



Avaya Solution & Interoperability Test Lab

Application Notes for configuring novaalert v10.5 from novalink with Avaya Aura® Session Manager R10.1 and Avaya Aura® Communication Manager R10.1 – Issue 1.0

Abstract

These Application Notes describe the configuration for connecting novalink novaalert v10.5 via SIP trunks to Avaya Aura® Communication Manager R10.1 using Avaya Aura® Session Manager R10.1.

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, in the form of alert announcements, 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 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.

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. The focus of these Application Notes is for alarm triggering restricted to those methods which involve interaction with Communication Manager, that being alarms in the form of announcements being sent from novaalert to endpoints on Communication Manager, also using these endpoints to call into novaalert and record announcement messages to be sent out to other Communication Manager endpoints.

Alarms which are triggered via Communication Manager can include pre-recorded or ad hoc voice messages. 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 Remote Access feature on Communication Manager followed by the Service Observe feature 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 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.

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 Session Manager 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, DECT and softphone endpoints, listed in **Section 4**.

- 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 individual SIP/H.323/Digital endpoints
- 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
- Intrusion calls to deliver alarms on busy endpoints
- Verification of Calling Party Name
- Over-ride forwarding to deliver alarms
- Following forwarding to deliver alarms
- Alarms delivered to Voicemail
- DTMF PIN Entry to demonstrate permission verification to trigger alarms
- Serviceability testing consisted of verifying the ability of novaalert to recover from power or network interruption to both Session Manager and novaalert.

2.2. Test Results

All test cases were executed successfully. With the exception of the following issue noted.

1. There is an issue with messages being displayed on the H323 and Digital phones when less than the maximum number of characters are being sent by novaalert. The SIP messaging (traceSM) shows that the characters are being sent to CM and received by CM (in the FROM, CONTACT and PAI headers) but for some reason the phoneset is not displaying them unless all characters are being used. This does not appear to be the case for SIP phones. Avaya are investigating the issue.
2. DECT phones (3720 and 3725) were used to receive alarm messages via announcement, no messages were displayed on the DECT handsets and no AIWS was present to test any SMS messages being received by the DECT handsets.
3. Remote Access on Communication Manager is used to allow Call Intrusion to work using the Service Observe Feature Access Code, this is to allow the Feature Access Code to be used by novaalert via the SIP Trunk.

2.3. Support

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

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

3. Reference Configuration

The configuration in **Figure 1** is used to compliance test novaalert with Communication Manager, having novaalert register with Session Manager as a third-party SIP entity. Alarms/Alerts are received from novaalert over SIP trunks. Alarms may be triggered directly on the novaalert GUI or from a call into novaalert via SIP trunk. These alarms are configured to be sent to individual endpoints or a group of endpoints on the Avaya PBX.

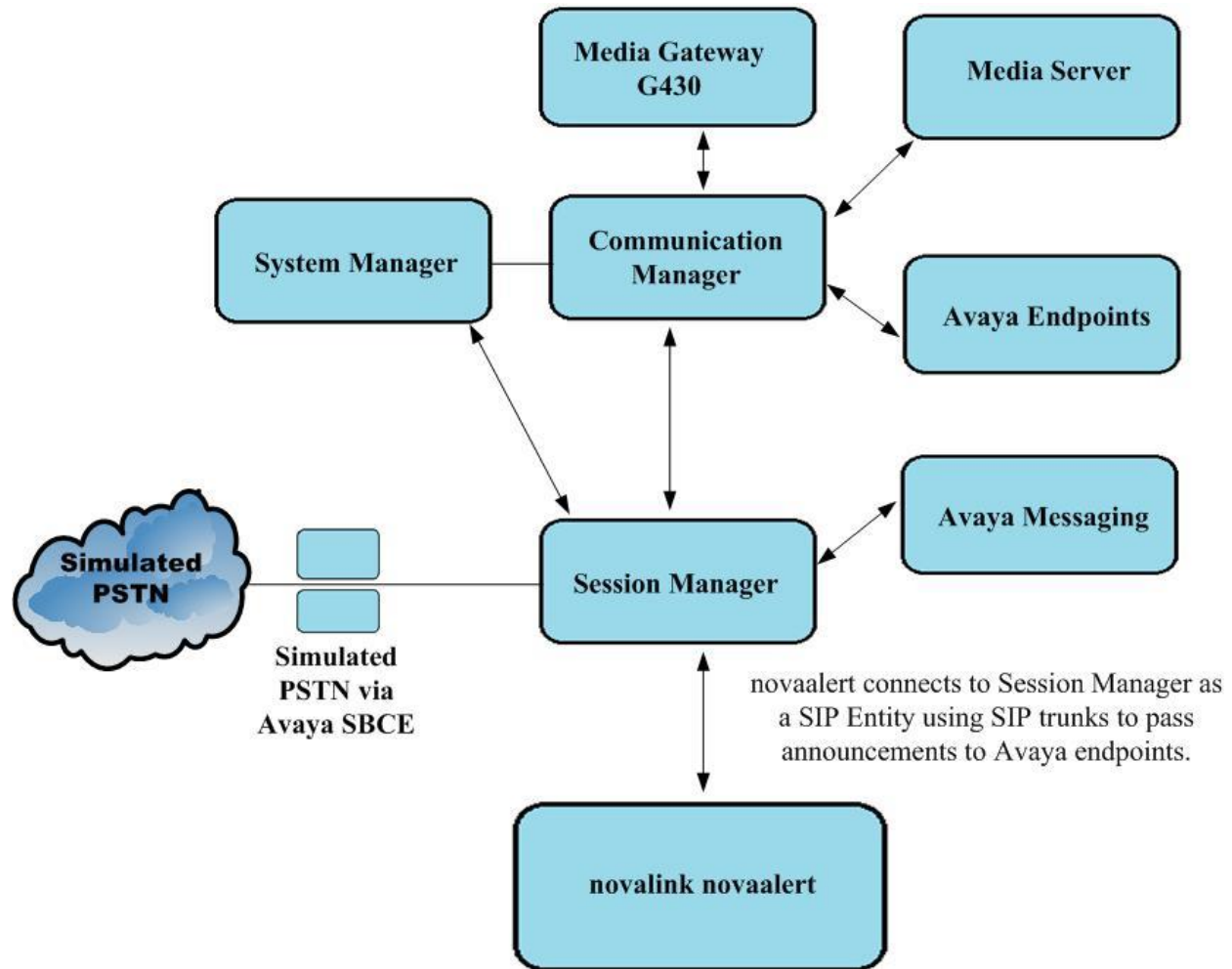


Figure 1: Connection of novaalert from novalink with Avaya Aura® Communication Manager and Avaya Aura® Session Manager

4. Equipment and Software Validated

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

Avaya Equipment	Software / Firmware Version
Avaya Aura® System Manager running on a virtual server	10.1.0.0 Build No. – 10.1.0.0.537353 SW Update Revision No: 10.1.0.0.0614254
Avaya Aura® Session Manager running on a virtual server	10.1 Build No. – 10.1.0.0.1010019
Avaya Aura® Communication Manager running on a virtual server	10.1 Update ID 01.0.974.0-27293
Avaya Messaging running on MS Windows Server 2019	10.8.20.1502
Avaya Session Border Controller for Enterprise	8.1.1.0-26-19214
Avaya G430 Media Gateway	41.16.0/1
Avaya J179 H.323 Deskphone	6.8304
Avaya J159 SIP Deskphone	4.0.7.1.5
Avaya 9408 Digital Phone	2.00
Avaya Workplace for Windows	3.26.0.64
Avaya DECT Base Station Avaya DECT handsets 3720 & 3725	IPBS2 10.0.6 4.3.13
novalink novaalert running on a Windows 2019 virtual server	10.5.0.9

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 1111**.

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

- Verify System Parameters
- Configure Network Region and IP Codec
- Configure Routing to novaalert
- Configure Remote Access

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

5.1. Verify System Parameters

Various system wide parameters can be checked to ensure that the setup is the same as that which was used for compliance testing as well as give some focus as to what parameters needed to be set.

5.1.1. Check 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 12
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		12000	10
Maximum Concurrently Registered IP Stations:		2400	1
Maximum Administered Remote Office Trunks:		12000	0
Max Concurrently Registered Remote Office Stations:		2400	0
Maximum Concurrently Registered IP eCons:		128	0
Max Concur Reg Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		36000	0
Maximum Video Capable IP Softphones:		150	1
Maximum Administered SIP Trunks:		12000	45
Max Administered Ad-hoc Video Conferencing Ports:		12000	0
Max Number of DS1 Boards with Echo Cancellation:		688	0

5.1.2. Check System Features

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 11** 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
```

5.1.3. Check Feature Access Codes

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 12
                        FEATURE ACCESS CODE (FAC)
                        Abbreviated Dialing List1 Access Code: *11
                        Abbreviated Dialing List2 Access Code: *12
                        Abbreviated Dialing List3 Access Code: *13
                        Abbreviated Dial - Prgm Group List Access Code: *10
                        Announcement Access Code: *27
                        Answer Back Access Code: #02
                        Attendant Access Code:
                        Auto Alternate Routing (AAR) Access Code: 8
                        Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2:
                        Automatic Callback Activation: *05      Deactivation: #05
                        Call Forwarding Activation Busy/DA: *03      All: *04      Deactivation: #04
                        Call Forwarding Enhanced Status: *73      Act: *74      Deactivation: #74
                        Call Park Access Code: *02
                        Call Pickup Access Code: *09
                        CAS Remote Hold/Answer Hold-Unhold Access Code:
                        CDR Account Code Access Code: *14
                        Change COR Access Code:
                        Change Coverage Access Code:
```


On **Page 5**, note the **Service Observing Listen/Talk Access Code**, this will be used again in **Section 7**.

display feature-access-codes	Page 5 of 12
FEATURE ACCESS CODE (FAC)	
Call Center Features	
AGENT WORK MODES	
After Call Work Access Code: *51	
Assist Access Code: *55	
Auto-In Access Code: *52	
Aux Work Access Code: *53	
Login Access Code: *50	
Logout Access Code: #50	
Manual-in Access Code: *54	
SERVICE OBSERVING	
Service Observing Listen Only Access Code: *56	
Service Observing Listen/Talk Access Code: *57	
Service Observing No Talk Access Code: #57	
Service Observing Next Call Listen Only Access Code:	
Service Observing by Location Listen Only Access Code:	
Service Observing by Location Listen/Talk Access Code:	
AACC CONFERENCE MODES	
Restrict First Consult Activation:	Deactivation:
Restrict Second Consult Activation:	Deactivation:

5.2. Configure Network Region and IP Codec

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager in **Section 6.1**. In this configuration, the domain name is **greaney.sil6.avaya.com**. The **IP Network Region** form also specifies the **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 in the **Appendix**.

```
display ip-network-region 1                                     Page 1 of 20
IP NETWORK REGION
Region: 1              NR Group: 1
Location:              Authoritative Domain: greaney.sil6.avaya.com
Name: PGDefault        Stub Network Region: n
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
                      Inter-region IP-IP Direct Audio: yes
                      IP Audio Hairpinning? n
Codec Set: 1
UDP Port Min: 2048
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
H.323 IP ENDPOINTS    AUDIO RESOURCE RESERVATION PARAMETERS
                      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 codecs 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 on the previous page. 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 one of the entries for **Media Encryption** has been set to **none**, this allows the media to be unencrypted between novaalert and Communication Manager. Avaya uses Media Encryption as a preferred option between endpoints.

change ip-codec-set 1

Page 1 of 2

IP MEDIA PARAMETERS

Codec Set: 1

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

Media Encryption

Encrypted SRTCP: best-effort

1: 1-srtp-aescm128-hmac80
2: none
3:
4:
5:

5.3. Configure routing to novaalert

It was decided for compliance testing that all calls beginning with 32 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 uniform dialplan and aar routing analysis need to be changed to allow this.

Below shows the dialplan that was used for compliance testing. Type **display dialplan analysis** to observe the dial plan.

display dialplan analysis						Page 1 of 12					
DIAL PLAN ANALYSIS TABLE											
Location: all						Percent Full: 2					
	Dialed String	Total Length	Call Type		Dialed String	Total Length	Call Type		Dialed String	Total Length	Call Type
1		4	udp								
2		4	udp								
3		4	ext								
4		4	ext								
5		4	udp								
666		4	ext								
8		1	fac								
9		1	fac								
*		3	fac								
*8		4	dac								
#		3	fac								

Use the **change uniform-dialplan x** command to configure the routing of the dialed digits. In the example below calls to numbers beginning with **32** 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 3						Page 1 of 2
UNIFORM DIAL PLAN TABLE						
						Percent Full: 0
Matching			Insert		Node	
Pattern	Len	Del	Digits	Net Conv	Num	
32	4	0		aar n		
5	4	0		aar n		
666	4	0		aar n		
				n		
				n		
				n		
				n		
				n		
				n		

Use the **change aar analysis x** command to further configure the routing of the dialed digits. Calls to novaalert begin with **32** 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 3						Page 1 of 2
AAR DIGIT ANALYSIS TABLE						
Location: all						Percent Full: 1
Dialed String	Total Min	Max	Route Pattern	Call Type	Node Num	ANI Reqd
31	4	4	11	lev0		n
32	4	4	1	aar		n
4	7	7	999	aar		n
5	4	4	1	aar		n
666	4	4	66	aar		n
7	7	7	999	aar		n
8	7	7	999	aar		n
9	7	7	999	aar		n
						n
						n
						n
						n
						n
						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 the **Appendix**.

change route-pattern 1										Page 1 of 4
Pattern Number: 1 Pattern Name: SIP TRK IN-OUT										
SCCAN? n Secure SIP? n Used for SIP stations? n										
Grp No	FRL	NPA	Pfx	Hop	Toll	No.	Inserted			DCS/ IXC
				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 Sub Numbering LAR										
	0	1	2	M	4	W	Request	Dgts	Format	
1:	y	y	y	y	y	n	n	unre	lev0-pvt	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

5.4. Configure Remote Access

To allow novaalert to use the Feature Access Code for Service Observe (*57), the remote-access feature on Communication Manager needs to be configured with an extension number. Type **change remote-access**, to assign the **Remote Access Extension** as shown below, this will be used again in **Section 7.2**.

change remote-access				Page 1 of 1			
REMOTE ACCESS							
Remote Access Extension: 3150				Barrier Code Length:			
Authorization Code Required? n							
	Barrier Code	COR	TN	COS	Expiration Date	No. of Calls	Calls Used
1:	none						
2:							
3:							
4:							
5:							
6:							
7:							
8:							
9:							
10:							
Permanently Disable? n							
(NOTE: You must logoff to effect permanent disabling of Remote Access)							

6. Configure Avaya Aura® Session Manager

To make changes in Session Manager, a web session to System Manager is opened. Navigate to <https://<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:

Password:

[Change Password](#)

Supported Browsers: Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0).

6.1. Configuration of a Domain

Click on **Routing** highlighted below.

AVAYA Aura® System Manager 10.1

Users Elements Services Widgets Shortcuts

Search admin

Disk Space Utilization

Alarms

Notifications (2)

Application State

Information

Shortcuts

Elements

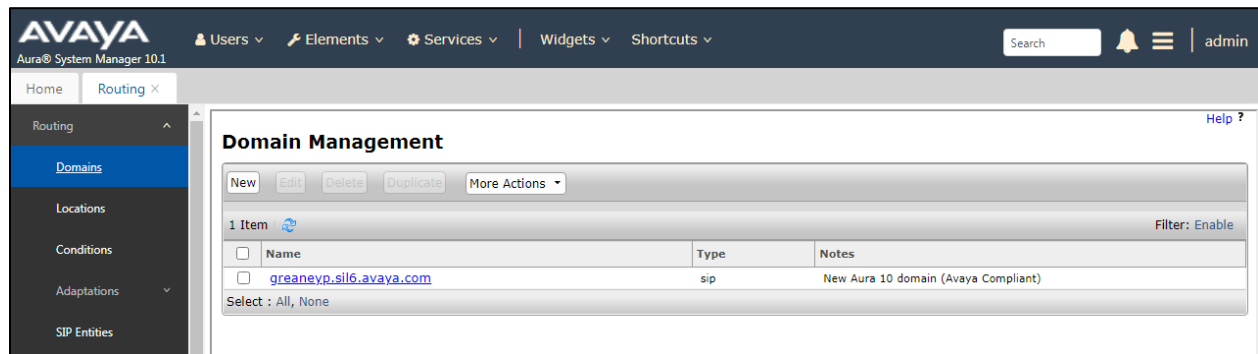
- Avaya Breeze®
- Communication Manager
- Communication Server 1000
- Device Adapter
- Device Services
- IP Office
- Media Server
- Meeting Exchange
- Messaging
- Presence
- Routing**
- Session Manager
- Web Gateway

Current Usage:

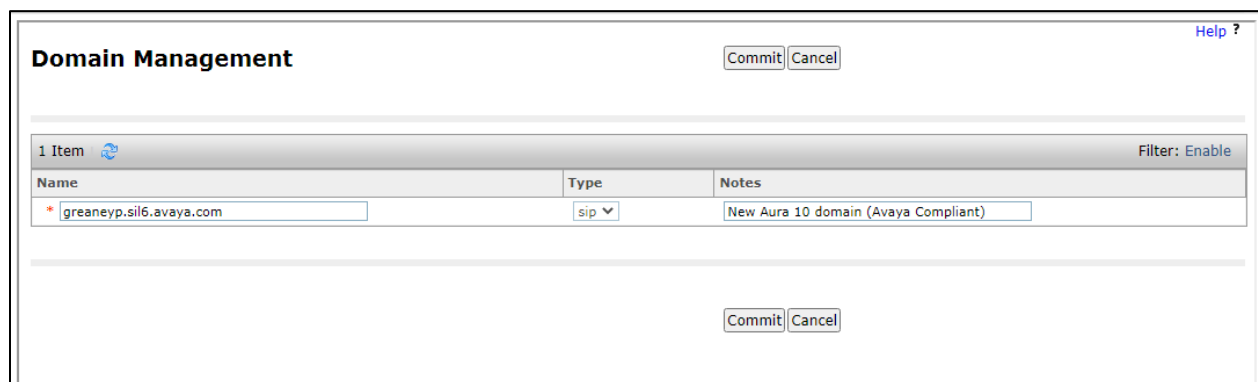
7/250000 USERS

1/50

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 **greanep.sil6.avaya.com** which has already been configured.

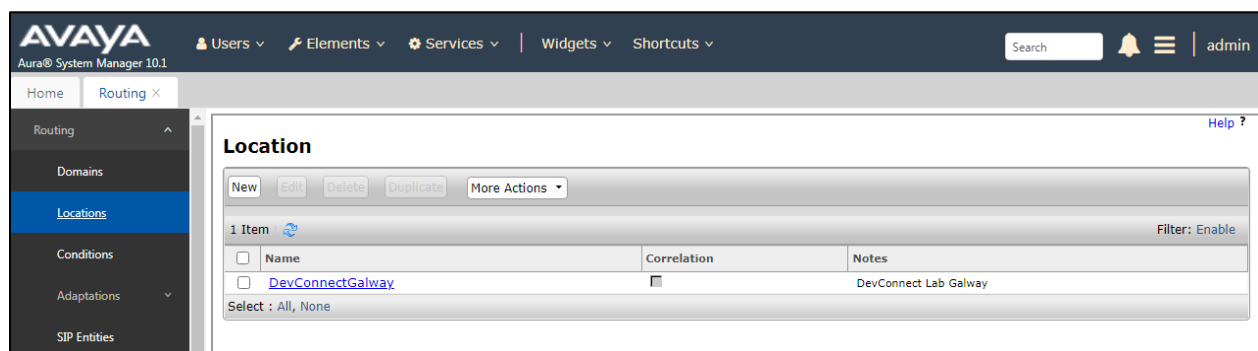


Clicking on the domain name above will open the window below, this is simply to show an example of such a domain. When entering a new domain, the following should be entered. Once the domain name is entered, click on **Commit** to save this.



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 **DevConnectGalway** is already setup and configured and clicking into this will show its contents.



The Location below shows a suitable **Name** with a **Location Pattern** of **10.10.40.*** and **10.10.41.***. Once this is configured, click on **Commit**.

Location Details

CommitCancel

Help?

General

* Name: DevConnectGalway

Notes: DevConnect Lab Galway

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

AddRemove

2 Items

Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.10.40.*	Main Subnet
<input type="checkbox"/>	* 10.10.41.*	Secondary Subnet

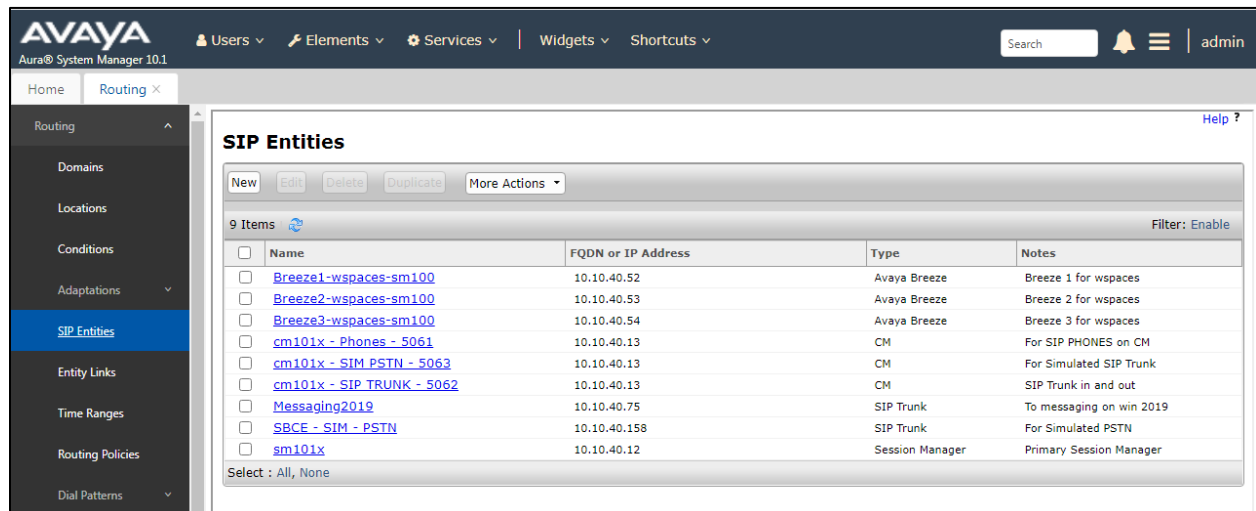
PG; Reviewed:
SPOC 8/18/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

17 of 49
novaalertCM101

6.3. Configuration of SIP Entity

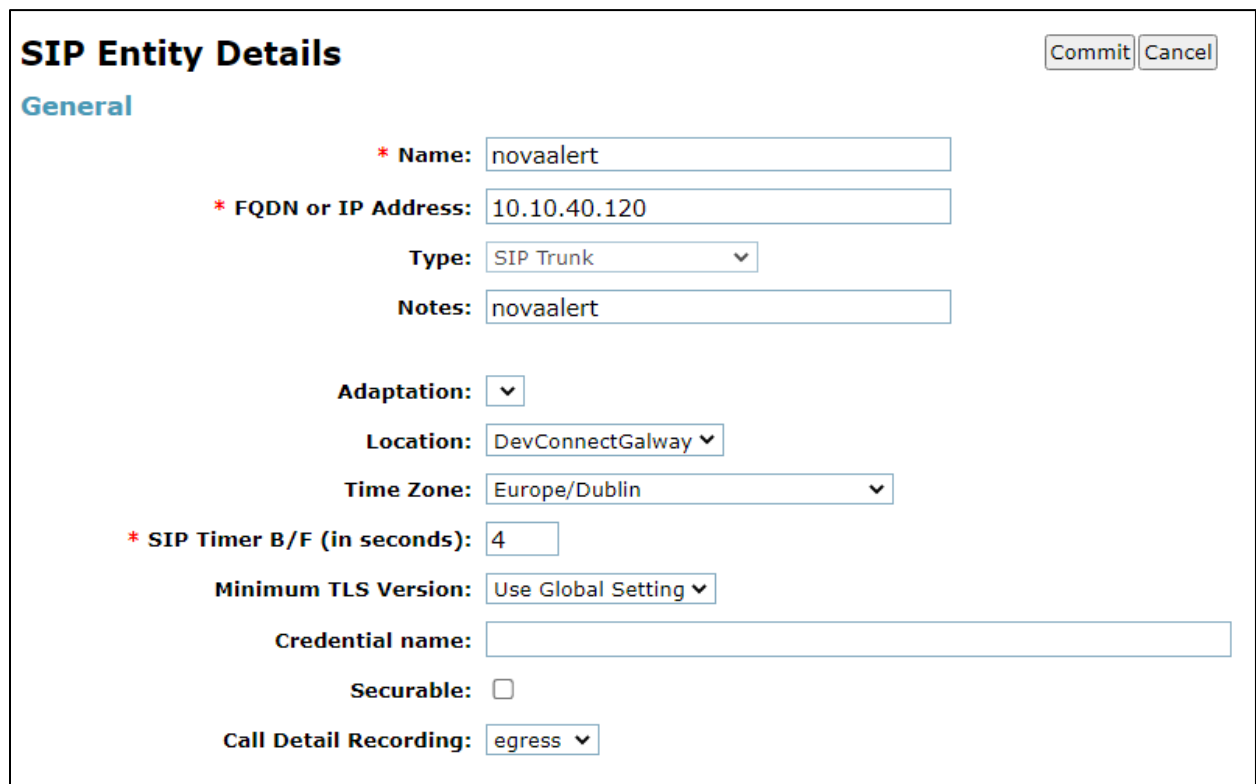
Clicking on **SIP Entities** in the left window shows what SIP Entities have been added to the system and allows the addition of any new SIP Entity that may be required. Please note that both the Communication Manager and Session Manager SIP Entities were already present for the compliance testing of novaalert. To add a SIP entity, click on **New**.



The screenshot shows the Avaya Aura System Manager 10.1 interface. The left sidebar contains a navigation menu with options: Home, Routing, Domains, Locations, Conditions, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, and Dial Patterns. The main content area displays the 'SIP Entities' page with a table of 9 items. The table has columns for Name, FQDN or IP Address, Type, and Notes. The entities listed are:

Name	FQDN or IP Address	Type	Notes
Breeze1-wspaces-sm100	10.10.40.52	Avaya Breeze	Breeze 1 for wspaces
Breeze2-wspaces-sm100	10.10.40.53	Avaya Breeze	Breeze 2 for wspaces
Breeze3-wspaces-sm100	10.10.40.54	Avaya Breeze	Breeze 3 for wspaces
cm101x - Phones - 5061	10.10.40.13	CM	For SIP PHONES on CM
cm101x - SIM PSTN - 5063	10.10.40.13	CM	For Simulated SIP Trunk
cm101x - SIP TRUNK - 5062	10.10.40.13	CM	SIP Trunk in and out
Messaging2019	10.10.40.75	SIP Trunk	To messaging on win 2019
SBCE - SIM - PSTN	10.10.40.158	SIP Trunk	For Simulated PSTN
sm101x	10.10.40.12	Session Manager	Primary Session Manager

Enter a suitable **Name** as well as the **IP Address** of novaalert. Select **SIP Trunk** as the **Type**. Scroll down to Entity Links.



The screenshot shows the 'SIP Entity Details' form. The 'General' tab is selected. The form contains the following fields:

- Name:** novaalert
- FQDN or IP Address:** 10.10.40.120
- Type:** SIP Trunk
- Notes:** novaalert
- Adaptation:** (dropdown menu)
- Location:** DevConnectGalway
- Time Zone:** Europe/Dublin
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (text input field)
- Securable:** (checkbox, unchecked)
- Call Detail Recording:** egress

An Entity Link between novaalert and Session Manager is required, scroll down and to the **Entity Links** section and click on **Add**.

Monitoring

SIP Link Monitoring:

CRLF Keep Alive Monitoring:

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐


Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

Entity Links

Override Port & Transport with DNS SRV: ☐


Add Remove

0 Items  Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
--------------------------	------	--------------	----------	------	--------------	------	-------------------	------------------

SIP Responses to an OPTIONS Request

Add Remove

0 Items  Filter: Enable


<input type="checkbox"/>	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
--------------------------	-------------------------------	---------------------	-------

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.

Entity Links

Override Port & Transport with DNS SRV: ☐

Add Remove

1 Item  Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	* sm101x_novaalert_5060	sm101x	UDP	* 5060	novaalert	* 5060	trusted

Select : All, None

6.4. Configure Routing Policy for novaalert

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

The screenshot shows the Avaya Aura System Manager 10.1 interface. The left sidebar contains a menu with 'Routing' selected. The main content area is titled 'Routing Policies' and shows a list of 7 items. The list has columns for Name, Disabled, Retries, and Destination. The items are:

<input type="checkbox"/>	Name	Disabled	Retries	Destination
<input type="checkbox"/>	To cm101x - SIM PSTN	<input type="checkbox"/>	0	cm101x - SIM PSTN - 5063
<input type="checkbox"/>	To cm101x - SIP Phones	<input type="checkbox"/>	0	cm101x - Phones - 5061
<input type="checkbox"/>	To cm101x - SIP Trunk	<input type="checkbox"/>	0	cm101x - SIP TRUNK - 5062
<input type="checkbox"/>	To IP Office SE	<input type="checkbox"/>	0	IP Office - SE

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

The screenshot shows the 'Routing Policy Details' form in the Avaya Aura System Manager 10.1 interface. The form has a 'General' section and a 'SIP Entity as Destination' section. The 'General' section contains fields for Name, Disabled, Retries, and Notes. The 'SIP Entity as Destination' section contains a 'Select' button and a table with columns for Name, FQDN or IP Address, Type, and Notes. The 'Time of Day' section contains a table with columns for Ranking, Name, Mon, Tue, Wed, Thu, Fri, Sat, Sun, Start Time, End Time, and Notes.

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes

Time of Day

Add Remove View Gaps/Overlaps

1 Item

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select the **novalert** SIP Entity created in **Section 6.3** and click on **Select** when done.

SIP Entities Select Cancel				
SIP Entities				
10 Items Filter: Enable				
	Name	FQDN or IP Address	Type	Notes
<input type="radio"/>	Breeze1-wspaces-sm100	10.10.40.52	Avaya Breeze	Breeze 1 for wspaces
<input type="radio"/>	Breeze2-wspaces-sm100	10.10.40.53	Avaya Breeze	Breeze 2 for wspaces
<input type="radio"/>	Breeze3-wspaces-sm100	10.10.40.54	Avaya Breeze	Breeze 3 for wspaces
<input type="radio"/>	cm101x - Phones - 5061	10.10.40.13	CM	For SIP PHONES on CM
<input type="radio"/>	cm101x - SIM PSTN - 5063	10.10.40.13	CM	For Simulated SIP Trunk
<input type="radio"/>	cm101x - SIP TRUNK - 5062	10.10.40.13	CM	SIP Trunk in and out
<input type="radio"/>	IP Office - SE	10.10.40.19	SIP Trunk	IP Office Server Edition
<input type="radio"/>	Messaging2019	10.10.40.75	SIP Trunk	To messaging on win 2019
<input checked="" type="radio"/>	novalert	10.10.40.120	SIP Trunk	novalert
<input type="radio"/>	SBCE - SIM - PSTN	10.10.40.158	SIP Trunk	For Simulated PSTN
Select : None				

The following Routing Policy can then be saved by clicking on **Commit**.

AVAYA

Users
Elements
Services
Widgets
Shortcuts

Search

admin

Home

Session Manager

Routing

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Routing Policy Details

Commit Cancel

General

Name: To NovaAlert

Disabled: ☐

Retries: 0

Notes: To NovaAlert

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
novalert	10.10.40.120	SIP Trunk	novalert

Time of Day

Add Remove View Gaps/Overlaps

1 Item

Filter: Enable

6.5. Configure Dial Pattern for novalink

To route calls to 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.

Note: As part of the initial installation of the Aura platform, 3 was added as a dial pattern to ensure that all calls beginning with 3 were routed to Communication Manager. Similarly with 3539173 and 3539184 below, these are for calls routed to the PSTN.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar shows a tree view with 'Routing' selected, containing 'Domains', 'Locations', 'Conditions', 'Adaptations', 'SIP Entities', and 'Entity Links'. The main content area is titled 'Dial Patterns' and features a table with 6 items. The table columns are: Pattern, Min, Max, Emergency Call, Emergency Type, and Emergency Priority. The rows show patterns 3, 3201, 3539173, 3539184, 5, and 6667, all with Min and Max values of 4 or 11, and Emergency Call checkboxes.

Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority
3	4	4	<input type="checkbox"/>		
3201	4	4	<input type="checkbox"/>		
3539173	11	11	<input type="checkbox"/>		
3539184	11	11	<input type="checkbox"/>		
5	4	4	<input type="checkbox"/>		
6667	4	4	<input type="checkbox"/>		

Enter the number to be routed, noting this will be the same number outlined in **Section 5.3**. Note the **SIP Domain** is that configured in **Section 6.1**. Click on **Add** to select the SIP Entity.

The screenshot shows the 'Dial Pattern Details' form. The 'General' tab is active, showing fields for Pattern (3201), Min (4), Max (4), Emergency Call (unchecked), SIP Domain (greaney.sil6.avaya.com), and Notes (To NovaAlert). The 'Originating Locations and Routing Policies' section shows a table with 1 item, containing columns for Originating Location Name, Originating Location Notes, Routing Policy Name, Rank, Routing Policy Disabled, Routing Policy Destination, and Routing Policy Notes. The table is currently empty, and the 'Add' button is visible.

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.

Originating Location

☐ Apply The Selected Routing Policies to All Originating Locations

1 Item		Filter: Enable
<input checked="" type="checkbox"/>	Name	Notes
<input checked="" type="checkbox"/>	DevConnectGalway	DevConnect Lab Galway

Select : All, None

Routing Policies

7 Items					Filter: Enable
<input type="checkbox"/>	Name	Disabled	Destination	Notes	
<input type="checkbox"/>	To cm101x - SIM PSTN	<input type="checkbox"/>	cm101x - SIM PSTN - 5063	Calls from SIM PSTN	
<input type="checkbox"/>	To cm101x - SIP Phones	<input type="checkbox"/>	cm101x - Phones - 5061	Route to CM101x - SIP Phones	
<input type="checkbox"/>	To cm101x - SIP Trunk	<input type="checkbox"/>	cm101x - SIP TRUNK - 5062	Route to CM101x - SIP Trunk	
<input type="checkbox"/>	To IP Office SE	<input type="checkbox"/>	IP Office - SE	To IP Office SE	
<input type="checkbox"/>	To Messaging2019	<input type="checkbox"/>	Messaging2019	To Messaging on Win 2019	
<input checked="" type="checkbox"/>	To NovaAlert	<input type="checkbox"/>	novaalert	To NovaAlert	
<input type="checkbox"/>	To SIM PSTN	<input type="checkbox"/>	SBCE - SIM - PSTN	Simulated PSTN	

Select : All, None

With the new Dial pattern in place, click on **Commit** as shown below.

Dial Pattern Details

Commit Cancel

General

* Pattern: 3201

* Min: 4

* Max: 4

Emergency Call: ☐

SIP Domain: greaney.sil6.avaya.com

Notes: To NovaAlert

Originating Locations and Routing Policies

Add Remove

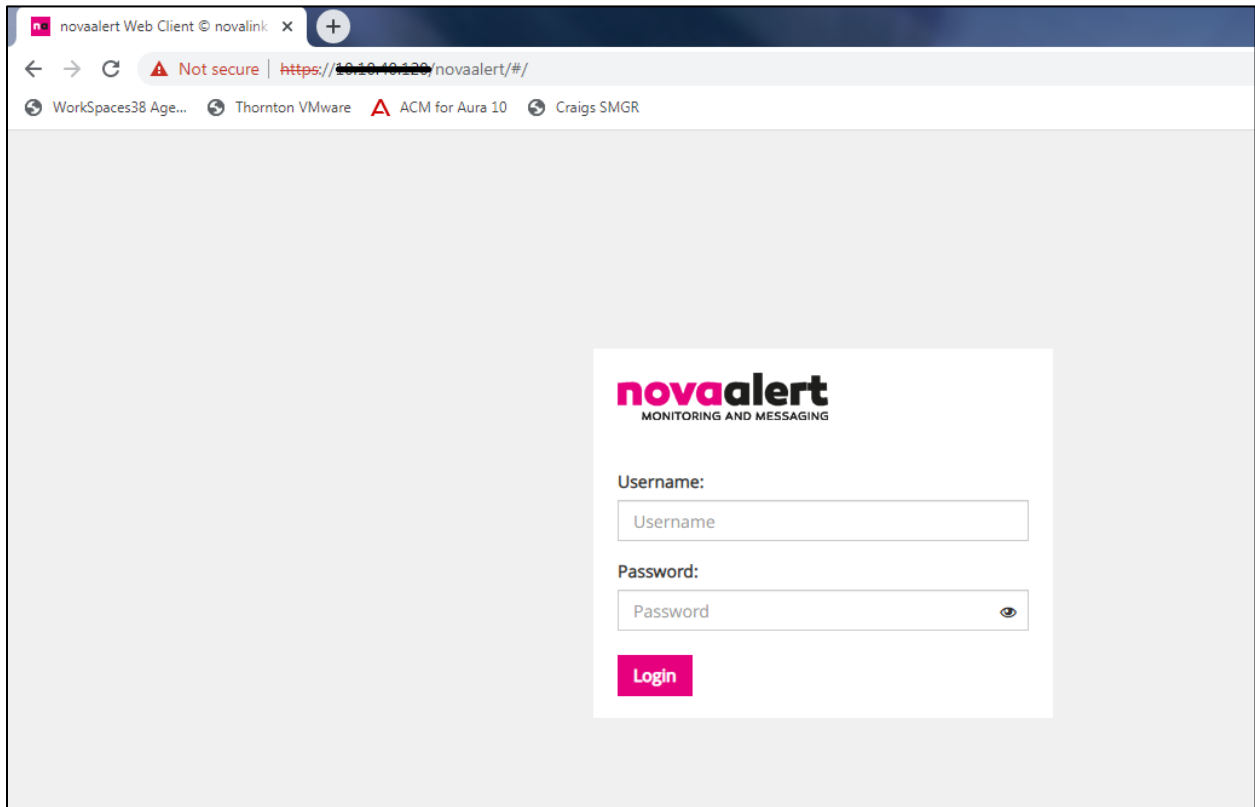
1 Item							
<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	DevConnectGalway	DevConnect Lab Galway	To NovaAlert	0	<input type="checkbox"/>	novaalert	To NovaAlert

Select : All, None

7. Configuration of novalink novaalert

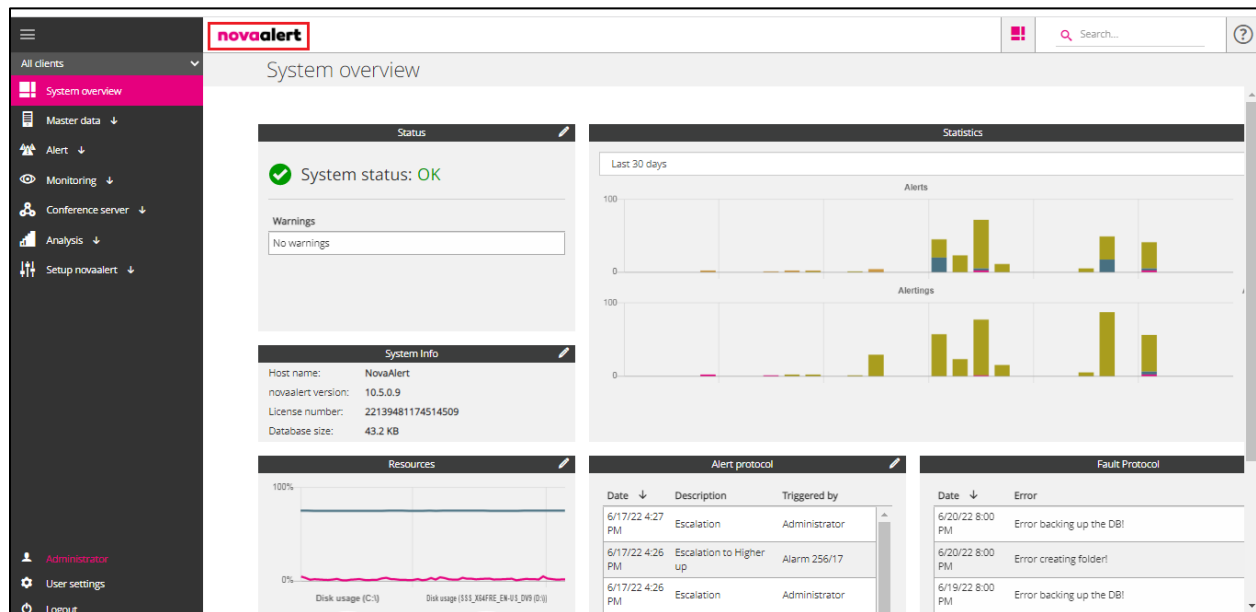
It is assumed that novaalert is already installed and configured by a novalink certified engineer. The following shows the steps that can be carried out in order to make changes or to examine a working system. The screen shots were taken after compliance testing was completed successfully and will show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

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, for compliance testing **https://<IPofnovaalert>/novaalert** was used. The following screen shown is asking for the **Username** and **Password**, enter these and click on the **Login** button.



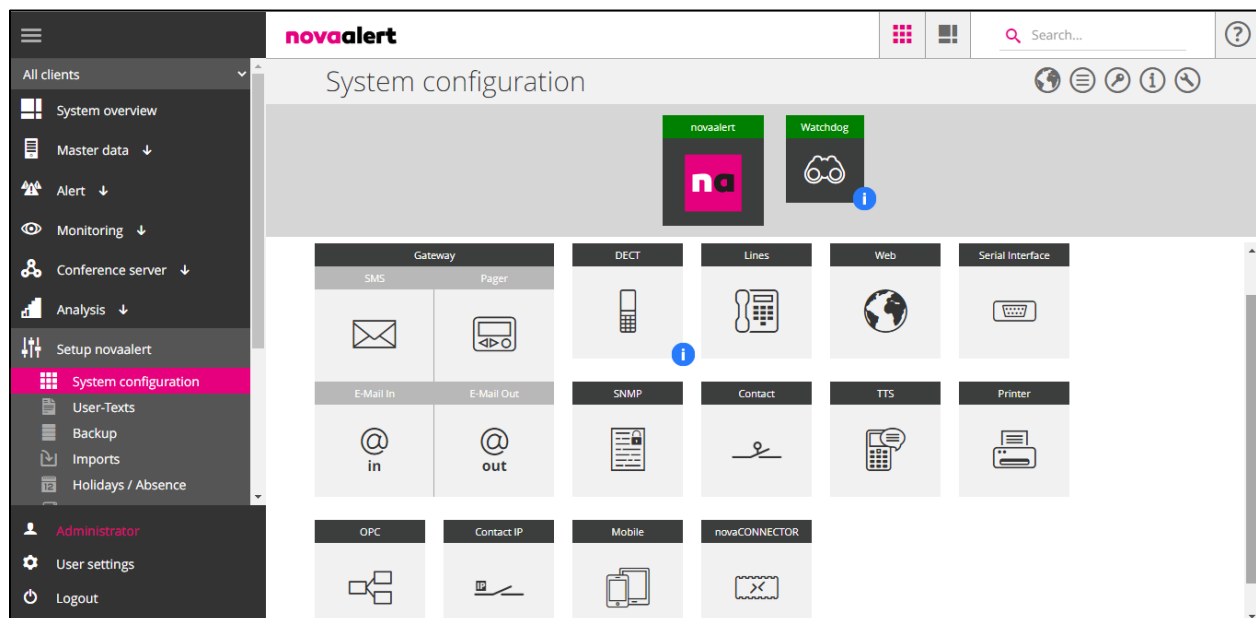
The screenshot shows a web browser window with the title 'novaalert Web Client © novalink'. The address bar displays 'https://10.10.10.100/novaalert/#/'. The browser tabs include 'WorkSpaces38 Age...', 'Thornton VMware', 'ACM for Aura 10', and 'Craigs SMGR'. The main content area is a light gray background with a white login form in the center. The form has the 'novaalert MONITORING AND MESSAGING' logo at the top. Below the logo, there are two input fields: 'Username:' and 'Password:'. The 'Password:' field has a small eye icon to its right. At the bottom of the form is a red 'Login' button.

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



7.1. Configure novaalert SIP Trunk Connection

To begin the configuration of novaalert to connect to Session Manager using SIP trunks, click on the **Lines** icon in the main window. All configuration with regards to the SIP connection to Session Manager is set in this area.



Under the **Line Configuration (Lines)** section, the Feature Access Code for Service Observe Talk and Listen is used for the **Intrusion code**. The Intrusion Code is required if an alarm needs to get to a telephone, even if it is busy. This access code may differ on other systems so best to view the Feature Access Code first as per **Section 5.1.3**. Other settings were left as default or as shown below.

Note: The Remote Access extension is placed before the Feature Access Code as shown below, the remote access code being **3150** and the Feature Access Code is ***57**. Remote Access was configured in **Section 5.4**.

System configuration > **Lines**

Lines

Search...

?

Line Configuration (Lines)

Intrusion code	3150*57	(AufschaltCode)	+	-	✖
Digits for intrusion analog?					
Line allocation 1	1	(Linie1)	+	-	✖
Line allocation 2	2	(Linie2)	+	-	✖
Line allocation 3	3	(Linie3)	+	-	✖
Line allocation 4	4	(Linie4)	+	-	✖
Min Connection Time	5	(MinAnhoeren)	+	-	✖
Reserved Lines for Alarm Triggering	0	(NurAusloesen)	+	-	✖
Static Direct Alarm		(DirektAlarmNummer1)	+	-	✖
Timeout external calls	30	(CallLängeExtern)	+	-	✖
Timeout internal calls	30	(CallLängeIntern)	+	-	✖
Word Replacement Type	Words separated by "space" are replaced	(Ersetzungsart)	+	-	✖

Setup lines

Add entry

Close

Save

Under the **Voice over IP Configuration (VoIP)** section the **Driver Preferences** is set to SIP and the IP address and SIP Domain name for Session Manager are added. The SIP Gateway fields should point to Session Manager with the **Realm** showing the SIP domain as per **Section 6.1** and the **IP-Address** showing that of the Session Manager SIP IP address. If DNS is not being used, please enter the IP Address in both fields, Realm and IP-Address. The **Local User Name** can also be filled in this will be shown on the phone display as a name of the alarm.

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	Prefix	(H323_Gateway)	+	✖
	IP-Address	Prefix		-	
				+	
H323 Use H245 Tunneling	No		(H323_UseH245Tunneli...	+	✖
Local User Name	DevConnect		(LocalUserName)	+	✖
SIP Alias	Host	Alias	Username	Password	Realm
	Host	Alias	Username	Password	Realm
SIP Gateway	Realm	IP-Address	Prefix	Local Interface	(SIP_Gateway)
	greaney.sil6	10.10.40.12	Prefix	Local Interface	

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)>

Close Save

Under the section **Call Control (Callinfo)** the following settings are noted, **Card Driver** should be set to **VoIP (H.323/SIP)** and the **Default Calling Party** should be set to something appropriate that would represent the CLID of the alarm being sent, again this will show on the phone display when called to by novaalert. The **PBX Type** should be set to **Avaya CM**. **Signaling outgoing DTMF** was set to SIP Info, however this will be dictated by Communication Manager so this setting may not be critical.

Note: Intrusion Configuration was set to **Recall with add. Intrusion prior call no.** This will allow novaalert to make a second call this time adding the feature for remote access and service observe before the extension to be called to allow the intrusion to take place.

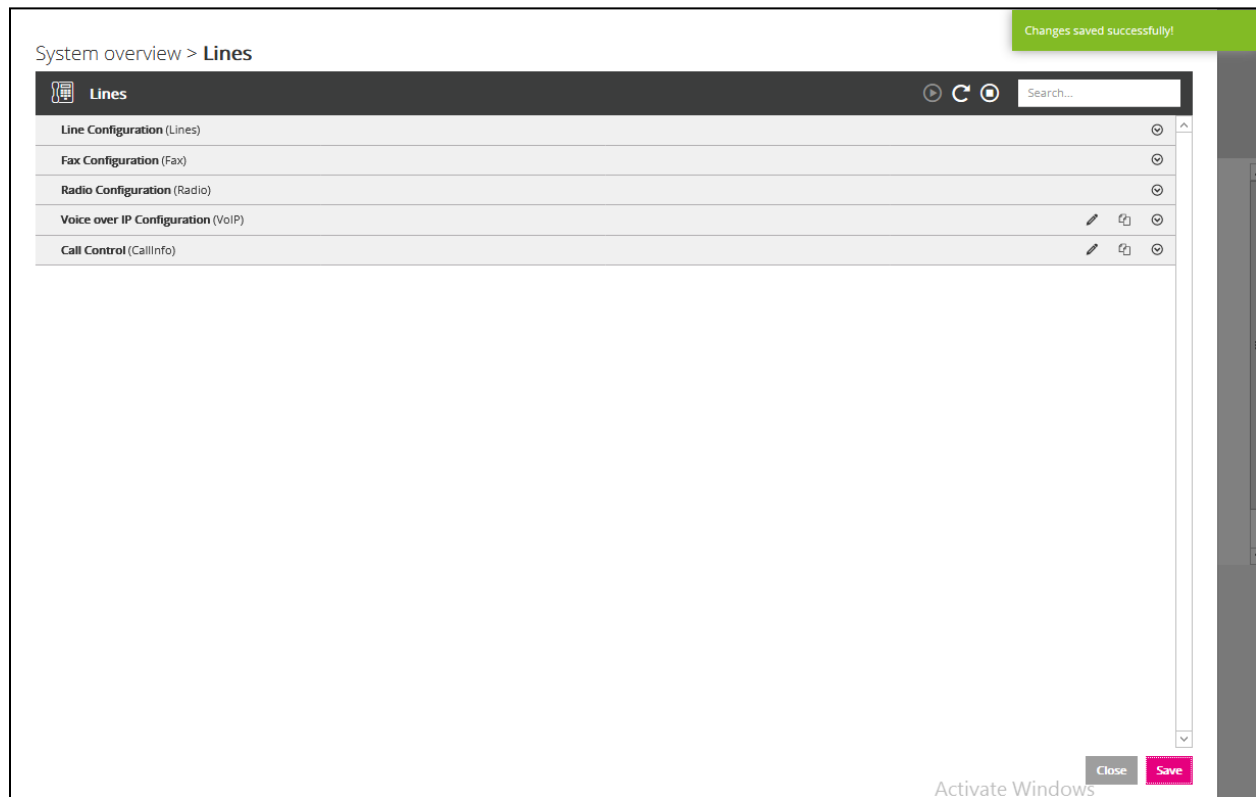
System configuration > **Lines**

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 CM	(PBXType)	
QSIG Standard	Disabled	(QSIGStandard)	
Signaling outgoing DTMF	As sound formatted information message (H.245 signa	(OutgoingDTMFMode)	
Timeout Call List	8	(RufZeitAnrufliste)	

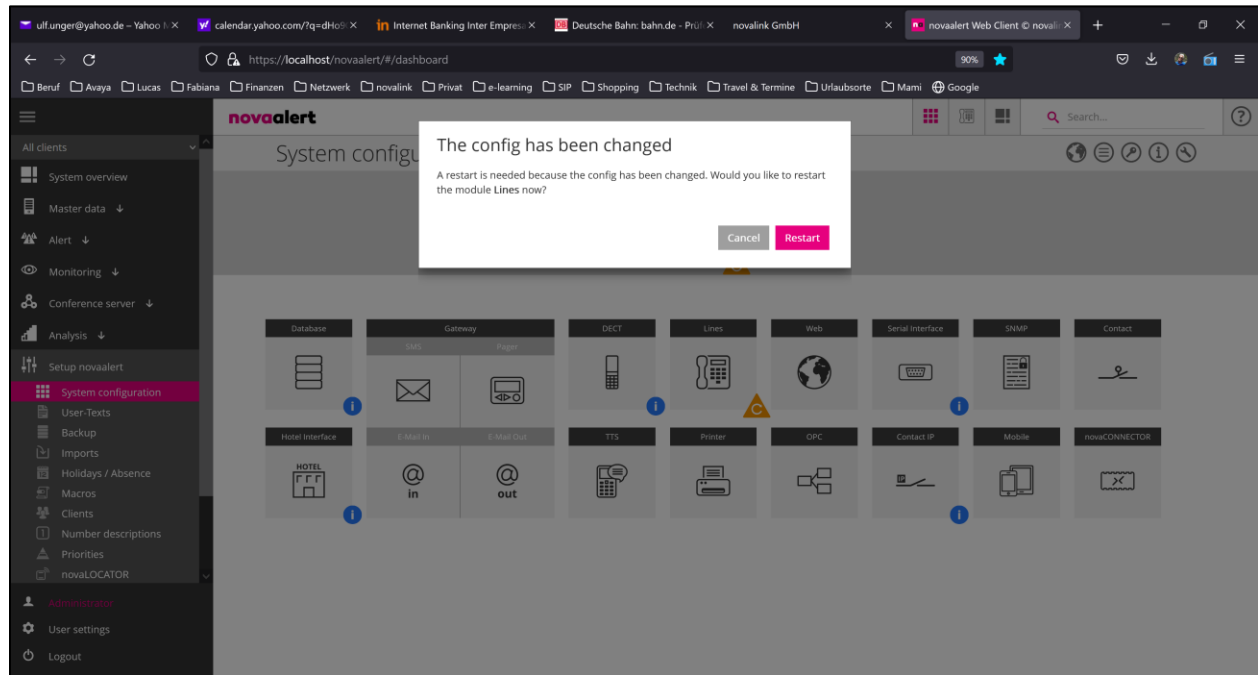
Close Save

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

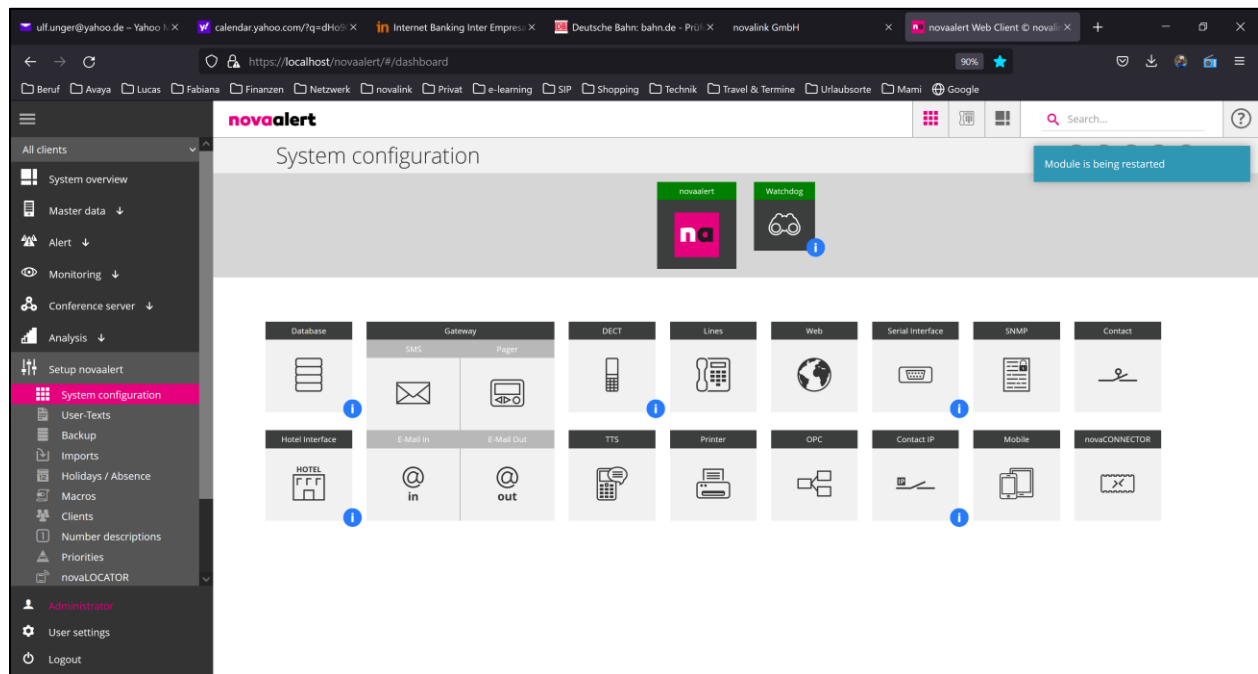
Changes saved successfully should be displayed at the top right of the screen and **Close** can then be clicked at the bottom right.



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



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



7.2. Configure Alerting

To send an alarm to an extension/phone on Communication Manager, that same extension will need to be added here to novaalert. 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. For compliance testing, a SIP extension 3101 was used. Under the **Common** tab, enter the details of the extension to be added. A **PIN code** will need to be added also.

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

The screenshot shows the 'novaalert' web application interface. On the left is a sidebar menu with options: All clients, System overview, Master data, User master data (highlighted), Group definition, Alert definition, On-Call-Duty lists, On-Call-Duty templates, Alert interfaces, SNMP, Directalerts, Scheduled alerts, IP-inputs, IP-outputs, Info phone, and Routes. The main area is titled 'Edit person' and 'SIP Phone (6)'. It features a list of existing clients on the left and a form for editing a selected client on the right. The selected client is 'SIP Phone' (No. 6). The form has tabs for 'Common', 'Numbers', 'Authorization', 'Mobile/Desktop', and 'Allocation'. The 'Common' tab is active, showing fields for Name, PIN code, Client, Personal number, Inactive status, Street, Logged in status, and Zip / City. The 'Name' field contains 'SIP Phone', 'PIN code' contains '1234', 'Client' is set to 'Global', and 'Logged in' is indicated by a green dot.

No.	Name
5	H323 Phone
11	Hunt Group
18	Hunt Group IP500V2
20	Hunt Group IPO ALL
19	Hunt Group SE
16	IP500V2 Digital 5201
17	IP500V2 SIP 5221
3	Paul Greaney
13	SE H323 5350
14	SE SIP 5321
15	SE Workplace 5322
6	SIP Phone
4	Station A
2	Ulf Unger

Edit person SIP Phone (6) Add new

Common Numbers Authorization Mobile/Desktop Allocation

Name: SIP Phone **Client:** Global

PIN code: 1234 **Personal number:**

Additional information:

Street:

Zip / City:

Inactive: ☐ **Logged in:** ☒ **No parallel alerts:** ☐

The extension number is added under the **Numbers** tab as shown below, this is all that needs to be added to get the basics working.

Filter person...

Edit person SIP Phone (6) Add new

Common **Numbers** Authorization Mobile/Desktop Allocation

Office 1:
3101 ☒

Office 2:
 ☒

Home 1:
 ☒

Home 2:
 ☒

Mobile 1:

Close Save

No.	Name ↑
5	H323 Phone
11	Hunt Group
18	Hunt Group IP500V2
20	Hunt Group IPO ALL
19	Hunt Group SE
16	IP500V2 Digital 5201
17	IP500V2 SIP 5221
3	Paul Greaney
13	SE H323 5350
14	SE SIP 5321
15	SE Workplace 5322
6	SIP Phone
4	Station A
2	Ulf Unger
10	Workplace

1 / 1

An Alert will also need to be added to allow the alert to get sent. The extension added on the previous page will be associated with the Alert. Navigate to **Master data → Alert definition** in the left window and click on **Add new** in the main window.

novaaalert

Alert definition Add new

Search alert...

No.	Description ↑	PIN code	Client
22	ALERT - IP500V2 - DIGITAL	1234	Global
25	ALERT - IP500V2 - ONLY	1234	Global
21	ALERT - IP500V2 - SIP	1234	Global
19	ALERT - IPO SE - H323	1234	Global
24	ALERT - IPO SE - ONLY	1234	Global
20	ALERT - IPO SE - SIP	1234	Global
23	ALERT - IPO SE - Workplace	1234	Global
12	Alert from Phone	1234	Global
27	Alert HG IP500V2	1234	Global
29	Alert HG IPO All	1234	Global
8	Alert to DECT 3021	1234	Global

Enter the details of the alert in the **Common** tab. These are the details that were used for compliance testing to send an alert to one SIP phone on Communication Manager.

Search alert...

No. Description

26 Alert to IPO - ALL EXTS

13 Alert to Non SIP Phones

5 Alert to SIP

10 Alert to SIP phones only

9 Alert to Workplace

14 CM Hunt Group Alert

7 Conference Alert

1 Default Alarm. You should NOT be here

17 Escalation

18 Escalation to Higher up

28 HG SE

30 Paging Alert

15 Pauls Group Alert

Edit alert Alert to SIP (5)

Common

Messages

Alert-list

Alert interfaces

Escalation

Mobile/Desktop

Various

Description:

Alert to SIP

PIN code for trigger:

1234

Priority:

Highest Priority

Voice-No.:

59

Alert type:

Group Call

Client:

Global

Number of attempts:

1

Notes:

Number of person to be contacted:

All

Select contact group:

Compile individual alert list

Close

Save

A message can be sent to the display of the phone set in question, this message can be changed, as shown below, under the **Phone display** section of the **Messages** tab.

The screenshot shows the 'Edit alert' window for 'Alert to SIP (5)'. The 'Messages' tab is active. On the left, a list of alerts is shown, with 'Alert to SIP' (ID 5) selected. The main area displays a table of messages with the alert description. The 'Phone display' message is selected, showing the text 'Fire in the Building' in the 'Message' field. The 'Event text' field is set to 'Additionally'. The 'Add new' button is in the top right, and 'Close' and 'Save' buttons are in the bottom right.

No.	Description
26	Alert to IPO - ALL EXTS
13	Alert to Non SIP Phones
5	Alert to SIP
10	Alert to SIP phones only
9	Alert to Workplace
14	CM Hunt Group Alert
7	Conference Alert
1	Default Alarm. You should NOT be here
17	Escalation
18	Escalation to Higher up
28	HG SE
30	Paging Alert
15	Pauls Group Alert

Fill messages with alert description	
Email/Printer	(Alert to H323)
Fax	(Alert to H323)
Mobile/Desktop	(Alert to H323)
Pager alphanumeric	(Alert to H323)
Pager numeric	(Alert to H323)
Phone display	(Fire in the Building)

Message: Fire in the Building

Event text: Additionally

The extension that was created previously can be added under the **Alert-list** tab. Click on **Add entry** in the main window.

The screenshot shows the 'Edit alert' window for 'Alert to SIP (5)'. The 'Alert-list' tab is active. The main area is empty except for a green 'Add entry' button in the top left corner. The 'Add new' button is in the top right, and 'Close' and 'Save' buttons are in the bottom right.

Under **Person / IP output**, select the appropriate entry from the drop-down menu, once this is added the **Medium / State** should be automatically populated too. The SIP Phone that was created previously was selected as shown below.

Edit entry

Person / IP output:

SIP Phone (6)

Medium / State:

Office 1 (3101)

Chat/Alert conference:

☐

Acknowledge:

☐

Intrusion:

☐

Logged in:

☒

Delay:

0

Close

OK

Once this entry is added under **Alert-list**, click on **Save**. Please note that other options may be selected depending on what is required but to send the basic alert, the following selected.

Edit alertAlert to SIP (5)

Add new

CommonMessagesAlert-listAlert interfacesEscalationMobile/DesktopVarious

Add entry

<input type="checkbox"/>	Name	Medium / State	Chat/Alert conf	Acknowledge	Intrusion	Logged in	Delay	
<div>↑↓</div>	SIP Phone (6)	Office 1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<div>0</div>	<div><div></div><div></div><div></div></div>

Edit alert-listRenumbr positions

1 / 1

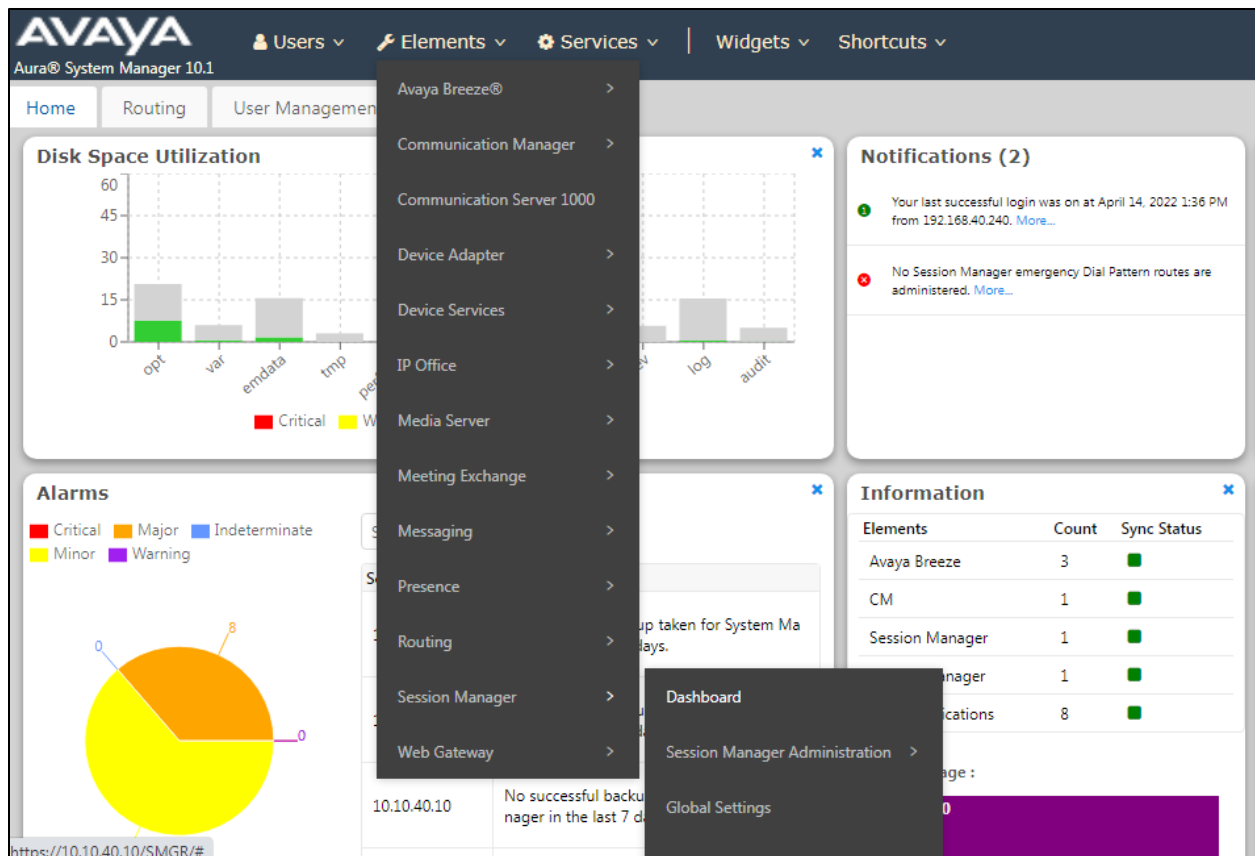
CloseSave

8. Verification Steps

This section illustrates the steps necessary to verify that the novaalert is configured correctly to allow alarms and notifications to be sent 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**.

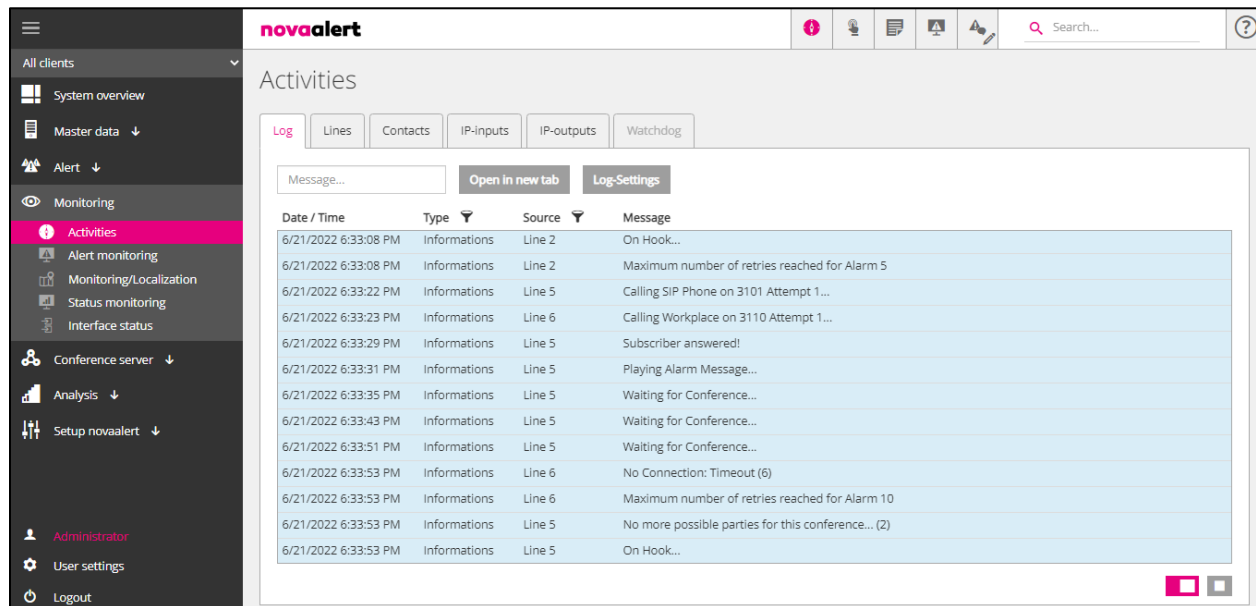
The screenshot shows the Avaya Aura System Manager 10.1 interface. The left sidebar contains a navigation menu with options like Session Manager, Dashboard, Session Manager..., Global Settings, Communication Prof..., Network Configur..., Device and Locati..., Application Confi..., System Status, Load Factor, SIP Entity Monit..., and Managed Band... The main content area is titled "SIP Entity Link Monitoring Status Summary". It includes a "Run Monitor" button and a timestamp "As of 4:29 PM". Below this, there is a table titled "SIP Entities Status for All Monitoring Session Manager Instances" showing 1 item. The table has columns for Session Manager, Type, Monitored Entities (Down, Partially Up, Up, Not Monitored, Deny, Total). The data row shows "sm101x" as the Session Manager, Core as the Type, and 0 Down, 0 Partially Up, 5 Up, 0 Not Monitored, 0 Deny, and 5 Total. Below the table, there is a "Select : All, None" option. Another section titled "All Monitored SIP Entities" shows 5 items, including "Messaging2019" and "cm101x - Phones - 5061".

Choose the **novalink** SIP entity (not shown). The **Link Status** and **Conn. Status** should both show as **UP** as is shown below.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The left sidebar contains a navigation menu with options like Application Confi..., System Status, Load Factor, SIP Entity Monit..., Managed Band..., Security Module..., SIP Firewall Status, and Registration Su... The main content area is titled "SIP Entity, Entity Link Connection Status". It includes a "Run Monitor" button and a timestamp "As of 4:29 PM". Below this, there is a table titled "All Entity Links to SIP Entity: novaalert". The table has columns for Session Manager Name, Session Manager IP Address Family, SIP Entity Resolved IP, Port, Proto., Deny, Conn. Status, Reason Code, and Link Status. The data row shows "sm101x" as the Session Manager Name, IPv4 as the Session Manager IP Address Family, 10.10.40.120 as the SIP Entity Resolved IP, 5060 as the Port, UDP as the Proto., FALSE as the Deny, UP as the Conn. Status, 200 OK as the Reason Code, and UP as the Link Status. Below the table, there is a "Select : None" option.

8.2. Verify novaalert Status

Log into novaalert as per **Section 7**, navigate to **Monitoring → Activities** in the left column. In the main window there are a number of tabs that can be selected to view real-time activities and shown below are a number of log entries for an alarm being sent but not answered in a conference scenario. An Alarm can be sent to various voice endpoints and will answer the call and hear the alarm message. 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.



The screenshot displays the novaalert web interface. The left sidebar contains a navigation menu with options: All clients, System overview, Master data, Alert, Monitoring, Activities (selected), Alert monitoring, Monitoring/Localization, Status monitoring, Interface status, Conference server, Analysis, Setup novaalert, Administrator, User settings, and Logout. The main content area is titled 'Activities' and features tabs for Log, Lines, Contacts, IP-inputs, IP-outputs, and Watchdog. The 'Log' tab is active, showing a table of log entries. Above the table are input fields for 'Message...' and buttons for 'Open in new tab' and 'Log-Settings'.

Date / Time	Type	Source	Message
6/21/2022 6:33:08 PM	Informations	Line 2	On Hook...
6/21/2022 6:33:08 PM	Informations	Line 2	Maximum number of retries reached for Alarm 5
6/21/2022 6:33:22 PM	Informations	Line 5	Calling SIP Phone on 3101 Attempt 1...
6/21/2022 6:33:23 PM	Informations	Line 6	Calling Workplace on 3110 Attempt 1...
6/21/2022 6:33:29 PM	Informations	Line 5	Subscriber answered!
6/21/2022 6:33:31 PM	Informations	Line 5	Playing Alarm Message...
6/21/2022 6:33:35 PM	Informations	Line 5	Waiting for Conference...
6/21/2022 6:33:43 PM	Informations	Line 5	Waiting for Conference...
6/21/2022 6:33:51 PM	Informations	Line 5	Waiting for Conference...
6/21/2022 6:33:53 PM	Informations	Line 6	No Connection: Timeout (6)
6/21/2022 6:33:53 PM	Informations	Line 6	Maximum number of retries reached for Alarm 10
6/21/2022 6:33:53 PM	Informations	Line 5	No more possible parties for this conference... (2)
6/21/2022 6:33:53 PM	Informations	Line 5	On Hook...

8.3. Trigger an alert on novaalert

From the novaalert web browser, navigate to **Master data** → **Alert** → **Trigger alert** in the left window and in the main window enter the **Alert to be triggered**, as shown below. Click on **Trigger alert** at the bottom right of the screen.

The screenshot displays the novaalert web interface. On the left is a dark sidebar with a menu. The main content area is titled 'Manual alert trigger' and contains a form with the following fields:

- Person triggering alert:** A dropdown menu with 'Administrator' selected.
- Alert to be triggered:** A dropdown menu with 'Alert to SIP (5)' selected.
- Call type:** A dropdown menu with '<Adopt call type defined in Alarm>' selected.
- Plaintext:** A text input field.
- Calling number:** A text input field.
- Alert message:** A checkbox and a text input field with the placeholder 'Filename: _ManualAlert_'.

At the bottom right of the form is a pink button labeled 'Trigger alert'. The sidebar menu includes options like 'System overview', 'Master data', 'Alert', 'Monitoring', 'Conference server', 'Analysis', and 'Setup novaalert'.

8.4. Use traces to observe the SIP messaging

Before the alert is triggered as per **Section 0**, open traceSM on Session Manager using PuTTY to open an SSH session with Session Manager as shown below. This will show the SIP messaging for all devices connected to Session Manager including calls between Session Manager, novaalert and Communication Manager. The **INVITE** below originating from **novaalert** to Session Manager (**SM100**) and then to Communication Manager (**cm101x – SIP Trunk**) and to the SIP phone (**3101**), with the correct replies to novaalert, shows that the call should be successful. However, if the call was not successful this trace is a best way to start to diagnose the issue.

```
sm101x@greaney.sil6.avaya.com - traceSM V10.10.0.003 - Captured: 121 Displayed: 52

novaalert      cm101x - SIP TRUNK - 5      3110
SM100          3101

16:01:15.023  --INVITE-->
16:01:15.024  <--Trying--
16:01:15.027  --INVITE-->
16:01:15.028  <--Trying--
16:01:15.030  --INVITE-->
16:01:15.049  <--Trying--
16:01:15.060  --INVITE-->
16:01:15.095  <--Trying--
16:01:15.220  <--Ringing--
16:01:15.241  <--Ringing--
16:01:15.242  <--Ringing--
16:01:15.244  <--Ringing--
16:01:15.246  --PRACK-->
16:01:15.247  <--PRACK-->
16:01:15.247  <--200 OK-->
16:01:17.558  --OPTIONS-->
16:01:17.559  <--200 OK-->
16:01:18.927  --PING-->
16:01:18.927  <--PONG-->
16:01:28.749  --PING-->
16:01:28.760  <--OPTIONS-->
16:01:29.761  <--200 OK-->
16:01:37.637  --OPTIONS-->
16:01:37.638  <--200 OK-->
16:01:37.814  <--200 OK-->
16:01:37.816  <--200 OK-->
16:01:37.817  <--ACK-->
16:01:37.818  <--PUBLISH-->
16:01:37.818  <--ACK-->
16:01:37.829  <--200 OK-->
16:01:37.831  <--200 OK-->
16:01:37.842  <--ACK-->
16:01:37.843  <--ACK-->
16:01:37.860  <--NOTIFY-->
16:01:37.860  <--200 OK-->
16:01:37.891  <--reINVITE-->
16:01:37.892  <--Trying-->
16:01:37.893  <--reINVITE-->
16:01:37.894  <--200 OK-->
16:01:37.895  <--200 OK-->

(2) T:3101 F:0049123456789 U:3101
(2) 100 Trying
(2) T:3101 F:0049123456789 U:3101 P:imsterm
(2) 100 Trying
(3) T:3101 F:0049123456789 U:3101 P:termdone
(3) 100 Trying
(3) T:3101 F:0049123456789
(3) 100 Trying
(3) 180 Ringing
(3) 180 Ringing
(3) 180 Ringing
(2) 180 Ringing
(2) sip:3101@greaney.sil6.avaya.com
(2) sip:3101@greaney.sil6.avaya.com
(2) 200 OK (PRACK)
(2) 200 OK (PRACK)
(4) sip:10.10.40.12
(4) 200 OK (OPTIONS)
PING from 10.10.40.193
PONG to 10.10.40.193
PING from 10.10.40.13
(8) sip:10.10.40.13
(8) 200 OK (OPTIONS)
(11) sip:10.10.40.12
(11) 200 OK (OPTIONS)
(3) 200 OK (INVITE)
(3) 200 OK (INVITE)
(3) sips:3101@192.168.40.184:6223
(12) sips:3101@greaney.sil6.avaya.com
(3) sips:3101@192.168.40.184:6223
(2) 200 OK (INVITE)
(2) 200 OK (INVITE)
(2) sip:3101@10.10.40.13:5061
(2) sip:3101@10.10.40.13:5061
(13) <sips:3101@greaney.sil6.avaya.com> Ev:dialog
(12) 200 OK (PUBLISH)
(2) T:0049123456789 F:3101 U:0049123456789
(2) 100 Trying
(2) T:0049123456789 F:3101 U:0049123456789
(2) 200 OK (INVITE)
(2) 200 OK (INVITE)

SIP RPN CHLP TLS Push Notification | s=Stop q=Quit ENTER=Details f=Filters w=Write a=ShowSM c=Clear i=IP r=RTF g=GoTo d=Calls
```

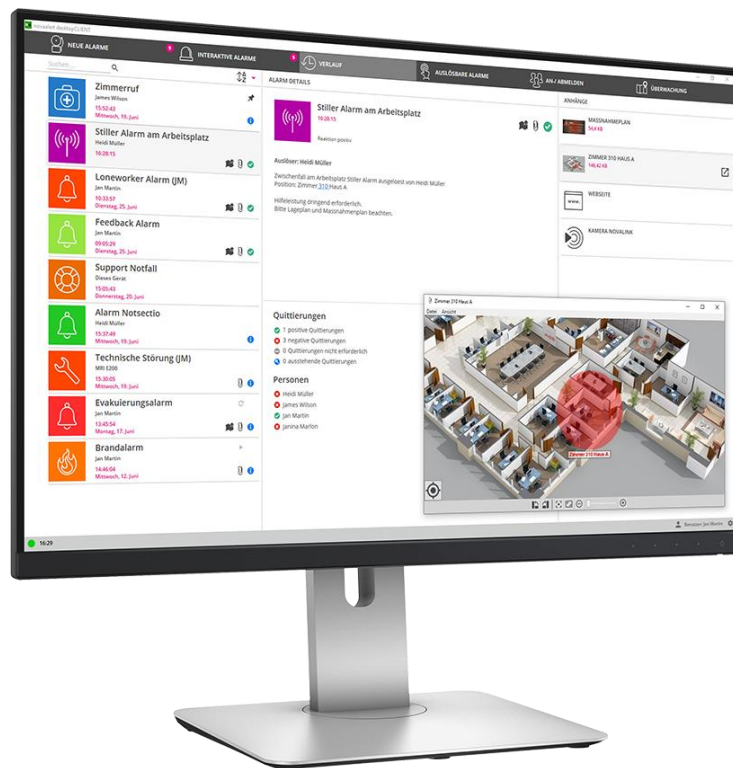
9.1. novaalert on different media

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

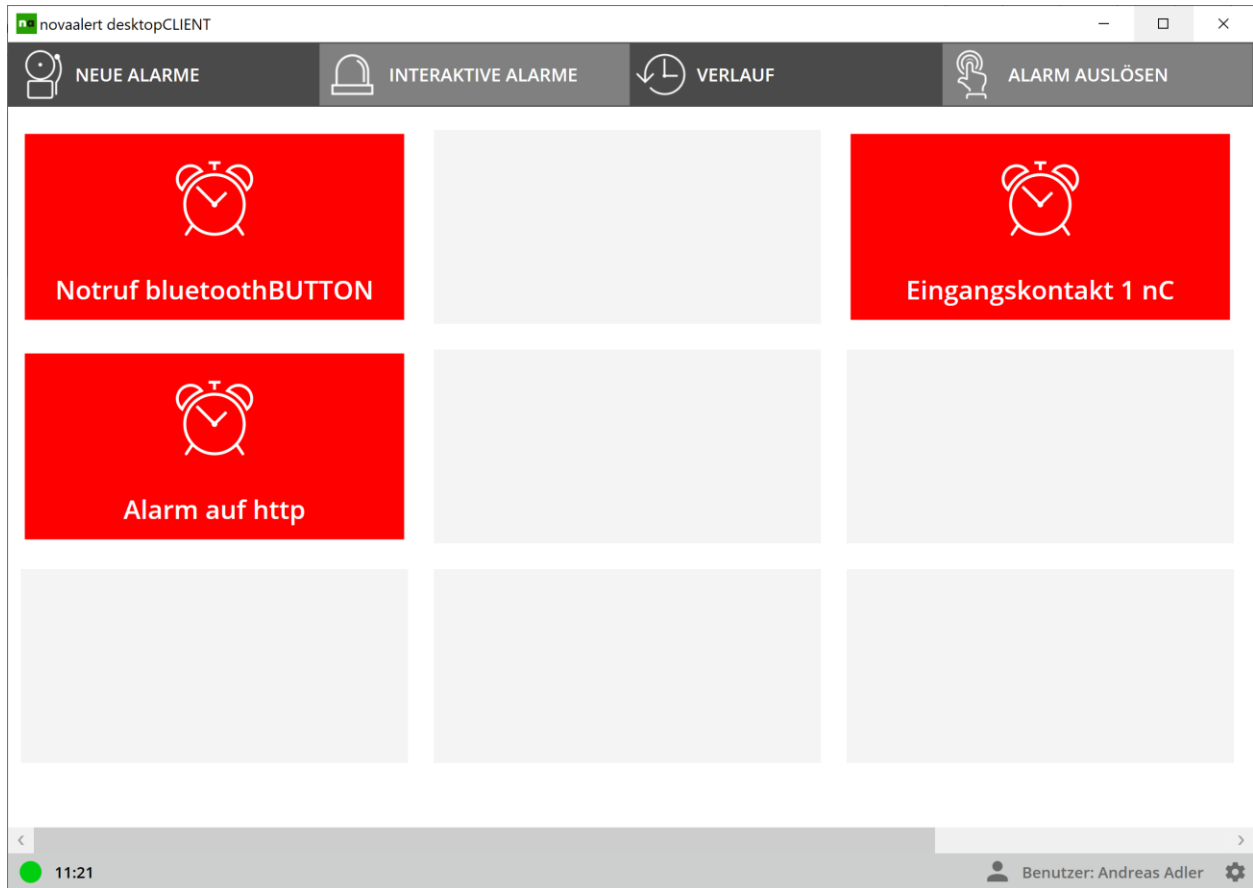
Note: These were not taken as part of compliance testing but are here to demonstrate the use of novaalert on different media.



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



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



10. Conclusion

These Application Notes describe the configuration steps required for novaalert v10.5 from novalink to successfully interoperate with Avaya Aura® Session Manager R10.1 and Avaya Aura® Communication Manager R10.1. All feature test cases were completed successfully with any observations noted in **Section 2.2**.

11. 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](ftp://support.novalink.ch/Technikerhandbuch/English/Technikerhandbuch%20novalink%20GmbH%20EN.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 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 **sm101x**).
- 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 5.2**. 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 can be set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833. Or, if SIP INFO is to be used, which is the preference of novalink, set this to **out-of-band**.
- 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.

display signaling-group 1		Page 1 of 3
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	Clustered? n
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: sm101x
Near-end Listen Port: 5061		Far-end Listen Port: 5061
Far-end Network Region: 1		
Far-end Domain: greanexp.sil6.avaya.com		
Incoming Dialog Loopbacks: eliminate		Bypass If IP Threshold Exceeded? n
DTMF over IP: out-of-band		RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3		Direct IP-IP Audio Connections? y
Enable Layer 3 Test? y		IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n		Initial IP-IP 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.

```
Display trunk-group 1                                     Page 1 of 5
                                     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 novalink 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.

```
display trunk-group 1                                     Page 2 of 5
  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

Caller ID for Service Link Call to H.323 1xC: station-extension
```

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

display trunk-group 1	Page 3 of 5
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Suppress # Outpulsing? n	Numbering Format: private
	UII Treatment: shared
	Maximum Size of UII Contents: 128
	Replace Restricted Numbers? n
	Replace Unavailable Numbers? n
	Modify Tandem Calling Number: no
Send UCID? y	
Show ANSWERED BY on Display? y	
DSN Term? n	

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

display trunk-group 1	Page 4 of 5
SHARED UII FEATURE PRIORITIES	
ASAI: 1	
Universal Call ID (UCID): 2	
MULTI SITE ROUTING (MSR)	
In-VDN Time: 3	
VDN Name: 4	
Collected Digits: 5	
Other LAI Information: 6	
Held Call UCID: 7	
ECD UII: 8	

Page 5 is set as follows.

display trunk-group 1	Page 5 of 5
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
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: 101	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
Resend Display UPDATE Once on Receipt of 481 Response? n	
Identity for Calling Party Display: From	
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	

©2022 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.