



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

---

# **Application Notes for configuring novalink novaalert V10 with Avaya IP Office R10.1 - Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps for novaalert from novalink with Avaya IP Office R10.1. novaalert integrates with Avaya IP Office using SIP trunks.

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

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

# 1. Introduction

These Application Notes describe the configuration steps for novaalert from novalink to interoperate with Avaya IP Office R10.1. The Avaya IP Office consists of a primary server which is the Avaya IP Office Server Edition and the Server Edition Expansion that being the Avaya IP Office IP500 V2. novaalert integrates with Avaya IP Office using SIP trunks connecting to the primary server.

novaalert is an application which is used in a health care, hotel or industrial environment for alerting, messaging or information services. novaalert can react to external alarm stimuli which indicate the existence of an emergency situation by informing affected persons of the situation. Alarms can be triggered from various possible input sources including manual input via Web browser, Smartphone Apps, Databases, E-Mails, serial interfaces, potential free contacts, SNMP, OPC, SMS, IP, etc. “Direct” alarms can also be defined which allow alarms to be input and triggered via telephone calls. The alarm triggering described is restricted to those methods which involve interaction with Avaya IP Office.

Once an alarm has been triggered, the medium selected when the alarm was configured is used to deliver the alarm. Possible delivery interfaces include phone calls (including conferences), Smartphone App’s, Desktop-Clients, E-Mail, Pager, SMS, Fax, Printers, etc. Multiple recipients can be configured for an alarm, thus possibly creating multiple simultaneous telephone calls. This test plan focuses on those delivery methods which involve interaction with Avaya IP Office.

Alarms which are triggered via Avaya IP Office can include pre-recorded or ad hoc voice messages, or can generate voice messages via a text-to-speech mechanism. The calling party name can also be configured to contain a brief alarm message, so that this alarm message will appear in the caller list of intended recipients who are unable to answer an alarm call.

## 2. General Test Approach and Test Results

This section describes the compliance testing used to verify interoperability of novaalert with IP Office and covers the general test approach and the test results. Alarms were initiated from novaalert and sent to IP Office phone sets and hunt groups over SIP trunks. IP Office Server Edition with a Server Edition Expansion (IP500 V2) was used for compliance testing. Various Avaya endpoints were registered to the Server Edition and the IP500V2, see **Section 4**, using all endpoints during compliance testing. The SIP trunk was connected between the Server Edition and novaalert with a dial-plan setup with that in mind.

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

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

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

For the testing associated with these Application Notes, the interface between Avaya systems and novaalert did not include use of any specific encryption features as requested by novalink.

## 2.1 Interoperability Compliance Testing

The interoperability compliance testing evaluated the ability of novaalert to carry out a variety of alarming functions, in various conditions, to multiple types of endpoint according to the configuration made via the web interface. These included recording of alarms from SIP/H.323/Digital endpoints.

- Delivery of voice recorded and TTS alarm to SIP/H.323/Digital endpoints.
- Delivery of voice recorded and TTS alarm to Hunt Groups.
- Verification of Alarm Display messages on each handset.
- Delivery of Alarms to the phone set speaker directly using Dial Paging.
- Following Call Forwarding to deliver alarms.
- DTMF PIN entry.
- Intrusion of Alarms to busy extensions using the Call Intrusion Short Code.
- Serviceability testing.

Serviceability testing consisted of verifying the ability of novaalert to recover from simulated network interruption to both IP Office and novaalert.

## 2.2 Test Results

All functionality and serviceability test cases were completed successfully. The following issues and observations were noted during the compliance testing.

1. 'Special Characters' such as ö,ü,ä, did not show up on the phone set display.
2. 'Local User Name' did not show up on the phone set display. Shown is the calling Party number e.g. 911 (to be defined in novaalert).
3. A Short Code for FNE was added in order to initiate the Call Intrusion Short Code; this was done because using the Call Intrusion Short Code directly by novaalert results in a forbidden so it must use the FNE for Mobile Call Control.
4. DTMF will only work using SIP INFO. See **Section 6.1** to view this specific setup.

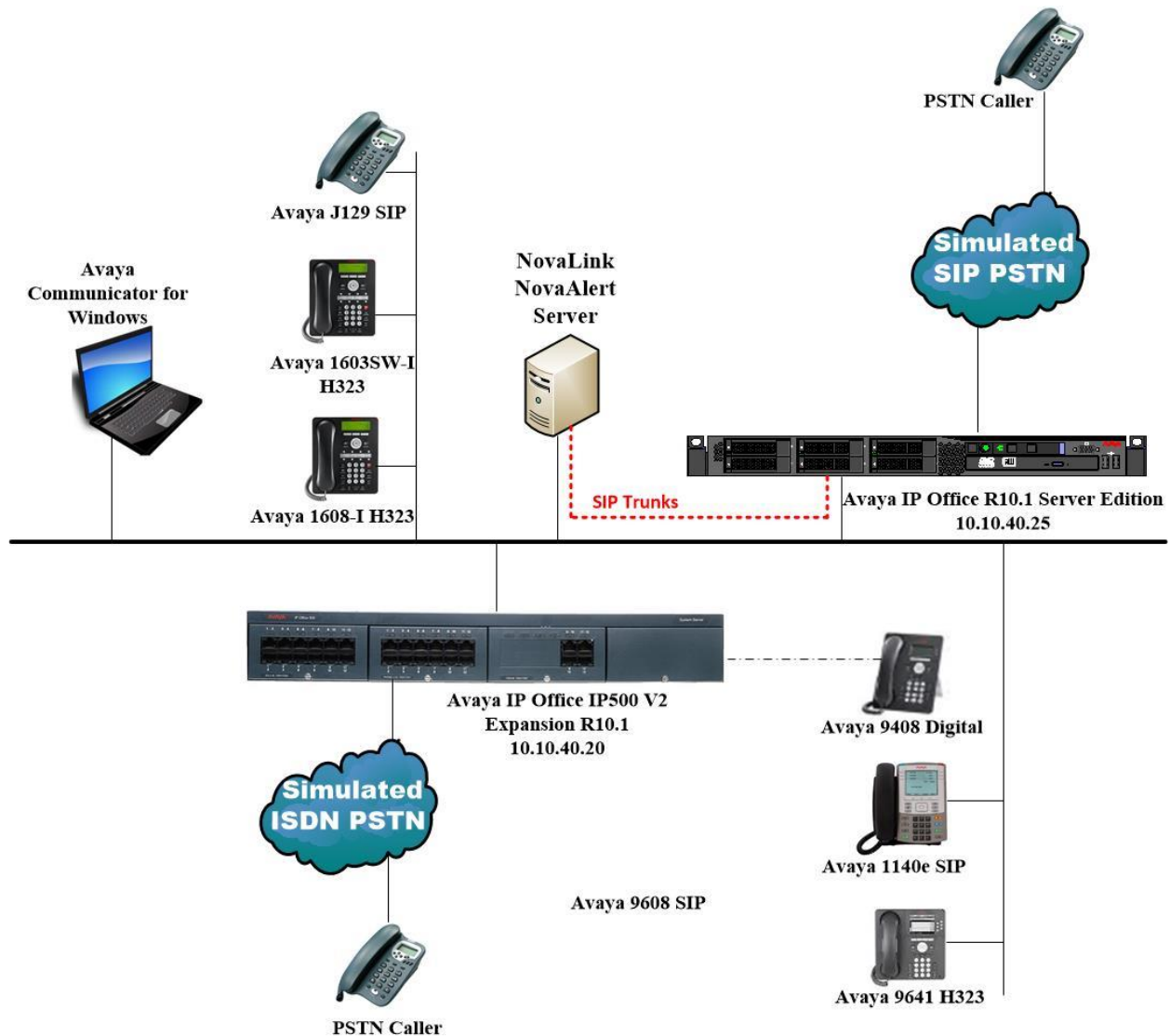
## 2.3 Support

Technical support can be obtained for novaalert from the website <http://www.novalink.ch/en/> or from the following.

novalink GmbH  
Businessstower  
Zuercherstrasse 310  
8500 Frauenfeld  
Switzerland  
helpdesk@novalink.ch  
Phone: +41 52 762 66 77  
Fax: +41 52 762 66 99

### 3. Reference Configuration

The configuration in **Figure 1** is used to compliance test novalink novaalert with Avaya IP Office Server Edition and Avaya IP Office IP500 V2. The connection between the novaalert and the IP Office solution uses SIP trunks.



**Figure 1: Connection of novaalert from novalink with Avaya IP Office Server Edition & Expansion R10.1**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya IP Office Primary Server Server Edition running on a Virtual Platform	R10.1.0.1.0 Build 3
Avaya IP Office Expansion Server IP500 V2	R10.1.0.1.0 Build 3
Avaya IP Office Manager running on a Windows 7 PC	R10.1.0.1.0 Build 3
Avaya 1608-I H323 Deskphone	1608UA1_350B.bin
Avaya 1603SW-I H323 Deskphone	1603UA1_3110A.bin
Avaya 9641 H323 Deskphone	R6.6115
Avaya 1140e SIP Deskphone	R04.04.28.00
Avaya 9508 Digital Deskphone	R0.60
Avaya Communicator for Windows (SIP)	R2.1.8.80 (SIP)
Avaya J129 SIP Deskphone	R1.0.0.0.0.43
novalink novaalert running on a Windows 2012 virtual server	10.0.1.4

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.

Testing was performed with IP Office Server Edition R10.1. Note that IP Office Server Edition requires an Expansion IP Office IP500 V2 R10.1 to support analog or digital endpoints.

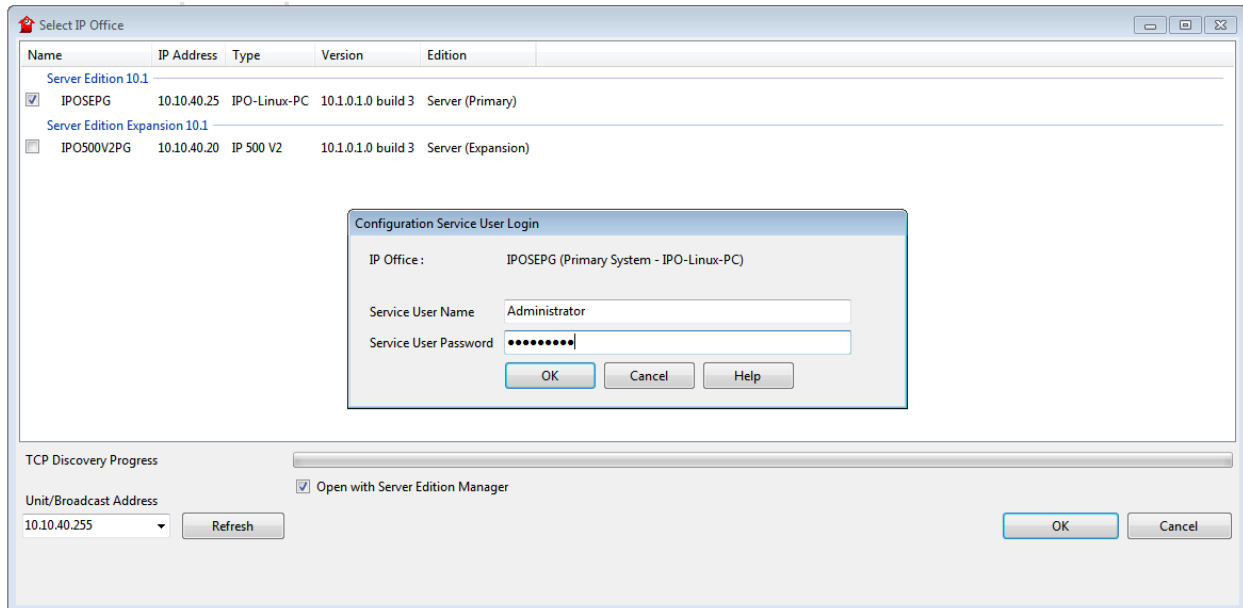
## 5. Configuration of Avaya IP Office

Configuration and verification operations on the Avaya IP Office illustrated in this section were all performed using Avaya IP Office Manager. The information provided in this section describes the configuration of the Avaya IP Office for this solution. It is implied a working system is already in place. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 9**. The configuration operations described in this section can be summarized as follows:

- Launch Avaya IP Office Manager.
- Display LAN Configuration.
- Configure Incoming Route for SIP Trunk.
- Configure SIP Trunk.
- Configure User for Mobile Call Control.
- Configure Short Codes.
- Save Configuration.

### 5.1 Launch Avaya IP Office Manager

From the Avaya IP Office Manager PC, go to **Start → Programs → IP Office → Manager** to launch the Manager application (not shown). Tick the required server to log in to, this should be the **Primary Server (Server Edition)** and log in to Avaya IP Office using the appropriate credentials to receive its configuration.



Click on **Configuration**, highlighted below.

**Server Edition**

**Summary**

Server Edition Primary

**Hardware Installed**

- Control Unit: IPO-Linux-PC
- Secondary Server: NONE
- Expansion Systems: 10, 10, 40, 20
- System Identification: ad7eda2f5eb0bdb66b99fc8e123999283dd6fb0
- Serial Number: 005056948621

**System Settings**

- IP Address: 10.10.40.25
- Sub-Net Mask: 255.255.255.0
- System Locale: Ireland (UK English)
- Device ID: NONE
- Number of Extensions on System: 11

**Open...**

- Configuration**
- System Status
- Voicemail Administration
- Resiliency Administration
- On-boarding
- IP Office Web Manager
- Help
- Set All Nodes to Select
- Set All Nodes Licence Source

**Add...**

- Secondary Server
- Expansion System

Description	Name	Address	Primary Link	Users Configured	Extensions Configured
Solution				34	45
Primary Server	IPOSEPG	10.10.40.25		13	11
Expansion System	IPO500V2PG	10.10.40.20	Bothway	21	34

## 5.2 Display LAN Configuration

In the IP Office window expand the configuration tree in the left pane and double-click **System** (this may have a different name depending on the site). Select the **LAN Settings** tab within the **LAN1** tab and note the IP Address of the IP Office that will be required in **Section 6.1** for the configuration of the SIP Trunk on novaalert.

**Configuration**

**System**

**IPOSEPG**

**LAN Settings**

IP Address: 10 . 10 . 40 . 25

IP Mask: 255 . 255 . 255 . 0

Number Of DHCP IP Addresses: 200

DHCP Mode: ☐ Server ☐ Client ☒ Disabled

Advanced



Click on the **VoIP** tab and ensure that the following are set correctly.

1. **SIP Trunks Enable.**
2. **SIP Registrar Enable.**
3. **Domain Name**, set this to the telephony domain name.
4. **UDP** set the UDP Port to **5060**.
5. **TCP** set the TCP Port to **5060**.

**Note:** novaalert uses UDP to connect to IP Office.

The screenshot shows the 'IPOSEPG' configuration window with the 'VoIP' tab selected. The 'VoIP' tab is highlighted with a red box. The configuration is divided into several sections:

- LAN Settings:** Includes 'H323 Gatekeeper Enable' (checked), 'Auto-create Extn' (unchecked), 'Auto-create User' (unchecked), 'H323 Remote Extn Enable' (unchecked), 'H.323 Signalling over TLS' (Disabled), and 'Remote Call Signalling Port' (1720).
- SIP Trunks Enable:** Checked.
- SIP Registrar Enable:** Checked.
- Auto-create Extn/User:** Unchecked.
- SIP Remote Extn Enable:** Unchecked.
- SIP Domain Name:** devconnect.local
- SIP Registrar FQDN:** (Empty field)
- Layer 4 Protocol:** Includes checkboxes for UDP, TCP, and TLS, all of which are checked. Each has a corresponding port field: UDP Port (5060), TCP Port (5060), and TLS Port (5061). Remote ports are also set to 5060 for UDP and TCP, and 5061 for TLS.
- Challenge Expiry Time (secs):** 10
- RTP:** Includes 'Port Number Range' (Minimum: 40750, Maximum: 50750) and 'Port Number Range (NAT)' (Minimum: 40750, Maximum: 50750).
- Enable RTCP Monitoring on Port 5005:** Checked.
- RTCP collector IP address for phones:** 0 . 0 . 0 . 0
- Keepalives:** Includes 'Scope' (RTP-RTCP), 'Periodic timeout' (30), and 'Initial keepalives' (Enabled).

Click on the **Telephony** tab. Ensure that Telephony settings are correct for that particular setup. Below is just an example of what was used during compliance testing.

**IPOSEPG**

System | LAN1 | LAN2 | DNS | Voicemail | **Telephony** | Directory Services | System Events | SMTP | SMDR | VoIP | VoIP Security | Contact Center

Telephony | Park & Page | Tones & Music | Ring Tones | SM | Call Log | TUI

Dial Delay Time (secs): 8  
Dial Delay Count: 2  
Default No Answer Time (secs): 30  
Hold Timeout (secs): 120  
Park Timeout (secs): 300  
Ring Delay (secs): 10  
Call Priority Promotion Time (secs): Disabled  
Default Currency: EUR  
Default Name Priority: Favour Trunk  
Media Connection Preservation: Enabled  
Phone Failback: Automatic

Login Code Complexity  
☒ Enforcement  
Minimum length: 4  
☐ Complexity

RTCP Collector Configuration  
☐ Send RTCP to an RTCP Collector  
Server Address: 0 . 0 . 0 . 0  
UDP Port Number: 5005  
RTCP reporting interval (secs): 5

Companding Law  
Switch: ☐ U-Law ☒ A-Law  
Line: ☐ U-Law Line ☒ A-Law Line

☐ DSS Status  
☒ Auto Hold  
☒ Dial By Name  
☒ Show Account Code  
☐ Inhibit Off-Switch Forward/Transfer  
☐ Restrict Network Interconnect  
☐ Include location specific information  
☒ Drop External Only Impromptu Conference  
☐ Visually Differentiate External Call  
☒ High Quality Conferencing  
☒ Directory Overrides Barring  
☐ Advertise Callee State To Internal Callers  
☐ Internal Ring on Transfer

Click on the **VoIP** tab. Ensure that the correct codecs are selected. Again, below servers to show what was used during compliance testing.

**IPOSEPG**

System | LAN1 | LAN2 | DNS | Voicemail | Telephony | Directory Services | System Events | SMTP | SMDR | **VoIP** | VoIP Security | Contact Center

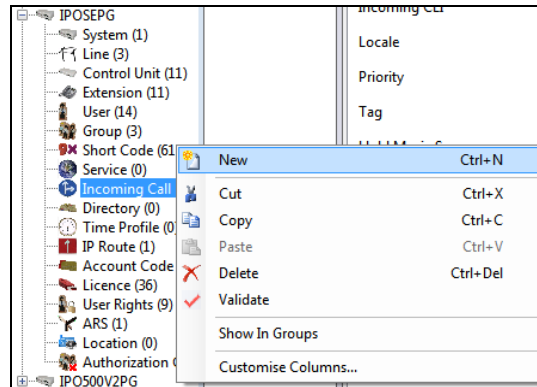
☒ Ignore DTMF Mismatch For Phones  
☐ Allow Direct Media Within NAT Location  
RFC2833 Default Payload: 101

Available Codecs  
☒ G.711 ULAW 64K  
☒ G.711 ALAW 64K  
☒ G.722 64K  
☒ G.729(a) 8K CS-ACELP

Default Codec Selection  
Unused  
Selected  
G.711 ALAW 64K  
G.711 ULAW 64K  
G.722 64K  
G.729(a) 8K CS-ACELP

### 5.3 Configure Incoming Route for SIP Trunk

An incoming route must be added for the SIP trunk that will be setup in **Section 5.4**. Navigate to **Primary Server → Incoming Call Route**. Right click on Incoming Call Route select **New**.



From the **Standard** tab, enter the **Line Group ID**; this can be kept the same as the SIP Line that is to be created for convenience. **Bearer Capability** can be set to **Any Voice**.

A screenshot of a configuration form titled '21'. It has three tabs: 'Standard', 'Voice Recording', and 'Destinations'. The 'Standard' tab is active. The form contains the following fields:

- Bearer Capability: A dropdown menu set to 'Any Voice'.
- Line Group ID: A dropdown menu set to '21'.
- Incoming Number: An empty text field.
- Incoming Sub Address: An empty text field.
- Incoming CLI: An empty text field.
- Locale: A dropdown menu.
- Priority: A dropdown menu set to '1 - Low'.
- Tag: An empty text field.
- Hold Music Source: A dropdown menu set to 'System Source'.
- Ring Tone Override: A dropdown menu set to 'None'.

From the **Destinations** tab, select . for the **Destination**. Click on **OK** at the bottom of the screen (not shown).

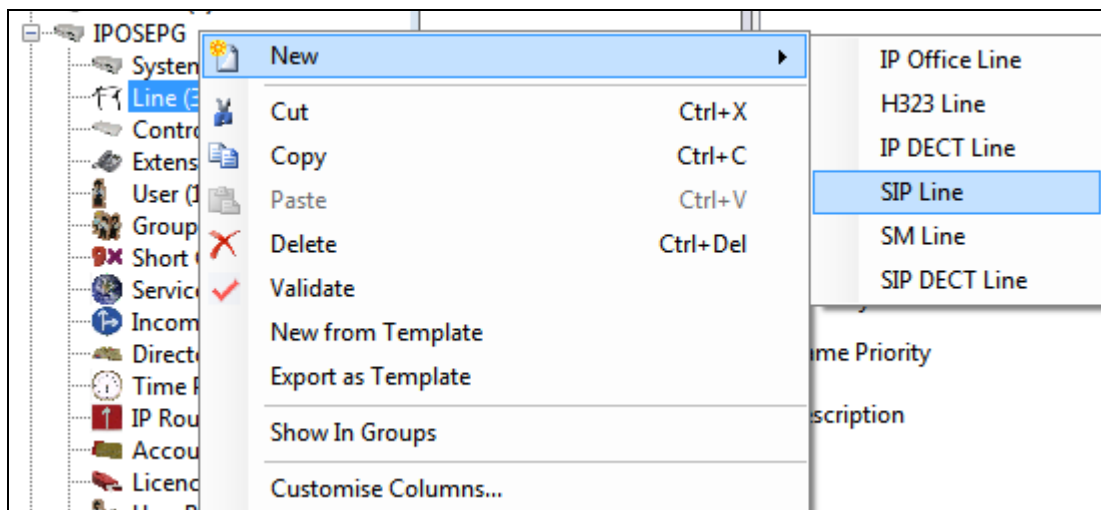
A screenshot of the same configuration form, now with the 'Destinations' tab selected. The form displays a table with three columns: 'TimeProfile', 'Destination', and 'Fallback Extension'.

TimeProfile	Destination	Fallback Extension
Default Value	.	

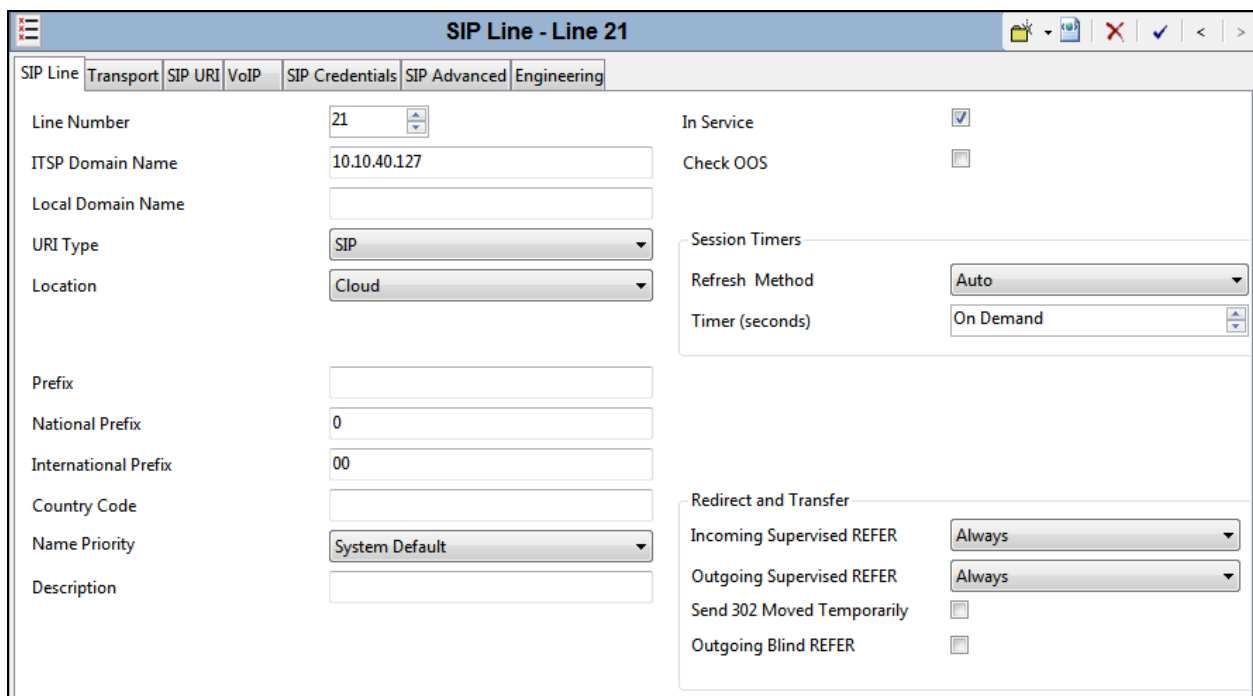
## 5.4 Configure SIP Trunk

This section shows how to add a new SIP Trunk in order to facilitate the connection to novaalert. Navigate to the Server Edition or the IP Office module that novaalert is connecting to. During compliance testing novaalert connected to the IP Office Server Edition using SIP trunks, the SIP Line was therefore created on the Server Edition.

Navigate to **Primary Server → Line**, then right click on **Line** and select **New → SIP Line**.



Click the **SIP Line** tab and select the new **Line Number** and insert the IP Address of the novaalert server for the **ITSP Domain Name**.

A screenshot of the 'SIP Line - Line 21' configuration page. The page has tabs for SIP Line, Transport, SIP URI, VoIP, SIP Credentials, SIP Advanced, and Engineering. The 'SIP Line' tab is active. The form contains the following fields and options:

- Line Number: 21
- ITSP Domain Name: 10.10.40.127
- Local Domain Name: (empty)
- URI Type: SIP (dropdown)
- Location: Cloud (dropdown)
- Prefix: (empty)
- National Prefix: 0
- International Prefix: 00
- Country Code: (empty)
- Name Priority: System Default (dropdown)
- Description: (empty)
- In Service: ☒
- Check OOS: ☐
- Session Timers:
  - Refresh Method: Auto (dropdown)
  - Timer (seconds): On Demand (dropdown)
- Redirect and Transfer:
  - Incoming Supervised REFER: Always (dropdown)
  - Outgoing Supervised REFER: Always (dropdown)
  - Send 302 Moved Temporarily: ☐
  - Outgoing Blind REFER: ☐

Click on the **Transport** tab and enter the IP Address of the novaalert server for **ITPS Proxy Address**. Ensure that the **Layer 4 Protocol** is set to **UDP** and that the **Send Port** and **Listen Port** are both set to **5060**.

The screenshot shows the 'SIP Line - Line 21' configuration window with the 'Transport' tab selected. The 'ITSP Proxy Address' field contains '10.10.40.127'. Under 'Network Configuration', 'Layer 4 Protocol' is set to 'UDP', 'Send Port' is '5060', 'Use Network Topology Info' is set to 'None', and 'Listen Port' is '5060'. The 'Explicit DNS Server(s)' field shows two sets of IP addresses: '0 . 0 . 0 . 0' and '0 . 0 . 0 . 0'. The 'Calls Route via Registrar' checkbox is unchecked. The 'Separate Registrar' field is empty.

Click on the **SIP URI** tab and click on **Add**.

The screenshot shows the 'SIP Line - Line 21' configuration window with the 'SIP URI' tab selected. A table with columns 'Channel', 'Groups', 'Via', 'Local URI', 'Contact', 'Display Name', 'PAI', 'Credential', and 'Max Calls' is visible. To the right of the table are three buttons: 'Add...' (highlighted with a red border), 'Remove', and 'Edit...'.

The following should be set as shown below; anything else can be left as default or as it is displayed in the screen shot below. Click on **OK** to continue.

<b>Local URI</b>	Set to <b>Auto</b>
<b>Contact</b>	Set to <b>Auto</b>
<b>Display Name</b>	Set to <b>Auto</b>
<b>Identity</b>	Set to <b>None</b>
<b>Incoming Group</b>	Set to the incoming group number for the SIP trunk ( <b>21</b> as per <b>Section 5.3</b> )
<b>Outgoing Group</b>	Set to the outgoing group number for the SIP trunk ( <b>21</b> as per <b>Section 5.3</b> )
<b>Max Calls per Channel</b>	Will depend on the number of SIP Licenses on IP Office and novaalert

**SIP Line - Line 21**

URI	Groups	Local URI	Contact	Display Name	Identity	Header	Originator Number	Send Caller ID	Diversion Header	Credent
1	21 21	Auto	Auto	Auto	None	PAI		None	None	0: <Non

**Edit URI**

Local URI: **Auto**

Contact: **Auto**

Display Name: **Auto**

**Identity**

Identity: **None**

Header: **P Asserted ID**

**Forwarding And Twinning**

Originator Number:

Send Caller Id: **None**

Diversion Header: **None**

Registration: **0: <None>**

Incoming Group: **21**

Outgoing Group: **21**

Max Sessions: **10**

**OK** **Cancel** **Help**

Select the **VoIP** tab and ensure that the correct **Codecs** are **Selected**. The **Re-invite Supported** and **Prack/100rel Supported** boxes are also ticked. **DTMF Support** must be set to **Info** in order to support the DTMF on novaalert which will be setup to use SIP INFO. Everything else can be left as default or as is shown below.

The screenshot shows the 'SIP Line - Line 21' configuration window with the 'VoIP' tab selected. The 'Codec Selection' section has a dropdown set to 'System Default'. Below it, the 'Unused' list is empty, and the 'Selected' list contains: G.711 ALAW 64K, G.711 ULAW 64K, G.722 64K, and G.729(a) 8K CS-ACELP. To the right, the 'Local Hold Music' checkbox is unchecked, 'Re-invite Supported' is checked, 'Codec Lockdown' is unchecked, 'Allow Direct Media Path' is unchecked, 'Force direct media with phones' is unchecked, and 'PRACK/100rel Supported' is checked. At the bottom, 'Fax Transport Support' is set to 'None', 'DTMF Support' is set to 'Info', and 'Media Security' is set to 'Disabled'.

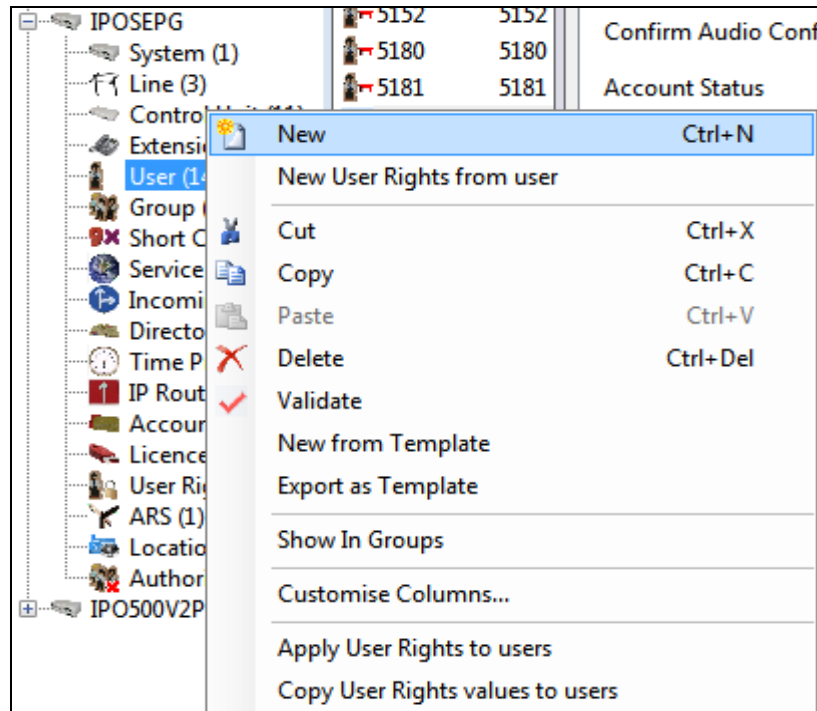
Under the **SIP Advanced** Tab, ensure that **Caller ID from From header** and **Send From In Clear** are both ticked. Click on **OK** at bottom of screen (not shown) and that will complete the **SIP Line** setup.

The screenshot shows the 'SIP Line - Line 21' configuration window with the 'SIP Advanced' tab selected. The 'Addressing' section has 'Association Method' set to 'By Source IP address' and 'Call Routing Method' set to 'Request URI'. 'Suppress DNS SRV Lookups' is unchecked. The 'Identity' section has 'Use "phone-context"', 'Add user=phone', 'Use + for International', 'Use PAI for Privacy', 'Use Domain for PAI', 'Swap From and PAI/Diversion', 'Cache Auth Credentials', and 'Add UII header to redirected calls' all unchecked. 'Caller ID from From header' and 'Send From In Clear' are checked. 'Send Location Info' is set to 'Never'. The 'Media' section has 'Allow Empty INVITE', 'Send Empty re-INVITE', 'Allow To Tag Change', 'Send SilenceSupp=Off', 'Force Early Direct Media', 'Media Connection Preservation', and 'Indicate HOLD' all unchecked. 'P-Early-Media Support' is set to 'None'. The 'Call Control' section has 'Call Initiation Timeout (s)' set to 4, 'Call Queuing Timeout (m)' set to 5, 'Service Busy Response' set to '486 - Busy Here', 'on No User Responding Send' set to '408-Request Timeout', and 'Action on CAC Location Limit' set to 'Reject Call'. 'Suppress Q.850 Reason Header', 'Emulate NOTIFY for REFER', and 'No REFER if using Diversion' are all unchecked.

## 5.5 Configure User for Mobile Call Control

A new user needs to be created on IP Office in order to use FNE - Mobile Call Control. The FNE Short Code is used by novaalert in order to initiate the Call Intrude and Coaching Intrusion Short Codes.

Navigate to **Primary Server** → **Users** and right-click and select **New** as shown below.





Under the **User** tab, enter a suitable **Name**, **Password** and **Extension** and ensure that **Power User** is selected as the **Profile**.

**NovaAlert: 5155**

User | Voicemail | DND | ShortCodes | Source Numbers | Telephony | Forwarding | Dial In | Voice Recording | Button Programming | Menu Programming | Mobility

Name: NovaAlert

Password: ••••

Confirm Password: ••••

Unique Identity:

Audio Conference PIN:

Confirm Audio Conference PIN:

Account Status: Enabled

Full Name:

Extension: 5155

Email Address:

Locale:

Priority: 5

System Phone Rights: None

Profile: Power User

- ☐ Receptionist
- ☒ Enable Softphone
- ☒ Enable one-X Portal Services
- ☒ Enable one-X TeleCommuter
- ☒ Enable Remote Worker
- ☒ Enable Communicator
- ☒ Enable Mobile VoIP Client
- ☐ Send Mobility Email
- ☐ Web Collaboration

☐ Exclude From Directory

Device Type: All Other Phone Types

Under the **Telephony** tab and again under the **Supervisor Settings** tab ensure that **Can Intrude** is ticked as shown.

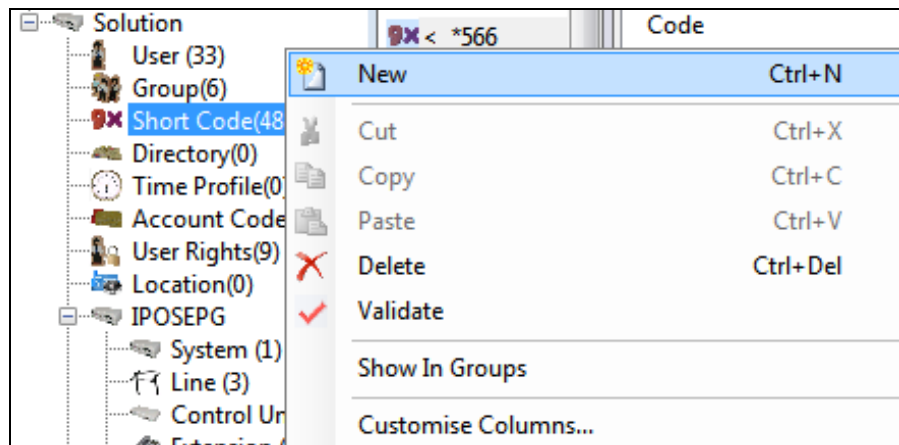
The screenshot shows the 'NovaAlert: 5155' web interface. The 'Telephony' tab is selected, and within it, the 'Supervisor Settings' sub-tab is active. The 'Call Settings' section includes fields for 'Login Code', 'Confirm Login Code', 'Login Idle Period (secs)', 'Monitor Group', 'Coverage Group', 'Status on No-Answer', and 'Privacy Override Group'. The 'Reset Longest Idle Time' section has radio buttons for 'All Calls' (selected) and 'External Incoming'. On the right, a list of checkboxes includes 'Force Login', 'Force Account Code', 'Force Authorization Code', 'Incoming Call Bar', 'Outgoing Call Bar', 'Inhibit Off-Switch Forward/Transfer', 'Can Intrude' (checked), 'Cannot be Intruded', 'Can Trace Calls', and 'Deny Auto Intercom Calls'.

Under the **Mobility** tab tick the **Mobility Features** box and enter the number associated with novaalert, this is the number configured in **Section 6.1**. Ensure that all the tick boxes shown below are selected. Click on **OK** at the bottom of the screen to complete the setup (not shown).

The screenshot shows the 'NovaAlert: 5155' web interface with the 'Mobility' tab selected. The 'Internal Twinning' section includes a 'Twinned Handset' dropdown, a 'Maximum Number of Calls' dropdown, and checkboxes for 'Twin Bridge Appearances', 'Twin Coverage Appearances', and 'Twin Line Appearances'. The 'Mobility Features' section is checked and contains a 'Mobile Twinning' subsection with fields for 'Twinned Mobile Number (including dial access code)', 'Twinning Time Profile', 'Mobile Dial Delay (secs)', and 'Mobile Answer Guard (secs)'. Below these are several checked checkboxes: 'Hunt group calls eligible for mobile twinning', 'Forwarded calls eligible for mobile twinning', 'Twin When Logged Out', 'one-X Mobile Client', 'Mobile Call Control', and 'Mobile Callback'.

## 5.6 Configure Short Codes

Short Codes can be created for both systems, i.e., both the Primary Server and the Expansion Server. A short code such as Call Intrude or Coaching Intrusion would need to be created across all systems so navigate to **Solution** → **Short Code**, right-click on **Short Code** and select **New** as shown.



### 5.6.1 Short Code for FNE Service

FNE – Mobile Call Control is used to allow a user called or calling the system to invoke mobile call control and to then handle and make calls as if they were at their system extension. FNE **31** is setup as a short code and this is done as shown below. **\*566** is used to initiate the **FNE Service** and this will be configured on the novaalert system in **Section 6.1**.

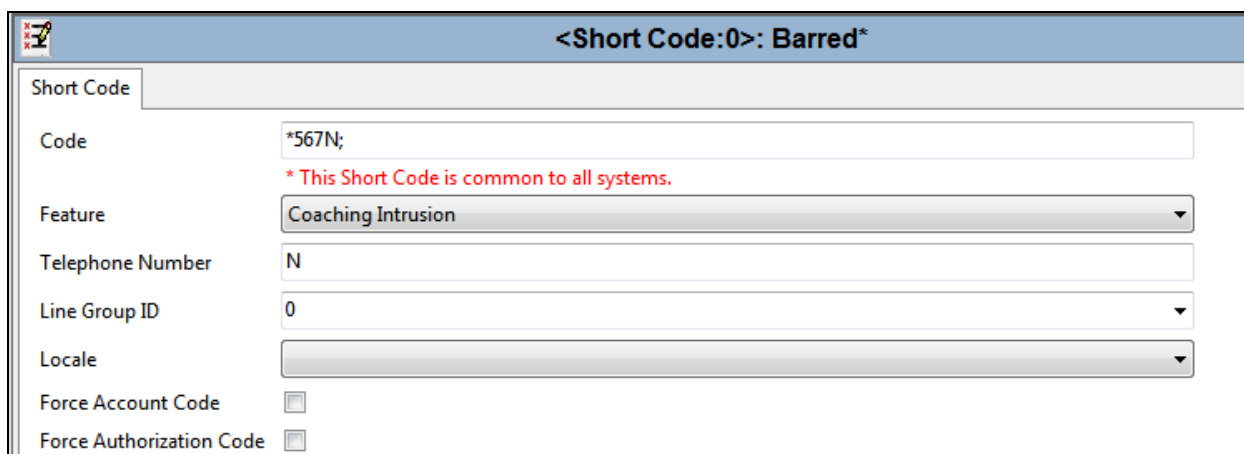
*566: FNE Service	
Short Code	
Code	<input type="text" value="*566"/>
* This Short Code is common to all systems.	
Feature	<input type="text" value="FNE Service"/>
Telephone Number	<input type="text" value="31"/>
Line Group ID	<input type="text" value="0"/>
Locale	<input type="text"/>
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

## 5.6.2 Short Code for Coaching Intrusion

Coaching Intrusion is used in order to break in on an existing call when the phone set is busy.

**\*567N;** was used for this Short Code where N is the number that was dialed. This same Short Code will be configured in **Section 6.1**.

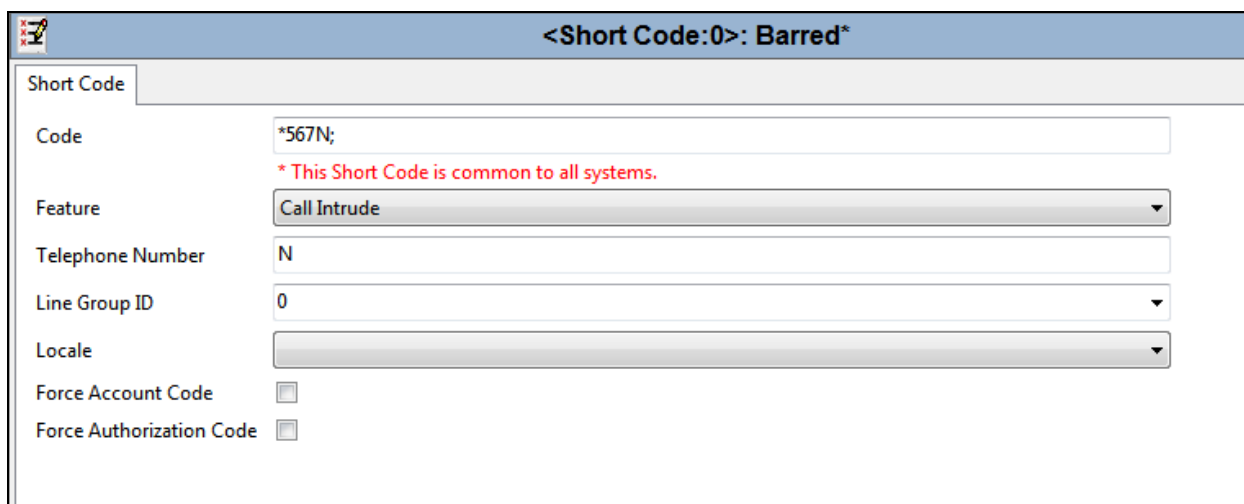
**Note:** Each user must have "Cannot be intruded" unchecked under the telephony tab.



The screenshot shows a configuration window titled "<Short Code:0>: Barred\*". The "Short Code" tab is selected. The "Code" field contains "\*567N;" with a red note below it stating "\* This Short Code is common to all systems." The "Feature" dropdown is set to "Coaching Intrusion". The "Telephone Number" field contains "N". The "Line Group ID" dropdown is set to "0". The "Locale" dropdown is empty. At the bottom, there are two unchecked checkboxes: "Force Account Code" and "Force Authorization Code".

## 5.6.3 Short Code for Call Intrude

The same Short Code is illustrated here for Call Intrude. Note that the difference between Call Intrude and Coaching Intrusion is that Coaching Intrusion allows the Alarm to intrude on another user's call and play without being heard by the other call parties to which they can still talk. Call Intrude will play the Alarm to all users on the call.



The screenshot shows a configuration window titled "<Short Code:0>: Barred\*". The "Short Code" tab is selected. The "Code" field contains "\*567N;" with a red note below it stating "\* This Short Code is common to all systems." The "Feature" dropdown is set to "Call Intrude". The "Telephone Number" field contains "N". The "Line Group ID" dropdown is set to "0". The "Locale" dropdown is empty. At the bottom, there are two unchecked checkboxes: "Force Account Code" and "Force Authorization Code".

## 5.6.4 Short Code for Dial Paging

Dial paging is used to play an alarm directly to the phoneset speaker. When novaalert uses this short code with the extension number, that alarm gets played out on the extension's speaker.

**\*568** was used as the Short Code for **Dial Paging**, seeing as 51xx is the extension range for the Primary Server the full Short Code is **\*56851XX** and this was used to initiate the alarm to extensions 51xx.

The screenshot shows a configuration window titled **\*56851XX: Dial Paging**. It contains the following fields:

- Short Code**: A tabbed interface with the **Code** sub-tab selected.
- Code**: Text input field containing **\*56851XX**.
- Feature**: Dropdown menu set to **Dial Paging**.
- Telephone Number**: Text input field containing **51N**.
- Line Group ID**: Dropdown menu set to **0**.
- Locale**: Dropdown menu.
- Force Account Code**: Check box, currently unchecked.
- Force Authorization Code**: Check box, currently unchecked.

## 5.7 Save Configuration

Once the configuration has been made it must be sent to the IP Office. Click on the **Save** Icon at the top left of the screen as shown below. Once the **Save Configuration** window opens, either the **Merge** or **Immediate** button will be filled in depending on the changes that are made. Click on the **OK** button.

The screenshot shows the Avaya IP Office Manager interface. The **Configuration** pane on the left shows a tree view with **Short Code** selected. The main pane shows the configuration for **\*567N:: Call Intrude**. The **Send Multiple Configurations** window is open, showing a table with the following data:

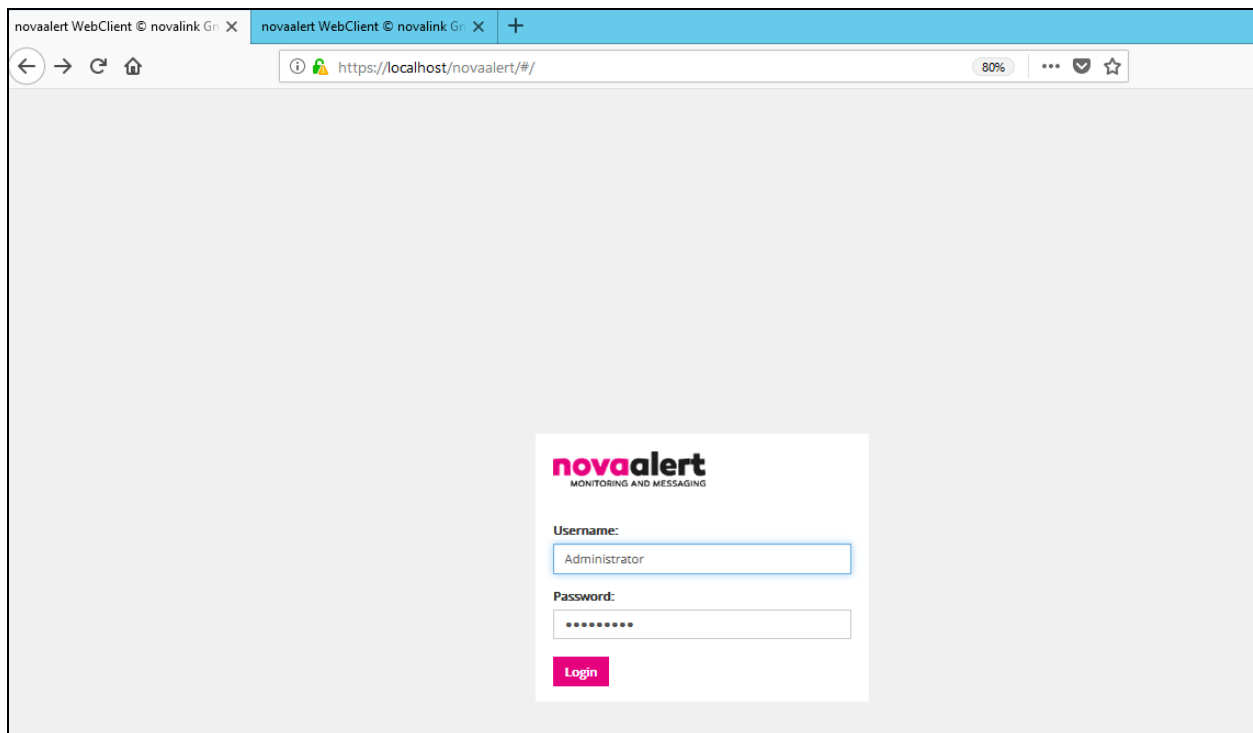
Select	IP Office	Change Mode	RebootTime	Incoming Call Barring	Outgoing Call Barring	Error Status	Progress
<input checked="" type="checkbox"/>	IPOSEPG	Merge	16:14	<input type="checkbox"/>	<input type="checkbox"/>		0%
<input checked="" type="checkbox"/>	IPOS00V2PG	Merge	16:14	<input type="checkbox"/>	<input type="checkbox"/>		0%

The window has **OK**, **Cancel**, and **Help** buttons at the bottom.

## 6. Configuration of novaalert

It is assumed that novaalert is already installed and configured by a novalink engineer. The following shows the steps that can be carried out in order to make changes or to examine a working system. The screen shots were taken after compliance testing was completed successfully and will show the configuration that was used for a successful integration to IP Office. This can be used as an example of a fully working system.

All configuration changes are made to novaalert using a web browser session to the novaalert server. Open a web browser session to the IP Address of the novaalert server followed by /novaalert, for example, for compliance testing **https://localhost/novaalert** was used. The following screen shown is asking for the **User Name** and **Password**, enter these and click on the **Login** button.



## 6.1 Connection setup to Avaya IP Office (SIP trunk connection)

Once logged in, the following screen is presented to the user. Click on the **Lines** icon, highlighted below. All configuration with regards to the SIP connection to IP Office is set in this area.

The screenshot displays the 'novaalert' System overview interface. The left sidebar contains navigation options: Master data, Alert, Monitoring, novaconf, and Analysis. The main area shows a 'System overview' dashboard with a grid of icons representing different system components. The 'Lines' icon, which depicts a telephone handset, is highlighted with a red rectangular box. Other icons include Database, Gateway (SMS, Pager), DECT, Web, Serial Interface, SNMP, novamail, E-Mail In, E-Mail Out, Contact, Hotel Interface, TTS, Printer, OPC, Contact IP, Mobile, and novaCONNECTOR. Below the dashboard, there is a message log table with columns for Date / Time, Type, Source, and Message. The log shows a warning message: 'Not Connected!' from DECT on 2/23/2018 at 1:34:23 PM. The bottom right corner of the screen displays an 'Activate Windows' watermark.

Date / Time	Type	Source	Message
2/23/2018 1:34:23 PM	Warnings	DECT	Not Connected!

The first section shows the **Line Configuration**. This was the setup used for compliance testing; the most notable field is the Intrusion Code which is referenced in **Section 5.6**. The **Intrusion code** is entered using the FNE short code first followed by the Call Intrude/Coaching Intrusion short code and this looks like **\*566!\*567<Nr>#**. This will call \*566 first then using the FNE Mobile Call Control Service using that \*567xxxx# is entered using DTMF.

System overview > Lines

Lines
 ▶ ↺ ⌂

Line Configuration (Lines)			
Static Direct Alarm	<input type="text" value=""/>	(DirektAlarmNummer1)	<input type="text" value="+ -"/>
Word Replacement Type	Words separated by "space" are replaced	(Ersetzungsart)	<input type="text" value="+ -"/>
Timeout internal calls	<input type="text" value="30"/>	(CallLängeIntern)	<input type="text" value="+ -"/>
Timeout external calls	<input type="text" value="30"/>	(CallLängeExtern)	<input type="text" value="+ -"/>
Polling Interval	<input type="text" value="5"/>	(Intervall)	<input type="text" value="+ -"/>
Intrusion code	<input type="text" value="*566!*567&lt;Nr&gt;#"/>	(AufschaltCode)	<input type="text" value="+ -"/>
Reserved Lines for Alarm Triggering	<input type="text" value="0"/>	(NurAusloesen)	<input type="text" value="+ -"/>
Line allocation 1	<input type="text" value="1"/>	(Linie1)	<input type="text" value="+ -"/>
Line allocation 2	<input type="text" value="2"/>	(Linie2)	<input type="text" value="+ -"/>
Line allocation 3	<input type="text" value="3"/>	(Linie3)	<input type="text" value="+ -"/>
Line allocation 4	<input type="text" value="4"/>	(Linie4)	<input type="text" value="+ -"/>
Min Connection Time	<input type="text" value="5"/>	(MinAnhoeren)	<input type="text" value="+ -"/>



Select **Voice over IP Configuration** which is the next section. The settings shown below are what were used during compliance testing. Most notable that being **Driver Preferences**, which should be set to **SIP** and the **SIP Gateway** which has the IP Address of the IP Office Primary Server as per **Section 5.1**.

System overview > Lines

**Lines** Search...

**Voice over IP Configuration (VoIP)**

<b>Driver Preferences</b>	SIP	(DriverPref)	+ -	⊗
<b>Local User Name</b>	AlertAlert	(LocalUserName)	+ -	⊗
<b>H323 Gateway</b>	<div>IP</div> <div>Vorwahl</div> <div>-</div> <div>+</div>	(H323_Gateway)	+ -	⊗
<b>H323 Use Fast Start</b>	No	(H323_UseFastStart)	+ -	⊗
<b>H323 Use H245 Tunneling</b>	No	(H323_UseH245Tunneling)	+ -	⊗
<b>H323 Listener Configuration</b>	*:1720	(H323_ListenerConfig)	+ -	⊗
<b>H323 Use GateKeeper</b>	No	(H323_UseGateKeeper)	+ -	⊗
<b>H323 GateKeeper Address</b>		(H323_GateKeeperAddress)	+ -	⊗
<b>H323 GateKeeper Zone</b>		(H323_GateKeeperZone)	+ -	⊗
<b>H323 GateKeeper Password</b>		(H323_GateKeeperPwd)	+ -	⊗
<b>SIP Gateway</b>	<div>Realm</div> <div>IP-Address</div> <div>Prefix</div> <div>Local Interface</div> <div>10.10.40.25</div> <div>10.10.40.25</div> <div>Prefix</div> <div>Local Interface</div> <div>-</div> <div>+</div>	(SIP_Gateway)	+ -	⊗
<b>SIP Alias</b>	<div>Host</div> <div>Alias</div> <div>Username</div> <div>Password</div> <div>Realm</div> <div>Host</div> <div>Alias</div> <div>Username</div> <div>Password</div> <div>0001</div> <div>-</div> <div>+</div>	(SIP_Alias)	+ -	⊗
<b>SIP Listener Config</b>	*:5060	(SIP_ListenerConfig)	+ -	⊗
<b>Fax Transport Codec</b>	T.30	(FaxTransportCodec)	+ -	⊗

Add entry

**Call Control (CallInfo)**

Click on **Call Control**, which is the next section down. The following shows the configuration used for compliance testing. The **PBX Type** is set to **Avaya IPO** and the **Card Driver** set to **VoIP (H.323/SIP)**. The **Default Calling Party** is entered and this much match exactly the Twinned Mobile Number configured for the FNE User in **Section 5.5. Signaling outgoing DTMF** is chosen as shown on the next page.

System overview > Lines

**Lines** Search...

**Call Control (CallInfo)**

<b>PBX Type</b>	Avaya IPO	(PBXType)	+ -	⊗
<b>Card Driver</b>	VoIP (H.323/SIP)	(CardDriver)	+ -	⊗
<b>Interface</b>	VoIP	(Interface)	+ -	⊗
<b>Dialed Number Identification</b>	Use called party information	(GewählteNummer)	+ -	⊗
<b>Minimum Digits</b>	0	(MinDigits)	+ -	⊗
<b>Intrusion Configuration</b>	Recall with add. intrusion digits prior call no.	(AufschaltenAktiv)	+ -	⊗
<b>Calling Party Configuration</b>	Yes	(CallingPartyAktiv)	+ -	⊗
<b>Default Calling Party</b>	0049123456789	(DefaultCallingParty)	+ -	⊗
<b>Calling Name Identification</b>	Yes	(CNIPAktiv)	+ -	⊗
<b>QSIG Standard</b>	Disabled	(QSIGStandard)	+ -	⊗
<b>Call Retries</b>	2	(CallVersuche)	+ -	⊗
<b>Timeout Call List</b>	8	(RufZeitAnrufliste)	+ -	⊗
<b>Signaling outgoing DTMF</b>	As sound formatted information message (H.245 sign)	(OutgoingDTMFMode)	+ -	⊗
<b>TLS mode</b>	Disabled	(TLSmode)	+ -	⊗
<b>TLS Secure RTP</b>	Both	(TLSsecureRTP)	+ -	⊗
<b>TLS local certificate</b>	No certificate	(TLSlocalCertificate)	+ -	⊗

Add entry

**Signaling outgoing DTMF** will determine what DTMF is used by novaalert when sending digits to IP Office. For compliance testing SIP Info was used and this must be set up on the SIP Line as shown in **Section 5.4**. The corresponding setting here is **As sound formatted information message (H.245 signal or SIP INFO)**.

<b>Signaling outgoing DTMF</b>	As sound formatted information message (H.245 sign ▼
<b>TLS mode</b>	<No selection> Default setting for the chosen protocol
<b>TLS Secure RTP</b>	Q.931 Information Elements (H.323 only) Simple string as information message (H.245 string or SIP INFO)
<b>TLS local certificate</b>	<b>As sound formatted information message (H.245 signal or SIP INFO)</b> According to RFC 2833 as RTP package In-Band DTMF tones

With this all set, click **Save** at the bottom right of the screen.

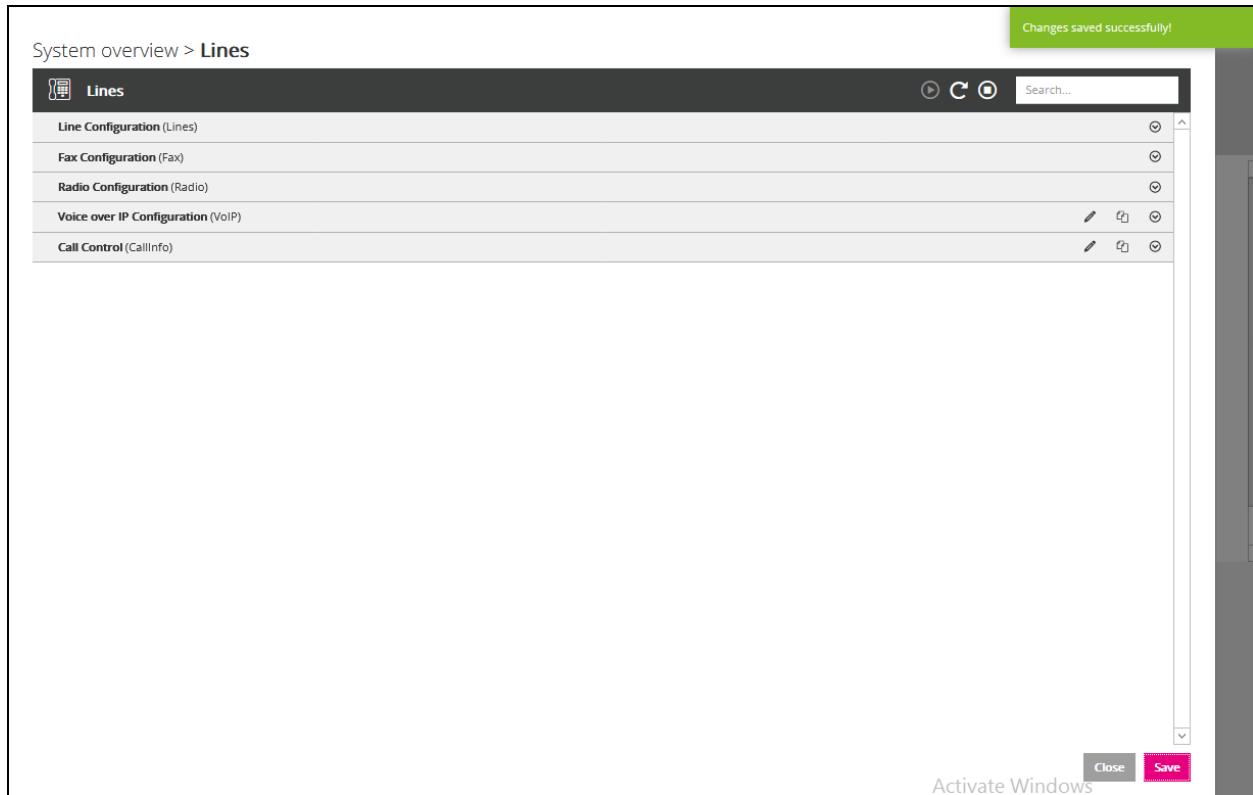
System overview > Lines

Lines			
Card Driver	VoIP (H.323/SIP)	(CardDriver)	+
Interface	VoIP	(Interface)	+
Dialed Number Identification	Use called party information	(GewählteNummer)	+
Minimum Digits	0	(MinDigits)	+
Intrusion Configuration	Recall with add. intrusion digits prior call no.	(AufschaltenAktiv)	+
Calling Party Configuration	Yes	(CallingPartyAktiv)	+
Default Calling Party	0049123456789	(DefaultCallingParty)	+
Calling Name Identification	Yes	(CNIPAktiv)	+
QSIG Standard	Disabled	(QSIGStandard)	+
Call Retries	2	(CallVersuche)	+
Timeout Call List	8	(RufZeitAnrufliste)	+
Signaling outgoing DTMF	As sound formatted information message (H.245 sign ▼	(OutgoingDTMFMode)	+
TLS mode	Disabled	(TLSmode)	+
TLS Secure RTP	Both	(TLSsecureRTP)	+
TLS local certificate	No certificate	(TLSlocalCertificate)	+

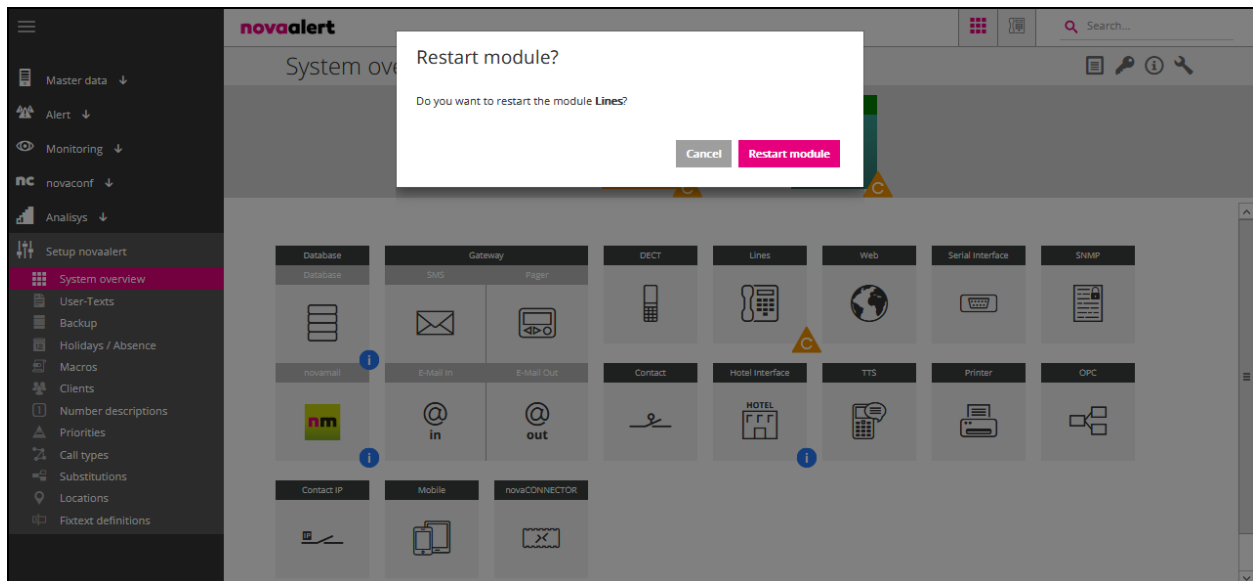
Add entry

Close Save

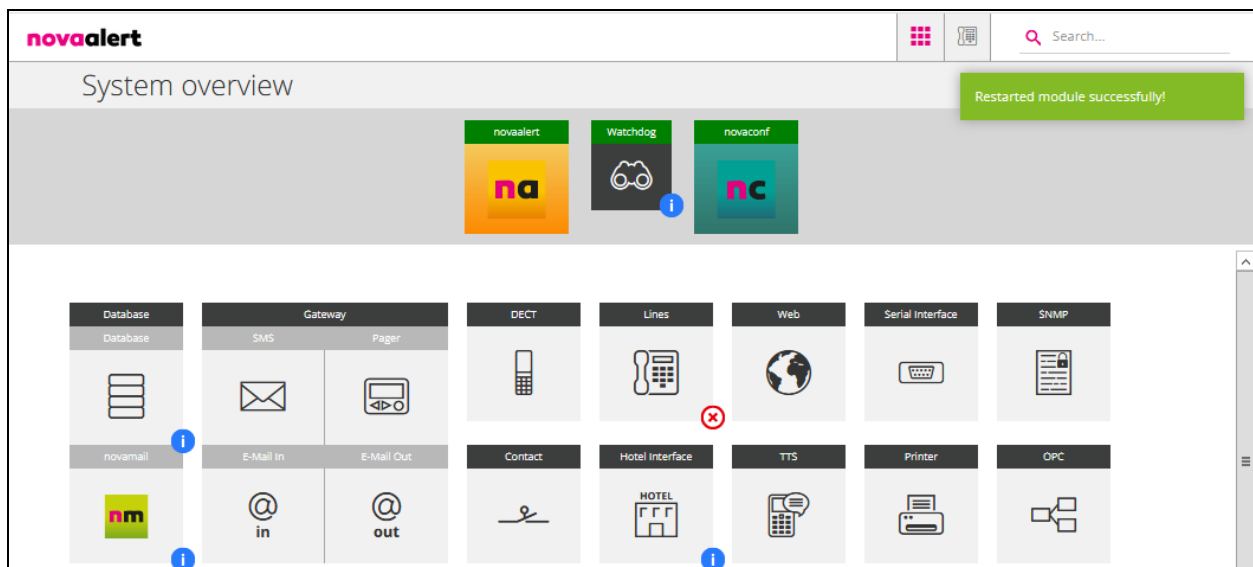
Changes saved successfully should be displayed at the top right of the screen and **Close** can then be clicked at the bottom right.



Once the setup is saved click on the **C** “triangle icon” under the **Lines** icon and the following screen is popped asking to **Restart module?**, click on **Restart module**.



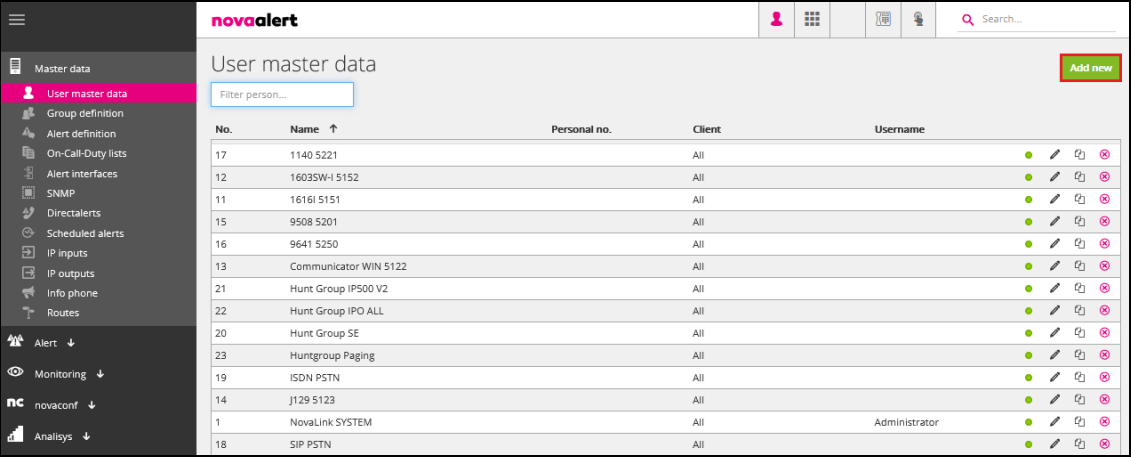
A message is displayed in the top right corner saying **Restarted module successfully**.



## 6.2 Creating an Alarm for Avaya IP Office

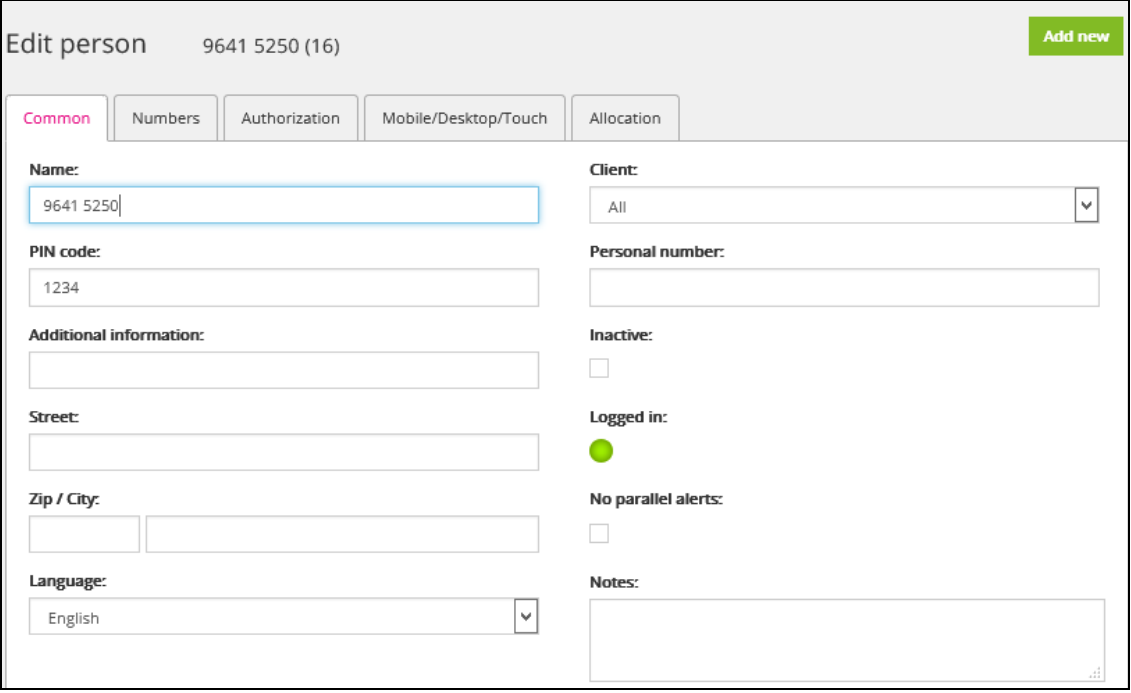
An alarm can be created and sent to a single IP Office user or a group of IP Office users. This section outlines the steps required to create an alarm that is ready to be sent.

In order to send an alarm to IP Office, a user/extension will need to be added. This extension is then called by novaalert when the alarm is activated. From the main menu, navigate to **Master data** → **User master data**. In the main window select **Add new** as shown below.



No.	Name	Personal no.	Client	Username
17	1140 5221		All	
12	1603SW-I 5152		All	
11	1616I 5151		All	
15	9508 5201		All	
16	9641 5250		All	
13	Communicator WIN 5122		All	
21	Hunt Group IP500 V2		All	
22	Hunt Group IPO ALL		All	
20	Hunt Group SE		All	
23	Huntgroup Paging		All	
19	ISDN PSTN		All	
14	J129 5123		All	
1	NovaLink SYSTEM		All	Administrator
18	SIP PSTN		All	

**Note:** The following screens show the data for an existing user, these are used to demonstrate what is required when adding a new user. Click on the **Common** tab and enter a suitable **Name** and **PIN code**.



**Edit person** 9641 5250 (16) Add new

**Common** Numbers Authorization Mobile/Desktop/Touch Allocation

**Name:** 9641 5250

**PIN code:** 1234

**Additional information:**

**Street:**

**Zip / City:**

**Language:** English

**Client:** All

**Personal number:**

**Inactive:** ☐

**Logged in:** ☒

**No parallel alerts:** ☐

**Notes:**

Click on the **Numbers** tab and enter the IP Office telephone number for this user and click on **Save Changes** at the bottom of the screen (not shown).

Common	<b>Numbers</b>	Authorization	Mobile/Desktop/Touch	Allocation
<div> <div>Office 1:</div> <div>5250 <input type="checkbox"/></div> </div> <div> <div>Office 2:</div> <div><input type="text"/> <input type="checkbox"/></div> </div> <div> <div>Home 1:</div> <div>5250 <input type="checkbox"/></div> </div> <div> <div>Home 2:</div> <div><input type="text"/> <input type="checkbox"/></div> </div> <div> <div>Mobile 1:</div> <div><input type="text"/> <input type="checkbox"/></div> </div> <div> <div>Mobile 2:</div> <div><input type="text"/> <input type="checkbox"/></div> </div> <div> <div>Pager 1:</div> <div><input type="text"/> Tone call <input type="checkbox"/></div> </div> <div> <div>Pager 2:</div> <div><input type="text"/> Tone call <input type="checkbox"/></div> </div> <div> <div>SMS GSM 1:</div> <div><input type="text"/> <input type="checkbox"/></div> </div> <div> <div>SMS GSM 2:</div> <div><input type="text"/> <input type="checkbox"/></div> </div>				

The next step is to create the Alert Definition, navigate to **Alert definition** in the left window and click on **Add new** in the main window.

</

Again this example below shows an existing Alert but is used to demonstrate what needs to be configured for any Alert definition. Click on the **Common** tab and enter a suitable **Description**. The **Alert type** can be set depending on the type of Alert; this was set to **Group Call** for the example below. A **PIN code for trigger** also needs to be added.

**Edit alert** Alarm to H323 5250 (13) Add new

**Common** Messages Alert-list Alert interfaces Escalation Mobile/Desktop/Touch Various

**Description:**  
Alarm to H323 5250

**PIN code for trigger:**  
1234

**Priority:**  
Highest Priority

**Alert type:**  
Group Call

**Number of attempts:**  
1

**Number of person to be contacted:**  
All

**Voice-No.:**  
68

**Client:**  
All

**Notes:**

Click on the **Messages** tab, a message can be delivered to the phone set display by opening the **Phone display** section and entering a suitable **Message** as shown below.

Common **Messages** Alert-list Alert interfaces Escalation Mobile/Desktop/Touch Various

**Fill messages with alert description**

**Phone display**

**Message:**  
This is an Alarm Message

**Event text:**  
No

**Call type:**  
Duration

Phone TTS

Numeric pager

Alphanumeric pager

SMS GSM

WLAN/DECT paging



The list of users to be alerted by this alarm is entered under the **Alert-list** tab. In the example below one user **5250** (that created previously in this section) was added. However, a number of users can be added here depending on who should receive the alarm. The **Intr.** tick box was checked which would allow call intrusion for this user. If the user is busy then the alarm can intrude on the call and get played.

Name	Medium / State	Conf.	Aknw.	Intr.	Logg.	Delay
↑↓ 9641 5250 (16)	Office 1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0 <input type="button" value="v"/> <input type="button" value="edit"/> <input type="button" value="delete"/>

Under the **Escalation** tab an Escalation can be added in order to send the alarm to another user such as a manager or perhaps a secretary if the initial user fails to answer the alarm. This escalation must be configured first (not shown here) but can then be referenced under this Escalation tab.

Click on **Save** at the bottom right of the screen (not shown below) and this will save the Alert Definition. This concludes the setup of an alarm that will be sent to this IP Office user 5250.

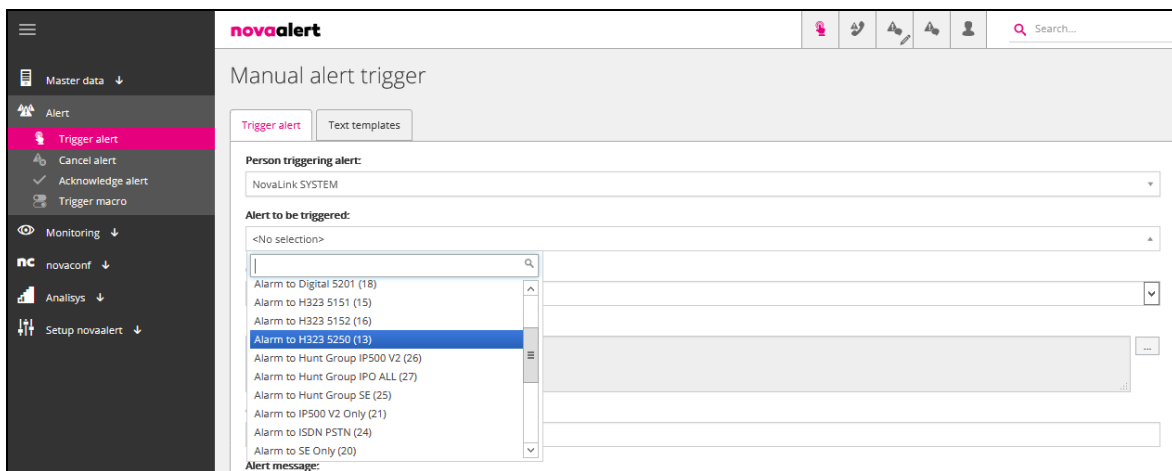
Condition	Pers. count	Add	Alert	Ori. text
↑↓ Num. of persons <	1	<input type="checkbox"/>	Escalation (33)	<input type="checkbox"/> <input type="button" value="edit"/> <input type="button" value="copy"/> <input type="button" value="delete"/>

## 7. Verification Steps

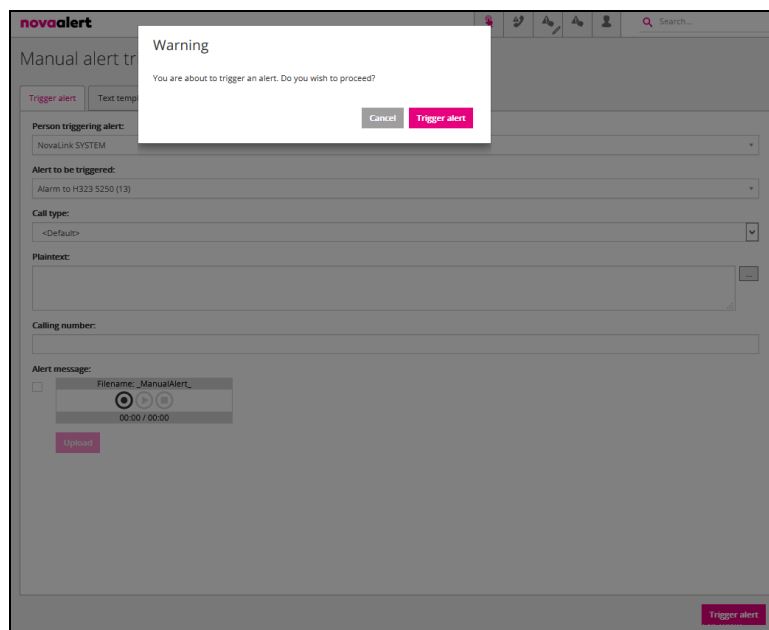
This section illustrates the steps necessary to verify that the novaalert is configured correctly to send an alarm to extensions on IP Office using SIP trunks.

### 7.1 Trigger an Alarm on novaalert

Log into novaalert as per **Section 6**. From the left menu navigate to **Alert → Trigger alert**. From the main window click on the **Alert to be triggered** drop down box and select the Alert to be triggered. In the example below the alert was **Alarm to H323 5250** which was created in **Section 6.2**.



Click on **Trigger alert** at the bottom right of the screen and a window opens asking to confirm the alarm trigger. Click on **Trigger alert** in that window.



## 7.2 Verify SIP trunk messages

SIP messages can be viewed by opening the IP Office **SysMonitor** as shown below. This monitor displays all the SIP messages coming to and going from the IP Office. If there is an issue with the alarms not being sent then this is a way to try and troubleshoot what is happening.

The screenshot shows the Avaya IP Office SysMonitor application window. The title bar reads "Avaya IP Office SysMonitor - Monitoring 10.10.40.25 (IPOSEPG (Server Edition(P))); Log Settings - C:\Users\...\sysmonitorsettings.ini". The menu bar includes File, Edit, View, Filters, Status, and Help. Below the menu is a toolbar with various icons. The main display area shows a log of SIP messages. The first message is an INVITE received at 246229960mS. The second message is a 100 Trying response received at 246229961mS. The third message is another INVITE received at 246229994mS. Each message is displayed with its full SIP header and body information.

```
Avaya IP Office SysMonitor - Monitoring 10.10.40.25 (IPOSEPG (Server Edition(P))); Log Settings - C:\Users\...\sysmonitorsettings.ini
File Edit View Filters Status Help

Max-Forwards: 70

***** SysMonitor v10.1.0.1.0 build 3 [connected to 10.10.40.25 (IPOSEPG (Server Edition(P)))] *****
246229960mS SIP Call Rx: 21
    INVITE sip:5250@10.10.40.25 SIP/2.0
    CSeq: 1 INVITE
    Via: SIP/2.0/UDP 10.10.40.127:5060;branch=z9hG4bKf93f41ed-a517-1910-9f60-00505694bcb9;rport
    User-Agent: NovaVoice/2.1.0.9
    From: "Department Alarm" <sip:5555@10.10.40.127>;tag=f93f41ed-a517-1910-9f5d-00505694bcb9
    Call-ID: f93f41ed-a517-1910-9f5e-00505694bcb9@NovaLinkWIN2012
    Supported: x-siemens-sipqv2,100rel,replaces
    Organization: NovaLink
    To: <sip:5250@10.10.40.25>
    Contact: "Department Alarm" <sip:5555@10.10.40.127>
    Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,REFER,MESSAGE,INFO,PING,PRACK
    Content-Length: 305
    Content-Type: application/sdp
    Max-Forwards: 70

    v=0
    o=- 1519644752 1 IN IP4 10.10.40.127
    s=NovaVoice/2.1.0.9
    c=IN IP4 10.10.40.127
    t=0 0
    m=audio 6012 RTP/AVP 0 8 101 100
    a=sendrecv
    a=rtpmap:0 PCMU/8000/1
    a=rtpmap:8 PCMA/8000/1
    a=rtpmap:101 telephone-event/8000
    a=fmtp:101 0-16,32,36
    a=rtpmap:100 NSE/8000
    a=fmtp:100 192-193
    a=maxptime:240
246229961mS SIP Call Tx: 21
    SIP/2.0 100 Trying
    Via: SIP/2.0/UDP 10.10.40.127:5060;branch=z9hG4bKf93f41ed-a517-1910-9f60-00505694bcb9;rport
    From: "Department Alarm" <sip:5555@10.10.40.127>;tag=f93f41ed-a517-1910-9f5d-00505694bcb9
    Call-ID: f93f41ed-a517-1910-9f5e-00505694bcb9@NovaLinkWIN2012
    CSeq: 1 INVITE
    Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,REFER,NOTIFY,UPDATE
    Supported: timer,100rel
    Server: IP Office 10.1.0.1.0 build 3
    To: <sip:5250@10.10.40.25>;tag=b413404ebfee6333
    Content-Length: 0
246229994mS SIP Call Tx: 21
    SIP/2.0 180 Ringing
    Via: SIP/2.0/UDP 10.10.40.127:5060;branch=z9hG4bKf93f41ed-a517-1910-9f60-00505694bcb9;rport
    From: "Department Alarm" <sip:5555@10.10.40.127>;tag=f93f41ed-a517-1910-9f5d-00505694bcb9
    Call-ID: f93f41ed-a517-1910-9f5e-00505694bcb9@NovaLinkWIN2012
    CSeq: 1 INVITE
    Contact: <sip:5250@10.10.40.25:5060;transport=udp>
    Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,REFER,NOTIFY,UPDATE
    Supported: timer,100rel
    Server: IP Office 10.1.0.1.0 build 3
    To: <sip:5250@10.10.40.25>;tag=b413404ebfee6333
    Content-Length: 0
```

## 8. Conclusion

These Application Notes describe the configuration steps required for novaalert from novalink to interoperate with Avaya IP Office R10.1. All feature functionality and serviceability test cases were completed successfully with any issues and observations noted in **Section 2.2**.

## 9. Additional References

This section references the Avaya and novalink product documentation that are relevant to these Application Notes.

Product documentation for Avaya products may be found at <http://support.avaya.com>.

[1] *Avaya IP Office R10.1 Manager 10.1, Document Number 15-601011*

[2] *Avaya IP Office R10.1 Doc library*

Technical support can be obtained for novaalert from the website <http://www.novalink.ch/en/> or from the following.

novalink GmbH  
Business tower  
Zuercherstrasse 310  
8500 Frauenfeld  
Switzerland  
helpdesk@novalink.ch  
Phone: +41 52 762 66 77  
Fax: +41 52 762 66 99

---

**©2018 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).