



Avaya Solution & Interoperability Test Lab

Application Notes for New Voice Technologies Mobicall 8.0.3 with Avaya Aura® Communication Manager 7.0 using Avaya Aura Session Manager 7.0 - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate New Voice Technologies Mobicall with Avaya Aura® Communication Manager using Avaya Aura Session Manager. Mobicall is an Alarm generation and distribution solution that connects to Session Manager as a SIP entity.

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

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

1. Introduction

These Application Notes describe the configuration steps required to successfully integrate New Voice Technologies Mobicall with Avaya Aura® Communication Manager using Avaya Aura Session Manager. Mobicall is an Alarm generation and distribution solution that connects to Session Manager as a SIP entity. System alarms are recorded on the Mobicall server and distributed to Communication Manager endpoints.

2. General Test Approach and Test Results

The general test approach was to configure the Mobicall Server to communicate with Communication Manager (CM) via a SIP Trunk connected to Session Manager. Stations present on CM were configured on the Mobicall server and a number was configured to dial Mobicall and create and initiate alarms.

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

2.1. Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on setting and distributing alarms in different call scenarios with good quality audio. The tests included:

- Mobicall SIP trunk is connected and in Service.
- Mobicall can route Alarms to SIP, Digital and H.323 endpoints.
- Alarms can be set and distributed from CM to Mobicall.
- Priority calling and Whisper Paging functionality can be initiated from Mobicall
- Failover/Service – Tests the behaviour of Eurocross Connect Client during certain failed conditions.

2.2. Test Results

All test cases were passed.

2.3. Support

Provide details for technical support for the member. Please include web sites and telephone number.

Telefon	+41 58 750 11 11
Fax	+41 58 750 11 12
Email	support@newvoice.ch
Internet	mobilisierung.com

3. Reference Configuration

The configuration shown in Figure 1 was used during the compliance test of New Voice Technologies Mobicall with Communication Manager via Session Manager. Mobicall utilizes a SIP trunk to communicate with Communication Manager handsets

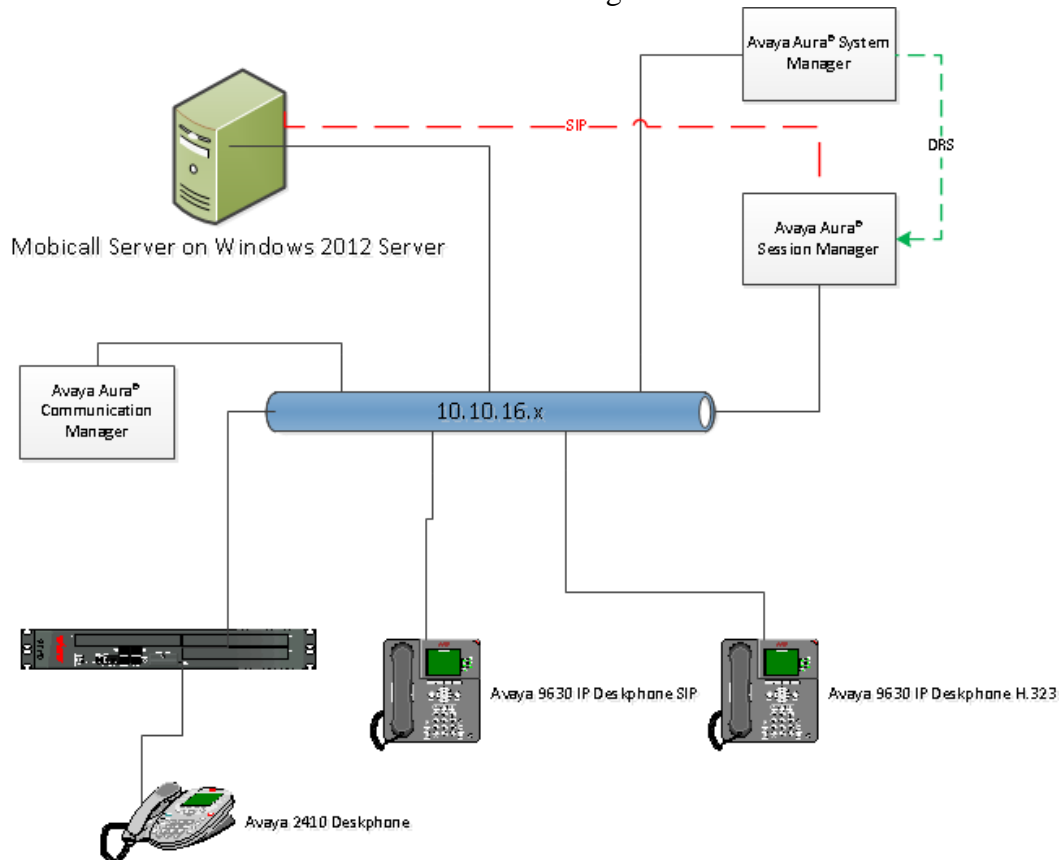


Figure 1: Connection of Mobicall with Avaya Aura® Communication Manager via Session Manager

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communicaiton Manager running on VMware Virtual Machine	R7 SP1 R017.00.0.441.22438
Avaya Aura® Session Manager	R7.0 7.0.0.0.700007
Avaya Aura® System Manager	R7.0 7.0.0.0.1626-7.0.9.912
Avaya G430 Media Gateway	FW 37.19.0
Avaya 96x1 Series IP Deskphones H.323	6.6.0.29
Avaya 96x1 Series IP Deskphones SIP	6.5.0
Avaya 2410 Digital Deskphone	N/A
Mobicall	8.0.3

5. Configure Avaya Aura® Communication Manager

This section describes the steps required to allow Communication Manager to communicate with Mobicall. It is assumed that Communication Manager is installed and configured before implementing the configuration step below. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

The configuration illustrated in this section was performed using Communication Manager System Administration Terminal (SAT).

Configuration steps include:

- Check SIP Trunk Licensing.
- Add entries in the Dial Plan for use with SIP Trunk and routing to Mobicall.
- SIP Trunk Administration (to Session Manager).
- Adding Mobicall Route Pattern.
- Adding Mobicall Access number.
- Setting feature Access Codes.

Using the *display system-parameters customer-options* command go to **page 2** and check that the system is sufficiently licensed for SIP Trunks.

display system-parameters customer-options	Page 2 of 11
OPTIONAL FEATURES	
IP PORT CAPACITIES	USED
Maximum Administered H.323 Trunks:	12000 0
Maximum Concurrently Registered IP Stations:	18000 3
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:	41000 0
Maximum Video Capable IP Softphones:	18000 0
Maximum Administered SIP Trunks:	24000 10

Use the *change node-names ip* command to add Session Manager

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
SM1677	10.10.16.77	
default	0.0.0.0	
procr	10.10.16.27	
procr6	::-	

Use *change dialplan analysis* to add a **3** digit dial access code(**dac**) for use in the SIP Trunk, a uniform dial plan(**udp**) entry for calling Mobicall and check that there is an entry for feature access codes(**fac**).

change dialplan analysis		Page 1 of 12
DIAL PLAN ANALYSIS TABLE		
Location: all		Percent Full: 2
Dialed String	Total Length	Call Type
2	7	udp
7	3	dac
8	5	udp
8	7	udp
827	7	ext
9	1	fac
*	3	fac
#	3	fac

Use *add-signaling-group x* where x is the number of the group required. Set **Transport Method** to **tcp**, **Near-end Node Name** to **procr** and **Far-end Node Name** to the entry added in **node-names**. Set the **Far-end Network Region** to **1** and **Direct IP-IP Audio Connections?** to **n**

add signaling-group 76		Page 1 of 2
SIGNALING GROUP		
Group Number: 76	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	
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: SM1677	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 1	
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? n	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
	Alternate Route Timer(sec): 6	

Use **add trunk-group x** where x is the number administered for the signaling group. On **Page 1** set the **Group Type** to **sip**. Set the **TAC** to suitable entry based on the dial plan **dac** administered above. Set the **Service Type** to **tie**, **Signaling group** to the one administered above and **Number of Members** to a number satisfactory for call routing required (**255** shown is the max for this type of trunk group).

add trunk-group 76		Page 1 of 21	
TRUNK GROUP			
Group Number: 76	Group Type: sip	CDR Reports: y	
Group Name: ToSM7	COR: 1	TN: 1	TAC: 776
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: tie	Auth Code? n		
		Member Assignment Method: auto	
		Signaling Group: 76	
		Number of Members: 255	

On **page 3** set the **Numbering Format** to **private**

add trunk-group 76		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
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			

Next a route pattern needs to be added so that call can be routed out of Communication Manager to Session Manager. Use ***change route-pattern x*** where x is the number of the SIP trunk created. Enter the Trunk group created above beside the first **Grp No**, an **FRL** of **0** and **Numbering Format** of **lev0-pvt**

change route-pattern 76										Page	1 of	3
Pattern Number: 76										Pattern Name: ToSM7		
SCCAN? n		Secure SIP? n		Used for SIP stations? n								
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted			DCS/	IXC	
No			Mrk	Lmt	List	Del	Digits			QSIG		
							Dgts			Intw		
1:	76	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		rest						lev0-pvt	none	

On page 4 enter a valid code for **Whisper Page Activation Access Code**.

change feature-access-codes		Page 4 of 10
FEATURE ACCESS CODE (FAC)		
Station Lock Activation:	Deactivation:	
Station Security Code Change Access Code:		
Station User Admin of FBI Assign:	Remove:	
Station User Button Ring Control Access Code:		
Terminal Dial-Up Test Access Code:		
Terminal Translation Initialization Merge Code:	Separation Code:	
Transfer to Voice Mail Access Code:		
Trunk Answer Any Station Access Code:		
User Control Restrict Activation:	Deactivation:	
Voice Coverage Message Retrieval Access Code:		
Voice Principal Message Retrieval Access Code:		
Whisper Page Activation Access Code: *80		

Mobicall uses a virtual extension that must be valid on the Communication Manager for Alarm routing to Mobicall for distribution to Communication Manager endpoints. Use **add station x** where x is a valid extension on Communication Manager but is not an extension that will be used to register a physical endpoint. On **Page 1** enter the **Extension, Type and Name**.

add station 8270999		Page 1 of 5
STATION		
Extension: 827-0999	Lock Messages? n	BCC: 0
Type: 9620	Security Code:	TN: 1
Port: S00020	Coverage Path 1:	COR: 1
Name: New Voice Virtual	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 827-0999	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english		
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? n	
	IP Video? n	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? y	

On page 2 set **EC500 State** to **enabled**

change station 8270999		Page 2 of 5
STATION		
FEATURE OPTIONS		
LWC Reception: spe	Auto Select Any Idle Appearance? n	
LWC Activation? y	Coverage Msg Retrieval? y	
LWC Log External Calls? n	Auto Answer: none	
CDR Privacy? n	Data Restriction? n	
Redirect Notification? y	Idle Appearance Preference? n	
Per Button Ring Control? n	Bridged Idle Line Preference? n	
Bridged Call Alerting? n	Restrict Last Appearance? y	
Active Station Ringing: single		
	EMU Login Allowed? n	
H.320 Conversion? n	Per Station CPN - Send Calling Number?	
Service Link Mode: as-needed	EC500 State: enabled	

Next use **change off-pbx-station-mapping x** where x is the virtual station added above. On Page 1 set **Application** as **EC500**, **Phone number** as the number used to call Mobicall and **Trunk Selection** as **aar**.

change off-pbx-telephone station-mapping 8270999						
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION						
Station	Application	Dial	CC	Phone Number	Trunk	Config
Extension		Prefix			Selection	Set
827-0999	EC500	-		88888	aar	3

On page 2 set **Call Limit** to the number of trunks configured on Mobicall and check that **Mapping Mode** and **Bridged Calls** are set to **both**

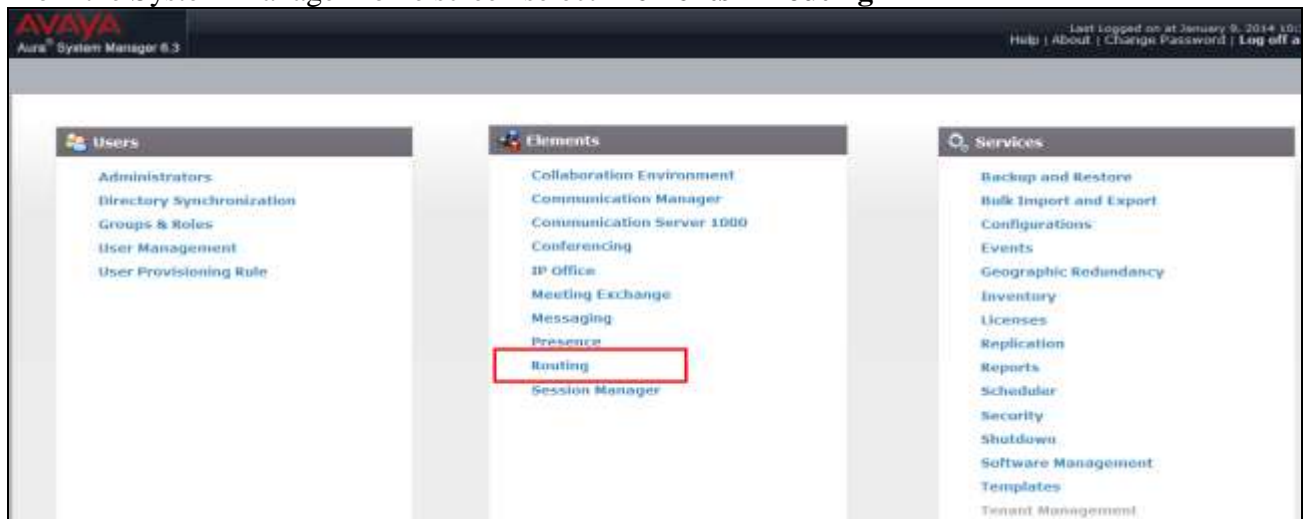
change off-pbx-telephone station-mapping 8270999						
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION						
Station	Appl	Call	Mapping	Calls	Bridged	Location
Extension	Name	Limit	Mode	Allowed	Calls	
827-0999	EC500	10	both	all	both	

6. Configure Avaya Aura® Session Manager

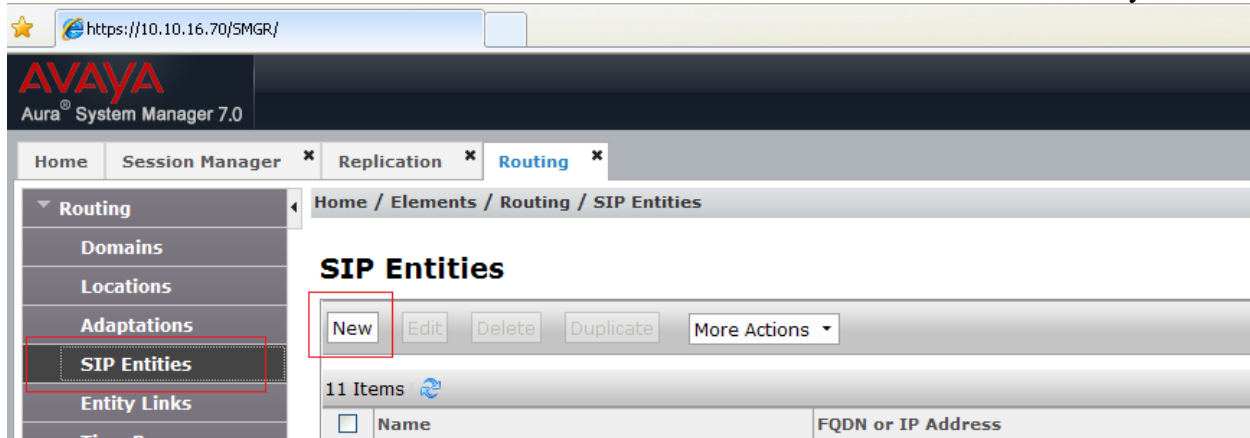
In this section the configuration steps required to connect Mobicall to Session Manager as a SIP entity are described. It is assumed that an existing Session manager instance has already been installed and configured as this is out with the scope of this document. All Configuration steps were carried out using Avaya Aura® System Manager. Configuration steps include:

- Adding Mobicall SIP Entity.
- Adding an Entity Link.
- Adding a Routing Policy.
- Adding a Dial Pattern.

From the System Manager home screen select **Elements→Routing**



Select **SIP Entities** from the left hand menu and click on **New** to add the Mobicall entity



AVAYA
Aura® System Manager 7.0

Home Session Manager Replication Routing

Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges

Home / Elements / Routing / SIP Entities

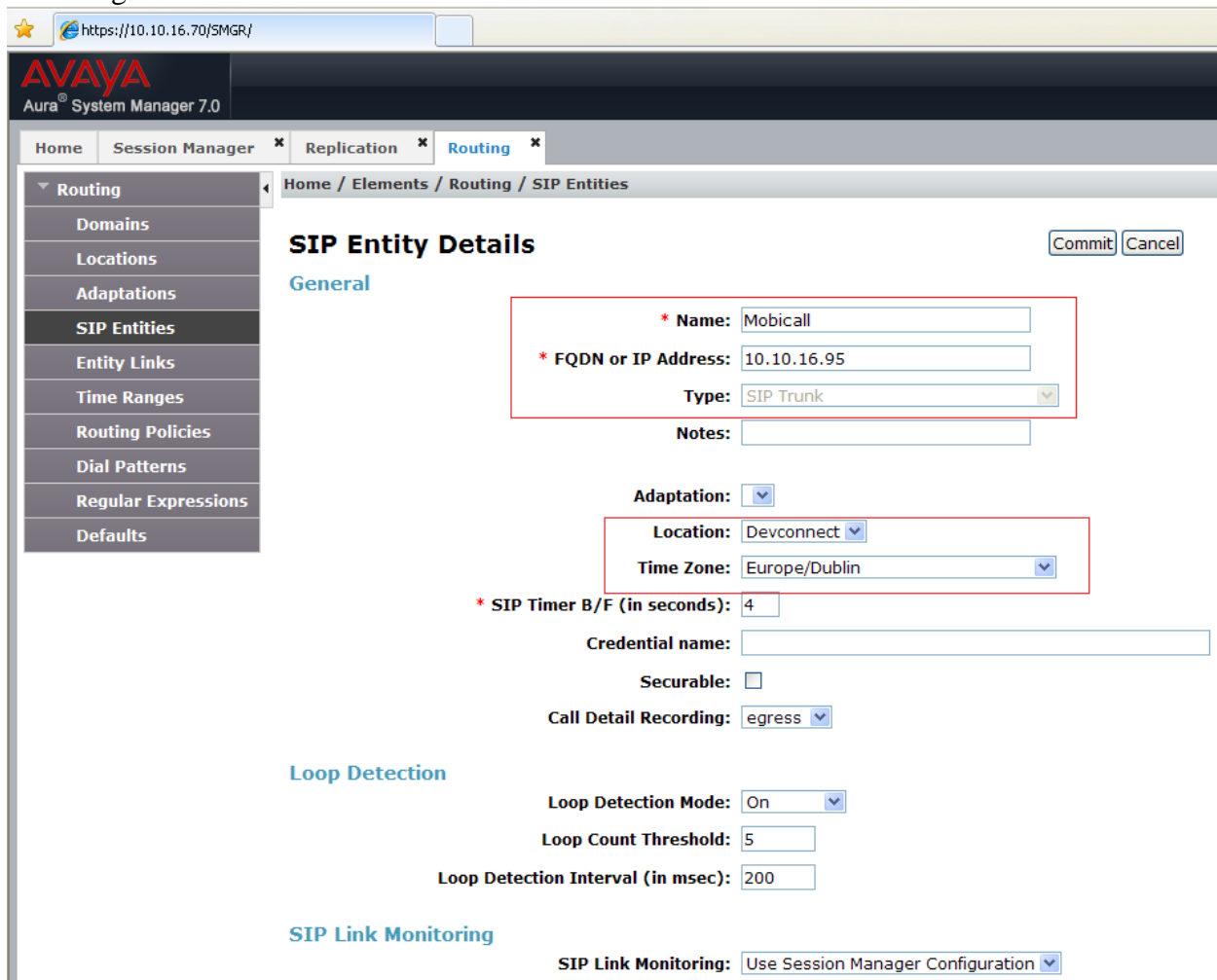
SIP Entities

New Edit Delete Duplicate More Actions

11 Items

Name	FQDN or IP Address
------	--------------------

Enter a descriptive **Name** and the **IP Address** of the Mobicall Server. Set **Type** as **SIP Trunk** and choose a **Location** and **Time Zone** from the drop down menus. Click on **Commit** to save the changes.



AVAYA
Aura® System Manager 7.0

Home Session Manager Replication Routing

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* Name: Mobicall

* FQDN or IP Address: 10.10.16.95

Type: SIP Trunk

Notes:

Adaptation:

Location: Devconnect

Time Zone: Europe/Dublin

* SIP Timer B/F (in seconds): 4

Credential name:

Securable:

Call Detail Recording: egress

Loop Detection

Loop Detection Mode: On

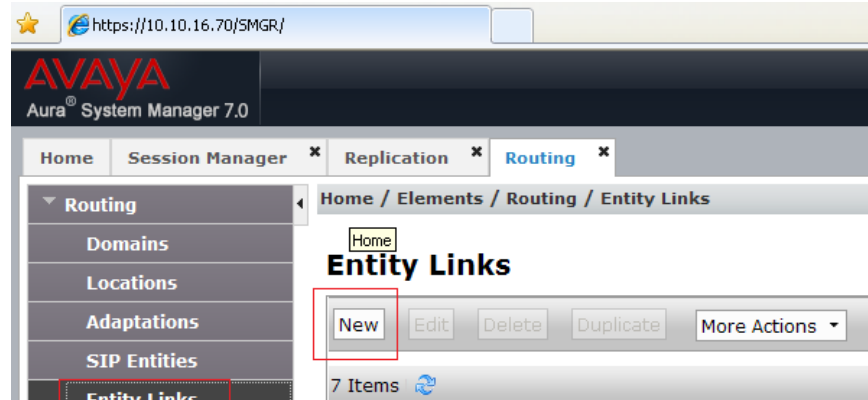
Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

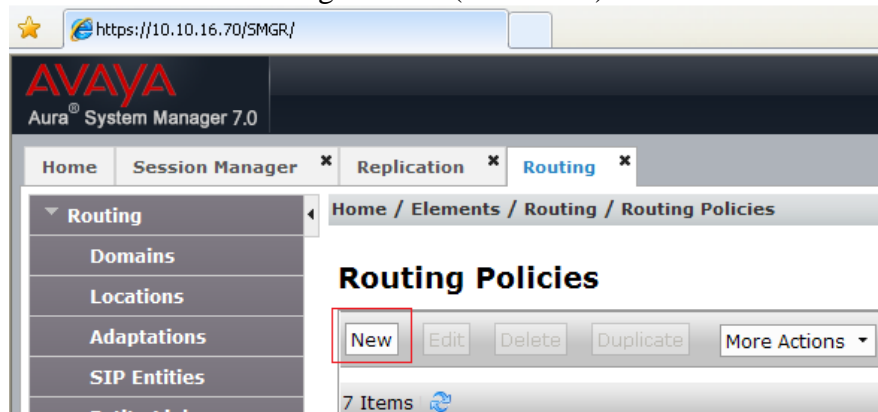
Next add an Entity link between the Mobicall and Session Manager entities. Select **Entity Links** from the left hand menu and click on **New**.



Enter a descriptive **Name** and then select the Session Manager as **SIP Entity 1** from the drop down. Select the **Mobicall** entity as **SIP Entity 2**. Select the **Protocol** administered on the mobicall server. **TCP** was used during testing. The ports will automatically change to the default **5060**. Click on **Commit** to save changes.



From the left hand menu select Routing Policies (not shown) and click on **New**.



Enter a descriptive **Name** and under **SIP Entity as Destination** click on **Select**.

Routing Policy Details

General

Name: Mobicall_RP

Disabled: ☐

Retries: 0

Notes: Additional notes with max. 255 characters.

SIP Entity as Destination

Select

From the list of **SIP Entities** select the **Mobicall** entity and click on **Select** to save changes.

SIP Entities

11 Items

	Name	FQDN or IP Address	Type
<input type="radio"/>	AAEP1620	10.10.16.20	Voice Portal
<input type="radio"/>	AMS1616	10.10.16.16	Media Server
<input type="radio"/>	CM1623	10.10.16.23	CM
<input type="radio"/>	CM1627	10.10.16.27	CM
<input type="radio"/>	EDP1672	10.10.16.73	Engagement Development Platform
<input type="radio"/>	EDP1674	10.10.16.75	Engagement Development Platform
<input checked="" type="radio"/>	Mobicall	10.10.16.95	SIP Trunk

Select Cancel

From the left hand menu select **Dial Patterns** (not shown) and click on **New**.

Dial Patterns

New Edit Delete Duplicate More Actions

Enter the **Pattern** that will route calls to the Mobicall server and set the **Min** and **Max** to the length of the number to be dialed. Under **Originating Location and Routing Policies** click on **Add**.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

General

* Pattern: 8xxxx

* Min: 5

* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

Select **Apply the Selected Routing Policy to All Originating Locations** and under **Routing Policies** select the Mobicall Routing Policy added above.

Home / Elements / Routing / Dial Patterns

Originating Location

Select Cancel

Originating Location

☒ Apply The Selected Routing Policies to All Originating Locations

1 Item

<input checked="" type="checkbox"/>	Name	No
<input type="checkbox"/>	Devconnect	

Select : All, None

Routing Policies

7 Items

<input type="checkbox"/>	Name	Disabled	Destination
<input type="checkbox"/>	AAEP1620_RP	<input type="checkbox"/>	AAEP1620
<input type="checkbox"/>	AMS1616_RP	<input type="checkbox"/>	AMS1616
<input type="checkbox"/>	CM1623_RP	<input type="checkbox"/>	CM1623
<input type="checkbox"/>	CM1627_RP	<input type="checkbox"/>	CM1627
<input checked="" type="checkbox"/>	Mobicall_RP	<input type="checkbox"/>	Mobicall

7. Configure NewVoice Technology MobiCall

Setting up the MobiCall installation is not described here. Please refer to the product documents in **Section 10**. All configuration is carried out in this section using the New Voice Setup Wizard

7.1. SIP Settings

Select **Main Settings**→**Dongle Settings**

Check the licenses on USB Dongle

The minimum required licenses are (1) **NewVoice Tool Version 8.x** with (2) **Number of Lines 2** and (3) **Registered for Types nvtvoip**.

New Voice Setup Wizard

Quick start wizard for MobiCall Alarmserver

Select Settings:

- Main Settings
- Language Settings
- Dongle Settings
- SQL Database Settings
- System and Device Supervision Settings
- Telephony Watchdog Settings
- Backup Settings
- Main Alarm Settings
- Group and Personnel Settings
- Alarm Data Import
- Personnel and Group Data Import
- Interface Settings
- Additional Components (TTS, Localisation, VoiceMail, Hotel)
- Conference Settings
- TMS Settings
- Event and Notification Settings
- Autostart Settings
- Web Server Settings
- Extended and System Settings

Dongle Settings

A dongle is a USB device used to protect our software. To run a MobiCall alarm server you need to connect the dongle to a USB port on the alarmserver.
To activate the dongle, the licence has to be updated with the code received from New Voice. Contact New Voice to receive your dongle update code.

☒ Activate the dongle supervision. If no dongle exists (demo version), deactivate this supervision
If the dongle is removed, following alarm is started: 9860 Dongle WatchDog
☐ Deactivate the dongle supervision alarm until the dongle is connected for the first time

Dongle Information: Refresh

(1) New Voice Tool Version: 8.0 Professional
Registered for Region: Demo Version

(3) Registered for Types: Dialogic (nvtmt) & Diva Server CAPI (nvtcf) & VOIP (nvtvoip) & AI-Logix (nvt)

(2) Number of Lines: 60
Number of Fax-lines: 0
Number of Contacts: 128
Number of Relais: 8
Number of Interfaces: 4
Text to Speech: 1

3G-4G Server for OS: iOS & Android & Blackberry & W-Mobile
Number of Clients: 10

Web Interface Packages: Mobilization & Conference & Group Organizer & Messenger & IVR & Playback & Visualizer

Web Interface Features: Extended Rights Management

Dongle Serial Number: Hex: A96E Dec: 43374 Update License

Previous Next OK Apply Cancel

Select Main Settings

Select Use VOIP over Network Connection for Calls. Set Number of VOIP Lines / Channels up to the licensed number

New Voice Setup Wizard

Quick start wizard for MobiCall Alarmserver

Select Settings:

- Main Settings
- Language Settings
- SIP Settings
- Line / Channel Settings
- Call Settings
- Dongle Settings
- SQL Database Settings
- System and Device Supervision Settings
- Telephony Watchdog Settings
- Backup Settings
- Main Alarm Settings
- Group and Personnel Settings
- Alarm Data Import
- Personnel and Group Data Import
- Interface Settings
- Additional Components (TTS, Localisation, VoiceMail, Hotel)
- Conference Settings
- TMS Settings
- Event and Notification Settings
- Autostart Settings
- Web Server Settings
- Extended and System Settings

General Settings

Activate the lines for outgoing and incoming phone calls. The number of available lines depends on the number of lines configured in your licence.
For ISDN calls a voice adapter needs to be existent and the correct drivers installed

☐ Use Voice Adapters for Calls (using PCI boards)

☒ Connected to PBX by ISDN / Q.SIG channels

☐ Connected to PBX by analog lines

Number of Voice Lines / Channels: 0

☒ Use VOIP over Network Connection for Calls (H.323 / SIP)

Number of VOIP Lines / Channels: 8

☐ Use the H323 protocol for Voip calls

☒ Use the SIP protocol for Voip calls

VOIP Protocol for default Route: SIP

☐ Activate CSTA Connection for special PBX Features (if supported) CSTA Settings

☐ Activate virtual NVE Lines for Offline processing (nvtme.exe)

Number of NVE Lines: 0

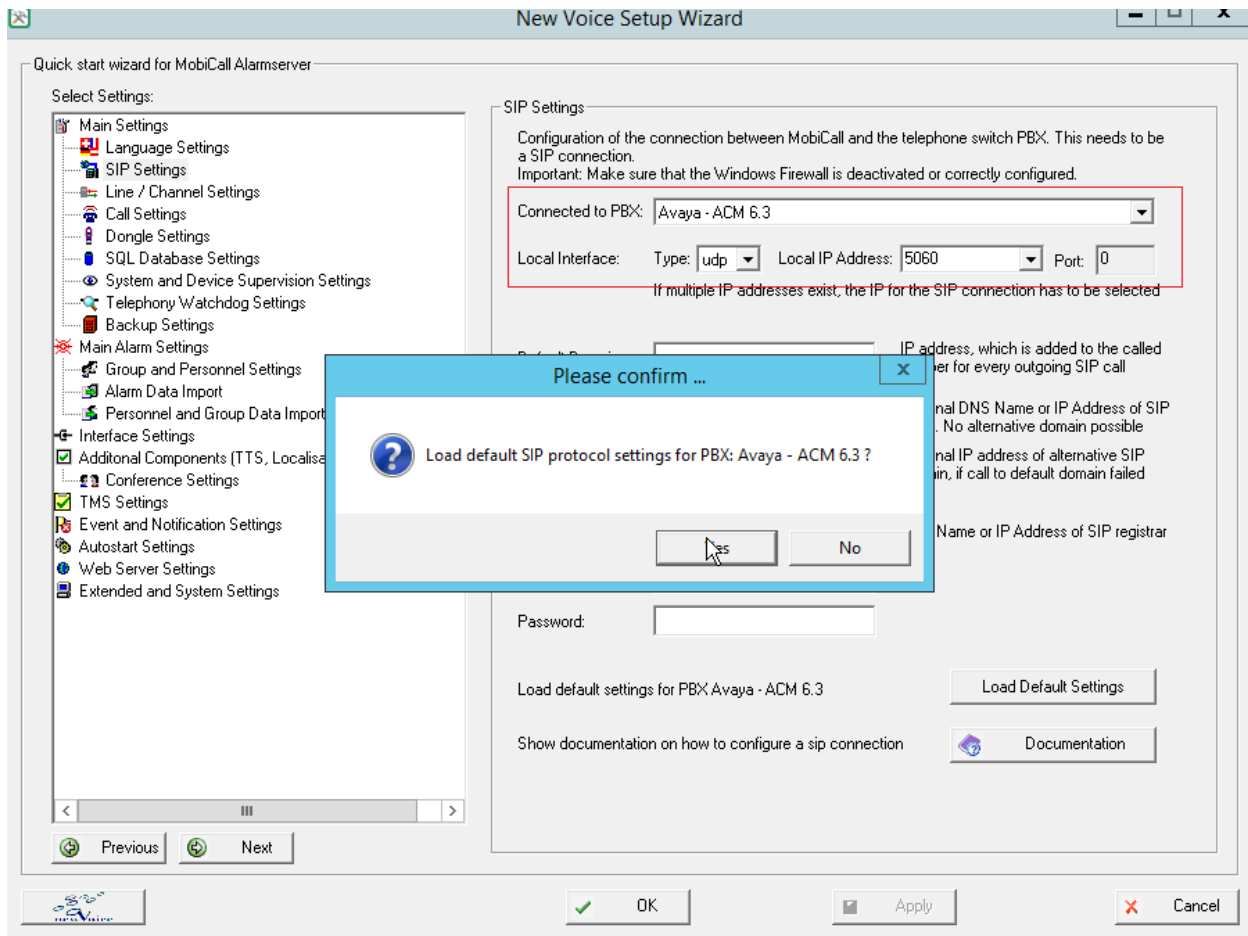
Previous Next

OK Apply Cancel

Select **Main Setting**→**SIP Settings**

Select Avaya-ACM 6.3 from the Connected to PBX drop down. When asked to Confirm click on **Yes**.

If there is no exact entry for the pbx software version, select the one below.



When the Profile is loaded enter the following required settings

- **Local Interface Type: tcp**
- **Local Interface IP Address: IP Address of MobiCall**
- **Local Interface Port: 5060**
- **Default Domain: IP Address of Avaya Session Manager**

Quick start wizard for MobiCall Alarmserver

Select Settings:

- Main Settings
- Language Settings
- SIP Settings**
- Line / Channel Settings
- Call Settings
- Dongle Settings
- SQL Database Settings
- System and Device Supervision Settings
- Telephony Watchdog Settings
- Backup Settings
- Main Alarm Settings
- Group and Personnel Settings
- Alarm Data Import
- Personnel and Group Data Import
- Interface Settings
- Additional Components (TTS, Localisation, VoiceMail, Hotel)
- Conference Settings
- TMS Settings
- Event and Notification Settings
- Autostart Settings
- Web Server Settings
- Extended and System Settings

SIP Settings

Configuration of the connection between MobiCall and the telephone switch PBX. This needs to be a SIP connection. Important: Make sure that the Windows Firewall is deactivated or correctly configured.

Connected to PBX: Avaya - ACM 6.3

Local Interface: Type: tcp Local IP Address: 10.10.16.95 Port: 5060
If multiple IP addresses exist, the IP for the SIP connection has to be selected

Default Domain: 10.10.16.27 IP address, which is added to the called number for every outgoing SIP call

☐ SIP Proxy: Optional DNS Name or IP Address of SIP proxy. No alternative domain possible

Alternative Domain: Optional IP address of alternative SIP domain, if call to default domain failed

SIP Registrar: DNS Name or IP Address of SIP registrar

User Name:

Password:

Load default settings for selected PBX Load Default Settings

Show documentation on how to configure a sip connection Documentation

Previous Next OK Apply Cancel

Select **Main Alarm Settings**

Select **Use Calling party number for outgoing calls** and enter and unused extension on the Communication Manager

General Settings

Alarm Server - General Settings

Program Language: English

First Alarm Number: 2000 First Entry Number (DDI): 10

Last Alarm Number: 9999 Last Entry Number (DDI): 1999

ISDN / Analog Connection

Connected to PBX: [Empty]

☒ Connected to PBX by ISDN (PRI / BRI) **ISDN Settings**

☐ Connected to PBX by Analog Lines

VOIP Connection by H.323 or SIP

Connected to PBX: Avaya - ACM 6.3

Settings for VOIP Connection and Gatekeeper **VOIP Settings**

CSTA Connection Settings

☐ Activate CSTA Connection for special PBX Features (if supported) **CSTA Settings**

Global Call Settings

Prefix for External Calls: 0 ☐ Use line specific prefixes to override default prefix **Settings**

Prefix for GSM Calls: 0 ☐ Use line specific prefixes to override default prefix **Settings**

☒ Use calling party number for outgoing calls: 8270003

☐ If alarm was launched by phone, use the caller number as calling party number for all outgoing calls

☐ Only send calling party number for external calls (phonetype EXT and GSM)

☐ Set number type plan for outgoing calls. Use default type: [Empty]

OK **Cancel**

7.2. Feature activation and configuration

All configuration in this section is carried out using the New Voice Alarm Central

Select **Main Settings**→ **VOIP Settings**

Activate the following features as shown.

- **Use Protocol as default Route**
- **Use the SIP Protocol for VOIP Calls**
- **The Three Activate Alarm options**

Use Protocol as default Route:

☐ Use the H323 Protocol for VOIP Calls

☐ Specific local IP Address: Only needed if more than one IP addresses are defined for this server

☒ Use Gatekeeper on IP Address: If the gatekeeper is running on the local server, check that gnugk.exe is enabled in autostart. For multiple IP addresses specify the correct IP and not the localhost IP (127.0.0.1)

User Name for Gatekeeper:

Password for gatekeeper:

Prefixes for incoming calls: Specify all prefixes which are routed to the mobinet server. Use a , to separate the prefixes

☒ Use the SIP Protocol for VOIP Calls

Local Interface: Format: <Protocol Type>\$<IP Address>:<Port Number>
Example: udp\$10.97.16.37:5060

Default SIP Domain: IP or DNS, which is added to the called number for every outgoing SIP call

☐ Optional SIP Proxy: Optional IP or DNS name of the SIP proxy server. In doubt, leave empty

Alternative SIP Domain: Optional IP or DNS of alternative SIP domain, if call to default domain failed

Multiple Connections to SIP Hosts:

SIP Registrar (DNS Name or IP):

User Name: Password:

☒ Activate alarm option for forced release if the called number is busy, if it is supported by the PBX.
If the internal phone number is busy, the connection is disconnected and the alarm call is repeated.

☒ Activate alarm option for intrusion if the called number is busy, if it is supported by the PBX.
If the internal phone number is busy, the intrusion message is played into the connection and the alarm call is repeated

☒ Activate alarm option for broadcast call, if it is supported by the PBX.
The loudspeaker is opened with internal call and the alarmmessage is played immediately

Extended VOIP settings for advanced users

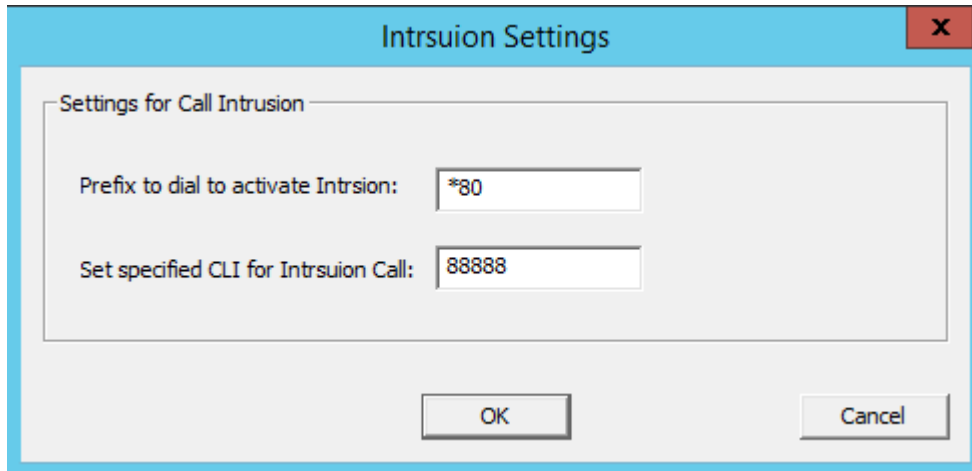
Load the default configuration settings for the selected PBX

)

Select Main Settings → VOIP Settings → Intrusion Settings

Set Prefix to dial to activate Intrusion: section 5: *change feature-access-codes*

Set specified CLI for Intrusion Call: section 5: *off-pbx-station-mapping*



The image shows a screenshot of a software dialog box titled "Intrusion Settings". The dialog has a blue header bar with the title and a red close button (X) on the right. Below the header is a light gray area containing a sub-section titled "Settings for Call Intrusion". Inside this sub-section, there are two text input fields. The first field is labeled "Prefix to dial to activate Intrusion:" and contains the text "*80". The second field is labeled "Set specified CLI for Intrusion Call:" and contains the text "88888". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

8. Verification Steps

This section describes the checks that can be carried out to verify the connection between Mobicall and Communication Manager.

8.1. Session Manager

Select Elements → Session Manager from the Home screen (not shown) and click on the value under Entity Monitoring

The screenshot shows the Session Manager Dashboard. The left sidebar contains a navigation menu with options like Session Manager, Administration, Communication, Profile Editor, Network, Configuration, Device and Location, Application, System States, and SIP Entity. The main content area is titled 'Session Manager Dashboard' and includes a section for 'Session Manager Instances'. A table lists the instances, with one instance 'SM1676' highlighted. The 'Entity Monitoring' column for SM1676 shows '2/7' in red, indicating a warning. A red box highlights the 'Entity Monitoring' column header and the '2/7' value. A tooltip at the bottom right of the table reads: 'Monitoring status entity down links/total links, click to review down links'.

Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	License Mode
2/7	0	3/3		✓	Normal

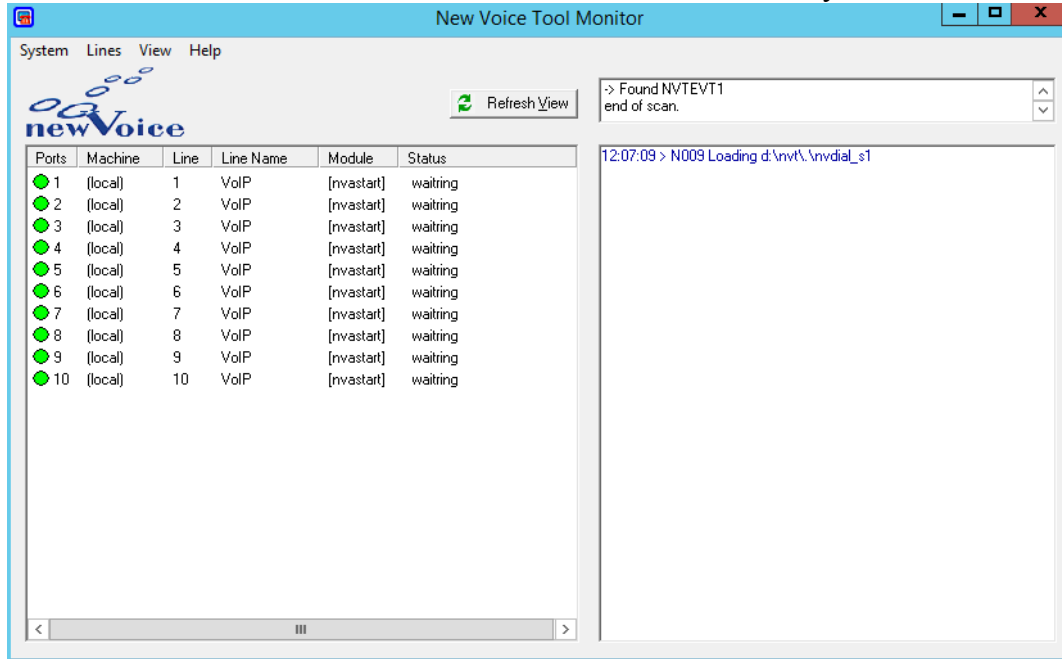
Verify that the Mobicall entry is UP.

<input type="radio"/> MSG1689	10.10.16.89	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/> SM214	10.10.16.214	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/> CM1627	10.10.16.27	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/> Mobicall	10.10.16.95	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/> CM1623	10.10.16.23	5060	TCP	FALSE	UP	200 OK	UP

8.2. MobiCall Line Monitor and Dial utility

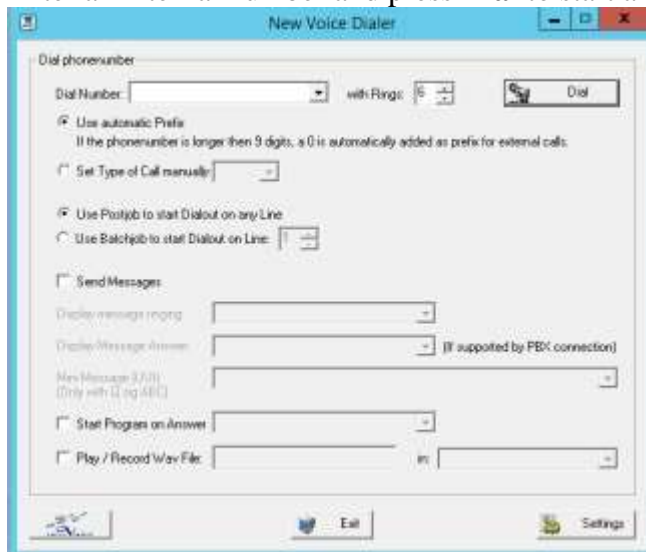
Newvoice Tool Monitor can be found as shortcut on the desktop.

A successful communication between MobiCall and the Session Manager can be verified via the tools “NewVoice Tool Monitor” and the “NewVoice Dial Utility”



Alarmcentral – Extras – Dial Utility

Enter an internal number and press **Dial** to start an outgoing call



9. Conclusion

These Application Notes describe the configuration steps required for New Voice Technologies Mobicall to interoperate with Avaya Aura® Communication Manager using Avaya Aura® Session Manager. All feature functionality and serviceability test cases were completed successfully as outlined in Section 2.2.

10. Additional References

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

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

- [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] *Administering Avaya Aura® Session Manager*, Release 6.3, 03-603324

Product documentation for NewVoice Technologies MobiCall can be obtained by visiting the following website www.mobilisierung.com

©2015 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.