Avaya Solution & Interoperability Test Lab

Application Notes for configuring novaalert V10 from novalink with Avaya IP Office R11.1 - Issue 1.0

Abstract

These Application Notes describe the configuration steps for novaalert from novalink with Avaya IP Office R11.1. 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 R11.1. novaalert integrates with Avaya IP Office using SIP trunks connecting to the primary server.

The Avaya IP Office consists of an IP Office Server Edition running on a virtual platform as the primary server with an IP Office IP500 V2 running as an expansion cabinet. Both systems are linked by IP Office Line IP trunks that can enable voice networking across these trunks to form a multi-site network. Each system in the solution automatically learns each other's extension numbers and usernames. This allows calls between systems and support for a range of internal call features.

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 IoT Devices, Web browser, Smartphone Apps, Databases, E-Mails, serial interfaces, potential free contacts, http(s) GET&POST, XML, 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), IoT Devices, XML, http(s) GET & POST, 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. If an alarm needs to be positively acknowledged, and it is not, novaalert can escalate that situation to other recipients, groups and devices. These Application Notes focus on those delivery methods which involve interaction with Avaya IP Office. The triggering of alarms was restricted to those methods which involve interaction with IP Office, that being alarms in the form of announcements being sent from novaalert to endpoints on IP Office, also using these endpoints to call into novaalert and record announcement messages to be sent out to other IP Office endpoints.

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. Alarms can be sent to busy stations that are already on a call by using the Service Observe feature. If novalalert detects a busy signal, it then uses the Coaching Intrusion or Call Intrude feature on IP Office to break into that call and play the alarm message.

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 Primary Server with an IP500 V2 Expansion 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 Primary Server and novaalert with a dial-plan setup accordingly.

novaalert was manually configured using the web interface to send alert messages to endpoints on IP Office.

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

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

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

For the testing associated with these Application Notes, the interface between Avaya IP Office 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 endpoints according to the configuration made via the web interface. These included recording of alarms from SIP/H.323/Digital endpoints.

- Triggering of Alarms from novaalert GUI.
- Triggering of Alarms from Avaya endpoints.
- Triggering of Alarms from the PSTN.
- Delivery of voice recorded and TTS alarm to groups of SIP/H.323/Digital endpoints.
- Conference, with "Conference" ticked in the Alarm, the endpoints will be held by novaalert after the alarm message and put into a voice conference with all other voice targets/endpoints.

- Delivery of voice recorded and TTS alarm to SIP/H.323/Digital endpoints.
- Delivery of voice recorded and TTS alarm to Hunt Groups.
- Delivery of voice recorded and TTS alarm to groups of SIP/H.323/Digital endpoints.
- Conference, with “Conference” ticked in the Alarm, the endpoints will be held by novaalert after the alarm message and put into a voice conference with all other voice targets/endpoints.
- 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 to demonstrate permission verification to trigger alarms.
- Intrusion of Alarms to busy extensions using the Call Intrude Short Code.
- Escalation, delivery of an alarm to another user such as a manager or perhaps a secretary if the initial user fails to answer the alarm.
- 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. A Short Code for FNE was added in order to initiate the Call Intrude Short Code; this was done because using the Call Intrude Short Code directly by novaalert results in a forbidden so it must use the FNE for Mobile Call Control followed by the Call Intrude Short Code.
2. 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
Businesstower
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 Expansion. The connection between the novaalert and the IP Office solution uses SIP trunks.

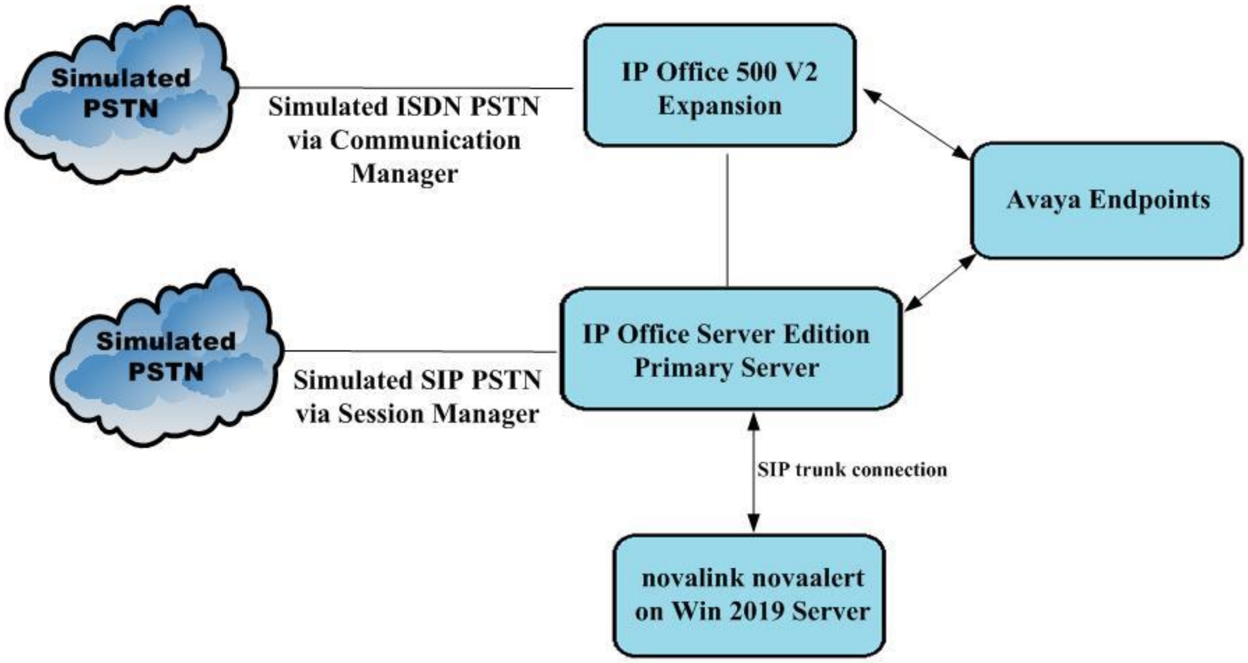

Simulated PSTN
Simulated ISDN PSTN via Communication Manager
IP Office 500 V2 Expansion
Avaya Endpoints
Simulated PSTN
Simulated SIP PSTN via Session Manager
IP Office Server Edition Primary Server
SIP trunk connection
novalink novaalert on Win 2019 Server

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

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya IP Office Server Edition Primary Server running on a Virtual Platform	11.1.2.2.0 Build 20
Avaya IP Office 500 V2 Expansion	11.1.2.2.0 Build 20
Avaya J179 IP Phone (H.323)	6.8304
Avaya J159 IP Phone (SIP)	4.0.7.0.7
Avaya 9508 Digital Deskphone	R0.60
Avaya Workplace for Windows (SIP)	R3.22.0.64(SIP)
novalink novaalert running on a Windows 2019 virtual server	10.5.0.9

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 R11.1. Note that IP Office Server Edition requires an Expansion IP500 V2 R11.1 to support analog or digital endpoints.

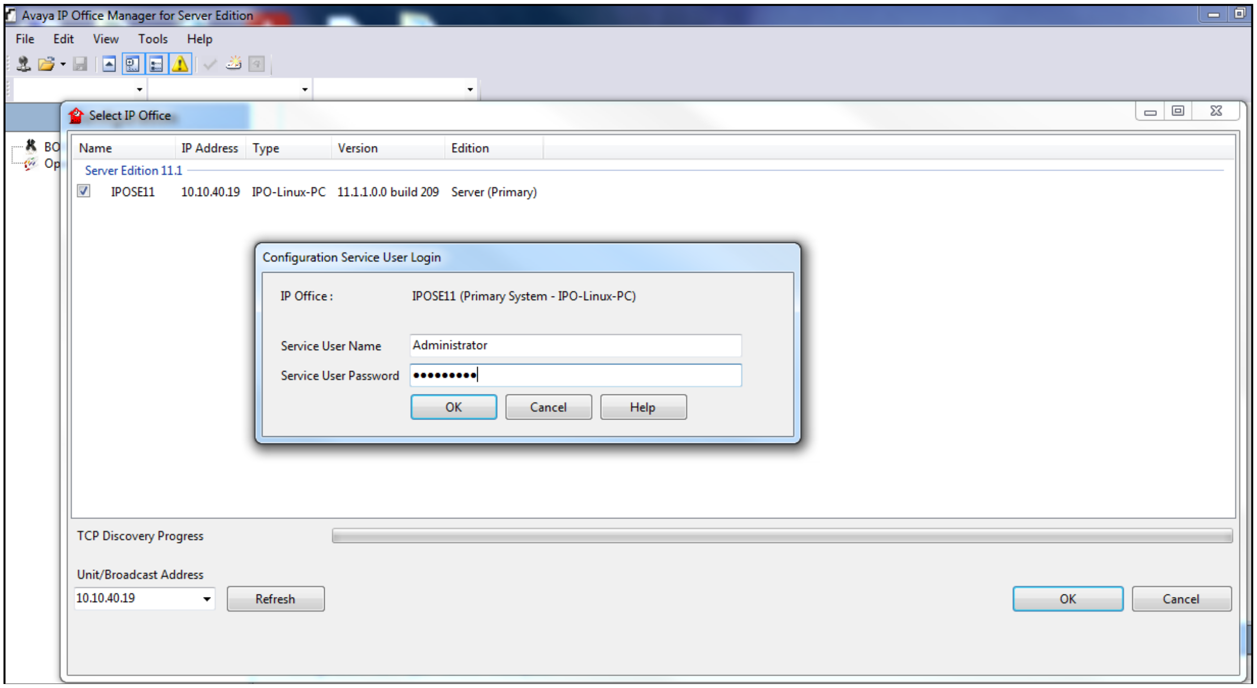
5. Configure Avaya IP Office

Configuration and verification operations on 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 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 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 IP Office Manager

From the 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 IP Office using the appropriate credentials to receive its configuration.



Name	IP Address	Type	Version	Edition
Server Edition 11.1				
☑ IPOSE11	10.10.40.19	IPO-Linux-PC	11.1.1.0.0 build 209	Server (Primary)

IP Office : IPOSE11 (Primary System - IPO-Linux-PC)

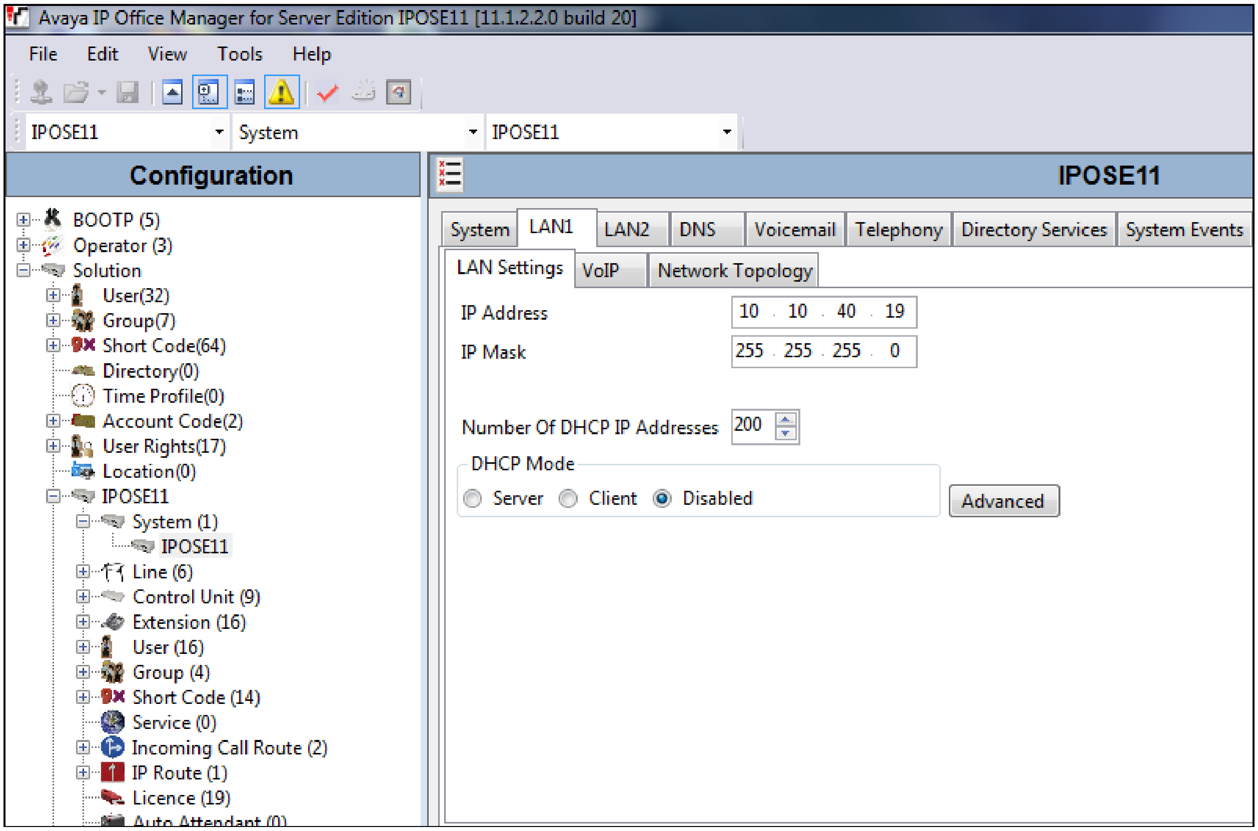
Service User Name: Administrator

Service User Password: •••••••••

Unit/Broadcast Address: 10.10.40.19

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.



IP Address 10 . 10 . 40 . 19

IP Mask 255 . 255 . 255 . 0

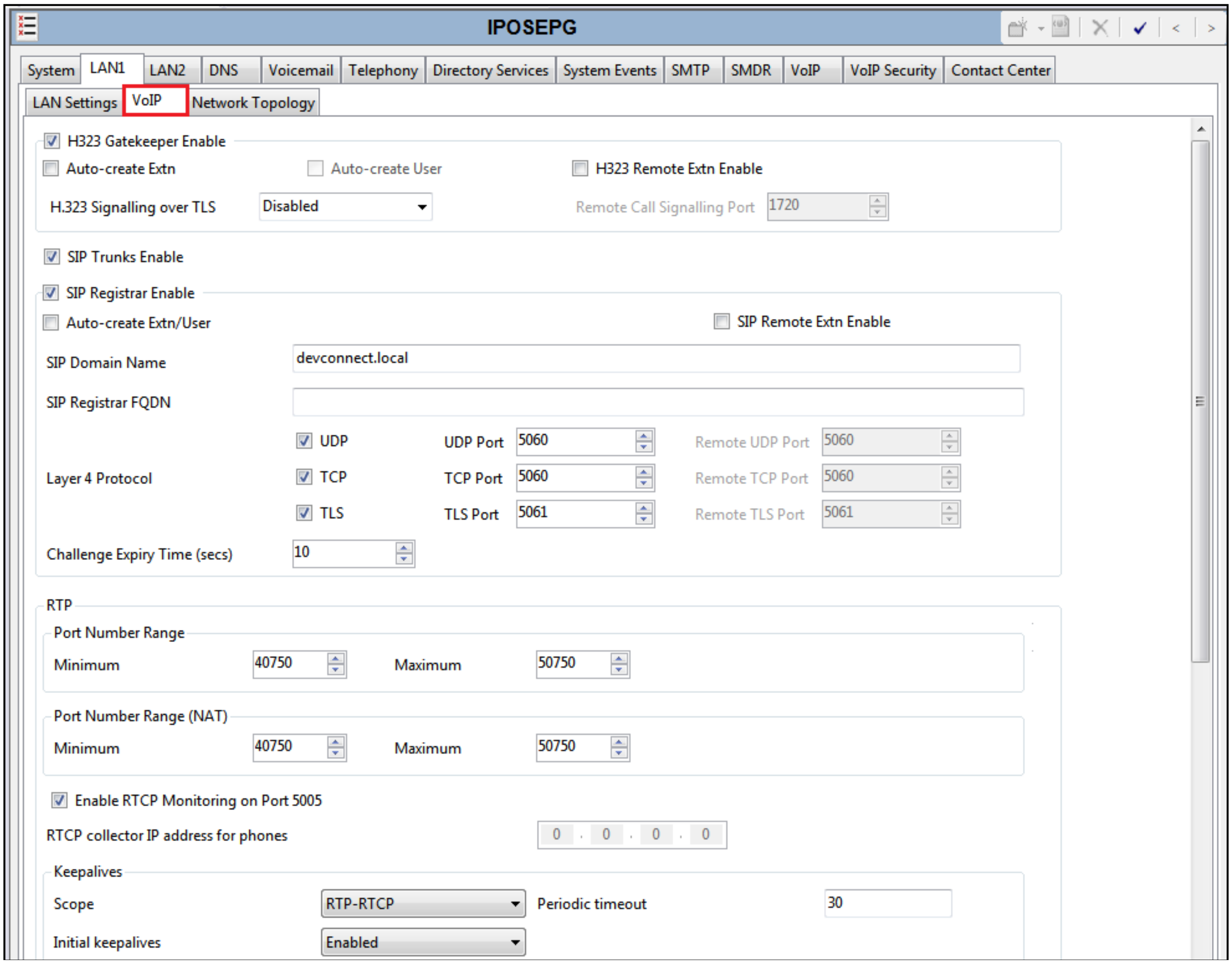
Number Of DHCP IP Addresses 200

DHCP Mode ○ Server ○ Client ● Disabled

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

1. **SIP Trunks Enable**.
2. **SIP Registrar Enable**.
3. **SIP 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.



☑ H323 Gatekeeper Enable

☐ Auto-create Extn ☐ Auto-create User ☐ H323 Remote Extn Enable

H.323 Signalling over TLS: Disabled Remote Call Signalling Port: 1720

☑ SIP Trunks Enable

☑ SIP Registrar Enable

☐ Auto-create Extn/User ☐ SIP Remote Extn Enable

SIP Domain Name: devconnect.local

SIP Registrar FQDN:

Layer 4 Protocol:
☑ UDP UDP Port: 5060 Remote UDP Port: 5060
☑ TCP TCP Port: 5060 Remote TCP Port: 5060
☑ TLS TLS Port: 5061 Remote TLS Port: 5061

Challenge Expiry Time (secs): 10

RTP

Port Number Range
Minimum: 40750 Maximum: 50750

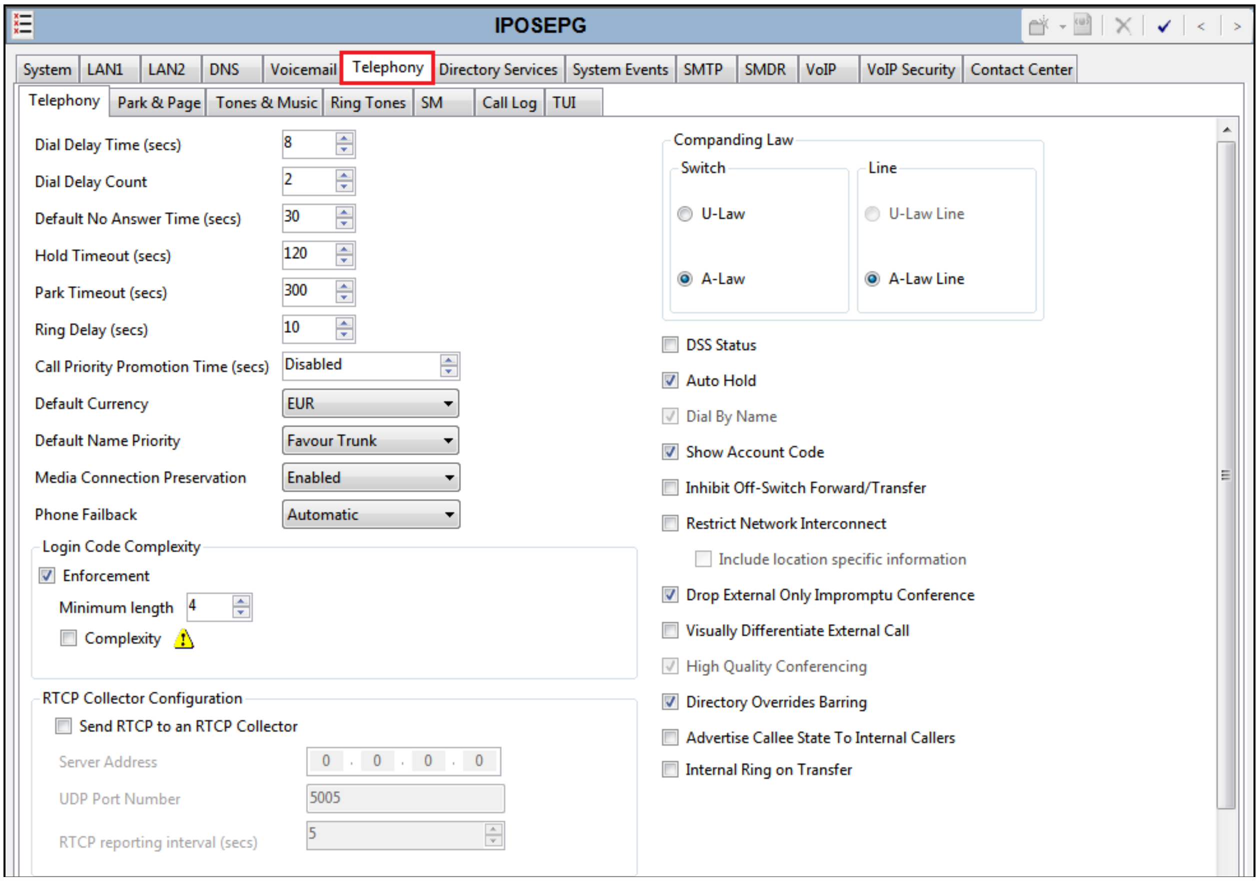
Port Number Range (NAT)
Minimum: 40750 Maximum: 50750

☑ Enable RTCP Monitoring on Port 5005

RTCP collector IP address for phones: 0 . 0 . 0 . 0

Keepalives
Scope: RTP-RTCP Periodic timeout: 30
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.



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

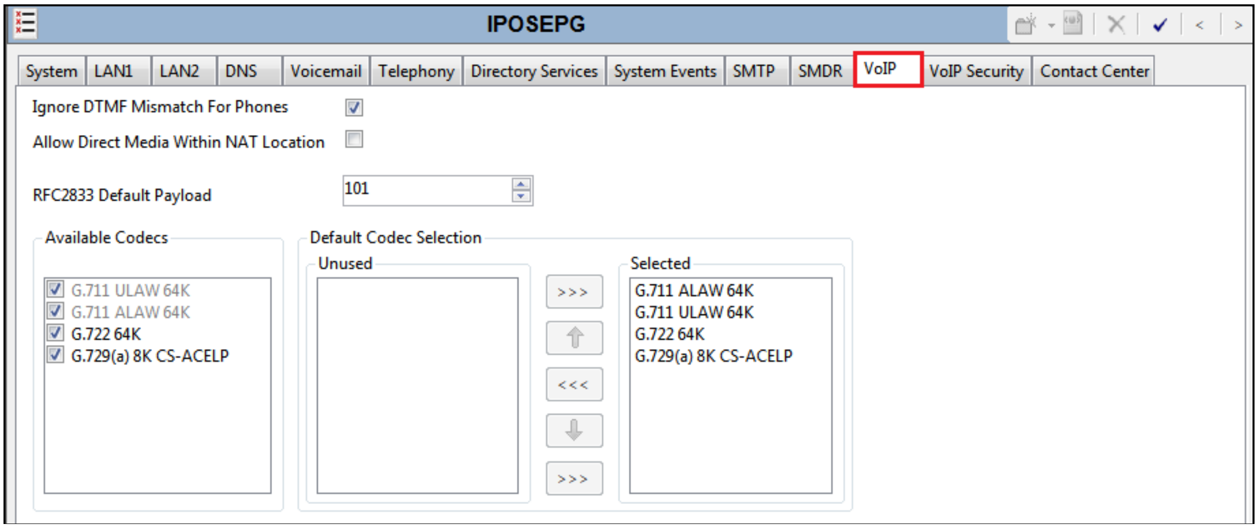
☑ High Quality Conferencing

☑ 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.



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

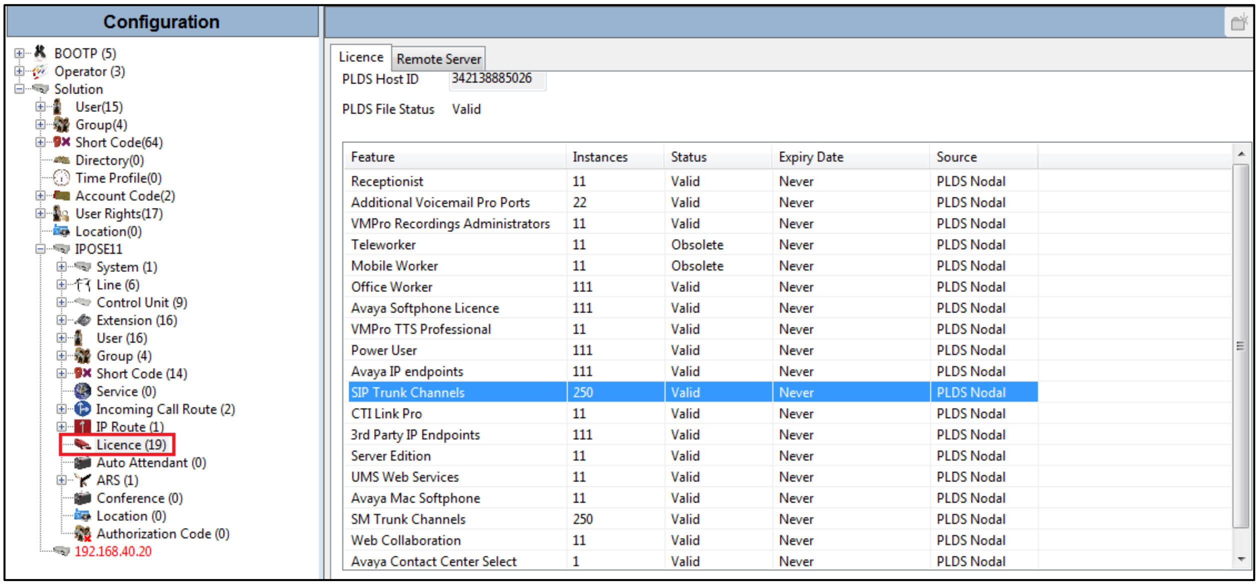
G.711 ULAW 64K

G.722 64K

G.729(a) 8K CS-ACELP

5.3. Display License Information

To ensure that there are enough licenses for all that is required, click on **License** in the left window and observe the licenses shown in the main window. **SIP Trunk Channels** is of significance here as the alarms are sent over a SIP trunk to IP Office.



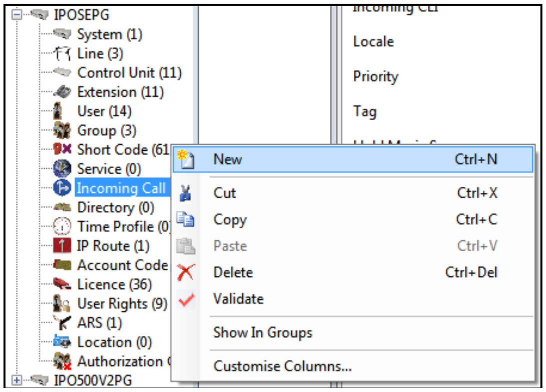
PLDS Host ID 342138885026

PLDS File Status Valid

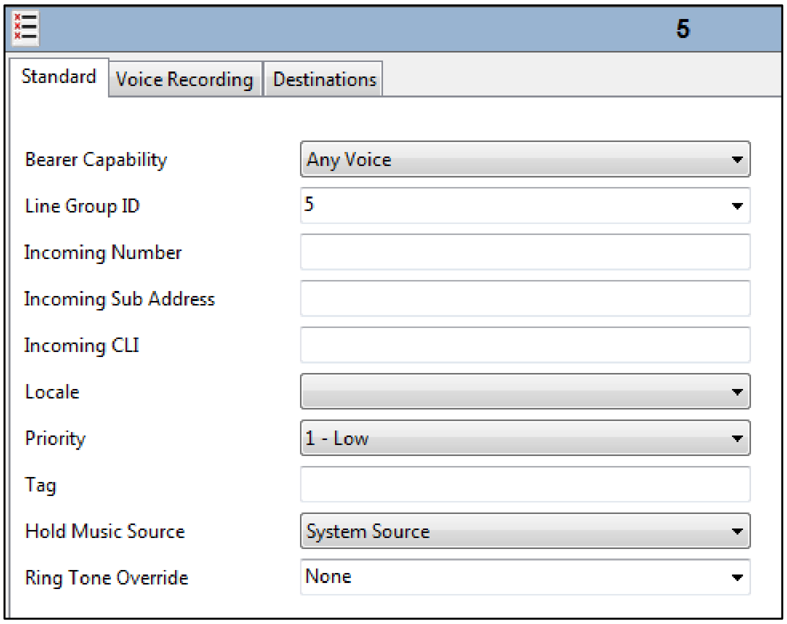
Feature	Instances	Status	Expiry Date	Source
Receptionist	11	Valid	Never	PLDS Nodal
Additional Voicemail Pro Ports	22	Valid	Never	PLDS Nodal
VMPro Recordings Administrators	11	Valid	Never	PLDS Nodal
Teleworker	11	Obsolete	Never	PLDS Nodal
Mobile Worker	11	Obsolete	Never	PLDS Nodal
Office Worker	111	Valid	Never	PLDS Nodal
Avaya Softphone Licence	111	Valid	Never	PLDS Nodal
VMPro TTS Professional	11	Valid	Never	PLDS Nodal
Power User	111	Valid	Never	PLDS Nodal
Avaya IP endpoints	111	Valid	Never	PLDS Nodal
SIP Trunk Channels	250	Valid	Never	PLDS Nodal
CTI Link Pro	11	Valid	Never	PLDS Nodal
3rd Party IP Endpoints	111	Valid	Never	PLDS Nodal
Server Edition	11	Valid	Never	PLDS Nodal
UMS Web Services	11	Valid	Never	PLDS Nodal
Avaya Mac Softphone	11	Valid	Never	PLDS Nodal
SM Trunk Channels	250	Valid	Never	PLDS Nodal
Web Collaboration	11	Valid	Never	PLDS Nodal
Avaya Contact Center Select	1	Valid	Never	PLDS Nodal

5.4. Configure Incoming Route for SIP Trunk

An incoming route must be added for the SIP trunk that will be setup in **Section 5.5**. Navigate to **Primary Server → Incoming Call Route**. Right click on **Incoming Call Route** select **New**.



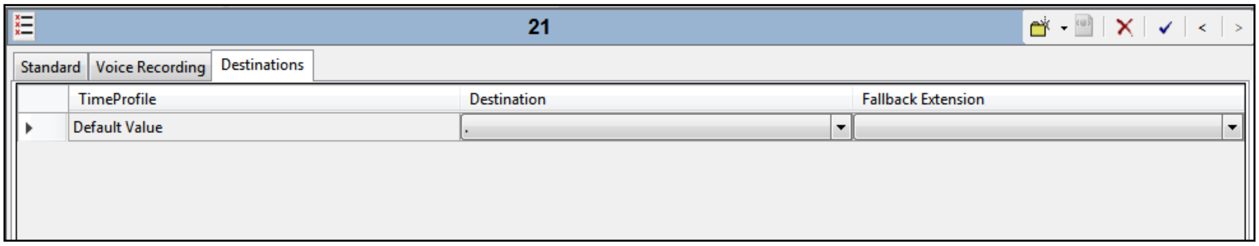
From the **Standard** tab, enter an available **Line Group ID**; this can be kept the same as the SIP Line that is to be created for convenience. **Bearer Capability** can be set to **Any Voice.**



5

Bearer Capability	Any Voice
Line Group ID	5
Incoming Number	
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None

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



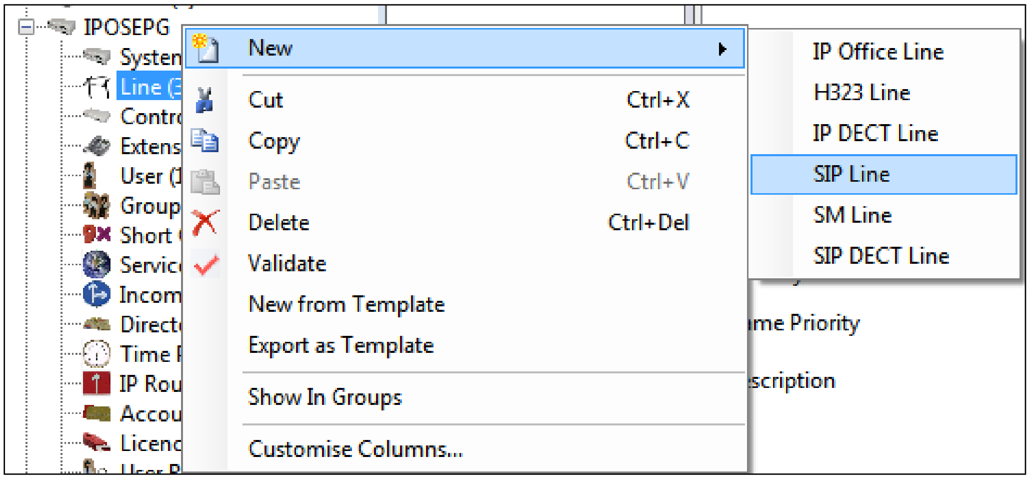
21

TimeProfile	Destination	Fallback Extension
Default Value	.	

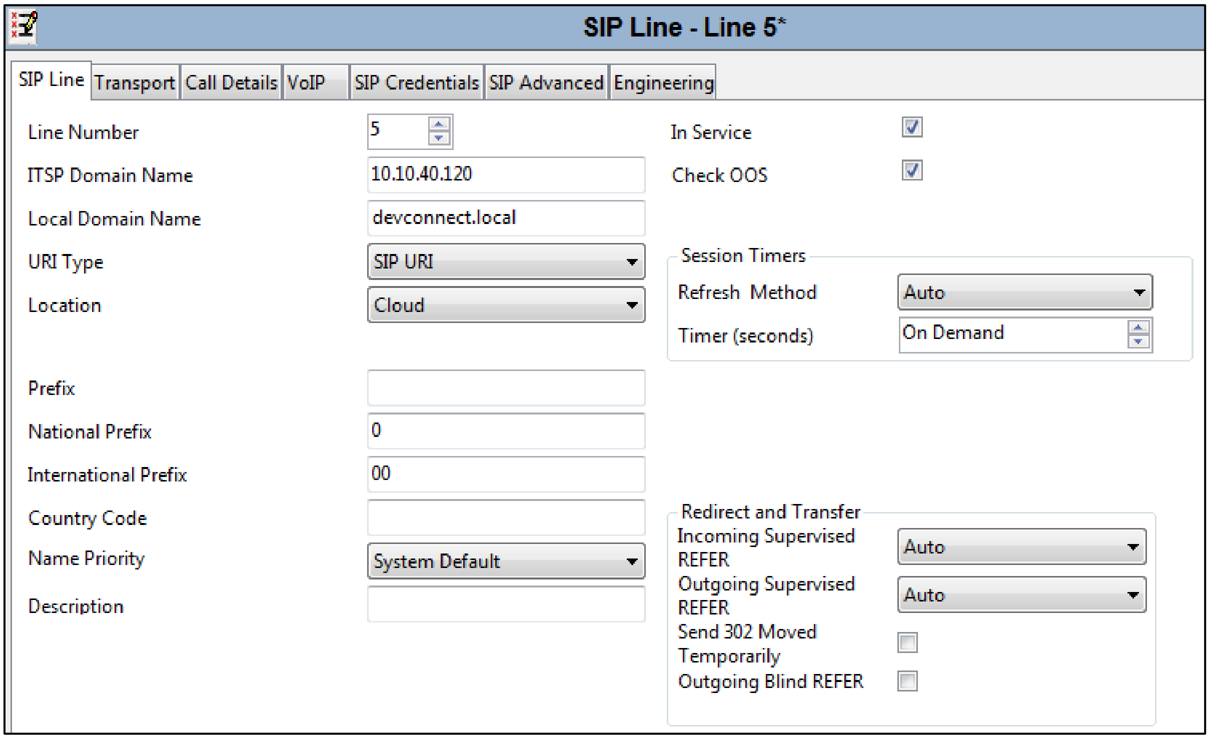
5.5. Configure SIP Trunk

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**.



Line Number	5
ITSP Domain Name	10.10.40.120
Local Domain Name	devconnect.local
URI Type	SIP URI
Location	Cloud
Prefix	
National Prefix	0
International Prefix	00
Country Code	
Name Priority	System Default
Description	
In Service	☑
Check OOS	☑

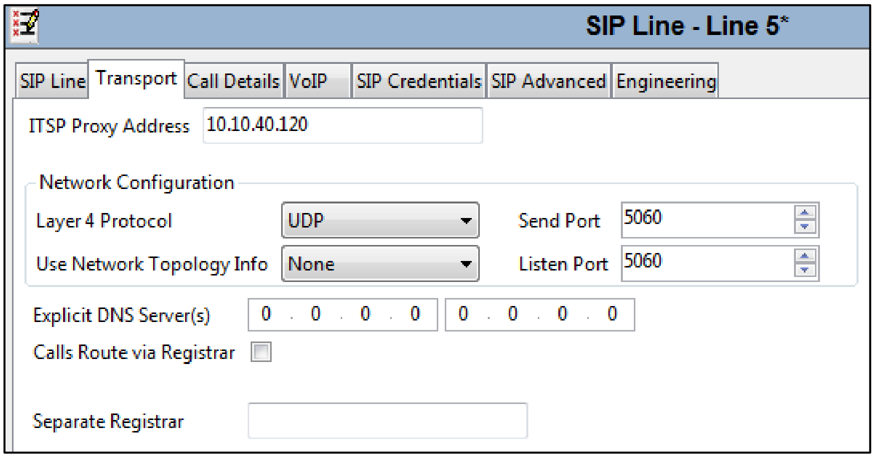
Session Timers

Refresh Method	Auto
Timer (seconds)	On Demand

Redirect and Transfer

Incoming Supervised REFER	Auto
Outgoing Supervised REFER	Auto
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**.



SIP Line - Line 5*

ITSP Proxy Address: 10.10.40.120

Network Configuration

Layer 4 Protocol: UDP

Send Port: 5060

Use Network Topology Info: None

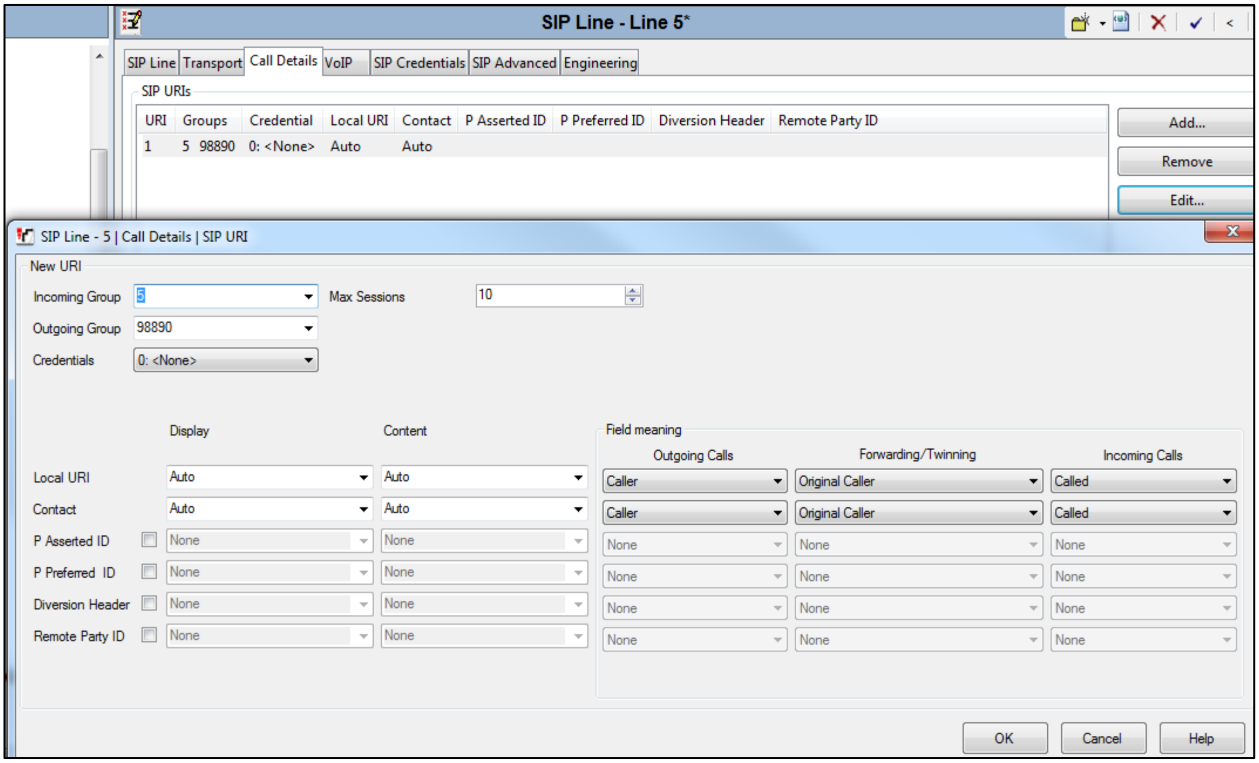
Listen Port: 5060

Explicit DNS Server(s): 0 . 0 . 0 . 0   0 . 0 . 0 . 0

Calls Route via Registrar □

Separate Registrar:

Click on the **Call Details** tab and click on **Add**. The **Incoming Group** and **Outgoing Group** are added here. **Max Sessions** was set to **10** for compliance testing, this number will depend on the number of SIP Licenses on IP Office and novaalert. Other settings were left as default, as shown below.



SIP Line - Line 5*

SIP URIs

URI	Groups	Credential	Local URI	Contact	P Asserted ID	P Preferred ID	Diversion Header	Remote Party ID
1	5 98890	0: <None>	Auto	Auto				

SIP Line - 5 | Call Details | SIP URI

New URI

Incoming Group: 5

Max Sessions: 10

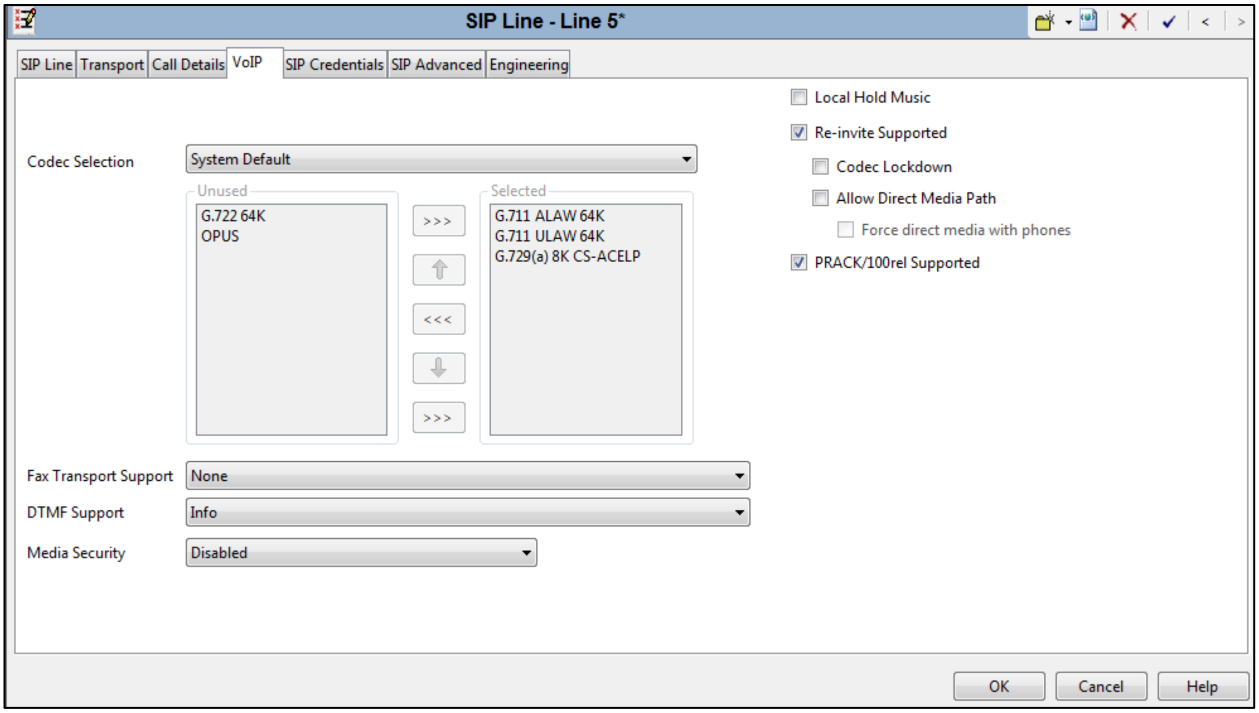
Outgoing Group: 98890

Credentials: 0: <None>

		Display	Content	Outgoing Calls	Forwarding/Twinning	Incoming Calls
Local URI		Auto	Auto	Caller	Original Caller	Called
Contact		Auto	Auto	Caller	Original Caller	Called
P Asserted ID	□	None	None	None	None	None
P Preferred ID	□	None	None	None	None	None
Diversion Header	□	None	None	None	None	None
Remote Party ID	□	None	None	None	None	None

Field meaning

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.



SIP Line - Line 5*

Codec Selection: System Default

Unused: G.722 64K, OPUS

Selected: G.711 ALAW 64K, G.711 ULAW 64K, G.729(a) 8K CS-ACELP

Fax Transport Support: None

DTMF Support: Info

Media Security: Disabled

□ Local Hold Music

☑ Re-invite Supported

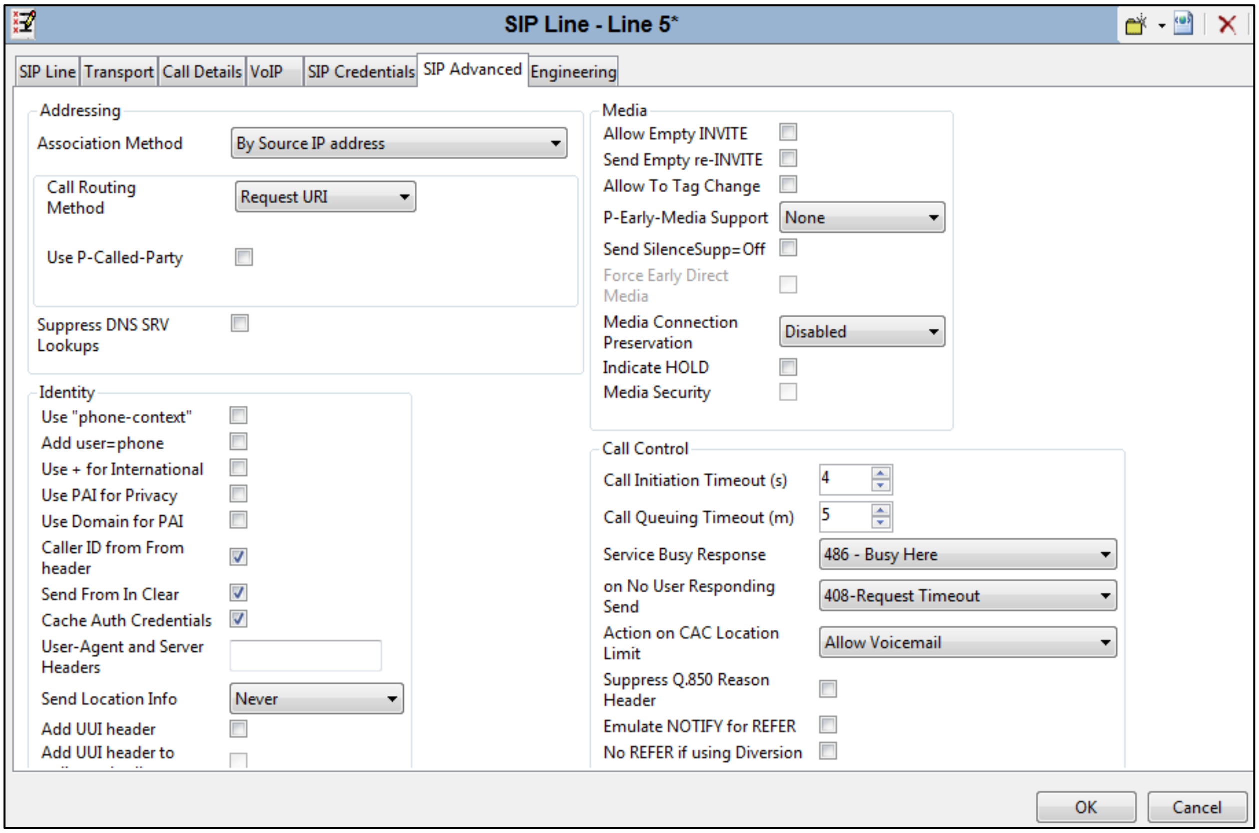
□ Codec Lockdown

□ Allow Direct Media Path

□ Force direct media with phones

☑ PRACK/100rel Supported

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 and that will complete the **SIP Line** setup.



SIP Line - Line 5*

Addressing

Association Method: By Source IP address

Call Routing Method: Request URI

Use P-Called-Party ☐

Suppress DNS SRV Lookups ☐

Identity

Use "phone-context" ☐

Add user=phone ☐

Use + for International ☐

Use PAI for Privacy ☐

Use Domain for PAI ☐

Caller ID from From header ☑

Send From In Clear ☑

Cache Auth Credentials ☑

User-Agent and Server Headers:

Send Location Info: Never

Add UUI header ☐

Add UUI header to ☐

Media

Allow Empty INVITE ☐

Send Empty re-INVITE ☐

Allow To Tag Change ☐

P-Early-Media Support: None

Send SilenceSupp=Off ☐

Force Early Direct Media ☐

Media Connection Preservation: Disabled

Indicate HOLD ☐

Media Security ☐

Call Control

Call Initiation Timeout (s): 4

Call Queuing Timeout (m): 5

Service Busy Response: 486 - Busy Here

on No User Responding Send: 408-Request Timeout

Action on CAC Location Limit: Allow Voicemail

Suppress Q.850 Reason Header ☐

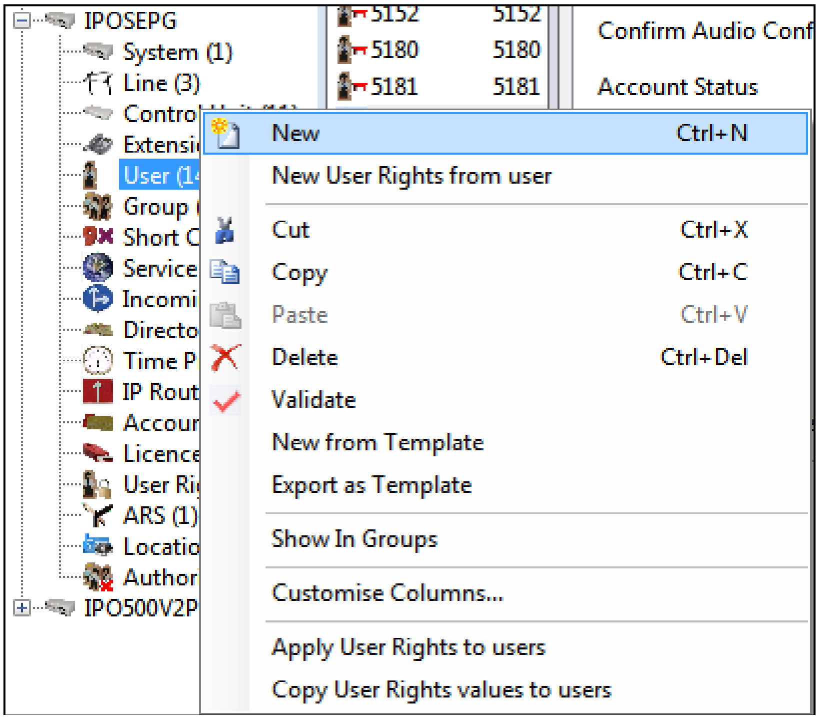
Emulate NOTIFY for REFER ☐

No REFER if using Diversion ☐

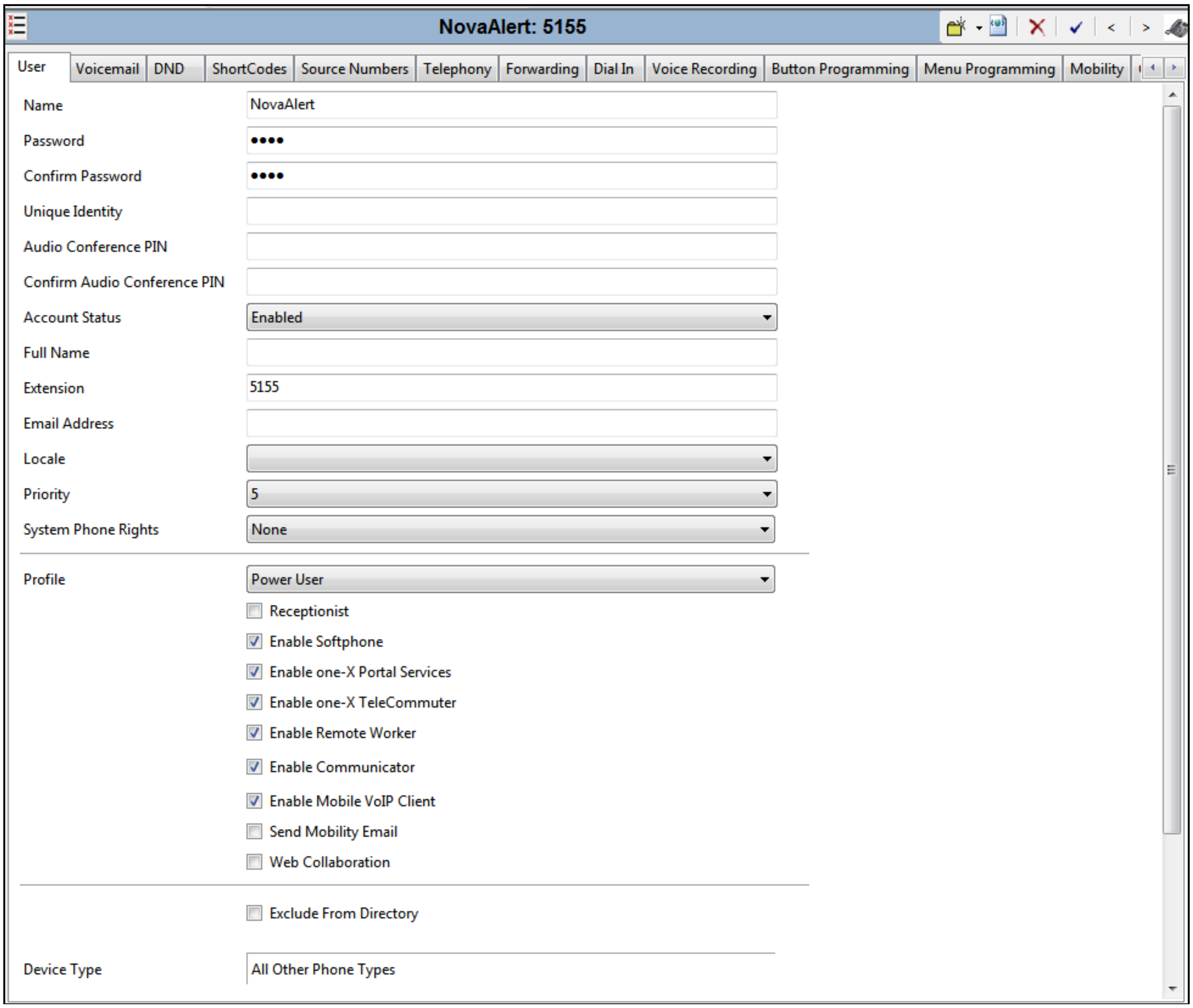
5.6. Configure User for Mobile Call Control

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**, **Confirm Password** and **Extension** and ensure that **Power User** is selected as the **Profile**.



NovaAlert: 5155

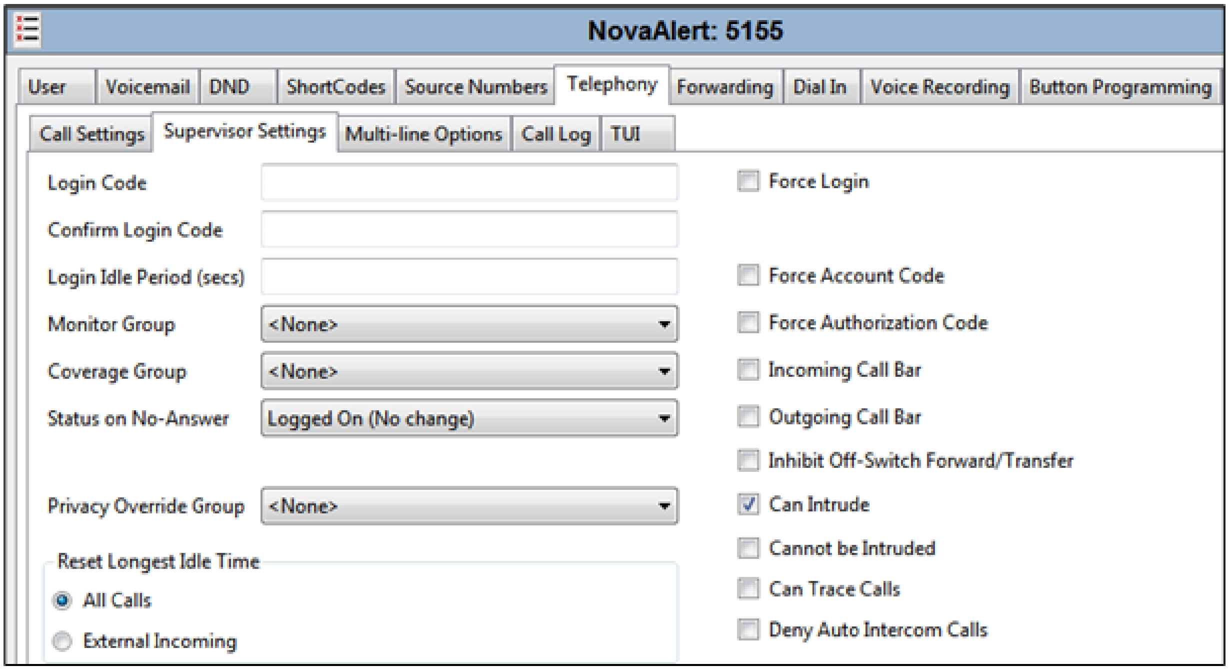
Name	NovaAlert
Password	••••
Confirm Password	••••
Unique Identity	
Audio Conference PIN	
Confirm Audio Conference PIN	
Account Status	Enabled
Full Name	
Extension	5155
Email Address	
Locale	
Priority	5
System Phone Rights	None
Profile	Power User

- □ 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.



Login Code

Confirm Login Code

Login Idle Period (secs)

Monitor Group <None>

Coverage Group <None>

Status on No-Answer Logged On (No change)

Privacy Override Group <None>

Reset Longest Idle Time

● All Calls

○ External Incoming

□ Force Login

□ Force Account Code

□ Force Authorization Code

□ Incoming Call Bar

□ Outgoing Call Bar

□ Inhibit Off-Switch Forward/Transfer

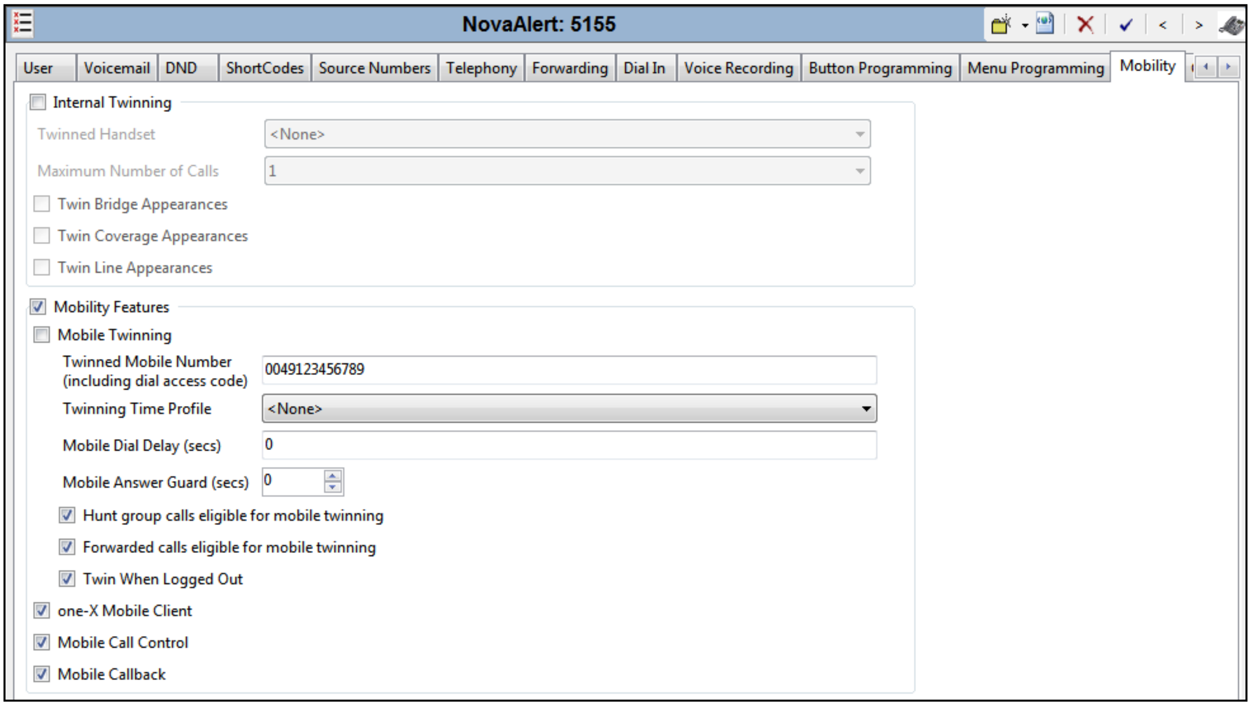
☑ Can Intrude

□ Cannot be Intruded

□ Can Trace Calls

□ 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).



□ Internal Twinning

Twinned Handset <None>

Maximum Number of Calls 1

□ Twin Bridge Appearances

□ Twin Coverage Appearances

□ Twin Line Appearances

☑ Mobility Features

□ Mobile Twinning

Twinned Mobile Number (including dial access code) 0049123456789

Twinning Time Profile <None>

Mobile Dial Delay (secs) 0

Mobile Answer Guard (secs) 0

☑ Hunt group calls eligible for mobile twinning

☑ Forwarded calls eligible for mobile twinning

☑ Twin When Logged Out

☑ one-X Mobile Client

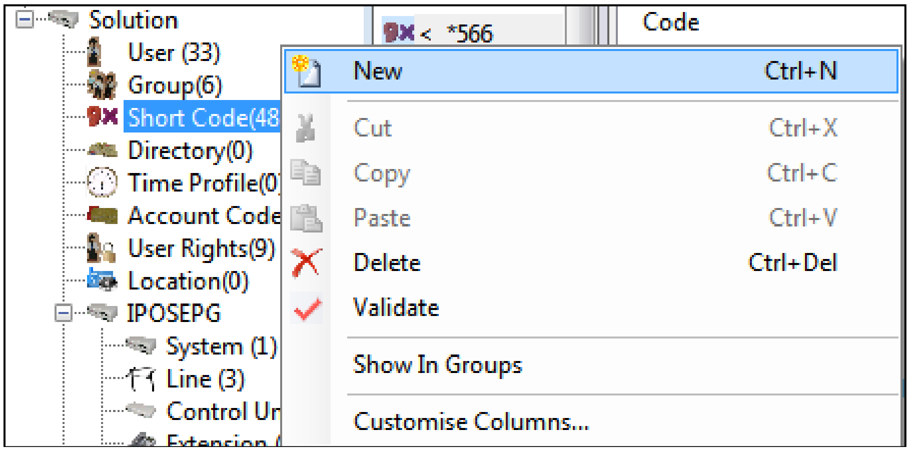
☑ Mobile Call Control

☑ Mobile Callback

5.7. Configure Short Codes

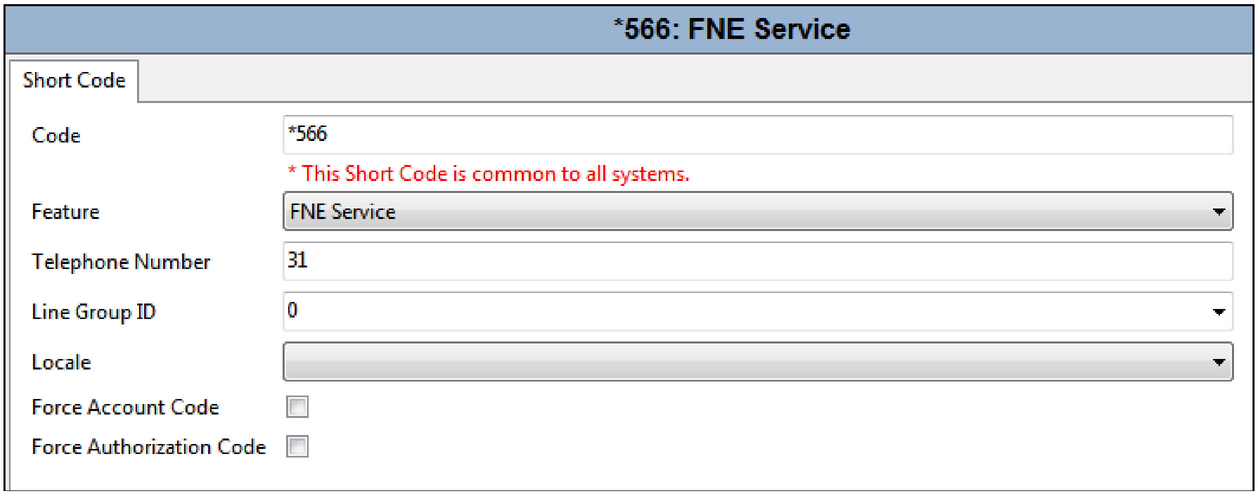
Short Codes can be created for both systems, i.e., both the Primary Server and the Expansion Server. A short code such as Call Intrude or Coaching Intrusion would need to be created across all systems so navigate to **Solution → Short Code**, right-click on **Short Code** and select **New** as shown.

Note: A short code may already be in place to dial out to the PSTN, however a new short code will need to be added to dial out to novaalert to create an alarm from IP Office phones.



5.7.1. 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

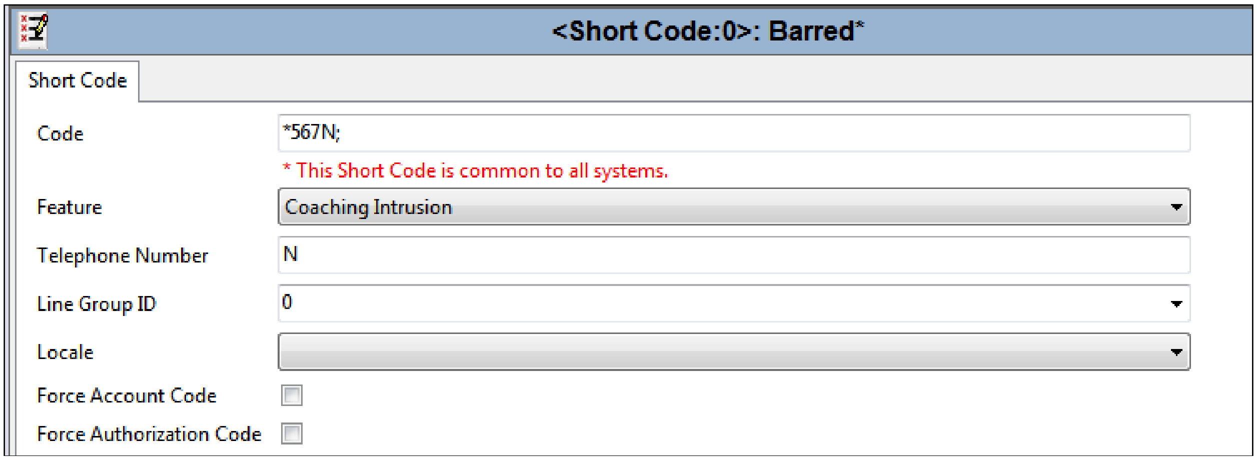
Short Code

Code	*566 * This Short Code is common to all systems.
Feature	FNE Service
Telephone Number	31
Line Group ID	0
Locale	
Force Account Code	□
Force Authorization Code	□

5.7.2. 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 dialled. This same Short Code will be configured in **Section 6.1**.

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

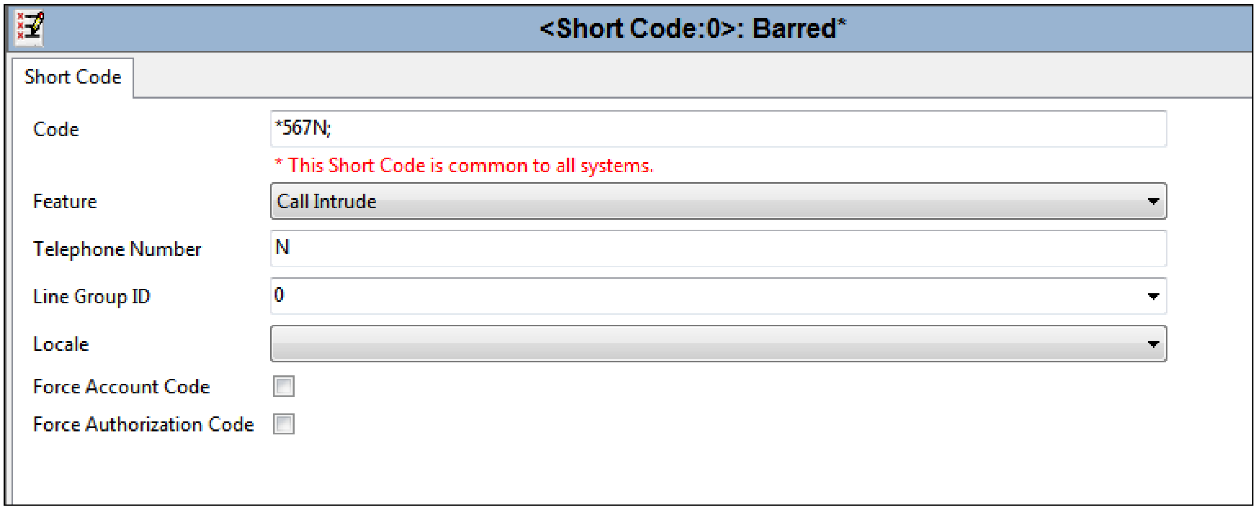


<Short Code:0>: Barred*

Code	*567N;
	* This Short Code is common to all systems.
Feature	Coaching Intrusion
Telephone Number	N
Line Group ID	0
Locale	
Force Account Code	□
Force Authorization Code	□

5.7.3. 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.

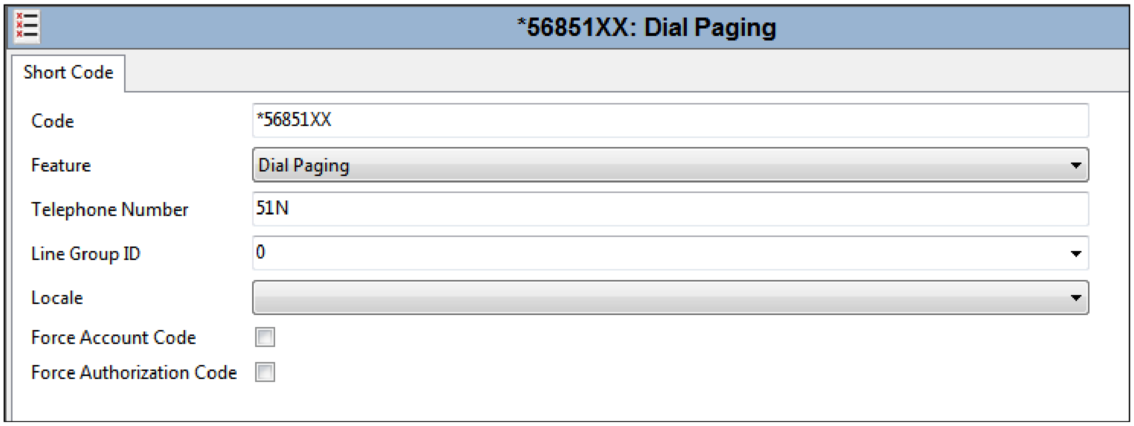


<Short Code:0>: Barred*

Code	*567N;
	* This Short Code is common to all systems.
Feature	Call Intrude
Telephone Number	N
Line Group ID	0
Locale	
Force Account Code	□
Force Authorization Code	□

5.7.4. 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.



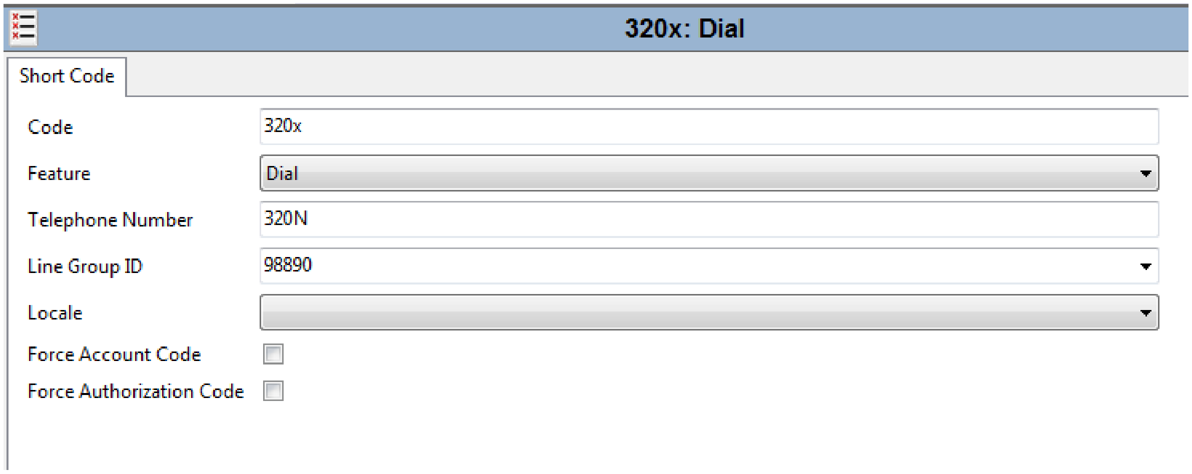
*56851XX: Dial Paging

Short Code

Code	*56851XX
Feature	Dial Paging
Telephone Number	51N
Line Group ID	0
Locale	
Force Account Code	□
Force Authorization Code	□

5.7.5. Short Code to dial into novaalert

The following short code was added to dial out from IP Office over the SIP Trunk created in **Section 5.5**. It was decided that 3200 – 3209 would be assigned to novaalert to dial into various services, therefore **320x** was added as a short code to dial out of the same **Line Group ID** that was created in **Section 5.5**.



320x: Dial

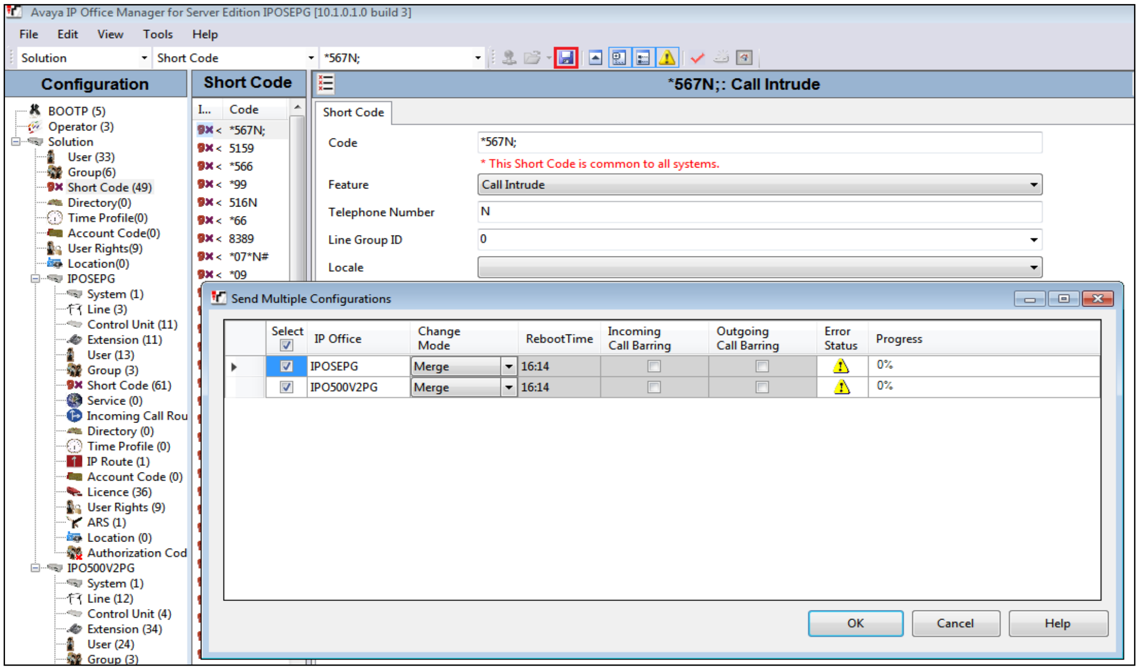
Short Code

Code	320x
Feature	Dial
Telephone Number	320N
Line Group ID	98890
Locale	
Force Account Code	□
Force Authorization Code	□

A similar Short Code was added on the Expansion Cabinet to allow calls to come across to the Primary Server, the Line Group ID will be that of the SCN line. Calls to 320x are made out from the Primary Server so these calls must come to the Primary Server from any and all expansion cabinets first.

5.8. 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.



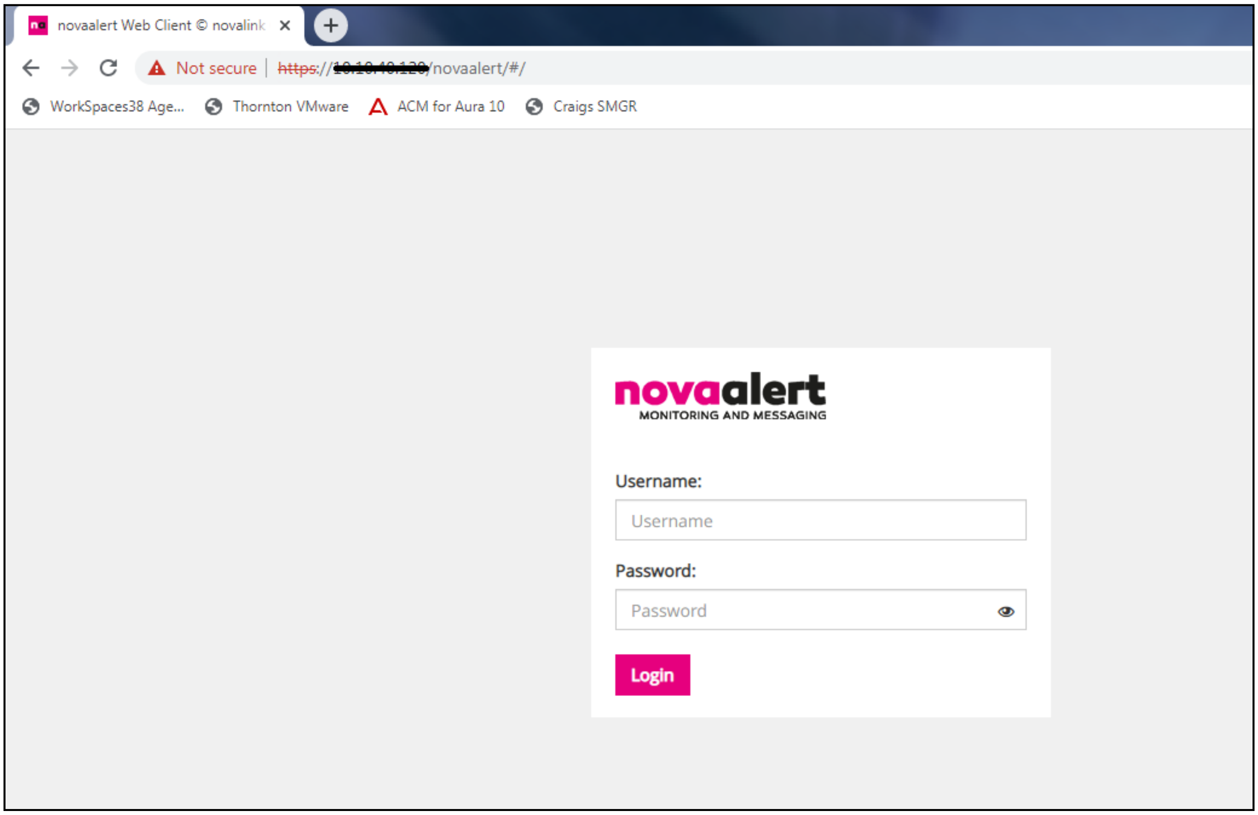
Code	*567N;
	* This Short Code is common to all systems.
Feature	Call Intrude
Telephone Number	N
Line Group ID	0
Locale	

Select ☑	IP Office	Change Mode	RebootTime	Incoming Call Barring	Outgoing Call Barring	Error Status	Progress
☑	IPOSEPG	Merge	16:14	☐	☐	⚠	0%
☑	IPO500V2PG	Merge	16:14	☐	☐	⚠	0%

6. Configuration of novalink novaalert

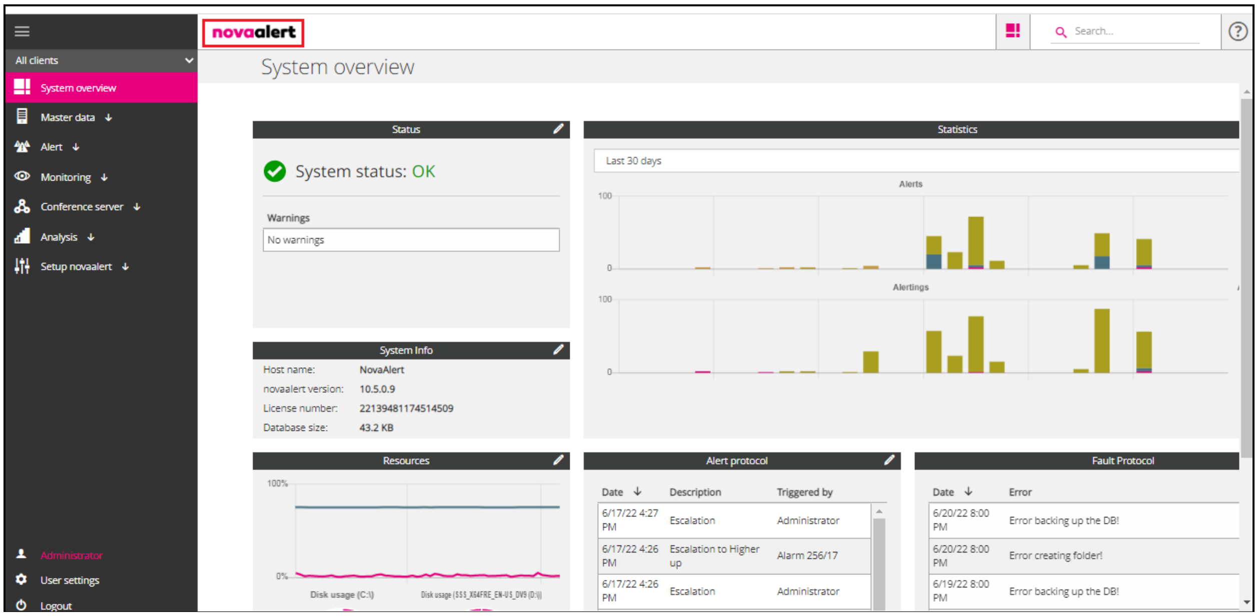
It is assumed that novaalert is already installed and configured by a novalink-certified engineer. The following shows the steps that can be carried out in order to make changes or to examine a working system. The screen shots were taken after compliance testing was completed successfully and will show 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://<novaalertIP>/novaalert** was used. The following screen shown is asking for the **Username** and **Password**, enter these and click on the **Login** button.



6.1. Connection setup to IP Office (SIP Trunk)

Once logged in, click on the **novaalert** icon at the top of the page, this will get to the System Configuration area.



System overview

System status: OK

Warnings: No warnings

System Info

Host name:	NovaAlert
novaalert version:	10.5.0.9
License number:	22139481174514509
Database size:	43.2 KB

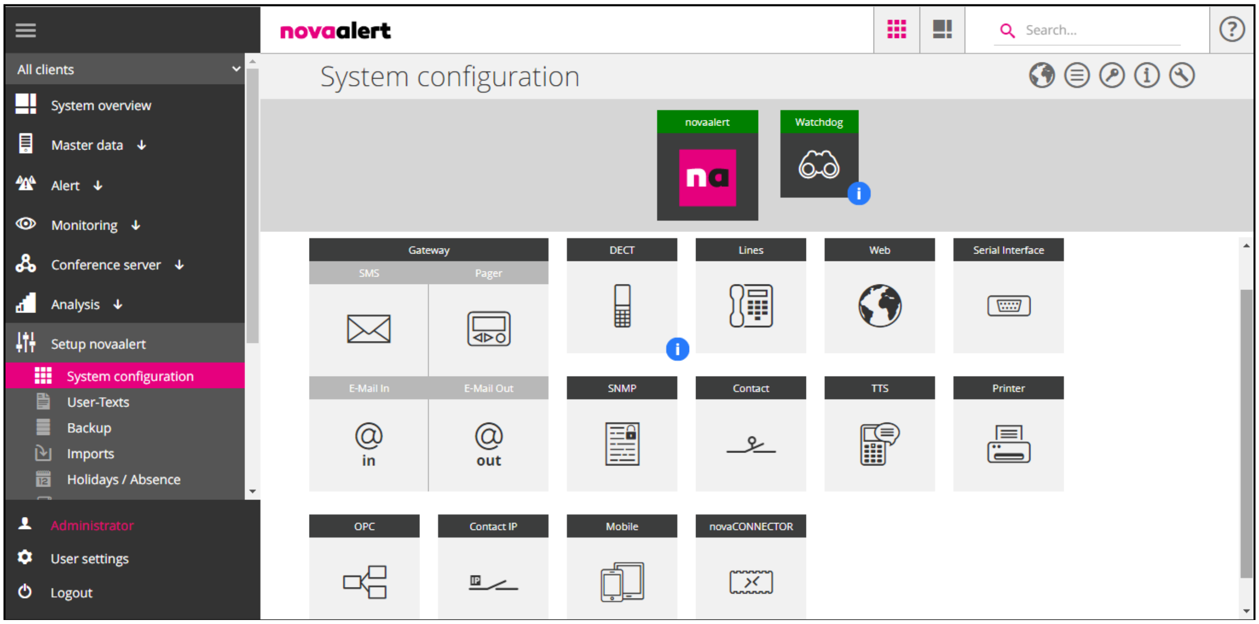
Alert protocol

Date	Description	Triggered by
6/17/22 4:27 PM	Escalation	Administrator
6/17/22 4:26 PM	Escalation to Higher up	Alarm 256/17
6/17/22 4:26 PM	Escalation	Administrator

Fault Protocol

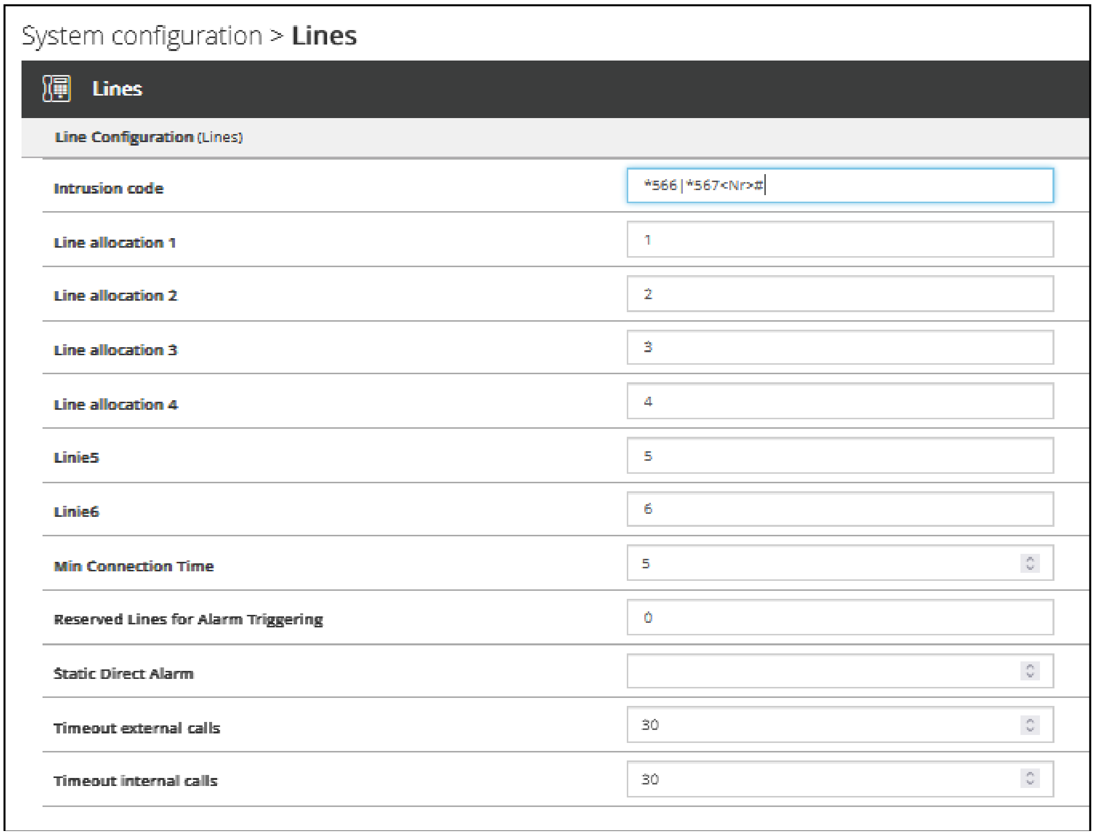
Date	Error
6/20/22 8:00 PM	Error backing up the DB!
6/20/22 8:00 PM	Error creating folder!
6/19/22 8:00 PM	Error backing up the DB!

Click on the **Lines** icon, in the main window. All configuration with regards to the SIP connection to IP Office is set in this area.



The first section shows the **Line Configuration**. Displayed below was the setup used for compliance testing; the most notable field is the **Intrusion code** which is referenced in **Section 5.7**. This allows an alarm to get to a telephone, even if it is busy. 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 *567xxxx# is entered using DTMF.

Note: It is important to copy and paste the following ***566¦*567<Nr>#** directly from here into the **Intrusion code** field on the PC, as the "pipe" icon may not work correctly if typed from the local keyboard.



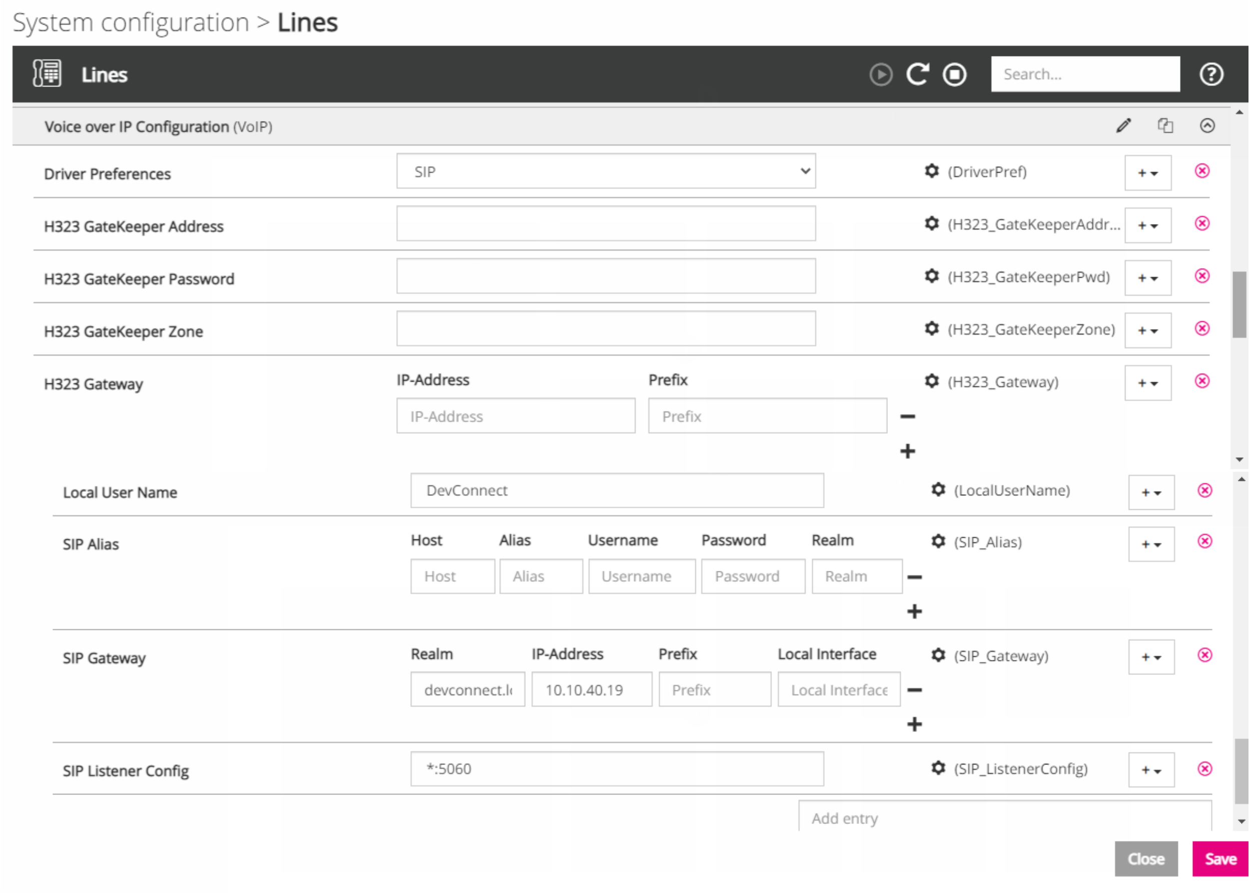
System configuration > **Lines**

Lines

Line Configuration (Lines)

Intrusion code	*566|*567<Nr>#
Line allocation 1	1
Line allocation 2	2
Line allocation 3	3
Line allocation 4	4
Linie5	5
Linie6	6
Min Connection Time	5
Reserved Lines for Alarm Triggering	0
Static Direct Alarm	
Timeout external calls	30
Timeout internal calls	30

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**. If DNS is not being used, please enter the IP Address in both fields, **Realm** and **IP-Address**.


System configuration > Lines

Lines

Voice over IP Configuration (VoIP)

Driver Preferences: SIP (DriverPref)

H323 GateKeeper Address: (H323_GateKeeperAddr...)

H323 GateKeeper Password: (H323_GateKeeperPwd)

H323 GateKeeper Zone: (H323_GateKeeperZone)

H323 Gateway: IP-Address: IP-Address, Prefix: Prefix (H323_Gateway)

Local User Name: DevConnect (LocalUserName)

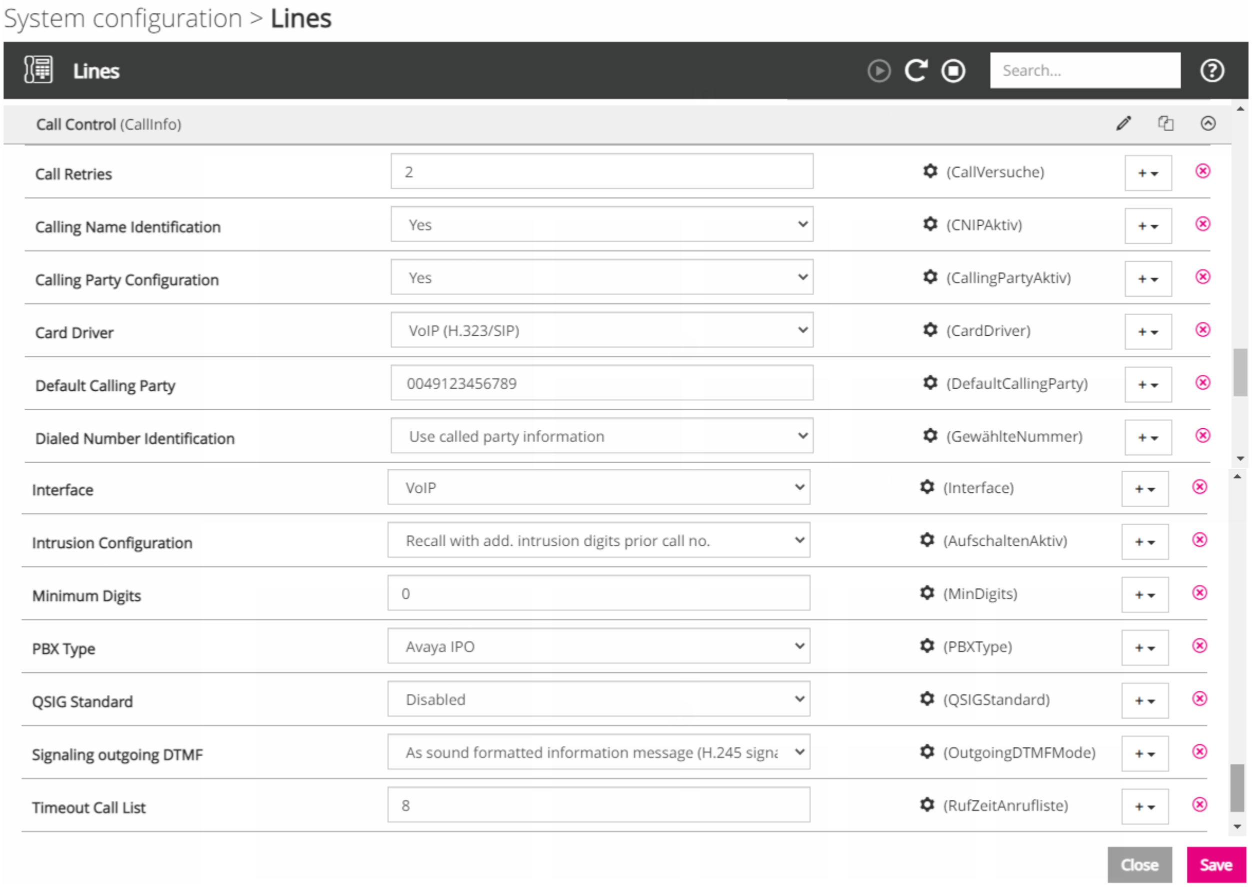
SIP Alias: Host: Host, Alias: Alias, Username: Username, Password: Password, Realm: Realm (SIP_Alias)

SIP Gateway: Realm: devconnect.l, IP-Address: 10.10.40.19, Prefix: Prefix, Local Interface: Local Interface (SIP_Gateway)

SIP Listener Config: *:5060 (SIP_ListenerConfig)

Add entry

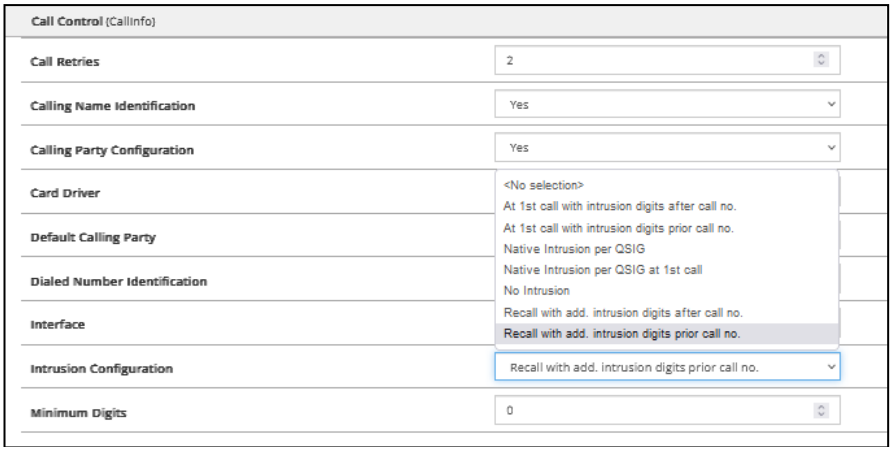
Click on **Call Control**, which is the next section down. The following shows the configuration used for compliance testing. The **PBX Type** is set to **Avaya IPO** and the **Card Driver** set to **VoIP (H.323/SIP)**. The **Default Calling Party** is entered and this much match exactly the Twinned Mobile Number configured for the FNE User in **Section 5.6**. **Signaling outgoing DTMF** is chosen as shown on the next page.



Call Control (CallInfo)

Call Retries	2	(CallVersuche)
Calling Name Identification	Yes	(CNIPAktiv)
Calling Party Configuration	Yes	(CallingPartyAktiv)
Card Driver	VoIP (H.323/SIP)	(CardDriver)
Default Calling Party	0049123456789	(DefaultCallingParty)
Dialed Number Identification	Use called party information	(GewählteNummer)
Interface	VoIP	(Interface)
Intrusion Configuration	Recall with add. intrusion digits prior call no.	(AufschaltenAktiv)
Minimum Digits	0	(MinDigits)
PBX Type	Avaya IPO	(PBXType)
QSIG Standard	Disabled	(QSIGStandard)
Signaling outgoing DTMF	As sound formatted information message (H.245 signa	(OutgoingDTMFMode)
Timeout Call List	8	(RufZeitAnrufliste)

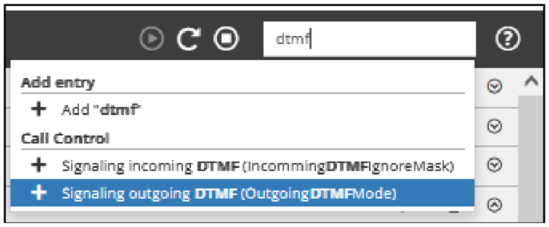
Intrusion Configuration is set as follows, **Recall with add. intrusion digits prior call no.**


<No selection>
At 1st call with intrusion digits after call no.
At 1st call with intrusion digits prior call no.
Native Intrusion per QSIG
Native Intrusion per QSIG at 1st call
No Intrusion
Recall with add. intrusion digits after call no.
Recall with add. intrusion digits prior call no.

Call Control (CallInfo)

Call Retries	2
Calling Name Identification	Yes
Calling Party Configuration	Yes
Card Driver	
Default Calling Party	
Dialed Number Identification	
Interface	
Intrusion Configuration	Recall with add. intrusion digits prior call no.
Minimum Digits	0

For compliance testing, the **Signaling outgoing DTMF** field was not present, and this field needed to be added manually. From the top right corner there is a search field where dtmf can be entered as shown below, this will bring up the various fields that can be added for DTMF. The **Signaling outgoing DTMF (OutgoingDTMFmode)** is added.


dtmf

Add entry

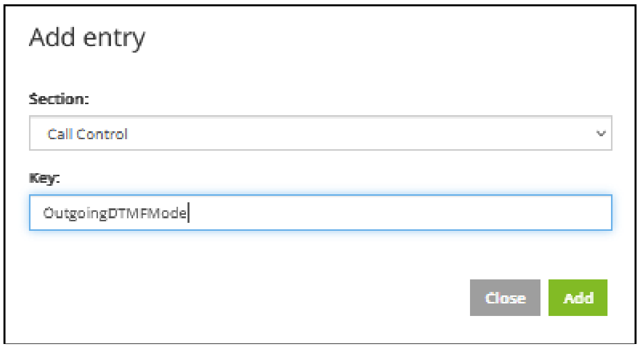
+ Add "dtmf"

Call Control

+ Signaling incoming DTMF (IncommingDTMFIgnoreMask)

+ Signaling outgoing DTMF (OutgoingDTMFMode)

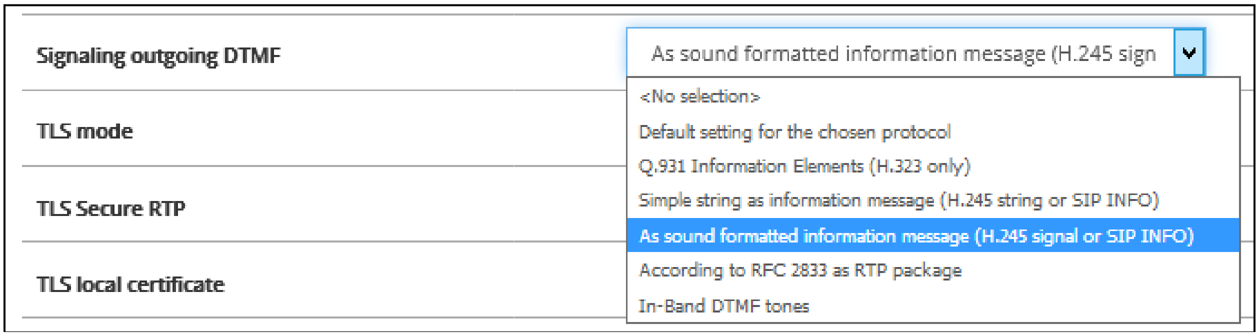
This entry is added to the **Call Control** Section and the **Key** is **OutgoingDTMFMode** as shown.


Add entry

Section: Call Control

Key: OutgoingDTMFMode

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 5.5**. The corresponding setting here is **As sound formatted information message (H.245 signal or SIP INFO)**.


Signaling outgoing DTMF: As sound formatted information message (H.245 sign

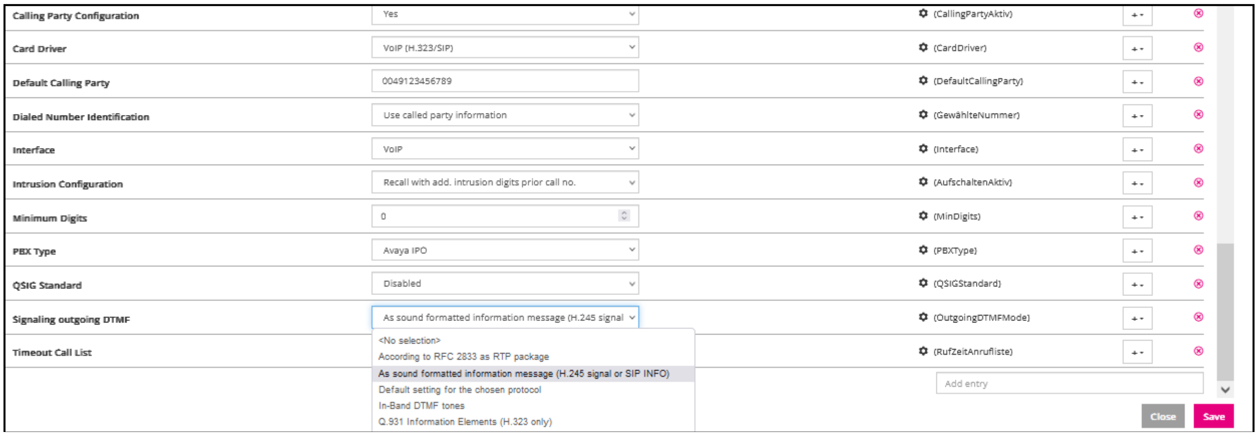
- <No selection>
- Default setting for the chosen protocol
- Q.931 Information Elements (H.323 only)
- Simple string as information message (H.245 string or SIP INFO)
- As sound formatted information message (H.245 signal or SIP INFO)
- According to RFC 2833 as RTP package
- In-Band DTMF tones

TLS mode

TLS Secure RTP

TLS local certificate

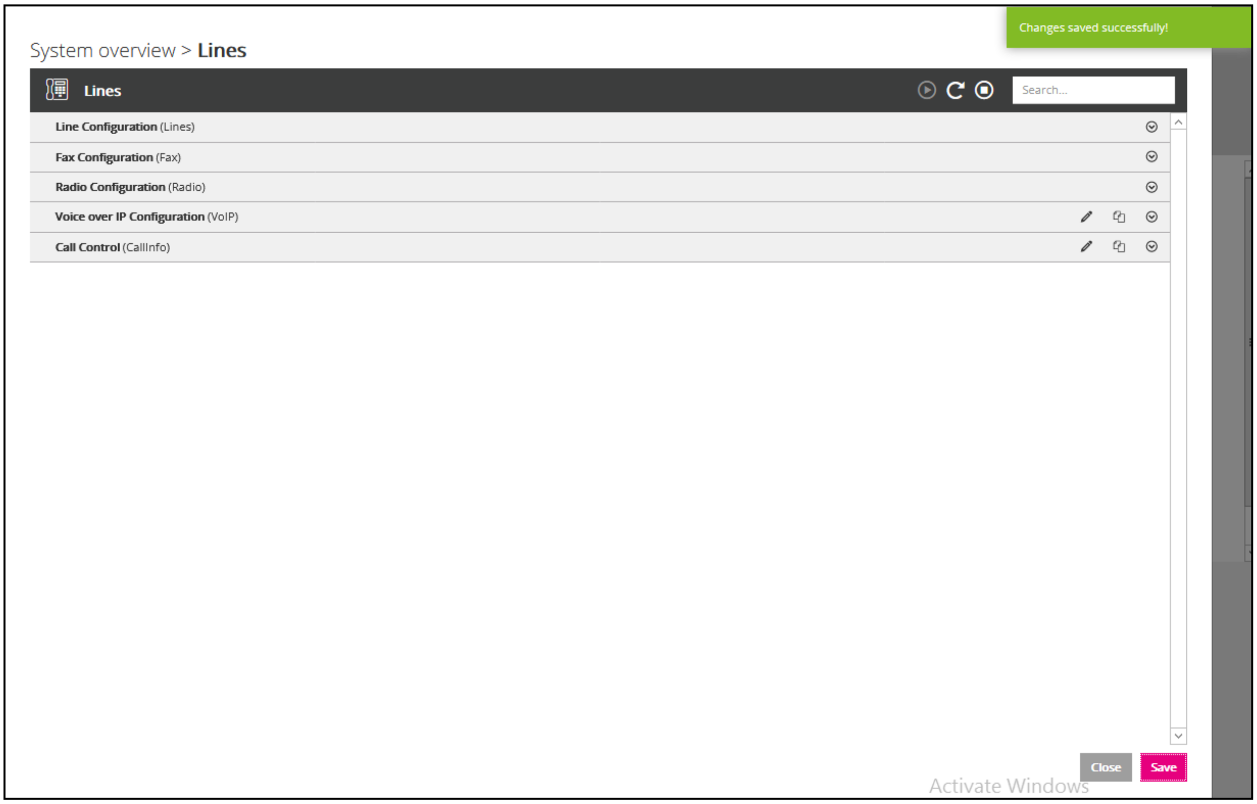
With everything entered correctly, click **Save** at the bottom right of the screen.



Calling Party Configuration	Yes	(CallingPartyAktiv)	+ -
Card Driver	VoIP (H.323/SIP)	(CardDriver)	+ -
Default Calling Party	0049123456789	(DefaultCallingParty)	+ -
Dialed Number Identification	Use called party information	(GewählteNummer)	+ -
Interface	VoIP	(Interface)	+ -
Intrusion Configuration	Recall with add. intrusion digits prior call no.	(AufschaltenAktiv)	+ -
Minimum Digits	0	(MinDigits)	+ -
PBX Type	Avaya IPO	(PBXType)	+ -
QSIG Standard	Disabled	(QSIGStandard)	+ -
Signaling outgoing DTMF	As sound formatted information message (H.245 signal	(OutgoingDTMFMode)	+ -
Timeout Call List		(RufZeitAnrufliste)	+ -

<No selection>
According to RFC 2833 as RTP package
As sound formatted information message (H.245 signal or SIP INFO)
Default setting for the chosen protocol
In-Band DTMF tones
Q.931 Information Elements (H.323 only)
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.



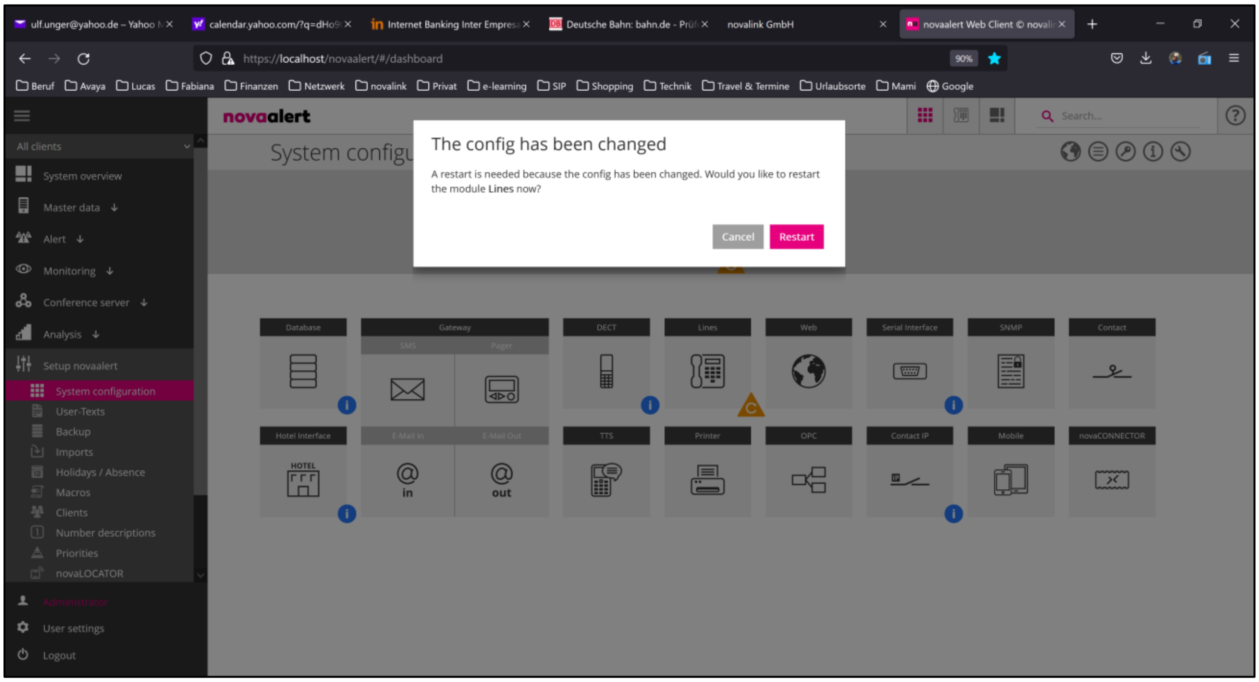
Changes saved successfully!

System overview > Lines

Lines

- Line Configuration (Lines)
- Fax Configuration (Fax)
- Radio Configuration (Radio)
- Voice over IP Configuration (VoIP)
- Call Control (CallInfo)

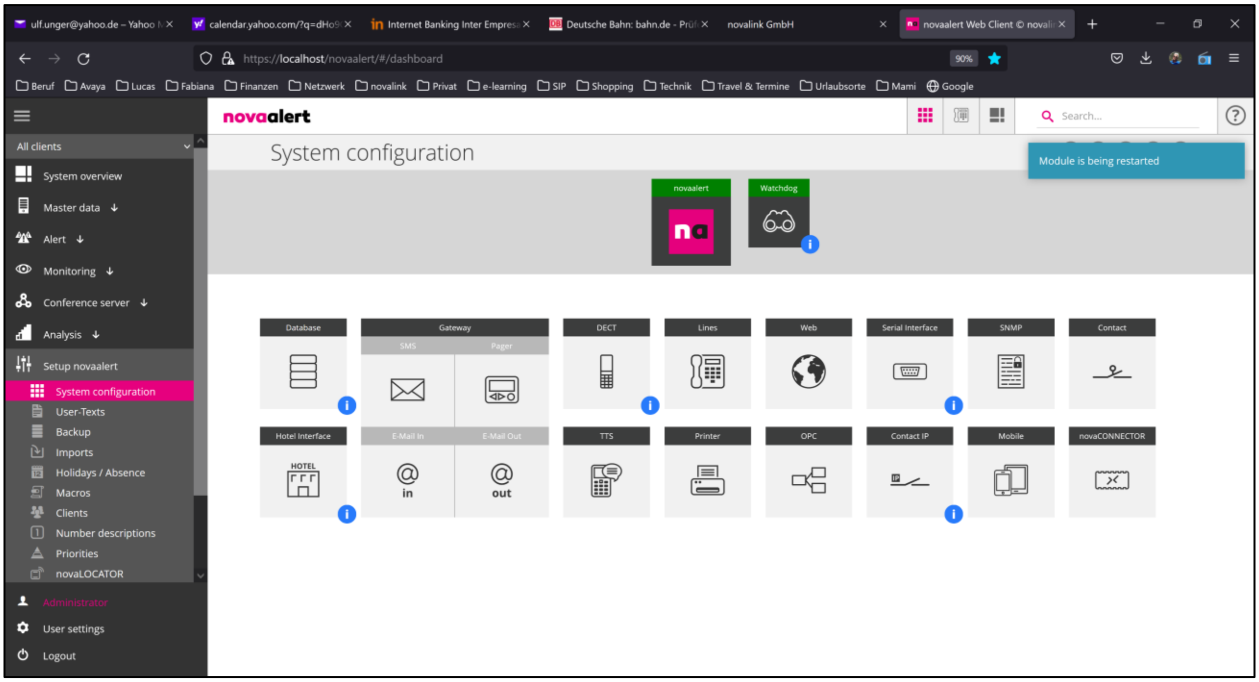
Once the setup is saved the following screen is popped asking to restart the module, click on **Restart**.



The config has been changed

A restart is needed because the config has been changed. Would you like to restart the module **Lines** now?

A message is displayed in the top right corner saying **Restarted module successfully** (not shown).

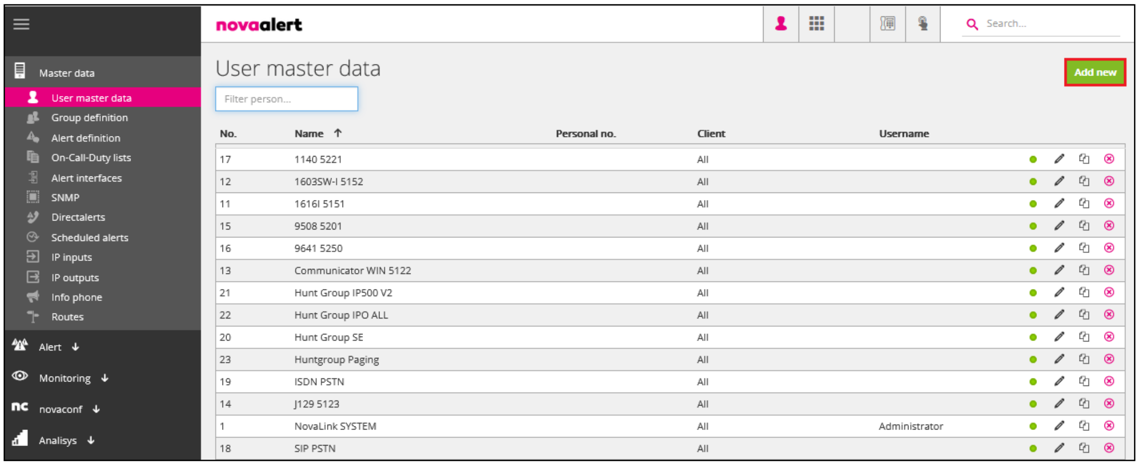


Module is being restarted

6.2. Create an Alarm to send to 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.

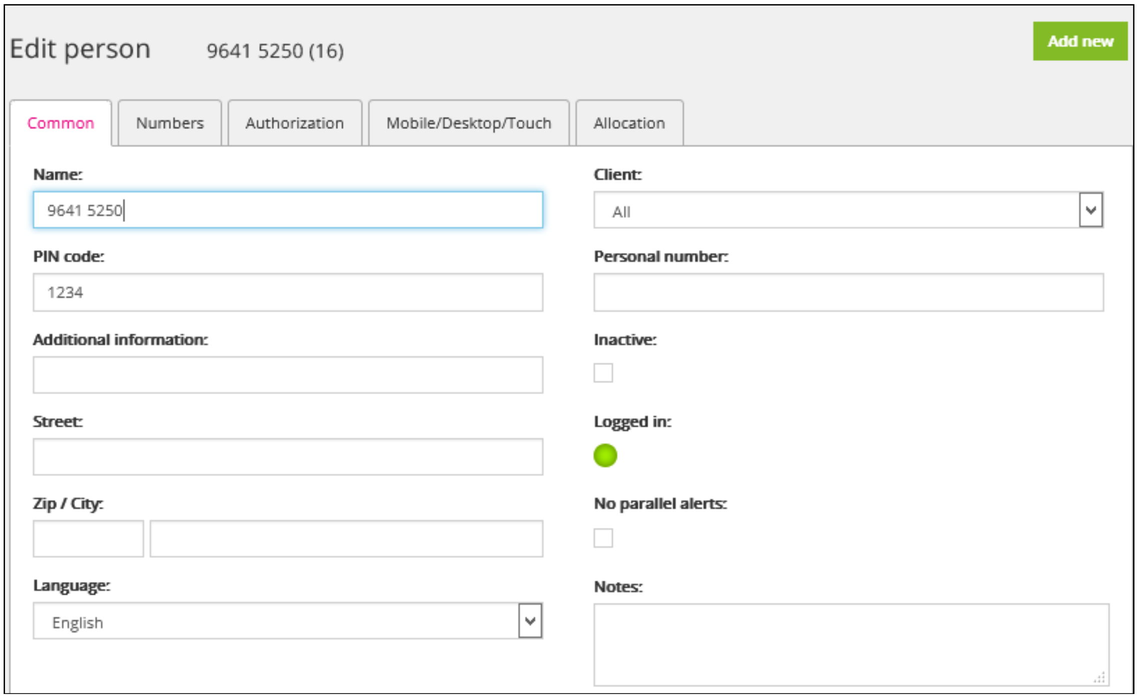


User master data

Filter person...

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)

Name: 9641 5250

PIN code: 1234

Additional information:

Street:

Zip / City:

Language: English

Client: All

Personal number:

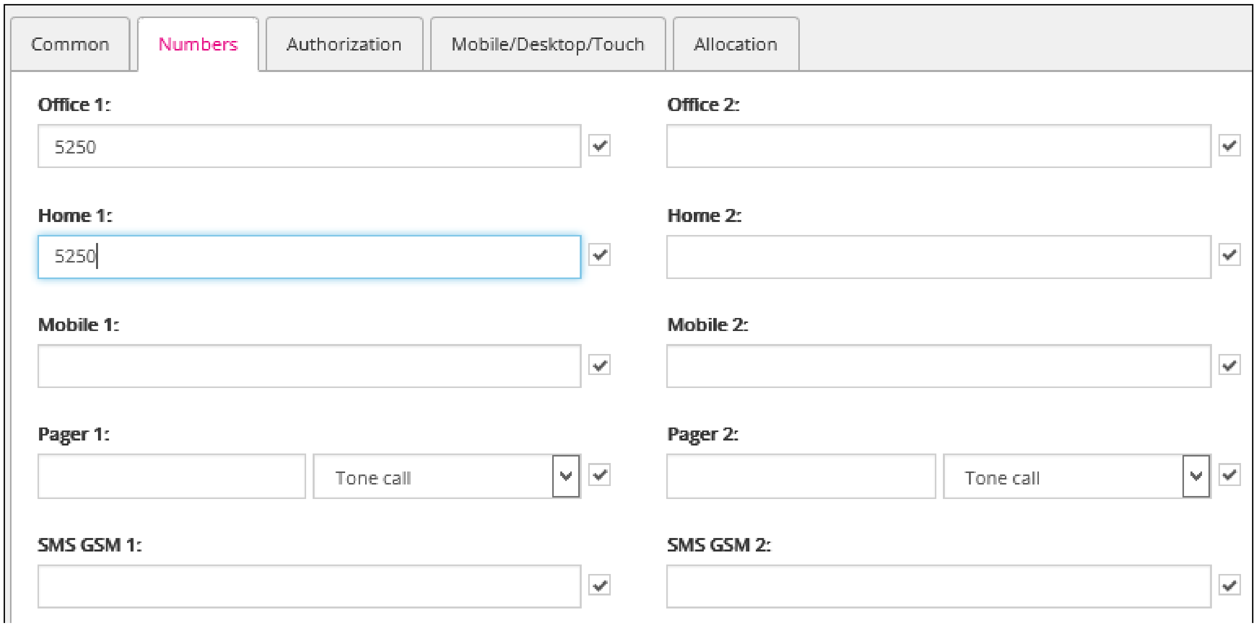
Inactive: □

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).



Office 1: 5250 ✓

Office 2: ✓

Home 1: 5250 ✓

Home 2: ✓

Mobile 1: ✓

Mobile 2: ✓

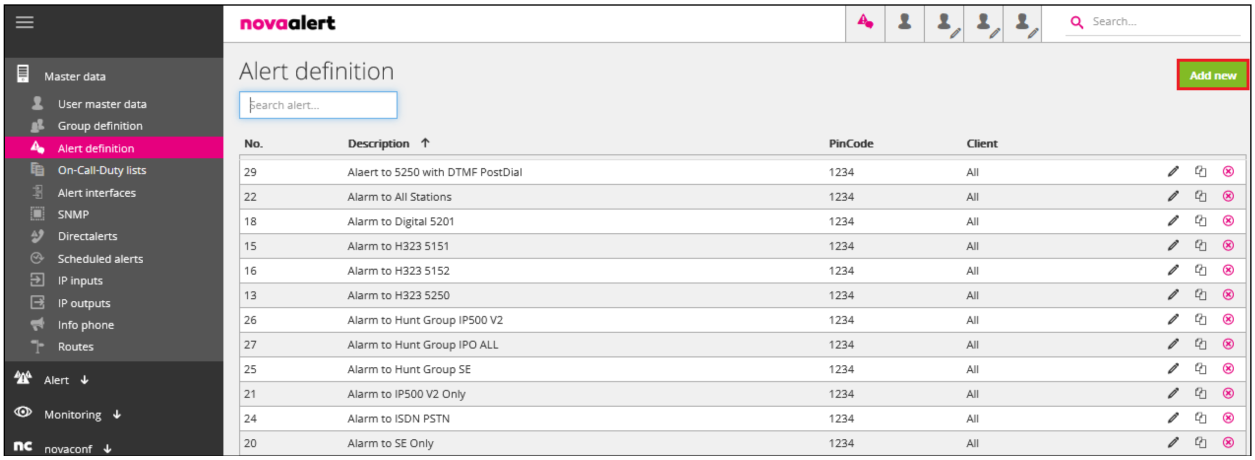
Pager 1: Tone call ✓

Pager 2: Tone call ✓

SMS GSM 1: ✓

SMS GSM 2: ✓

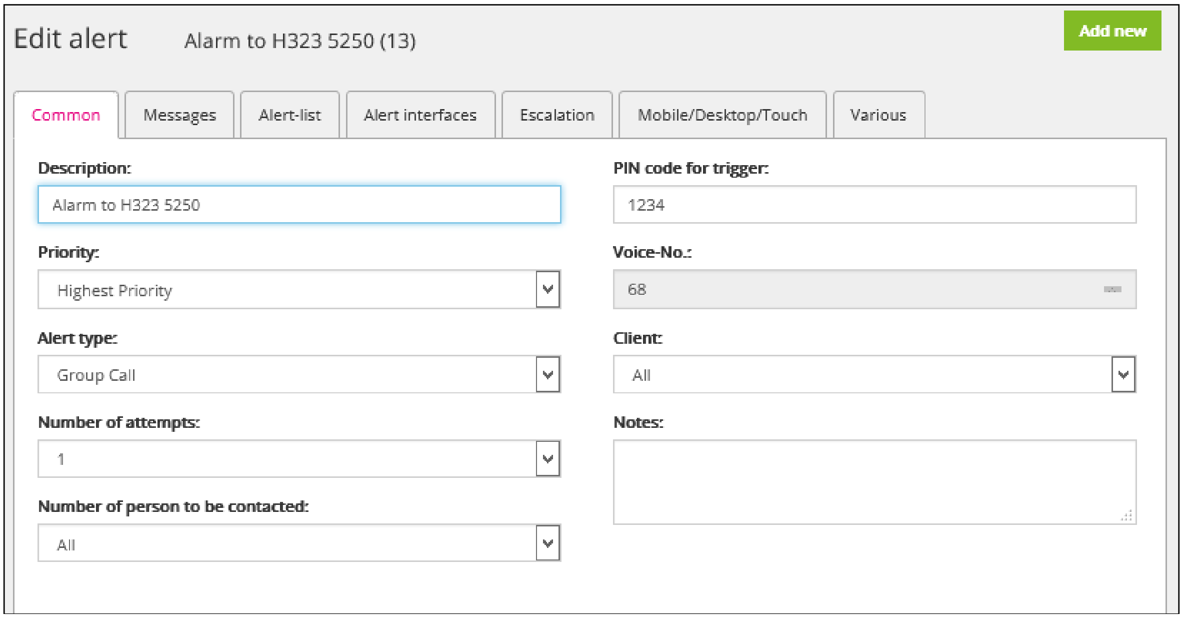
The next step is to create the Alert Definition, navigate to **Alert definition** in the left window and click on **Add new** in the main window.



Alert definition

No.	Description ↑	PinCode	Client
29	Alaert to 5250 with DTMF PostDial	1234	All
22	Alarm to All Stations	1234	All
18	Alarm to Digital 5201	1234	All
15	Alarm to H323 5151	1234	All
16	Alarm to H323 5152	1234	All
13	Alarm to H323 5250	1234	All
26	Alarm to Hunt Group IP500 V2	1234	All
27	Alarm to Hunt Group IPO ALL	1234	All
25	Alarm to Hunt Group SE	1234	All
21	Alarm to IP500 V2 Only	1234	All
24	Alarm to ISDN PSTN	1234	All
20	Alarm to SE Only	1234	All

Again, this example shows an existing Alert and 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)

Description: Alarm to H323 5250

PIN code for trigger: 1234

Priority: Highest Priority

Voice-No.: 68

Alert type: Group Call

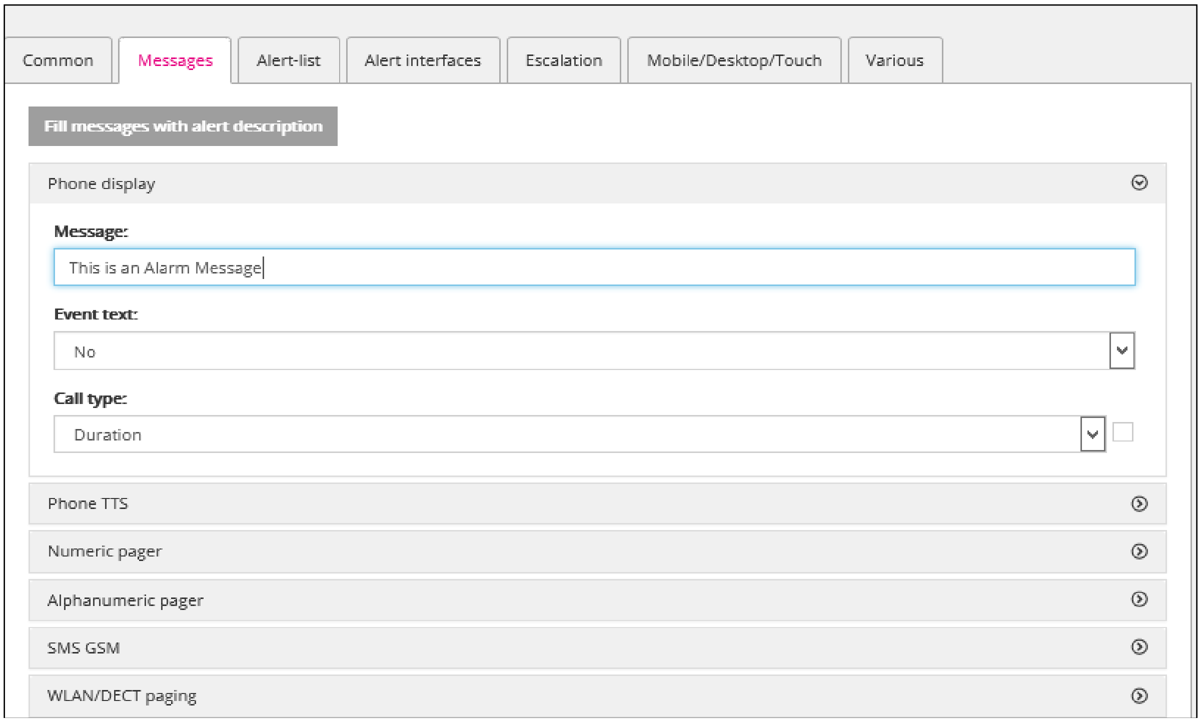
Client: All

Number of attempts: 1

Notes:

Number of person to be contacted: All

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.



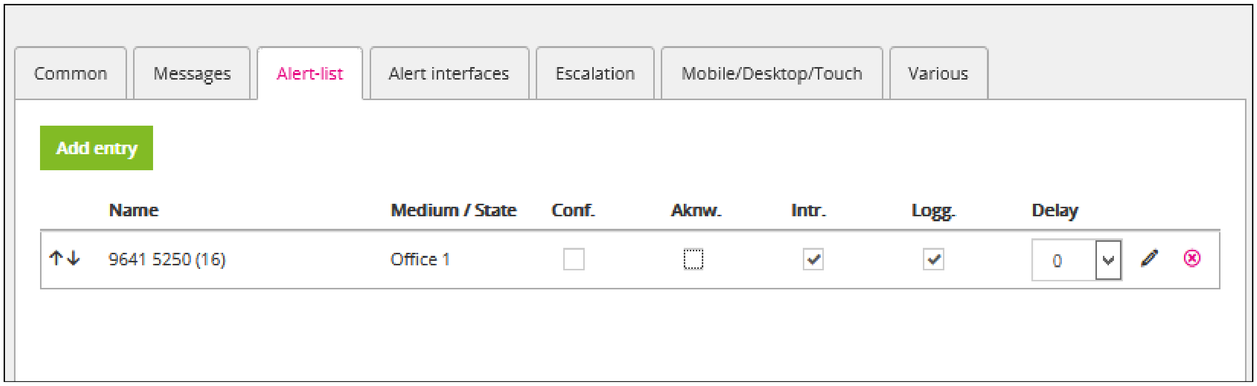
Phone display

Message: This is an Alarm Message

Event text: No

Call type: Duration

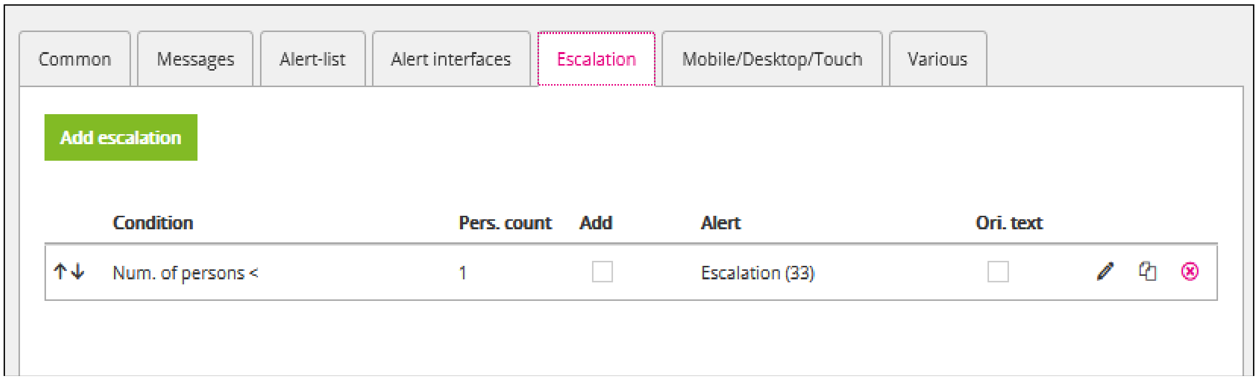
The list of users to be alerted by this alarm is entered under the **Alert-list** tab. In the example below one user **5250** (that created previously in this section) was added. However, a number of users can be added here depending on who should receive the alarm. The **Intr.** tick box was checked 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	☐	☐	☑	☑	0

Under the **Escalation** tab an Escalation can be added 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) 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	☐	Escalation (33)	☐

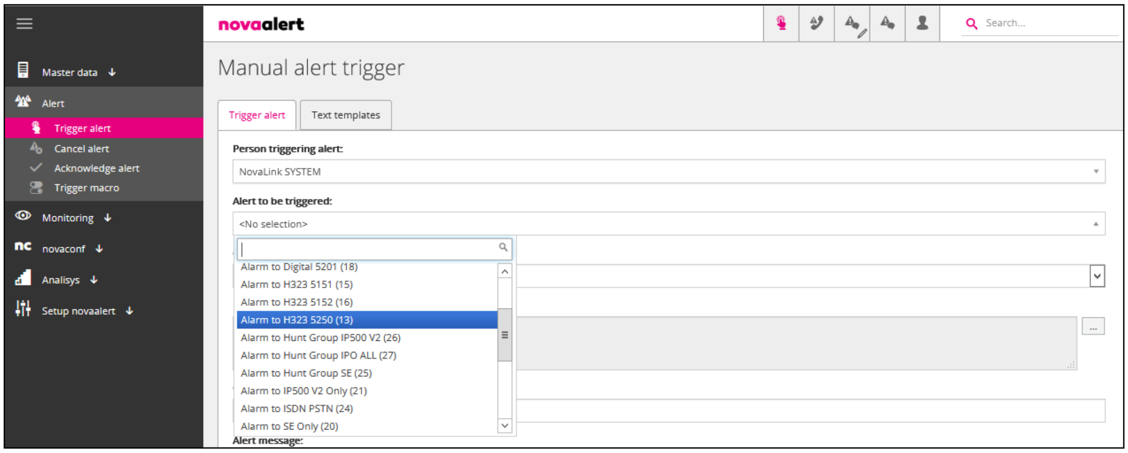
7. Verification Steps

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**.

Note: Typically, alarms are sent to multiple endpoints, but for simplicity of demonstrating this one endpoint was chosen.



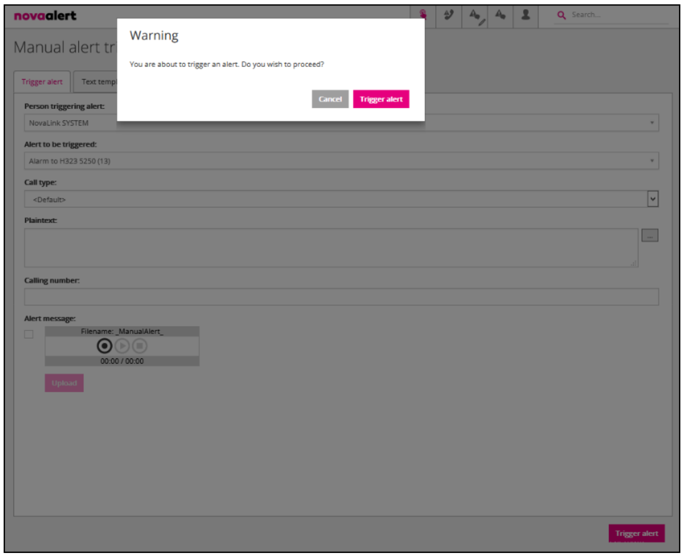
Person triggering alert: NovaLink SYSTEM

Alert to be triggered: <No selection>

Alarm to Digital 5201 (18)
Alarm to H323 5151 (15)
Alarm to H323 5152 (16)
Alarm to H323 5250 (13)
Alarm to Hunt Group IP500 V2 (26)
Alarm to Hunt Group IPO ALL (27)
Alarm to Hunt Group SE (25)
Alarm to IP500 V2 Only (21)
Alarm to ISDN PSTN (24)
Alarm to SE Only (20)

Alert message:

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.



Warning

You are about to trigger an alert. Do you wish to proceed?

Person triggering alert: NovaLink SYSTEM

Alert to be triggered: Alarm to H323 5250 (13)

Call type: <Default>

Plaintext:

Calling number:

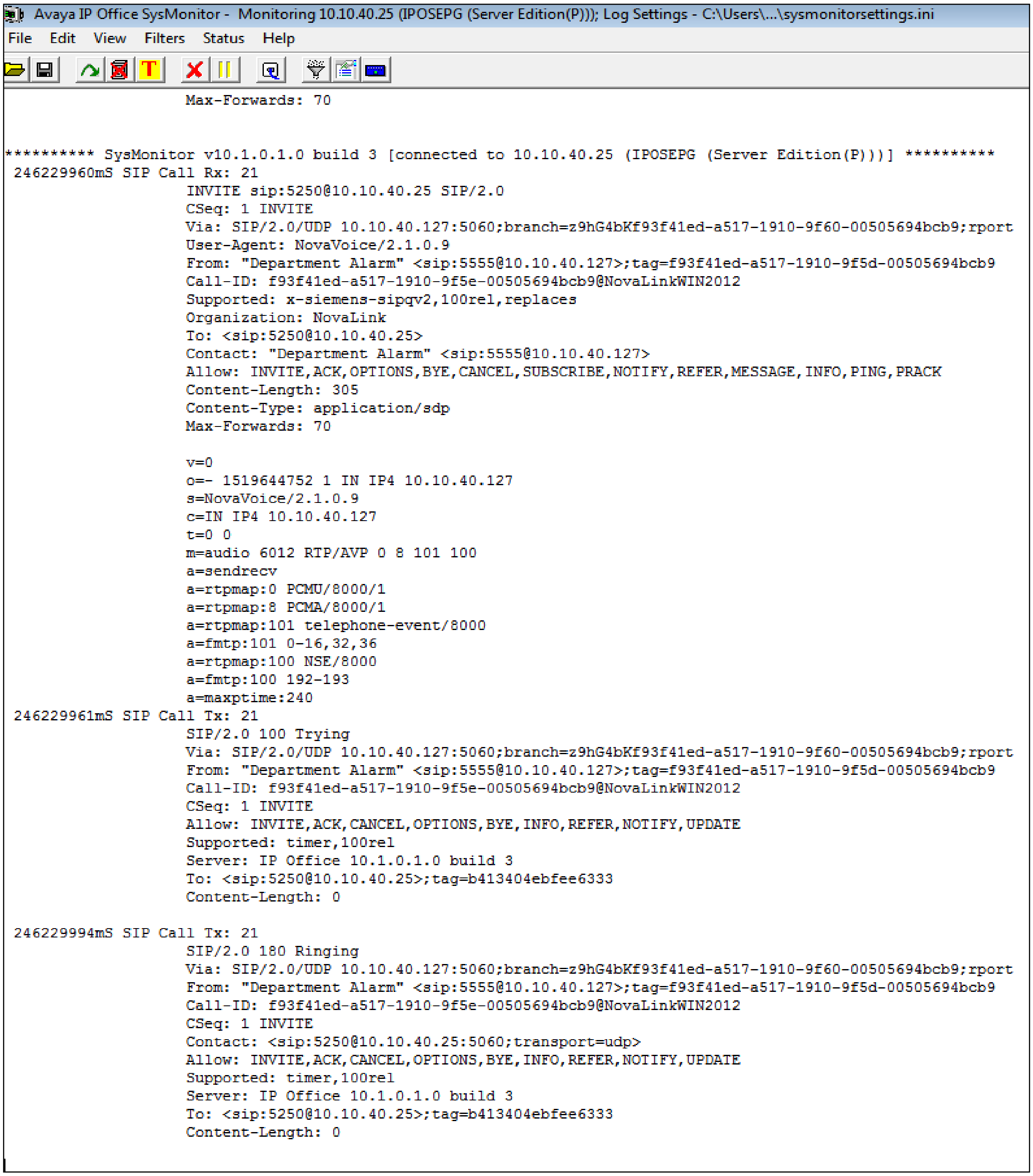
Alert message:

Filename: _ManualAlert_

00:00 / 00:00

7.2. Verify SIP Trunk Messages

SIP messages can be viewed by opening the IP Office **SysMonitor** as shown below. Click on **Filters** at the top of the screen and select the appropriate SIP messages that are to be viewed. This will then display all these filtered 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 troubleshoot what is happening.


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

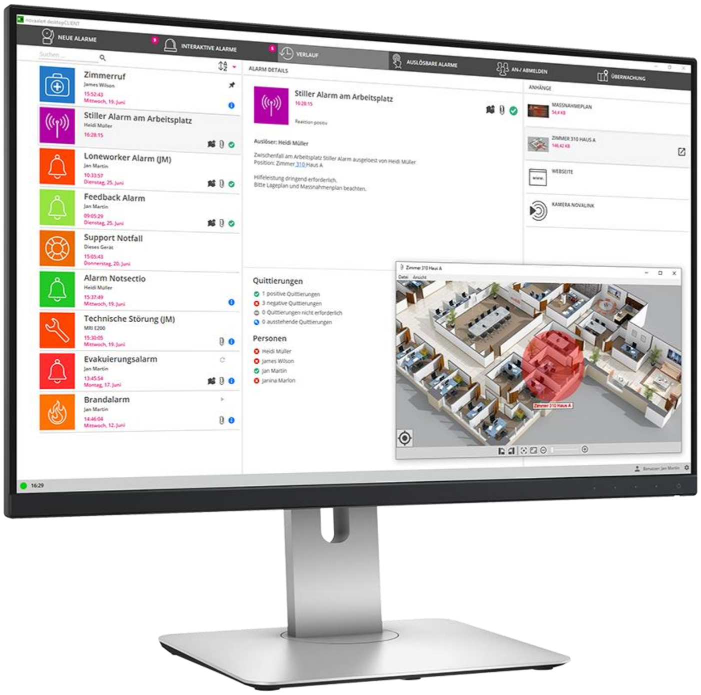
```
                    Max-Forwards: 70


********** 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
```

7.3. novaalert on different media

Below are screen shots which show novaalert in various other environments, for example a mobile phone with novaalert **mobileAPP**, showing an alert below.

Note: These were not taken as part of compliance testing but are here to demonstrate the use of novaalert on different media.

This example shows a Wallboard and **touchCLIENT**, to receive and trigger alerts.



Zimmerruf
James Wilson
15:52:43
Mittwoch, 19. Juni

Stiller Alarm am Arbeitsplatz
Heidi Müller
16:28:15

Loneworker Alarm (JM)
Jan Martin
10:33:57
Dienstag, 25. Juni

Feedback Alarm
Jan Martin
09:05:29
Dienstag, 25. Juni

Support Notfall
Dieses Gerät
15:05:43
Donnerstag, 20. Juni

Alarm Notsectio
Heidi Müller
15:37:49
Mittwoch, 19. Juni

Technische Störung (JM)
MRI E200
15:30:05
Mittwoch, 19. Juni

Evakuierungsalarm
Jan Martin
13:45:54
Montag, 17. Juni

Brandalarm
Jan Martin
14:46:04
Mittwoch, 12. Juni

Stiller Alarm am Arbeitsplatz
16:28:15
Reaktion positiv

Auslöser: Heidi Müller

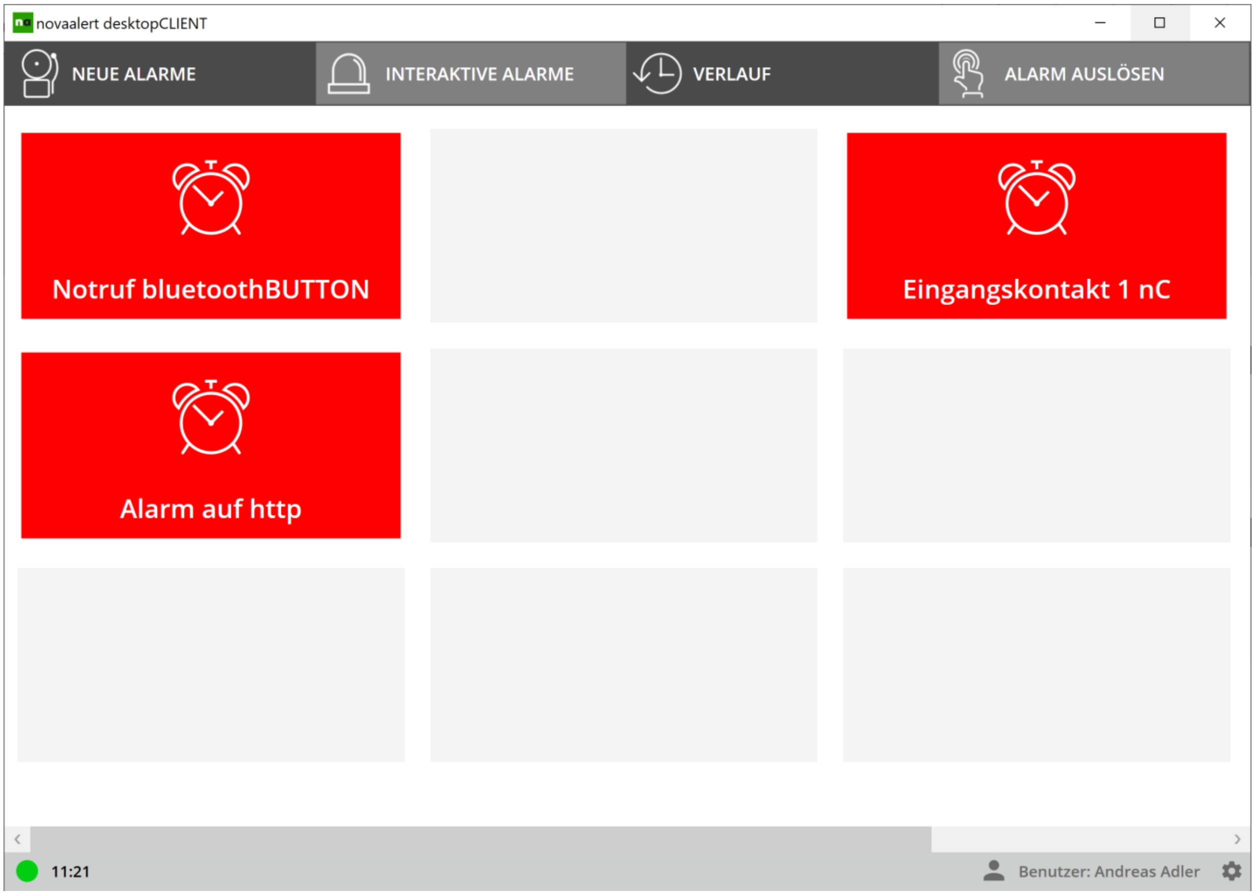
Zwischenfall am Arbeitsplatz Stiller Alarm ausgeloest von Heidi Müller
Position: Zimmer 310 Haus A

Hilfeleistung dringend erforderlich.
Bitte Lageplan und Massnahmenplan beachten.

Quittierungen
- 1 positive Quittierungen
- 3 negative Quittierungen
- 0 Quittierungen nicht erforderlich
- 0 ausstehende Quittierungen

Personen
- Heidi Müller
- James Wilson
- Jan Martin
- Janina Marlon

The example below shows the **desktopCLIENT**, to be used on Windows PCs., to receive and trigger alerts.



8. Conclusion

These Application Notes describe the configuration steps required for novaalert v10 from novalink to interoperate with Avaya IP Office R11.1. 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 R11.1 Manager 11.1*
[2] *Avaya IP Office R11.1 Doc library*

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

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

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.