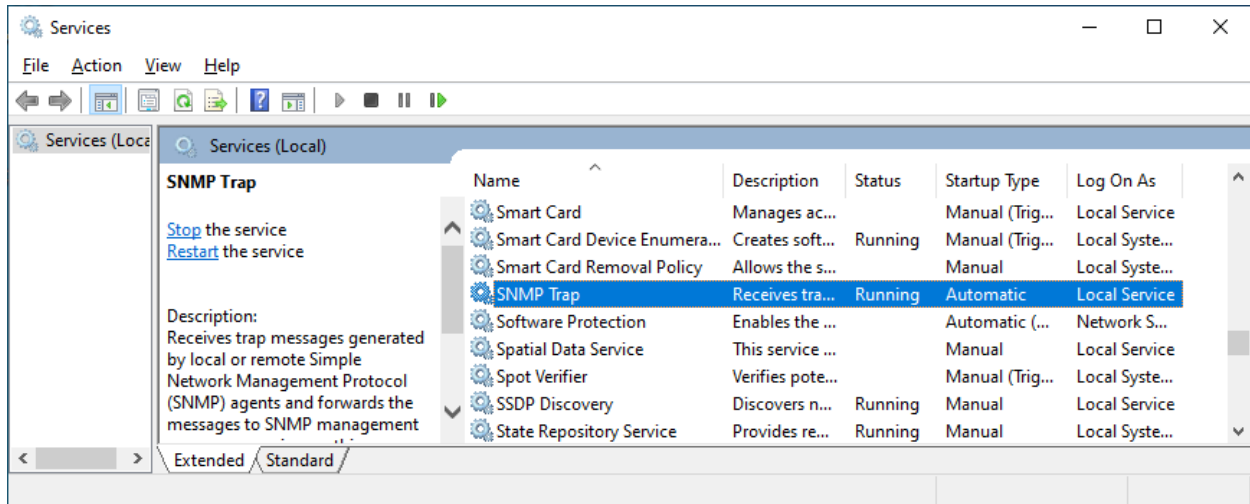
**Record-a-Call:**

- ☒ Beep before recording

At the bottom right of the window are three buttons: "Save", "SaveAs", and "Cancel".

## 6.8. Start Services

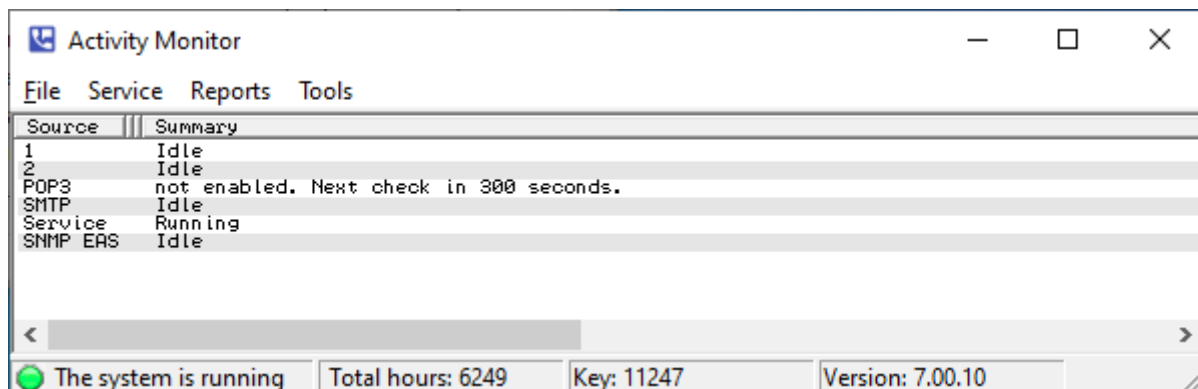
From the EAS server, navigate to **Windows → Windows System → Windows Administrative Tools → Services** to display the **Services** screen below. Locate the **SNMP Trap** service, set the **Startup Type** to “Automatic” and start the service as shown below.



From the EAS server, double-click on the **Activity Monitor** icon shown below, which was created as part of server installation.



Select **Service → Start** from the top menu to start the application.

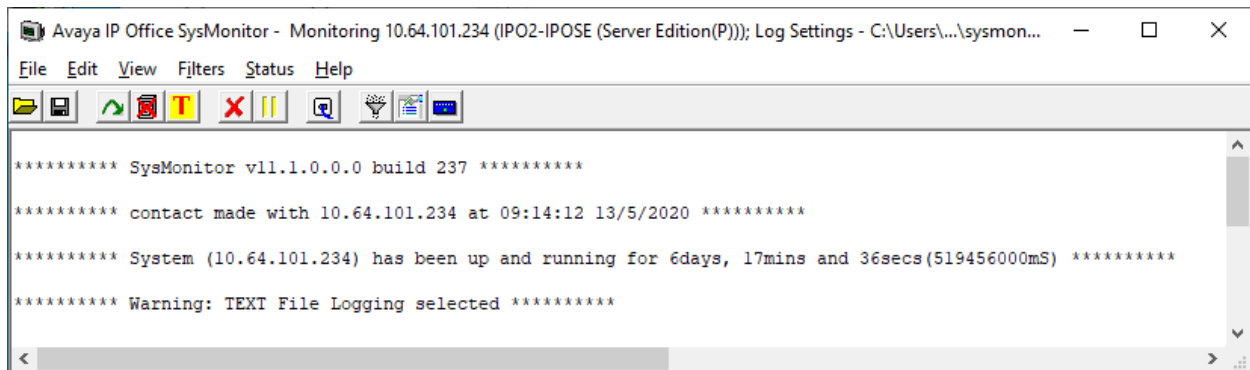


## 7. Verification Steps

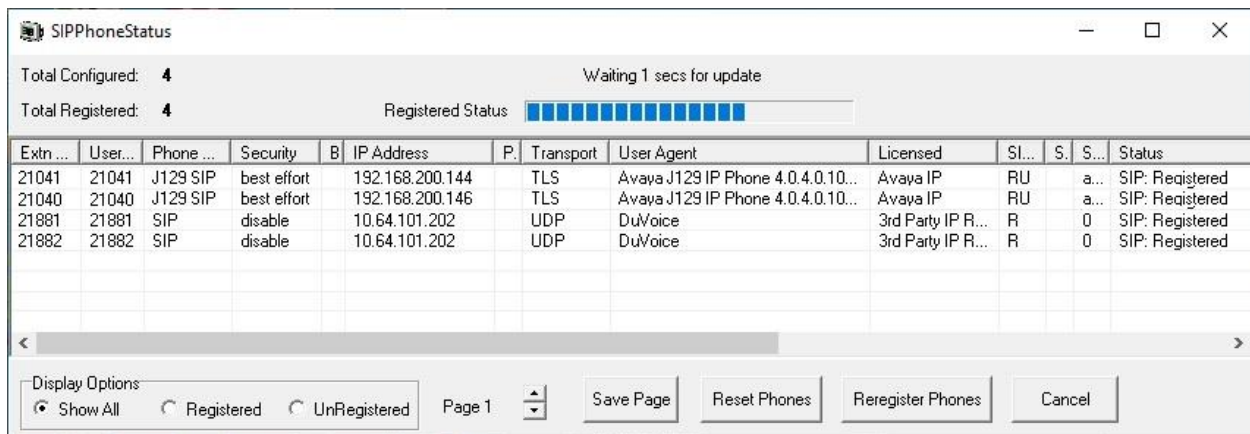
This section provides the tests that can be performed to verify proper configuration of IP Office and EAS.

### 7.1. Verify SIP User Integration

From a PC running the IP Office Monitor application, select **Start → All Programs → IP Office → Monitor** to launch the application, and connect to the primary IP Office system. The **Avaya IP Office SysMonitor** screen is displayed. Select **Status → SIP Phone Status** from the top menu.



The **SIPPhoneStatus** screen is displayed. Verify that there is an entry for each SIP extension from **Section 5.5**, that the **User Agent** is “DuVoice”, and that the **Status** is “SIP: Registered”, as shown below.



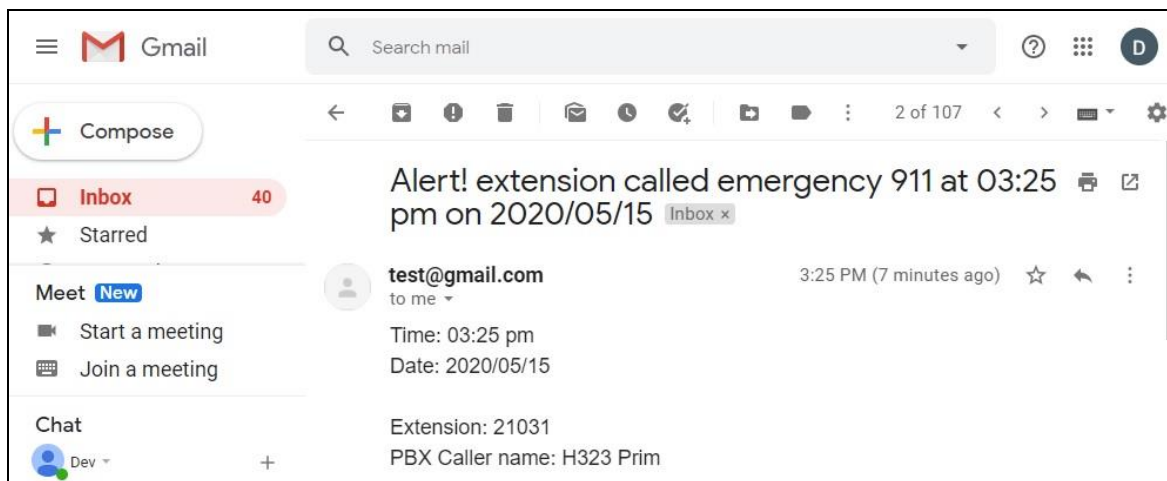
## 7.2. Verify Call Notification

Make an emergency call from an IP Office user. Verify that a call notification is placed from an available virtual SIP user by EAS to the configured call alert destination in **Section 6.4**.

Answer the call at the call alert destination, and verify that the user hears the proper announcement “An emergency number was dialed by extension 21031 for phone number 911, to replay this message press 1, for help press pound, to cancel this operation press star”, where “21031” is the extension of the emergency call originator, and “911” is the emergency number that was dialed.

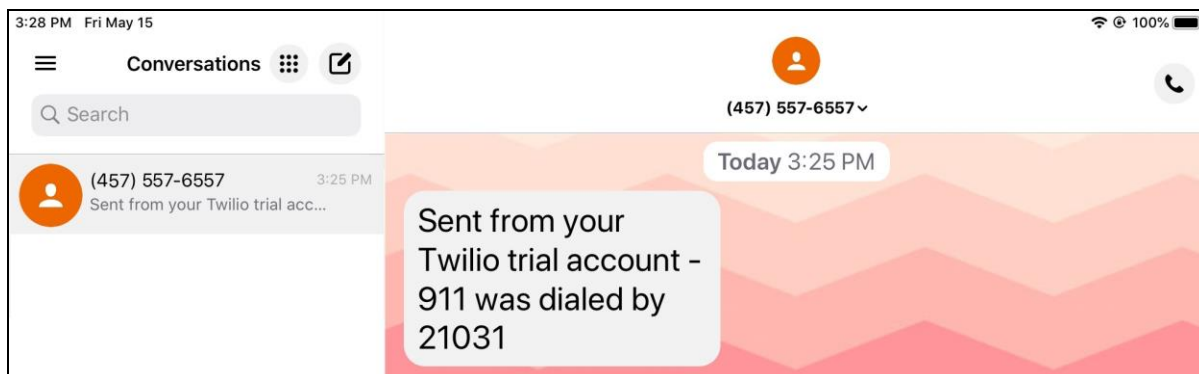
## 7.3. Verify Email Notification

Log the email alert destination into the applicable email application. Verify that there is email notification for the emergency call from **Section 7.2** as shown below, where “H323 Prim” is the name of the emergency call originator obtained from the SNMP trap.



## 7.4. Verify SMS Notification

Log the SMS alert destination into the applicable SMS application or cell phone. Verify that there is SMS notification for the emergency call from **Section 7.2** as shown below.



## 7.5. Verify EAS Report

Access the EAS web-based interface by using the URL <http://ip-address> where “ip-address” is the IP address of the EAS server.

The **DuVoice DV2000** screen below is displayed. Select **Emergency Alert System**.



The screen below is displayed next. Verify that there is an entry for each call, email, and SMS notification associated with the attempted emergency call from **Section 7.2**, as shown below.

Home Reports▼ Applications▼							
Show	50▼	entries		Print		Search:	
Date/Time	Extension	Name	Number	Result	Note	Source	
05/15 3:25:01 pm	21031		911	SMS	SMS alert sent to 18470567056	IP Office ()	
05/15 3:25:01 pm	21031		911	Callout message	Callout alert to mailbox 21041	IP Office ()	
05/15 3:25:00 pm	21031		911	Email	Email alert sent to dev@gmail.com	IP Office ()	
Showing 1 to 3 of 3 entries						Previous	1 Next
DuVoice DV2000 Emergency Alert System - 7.00.10 - 11247 - 2020/05/15 12:25:13							

## 8. Conclusion

These Application Notes describe the configuration steps required for DuVoice Emergency Alert System 7.0 to successfully interoperate with Avaya IP Office Server Edition 11.1. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

## 9. Additional References

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

1. *Administering Avaya IP Office™ Platform with Manager*, Release 11.1, Issue 1, April 2020, available at <http://support.avaya.com>.
2. *Making Use of the Emergency Services Access Enhancements in IP Office Release 9.0/9.1*, available at <http://support.avaya.com>.
3. *DV2000 7 System Reference Guide*, available at <http://support.duvoice.com/product/vs7/manual/home>.

---

**©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).