Application Notes for configuring novaalert from novalink with Avaya Aura® Communication Manager R7.0 – Issue 1.0

Abstract

These Application Notes describe the configuration for connecting novalink novaalert via SIP Trunks to Avaya Aura® Communication Manager using Avaya Aura® Session Manager.

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

The purpose of this document is to describe the configuration for connecting novalink novaalert, via a SIP trunk interface, to Avaya Aura® Session Manager in order for novaalert to send voice calls to various endpoints on Avaya Aura® Communication Manager.

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 indicates 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's, 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 within test plan is restricted to those methods which involve interaction with Communication Manager.

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 Communication Manager.

Alarms which are triggered via Communication Manager 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 Communication Manager and covers the general test approach and the test results. Calls were made to novaalert over SIP trunks connecting Session Manager and novaalert. novaalert was configured as a SIP Entity on Session Manager allowing calls route between novaalert and Communication Manager via Session Manager.

novaalert was manually configured using the web interface to send alert messages to endpoints on Communication Manager.

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

2.1. Interoperability Compliance Testing

The interoperability compliance 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 and softphone endpoints.

- Delivery of voice recorded and TTS alarm to SIP/H.323/Digital endpoints
- Intrusion calls to deliver alarms
- Verification of Calling Party Name
- Over-ride forwarding to deliver alarms
- Following forwarding to deliver alarms
- Alarms delivered to Voicemail
- DTMF PIN Entry
- Serviceability testing consisted of verifying the ability of novaalert to recover from power or network interruption to both Communication Manager and novaalert.

2.2. Test Results

All test cases were executed successfully.

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 novaalert with Communication Manager registering with Session Manager as a third party SIP entity. Alarms/Alerts are received from novaalert using SIP trunks.

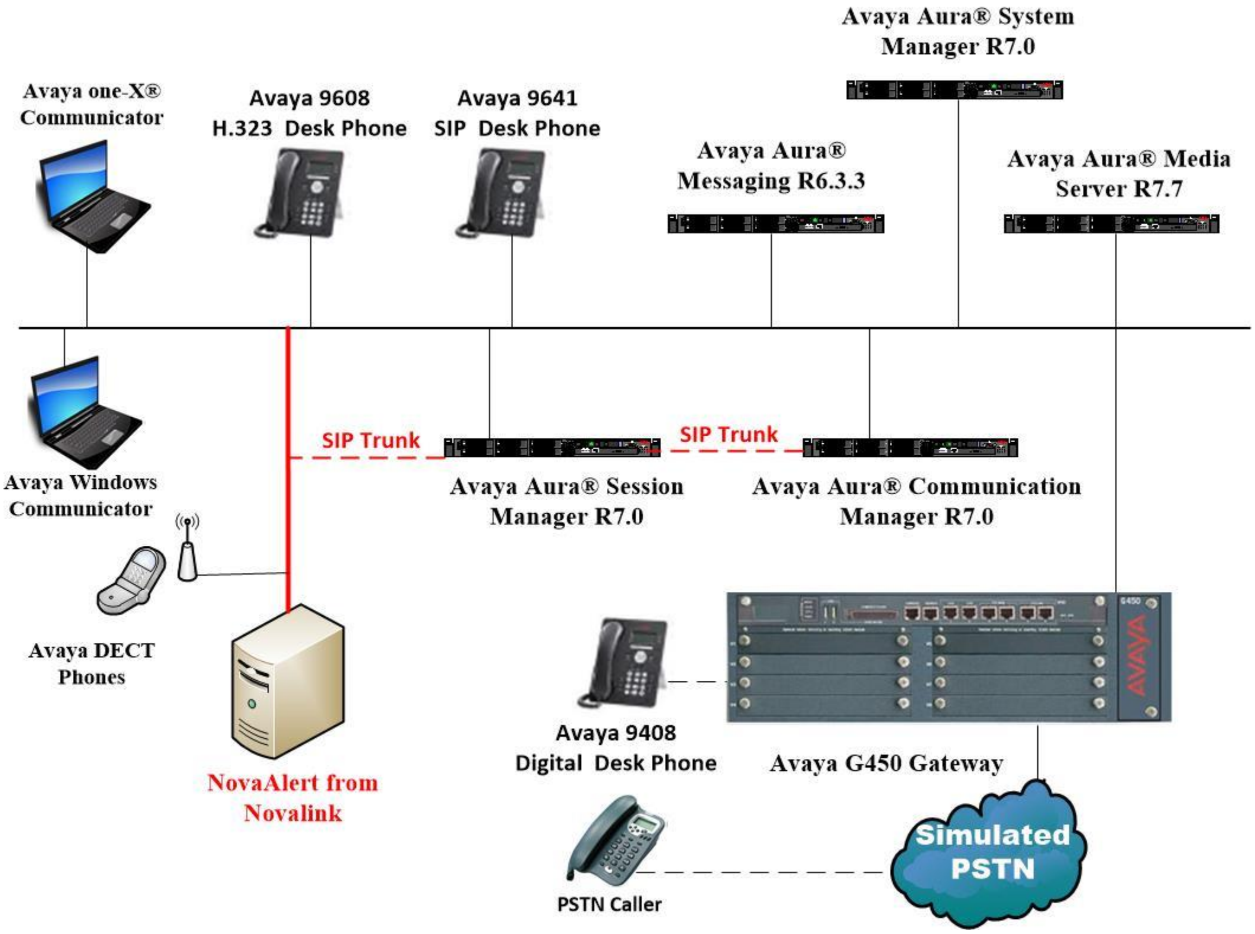

Avaya Aura® System Manager R7.0
Avaya one-X® Communicator
Avaya 9608 H.323 Desk Phone
Avaya 9641 SIP Desk Phone
Avaya Aura® Messaging R6.3.3
Avaya Aura® Media Server R7.7
Avaya Windows Communicator
SIP Trunk
SIP Trunk
Avaya Aura® Session Manager R7.0
Avaya Aura® Communication Manager R7.0
Avaya DECT Phones
NovaAlert from Novalink
Avaya 9408 Digital Desk Phone
Avaya G450 Gateway
Simulated PSTN
PSTN Caller

Figure 1: Connection of novaalert from novalink with Avaya Aura® Communication Manager and Avaya Aura® Session Manager

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager running on a virtual server	System Manager 7.0.1.1 Build No. - 7.0.0.0.16266 Software Update Revision No: 7.0.1.1.065378 Service Pack 1
Avaya Aura® Session Manager running on a virtual server	Session Manager R7.0 SP1 Build No. – 7.0.1.1.701114
Avaya Aura® Communication Manager running on a virtual server	R7.0 R017x.00.0.441.0 00.0.441.0-23169
Avaya Media Server running on a virtual server	Media Server SYSTEM R7.7.0.8 Media Server R7.7.0.200
Avaya G450 Gateway	37.19.0 /1
Avaya Aura® Messaging	R6.3.3
Avaya 9608 H323 Deskphone	96x1 H323 Release 6.6.028
Avaya 9641 SIP Deskphone	96x1 SIP Release 7.0.0.39
Avaya 9408 Digital Deskphone	V2.0
Avaya DECT Handsets	3725 DH4 (R3.3.11) 3720 DH3 (R3.3.11)
Avaya one-X® Communicator H.323	R6.2.4.07-FP4
Avaya Communicator for Windows	R2.1.3.80
novalink novaalert running on a Windows 2012 virtual server	9.8

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

The configuration operations described in this section can be summarized as follows:

- Verify System Parameters Customer Options.
- System Features and Access Codes.
- Administer Dial Plan.
- Administer Route Selection for calls to novaalert.
- Configure Network Region and IP Codec.

Note: The configuration of PSTN trunks and routes are outside the scope of these Application Notes.

5.1. Verify System Parameters Customer Options

The license file installed on the system controls these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative. Use the **display system-parameters customer-options** command to determine these values. On **Page 2**, verify that **Maximum Administered SIP Trunks** has sufficient capacity.

```
display system-parameters customer-options                     Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 12000 250
           Maximum Concurrently Registered IP Stations: 18000 2
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 0
                   Maximum Video Capable IP Softphones: 18000 0
                       Maximum Administered SIP Trunks: 24000 319
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
```

On **Page 3**, ensure that both **ARS** and **ARS/AAR Partitioning** are set to **y**.

```
display system-parameters customer-options                    Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                       CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                         CAS Main? n
Answer Supervision by Call Classifier? y                Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                      DCS (Basic)? y
```

On **Page 5**, ensure that **Uniform Dialing Plan** is set to **y**.

```
display system-parameters customer-options                    Page   5 of  11
                                OPTIONAL FEATURES

                Multinational Locations? n            Station and Trunk MSP? y
 Multiple Level Precedence & Preemption? n     Station as Virtual Extension? y
                     Multiple Locations? n
                                             System Management Data Transfer? n
             Personal Station Access (PSA)? y           Tenant Partitioning? y
                        PNC Duplication? n       Terminal Trans. Init. (TTI)? y
                   Port Network Support? y              Time of Day Routing? y
                        Posted Messages? y       TN2501 VAL Maximum Capacity? y
                                                        Uniform Dialing Plan? y
                     Private Networking? y     Usage Allocation Enhancements? y
```

5.2. System Features and Access Codes

For the testing, **Trunk-to Trunk Transfer** was set to **all** on **page 1** of the **system-parameters features** page. This is a system wide setting that allows calls to be routed from one trunk to another and is usually turned off to help prevent toll fraud. An alternative to enabling this feature on a system wide basis is to control it using COR (Class of Restriction). See **Section 10** for supporting documentation.

```
display system-parameters features                            Page   1 of  19
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? n
                                    Trunk-to-Trunk Transfer: all
              Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                      Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                  AAR/ARS Dial Tone Required? y

             Music (or Silence) on Transferred Trunk Calls? no
                      DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n

            Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                     Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

Use the **display feature-access-codes** command to verify that a FAC (feature access code) has been defined for both AAR and ARS. Note that **8** is used for AAR and **9** for ARS routing.

```
display feature-access-codes                                    Page   1 of  10
                              FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *25    Deactivation: #25
```

5.3. Administer Dial Plan

It was decided for compliance testing that all calls beginning with 49 with a total length of 4 digits were to be sent across the SIP trunk to Session Manager and therefore to novaalert. In order to achieve this, automatic alternate routing (aar) would be used to route the calls. The dial plan and aar routing analysis need to be changed to allow this.

Type **change dialplan analysis** in order to make changes to the dial plan. Ensure that **4** is added with a **Total Length** of **4** and a **Call Type** of **udp**.

```
change dialplan analysis                                     Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all          Percent Full: 2

    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type
   2           4   ext
   3           4   ext
   4           4   udp
   5           4   ext
   6           4   udp
   7           3   dac
   8           1   fac
   9           1   fac
   *           3   fac
   #           3   fac
```

5.4. Administer Route Selection for novaalert Calls

As digits**49xx** were defined in the dial plan as udp (**Section 5.3**) use the **change uniform-dialplan** command to configure the routing of the dialed digits. In the example below calls to numbers beginning with **49** that are **4** digits in length will be matched. No further digits are deleted or inserted. Calls are sent to **aar** for further processing.

```
change uniform-dialplan 4                                      Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                             Percent Full: 0

  Matching                   Insert              Node
  Pattern        Len Del     Digits      Net Conv Num
  49              4   0                  aar  n
                                              n
```

Use the **change aar analysis** x command to further configure the routing of the dialed digits. Calls to novaalert begin with **49** and are matched with the AAR entry shown below. Calls are sent to **Route Pattern 1**, which contains the outbound SIP Trunk Group.

```
change aar analysis 49                                        Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 1

    Dialed                  Total      Route    Call   Node  ANI
    String                 Min  Max   Pattern   Type   Num   Reqd
    49                     4    4      1        unku         n
```

Use the **change route-pattern *n*** command to add the SIP trunk group to the route pattern that AAR selects. In this configuration, **Route Pattern Number 1** is used to route calls to trunk group **(Grp No) 1**, this is the SIP Trunk configured in **Appendix**.

```
change route-pattern 1                                         Page   1 of   3
                    Pattern Number: 1   Pattern Name: SIPTRK
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                            DCS/ IXC
    No          Mrk Lmt List Del  Digits                              QSIG
                             Dgts                                     Intw
 1: 1    0                                                             n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            unre                                          none
 2: y y y y y n  n            rest                                          none
 3: y y y y y n  n            rest                                          none
 4: y y y y y n  n            rest                                          none
 5: y y y y y n  n            rest                                          none
 6: y y y y y n  n            rest                                          none
 6: y y y y y n  n            rest                                          none
```

5.5. Configure Network Region and IP Codec

In the Node Names IP form, note the IP Address of the **procr** and the Session Manager (**sm70vmpg**). The host names will be used throughout the other configuration screens of Communication Manager and Session Manager. Type **display node-names ip** to show all the necessary node names.

```
display node-names ip                                           Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
AMS77vmpg           10.10.40.17
CMS18vmpg           10.10.40.36
IPO500V2            10.10.40.20
IPOSE               10.10.40.25
PGDECT              10.10.40.50
aes70vmpg           10.10.40.26
default             0.0.0.0
procr               10.10.40.13
procr6              ::
sm70vmpg            10.10.40.12
```

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager in **Section 6.2**. In this configuration, the domain name is **devconnect.local**. The **IP Network Region** form also specifies the **IP Codec Set** to be used. This codec set will be used for calls routed over the SIP trunk to Session manager as **ip-network region 1** is specified in the SIP signaling group.

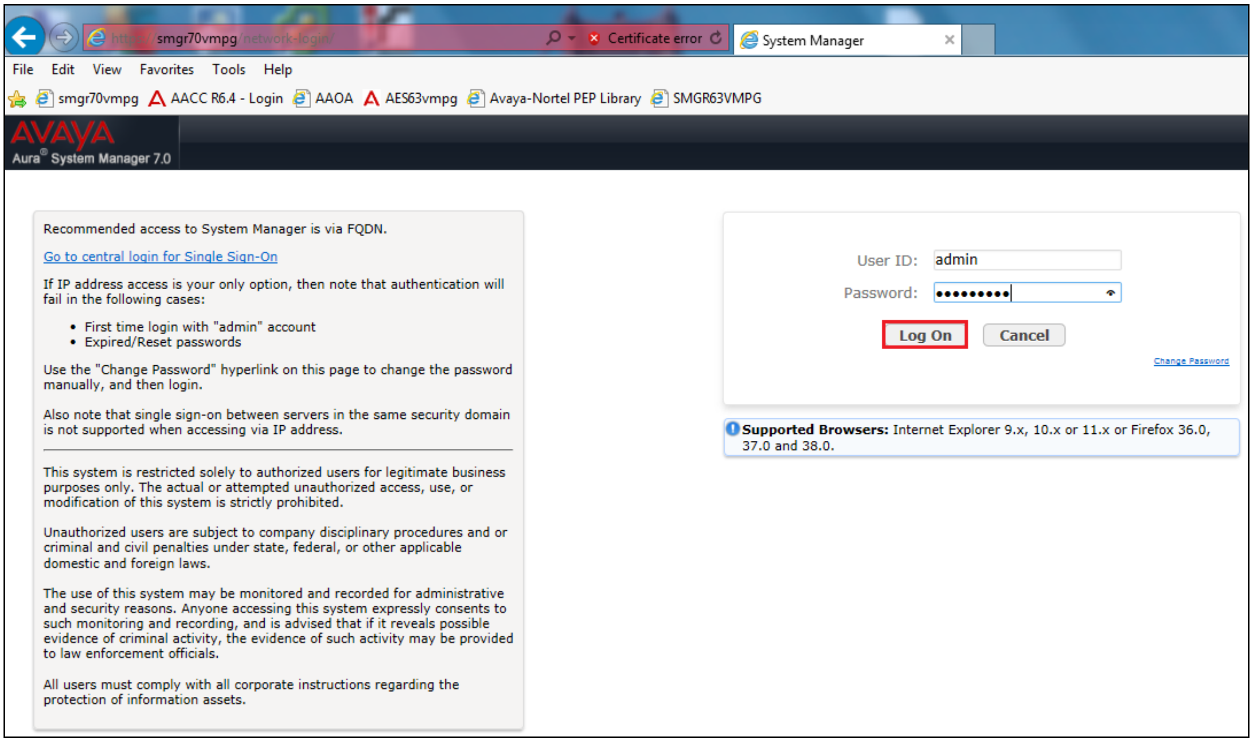
```
display ip-network-region 1                                    Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: devconnect.local
    Name: Default region
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                  RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

In the **IP Codec Set** form, select the audio codec's supported for calls routed over the SIP trunk to and from novaalert. The form is accessed via the **change ip-codec-set n** command. Note that IP codec set 1 was specified in IP Network Region 1 shown above. Multiple codecs may be specified in the **IP Codec Set** form in order of preference; the example below includes **G.711A** (a-law), which is supported by novaalert. Note the **Media Encryption** has been set to **none**. This ensures that no media is encrypted.

```
change ip-codec-set 1                                             Page   1 of   2

                          IP CODEC SET
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711A           n          2        20
 2:
 3:
 4:
 5:
 6:
 7:

     Media Encryption                   Encrypted SRTCP:
 1: none
 2:
 3:
 4:
 5:
```

6. Configure Avaya Aura® Session Manager

In order to make changes in Session Manager, a web session to System Manager is opened. Navigate to http://<System Manager IP Address>/SMGR, enter the appropriate credentials and click on **Log On** as shown below.



Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

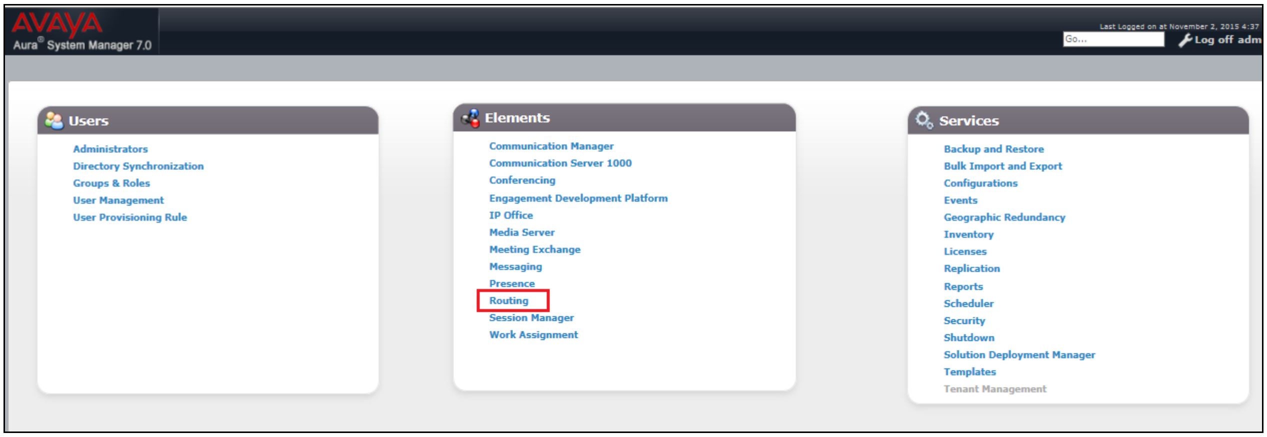
User ID: admin

Password: •••••••••

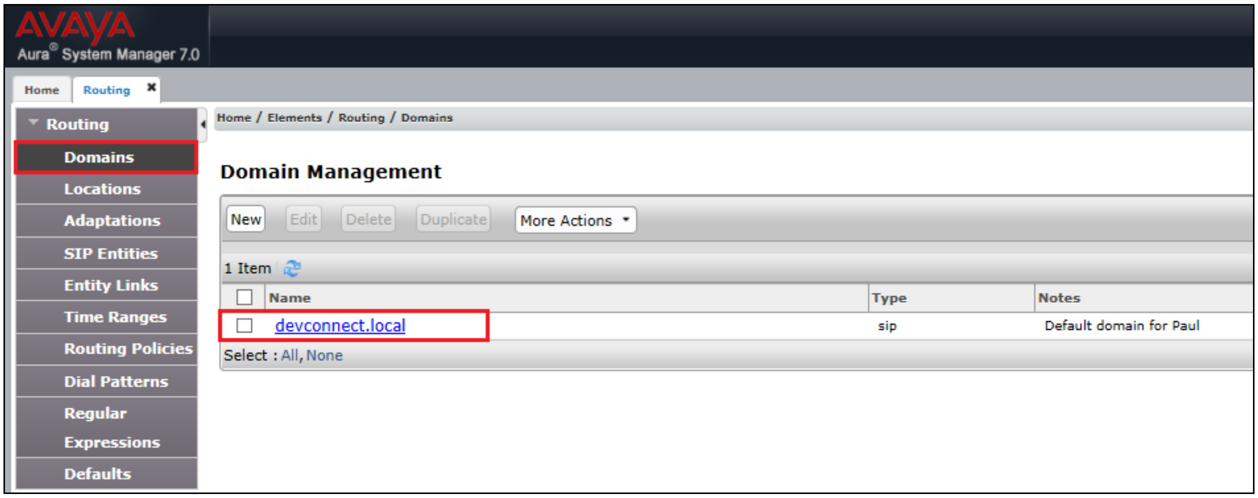
Supported Browsers: Internet Explorer 9.x, 10.x or 11.x or Firefox 36.0, 37.0 and 38.0.

6.1. Configuration of a Domain

Click on **Routing** highlighted below.



Click on **Domains** in the left window. If there is not a domain already configured click on **New**. In the example below there exists a domain called devconnect.local which has been already configured.



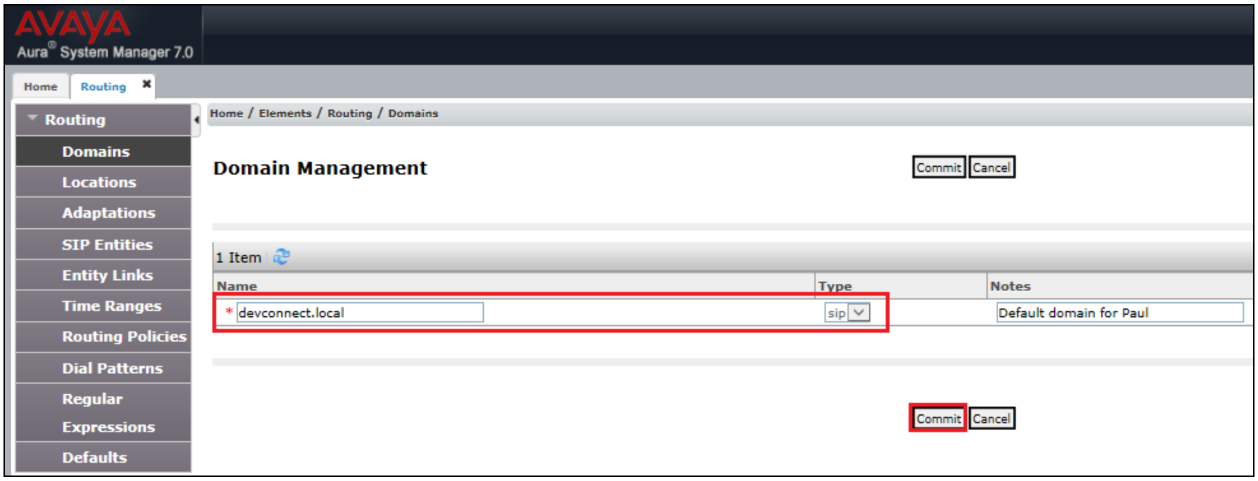
Home / Elements / Routing / Domains

Domain Management

1 Item

□	Name	Type	Notes
□	devconnect.local	sip	Default domain for Paul

Clicking on the domain name above will open the following window; this is simply to show an example of such a domain. When entering a new domain the following should be entered, once the domain name is entered click on **Commit** to save this.



Home / Elements / Routing / Domains

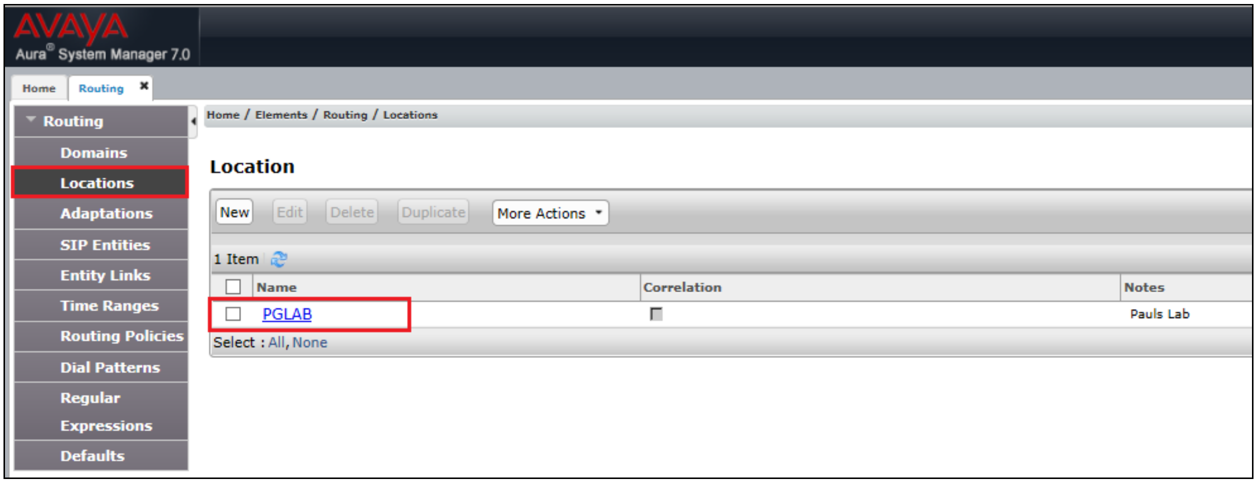
Domain Management

1 Item

Name	Type	Notes
* devconnect.local	sip	Default domain for Paul

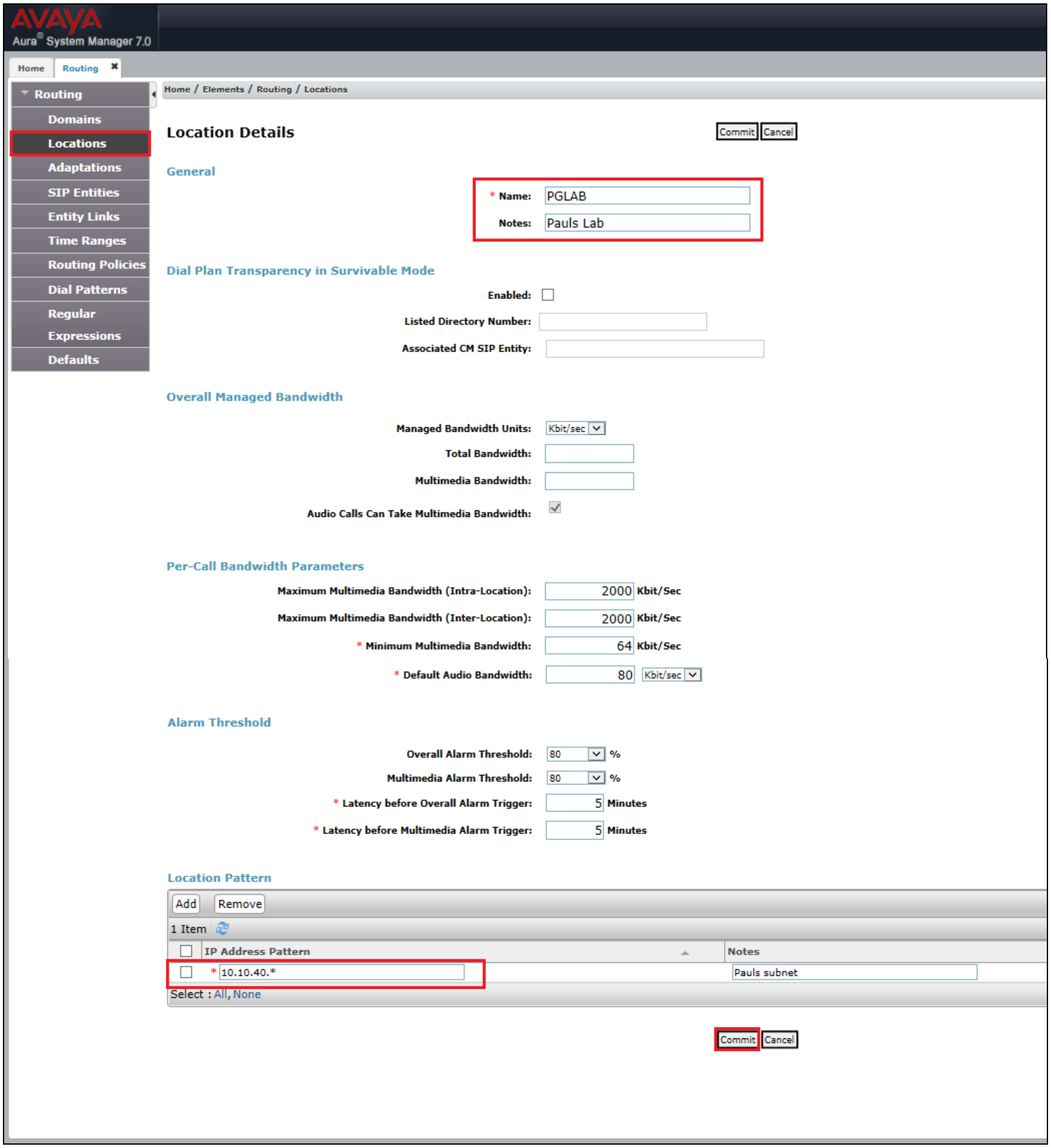
6.2. Configuration of a Location

Click on **Locations** in the left window and if there is no Location already configured then click on **New**, however in the screen below a location called **PGLAB** is already setup and configured and clicking into this will show its contents.



□	Name	Correlation	Notes
□	PGLAB	□	Pauls Lab

The Location below shows a suitable **Name** with a **Location Pattern** of **10.10.40.***. Once this is configured, click on **Commit**.



Location Details

General

* Name: PGLAB

Notes: Pauls Lab

Dial Plan Transparency in Survivable Mode

Enabled: □

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☑

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 2000 Kbit/Sec

* Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

* Latency before Overall Alarm Trigger: 5 Minutes

* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

1 Item

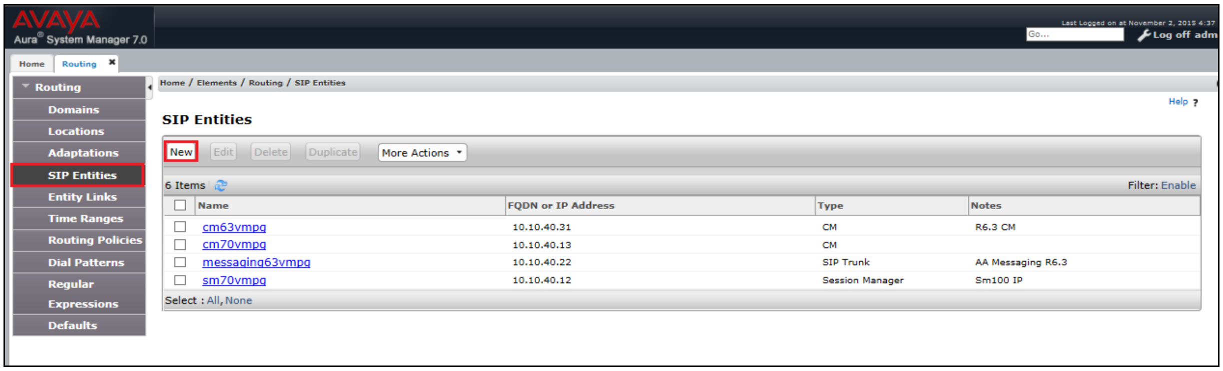
□	IP Address Pattern	Notes
□	* 10.10.40.*	Pauls subnet

6.3. Configuration of SIP Entities

Clicking on **SIP Entities** in the left window shows what SIP Entities have been added to the system and allows the addition of any new SIP Entity that may be required. Please note the SIP Entities already present for the compliance testing of novaalert.

- Communication Manager SIP Entity (cm70vmpg)
- Session Manager SIP Entity (sm70vmpg)

To add a SIP entity, click on **New**.



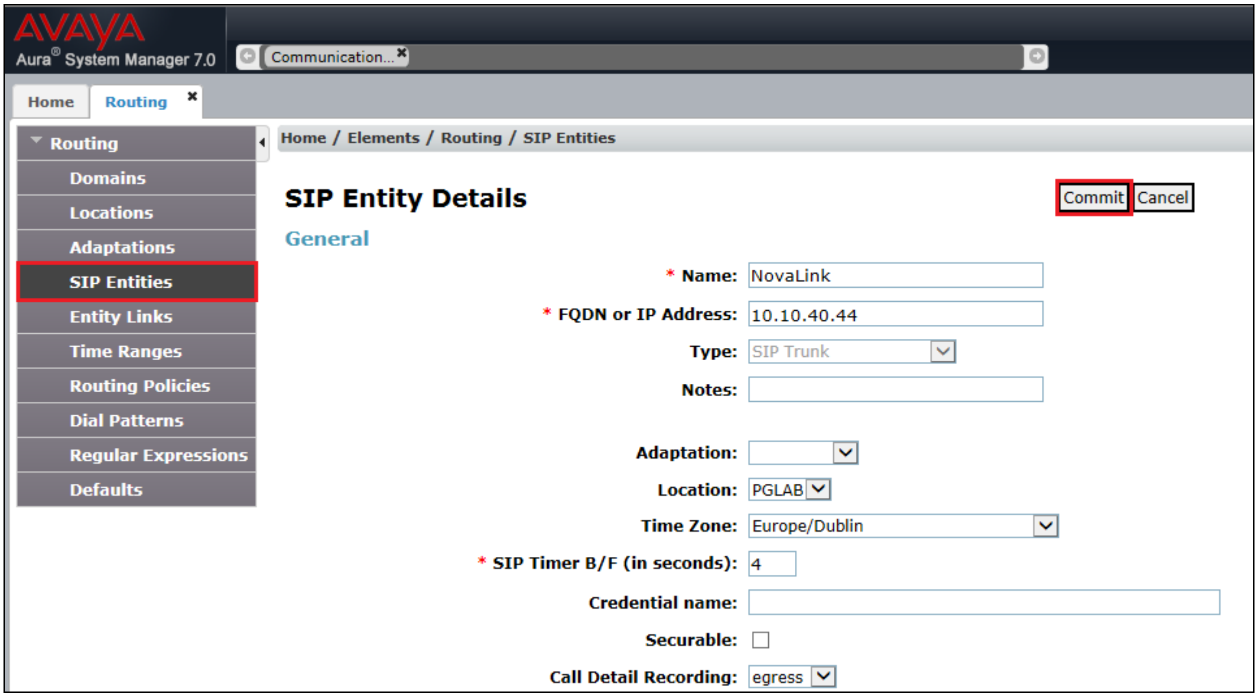
SIP Entities

6 Items

	Name	FQDN or IP Address	Type	Notes
□	cm63vmpg	10.10.40.31	CM	R6.3 CM
□	cm70vmpg	10.10.40.13	CM	
□	messaging63vmpg	10.10.40.22	SIP Trunk	AA Messaging R6.3
□	sm70vmpg	10.10.40.12	Session Manager	Sm100 IP

Enter a suitable **Name** as well as the **IP Address** of novaalert. Select **SIP Trunk** as the **Type**. Click on **Commit** once completed.

Note: In the remainder of this section including the screen shots below novaalert may also be referred to as novalink.

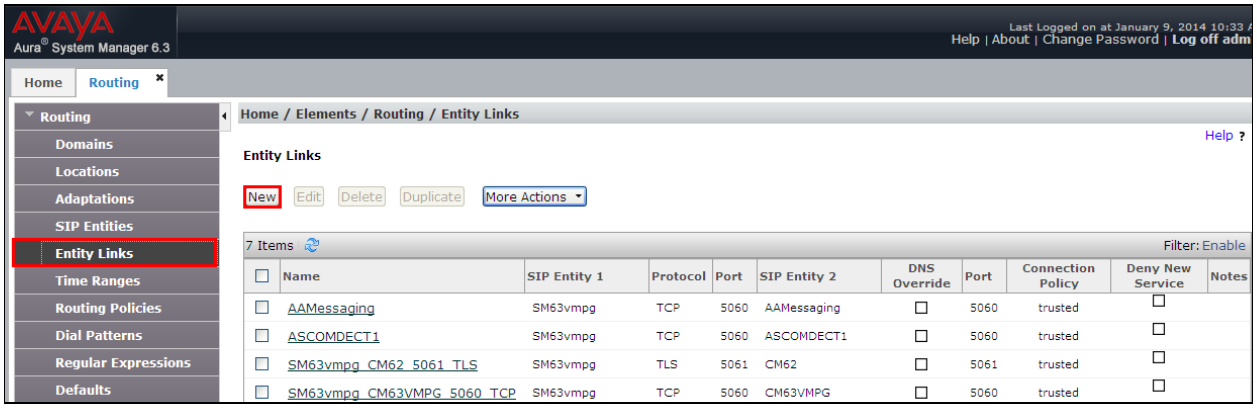


SIP Entity Details

General

* Name:	NovaLink
* FQDN or IP Address:	10.10.40.44
Type:	SIP Trunk
Notes:	
Adaptation:	
Location:	PGLAB
Time Zone:	Europe/Dublin
* SIP Timer B/F (in seconds):	4
Credential name:	
Securable:	□
Call Detail Recording:	egress

An Entity Link between novaalert and Session Manager is required, click on Entity Links in the left column and then on **New**.



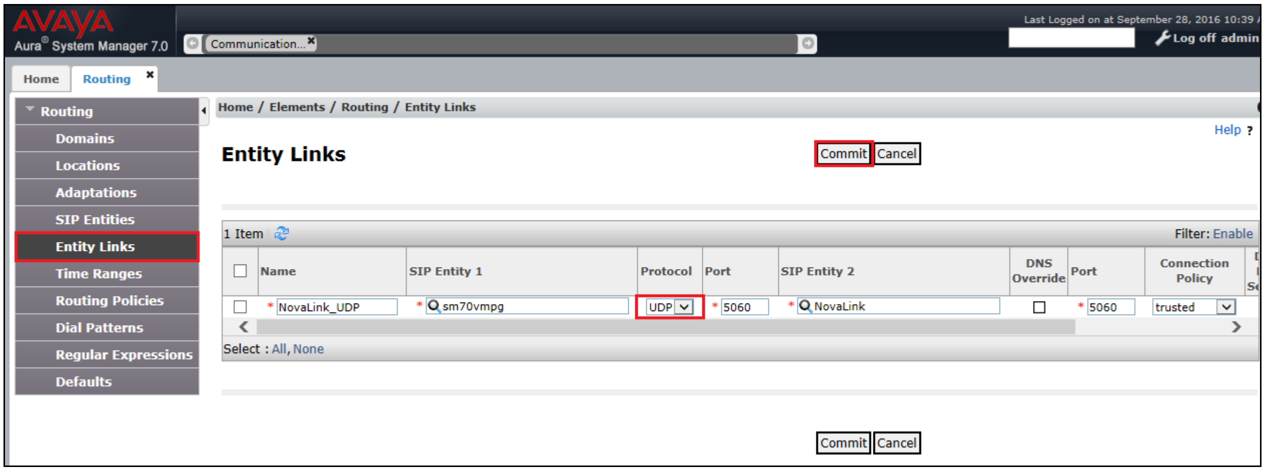
Home / Elements / Routing / Entity Links

Entity Links

7 Items

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
□	AAMessaging	SM63vmpg	TCP	5060	AAMessaging	□	5060	trusted	□	
□	ASCOMDECT1	SM63vmpg	TCP	5060	ASCOMDECT1	□	5060	trusted	□	
□	SM63vmpg_CM62_5061_TLS	SM63vmpg	TLS	5061	CM62	□	5061	trusted	□	
□	SM63vmpg_CM63VMPG_5060_TCP	SM63vmpg	TCP	5060	CM63VMPG	□	5060	trusted	□	

Enter a suitable **Name** and ensure that **UDP** is selected for the **Protocol** and **5060** for the **Port**. The **Connection Policy** must be setup as **trusted** as shown below. Click on **Commit** once completed.



Home / Elements / Routing / Entity Links

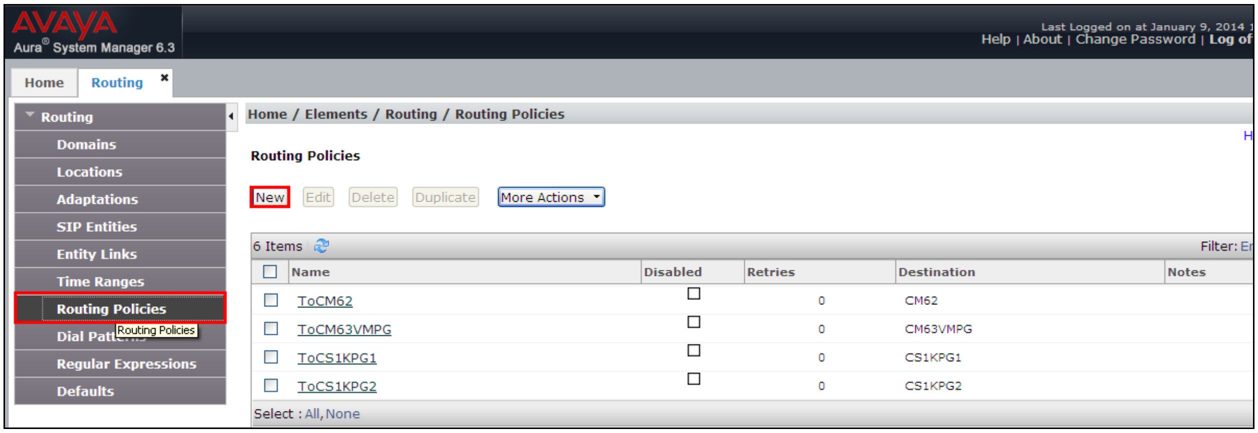
Entity Links

1 Item

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
□	* NovaLink_UDP	* sm70vmpg	UDP	* 5060	* NovaLink	□	* 5060	trusted

6.4. Configure Routing Policy for novalink

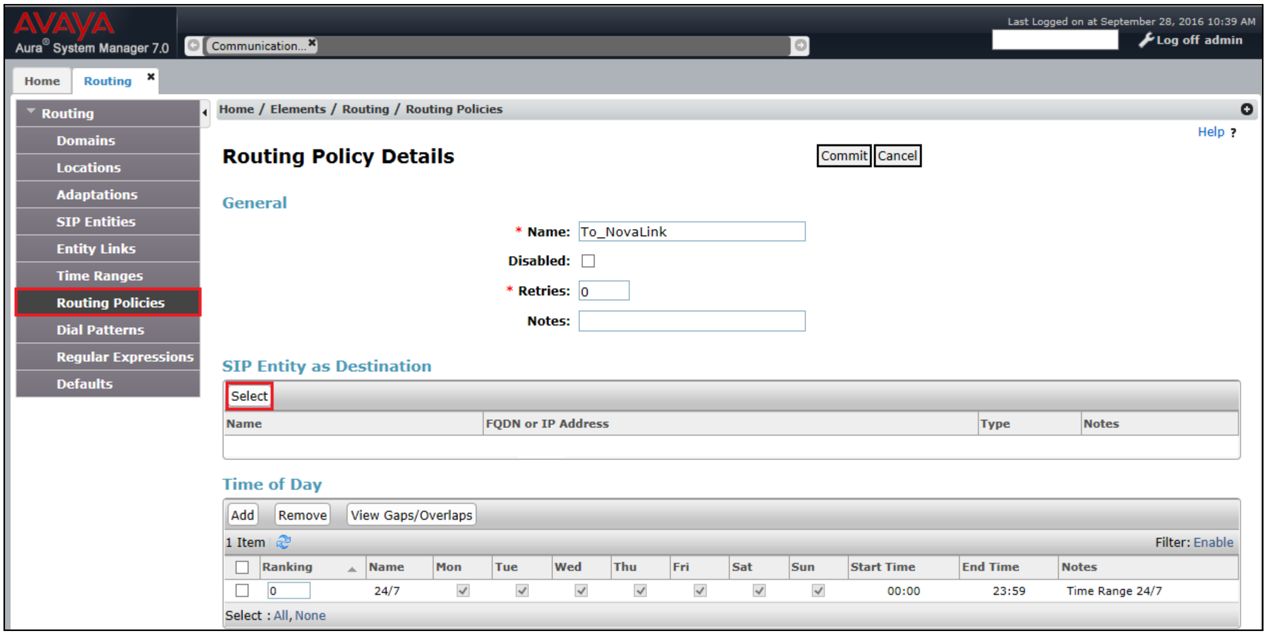
Select **Routing Policies** from the left window and click on **New** in the main window.



Routing Policies

□	Name	Disabled	Retries	Destination	Notes
□	ToCM62	□	0	CM62	
□	ToCM63VMPG	□	0	CM63VMPG	
□	ToCS1KPG1	□	0	CS1KPG1	
□	ToCS1KPG2	□	0	CS1KPG2	

Enter a suitable **Name** and click on **Select** highlighted in order to associate this routing policy with a SIP Entity.



Routing Policy Details

General

* Name: To_NovaLink

Disabled: □

* Retries: 0

Notes:

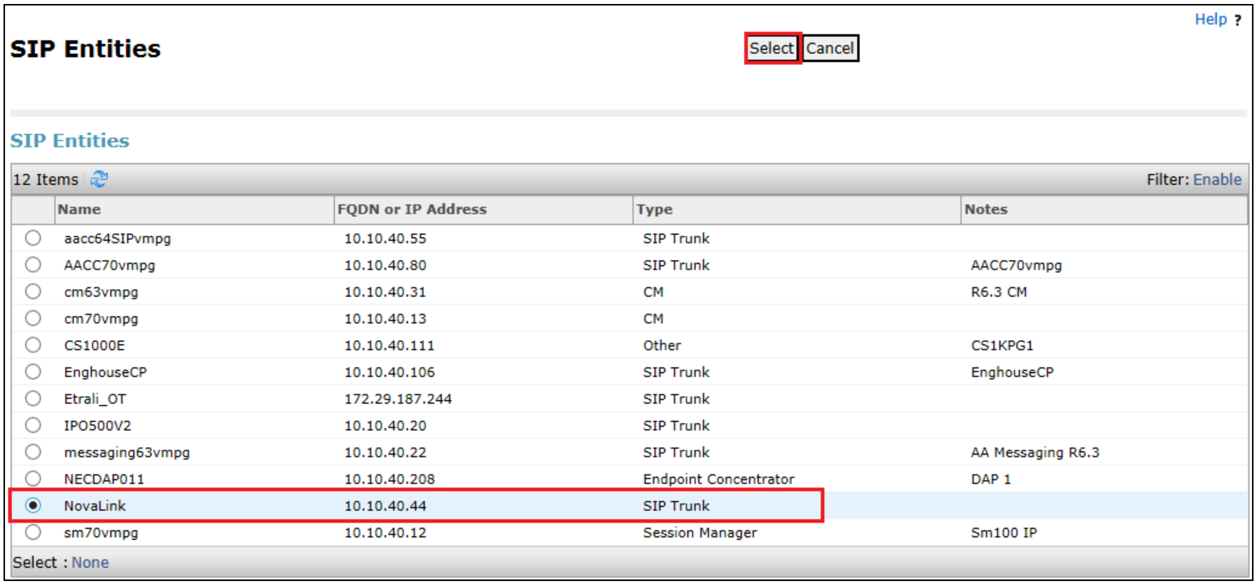
SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes

Time of Day

□	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select the **novalink** SIP Entity created in **Section 6.3** and click on **Commit** when done (not shown).



SIP Entities

Select Cancel

Help ?

SIP Entities

12 Items

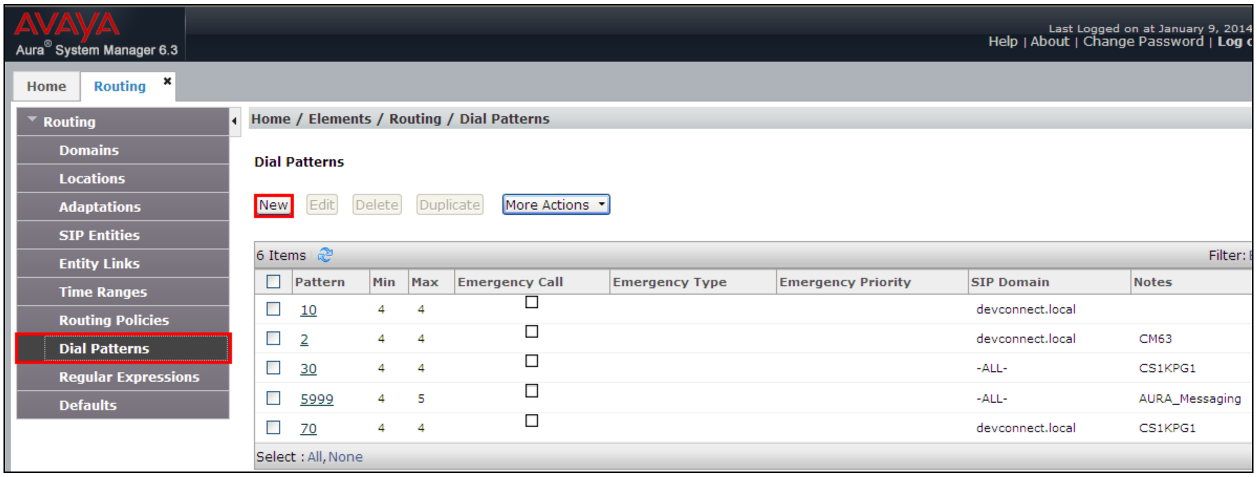
Filter: Enable

	Name	FQDN or IP Address	Type	Notes
○	aacc64SIPvmpg	10.10.40.55	SIP Trunk	
○	AACC70vmpg	10.10.40.80	SIP Trunk	AACC70vmpg
○	cm63vmpg	10.10.40.31	CM	R6.3 CM
○	cm70vmpg	10.10.40.13	CM	
○	CS1000E	10.10.40.111	Other	CS1KPG1
○	EnghouseCP	10.10.40.106	SIP Trunk	EnghouseCP
○	Etrali_OT	172.29.187.244	SIP Trunk	
○	IPO500V2	10.10.40.20	SIP Trunk	
○	messaging63vmpg	10.10.40.22	SIP Trunk	AA Messaging R6.3
○	NECDAP011	10.10.40.208	Endpoint Concentrator	DAP 1
●	NovaLink	10.10.40.44	SIP Trunk	
○	sm70vmpg	10.10.40.12	Session Manager	Sm100 IP

Select : None

6.5. Configure Dial Pattern for novalink

In order to route calls to the novaalert a dial pattern is created pointing to the SIP Entity. Select **Dial Patterns** from the left window and click on **New** in the main window.



Home / Elements / Routing / Dial Patterns

Dial Patterns

New Edit Delete Duplicate More Actions

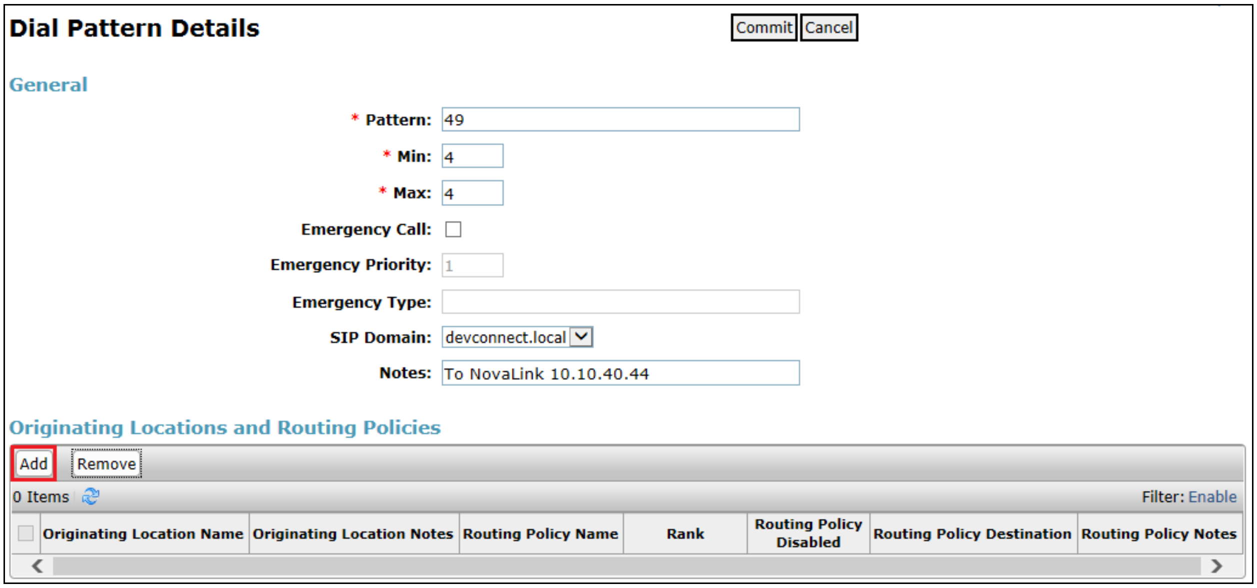
6 Items

Filter: E

☐	Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
☐	10	4	4	☐			devconnect.local	
☐	2	4	4	☐			devconnect.local	CM63
☐	30	4	4	☐			-ALL-	CS1KPG1
☐	5999	4	5	☐			-ALL-	AURA_Messaging
☐	70	4	4	☐			devconnect.local	CS1KPG1

Select : All, None

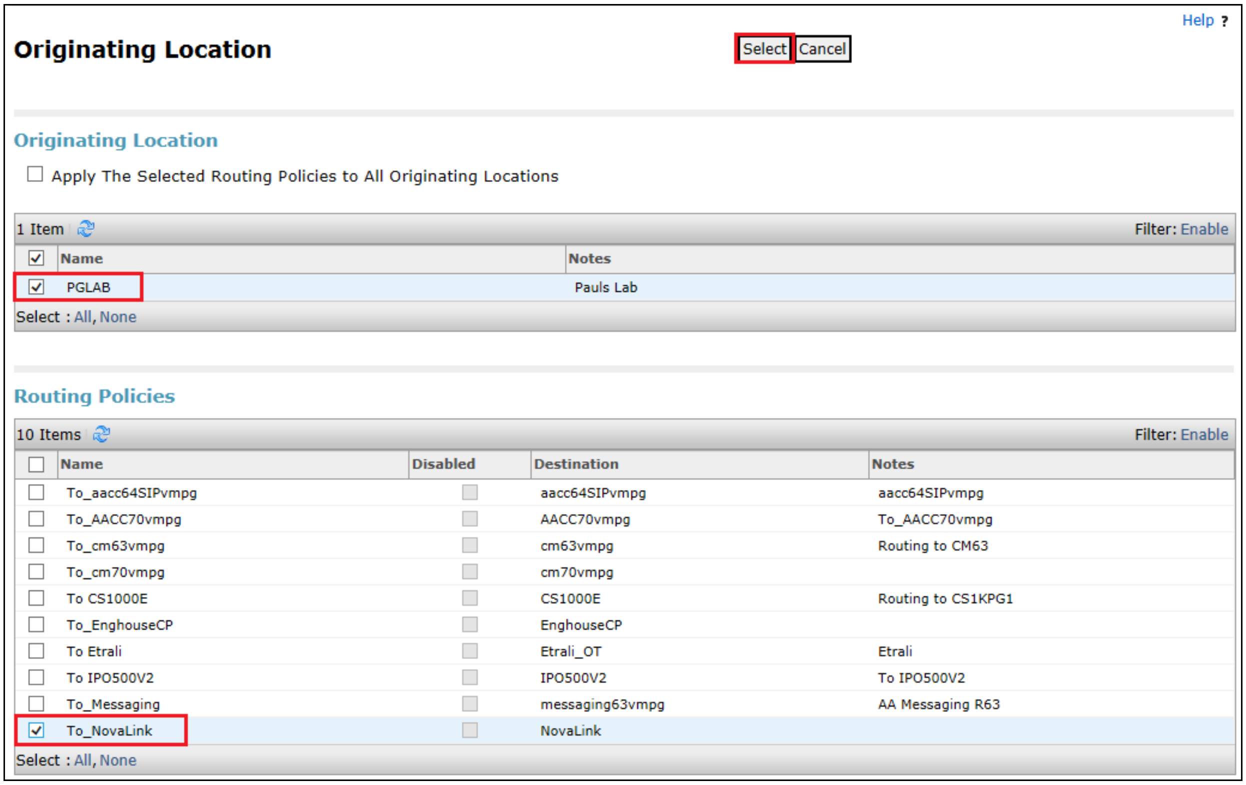
Enter the number to be routed noting this will be the same number outlined in **Section 5.4**. Note the **SIP Domain** is that configured in **Section 6.2**. Click on **Add** to select the SIP Entity.



* Pattern:	49
* Min:	4
* Max:	4
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	devconnect.local
Notes:	To NovaLink 10.10.40.44

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes

Tick on the **Originating Location** as shown below and select the **novalink** Routing Policy. Click on **Select** once complete.

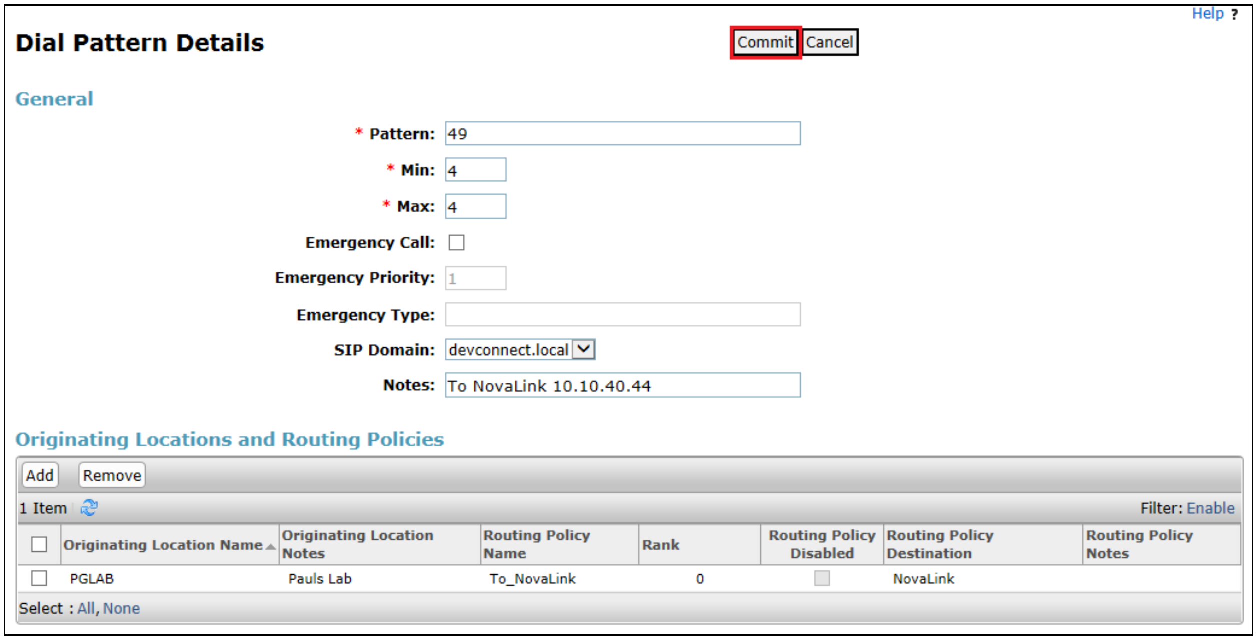


□ Apply The Selected Routing Policies to All Originating Locations

☑	Name	Notes
☑	PGLAB	Pauls Lab

□	Name	Disabled	Destination	Notes
□	To_aacc64SIPvmpg	□	aacc64SIPvmpg	aacc64SIPvmpg
□	To_AACC70vmpg	□	AACC70vmpg	To_AACC70vmpg
□	To_cm63vmpg	□	cm63vmpg	Routing to CM63
□	To_cm70vmpg	□	cm70vmpg	
□	To CS1000E	□	CS1000E	Routing to CS1KPG1
□	To_EnghouseCP	□	EnghouseCP	
□	To Etrali	□	Etrali_OT	Etrali
□	To IPO500V2	□	IPO500V2	To IPO500V2
□	To_Messaging	□	messaging63vmpg	AA Messaging R63
☑	To_NovaLink	□	NovaLink	

With the new Routing Policy in place, click on **Commit** as shown below.



Dial Pattern Details

General

* Pattern:	49
* Min:	4
* Max:	4
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	devconnect.local
Notes:	To NovaLink 10.10.40.44

Originating Locations and Routing Policies

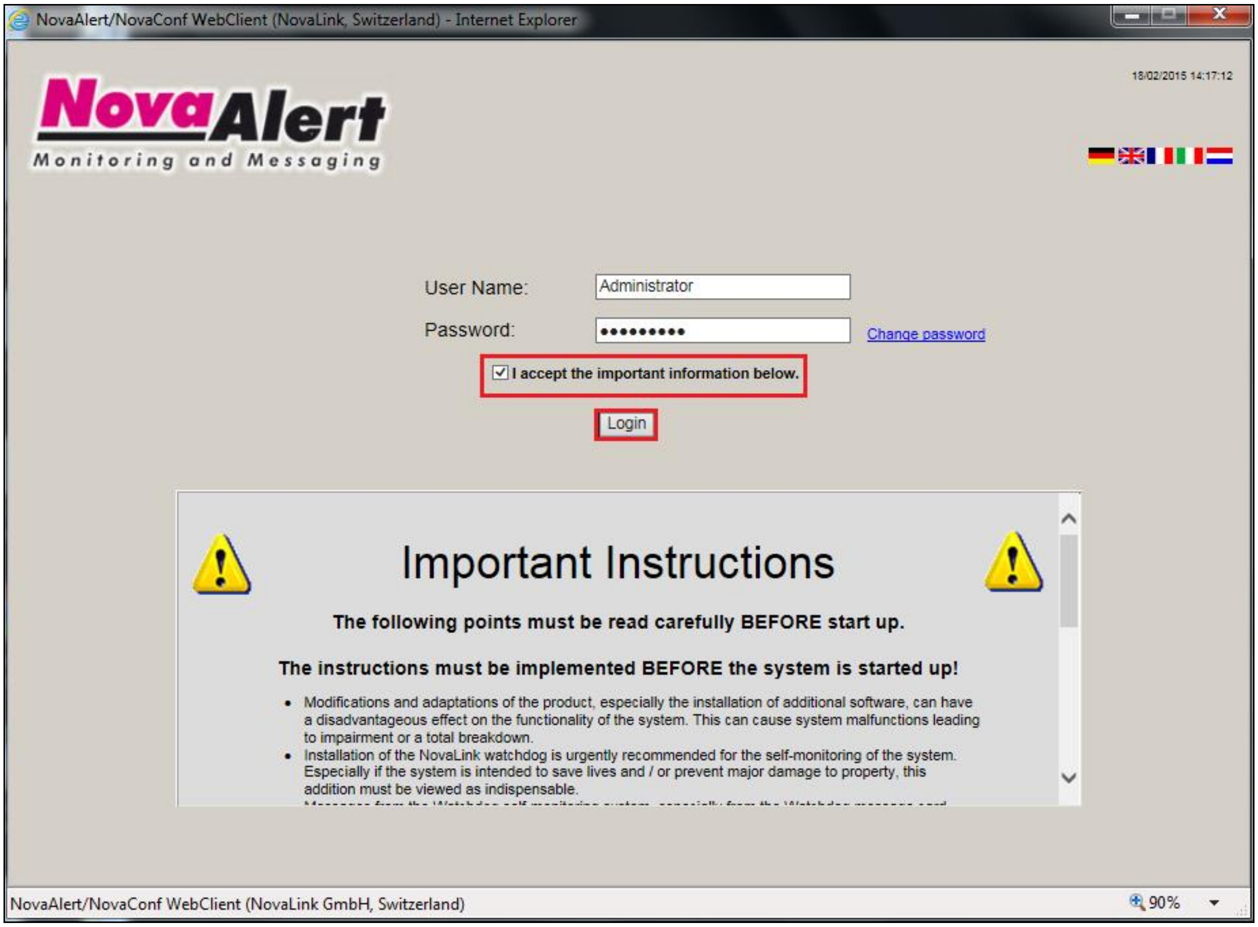
1 Item

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	PGLAB	Pauls Lab	To_NovaLink	0	□	NovaLink	

Select : All, None

7. Configure novaalert

The following sections describe the steps required to configure novaalert in order to successfully connect to Session Manager using SIP trunks. 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 what was used for compliance testing was **http://10.10.40.44/novaalert**. The following screen is shown asking for the **User Name** and **Password**. Enter these and click on the tick box as shown then click on the **Login** button.


NovaAlert/NovaConf WebClient (NovaLink, Switzerland) - Internet Explorer
18/02/2015 14:17:12
NovaAlert
Monitoring and Messaging
Change password
Login
NovaAlert/NovaConf WebClient (NovaLink GmbH, Switzerland)
90%

User Name: Administrator

Password: ••••••••••

☑ I accept the important information below.

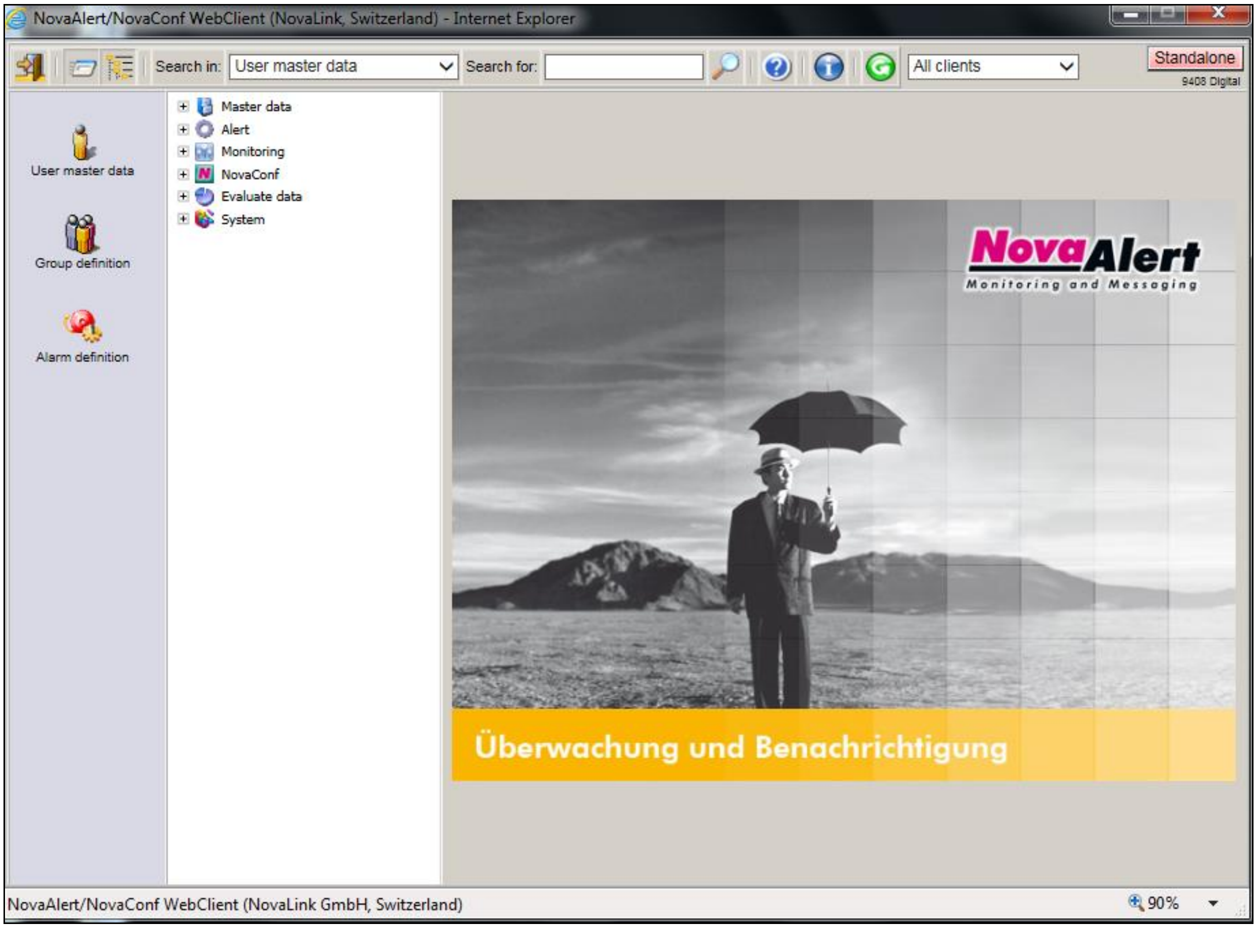
Important Instructions

The following points must be read carefully BEFORE start up.

The instructions must be implemented BEFORE the system is started up!

- Modifications and adaptations of the product, especially the installation of additional software, can have a disadvantageous effect on the functionality of the system. This can cause system malfunctions leading to impairment or a total breakdown.
- Installation of the NovaLink watchdog is urgently recommended for the self-monitoring of the system. Especially if the system is intended to save lives and / or prevent major damage to property, this addition must be viewed as indispensable.

Once logged in the following screen is presented to the user.


NovaAlert/NovaConf WebClient (NovaLink, Switzerland) - Internet Explorer
Search in: User master data
Search for:
All clients
Standalone
9408 Digital
User master data
Group definition
Alarm definition
Master data
Alert
Monitoring
NovaConf
Evaluate data
System
NovaAlert
Monitoring and Messaging
Überwachung und Benachrichtigung
NovaAlert/NovaConf WebClient (NovaLink GmbH, Switzerland)
90%

7.1. Configure novaalert SIP Trunk Connection

To begin the configuration of novaalert in order to connect to Session Manager using SIP trunks, from the main menu, expand **System** → **Setup/Maintenance** and click on **Edit configuration**. From the main window select **novaalert Basic Configuration**, from the drop-down menu.

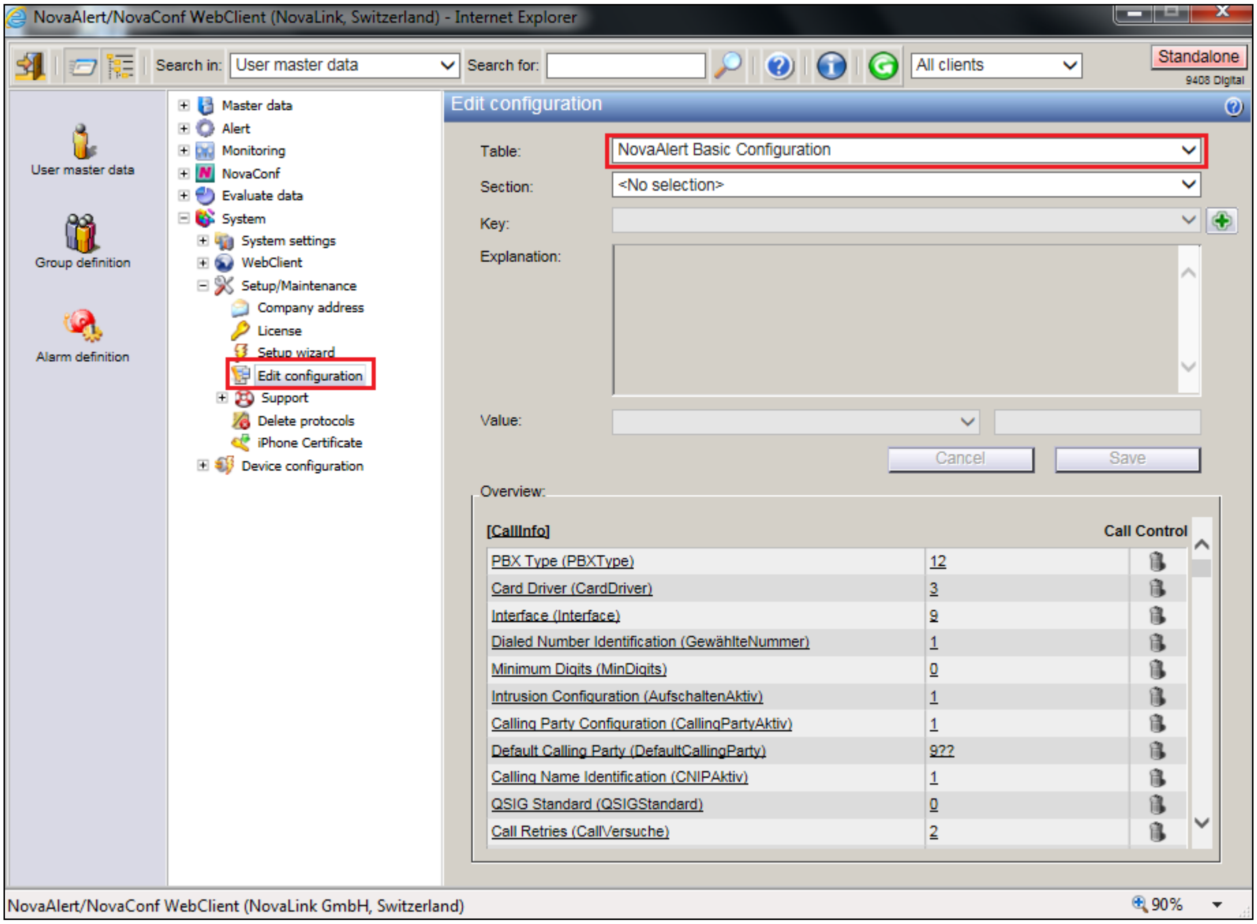


Table: NovaAlert Basic Configuration

Section: <No selection>

Key:

Explanation:

Value:

Overview:

[CallInfo]		Call Control
PBX Type (PBXType)	12	
Card Driver (CardDriver)	3	
Interface (Interface)	9	
Dialed Number Identification (GewählteNummer)	1	
Minimum Digits (MinDigits)	0	
Intrusion Configuration (AufschaltenAktiv)	1	
Calling Party Configuration (CallingPartyAktiv)	1	
Default Calling Party (DefaultCallingParty)	9??	
Calling Name Identification (CNIPAktiv)	1	
QSIG Standard (QSIGStandard)	0	
Call Retries (CallVersuche)	2	

Select **Call Control (CallInfo)** from the **Section** drop-down menu. Select **PBX Type** from the **Key** drop-down menu or click on **PBX Type** highlighted at the bottom of the screen. Ensure that the **Value** is set to **Avaya CM** and click on **Save**.

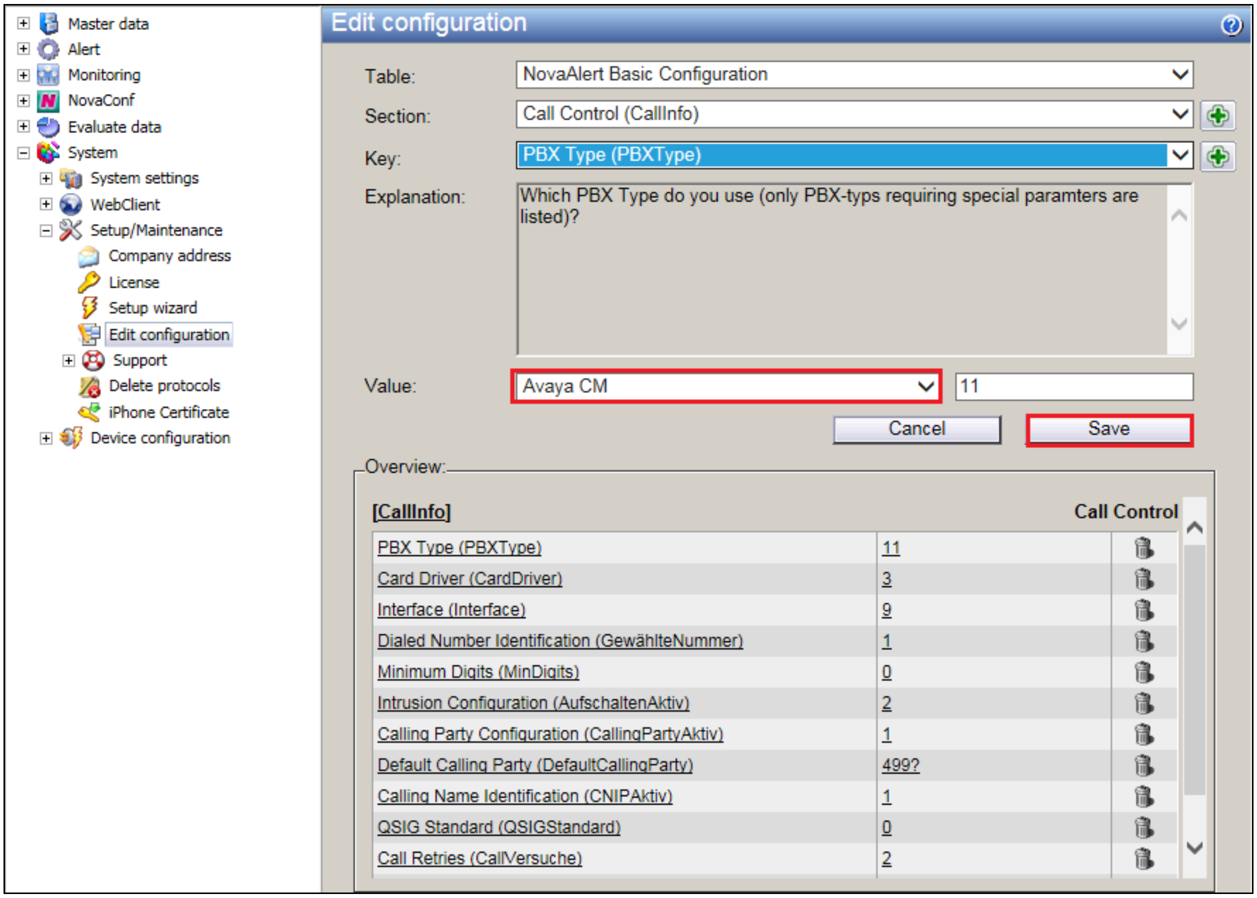


Table: NovaAlert Basic Configuration

Section: Call Control (CallInfo)

Key: PBX Type (PBXType)

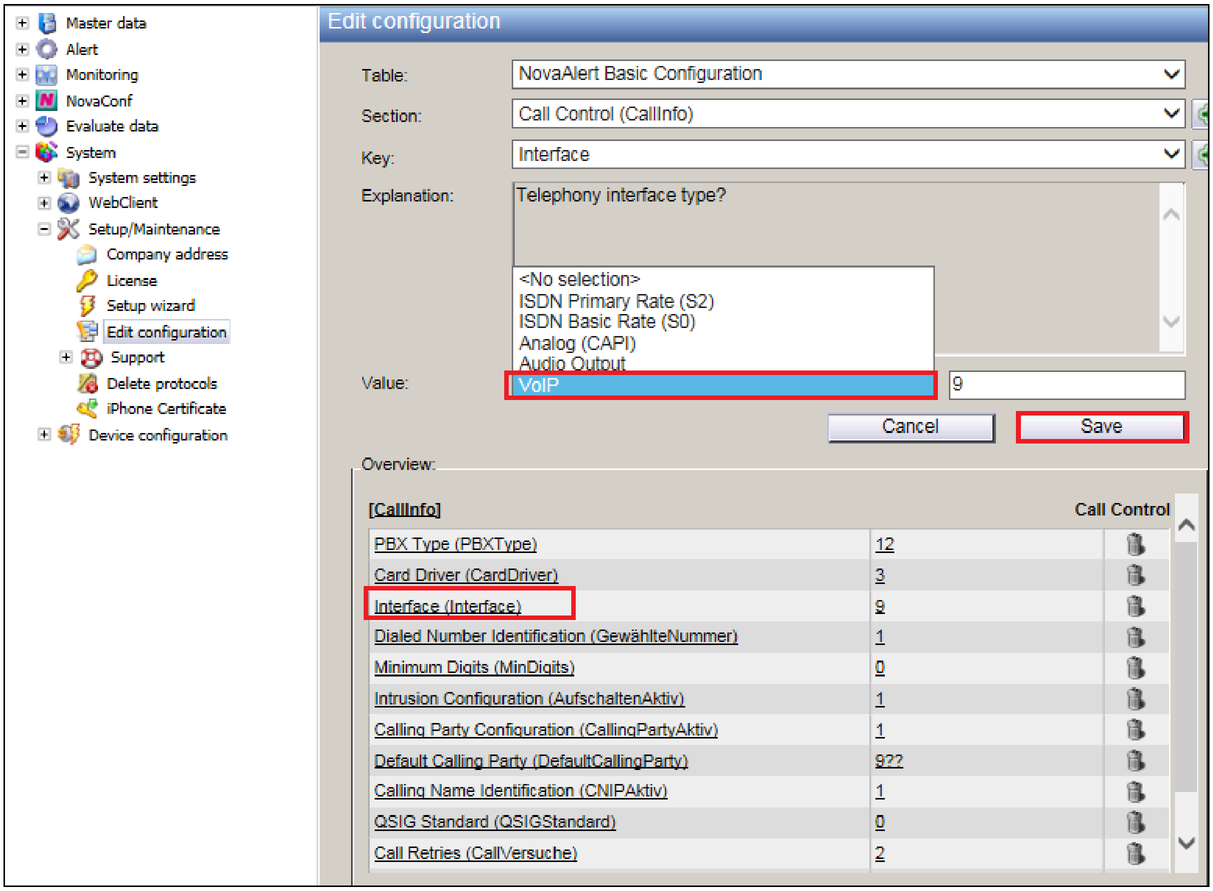
Explanation: Which PBX Type do you use (only PBX-typs requiring special paramters are listed)?

Value: Avaya CM 11

Overview:

[CallInfo]		Call Control
PBX Type (PBXType)	11	
Card Driver (CardDriver)	3	
Interface (Interface)	9	
Dialed Number Identification (GewählteNummer)	1	
Minimum Digits (MinDigits)	0	
Intrusion Configuration (AufschaltenAktiv)	2	
Calling Party Configuration (CallingPartyAktiv)	1	
Default Calling Party (DefaultCallingParty)	499?	
Calling Name Identification (CNIPAktiv)	1	
QSIG Standard (QSIGStandard)	0	
Call Retries (CallVersuche)	2	

Remaining in the same **Section**, select **Interface** from the **Key** drop-down menu and ensure that the **Value** is set to **VoIP**. Click on **Save** to complete.



Edit configuration

Table: NovaAlert Basic Configuration

Section: Call Control (CallInfo)

Key: Interface

Explanation: Telephony interface type?

Value: VoIP 9

<No selection>
ISDN Primary Rate (S2)
ISDN Basic Rate (S0)
Analog (CAPI)
Audio Output
VoIP

Overview:

[CallInfo]		Call Control
PBX Type (PBXType)	12	
Card Driver (CardDriver)	3	
Interface (Interface)	9	
Dialed Number Identification (GewählteNummer)	1	
Minimum Digits (MinDigits)	0	
Intrusion Configuration (AufschaltenAktiv)	1	
Calling Party Configuration (CallingPartyAktiv)	1	
Default Calling Party (DefaultCallingParty)	9??	
Calling Name Identification (CNIPAktiv)	1	
QSIG Standard (QSIGStandard)	0	
Call Retries (CallVersuche)	2	

In the same **Section** select the **Calling Party Configuration (CallingPartyAktiv) Key**. Set the **Value** to **Yes** and click on **Save**. This will send the calling party with the outgoing call.

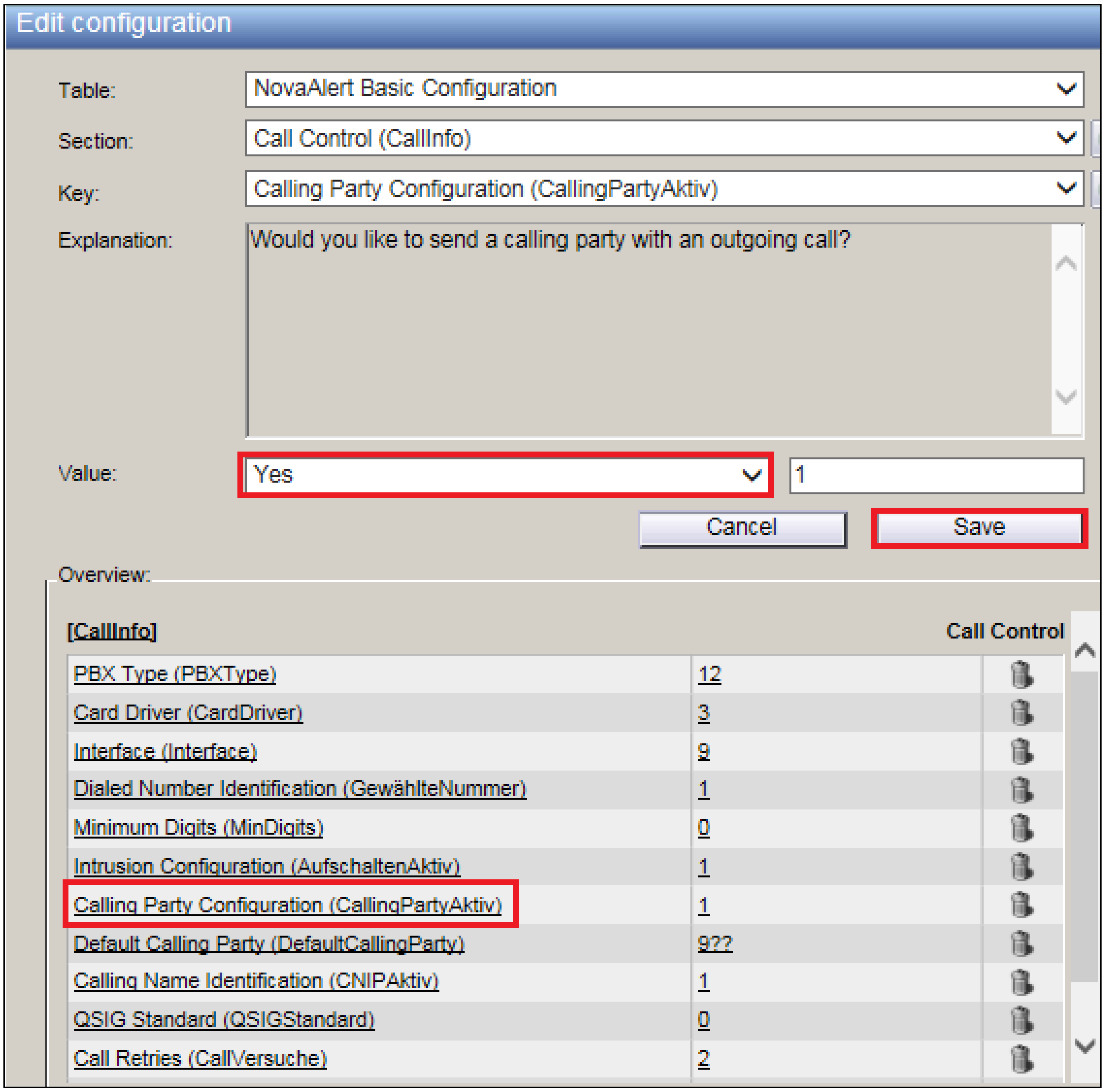


Table: NovaAlert Basic Configuration

Section: Call Control (CallInfo)

Key: Calling Party Configuration (CallingPartyAktiv)

Explanation: Would you like to send a calling party with an outgoing call?

Value: Yes 1

Overview:

[CallInfo]		Call Control
PBX Type (PBXType)	12	
Card Driver (CardDriver)	3	
Interface (Interface)	9	
Dialed Number Identification (GewählteNummer)	1	
Minimum Digits (MinDigits)	0	
Intrusion Configuration (AufschaltenAktiv)	1	
Calling Party Configuration (CallingPartyAktiv)	1	
Default Calling Party (DefaultCallingParty)	9??	
Calling Name Identification (CNIPAktiv)	1	
QSIG Standard (QSIGStandard)	0	
Call Retries (CallVersuche)	2	

In the same **Section** select the **Default Calling Party (DefaultCallingParty) Key**. Set the **Value** to **499?** and click on **Save.** Note this value will be used for dialing out from Communication Manager.

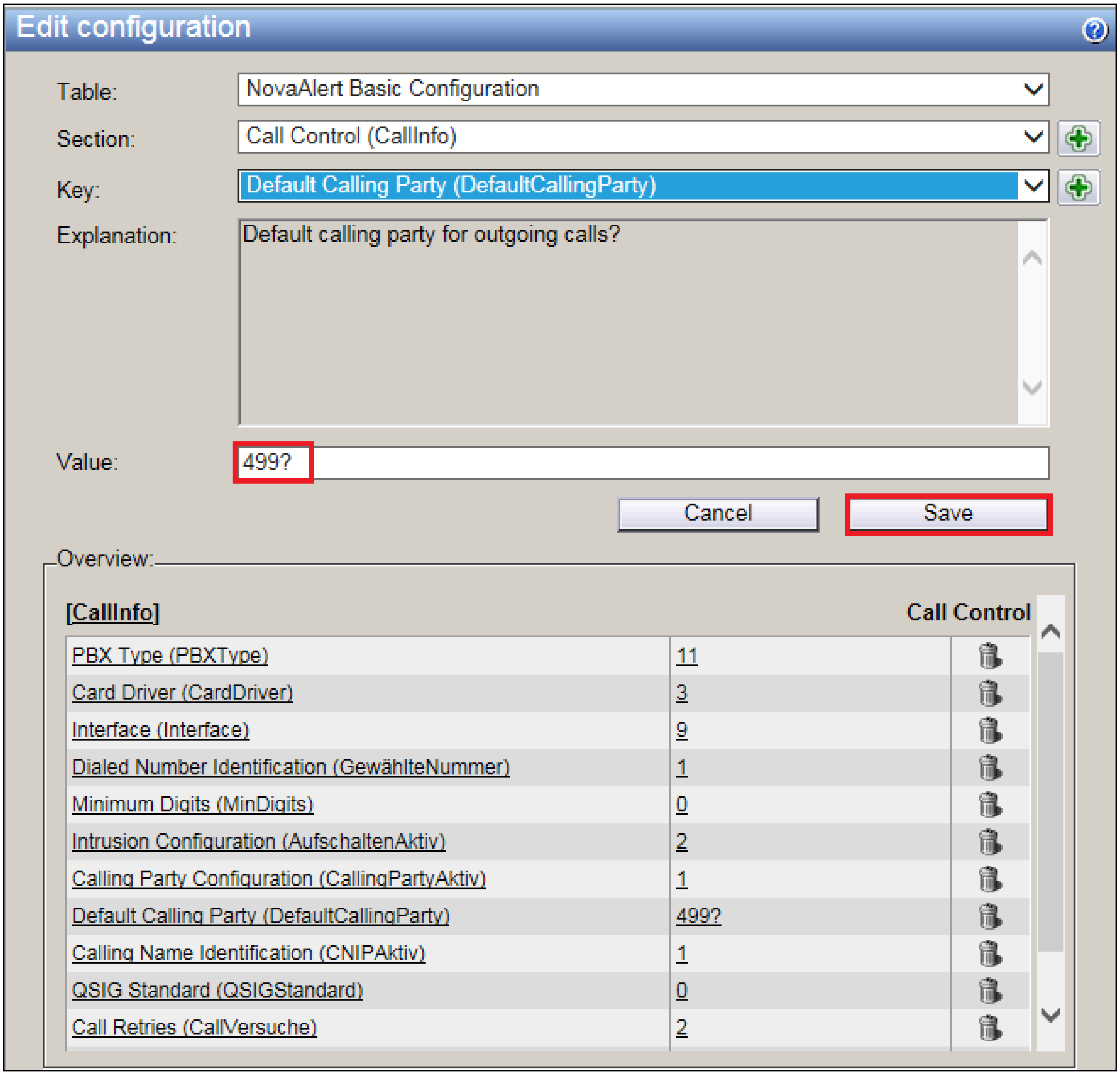


Table: NovaAlert Basic Configuration

Section: Call Control (CallInfo)

Key: Default Calling Party (DefaultCallingParty)

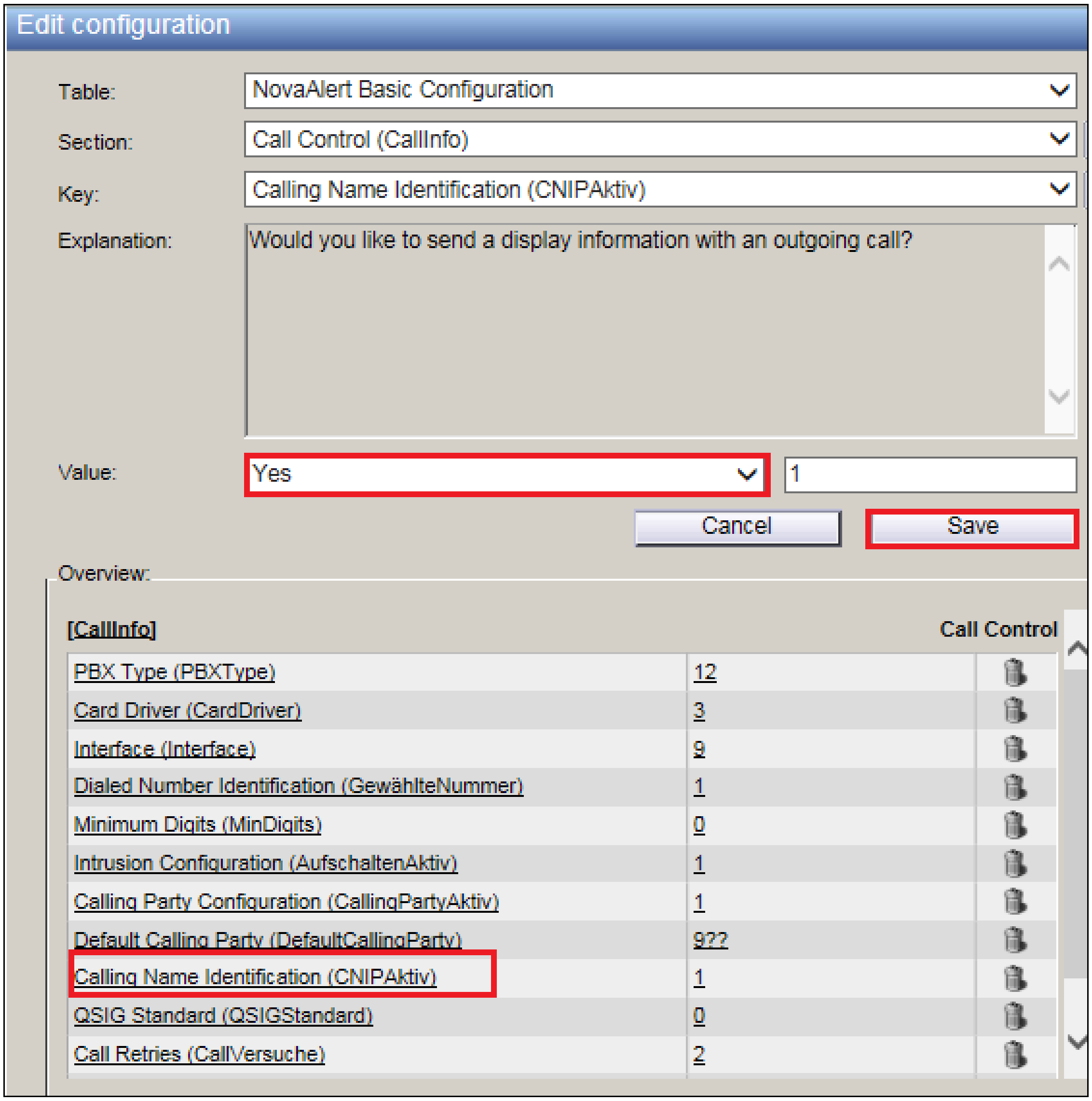
Explanation: Default calling party for outgoing calls?

Value: 499?

Overview:

[CallInfo]	Call Control
PBX Type (PBXType)	11
Card Driver (CardDriver)	3
Interface (Interface)	9
Dialed Number Identification (GewählteNummer)	1
Minimum Digits (MinDigits)	0
Intrusion Configuration (AufschaltenAktiv)	2
Calling Party Configuration (CallingPartyAktiv)	1
Default Calling Party (DefaultCallingParty)	499?
Calling Name Identification (CNIPAktiv)	1
QSIG Standard (QSIGStandard)	0
Call Retries (CallVersuche)	2

In the same **Section** select the **Calling Name Identification (CNIPAktiv) Key**. Set the **Value** to **Yes** and click on **Save**. This will send the CLID info on the outgoing call.



Edit configuration

Table: NovaAlert Basic Configuration

Section: Call Control (CallInfo)

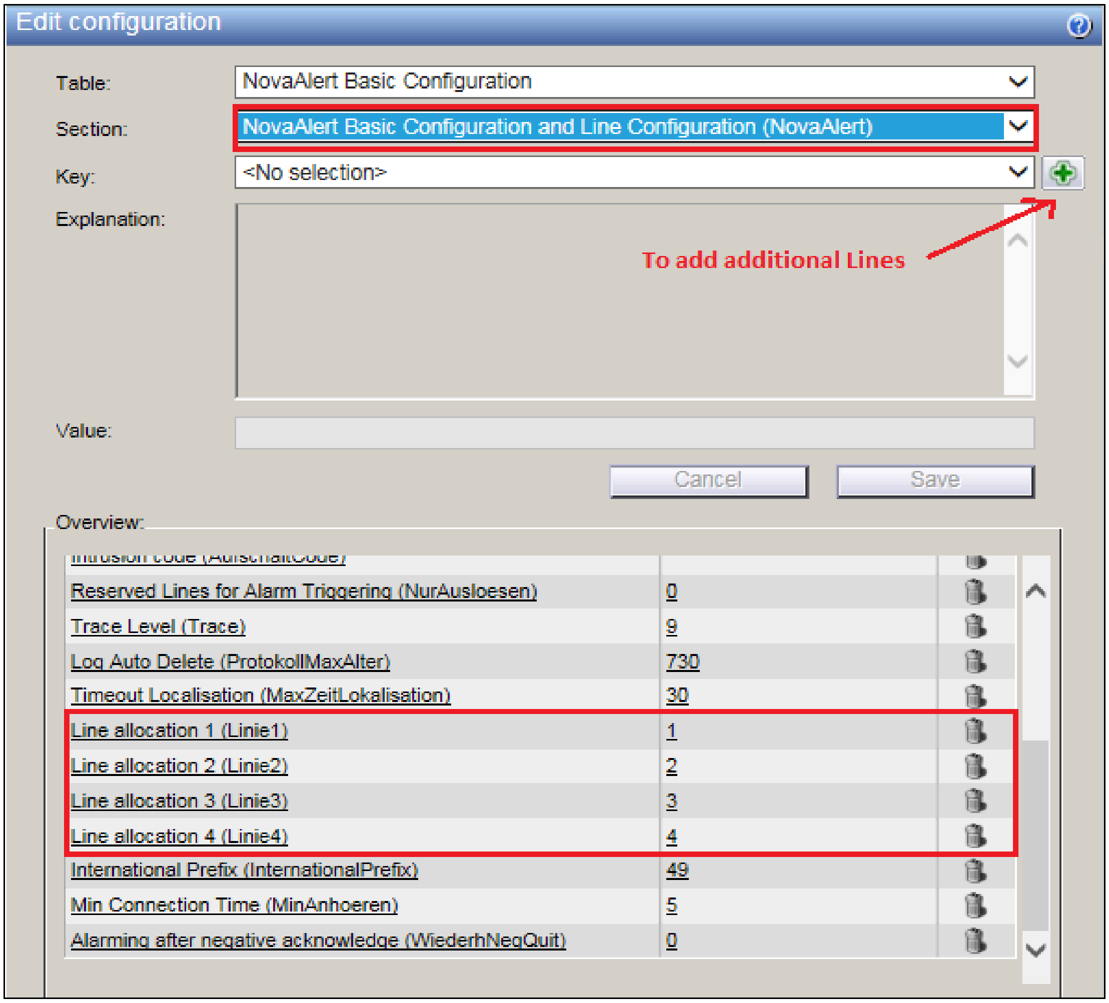
Key: Calling Name Identification (CNIPAktiv)

Explanation: Would you like to send a display information with an outgoing call?

Value: Yes 1

[CallInfo]	Call Control
PBX Type (PBXType)	12
Card Driver (CardDriver)	3
Interface (Interface)	9
Dialed Number Identification (GewählteNummer)	1
Minimum Digits (MinDigits)	0
Intrusion Configuration (AufschaltenAktiv)	1
Calling Party Configuration (CallingPartyAktiv)	1
Default Calling Party (DefaultCallingParty)	9??
Calling Name Identification (CNIPAktiv)	1
QSIG Standard (QSIGStandard)	0
Call Retries (CallVersuche)	2

Select **novaalert Basic Configuration and Line Configuration (novaalert)** from the **Section** drop-down menu. In order to add lines to any existing lines shown in the **Overview** window, click on the **+** icon to the right of the **Key** drop down menu, as is shown below.



Edit configuration

Table: NovaAlert Basic Configuration

Section: NovaAlert Basic Configuration and Line Configuration (NovaAlert)

Key: <No selection>

Explanation:

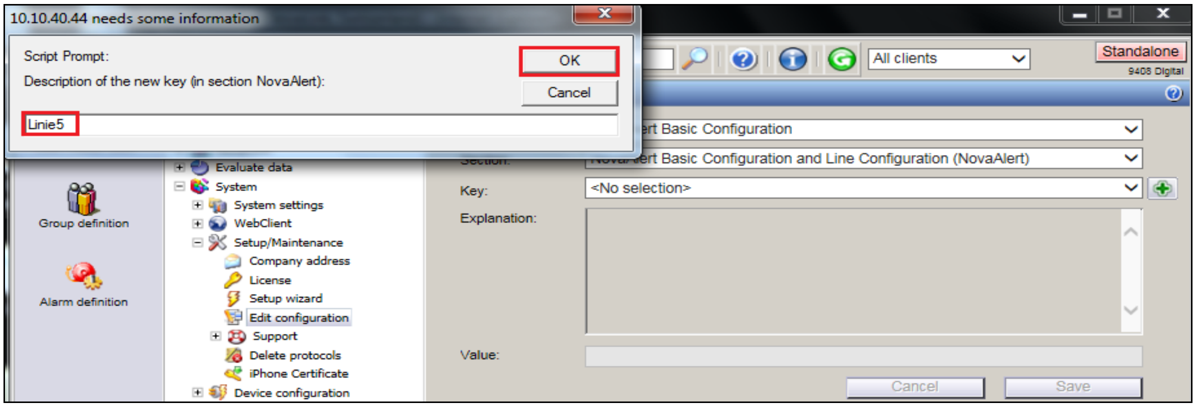
Value:

To add additional Lines

Overview:

Intrusion code (AufschaltCode)	
Reserved Lines for Alarm Triggering (NurAusloesen)	0
Trace Level (Trace)	9
Log Auto Delete (ProtokollMaxAlter)	730
Timeout Localisation (MaxZeitLokalisation)	30
Line allocation 1 (Linie1)	1
Line allocation 2 (Linie2)	2
Line allocation 3 (Linie3)	3
Line allocation 4 (Linie4)	4
International Prefix (InternationalPrefix)	49
Min Connection Time (MinAnhoeren)	5
Alarming after negative acknowledge (WiederhNegQuit)	0

The following window opens, enter **LinieX** into the window and click on **OK**, where X is the next line number to be added.



10.10.40.44 needs some information

Script Prompt:

Description of the new key (in section NovaAlert):

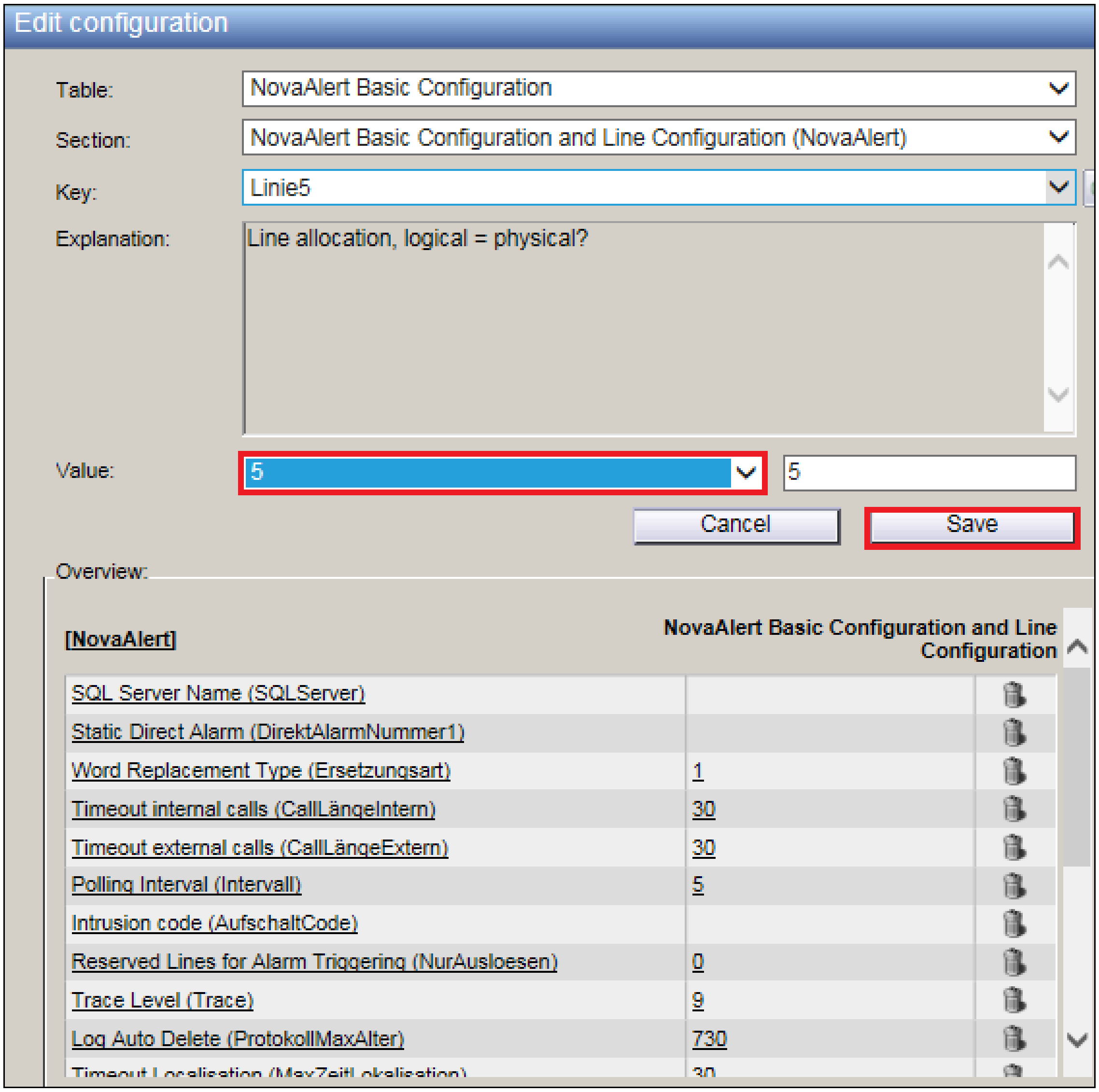
Linie5

Key: <No selection>

Explanation:

Value:

The Key added above, Linie5 should now populate the **Key** menu. Enter the **Value** X where X is the next line number to be added; in this case it is **5**. Click on **Save** to continue.



Edit configuration

Table: NovaAlert Basic Configuration

Section: NovaAlert Basic Configuration and Line Configuration (NovaAlert)

Key: Linie5

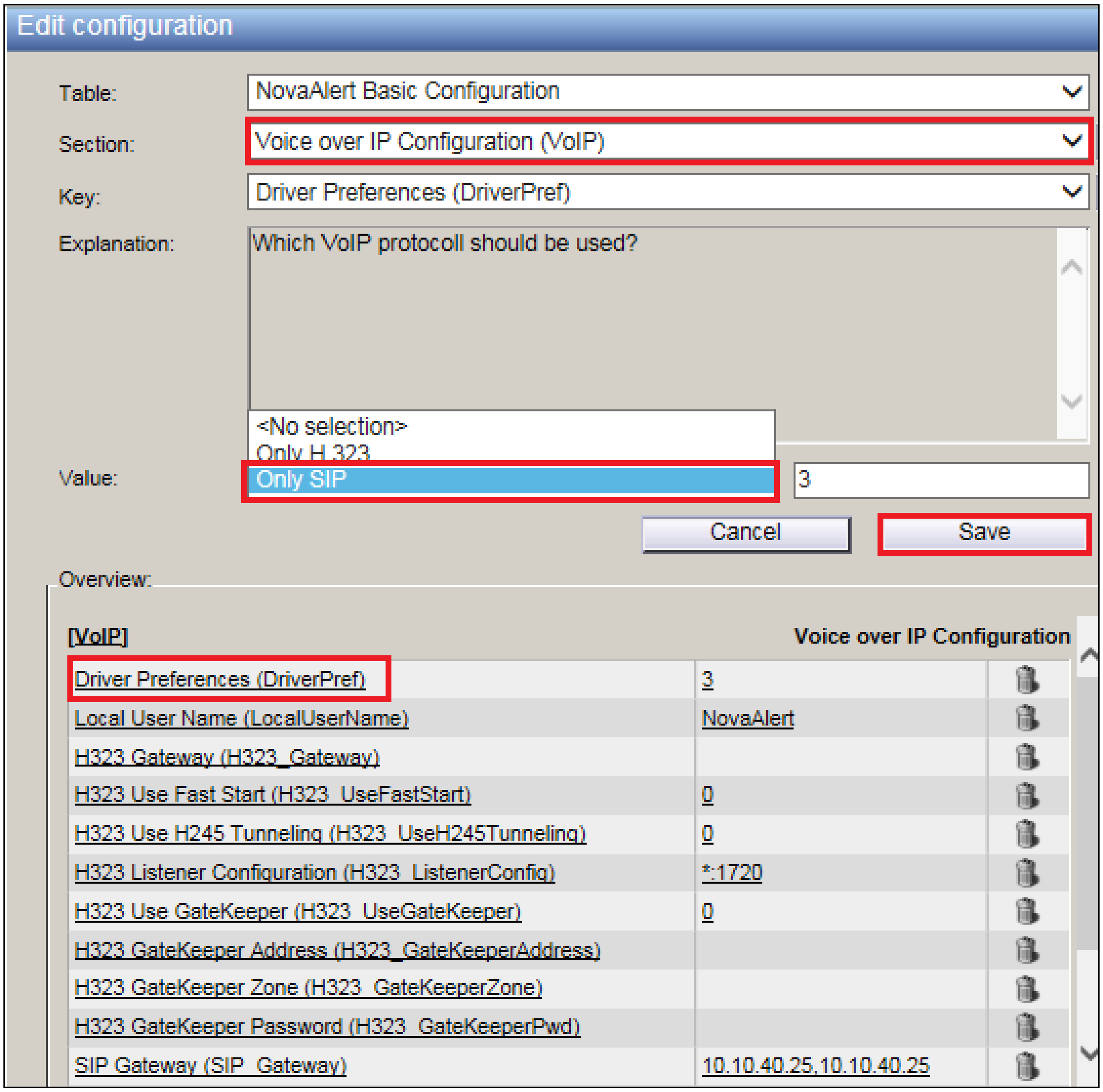
Explanation: Line allocation, logical = physical?

Value: 5 | 5

[NovaAlert] NovaAlert Basic Configuration and Line Configuration

SQL Server Name (SQLServer)	
Static Direct Alarm (DirektAlarmNummer1)	
Word Replacement Type (Ersetzungsart)	1
Timeout internal calls (CallLängeIntern)	30
Timeout external calls (CallLängeExtern)	30
Polling Interval (Intervall)	5
Intrusion code (AufschaltCode)	
Reserved Lines for Alarm Triggering (NurAusloesen)	0
Trace Level (Trace)	9
Log Auto Delete (ProtokollMaxAlter)	730
Timeout Localisation (MaxZeitLokalisation)	30

Choose a new section, **Voice over IP Configuration (VoIP)** from the **Section** drop-down menu. Select **Driver Preferences (DriverPref)** from the **Key** drop-down menu. Select **Only SIP** from the drop-down menu for **Value** and click on **Save** to continue.



Edit configuration

Table: NovaAlert Basic Configuration

Section: Voice over IP Configuration (VoIP)

Key: Driver Preferences (DriverPref)

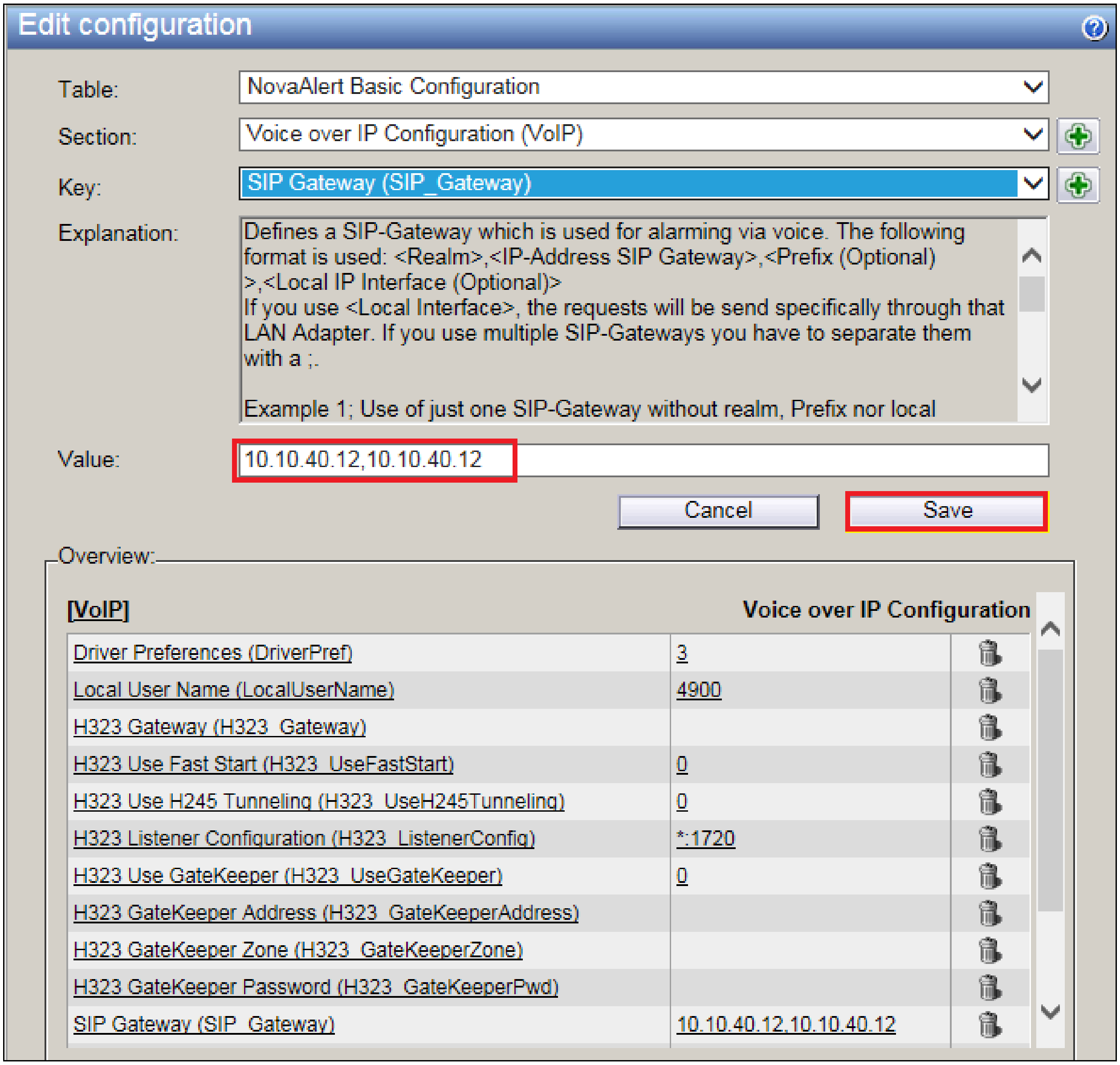
Explanation: Which VoIP protocoll should be used?

Value: Only SIP 3

Overview:

[VoIP]	Voice over IP Configuration	
Driver Preferences (DriverPref)	3	🗑
Local User Name (LocalUserName)	NovaAlert	🗑
H323 Gateway (H323_Gateway)		🗑
H323 Use Fast Start (H323_UseFastStart)	0	🗑
H323 Use H245 Tunneling (H323_UseH245Tunneling)	0	🗑
H323 Listener Configuration (H323_ListenerConfig)	*:1720	🗑
H323 Use GateKeeper (H323_UseGateKeeper)	0	🗑
H323 GateKeeper Address (H323_GateKeeperAddress)		🗑
H323 GateKeeper Zone (H323_GateKeeperZone)		🗑
H323 GateKeeper Password (H323_GateKeeperPwd)		🗑
SIP Gateway (SIP_Gateway)	10.10.40.25,10.10.40.25	🗑

Staying with the same **Section**, using the drop-down menu change the **Key** to **SIP Gateway (SIP_Gateway)**. Enter the **Value** for the SIP Gateway which will be the IP address of Session Manager. This is entered in the format IP Address, IP Address or **10.10.40.12**, **10.10.40.12** as is shown below. Click on **Save** to continue.



Edit configuration

Table: NovaAlert Basic Configuration

Section: Voice over IP Configuration (VoIP)

Key: SIP Gateway (SIP_Gateway)

Explanation: Defines a SIP-Gateway which is used for alarming via voice. The following format is used: <Realm>,<IP-Address SIP Gateway>,<Prefix (Optional)>,<Local IP Interface (Optional)>
If you use <Local Interface>, the requests will be send specifically through that LAN Adapter. If you use multiple SIP-Gateways you have to separate them with a ;.

Example 1; Use of just one SIP-Gateway without realm, Prefix nor local

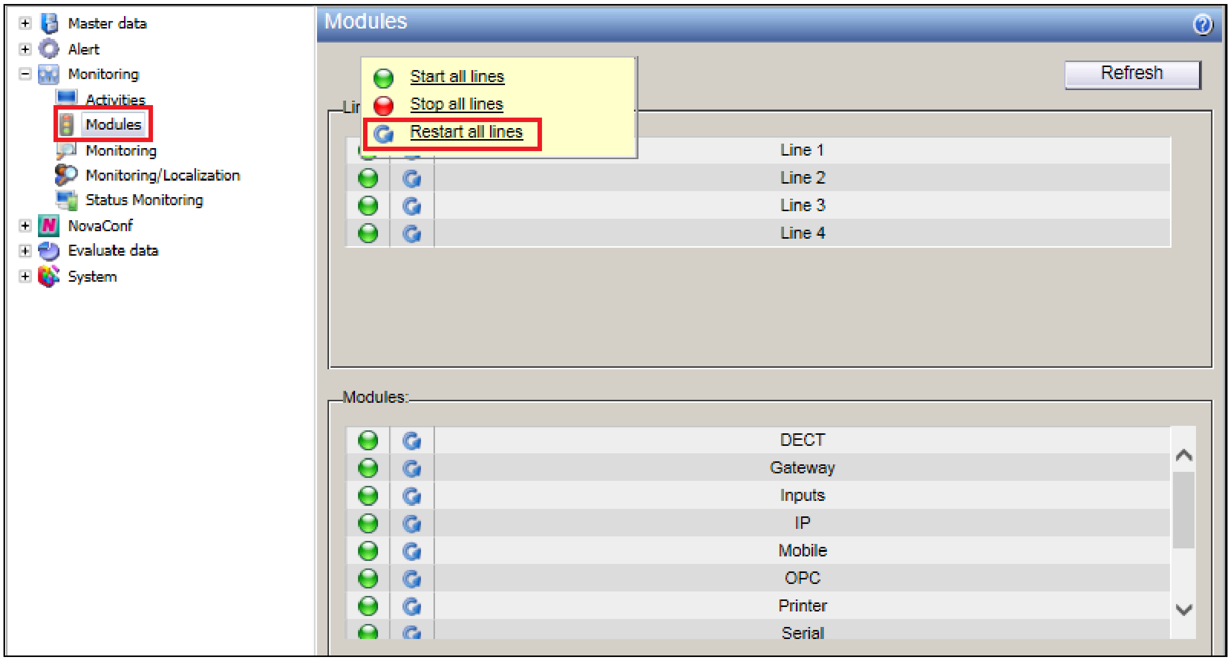
Value: 10.10.40.12,10.10.40.12

Overview:

[VoIP] Voice over IP Configuration

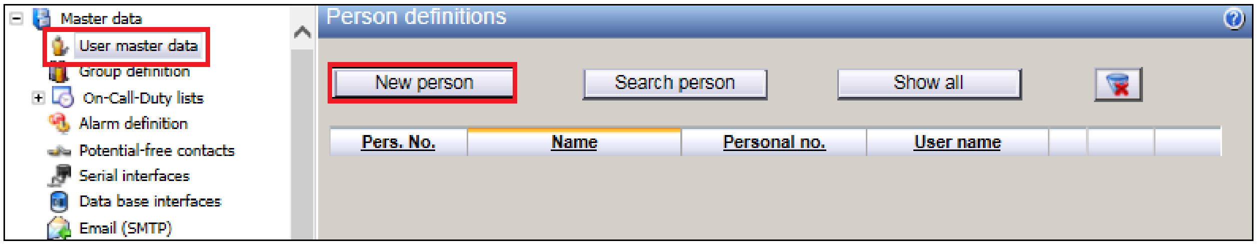
Driver Preferences (DriverPref)	3	🗑
Local User Name (LocalUserName)	4900	🗑
H323 Gateway (H323_Gateway)		🗑
H323 Use Fast Start (H323_UseFastStart)	0	🗑
H323 Use H245 Tunneling (H323_UseH245Tunneling)	0	🗑
H323 Listener Configuration (H323_ListenerConfig)	*:1720	🗑
H323 Use GateKeeper (H323_UseGateKeeper)	0	🗑
H323 GateKeeper Address (H323_GateKeeperAddress)		🗑
H323 GateKeeper Zone (H323_GateKeeperZone)		🗑
H323 GateKeeper Password (H323_GateKeeperPwd)		🗑
SIP Gateway (SIP_Gateway)	10.10.40.12,10.10.40.12	🗑

To finish out the configuration a restart of the lines is required. From the menu section navigate to **Monitoring → Modules** and from the main window click on the **refresh icon** beside any of the lines and select **Restart all lines**, as shown below.

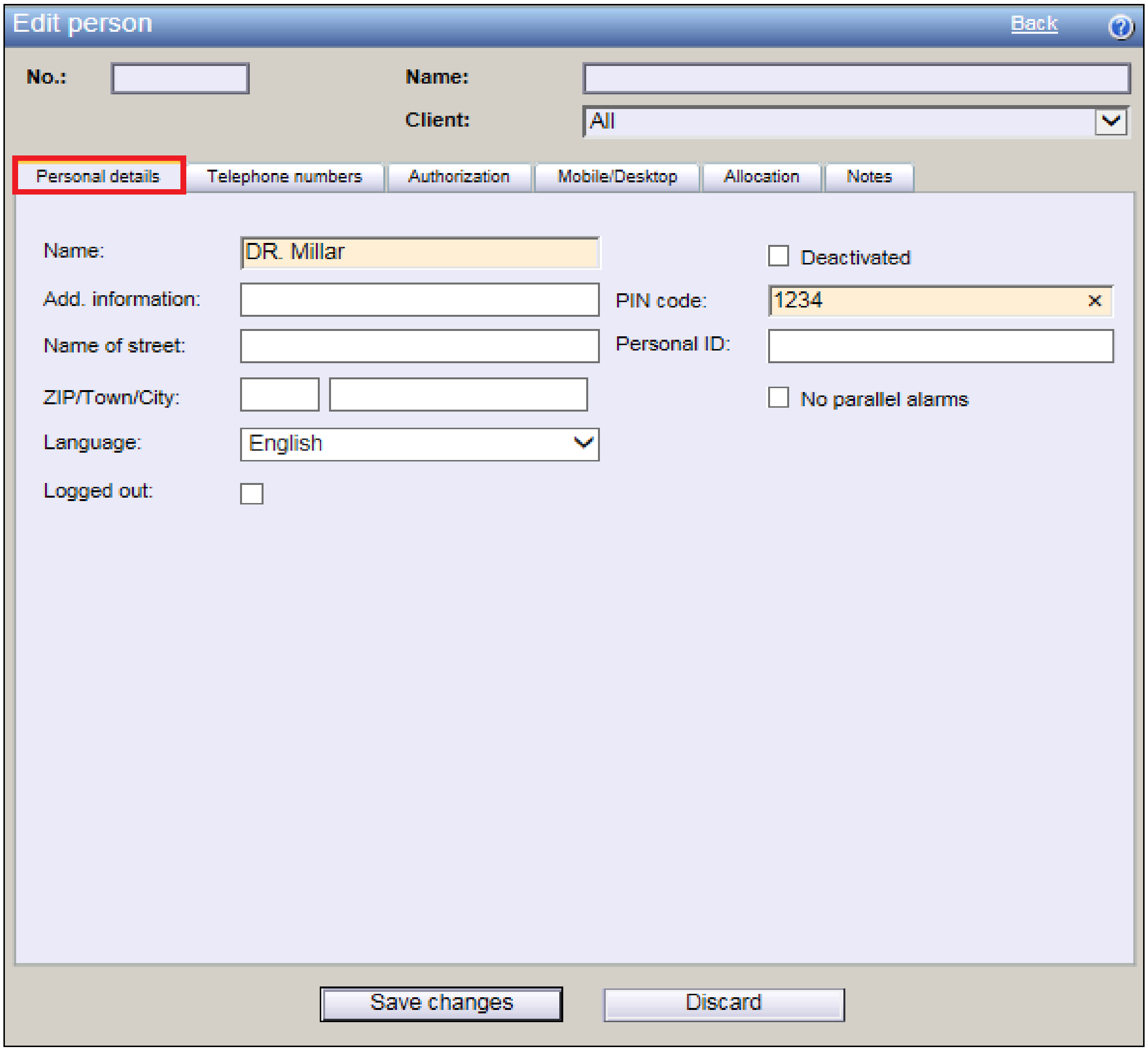


7.2. Add a Communication Manager extension to alert.

In order to send an alarm to Communication Manager, an 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 **New person** as shown below.



Click on the **Personal details** tab and enter a suitable **Name** and **Pin code**.



No.:

Name:

Client: All

Name: DR. Millar

Add. information:

Name of street:

ZIP/Town/City:

Language: English

Logged out: □

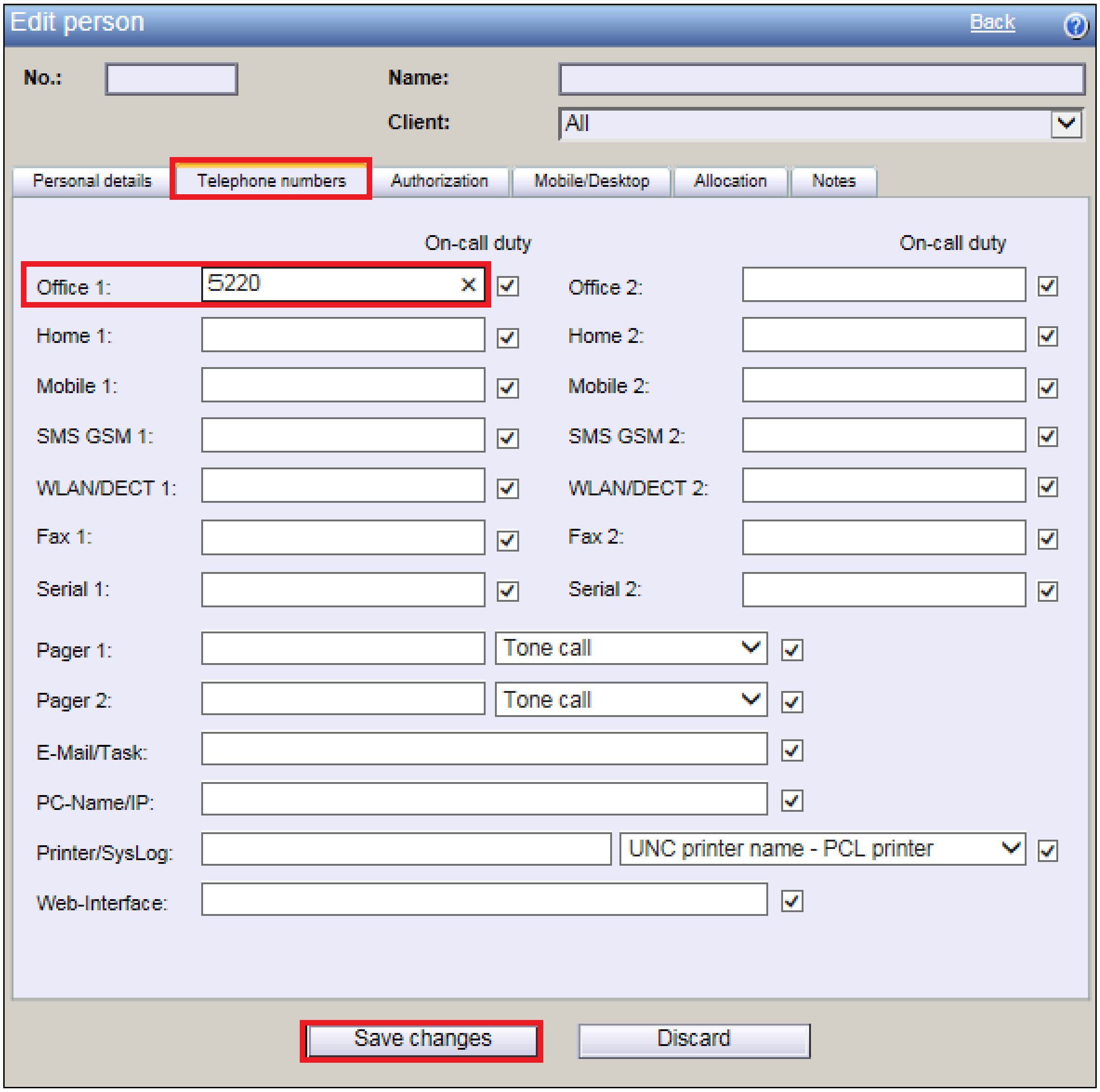
□ Deactivated

PIN code: 1234

Personal ID:

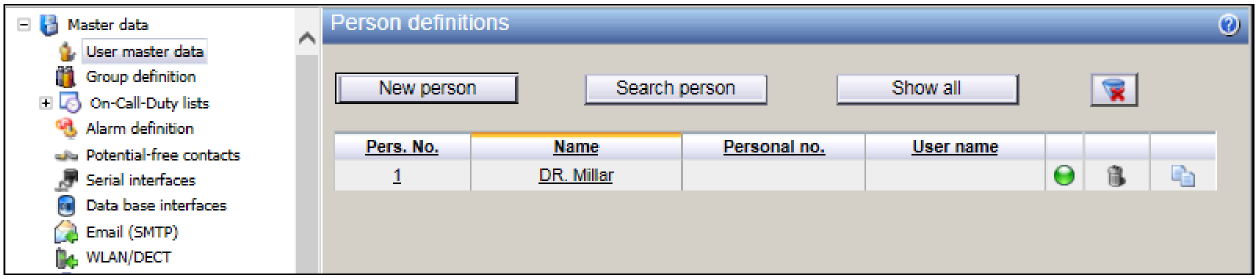
□ No parallel alarms

Click on the **Telephone numbers** tab and enter the Communication Manager telephone number for this user and click on **Save Changes** at the bottom of the screen.



No.:		Name:			
		Client:	All		
Office 1:	5220	☑	Office 2:		☑
Home 1:		☑	Home 2:		☑
Mobile 1:		☑	Mobile 2:		☑
SMS GSM 1:		☑	SMS GSM 2:		☑
WLAN/DECT 1:		☑	WLAN/DECT 2:		☑
Fax 1:		☑	Fax 2:		☑
Serial 1:		☑	Serial 2:		☑
Pager 1:		Tone call	☑		
Pager 2:		Tone call	☑		
E-Mail/Task:		☑			
PC-Name/IP:		☑			
Printer/SysLog:		UNC printer name - PCL printer	☑		
Web-Interface:		☑			

The new user/extension is now clearly shown.



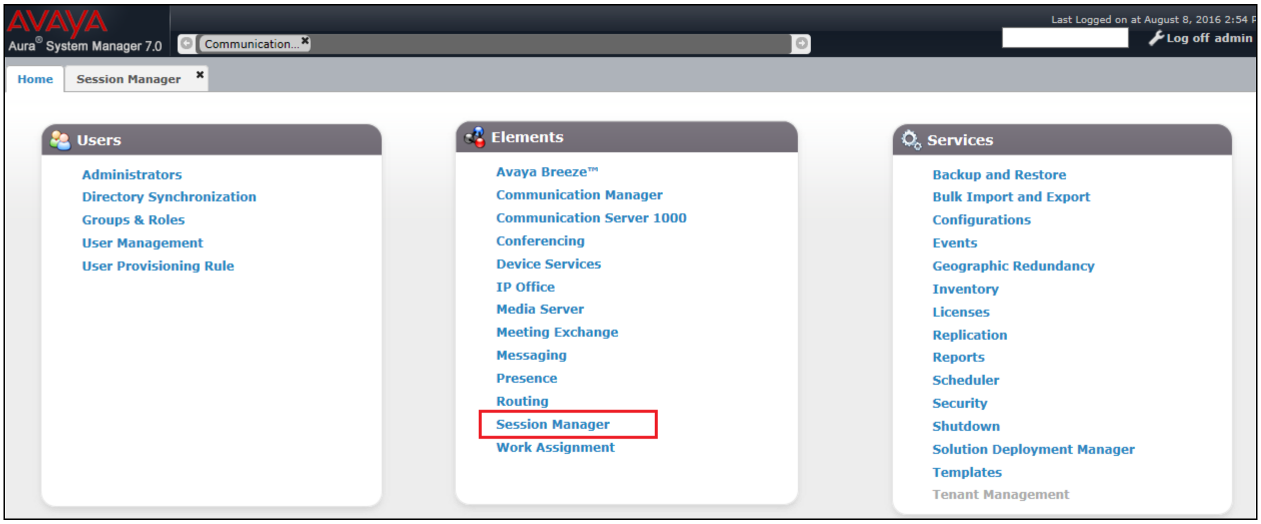
Pers. No.	Name	Personal no.	User name			
1	DR. Millar			●		

8. Verification Steps

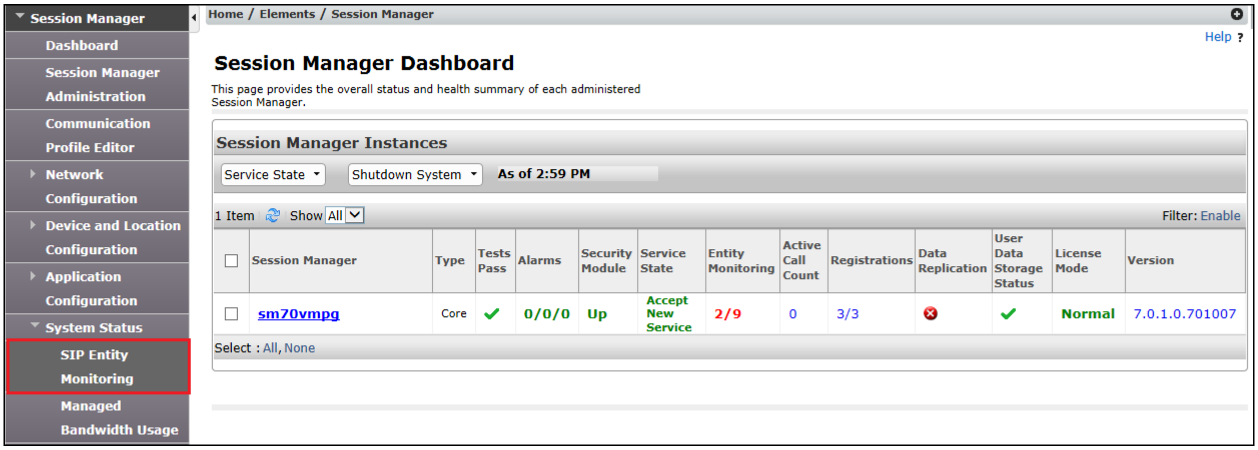
This section illustrates the steps necessary to verify that the novaalert is configured correctly to allow alarms and notifications be send to Communication Manager endpoints using SIP trunks.

8.1. Verify Link on Session Manager

Log in to System Manager as per **Section 6**. From the main menu select Session Manager as shown below.



Navigate to **System Status → SIP Entity Monitoring**.


Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
SIP Entity Monitoring
Managed Bandwidth Usage
Home / Elements / Session Manager
Help ?

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

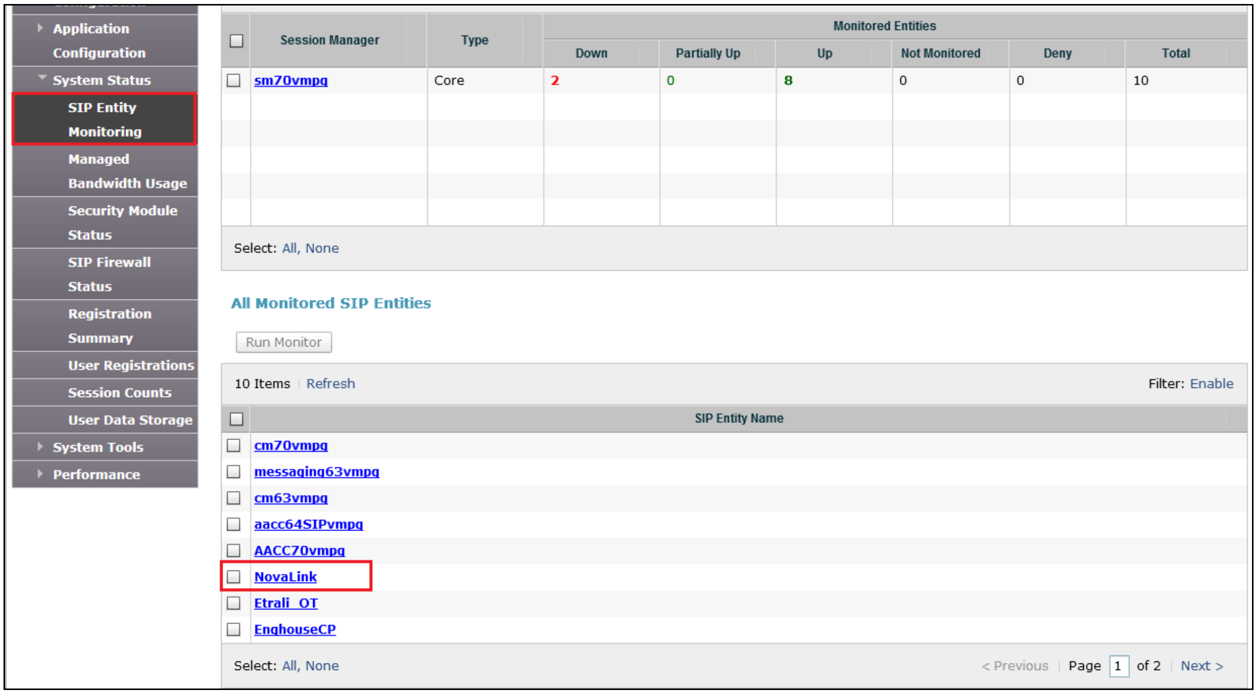
Service State ▾ Shutdown System ▾ As of 2:59 PM

1 Item Show All Filter: Enable

□	Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	License Mode	Version
□	sm70vmpg	Core	✓	0/0/0	Up	Accept New Service	2/9	0	3/3	☒	✓	Normal	7.0.1.0.701007

Select : All, None

Choose the **novalink** SIP entity as shown below.



□	Session Manager	Type	Monitored Entities					
			Down	Partially Up	Up	Not Monitored	Deny	Total
□	sm70vmpg	Core	2	0	8	0	0	10

Select: All, None

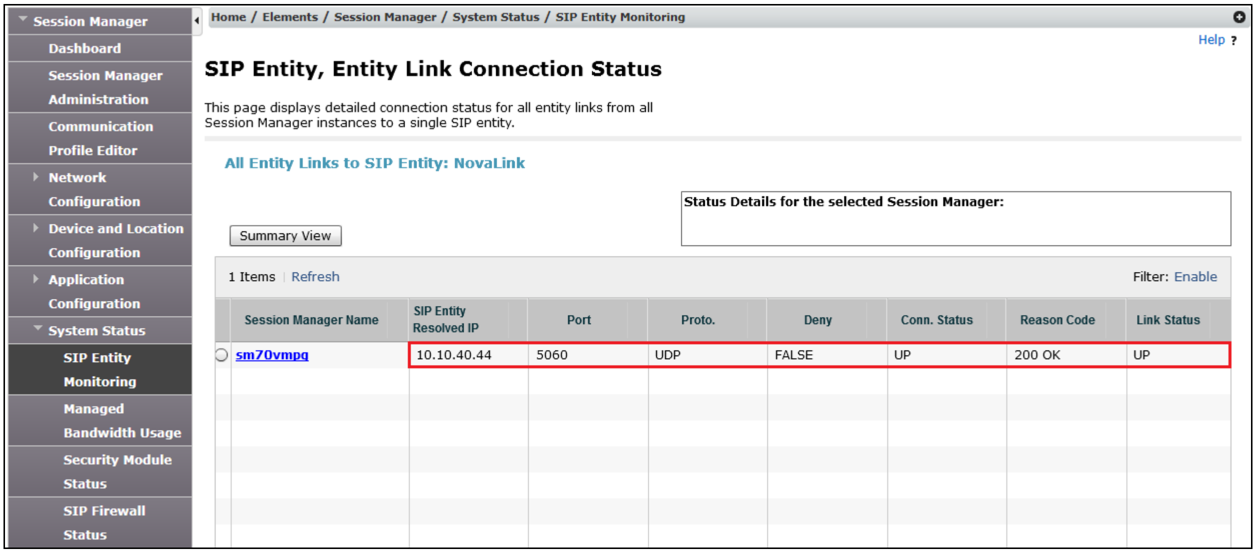
All Monitored SIP Entities

10 Items | Refresh Filter: Enable

□	SIP Entity Name
□	cm70vmpg
□	messaging63vmpg
□	cm63vmpg
□	aacc64SIPvmpg
□	AACC70vmpg
□	NovaLink
□	Etrali_OT
□	EnghouseCP

Select: All, None < Previous | Page 1 of 2 | Next >

The **Link Status** and **Conn. Status** should both show as **UP** as is shown below.



Home / Elements / Session Manager / System Status / SIP Entity Monitoring

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: NovaLink

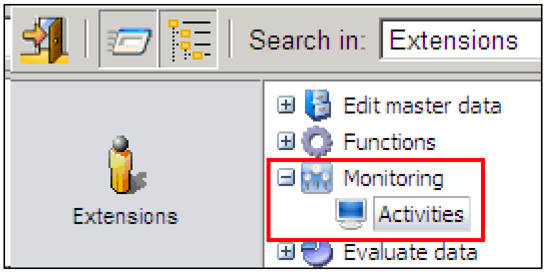
Status Details for the selected Session Manager:

1 Items | Refresh Filter: Enable

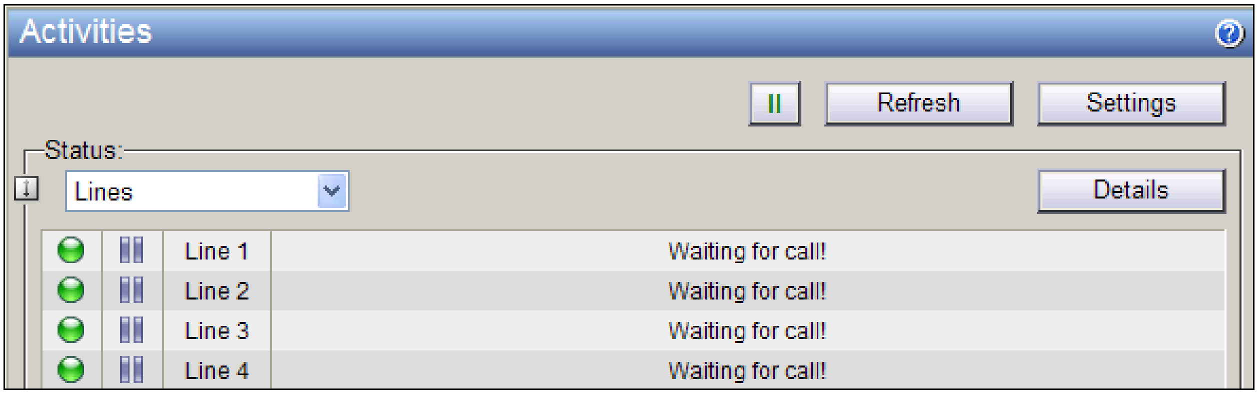
	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	sm70vmpg	10.10.40.44	5060	UDP	FALSE	UP	200 OK	UP

8.2. Verify novaalert Status

From the novaalert web interface (not shown), navigate to **Monitoring → Activities** in the left column.



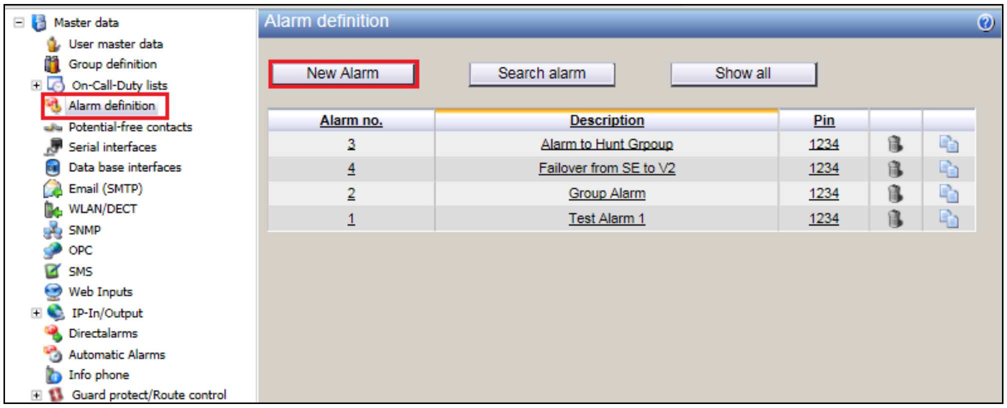
Verify that the icon in the left column is green indicating that the SIP trunks are in service and Session Manager can be reached.



●	▮▮	Line 1	Waiting for call!
●	▮▮	Line 2	Waiting for call!
●	▮▮	Line 3	Waiting for call!
●	▮▮	Line 4	Waiting for call!

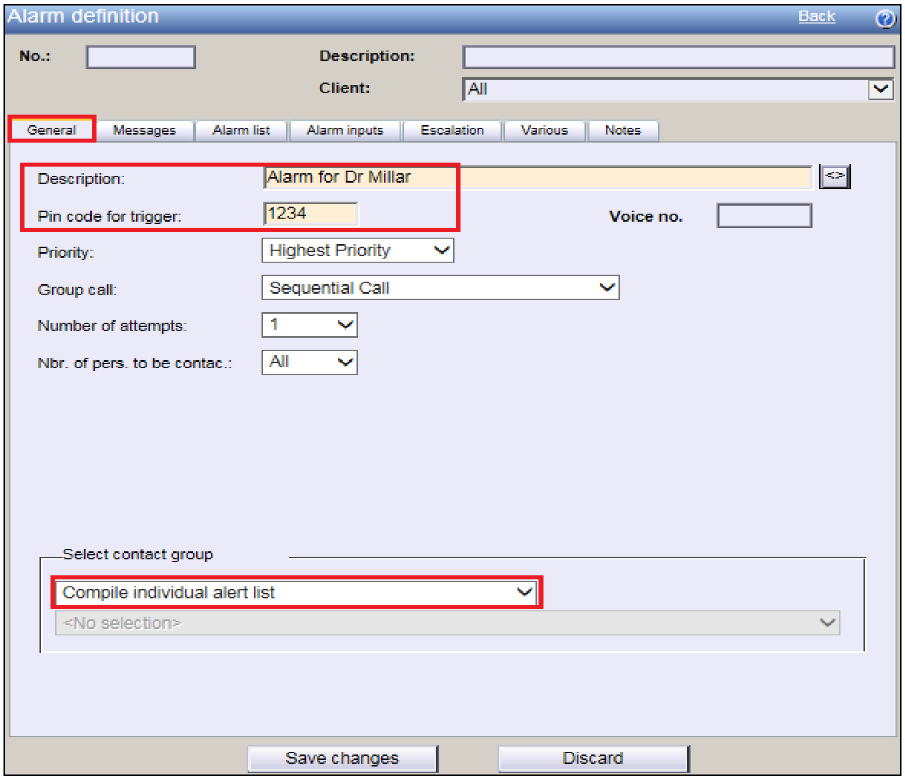
8.3. Create a new Alarm on novaalert

From the left column navigate to **Master data** → **Alarm definition** and from the main window, click on **New Alarm**, as shown below.



Alarm no.	Description	Pin
3	Alarm to Hunt Grpoup	1234
4	Failover from SE to V2	1234
2	Group Alarm	1234
1	Test Alarm 1	1234

In the **General** tab, enter a suitable **Description** and **Pin code for trigger** for the new alarm. Select **Compile individual alert list** from the **Select contact group** drop-down menu.



No.:

Description:

Client: All

Description: Alarm for Dr Millar

Pin code for trigger: 1234

Voice no.

Priority: Highest Priority

Group call: Sequential Call

Number of attempts: 1

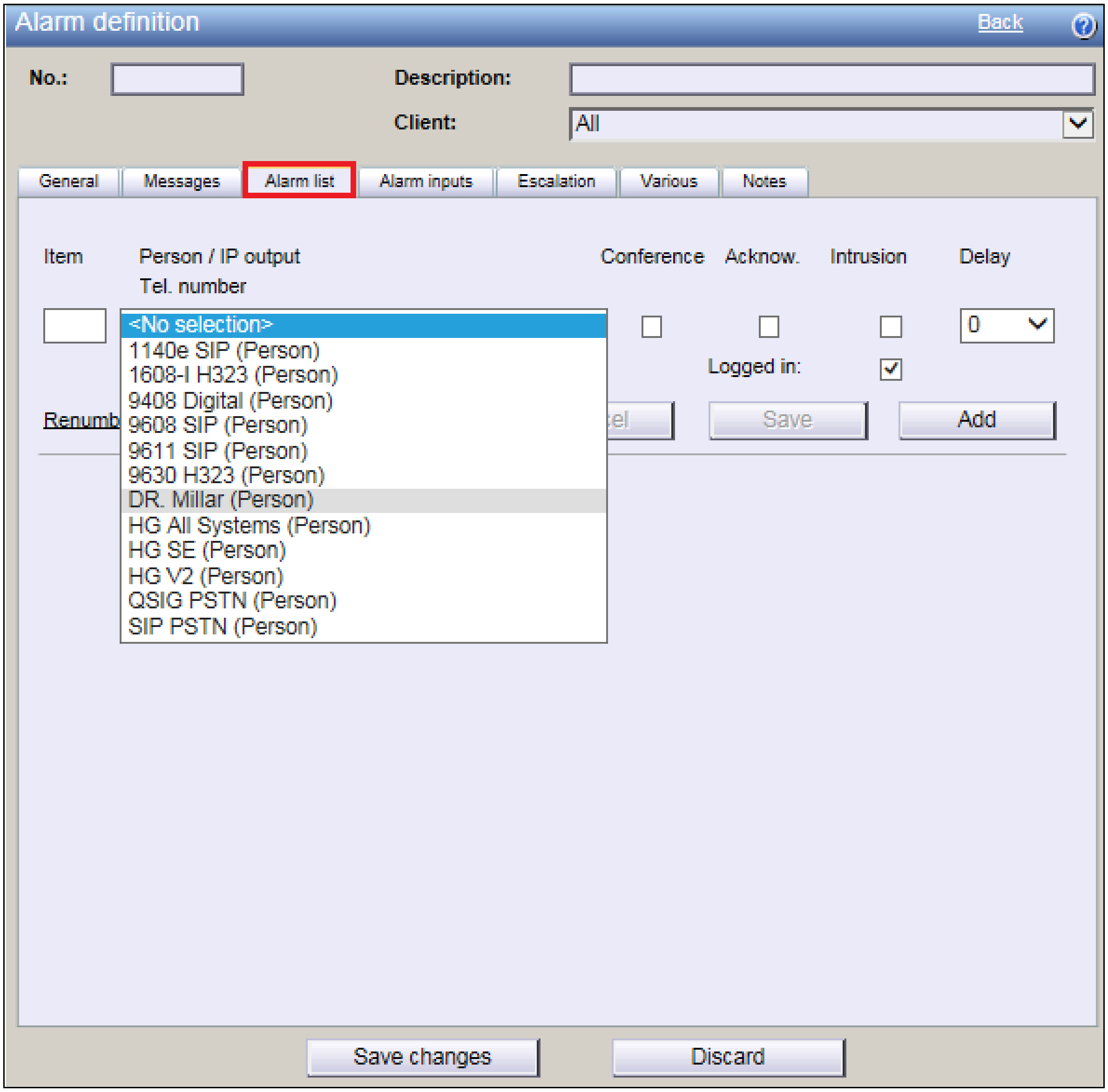
Nbr. of pers. to be contac.: All

Select contact group

Compile individual alert list

<No selection>

Click on the **Alarm list** tab and select the user that was created in **Section 6.2**.



No.:

Description:

Client: All

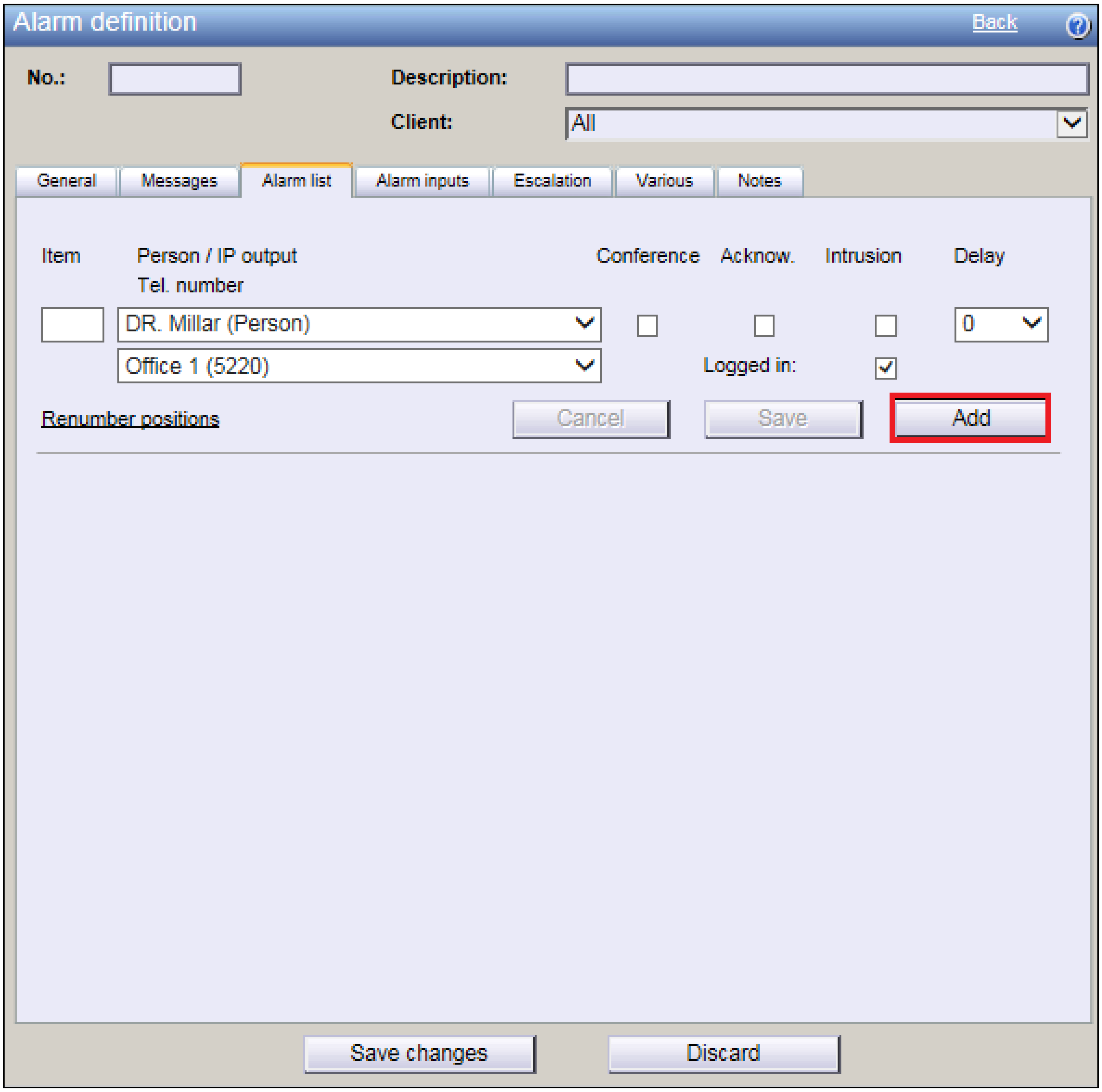
□ Conference □ Acknow. □ Intrusion Delay 0

Logged in: ☑

Person / IP output:

- <No selection>
- 1140e SIP (Person)
- 1608-I H323 (Person)
- 9408 Digital (Person)
- 9608 SIP (Person)
- 9611 SIP (Person)
- 9630 H323 (Person)
- DR. Millar (Person)
- HG All Systems (Person)
- HG SE (Person)
- HG V2 (Person)
- QSIG PSTN (Person)
- SIP PSTN (Person)

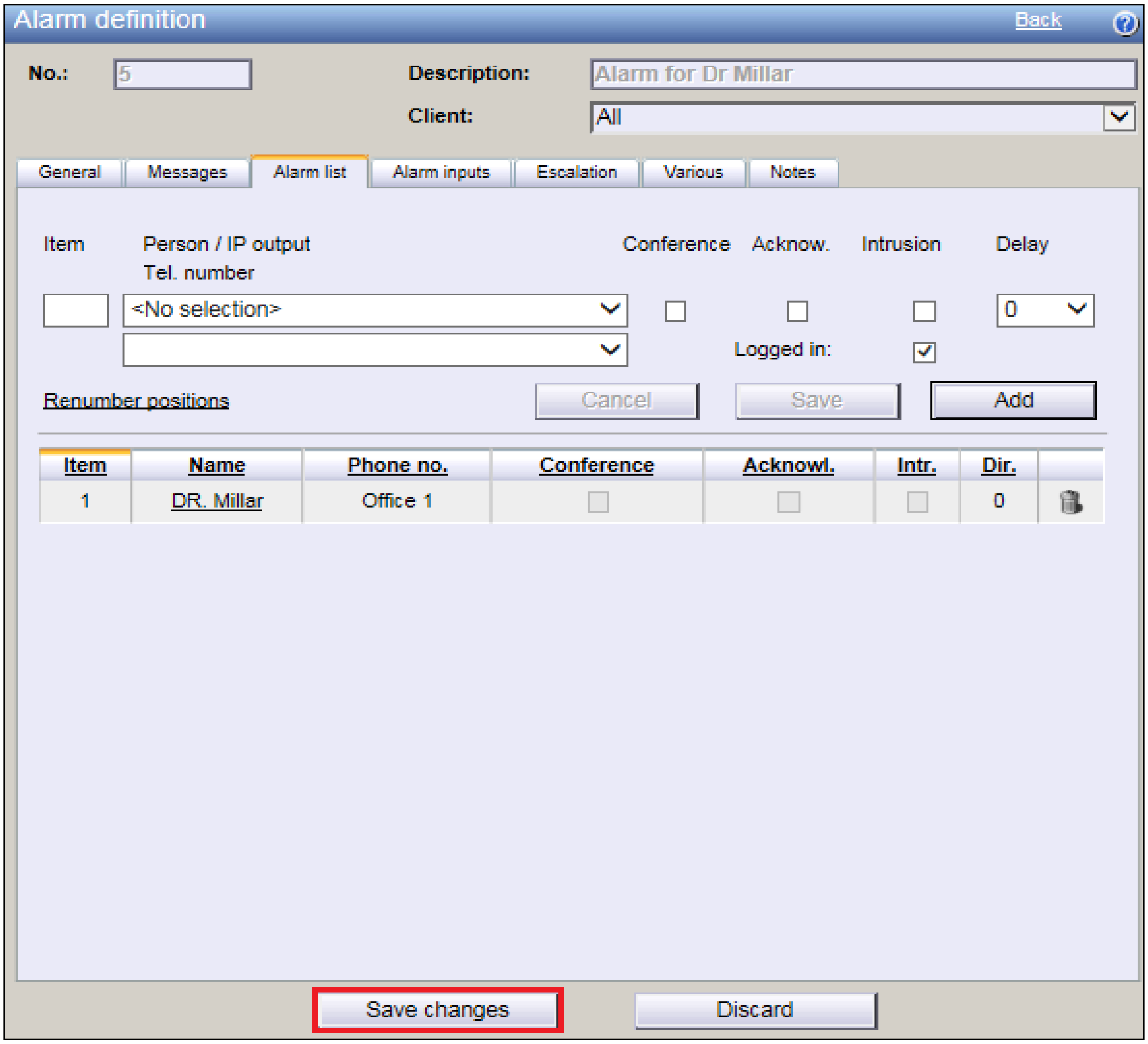
Once the **Person/IP output** has been correctly selected the **Tel. number** should also get populated automatically. Click on the **Add** button to add this new person.



No.:
Description:
Client: All

Item	Person / IP output Tel. number	Conference	Acknow.	Intrusion	Delay
	DR. Millar (Person)	□	□	□	0
	Office 1 (5220)		Logged in:	☑	

Click on **Save Changes** at the bottom of the screen.



Alarm definition

No.: 5

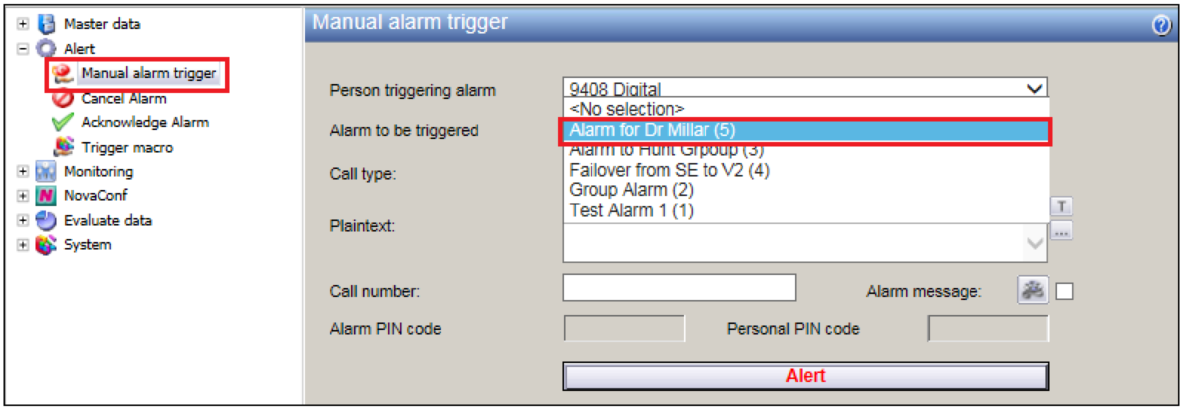
Description: Alarm for Dr Millar

Client: All

Item	Person / IP output Tel. number	Conference	Acknow.	Intrusion	Delay
	<No selection>	□	□	□	0
			Logged in:	☑	

Item	Name	Phone no.	Conference	Acknowl.	Intr.	Dir.	
1	DR. Millar	Office 1	□	□	□	0	

From the main menu, navigate to **Alert → Manual alarm trigger**. In the main window select the **Alarm to be triggered**, which should be the alarm created above.



Manual alarm trigger

Person triggering alarm: 9408 Digital

Alarm to be triggered: Alarm for Dr Millar (5)

Call type:

Plaintext:

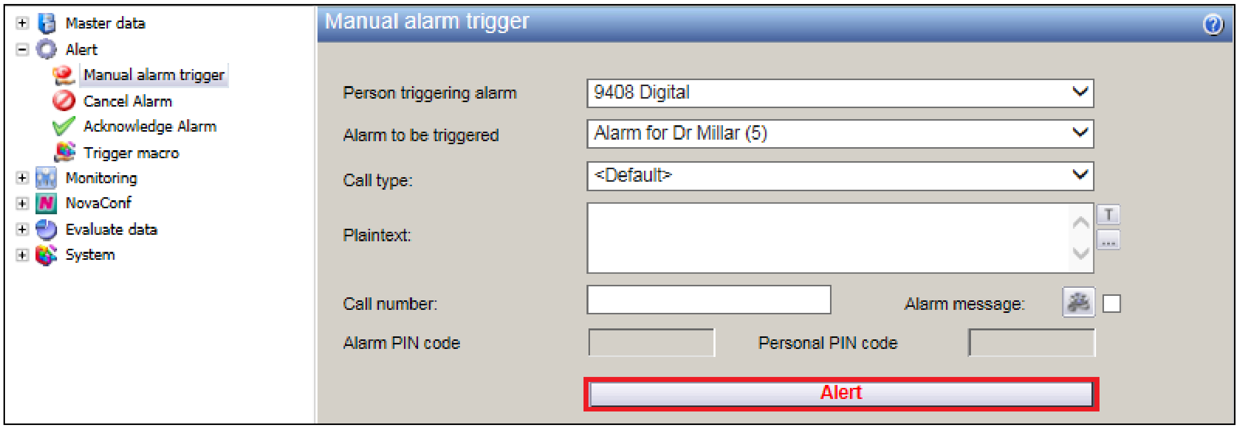
Call number:

Alarm message: □

Alarm PIN code

Personal PIN code

Click on the Alert button at the bottom of the screen.



Person triggering alarm: 9408 Digital

Alarm to be triggered: Alarm for Dr Millar (5)

Call type: <Default>

Plaintext:

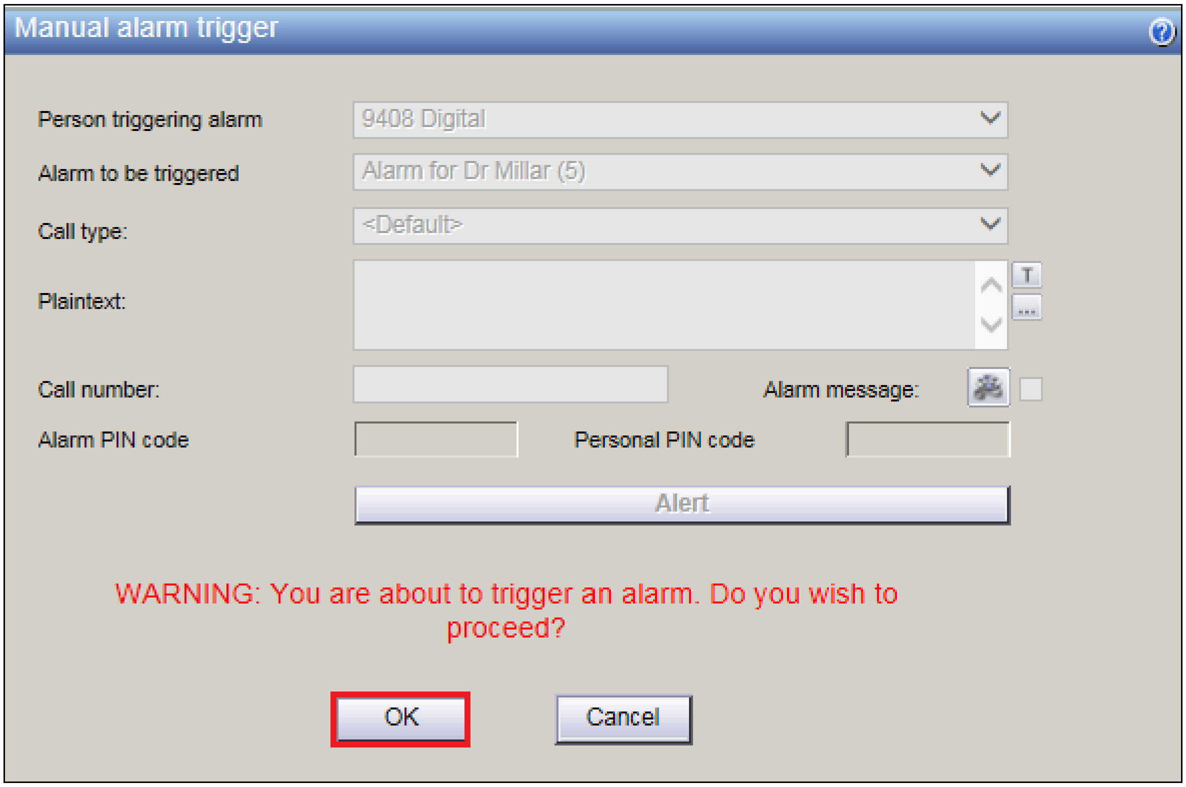
Call number:

Alarm message: □

Alarm PIN code

Personal PIN code

Click on **OK** to proceed.



Person triggering alarm: 9408 Digital

Alarm to be triggered: Alarm for Dr Millar (5)

Call type: <Default>

Plaintext:

Call number:

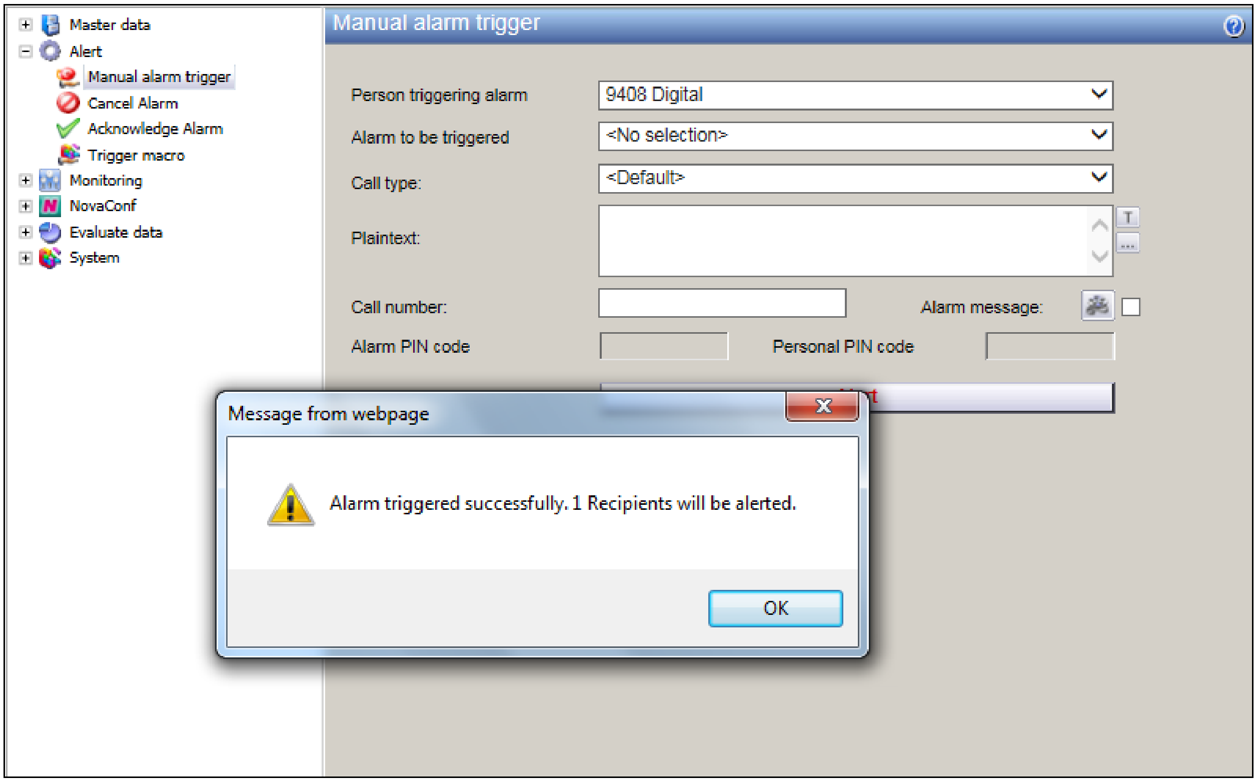
Alarm message: □

Alarm PIN code

Personal PIN code

WARNING: You are about to trigger an alarm. Do you wish to proceed?

The following screen should be displayed along with the telephone set ringing and an alarm message being played upon answer.



Person triggering alarm: 9408 Digital

Alarm to be triggered: <No selection>

Call type: <Default>

Plaintext:

Call number:

Alarm message: □

Alarm PIN code

Personal PIN code

Alarm triggered successfully. 1 Recipients will be alerted.

9. Conclusion

These Application Notes describe the configuration steps required for novaalert from novalink to successfully interoperate with Avaya Aura® Communication Manager. All feature test cases were completed successfully with any observations noted in **Section 2.2**.

10. Additional References

This section references documentation relevant to these Application Notes. The Avaya product documentation is available at http://support.avaya.com where the following documents can be obtained.

[1] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509

[2] *Avaya Aura® Communication Manager Feature Description and Implementation,* Document ID 555-245-205

[3] *Implementing Avaya Aura® Session Manager* Document ID 03-603473

[4] *Administering Avaya Aura® Session Manager*, Doc ID 03-603324

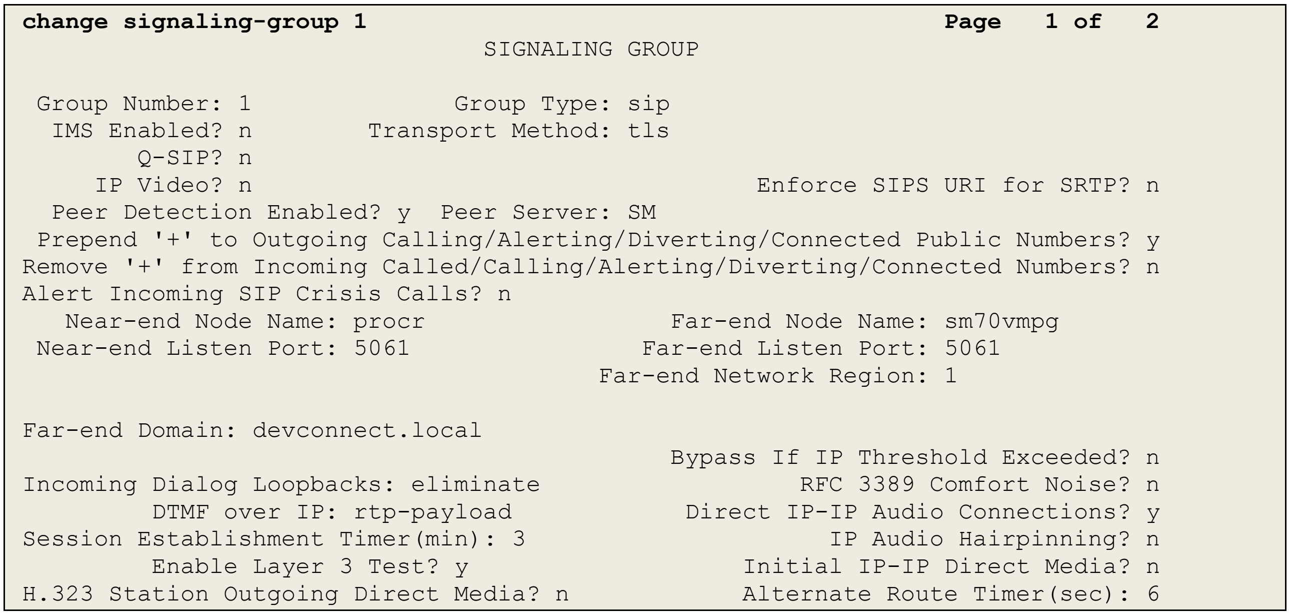
Technical support can be obtained for novaalert from the website http://www.novalink.ch/en/ or from ftp://support.novalink.ch/Technikerhandbuch/English/Technikerhandbuch novalink GmbH EN.chm (please request Login and Password from novalink).

Appendix

Configure SIP Trunk between Session Manager and Communication Manager

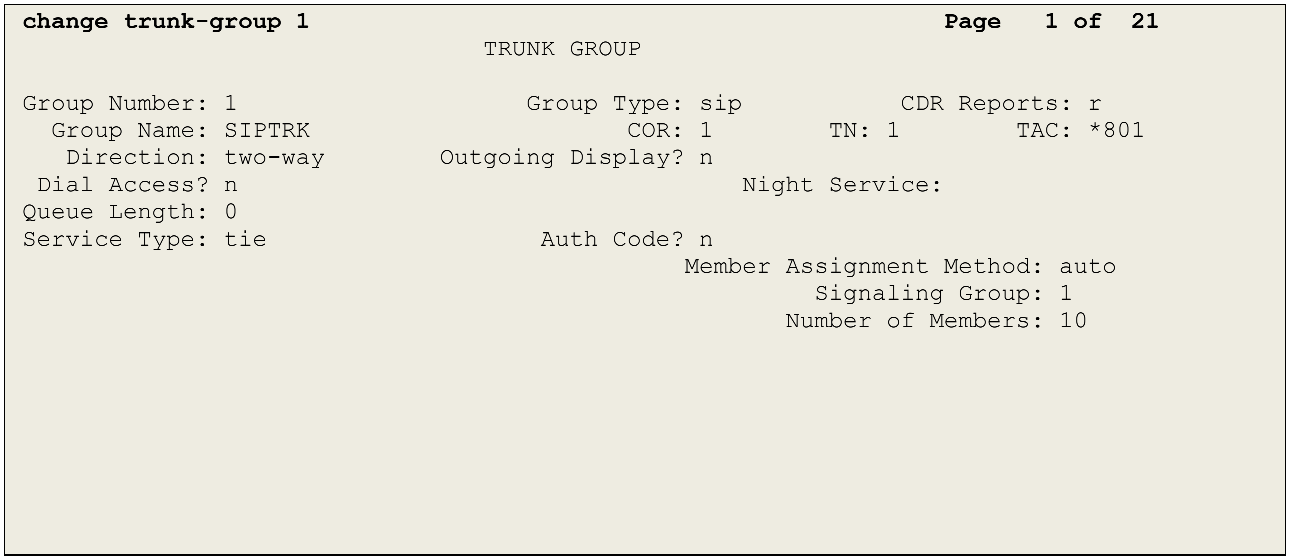
The following shows the SIP Signalling Group and SIP trunk that was used during compliance testing.

- Set the **Group Type** field to **sip**.
- For compliance testing **Transport Method** was set to **tls**.
- The **Peer Detection Enabled** field should be set to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager.
- Specify the node names for the procr and the Session Manager node name as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively.
- Set the **Near-end Node Name** to **procr**. Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **sm70vmpg**), as per **Section 5.5**.
- Ensure that the recommended TLS port value of **5061** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured in **Section 5.** This field logically establishes the **far-end** for calls using this signaling group as network region 1.
- **Far-end Domain** was set to the domain used during compliance testing.
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- The **Direct IP-IP Audio Connections** field is set to **y**.
- **Initial IP-IP Direct Media** was set to **N** for compliance testing.
- The default values for the other fields may be used.



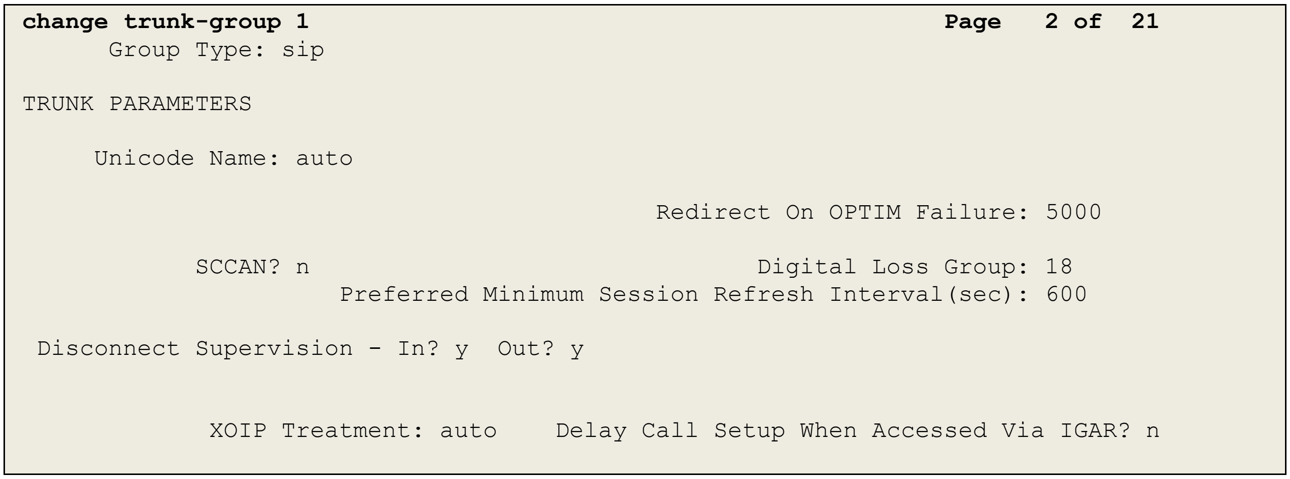
```
change signaling-group 1                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                     Far-end Node Name: sm70vmpg
 Near-end Listen Port: 5061                    Far-end Listen Port: 5061
                                        Far-end Network Region: 1

Far-end Domain: devconnect.local
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

Configure the Trunk Group form as shown below. This trunk group is used for calls to and from novaalert. Enter a descriptive name in the Group Name field. Set the Group Type field to sip. Enter a TAC code compatible with the Communication Manager dial plan. Set the Service Type field to tie. Specify the signaling group associated with this trunk group in the Signaling Group field, and specify the Number of Members supported by this SIP trunk group. Accept the default values for the remaining fields.



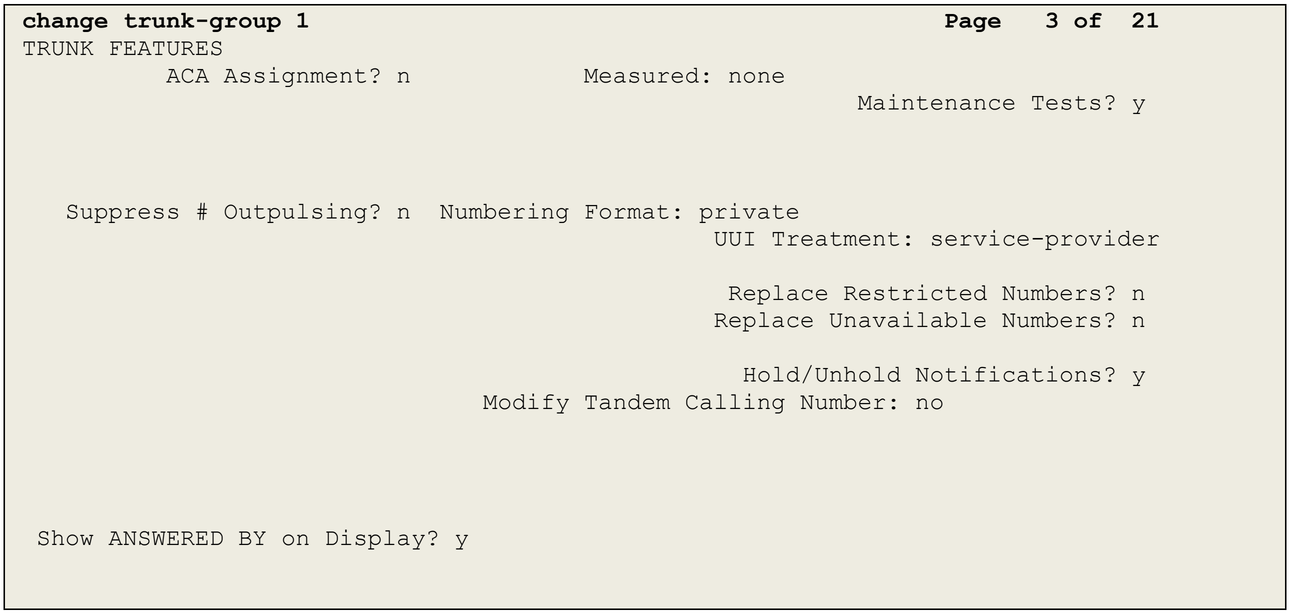
```
change trunk-group 1                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 1                    Group Type: sip           CDR Reports: r
  Group Name: SIPTRK                      COR: 1        TN: 1        TAC: *801
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 10
```

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with NEC to prevent unnecessary SIP messages during call setup. Session refresh is used throughout the duration of the call, to check the other side has not gone away, for the compliance test a value of **600** was used.



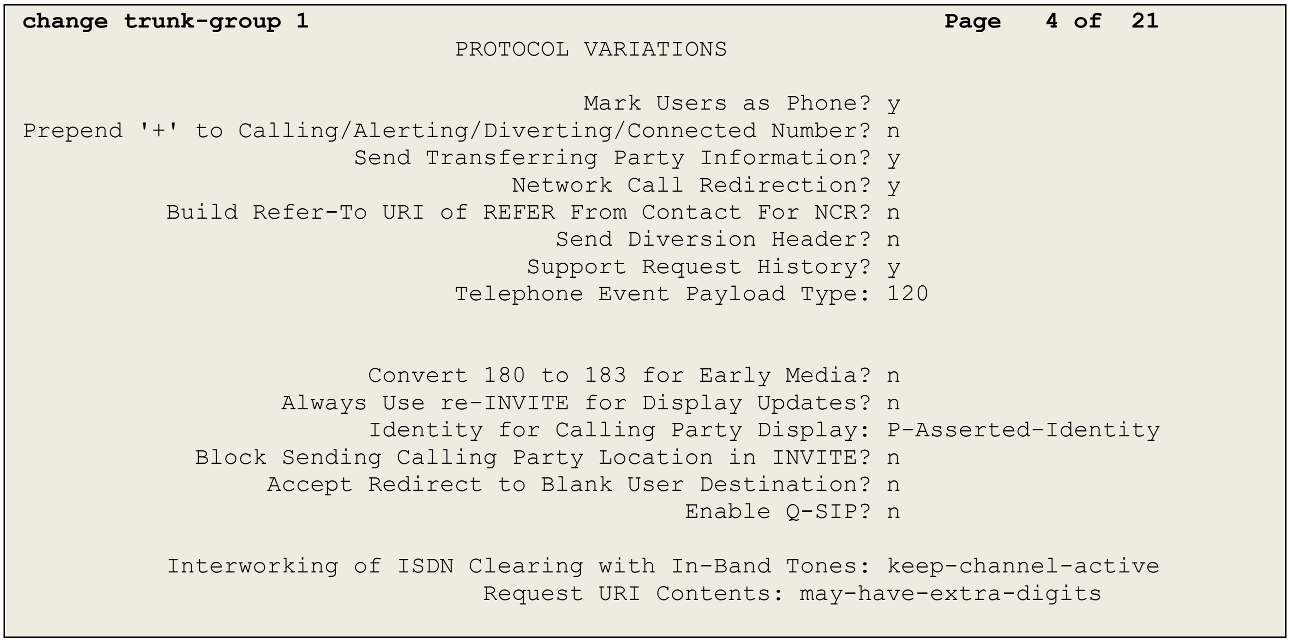
```
change trunk-group 1                                            Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 5000

            SCCAN? n                               Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 600

 Disconnect Supervision - In? y  Out? y


             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n
```

Settings on **Page 3** can be left as default. However the **Numbering Format** in the example below is set to **private**.



```
change trunk-group 1                                            Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



   Suppress # Outpulsing? n  Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n

                                                  Hold/Unhold Notifications? y
                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? y
```

Settings on **Page 4** are as follows.



```
change trunk-group 1                                            Page   4 of  21
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? y
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? y
                                  Network Call Redirection? y
          Build Refer-To URI of REFER From Contact For NCR? n
                                     Send Diversion Header? n
                                   Support Request History? y
                              Telephone Event Payload Type: 120


                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? n
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                              Enable Q-SIP? n

          Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
                                      Request URI Contents: may-have-extra-digits
```

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.