



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

---

# **Application Notes for Resource Software International Shadow Onsite Notification 2.2 with Avaya IP Office Server Edition 9.1 – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for Resource Software International Shadow Onsite Notification 2.2 to interoperate with Avaya IP Office Server Edition 9.1.

Resource Software International Shadow Onsite Notification is an E911 notification solution that uses DevLink, 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) 2.2 to interoperate with Avaya IP Office Server Edition 9.1.

RSI Shadow OSN is an E911 notification solution that uses DevLink, 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 DevLink with the primary IP Office system to monitor users at the Main site, and DevLink 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 TAPI and DevLink event messages.
- Use of TAPI to originate notification calls from designated originating extensions (TAPI notification originator) on IP Office to designated digital 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 verified. The following were observations on Shadow OSN from the compliance testing.

- By design, the canceling of push notification via the designated short code from any user will stop the active push notification on all IP notification points.
- During resiliency, where IP endpoints on the expansion IP500V2 failed over and registered with the primary IP Office system, the push notification associated with a failed over emergency caller contained the name without the extension.
- The TAPI notification call to a digital notification point will take the designated TAPI notification originator telephone offhook, and therefore all call treatments and progress tones are played back on the telephone via the speaker.
- The secure port on the proper IP Office system is required to be configured correctly on IP Office for the application to start up. In the rare event that the secure port on IP Office is disabled by the administrator, then the application can lock up with emergency monitoring ceased.

## 2.3. Support

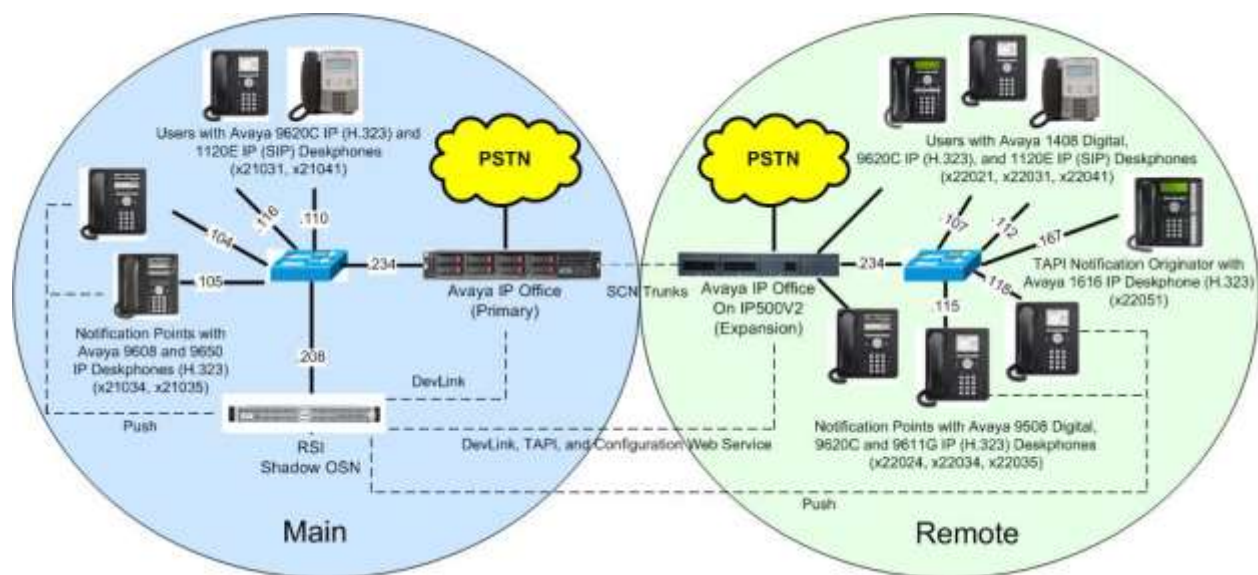
Technical support on Shadow OSN can be obtained through the following:

- **Phone:** (800) 891-6014
- **Email:** [support@telecost.com](mailto:support@telecost.com)
- **Web:** [www.telecost.com](http://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 DevLink connection to the primary IP Office system, with DevLink, 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
<b>Main Site</b>	
Avaya IP Office Server Edition (Primary) in Virtual Environment	9.1.400.137
Avaya 9620C & 9650 IP Deskphones (H.323)	3.250A
Avaya 9608 IP Deskphone (H.323)	6.6029
Avaya 1120E IP Deskphone (SIP)	4.4.18.0
RSI Shadow Onsite Notification on Windows 7 Enterprise <ul style="list-style-type: none"><li>Avaya DevLink (devlink.dll)</li></ul>	2.2.0.002 SP1 1.0.0.5
<b>Remote Site</b>	
Avaya IP Office on IP500 V2 (Expansion)	9.1.400.137
Avaya 1616 IP Deskphone (H.323)	1.350B
Avaya 9620C IP Deskphones (H.323)	3.250A
Avaya 9611G IP Deskphone (H.323)	6.6029
Avaya 1120E IP Deskphone (SIP)	4.4.18.0
Avaya 1408 & 9508 Digital Deskphones	NA
RSI Shadow Onsite Notification on Windows 7 Enterprise <ul style="list-style-type: none"><li>Avaya DevLink (devlink.dll)</li><li>Avaya IP Office TAPI2 Driver (tspi2w_64.tsp)</li><li>Avaya IP Office Configuration Web Service SDK</li></ul>	2.2.0.002 SP1 1.0.0.5 1.0.0.42 9.1

*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:

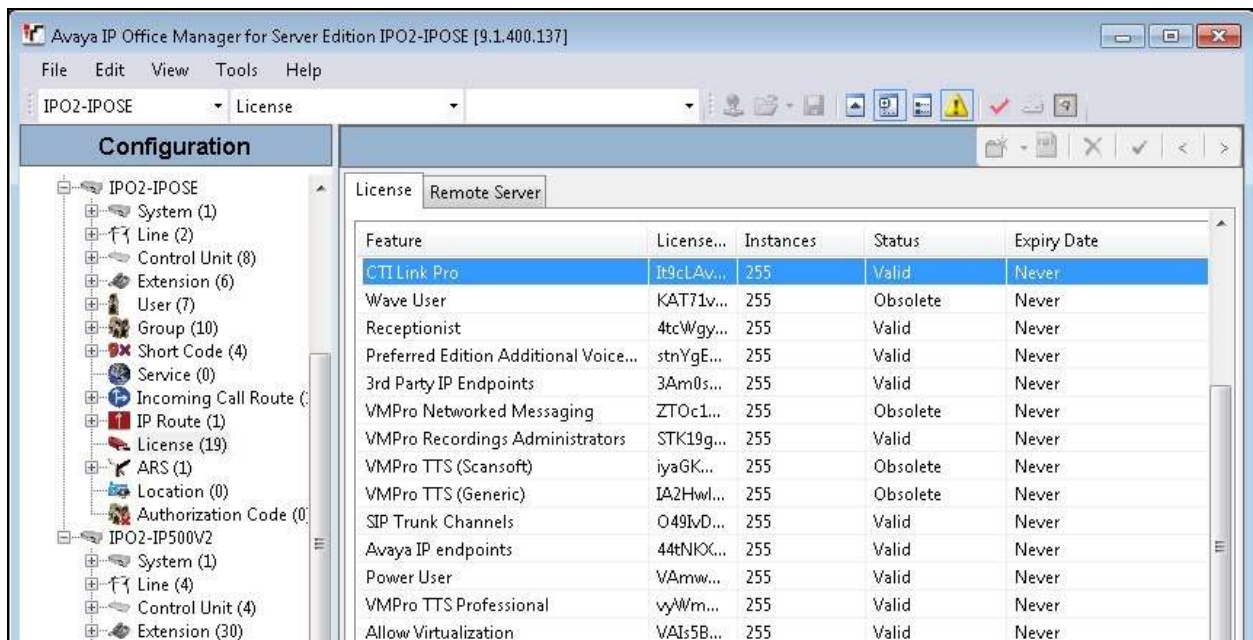
- Verify licenses
- Administer cancel notification short code
- Administer emergency short codes
- Administer security settings

### 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 IPO2-IPOSE** screen is displayed, where **IPO2-IPOSE** is the name of the primary IP Office system.

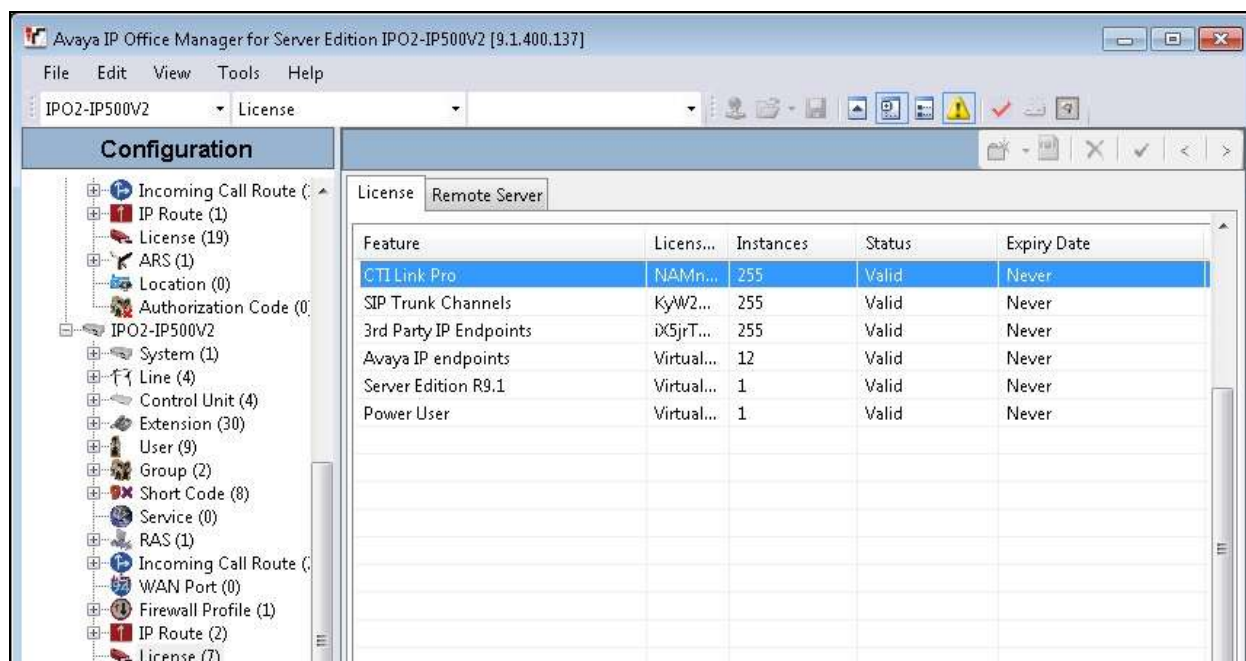
From the configuration tree in the left pane, select **License** under the primary IP Office system, in this case “IPO2-IPOSE”, to display a list of licenses in the right pane. Verify that there is a license for **CTI Link Pro** and that the **Status** is “Valid”, as shown below. This license is needed for the DevLink connection with Shadow OSN.



Feature	License...	Instances	Status	Expiry Date
CTI Link Pro	It9cLAv...	255	Valid	Never
Wave User	KAT71v...	255	Obsolete	Never
Receptionist	4tcWgy...	255	Valid	Never
Preferred Edition Additional Voice...	stnYgE...	255	Valid	Never
3rd Party IP Endpoints	3Am0s...	255	Valid	Never
VMPro Networked Messaging	ZTOc1...	255	Obsolete	Never
VMPro Recordings Administrators	STK19g...	255	Valid	Never
VMPro TTS (Scansoft)	iyaGK...	255	Obsolete	Never
VMPro TTS (Generic)	IA2Hwl...	255	Obsolete	Never
SIP Trunk Channels	O49IvD...	255	Valid	Never
Avaya IP endpoints	44tNKK...	255	Valid	Never
Power User	VAmw...	255	Valid	Never
VMPro TTS Professional	vyWm...	255	Valid	Never
Allow Virtualization	VAIs5B...	255	Valid	Never



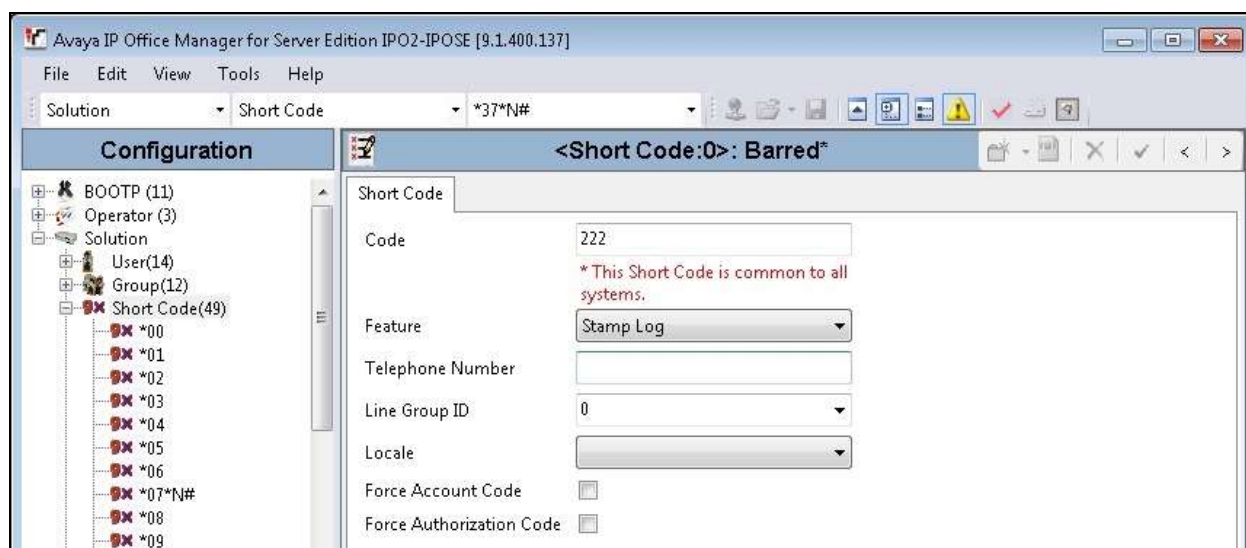
From the configuration tree in the left pane, select **License** under the expansion IP Office system, in this case “IPO2-IP500V2”, to display a list of licenses in the right pane. Verify that there is a license for **CTI Link Pro** and that the **Status** is “Valid”, as shown below. This license is needed for the DevLink and TAPI connections with Shadow OSN.



## 5.2. Administer Cancel Notification Short Code

From the configuration tree in the left pane, right-click on **Solution** → **Short Code** and select **New** from pop-up list to add a new common short code for canceling of push notifications.

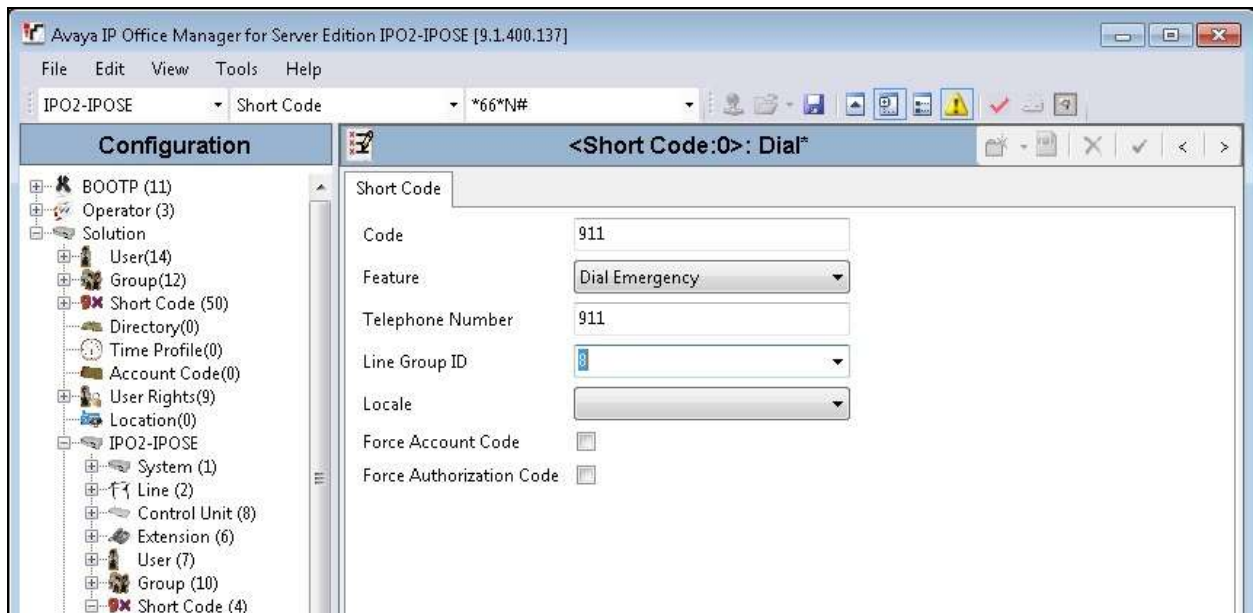
For **Code**, enter a desired value. For **Feature**, select a less pervasive feature, such as “Stamp Log” as recommended by RSI. Retain the default values in the remaining fields.



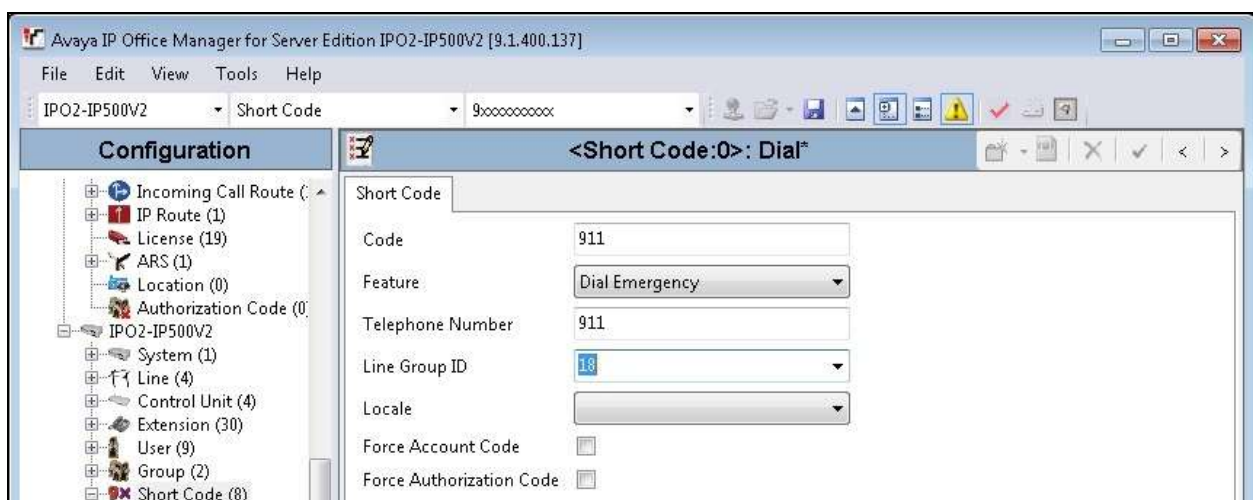
### 5.3. Administer Emergency Short Codes

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 “911”. 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.



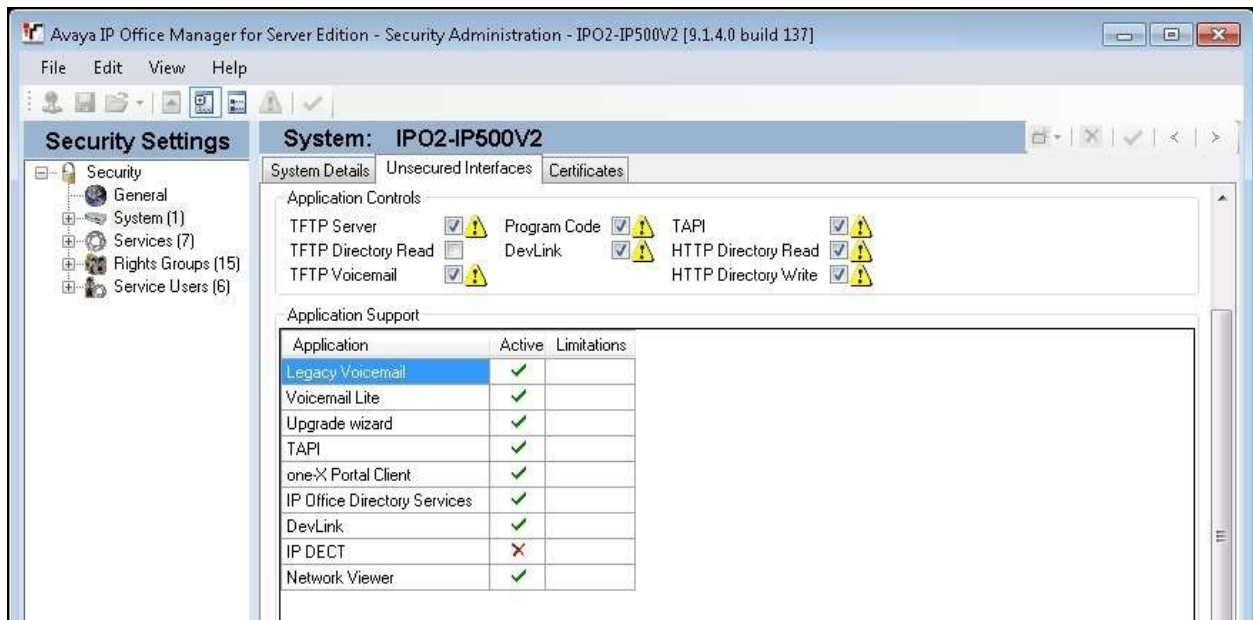
Repeat this section to add similar short code for the expansion IP Office system, as shown below.



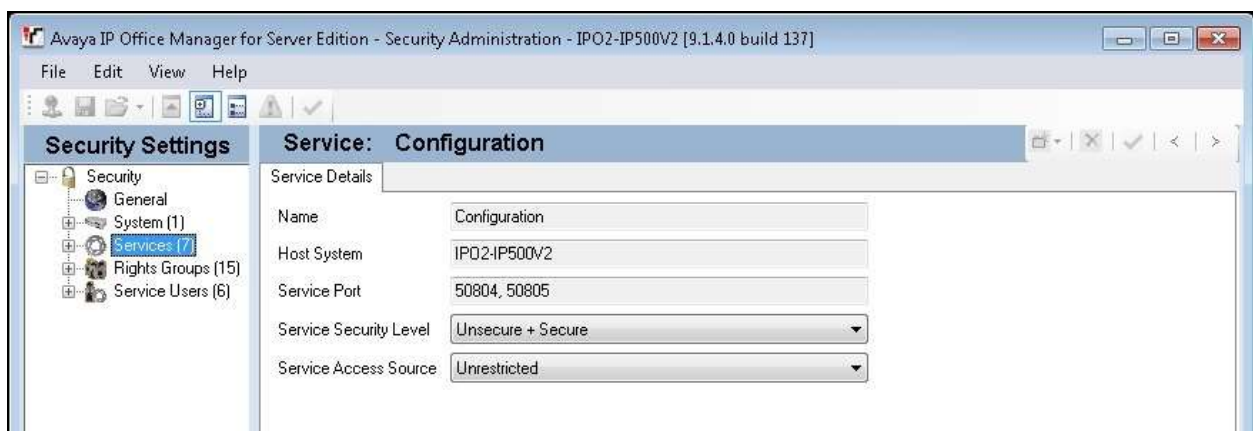
## 5.4. Administer Security Settings

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 “IPO2-IP500V2” (not shown), followed by **File → Advanced → Security Settings** from the top menu.

The **Avaya IP Office Manager for Server Edition – Security Administration - IPO2-IP500V2** screen is displayed, where **IPO2-IP500V2** 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.



```
##
##### PUSH INTERFACE SETTINGS #####
##
## TPSLIST (Trusted Push Server List) specifies a list of URI authority components
## (optionally including scheme and path components) to be trusted.
## A URI received in a Push Request will only be used to obtain Push content
## if it matches one of these values. The list can contain up to 255 characters.
## values are separated by commas without any intervening spaces.
## If the value of TPSLIST is null (the default), Push will be disabled.
## This parameter is supported by:
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.0.1 and later
## 96x0 H.323 R1.0 and later
## 96x0 SIP R2.2, R2.5 and later
## 46xx H.323 R2.1 and later
## 16xx H.323 R1.0 and later
## SET TPSLIST 135.20.21.20,push.avaya.com,http://135.20.21.33:80,http://apps.avaya.com/push
SET TPSLIST 10.64.101.208
##
```

### 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

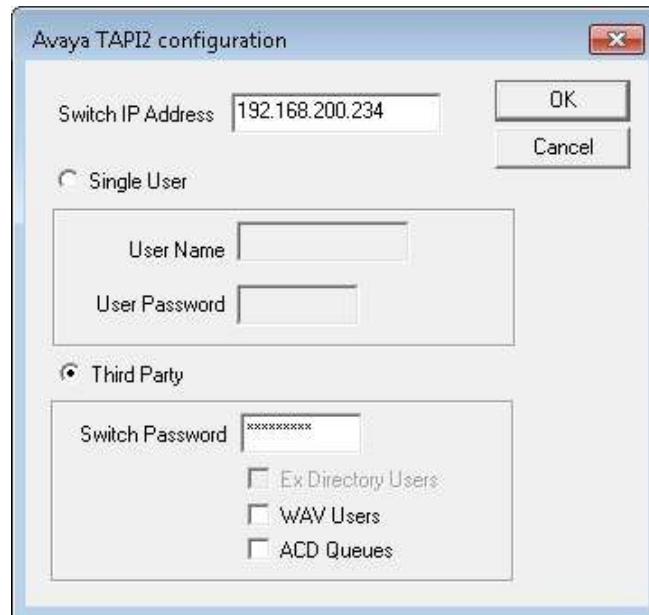
From the Shadow OSN server, select **Start → Control Panel → Phone and Modem**, to display the **Phone and Modem** screen below.

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





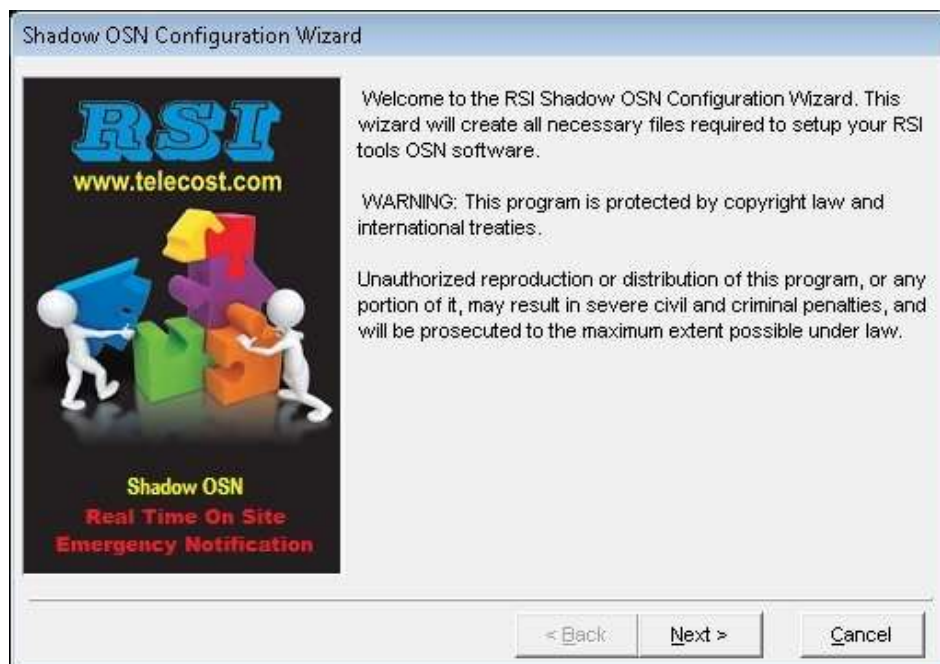
The **Avaya TAPI2 configuration** screen is displayed. For **Switch IP Address**, enter the IP address of the IP Office system that will be used for TAPI connectivity, in this case the expansion IP500V2 system. Select the radio button for **Third Party**, and enter the proper password for **Switch Password**.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



The image shows a Windows-style dialog box titled "Avaya TAPI2 configuration". It has a "Switch IP Address" text box containing "192.168.200.234". To the right are "OK" and "Cancel" buttons. Below is a section with two radio buttons: "Single User" (unselected) and "Third Party" (selected). Under "Single User" are "User Name" and "User Password" text boxes. Under "Third Party" is a "Switch Password" text box containing "XXXXXXXX", and three unchecked checkboxes: "Ex Directory Users", "WAV Users", and "ACD Queues".

## 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 image shows a window titled "Shadow OSN Configuration Wizard". On the left is a graphic with the "RSI" logo, the website "www.telecost.com", and the text "Shadow OSN Real Time On Site Emergency Notification" above an illustration of two figures with puzzle pieces. On the right, the text reads: "Welcome to the RSI Shadow OSN Configuration Wizard. This wizard will create all necessary files required to setup your RSI tools OSN software." followed by a "WARNING: This program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law." At the bottom are "< Back", "Next >", and "Cancel" buttons.

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

The screenshot shows the 'Shadow OSN Configuration Wizard - Customer Information' window. On the left is a logo for RSI (www.telecost.com) with the text 'Shadow OSN Real Time On Site Emergency Notification'. The main area contains the following fields: 'User's Name' with the value 'OSN'; '\*Company Name' with the value 'DEVCONNECT'; '\*City or Town' with the value 'BASKING RIDGE'; '\*Province/State' with the value 'NJ'; and '\*Phone Number' with the value '( 908 ) 848 - 5601'. A note at the bottom states: 'Please Note, fields marked with an asterik (\*) are mandatory.' At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

### 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 “DevLink”, enter the IP address and pertinent credential for the primary IP Office system, and click **Add**.

The screenshot shows the 'Shadow OSN Configuration Wizard - Connection Information' window. On the left is the same RSI logo as in the previous screen. The main area contains a 'Telephone System List' table (currently empty) with 'Delete' and 'Clear' buttons below it. To the right is the 'Telephone System Connection Information' section with 'Edit' and 'Add' tabs. The 'Add' tab is active, showing fields for 'Connection' (set to 'DevLink'), 'IP Address/Name' (set to '10.64.101.234'), and 'Password' (masked with asterisks). An 'Add' button is at the bottom of this section. Below these sections, a note states: 'Monitoring of emergency events will stop when the connection between the Shadow OSN software and the the telephone system fails. Use the following option to instruct Shadow OSN to automatically reset the connection with the telephone system if no telephone activity has occurred during the last X minutes.' Below this note is a field for 'Inactivity Reset Interval' set to '60' with a 'Minutes' label. At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

Repeat the same procedure to add a DevLink 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).

Shadow OSN Configuration Wizard - Connection Information

The RSI ShadowOSN software connects to your telephone system via your network. Once the connection is established the software monitors telephone activity from all extensions connected to the system. The following telephone connection information is required by the Shadow OSN software.

**Telephone System List**

10.64.101.234
192.168.200.234

Delete Clear

**Telephone System Connection Information**

Edit Add

Connection

IP Address/Name

Port 514

Password

Add

Monitoring of emergency events will stop when the connection between the Shadow OSN software and the the telephone system fails. Use the following option to instruct Shadow OSN to automatically reset the connection with the telephone system if no telephone activity has occurred during the last X minutes.

Inactivity Reset Interval 60 Minutes

< Back Next > Cancel



## 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.

Shadow OSN Configuration Wizard - Device Location Information

RSI  
www.telecost.com

Shadow OSN  
Real Time On Site  
Emergency Notification

RSI Shadow OSN can send Extension Location information with emergency notification messages delivered via email or network broadcast. Use the Extension Location information boxes provided below to define your extension location information. If location information is not required press the Next button.

21031  
21034  
21035  
21041  
22021  
22024  
22031  
22034  
22035  
22041

Add Edit  
Delete Clear

**Click an Extension to view its Location Information**

Name  
Site  
Building  
Floor Room  
Cubicle  
Description

☐ Include Extension Location Information in Computer/Network Broadcast notifications

< Back Next > Cancel

## 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, “911” was used as dialed digits for emergency calls, as shown under **Emergency List** in the screenshot below.

The screenshot shows the 'Shadow OSN Configuration Wizard - Security Features' window. On the left is a logo for RSI (www.telecost.com) with the text 'Shadow OSN Real Time On Site Emergency Notification'. The main area is titled 'Emergency Notification' and contains two sub-sections:

- Emergency Options**: This section explains that when an extension dials emergency digits, a notification message will be delivered to specified devices. It includes fields for 'Digits Dialed (i.e. 911)' and 'Stamp Log Code (i.e. 888)', each with an 'Add' button. There is also an 'Emergency List' with a table containing the entry '911' and buttons for 'Delete' and 'Clear'. A dropdown menu for 'Identify Extension placing emergency call using' is set to 'Device Name (Default)'.
- 911 Emergencies/Errors Notifications**: This section has tabs for 'Extensions', 'IP Phones', 'Email', and 'Computers'. Under the 'Extensions' tab, there are sub-tabs for 'Properties', 'Extension List', 'Notify List', and 'Configuration'. The 'Extension List' sub-tab is active, showing instructions to add or delete extensions from the notification list. It includes an 'Extension' dropdown menu with an 'Add' button, and 'Delete' and 'Clear' buttons at the bottom right.

At the bottom of the window are navigation buttons: '< Back', 'Next >', and 'Cancel'.

## 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 digital notification point from **Section 3**, and click **Add**.

In the compliance testing, “22024” was the only digital notification point, as shown in the resultant screenshot below.

The screenshot shows the 'Shadow OSN Configuration Wizard - Security Features' window. The 'Emergency Notification' tab is selected. On the left is a logo for RSI (www.telecost.com) with the text 'Shadow OSN Real Time On Site Emergency Notification'. The main area is divided into two sections. The top section, 'Emergency Options', contains fields for 'Digits Dialed (i.e. 911)' and 'Stamp Log Code (i.e. 888)', each with an 'Add' button. To the right is an 'Emergency List' with a table containing the value '911' and buttons for 'Delete' and 'Clear'. Below this is a dropdown menu for 'Identify Extension placing emergency call using' set to 'Device Name (Default)'. The bottom section, '911 Emergencies/Errors Notifications', has sub-tabs for 'Extensions', 'IP Phones', 'Email', and 'Computers'. The 'Extensions' sub-tab is active, and within it, the 'Extension List' sub-tab is selected. It contains instructions: 'Add an extension to the notification list by selecting it from the list box and pressing Add. Delete an Extension by selecting it from the List and pressing Delete.' Below the instructions is an 'Extension' dropdown menu with an 'Add' button. To the right is a list box containing the value '22024', with 'Delete' and 'Clear' buttons below it. At the bottom of the window are '< Back', 'Next >', and 'Cancel' buttons.

Select the **Notify List** sub-tab. Scroll the phone listing in the **Phone/Apearances** 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 “22051” was used.

Shadow OSN Configuration Wizard - Security Features

Emergency Notification

**Emergency Options**  
When an extension dials the Emergency Digits (all access codes must be included) or an Emergency Short Code a notification message will be delivered to the specified devices (i.e extensions, workstations, etc).

**Digits Dialed (i.e. 911)**  
[ ] [Add]

**Stamp Log Code (i.e. 888)**  
[ ] [Add]

**Emergency List**  
911 [Delete] [Clear]

Identify Extension placing emergency call using [Device Name (Default)]

**911 Emergencies/Errors Notifications**  
Extensions | IP Phones | Email | Computers

Properties | Extension List | **Notify List** | Configuration

Alert notifications to IP Office phones requires the use of an IP Office telephone extension. Select the extension(s) to be utilized to send the notification message.

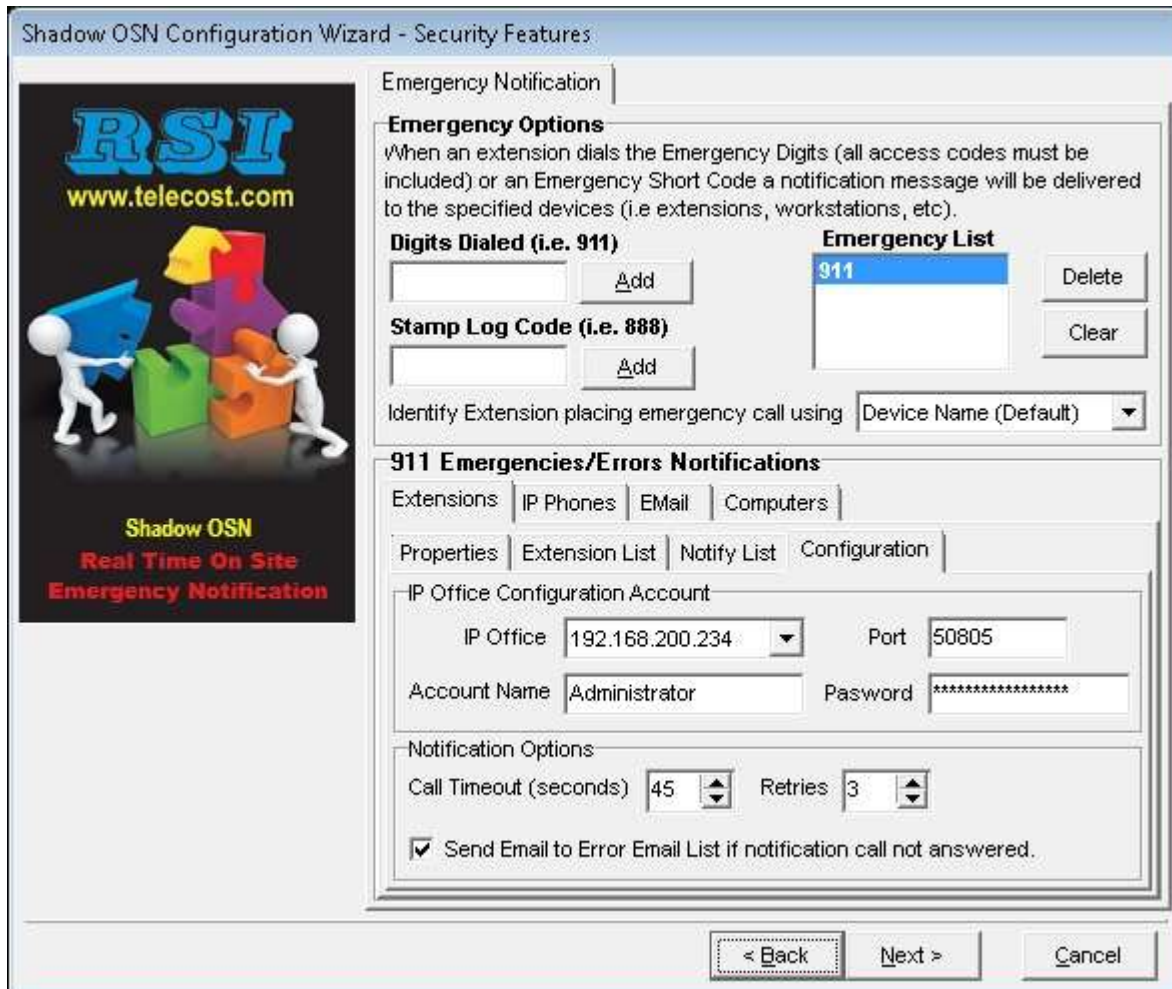
Phone/Apearances

- ☐ IP Office Phone: 22033
- ☐ IP Office Phone: 22034
- ☐ IP Office Phone: 22035
- ☐ IP Office Phone: 22041
- ☒ IP Office Phone: 22051

< Back Next > Cancel

Select the **Configuration** sub-tab. For **IP Office, Account Name, Password**, 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.



Shadow OSN Configuration Wizard - Security Features

Emergency Notification

**Emergency Options**  
When an extension dials the Emergency Digits (all access codes must be included) or an Emergency Short Code a notification message will be delivered to the specified devices (i.e extensions, workstations, etc).

**Digits Dialed (i.e. 911)**  
[ ] [Add]

**Stamp Log Code (i.e. 888)**  
[ ] [Add]

**Emergency List**  
911 [Delete]  
[ ] [Clear]

Identify Extension placing emergency call using [Device Name (Default)]

**911 Emergencies/Errors Notifications**  
Extensions | IP Phones | Email | Computers

Properties | Extension List | Notify List | Configuration

IP Office Configuration Account  
IP Office [192.168.200.234] Port [50805]  
Account Name [Administrator] Password [\*\*\*\*\*]

Notification Options  
Call Timeout (seconds) [45] Retries [3]  
☒ Send Email to Error Email List if notification call not answered.

< Back Next > Cancel



## 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.

Shadow OSN Configuration Wizard - Security Features

Emergency Notification

**Emergency Options**  
When an extension dials the Emergency Digits (all access codes must be included) or an Emergency Short Code a notification message will be delivered to the specified devices (i.e extensions, workstations, etc).

**Digits Dialed (i.e. 911)**  
[ ] [Add]

**Stamp Log Code (i.e. 888)**  
[ ] [Add]

**Emergency List**  
911 [Delete] [Clear]

Identify Extension placing emergency call using [Device Name (Default)]

**911 Emergencies/Errors Notifications**  
Extensions | IP Phones | Email | Computers

Message | Extension List | Configuration | Server

Notification Message  
On-Site Emergency Event at <Name>-<Extension> at <Date> using <Digits>

< Back Next > Cancel

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.

The screenshot shows the 'Shadow OSN Configuration Wizard - Security Features' window. The 'Emergency Notification' tab is selected. On the left is a logo for RSI (www.telecost.com) with the text 'Shadow OSN Real Time On Site Emergency Notification'. The main area is divided into sections: 'Emergency Options' with fields for 'Digits Dialed (i.e. 911)' and 'Stamp Log Code (i.e. 888)', each with an 'Add' button; an 'Emergency List' with a table containing '911' and buttons for 'Delete' and 'Clear'; a dropdown for 'Identify Extension placing emergency call using' set to 'Device Name (Default)'; and '911 Emergencies/Errors Nortifications' with sub-tabs for 'Extensions', 'IP Phones', 'Email', and 'Computers'. The 'Extensions' sub-tab is active, showing a 'Message' section with instructions, a table with columns 'Extension' and 'IP Address', and an 'Add Phone to Notification List' button. The table lists four entries: 21034 (10.64.101.104), 21035 (10.64.101.105), 22034 (192.168.200.115), and 22035 (192.168.200.118). At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

Extension	IP Address
21034	10.64.101.104
21035	10.64.101.105
22034	192.168.200.115
22035	192.168.200.118

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.

Shadow OSN Configuration Wizard - Security Features

**Emergency Notification**

**Emergency Options**  
When an extension dials the Emergency Digits (all access codes must be included) or an Emergency Short Code a notification message will be delivered to the specified devices (i.e extensions, workstations, etc).

**Digits Dialed (i.e. 911)**  
911

**Stamp Log Code (i.e. 888)**

**Emergency List**  
911

Identify Extension placing emergency call using

**911 Emergencies/Errors Notifications**

Extensions

Message

Use the Server settings to specify the IP Address and Port used to deliver the Top Line Messages to the IP phones. Please note these are system wide settings.

Message Server IP Address

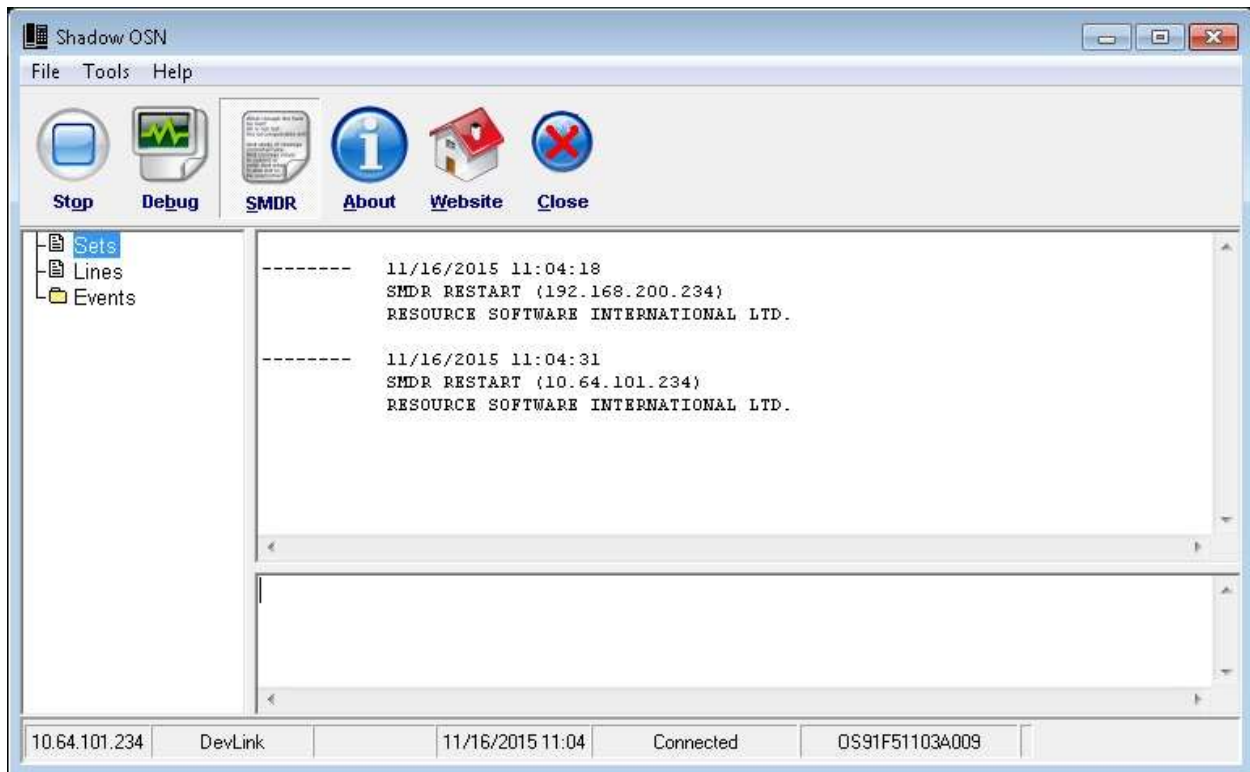
Message Server Port

< Back



## 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.



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

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.

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.

Shadow OSN

File Tools Help

Stop Debug SMDR About Website Close

```

11/16/2015 11:10:56 CALL:S 258.1031.0,0.1032.0,2,3,1,0,0,0,Extn22051(22051),Extn22024(22024),,0,0,8.18,100.100,22024,100.101
11/16/2015 11:10:56 CALL:D 258.1031.0,0.1032.0,12,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
11/16/2015 11:15:01 CALL:S 0.1034.0,0.1035.0,9,0,1,3,0,0,Extn22021(22021),,8.15,0,0,100.100,,100.101,22021,,100,100,,0,16
11/16/2015 11:15:04 CALL:S 0.1034.0,0.1035.0,7,0,0,0,0,0,Extn22021(22021),,Line 18,8.15,0,0,100.100,,100.101,22021,,100,,10
11/16/2015 11:15:04 CALL:S 0.1034.0,0.1035.0,8,1,1,0,1,0,Extn22021(22021),,Line 18,,8.15,0,0,100.119,911,100.101,22021,,100,
11/16/2015 11:15:13 CALL:S 0.1034.0,0.1035.0,2,1,0,1,0,Extn22021(22021),,Line 18,,8.15,0,0,100.119,911,100.101,22021,,100,
11/16/2015 11:15:13 CALL:S 0.1034.0,0.1035.0,2,2,1,0,1,0,Extn22021(22021),,Line 18,,8.15,0,0,100.119,911,100.101,22021,,100,
11/16/2015 11:15:24 CALL:S 258.1037.0,0.1038.0,1,1,1,2,0,0,Extn22051(22051),,Extn22024(22024),,0,0,0,0,100.100,22024,100.101,
11/16/2015 11:15:27 CALL:S 258.1037.0,0.1038.0,2,2,1,0,1,0,Extn22051(22051),Extn22024(22024),,0,0,8.18,100.100,22024,100.101
11/16/2015 11:15:42 CALL:S 258.1037.0,0.1038.0,2,3,1,0,0,0,Extn22051(22051),Extn22024(22024),,0,0,8.18,100.100,22024,100.101
11/16/2015 11:15:42 CALL:D 258.1037.0,0.1038.0,14,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,

```

2015/11/16 11:10:32 EMERGENCY EXT:21031 Extn21031 LINE 8 DIGITS 911

2015/11/16 11:10:53 Emergency Notification call to 22024 for emergency event [EMERGENCY 21031 (1)] answered.

2015/11/16 11:11:32 Top Line Push Message "On-Site Emergency Event at|Extn21031-21031 at 2015/11/16|11:10:32

2015/11/16 11:15:04 EMERGENCY EXT:22021 Extn22021 LINE 18 DIGITS 911

2015/11/16 11:15:27 Emergency Notification call to 22024 for emergency event [EMERGENCY 22021 (1)] answered.

2015/11/16 11:16:05 Top Line Push Message "On-Site Emergency Event at|Extn22021-22021 at 2015/11/16|11:15:04

10.64.101.234 DevLink 11/16/2015 11:10 Connected OS91F51103A009

## 9. Conclusion

These Application Notes describe the configuration steps required for RSI Shadow OSN 2.2 to successfully interoperate with Avaya IP Office Server Edition 9.1. 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 9.1.0, Issue 10.03, February 2015, 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://www.devconnectprogram.com>.
3. *Resource Software International Ltd. Shadow OSN for Avaya IP Office*, available from RSI Support.

---

**©2016 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).