Avaya Solution & Interoperability Test Lab

Application Notes for Resource Software International Shadow Onsite Notification 2.3 with Avaya IP Office Server Edition 10 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Resource Software International Shadow Onsite Notification 2.3 to interoperate with Avaya IP Office Server Edition 10.

Resource Software International Shadow Onsite Notification is an E911 notification solution that uses Syslog, TAPI, and Configuration Web Service interfaces from Avaya IP Office, and the PUSH interface from Avaya 96xx IP Deskphones to provide real-time monitoring and notification of emergency calls.

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

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

1. Introduction

These Application Notes describe the configuration steps required for Resource Software International (RSI) Shadow Onsite Notification (OSN) 2.3 to interoperate with Avaya IP Office Server Edition 10.

RSI Shadow OSN is an E911 notification solution that uses Syslog, TAPI, and Configuration Web Service interfaces from Avaya IP Office, and the PUSH interface from Avaya 96xx IP Deskphones to provide real-time monitoring and notification of emergency calls.

The Avaya IP Office Server Edition configuration consisted of two Avaya IP Office systems, a primary Linux server at the Main site and an expansion IP500V2 at the Remote site that were connected via Small Community Network (SCN) trunks.

In the compliance testing, one RSI Shadow OSN server was deployed. The RSI Shadow OSN server used Syslog with the primary IP Office system to monitor users at the Main site, and Syslog with the expansion IP Office system to monitor users at the Remote site.

Upon detection of an emergency call made by an IP Office user, RSI Shadow OSN used TAPI and Configuration Web Service to send notification to designated digital notification points, whom are users on the expansion IP500V2 IP Office system with Avaya Digital Deskphones; and used PUSH to send notification to designated IP notification points, whom are users on both IP Office systems with Avaya 96xx IP Deskphones.

The TAPI and Configuration Web Service connections must both be with the same IP Office system, and can be either the primary Linux server or the expansion IP500V2 system. The configuration shown in these Application Notes used the expansion IP Office system for connectivity of TAPI and Configuration Web Service. TAPI 2 in third party mode is used to place notification calls from designated originator extensions to digital notification points, and Configuration Web Service is used to change the name of the designated originators to reflect EMERGENCY along with the extension of the emergency caller.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Shadow OSN application, the application automatically obtained list of users from the IP Office system connected via TAPI and Configuration Web Service.

For the manual part of the testing, emergency calls were placed manually from IP Office users to the emulated PSTN.

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

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

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Shadow OSN:

- Proper handling of real-time Syslog event messages.
- Use of TAPI to originate notification calls from designated originating extensions (TAPI notification originator) on IP Office to designated notification points on the expansion IP Office IP500V2 system
- Use of Configuration Web Service to update the name of the designated TAPI notification originator for reflection of EMERGENCY along with the extension of the emergency caller.
- Use of PUSH interface to send notifications to IP notification points, including name of the emergency caller and dialed digits.
- Proper handling of emergency call scenarios involving emergency callers from both IP Office systems, IP notification points on both IP Office systems, digital notification point on expansion IP500V2 IP Office system, button activation of emergency call, push notification intervals and duration, push notification cancelation, digital notification point retries, simultaneous emergency callers, and simultaneous notification to all notification points.

The feature testing call flows included emergency calls with all resources within the primary IP Office at the Main site, emergency calls with all resources within the expansion IP Office at the Remote site, as well as emergency calls with resources between the two IP Office systems.

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

2.2. Test Results

All test cases were executed and completed successfully.

2.3. Support

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

- **Phone:** 905-576-4575 or 718-701-0945
- **Email:** support@telecost.com
- **Web:** www.telecost.com

3. Reference Configuration

The IP Office Server Edition configuration used in the compliance testing consisted of a primary Linux server at the Main site, and an expansion IP500V2 at the Remote site, with SCN trunks connectivity between the two systems. Each IP Office system has connectivity to the PSTN, for testing cross systems PSTN scenarios.

The detailed administration of IP Office resources is not the focus of these Application Notes and will not be described. As shown in **Figure 1** below, one Shadow OSN server was deployed with Syslog connection to the primary IP Office system, with Syslog, TAPI, and Configuration Web Service to the expansion IP Office system, and with PUSH to all IP notification points on both IP Office systems.

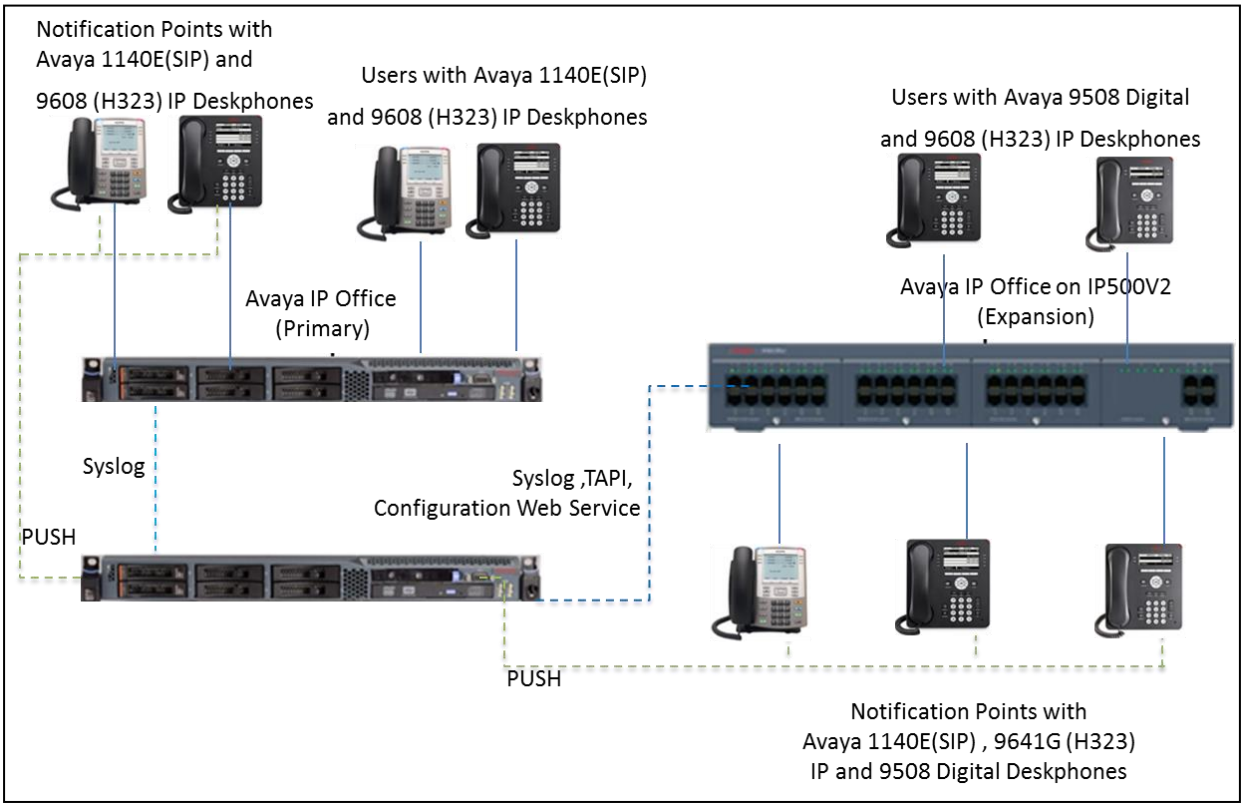


Figure 1: Compliance Testing Configuration

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	R10.0.0.3
Avaya IP Office on IP500 V2 (Expansion)	R10.0.0.3
Avaya 9508 Digital Deskphones	NA
Avaya 9608 and 9641G IP Deskphone (H.323)	6.6.4
Avaya 1140E IP Deskphone (SIP)	4.4.23
RSI Shadow Onsite Notification on Windows 2012 R2	2.3.0.004 SP1

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 the IP Office systems. The procedures include the following area:

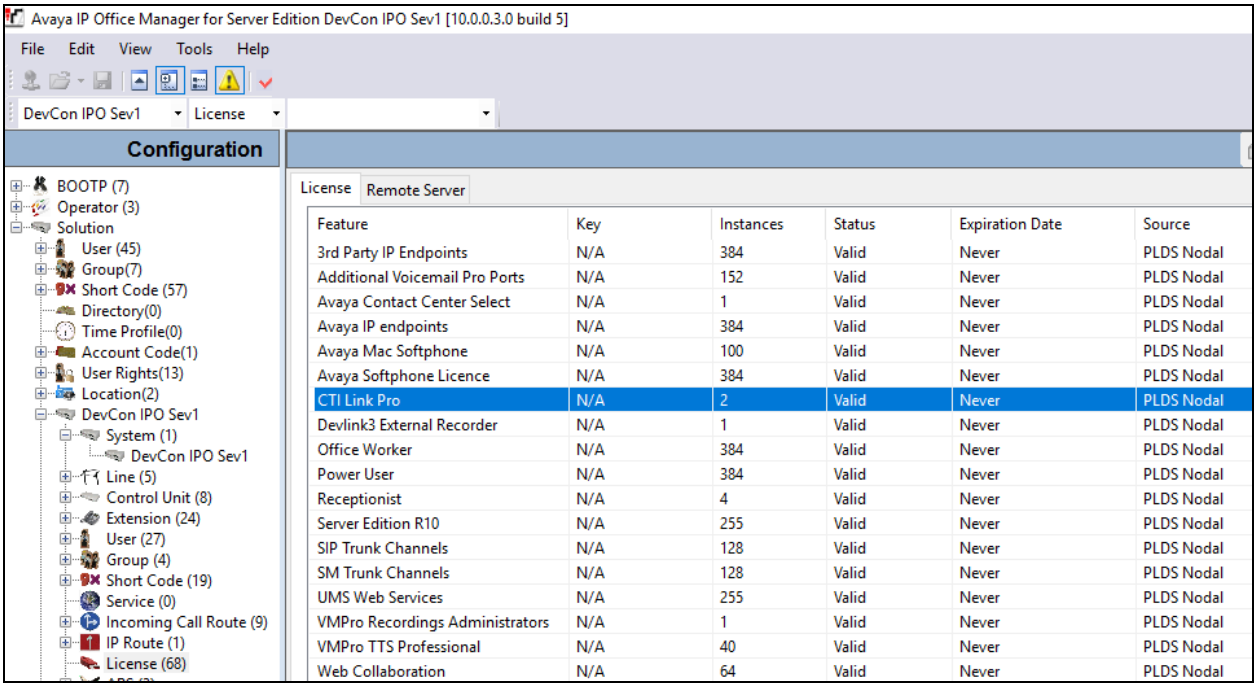
- Verify licenses
- Administer System Events
- Administer emergency short codes
- Administer security settings

5.1. Verify Licenses

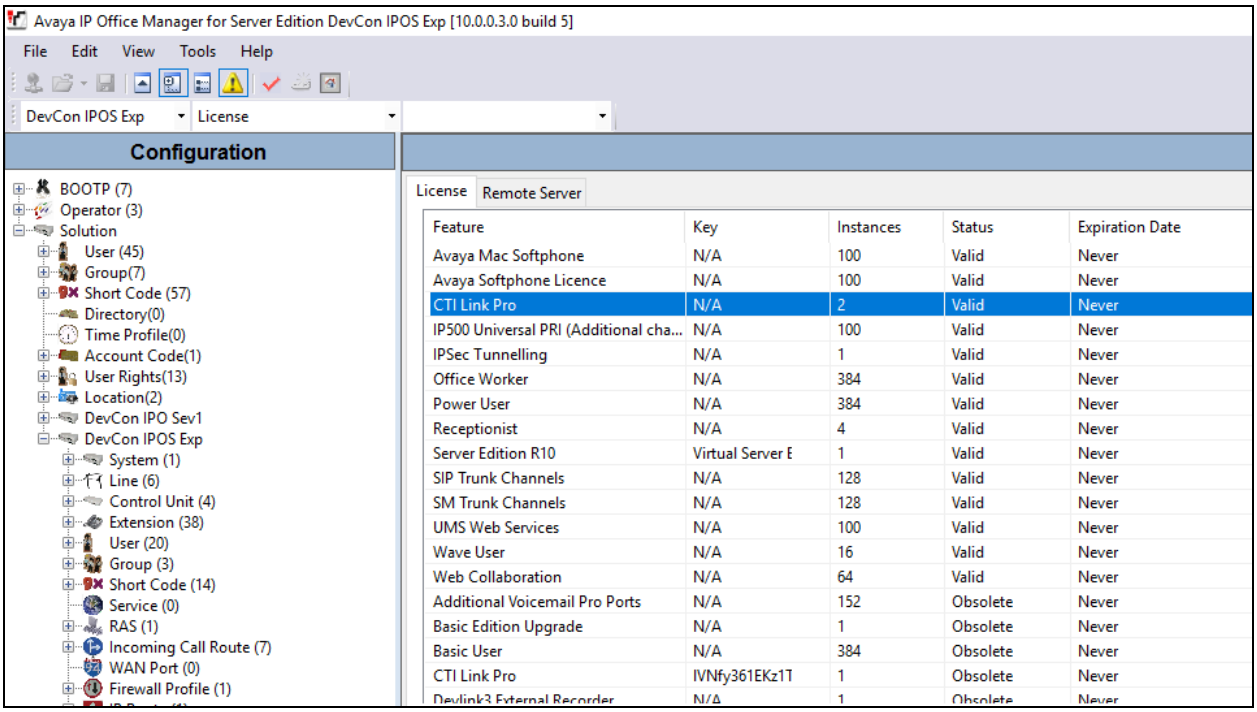
From a PC running the IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the application. Select the proper primary IP Office system, and log in using the appropriate credentials.

The **Avaya IP Office Manager for Server Edition DevCon IPO Sev1** screen is displayed, where **DevCon IPO Sev1** is the name of the primary IP Office system.

From the configuration tree in the left pane, select **License** under the primary IP Office system, in this case "**DevConn IPO Sev1**", to display a list of licenses in the right pane. Verify that there is a license for **CTI Link Pro** and that the **Status** is "Valid", as shown below. This license is only needed for TAPI connections with Shadow OSN.



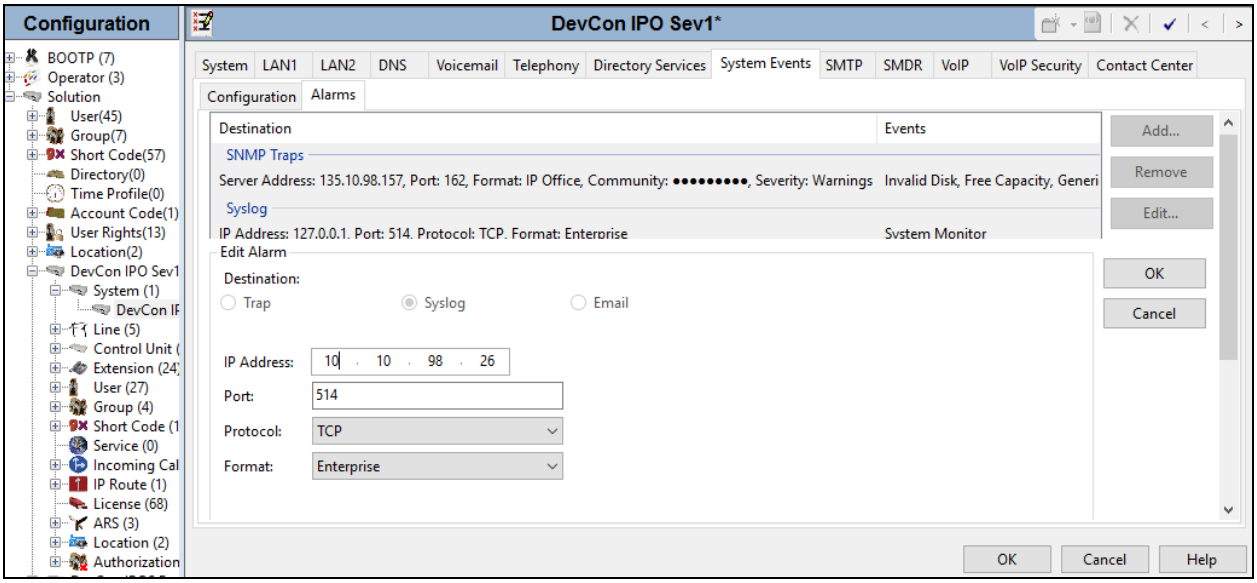
From the configuration tree in the left pane, select **License** under the expansion IP Office system, in this case "**DevConn IPOS Exp**", to display a list of licenses in the right pane. Verify that there is a license for **CTI Link Pro** and that the **Status** is "Valid", as shown below. This license is needed for TAPI connections with Shadow OSN.



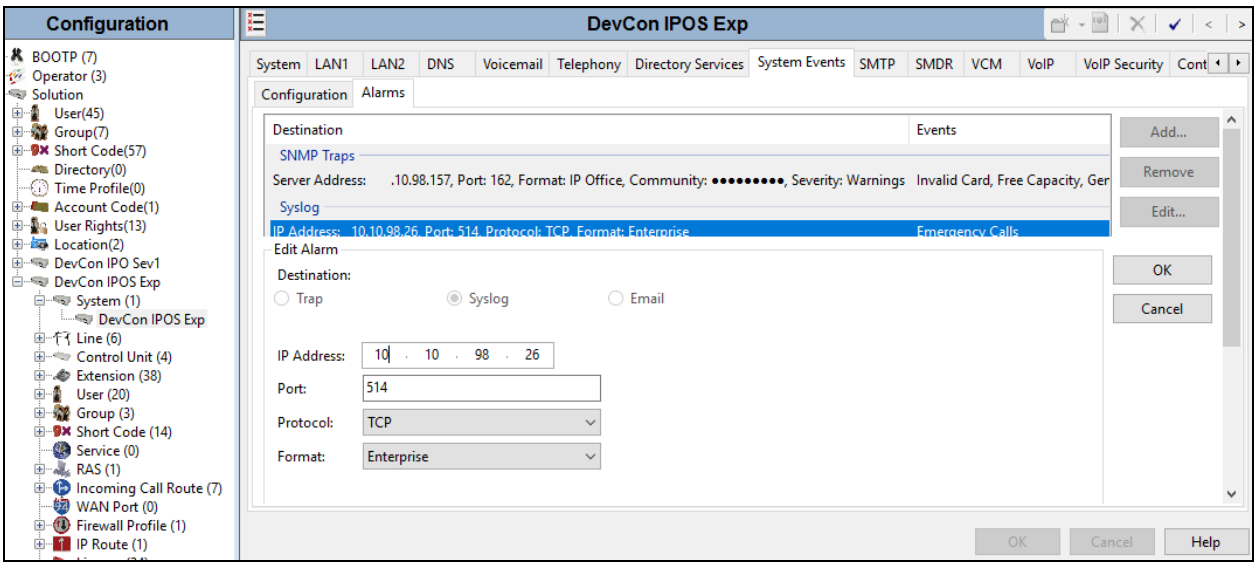
5.2. Administer System Events

From the configuration tree in the left pane, select primary IP Office system, in this case "**DevConn IPO Sev1**", select **System Events → Alarms.** Click **Add** to add OSN as new destination to receive events.

For **Destination** select **Syslog**, enter the IP Address of OSN machine, in this case "10.10.98.26". For **Port**, use default "514". Select "TCP" for **Protocol.** And retain the default values in the remaining fields.



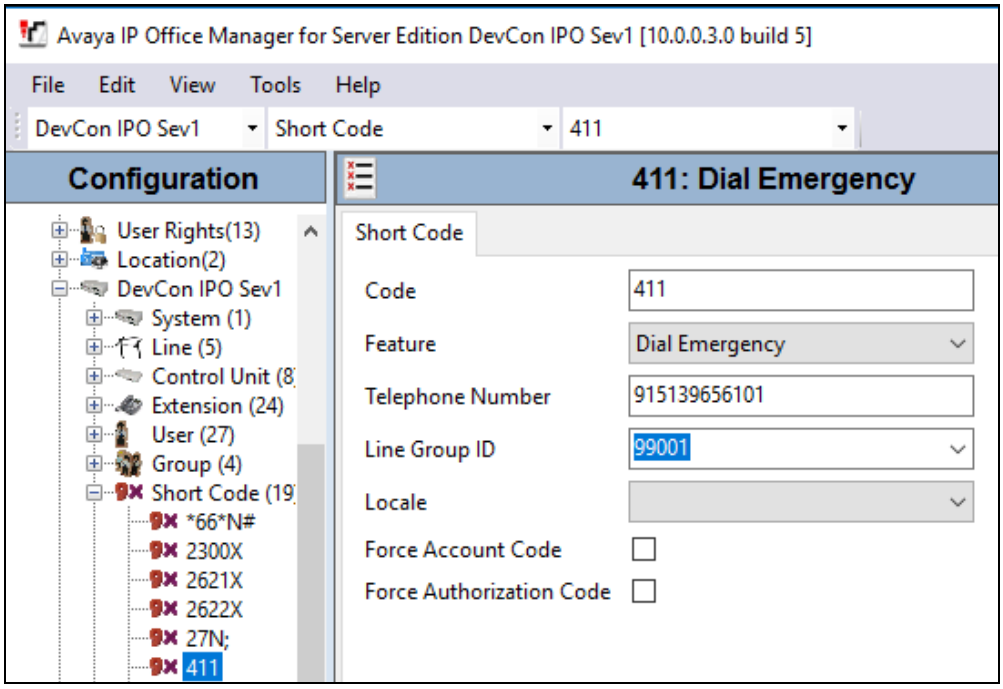
Repeat this section to add similar Syslog Destination for the expansion IP Office system, as shown below:



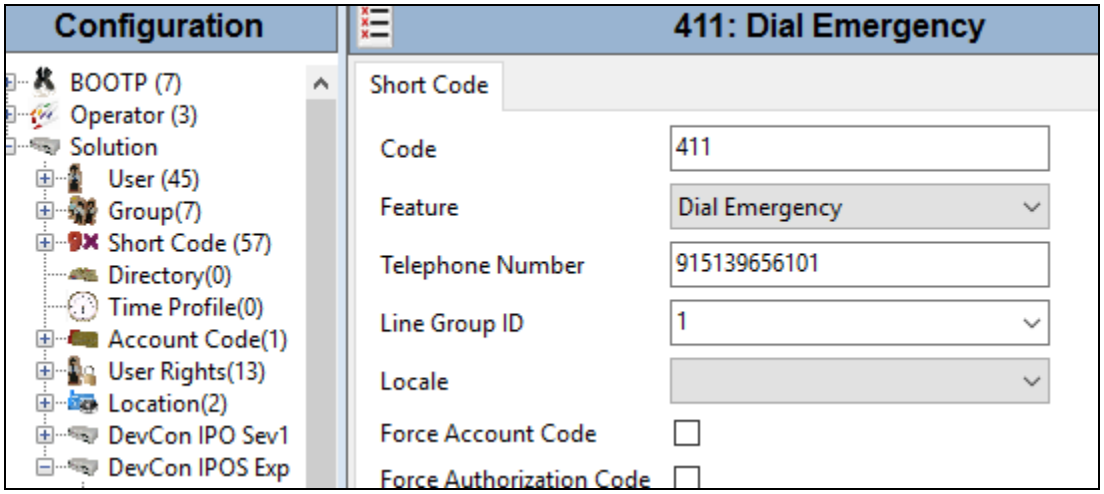
5.3. Administer Emergency Short Codes

From the configuration tree in the left pane, right-click on **Short Code** under the primary IP Office system, and select **New** from pop-up list to add a new short code for routing of emergency call, if not already defined and routable.

For **Code**, enter the digits that will be dialed for emergency calls, in this case "411". For **Feature**, select "Dial Emergency". Configure **Telephone Number** and **Line Group ID** as needed for proper routing of emergency calls to the PSTN, and retain the default values in the remaining fields.



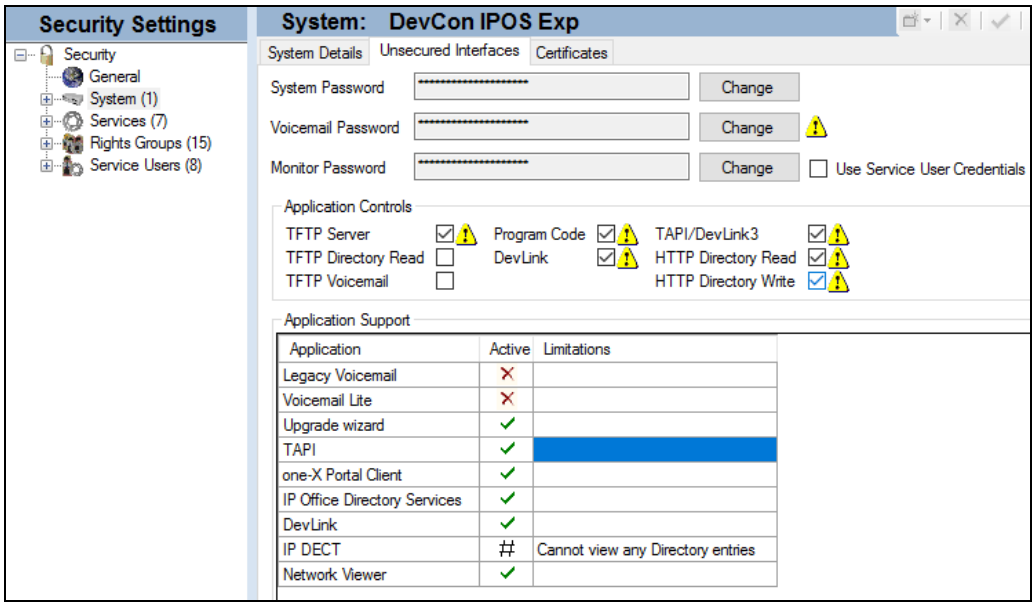
Repeat this section to add similar short code for the expansion IP Office system, as shown below.



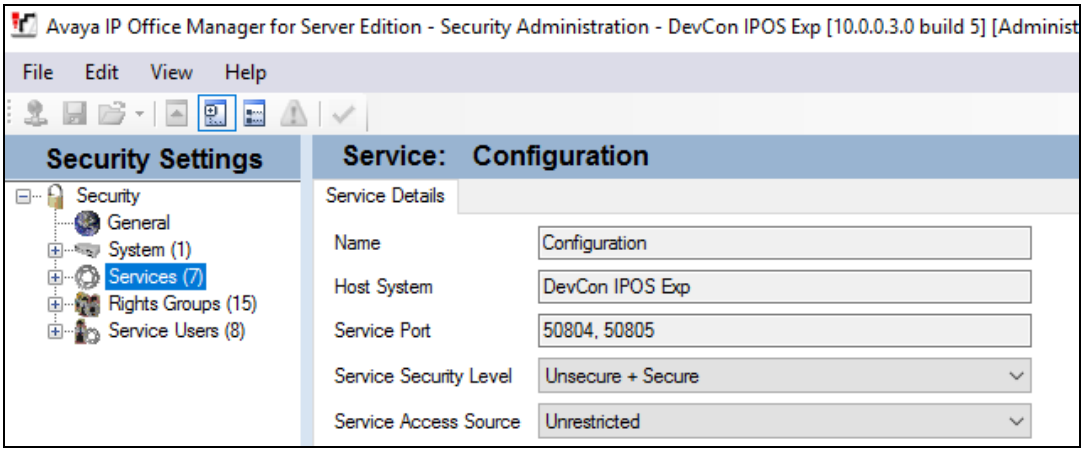
5.4. Administer Security Settings

This section is only applicable when OSN is configured with activated notifications feature to IP Office deskphones by placing a call using TAPI.

From the configuration tree in the left pane, select the IP Office system that will be used for TAPI and Configuration Web Service connection with Shadow OSN, in this case "**DevCon IPOS Exp**" (not shown), followed by **File → Advanced → Security Settings** from the top menu. The **Avaya IP Office Manager for Server Edition – Security Administration - DevCon IPOS Exp** screen is displayed, where **DevCon IPOS Exp** is the name of the selected IP Office system. Select **Security → System** to display the **System** screen in the right pane. Select the **Unsecured Interfaces** tab, and check **TAPI** as shown below.



Select **Security → Services** in the left pane to display the **Service: Configuration** screen in the right pane. For **Service Security Level**, select "Unsecure + Secure" as shown below. The additional "Secure" level is needed for the Configuration Web Service interface.



6. Configure Avaya 96xx IP Deskphones

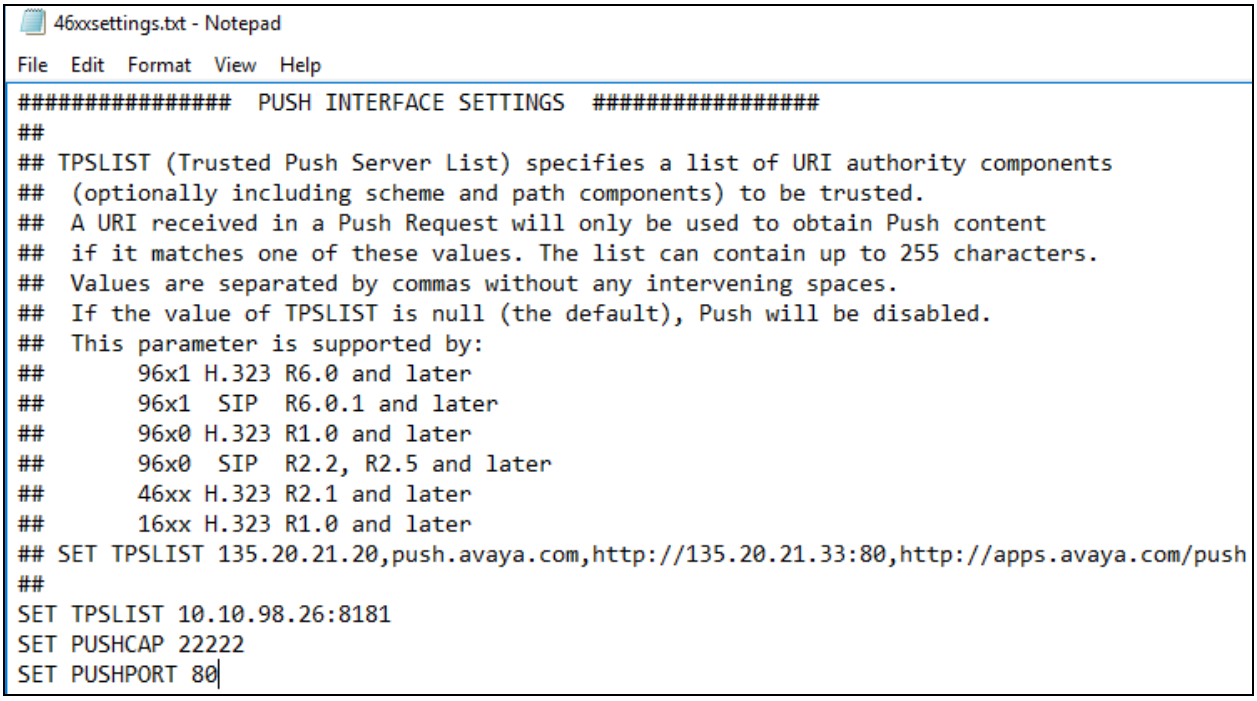
This section provides the procedures for configuring 96xx IP Deskphones. The procedures include the following areas:

- Administer phone parameters
- Reboot telephones

6.1. Administer Phone Parameters

From the file server serving the 96xx IP Deskphones, locate the **46xxsettings.txt** file and open with the desired application such as Notepad. Navigate to the **PUSH INTERFACE SETTINGS** sub-section.

Create a new line to set **TPSLIST** to the IP address of the Shadow OSN server, as shown below.



6.2. Reboot Telephones

After the Shadow OSN server has been configured in **Section 7**, manually reboot all 96xx IP Deskphones that will be used for emergency notifications, to pick up the new phone settings.

7. Configure RSI Shadow Onsite Notification

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

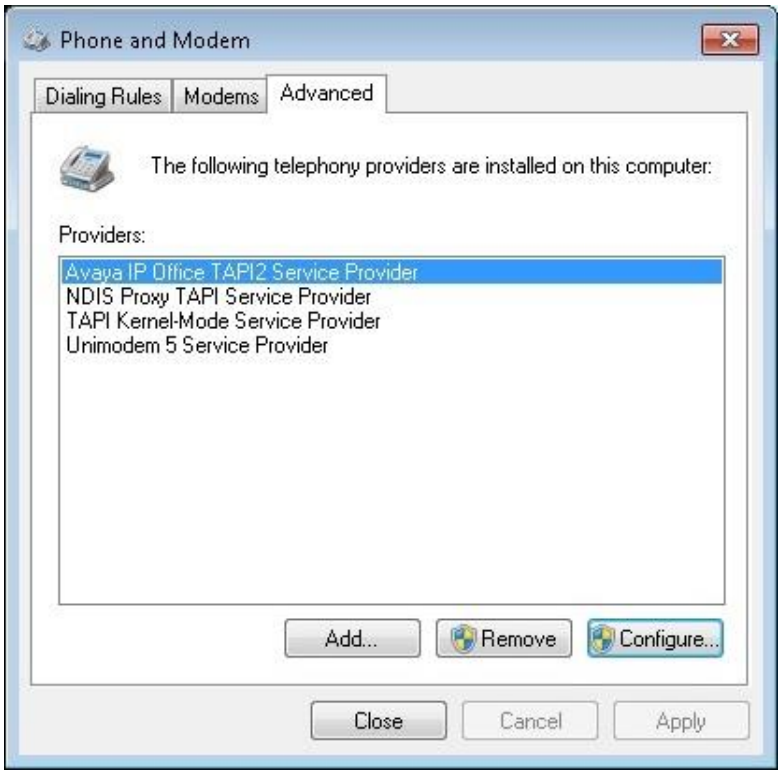
- Administer TAPI driver
- Launch Configuration Wizard
- Administer connection information
- Administer device location information
- Administer emergency options
- Administer 911 emergencies extensions
- Administer 911 emergencies IP phones
- Launch Onsite Notification

The configuration of Shadow OSN is typically performed by RSI Support Services. The procedural steps are presented in these Application Notes for informational purposes.

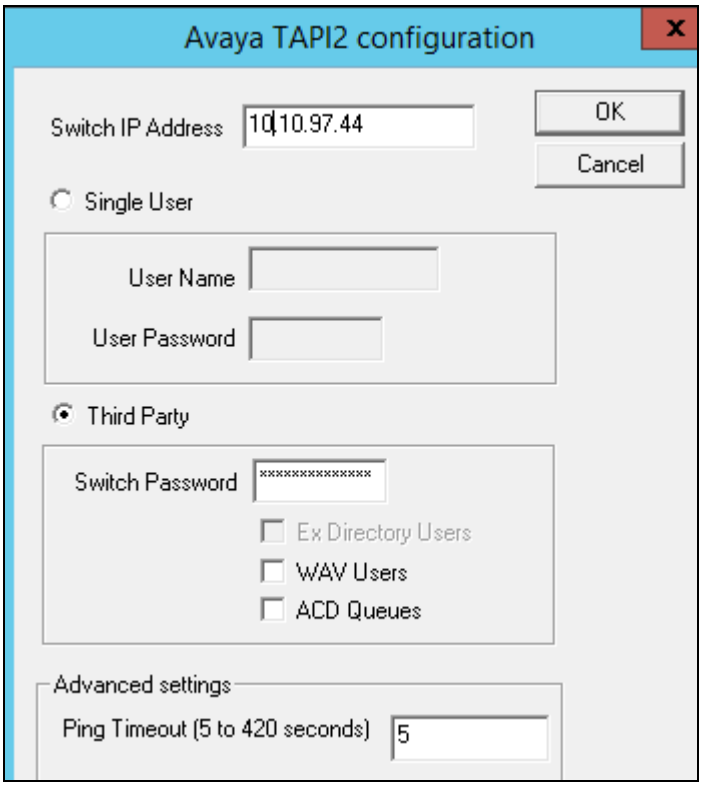
7.1. Administer TAPI Driver

From the Shadow OSN server, select **Start → Control Panel → Phone and Modem**, to display the **Phone and Modem** screen below.

Select the **Advanced** tab, followed by **Avaya IP Office TAPI2 Service Provider**, and click **Configure**.

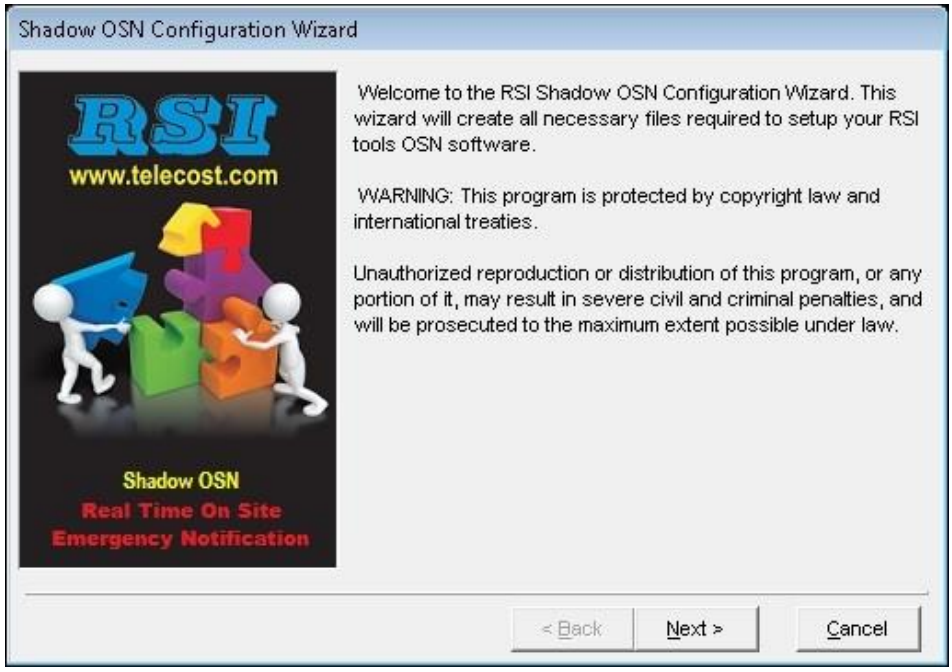


The **Avaya TAPI2 configuration** screen is displayed**.** For **Switch IP Address**, enter the IP address of the IP Office system that will be used for TAPI connectivity, in this case the expansion IP500V2 system. Select the radio button for **Third Party**, and enter the proper password for **Switch Password**. Reboot the Shadow OSN server.

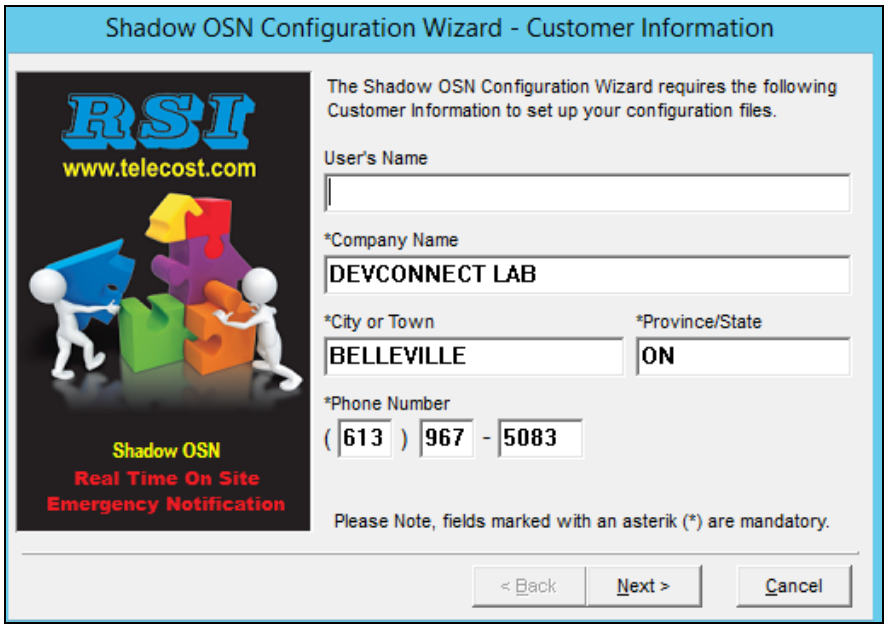


7.2. Launch Configuration Wizard

From the OSN server, select **Start → All Programs → RSI → Shadow OSN → Avaya → Configuration Wizard** to display the **Shadow OSN Configuration Wizard** screen. Click **Next**, and agree to the software license agreement in the next screen (not shown).

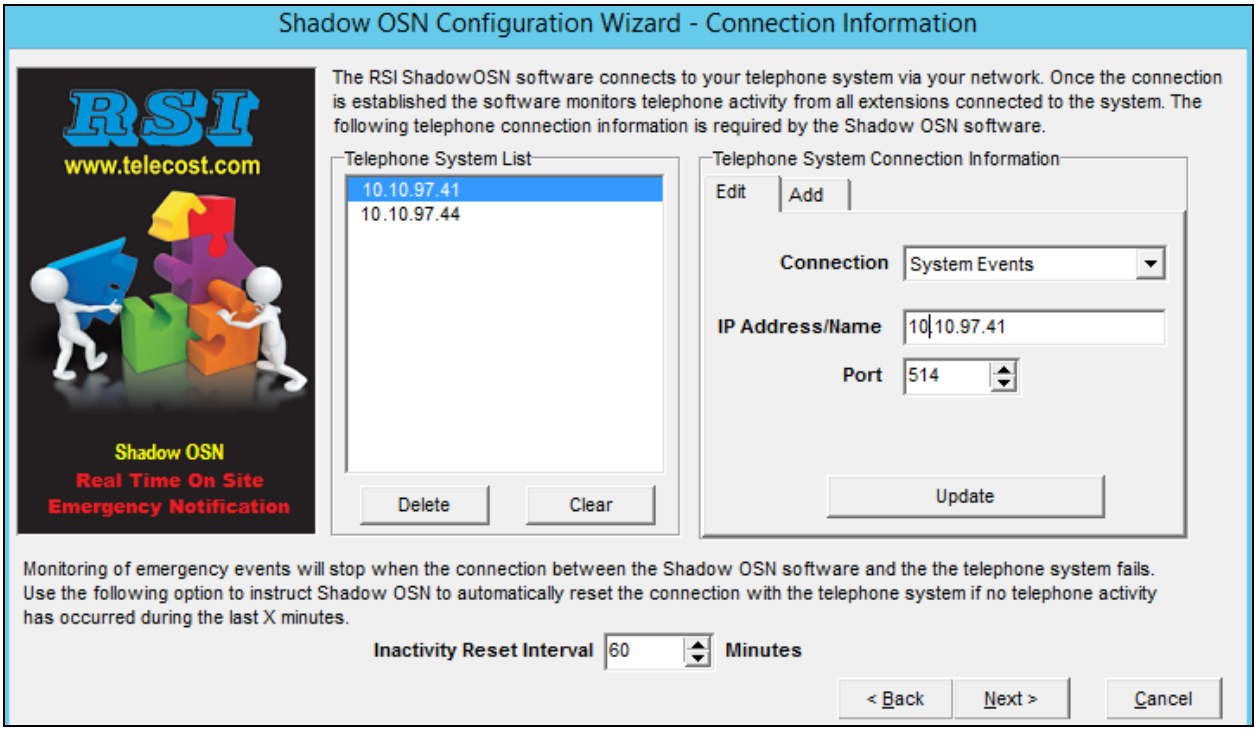


The **Customer Information** screen is displayed. Enter the pertinent customer information and click **Next**.

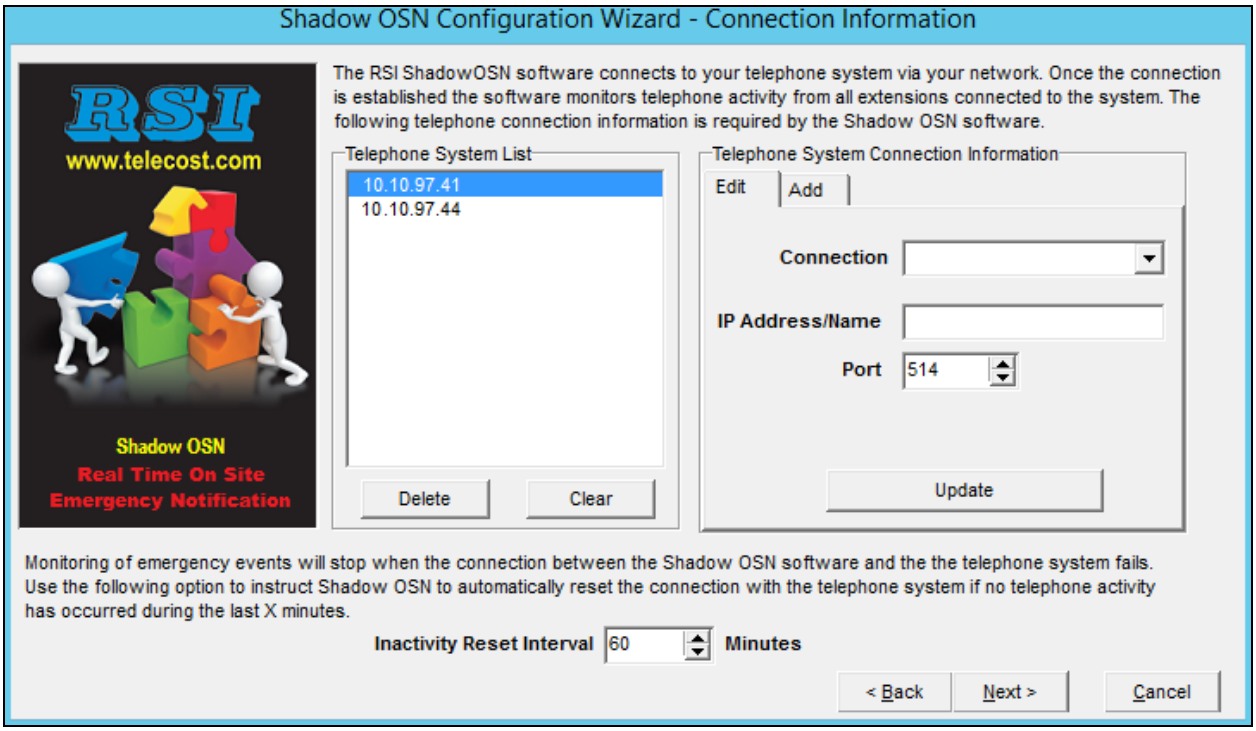


7.3. Administer Connection Information

The **Connection Information** screen is displayed next. In the **Add** tab under the **Telephone System Connection Information** sub-section, select "System Events", enter the IP address and pertinent credential for the primary IP Office system, and click **Add**.

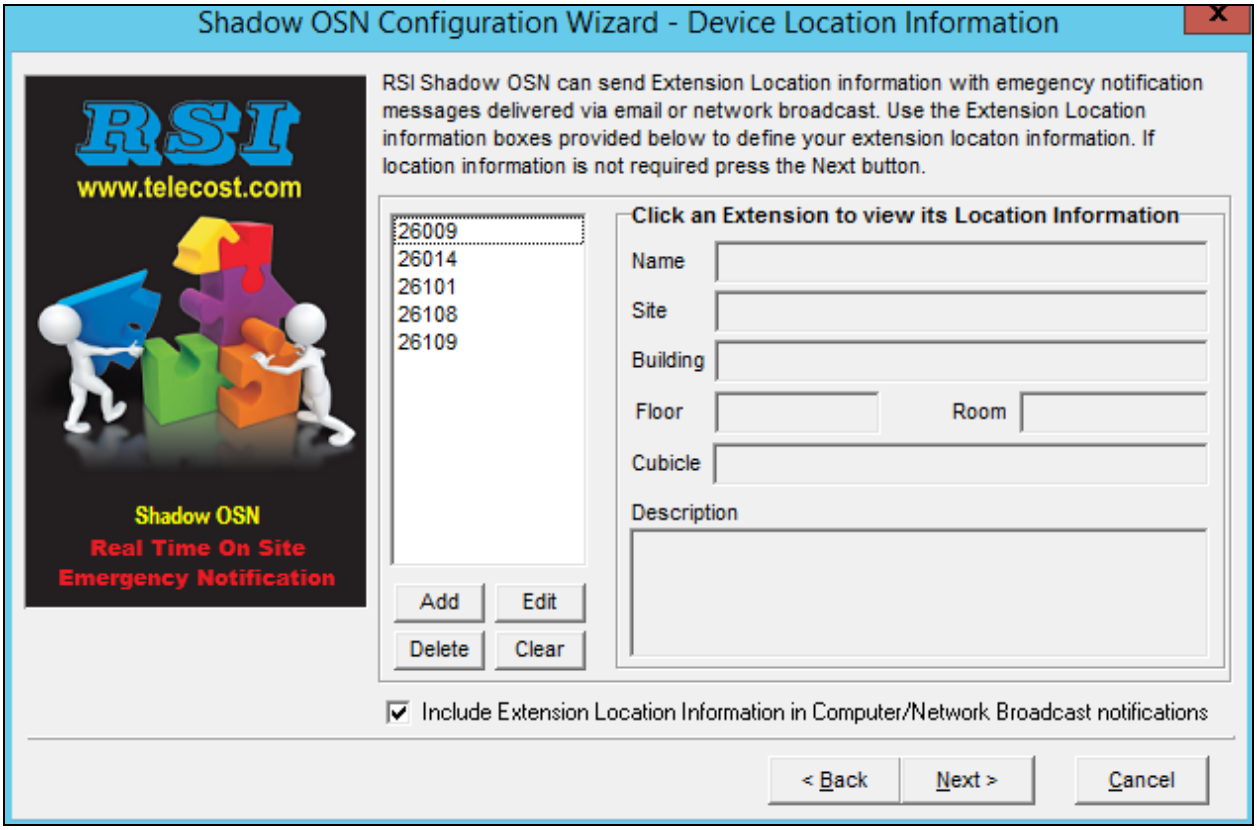


Repeat the same procedure to add a Syslog connection to the expansion IP Office system. The screenshot below shows the two added IP Office systems under the **Telephone System List** sub-section. Click **Next**, and retain all default values in the subsequent **Setup System Defaults** screen (not shown).



7.4. Administer Device Location Information

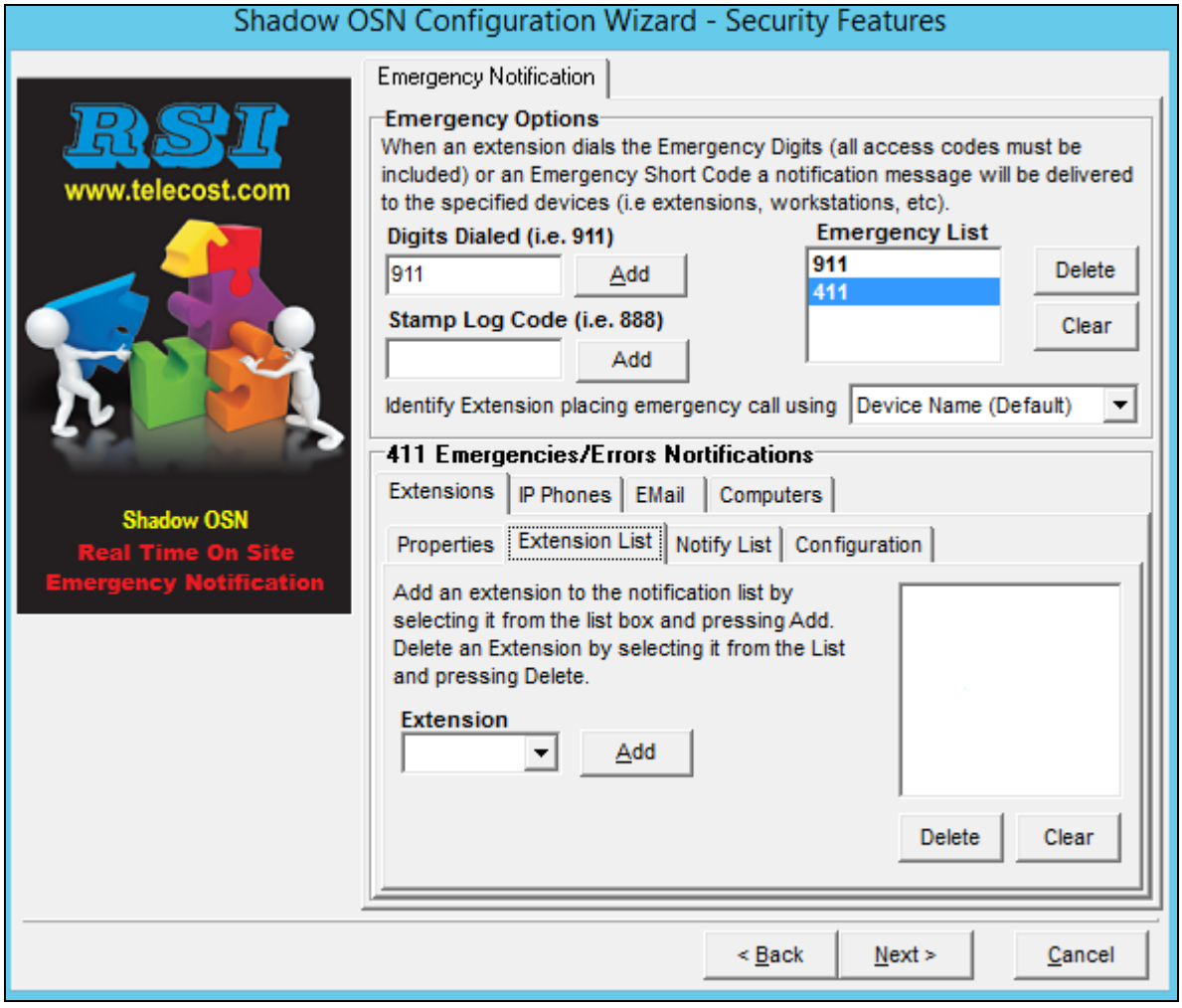
The **Device Location Information** screen is displayed next. Follow **reference [3]** to add an entry for each user and notification point on each IP Office system from **Section 3**. The screenshot below shows the entries created in the compliance testing.



7.5. Administer Emergency Options

The **Security Features** screen is displayed next. In the **Emergency Options** sub-section, enter the first set of digits that can be dialed for emergency calls in the **Digits Dialed** field and click **Add**. Repeat with additional set of dialed digits for emergency calls if applicable.

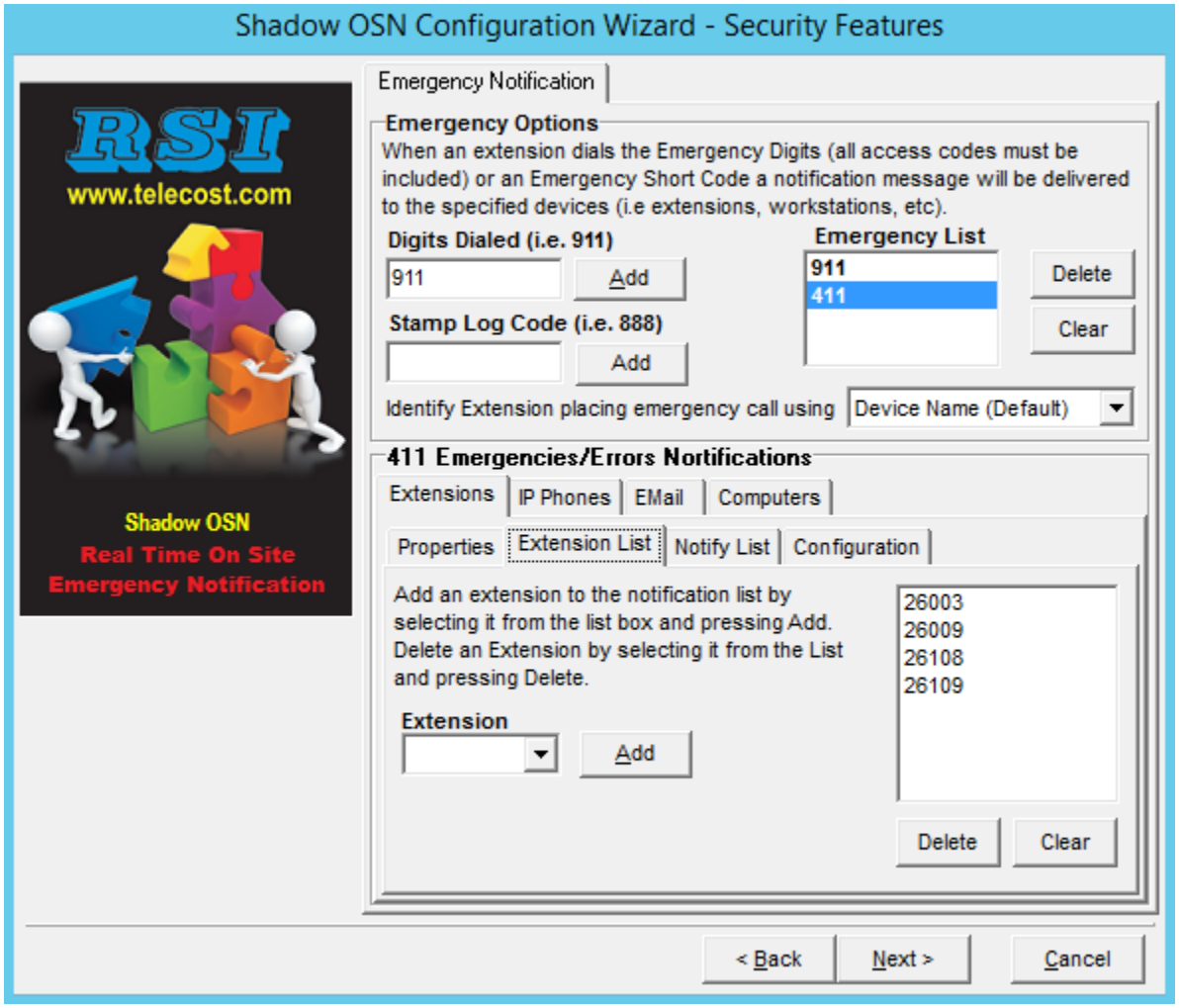
In the compliance testing, "411" was used as dialed digits for emergency calls, as shown under **Emergency List** in the screenshot below.



7.6. Administer 911 Emergencies Extensions

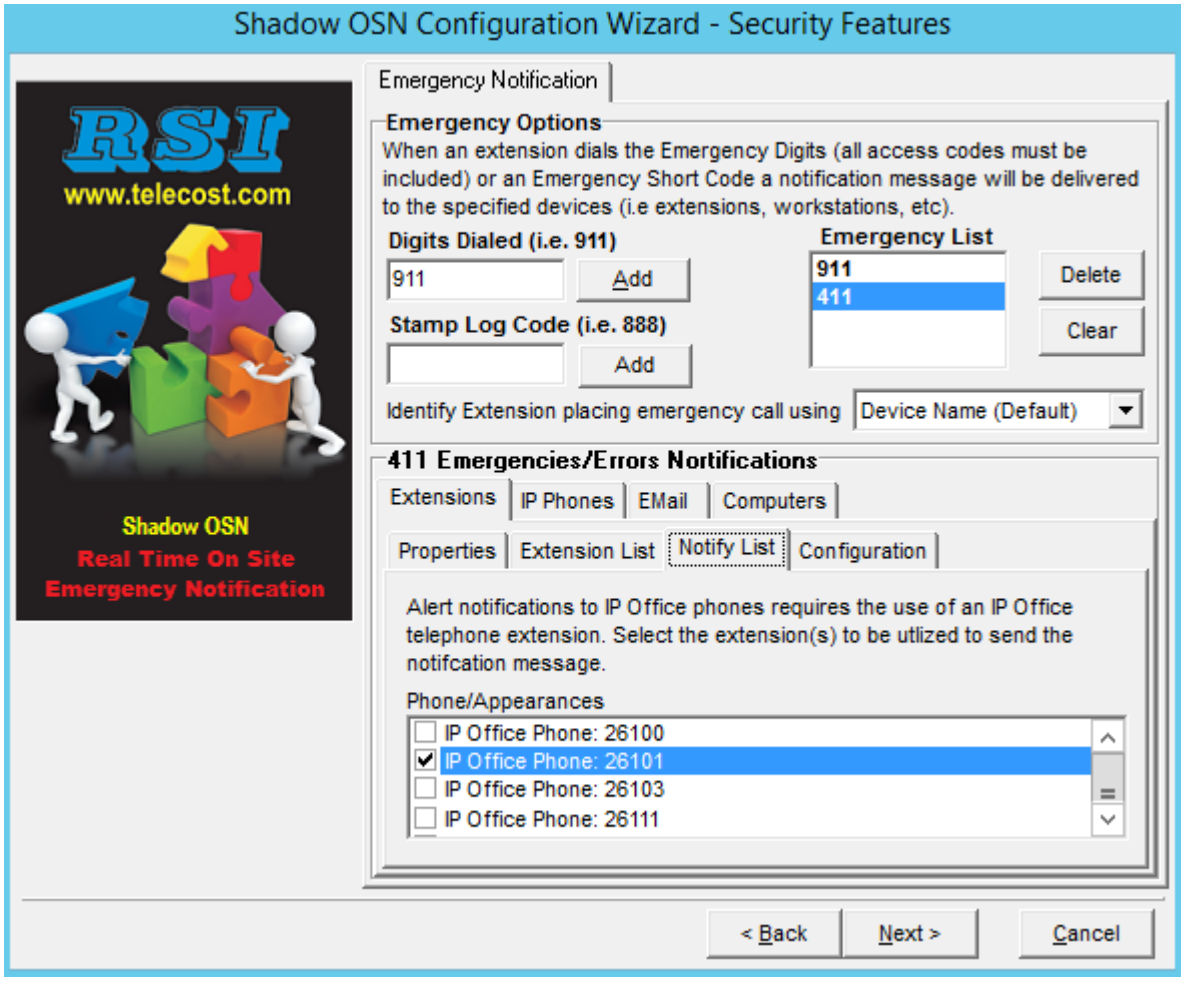
In the **911 Emergencies/Errors Notifications** sub-section, select the **Extensions** tab, followed by the **Extension List** sub-tab. For **Extension**, select the extension of each notification point from **Section 3**, and click **Add**.

In the compliance testing, below is list of notification points, as shown in the resultant screenshot below.



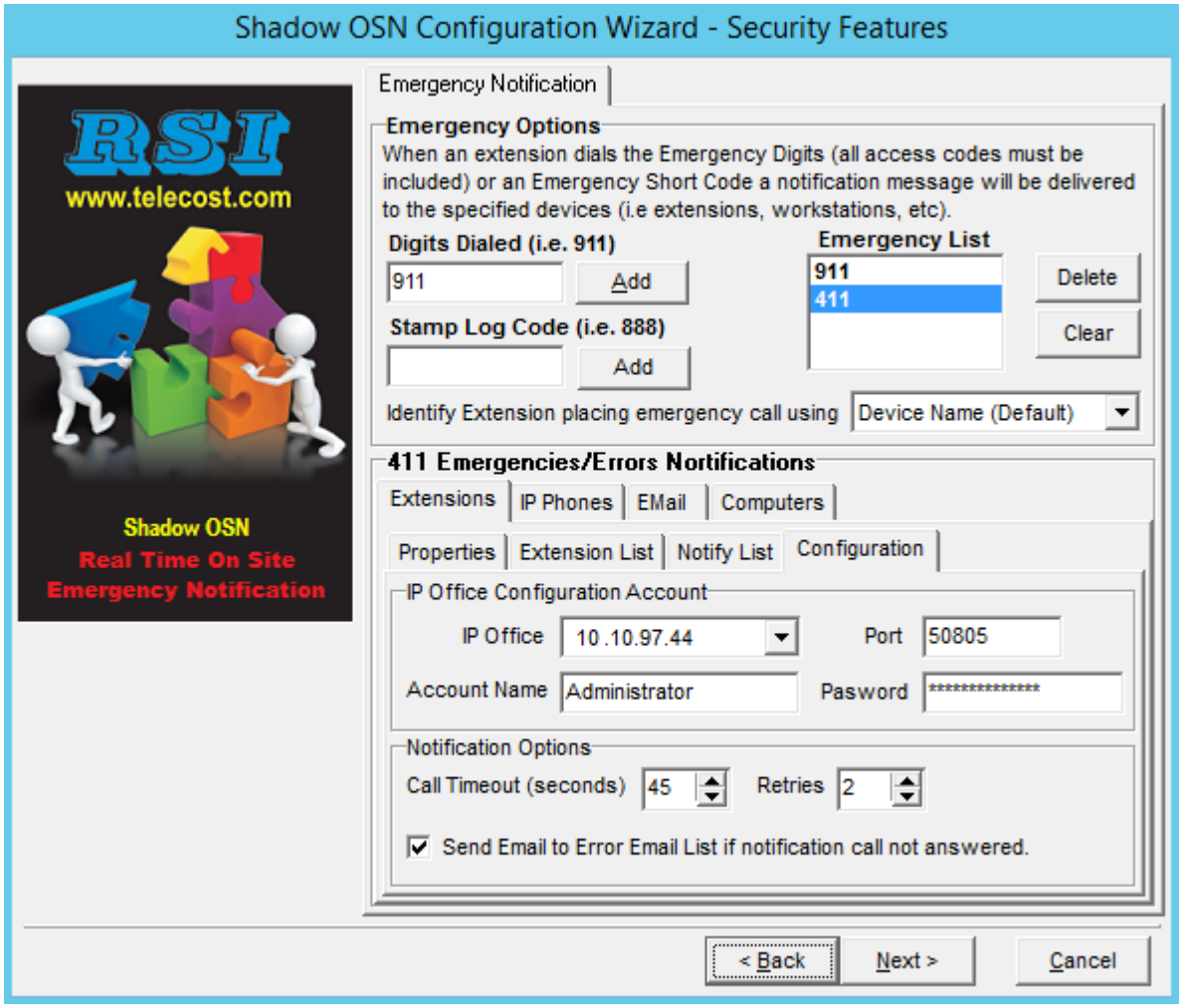
Select the **Notify List** sub-tab. Scroll the phone listing in the **Phone/Appearances** sub-section as necessary, which contains a listing of extensions picked up from the TAPI interface. Check all extensions from **Section 3** that will be used by Shadow OSN as TAPI notification originator for initiation of notification calls to digital notification points.

In the compliance testing, extension "26101" was used.



Select the **Configuration** sub-tab. For **IP Office**, **Account Name**, **Pasword**, select and enter pertinent information for the IP Office system used for Configuration Web Service connection, in this case the expansion IP Office system, as shown below. Retain the default values in the remaining fields.

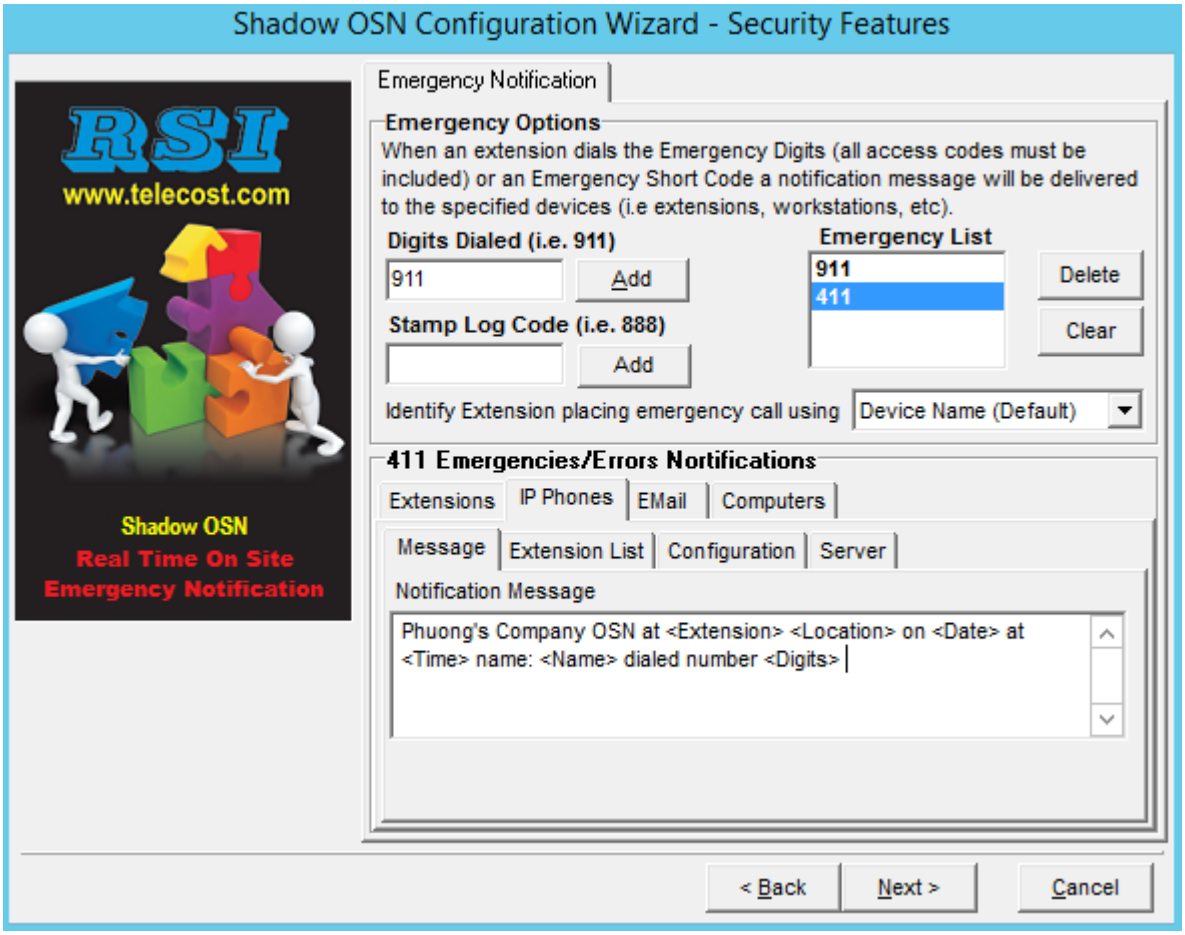
Note that the **Notification Options** parameters can be configured as desired.



7.7. Administer 911 Emergencies IP Phones

In the **911 Emergencies/Errors Notifications** sub-section, select the **IP Phones** tab, followed by the **Message** sub-tab. Follow **reference [3]** to configure the desired **Notification Message** that will be pushed to the IP notification points.

The message used in the compliance testing is shown below, which included the name and extension of the emergency caller, the current date, and the dialed digits.

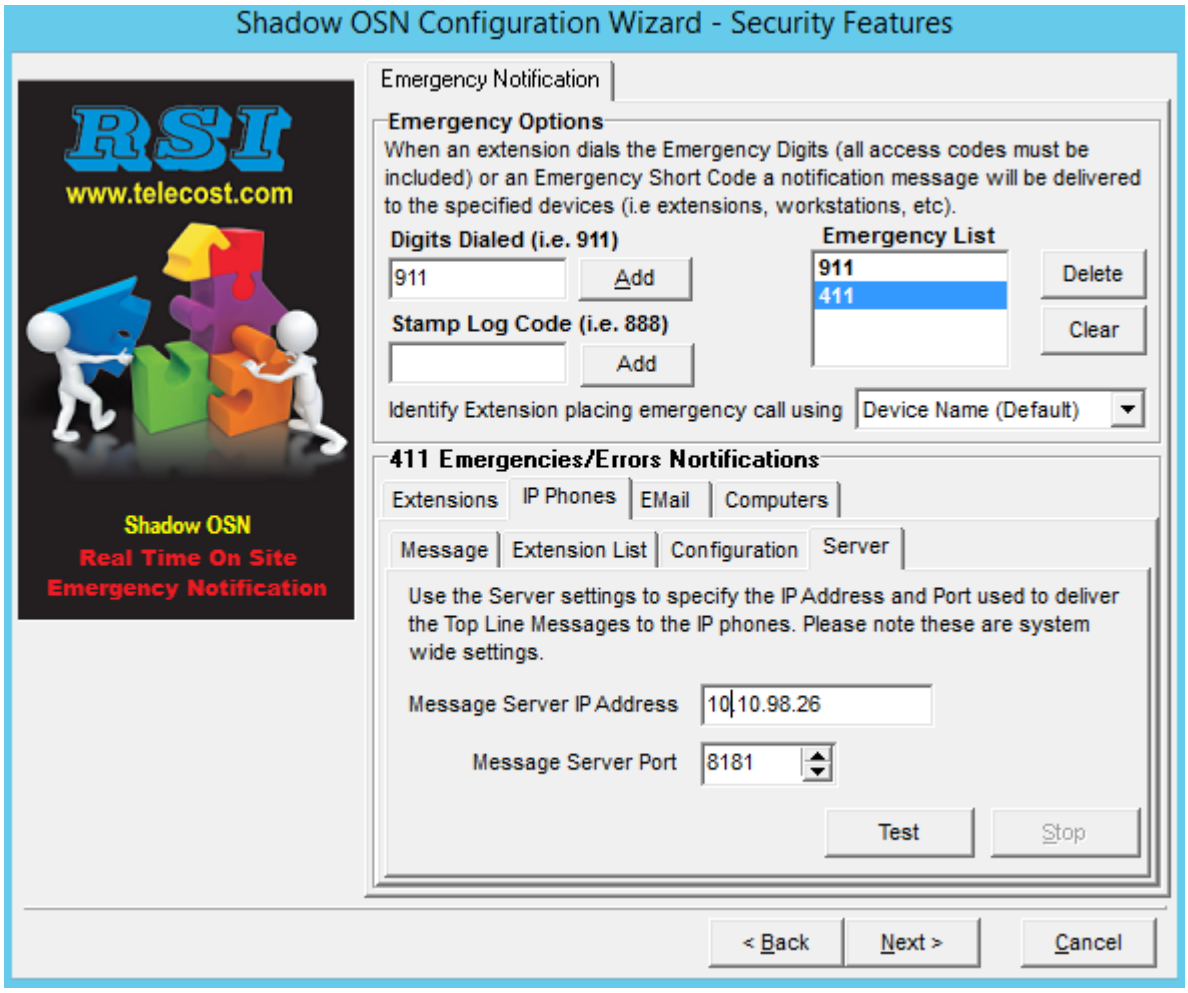


Select the **Extension List** sub-tab. For **Extension** and **IP Address**, enter the extension and IP address of each IP notification point from **Section 3**, and click **Add Phone to Notification List**.

In the compliance testing, four IP notification points were configured as shown in the resultant screenshot below.

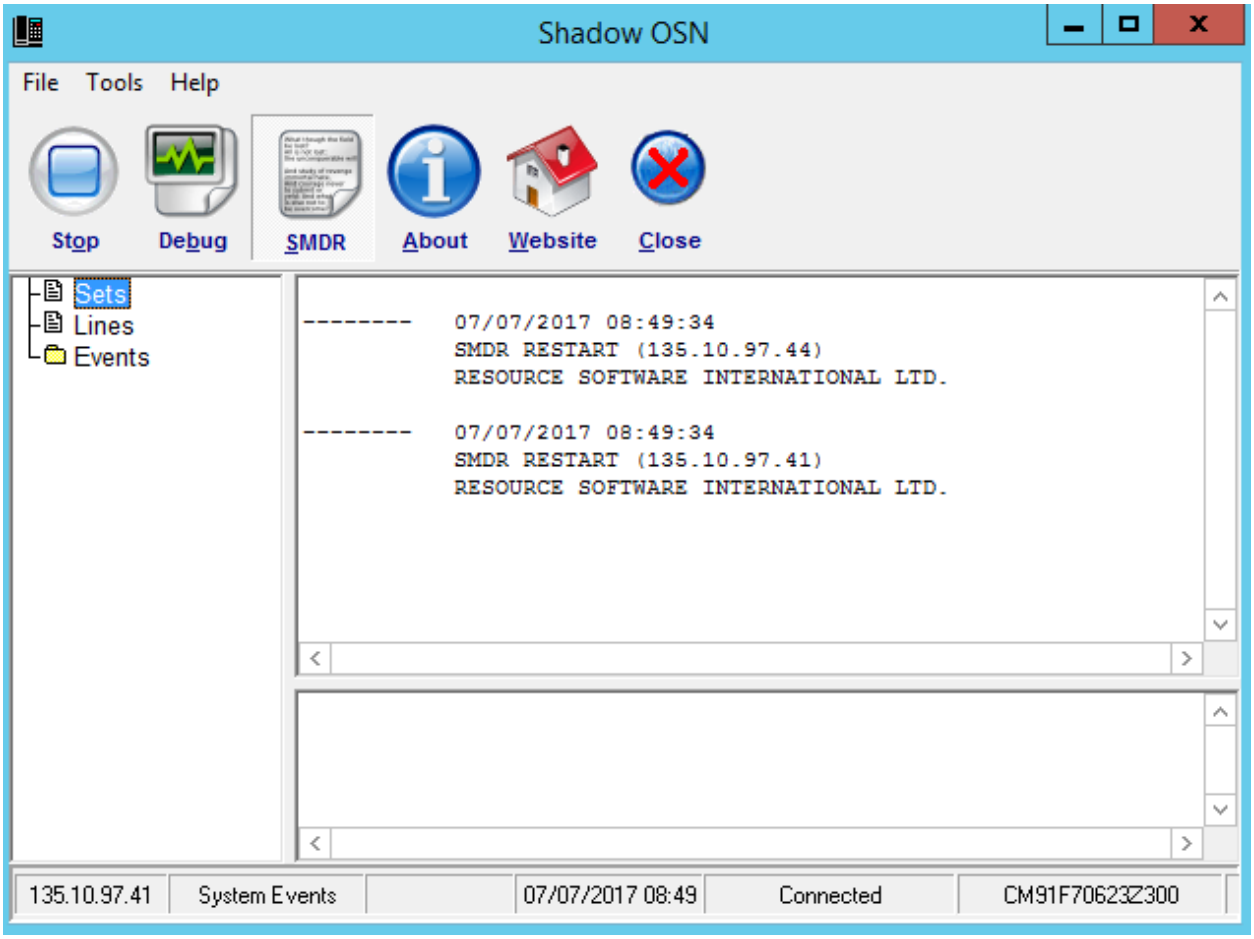
Select the **Server** sub-tab. For **Message Server IP Address**, enter the IP address of the Shadow OSN server. Retain the default values in the remaining fields.

Click **Next**, followed by **Finish** in the subsequent screen (not shown) to complete the Configuration Wizard.



7.8. Launch Onsite Notification

From the Shadow OSN server, select **Start → All Programs → RSI → Shadow OSN → Avaya → Onsite Notification** to display the **Shadow OSN** screen. Click **Start** to start the application, as shown below.



8. Verification Steps

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

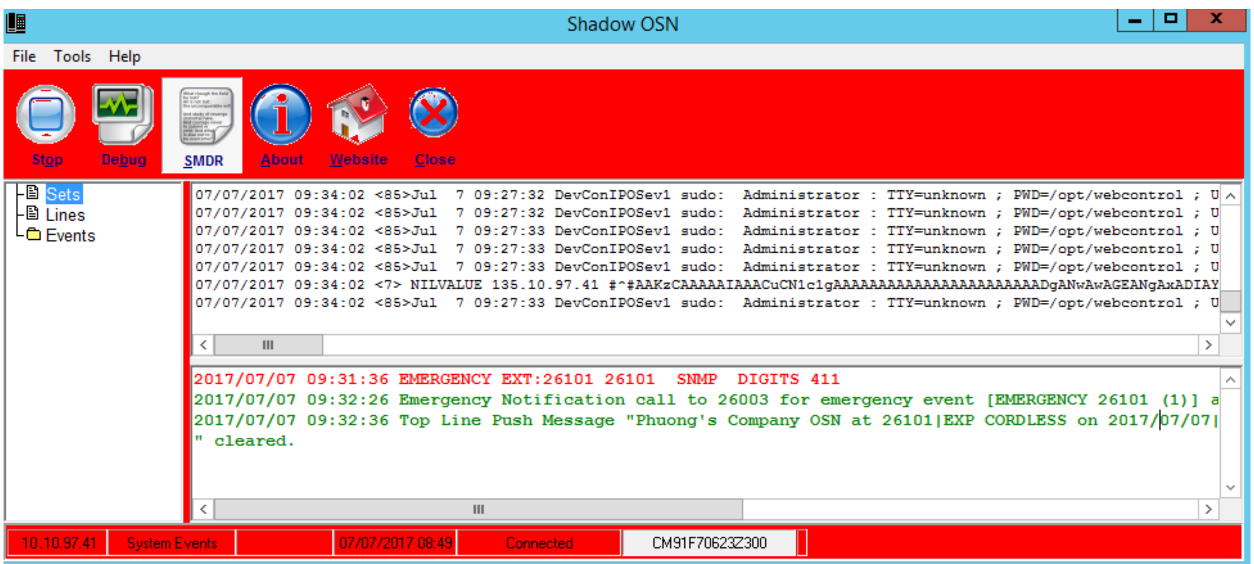
Establish an emergency 411 call from an IP Office user on the Main site with the PSTN.

Verify that all digital notification points from **Section 3** received a call alert, with display showing text "EMERGENCY" along with the extension of the emergency caller.

Verify that all IP notification points from **Section 3** received the push message containing the parameters defined in **Section 7.7**.

Also verify that the **Shadow OSN** screen on the Shadow OSN server showed the emergency call and the result of the alerts to the digital and IP notification points.

Repeat with an emergency call from an IP Office user on the Remote site, and verify similar notifications to the digital and IP notification points with pertinent information from the emergency caller. Also verify proper logging of the emergency call on the **Shadow OSN** screen, as shown below.



9. Conclusion

These Application Notes describe the configuration steps required for RSI Shadow OSN 2.3 to successfully interoperate with Avaya IP Office Server Edition 10. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

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

1. *Administering Avaya IP Office™ Platform with Manager*, Release 10.1, July 2017, available at http://support.avaya.com.

2. *Making Use of the Emergency Services Access Enhancements in IP Office Release 9.0/10*, available at http://www.devconnectprogram.com.

3. *Resource Software International Ltd. Shadow OSN for Avaya IP Office*, available from RSI Support.

4. *Description of Emergency Call Alarm Introduced in Release 10.0* available at http://www.devconnectprogram.com.

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.