Avaya Solution & Interoperability Test Lab

Application Notes for Configuring ATT-AudioText Telecom AG Alarm Management Server with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager R7.0 – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning ATT-AudioText Telecom AG Alarm Management Server to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any 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 for ATT-AudioText Telecom AG Alarm Management Server to successfully interoperate with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager R7.0. The ATT-AudioText Telecom AG Alarm Management Server (ATT AMX) generates preconfigured or ad hoc alarms which were signalled to Communication Manager as calls via a SIP Trunk between the ATT-AudioText Telecom AG Alarm Management Server and Avaya Aura® Session Manager.

2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of The ATT AMX server to send an Alarm notification both orally and visually to various Avaya endpoints. For the conformance tests described by these Application Notes, ATT AMX Alarm Management Server and Communication Manager were configured to operate a follows:

- Each alarm consisted of an audio message and a text message. The text message was sent as the calling party name (which can have a maximum length of fifteen characters) and was thus visible for alarms to local extensions and DECT endpoints (but not PSTN endpoints).
- Alarms were also configured such that the alarm recipient must acknowledge via keypad input, thus preventing alarms which were answered by voicemail systems from being considered as delivered.

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 compliance testing included the test scenarios shown below. Note that when applicable, all tests were performed with Avaya SIP deskphones, Avaya H.323 deskphones and PSTN endpoints.

- Alarm creation via text-to-speech and via telephone input
- Alarm delivery to idle station
- Alarm to busy station
- Alarm to station, no answer
- Alarm to station with coverage enabled, no answer
- Alarm to station with call forwarding enabled
- Alarm to unavailable station
- Alarm to tandem station
- Alarm to hunt group
- Alarm to multiple endpoints
- Automatic startup after power interruption
- Recovery from interruption to interface to PBX

2.2. Test Results

The following observations were noted during testing.

- If a local fixed extension which has no available call appearance receives an incoming alarm call, the caller receives a “busy” indication: it makes no difference if it is a “priority” call.
- If an alarm call is made to a diverted (call forwarding) station, the call is diverted: it makes no difference if it is a “priority” call.
- If the ATT AMX Alarm Management Server is disconnected from its LAN interface, no alarms will be generated. The unit continues normal operation when the LAN interface is reconnected.

2.3. Support

Support from Avaya is available by visiting the website http://support.avaya.com and a list of product documentation can be found in **Section 10** of these Application Notes.

Product information and support for ATT AG products may be found at:

- Website: www.attag.ch
- Help desk: +41 (0)44 908 60 04

3. Reference Configuration

Figure 1 shows the network topology during compliance testing. The ATT AMX server is connected to the telephony LAN and registers with Session Manager in order to be able to send alarms to the Avaya H.323 and SIP deskphones on Communication Manager.

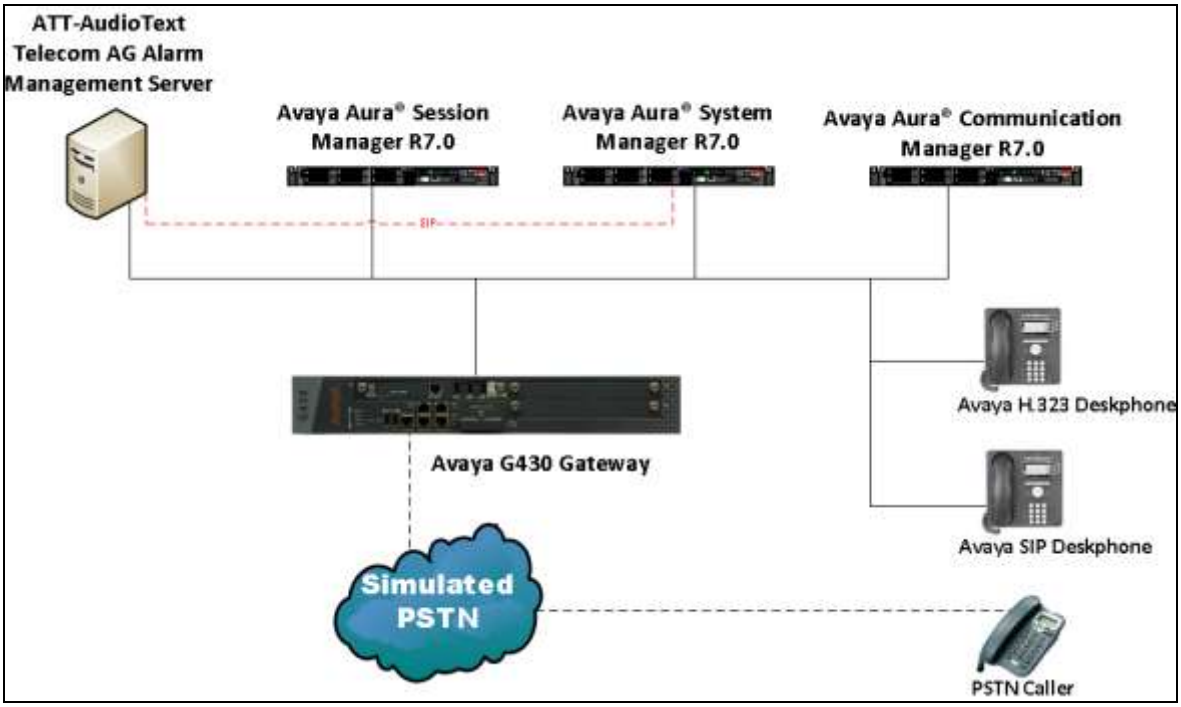


Figure 1: Network Solution of ATT-AudioText Telecom AG Alarm Management Server with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager R7.0

4. Equipment and Software Validated

The following equipment and software was used for the compliance test.

Equipment/Software	Version/Release
Avaya Aura® System Manager running on an Avaya S8800 Server	R7.0.0.1 Build 7.0.0.0.16266-7.0.9.7001011 Software Update Revision 7.0.0.1.4212
Avaya Aura® Communication Manager running on an Avaya S8800 Server	R7.0 SP1 Build 7.0.0.1.0.441.22477 Software Update Revision PLAT-rhel6.5-0010
Avaya G430 Media Gateway	37.20.0
Avaya Aura® Session Manager running on an Avaya S8800 Server	R7.0 SP1 7.0.0.1.700102
Avaya 9611G H.323 Deskphone Avaya 9641G H.323 Deskphone Avaya 9641G SIP Deskphone Avaya 9611G SIP Deskphone	Release 6.6029 Release 6.6029 Release 6.5.0 Release 6.5.0
ATT-AudioText Telecom AG Alarm Management Server	13.0.4.0

5. Configure Avaya Aura® Communication Manager

It is assumed that a fully functioning Communication Manager is in place with the necessary licensing with a SIP Trunk in place to Session Manager. For further information on the configuration of Communication Manager please see **Section 10** of these Application Notes. The following sections go through the following.

- Dial Plan Analysis
- IP Interfaces
- Network Region
- IP Codec

5.1. Configure Dial Plan Analysis

Use the **change dialplan analysis** command to configure the dial plan using the parameters shown below. Extension numbers (**ext**) are those beginning with **2**, **3**, **4** and **5**. Feature Access Codes (**fac**) use digits **8** and **9** or **#**.

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

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

5.2. Configure IP Interfaces

Shown below is an example of the nodes names used in the compliance testing. The name and IP address of Session Manager is added. Use the **change node-names ip** command to configure the IP address of Session Manager. **SM100** is the **Name** used for Session Manager and **10.10.40.34** is the **IP Address**.

```
change node-names ip                                            Page   1 of   2
                                    IP NODE NAMES
    Name                IP Address
SM100                 10.10.40.34
default               0.0.0.0
G430                  10.10.40.18
procr                 10.10.40.13
procr6                ::
```

5.3. Configure Network Region

Use the **change ip-network-region x** (where x is the network region to be configured) command to assign an appropriate domain name to be used by Communication Manager, in the example below **devconnect.local** is used. Note this domain is also configured in **Section 6.1** of these Application Notes.

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

5.4. Configure IP-Codec-Set

Use the **change ip-codec-set x** (where x is the ip-codec set used) command to designate a compatible codec set. **G.711A** and **G.729A** were used in this test.

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

                           IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711A            n         2        20
 2: G.729A            n         2        20
```

6. Configure Avaya Aura® Session Manager

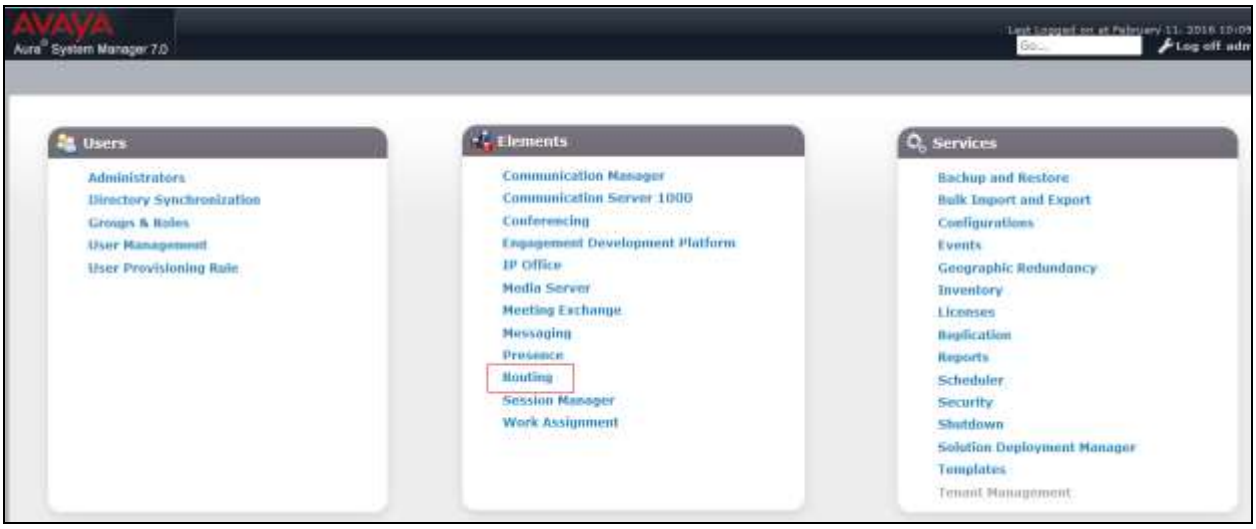
The ATT AMX Server is connected to Session manager as a SIP Trunk. The configuration for this is completed using the System Manager Web interface. The configuration of connections and routing to Communication Manager is out with the scope of this document and is assumed to be in place prior to testing.

6.1. Configuration of SIP Entity and Entity Link

A SIP Entity and Entity link are required in order for the Alarm server to send the alarm message to Communication Manager Stations.

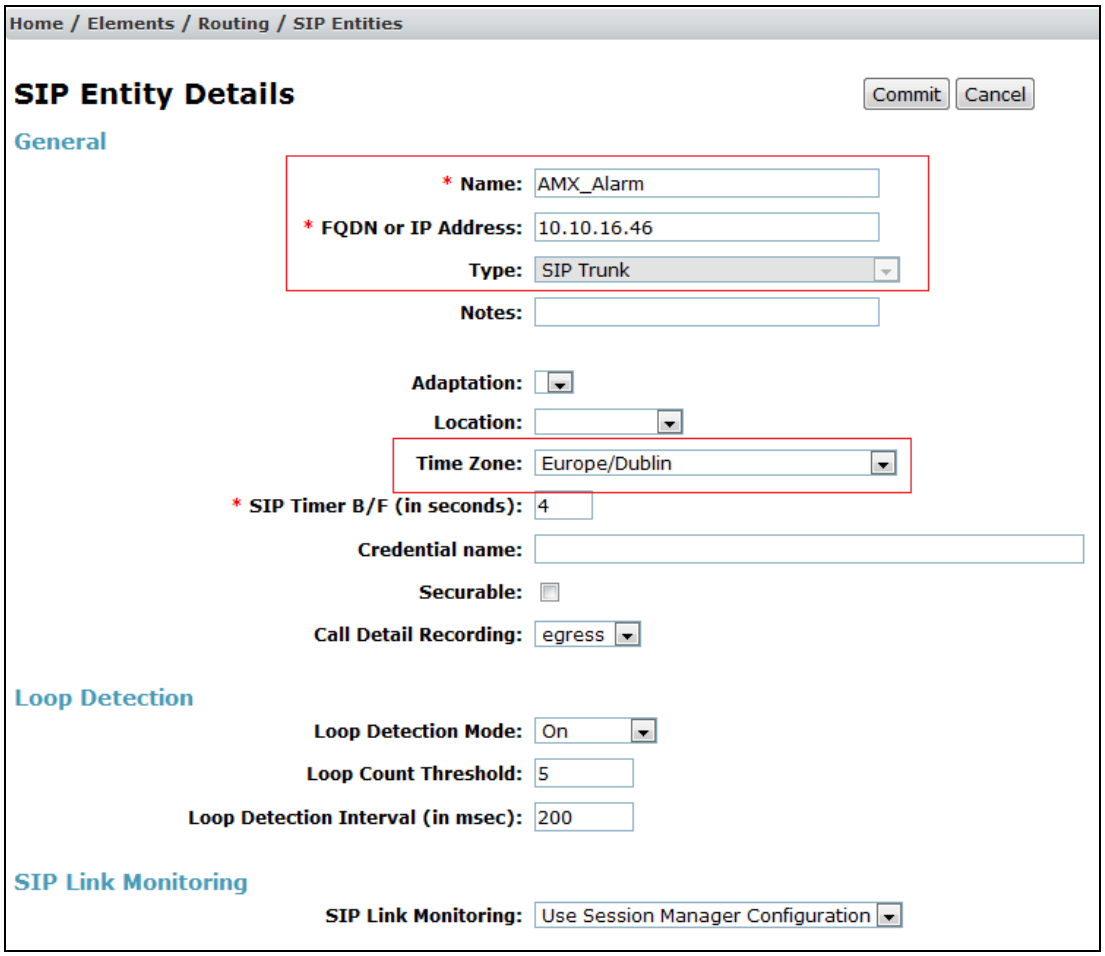
Navigate to http://<System Manager IP Address>/SMGR, enter the appropriate credentials and click on **Log On.**

Once logged in click on **Routing** highlighted below.

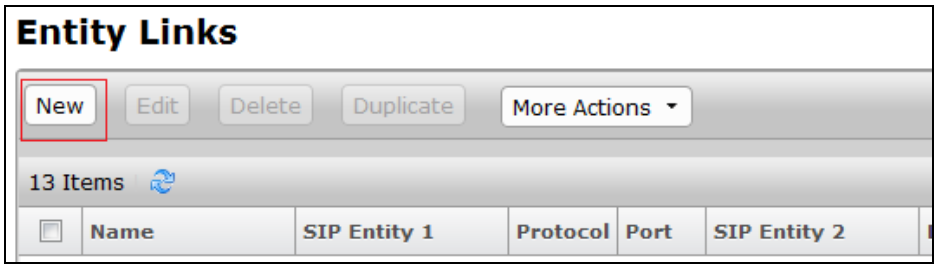


Select **SIP Entities** in the left window (not shown) and click on **New** in the main window.

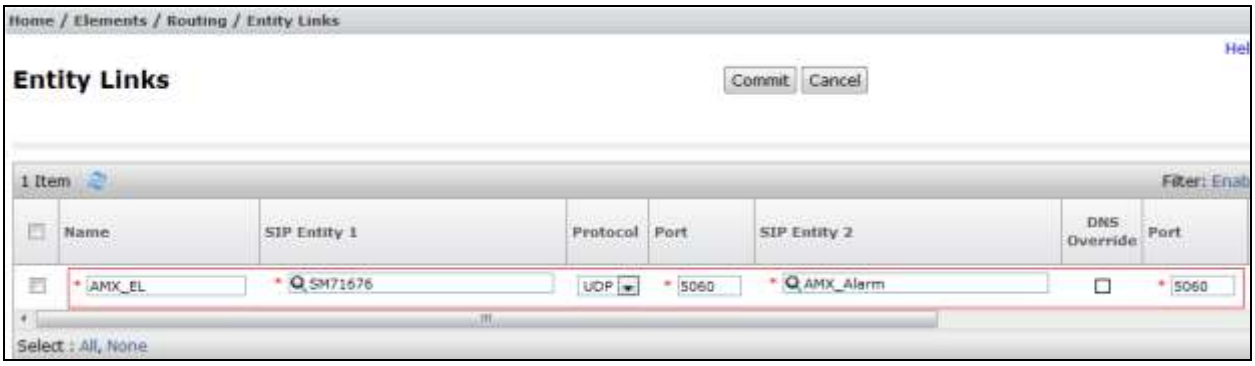
Enter a suitable **Name** and enter the **IP Address** of the ATT AMX Server. Select the **Type: SIP Trunk** and set the **Time Zone:** Click on **Commit** once completed.



Select **Entity Links** from the left window (not shown) and select **New** from the right window in order to add the new ATT AMX Entity Link.



Ensure that **UDP** is selected for the **Protocol** and **5060** for the **Port**. Click on **Commit** once completed.

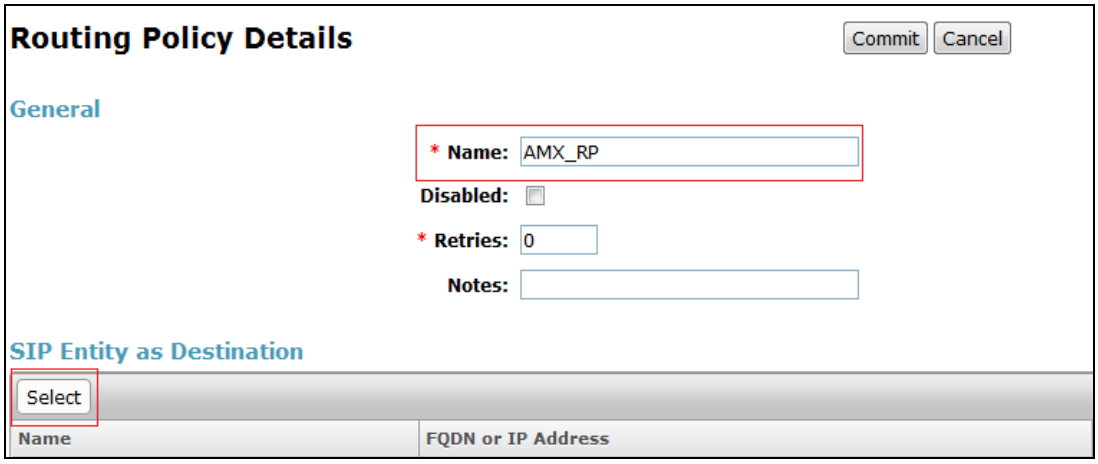


6.2. Configure a Routing Policy and Dial Pattern

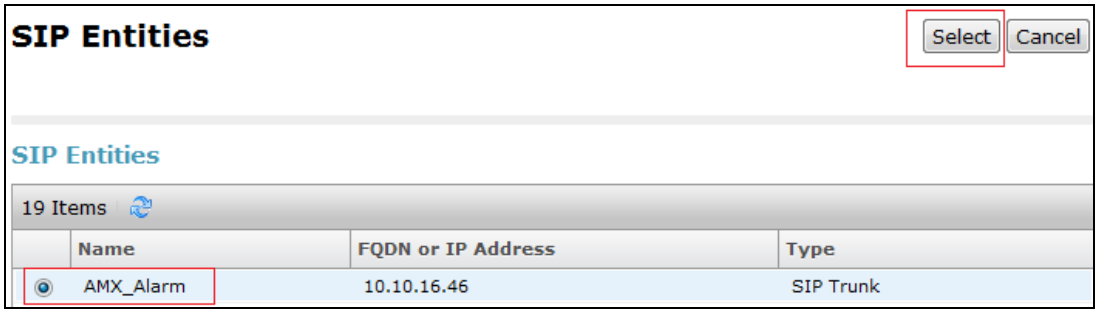
A Routing Policy and Dial are required to create Alarms for distribution to Communication Manager.

From the left hand menu select **Routing Policies** (not shown). Select **New**.

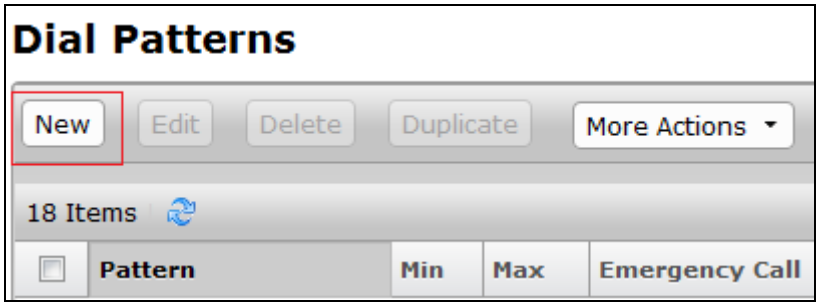
Give the Routing Policy a **Name:** and click **Select** under **Sip Entity as Destination**.



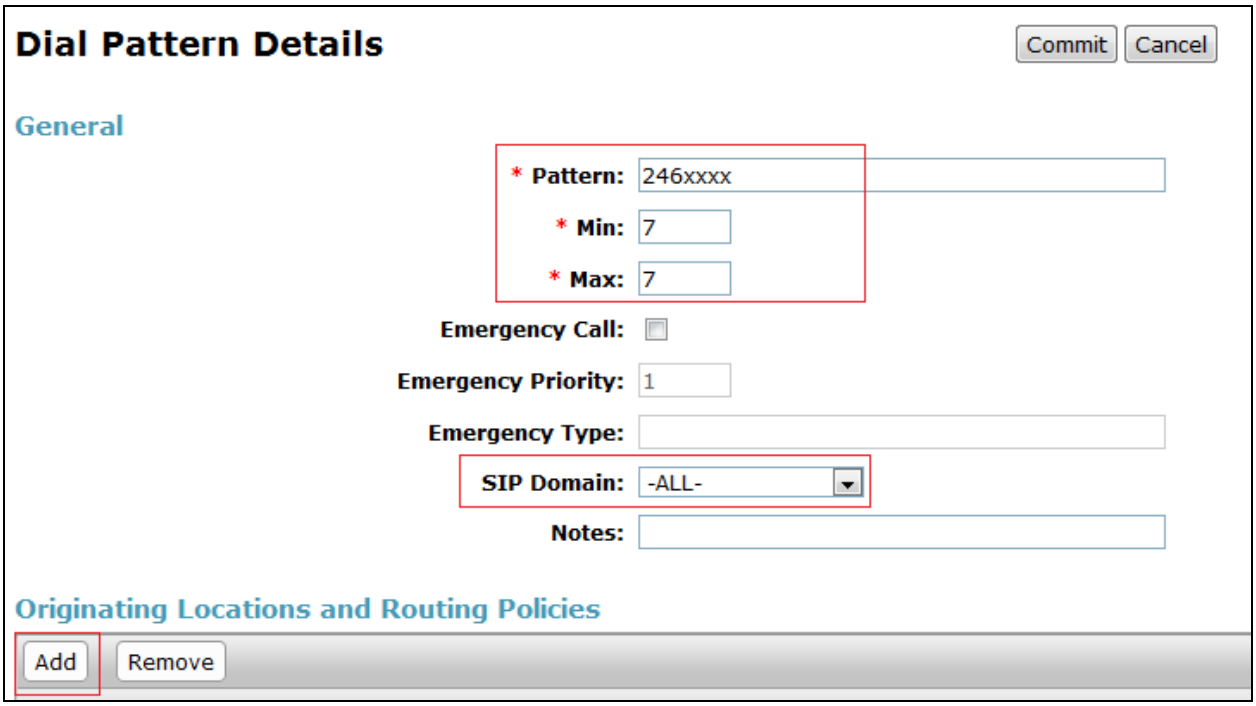
Select the ATT AMX SIP Entity created in **Section 6.1**. Click on **Select** to go back to the Details screen and click **Commit** (not shown) to save changes



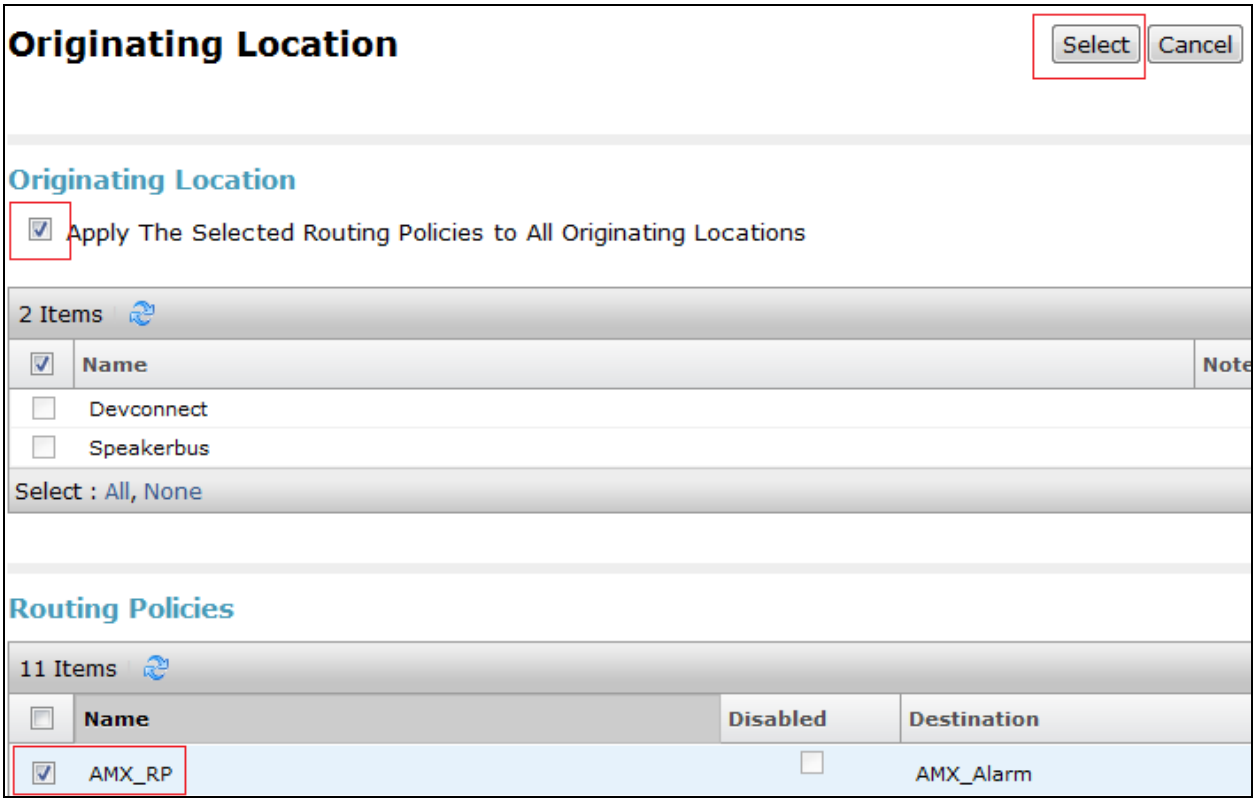
From the left hand menu select **Dial Patterns** (not shown). Select **New**.



Enter the **Pattern:** you want to dial from Communication Manager to record an alarm on ATT AMX and the **Min:/Max:** digits dialled. Select **-ALL-** for the **SIP Domain:** Click **Add** under **Originating Locations and Routing Policies**.



Select **Apply The Selected Routing Policy to All Originating Locations** under **Originating Location** and Select the Routing Policy added above under **Routing Policies**. Click **Select** to go back to the details screen and click **Commit** (not shown) to save changes.

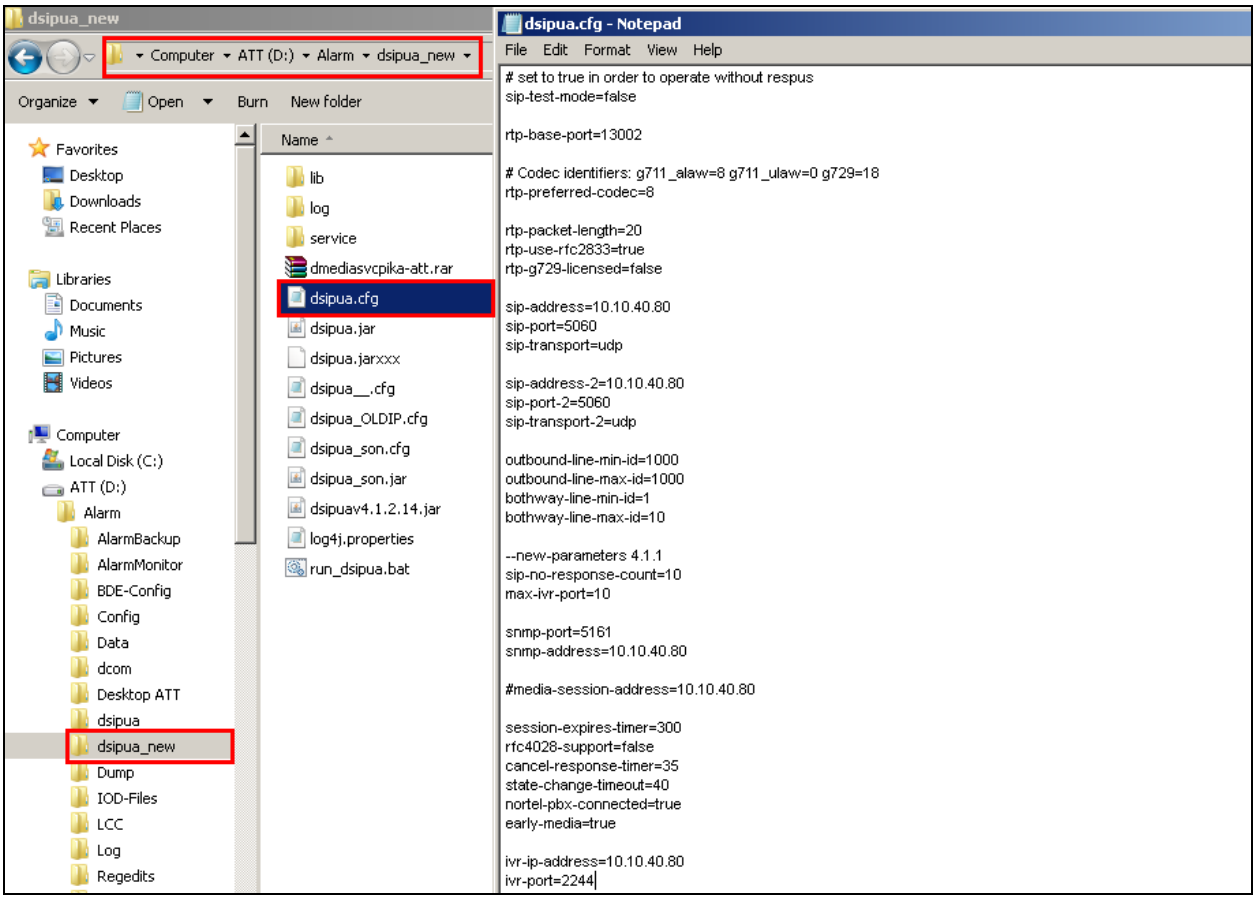


7. Configure ATT-AudioText Telecom AG Alarm Management Server

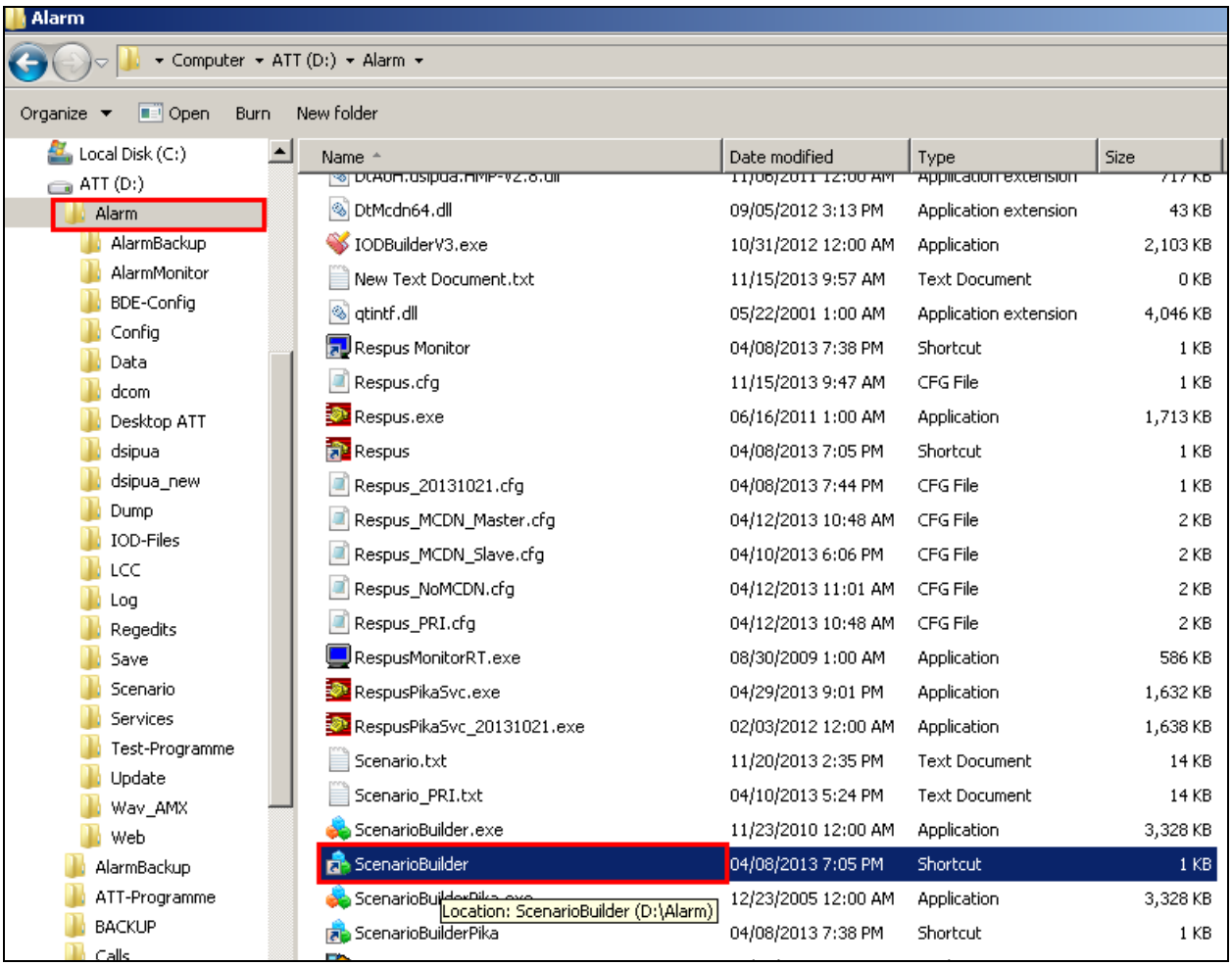
The configuration of the ATT AMX server involves the SIP connection between the AMX Alarm server and Session Manager also the addition of the extension(s) to call on Communication Manager to issue the alarm notification.

7.1. Configuring the SIP connection to Session Manager

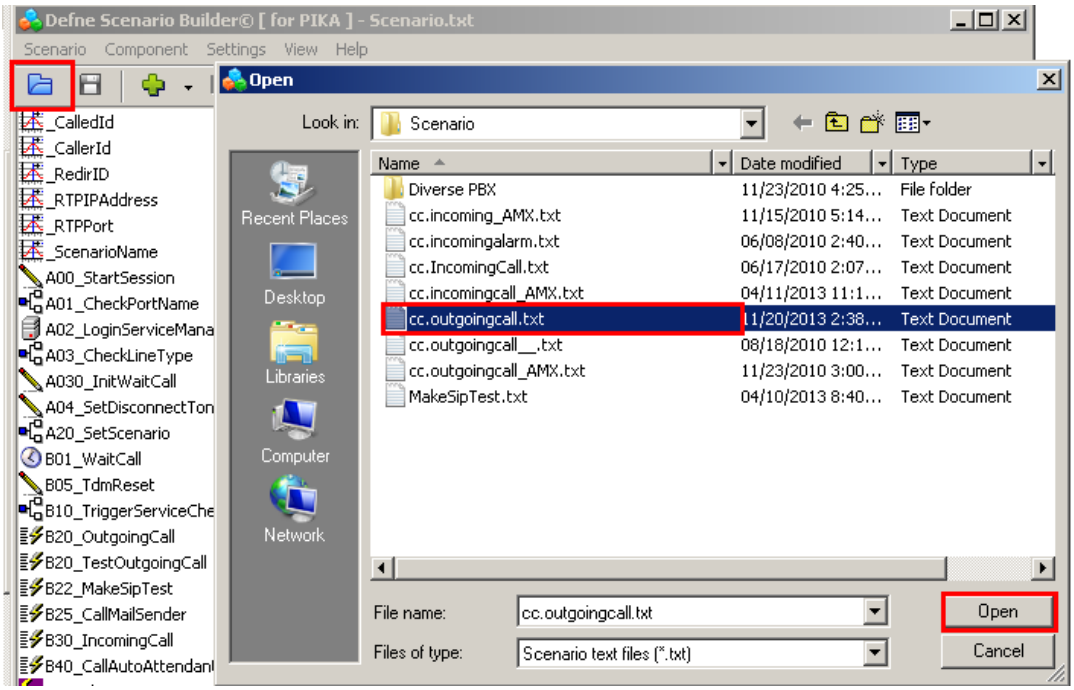
During the initial installation of AMX a folder called Alarm is created. Navigate to **Alarm→dsipua_new** open file called **dsipua.cfg**. Note the address below **10.10.40.80** is the IP address of the AMX server. The **sip-port** used is **5060** and the **sip-transport** is **udp**. All remaining fields were left as default.



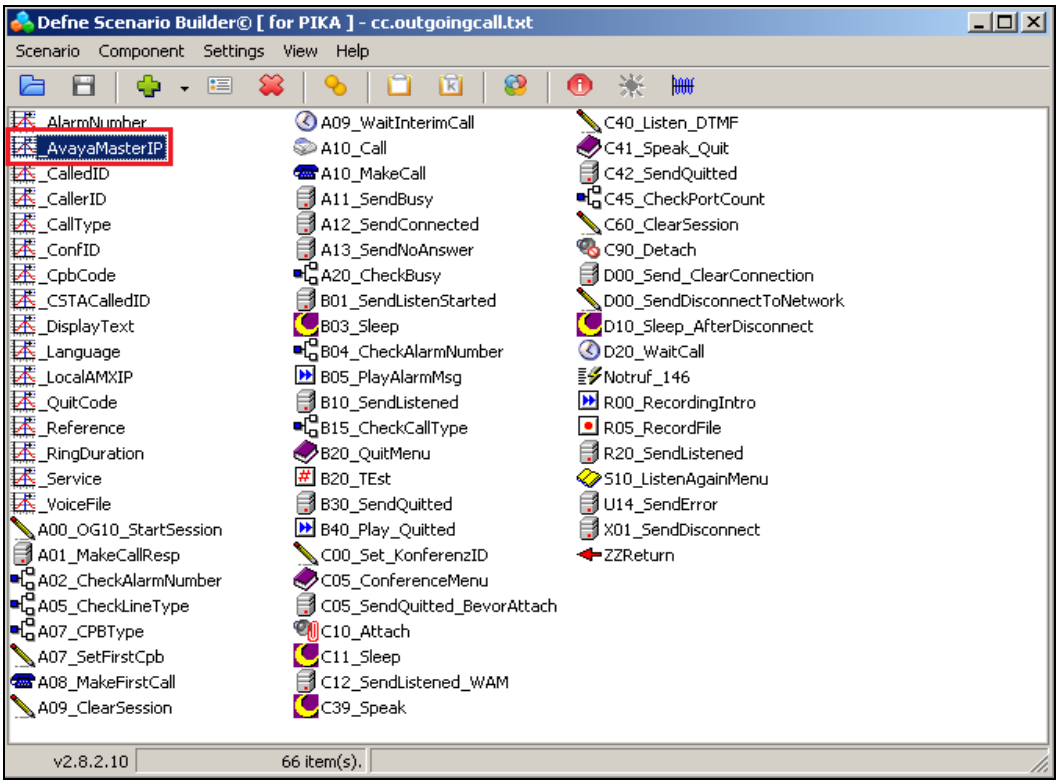
Open **ScenarioBuilder** which is also located in the **Alarm** folder.



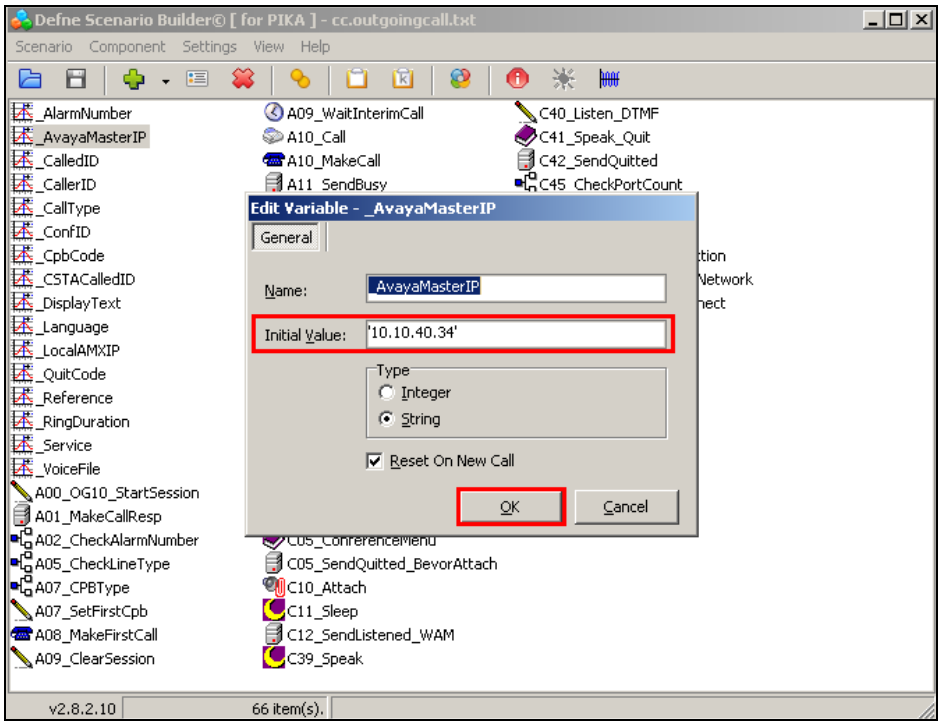
Click on the open icon at the top left of window, this opens the following window where **cc_outgoingcall.txt** is chosen and opened.



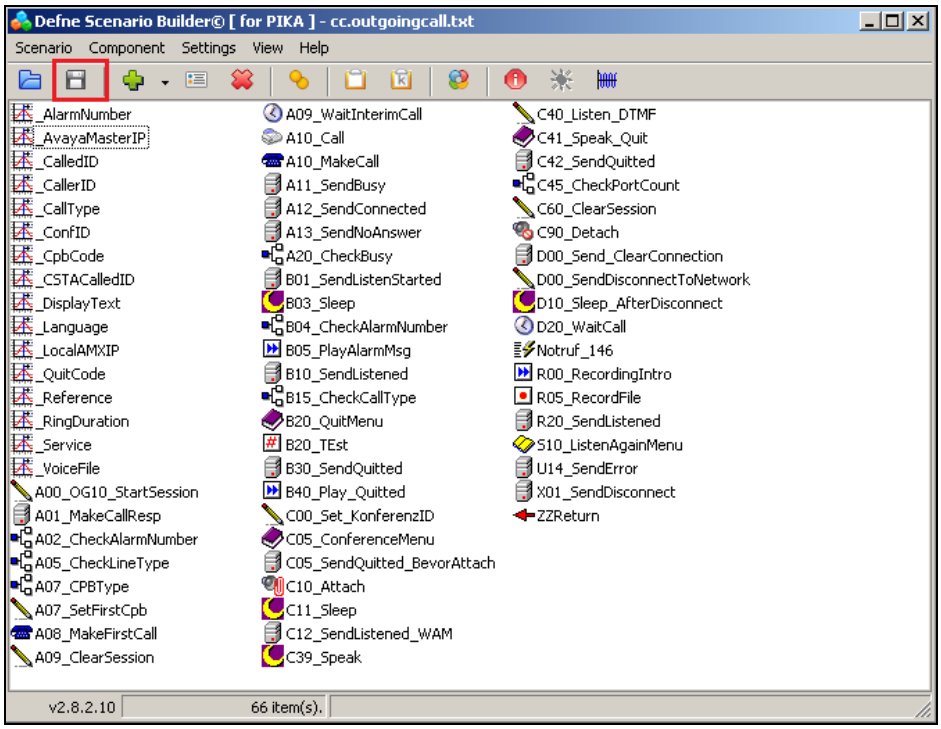
Select **_AvayaMasterIP** from the resulting window below.



Enter the IP address of the Session Manager into the **Initial Value field**. Everything else can be left as default, click on **OK** to continue.

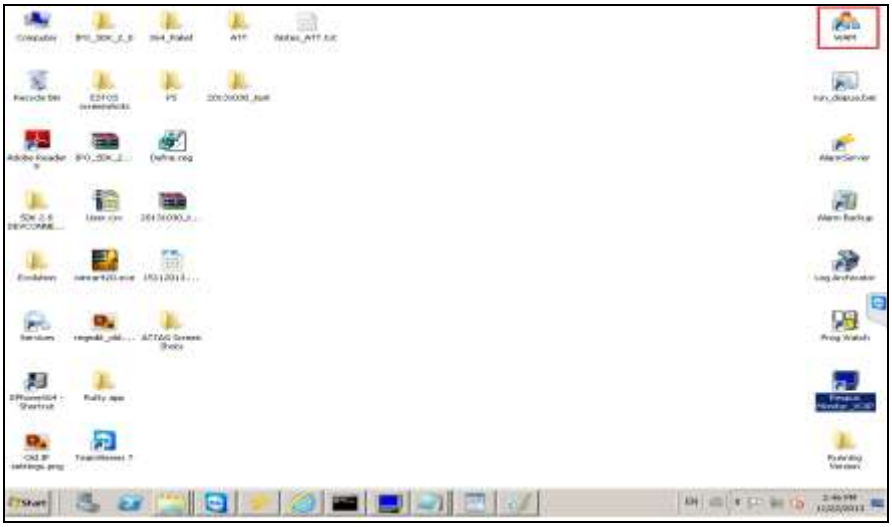


Save this file by clicking on the save icon highlighted

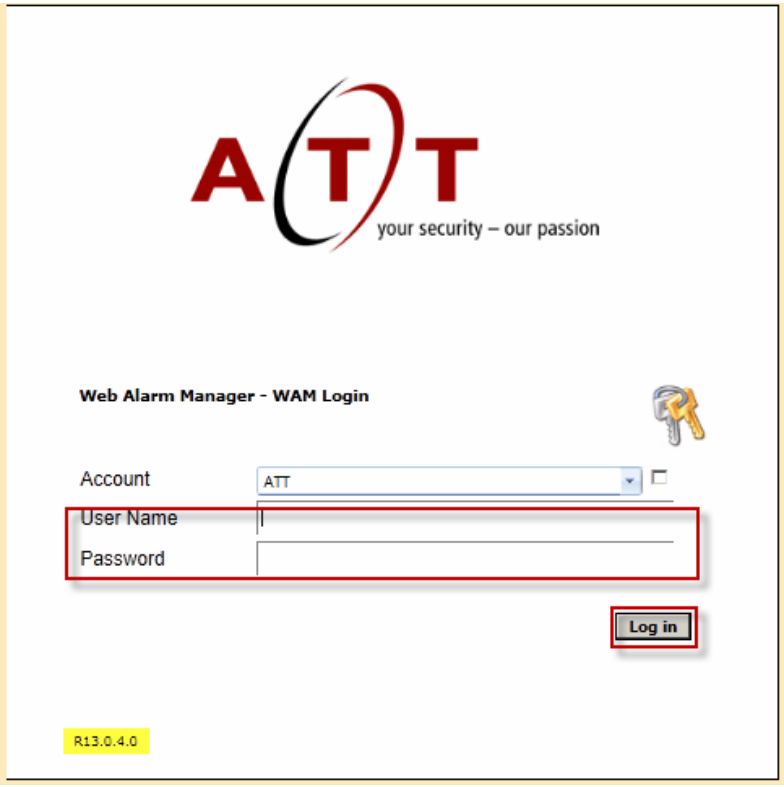


7.2. Adding extensions to call

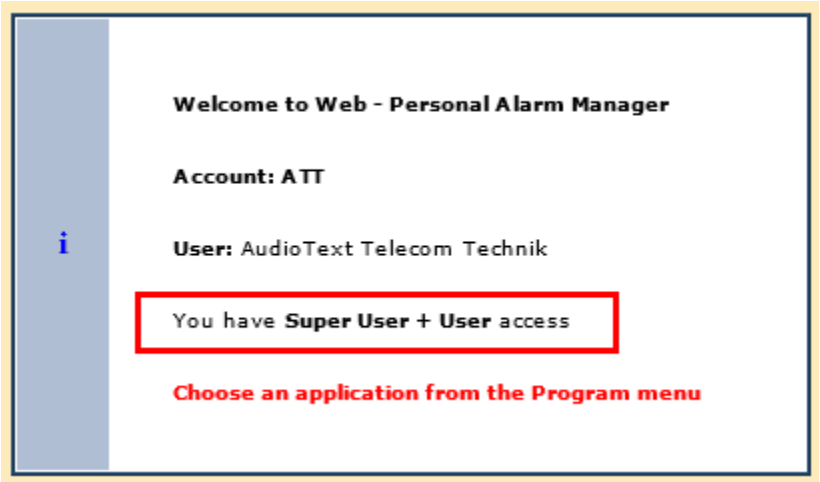
The section describes the steps necessary to create the extension numbers and groups that the Alarm server will call to in the event of an alarm. Open the **WAM** shortcut on the Alarm server desktop.



Enter the proper credentials for a "Super User" and click on Log in to continue.

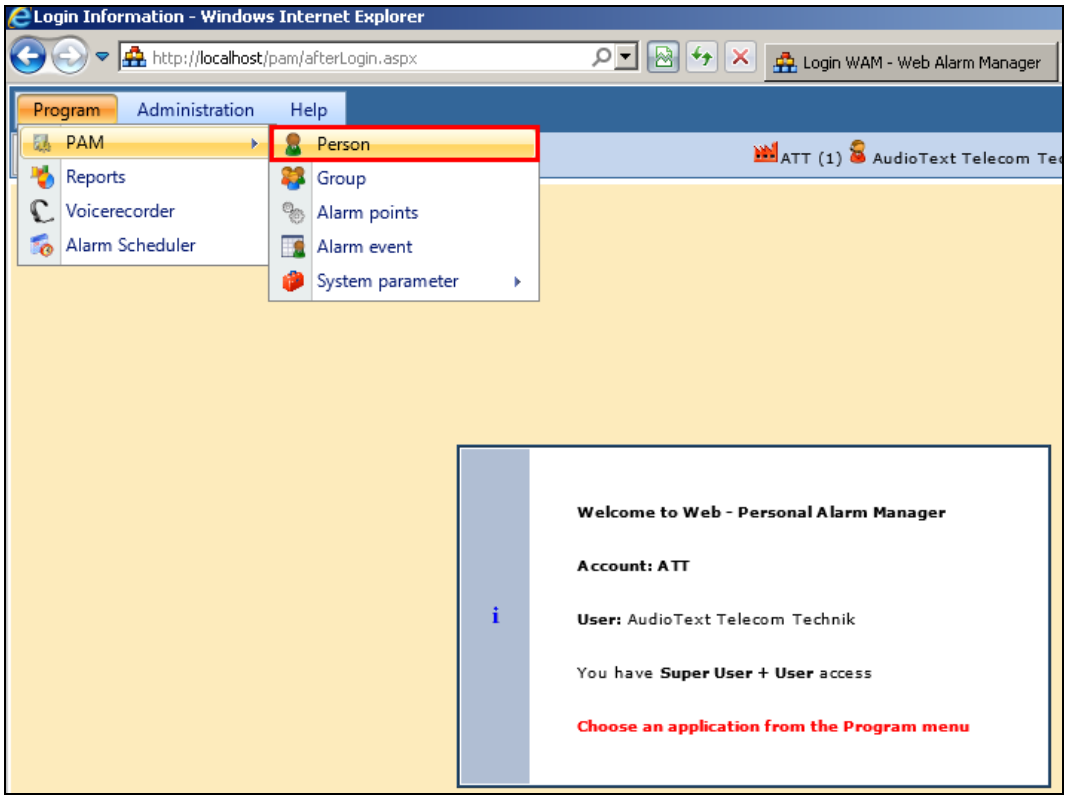


The following screen shows that the user is logged in correctly as a Super User.

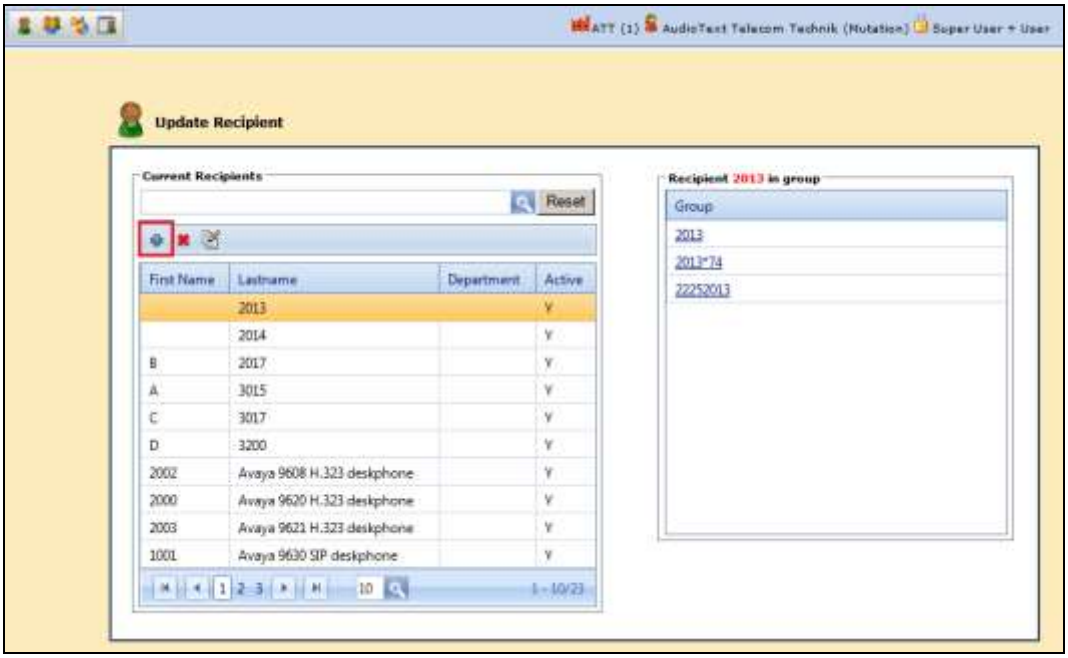


7.2.1. Add a new Person

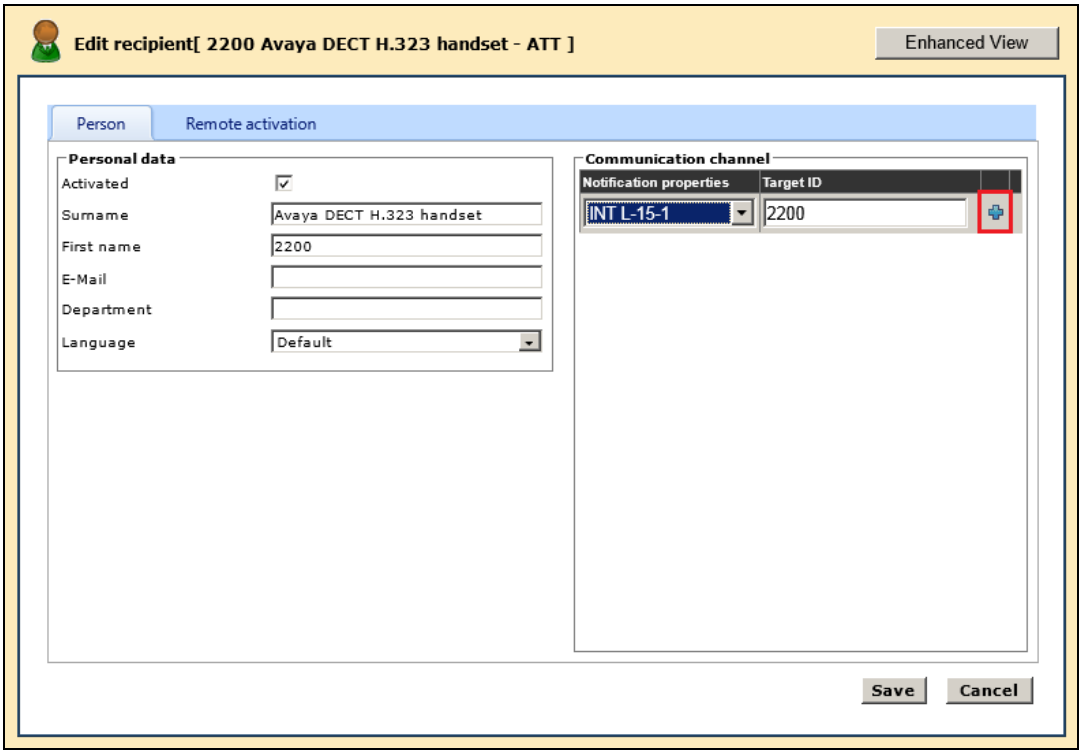
A new extension is represented as a person in the setup. To add a new person, select **Program→PAM→Person** as shown below.



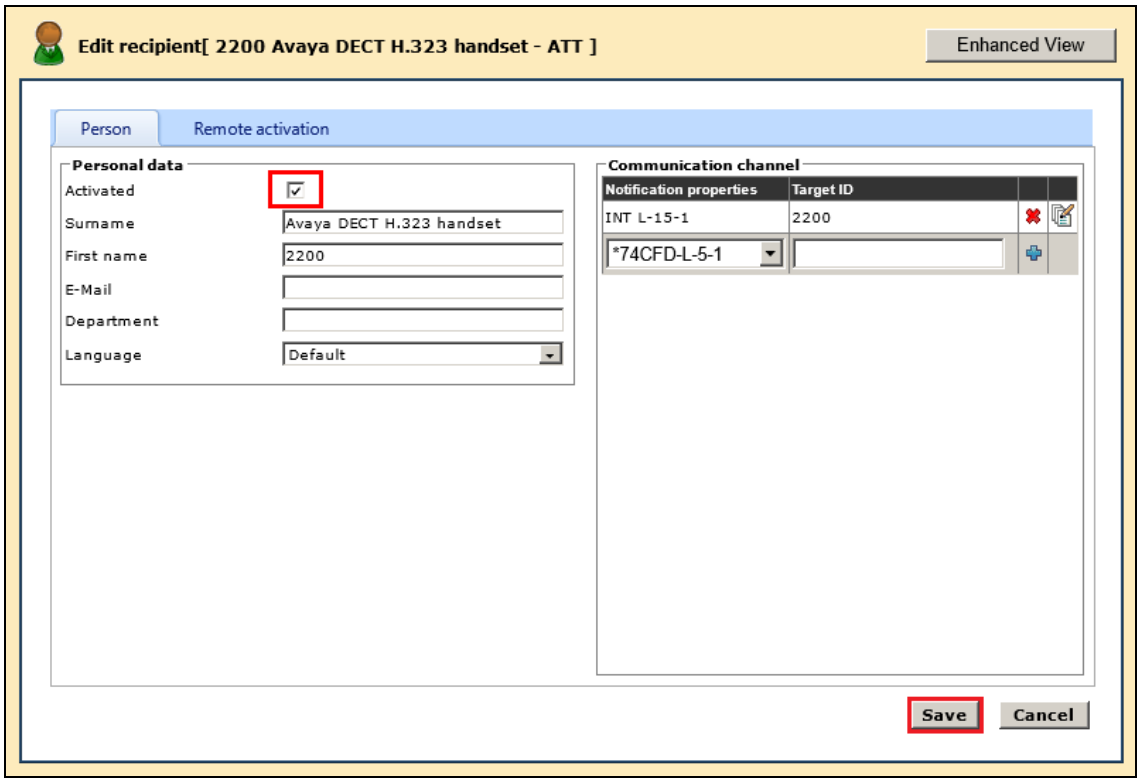
In the resulting window click on the **New** icon highlighted below.



Enter the person or extension details as shown and ensure that **INT L-15-1** is selected as the **Notification properties** and that the extension number is entered as the **Target ID** then click on the **Add** icon highlighted.

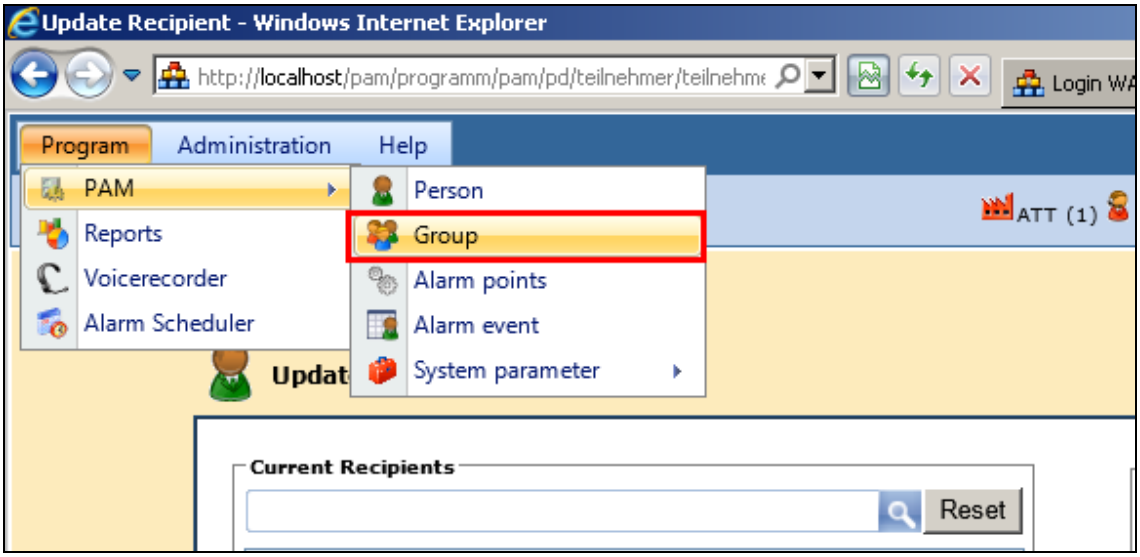


Ensure that the **Activated** box is ticked as shown and click on **Save** once the **Target ID** has been added correctly as shown below.

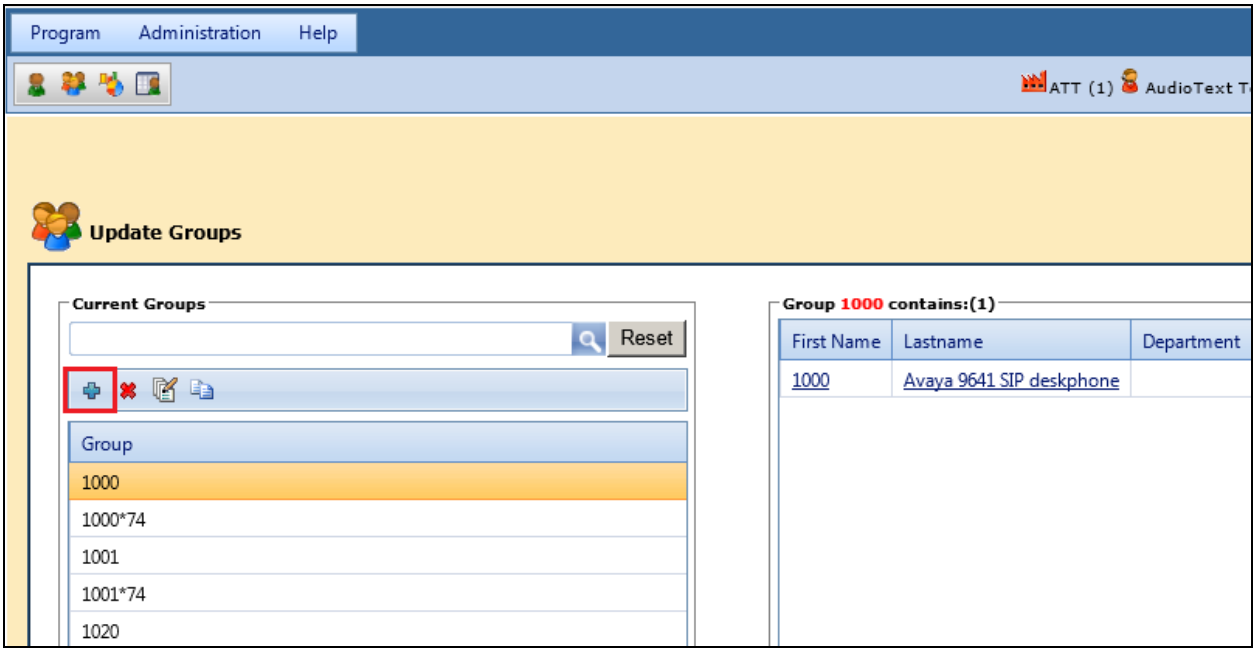


7.2.2. Add a new Group

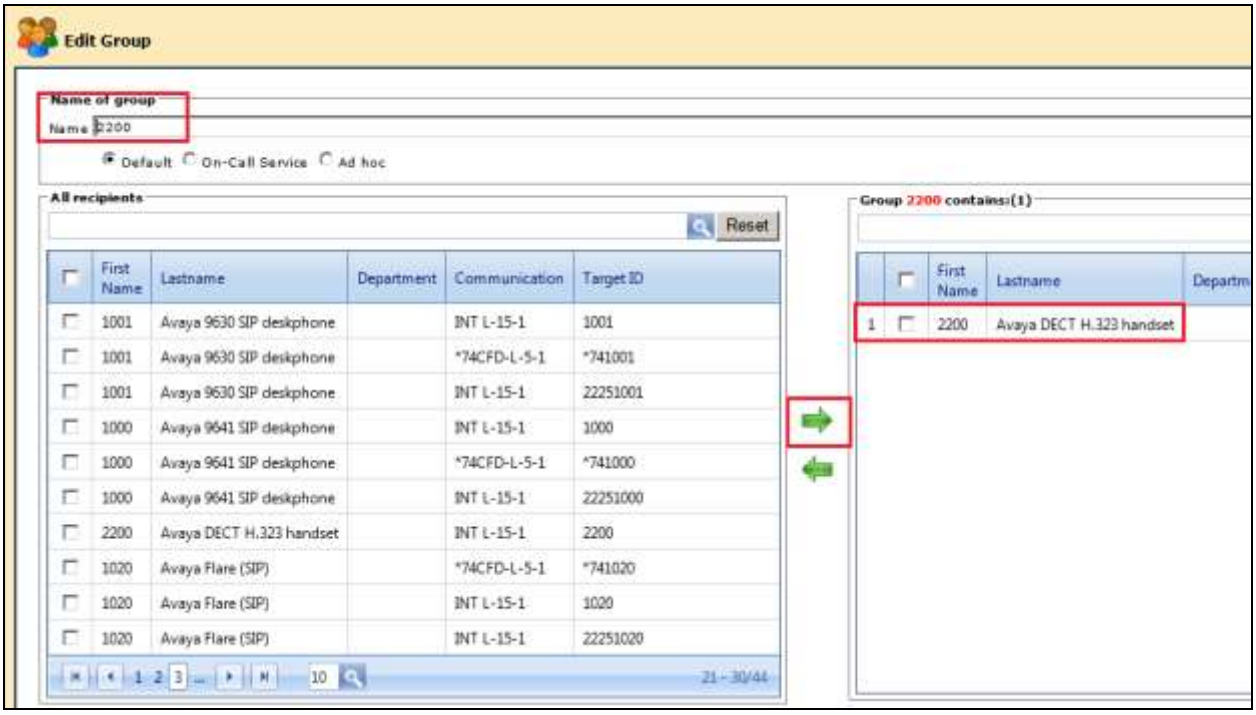
A new group must be added that contains the person or people involved in this group. Select **Program→PAM→Group**.



Click on the **New** icon highlighted below.

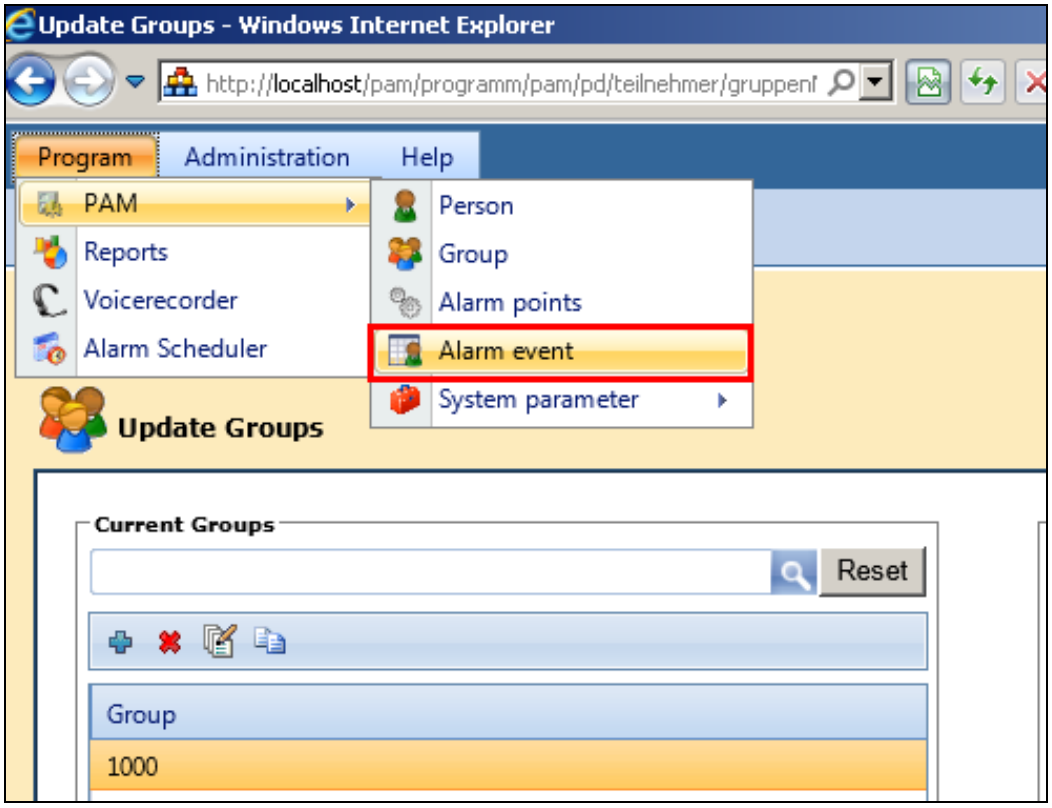


Enter a **Name** for the new group and from the left window locate the new user added previously and select this by clicking on the right arrow highlighted. Then click **Save** (not shown).

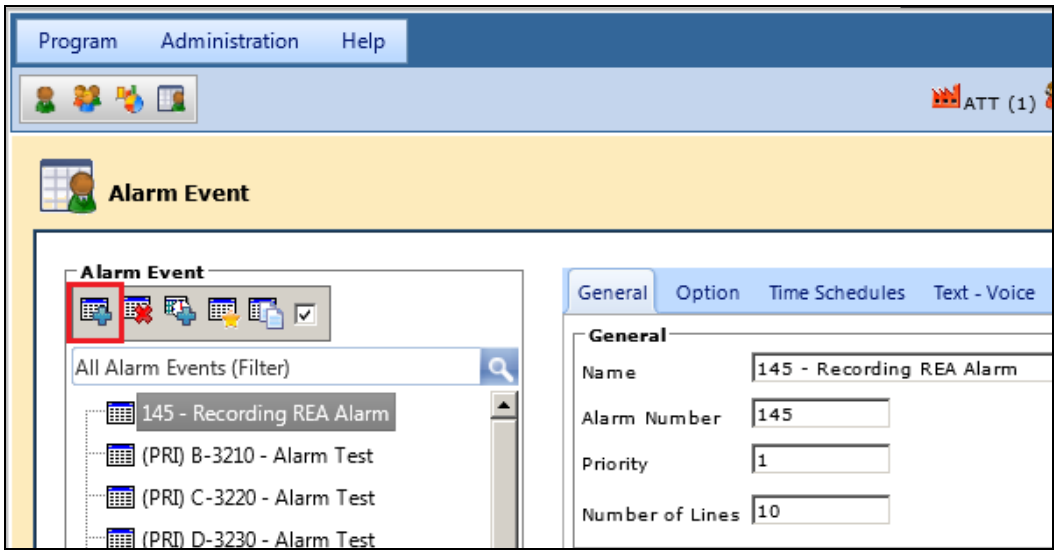


7.2.3. Create an Alarm Event

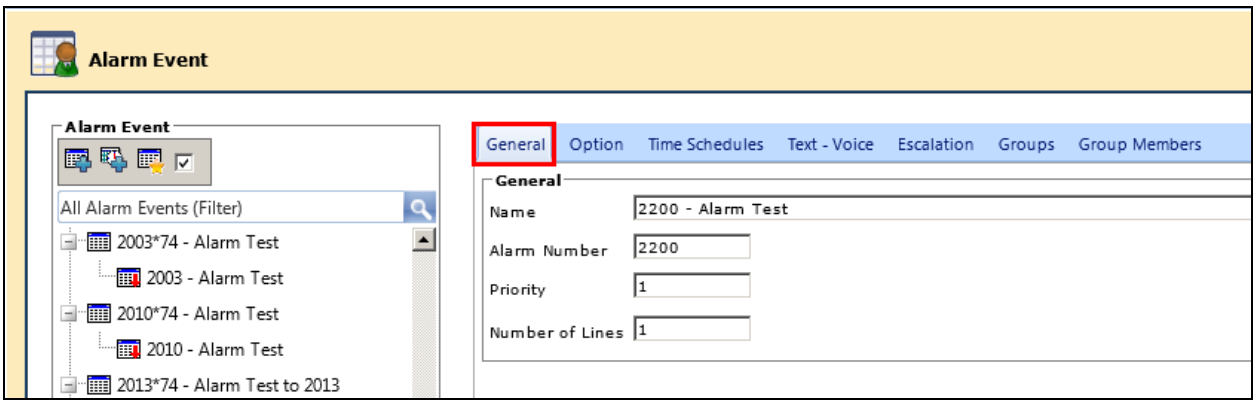
In order to send an alarm an alarm event must first be created. Select **Program→PAM→Alarm event**.



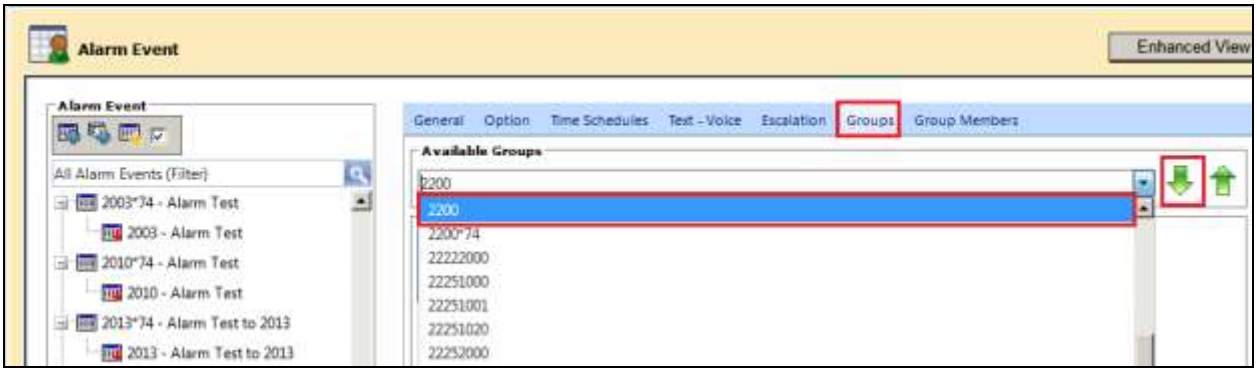
In the resulting window click on the **New** icon highlighted below.



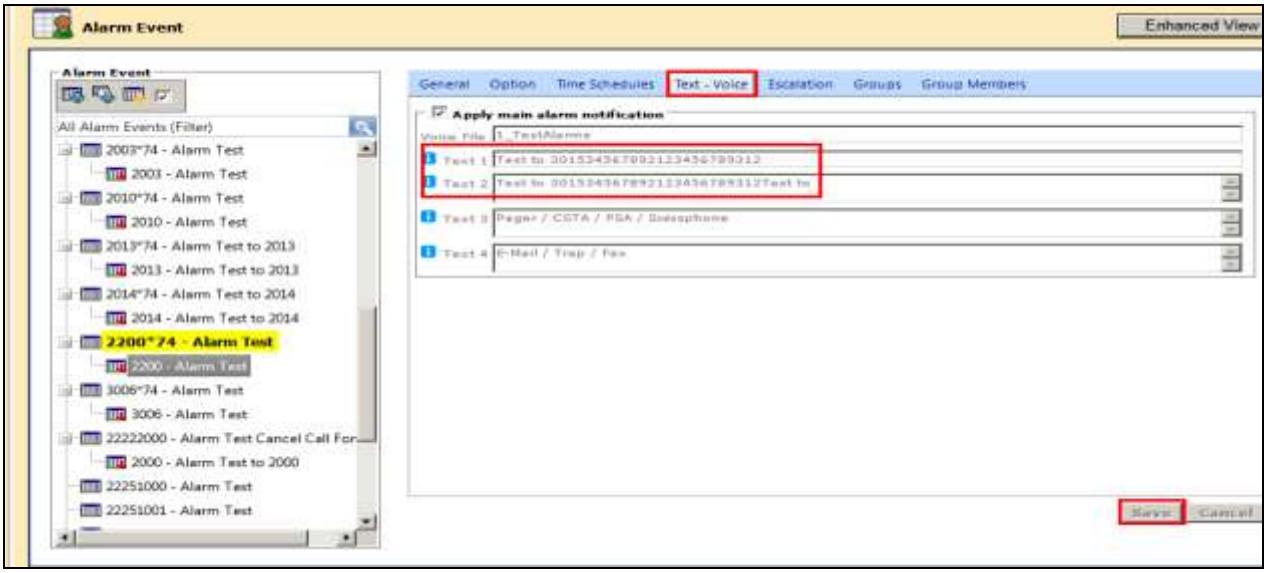
In the **General** tab enter the details of the new event such as the **Name** and the **Alarm Number**.



Click on the **Groups** tab and select the group created above. Click on the down arrow highlighted to add this to the Alarm Event.



All other tabs can be left as default such as **Text-Voice** shown below which has a certain text associated with it created during the install. Click on **Save** once complete.

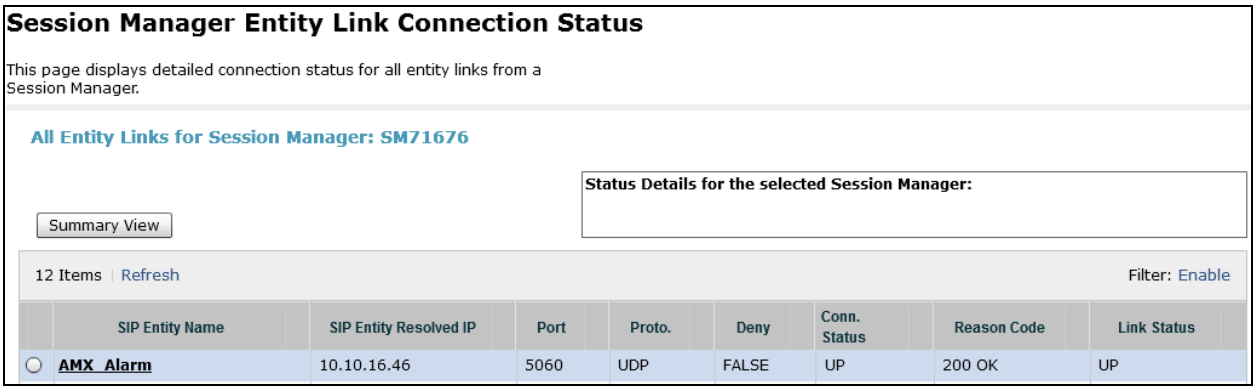


8. Verification Steps

The following steps can be taken to ensure that connections between ATT AMX server and Session Manager and Communication Manager are up.

8.1. Show SIP entity is up on Session Manager

Log into System Manager as done previously in **Section 6.1**, select **Session Manager** (not shown). Click on **SIP Entity Monitoring** as highlighted below. Note that the SIP Entity, **AMX_Alarm**, shows **Link Status UP** and **Reason Code 200 OK**.



Session Manager Entity Link Connection Status

This page displays detailed connection status for all entity links from a Session Manager.

All Entity Links for Session Manager: SM71676

Status Details for the selected Session Manager:

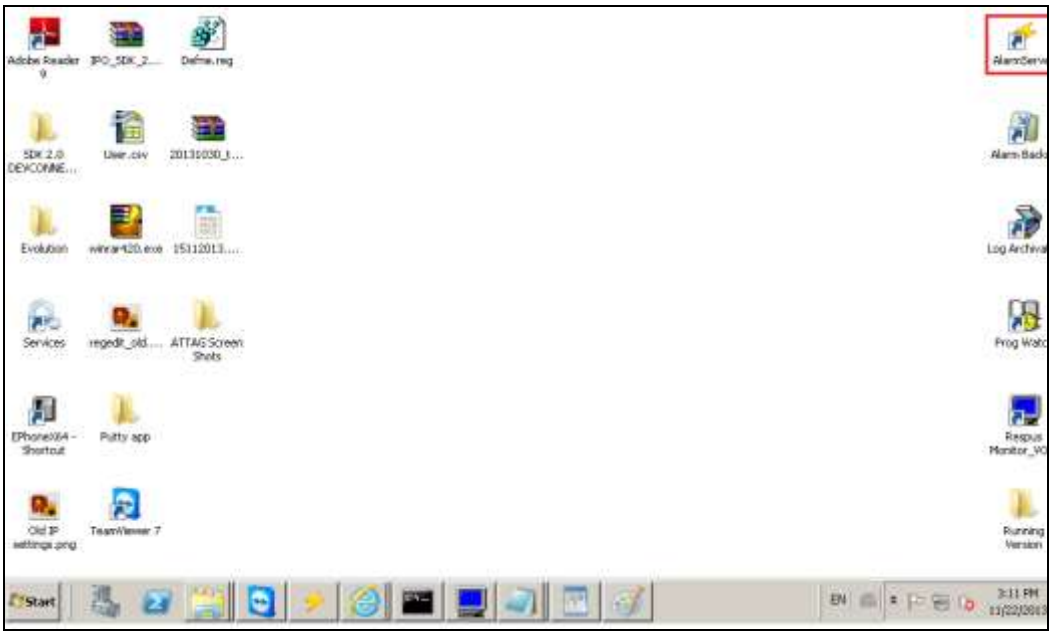
Summary View

12 Items | Refresh Filter: Enable

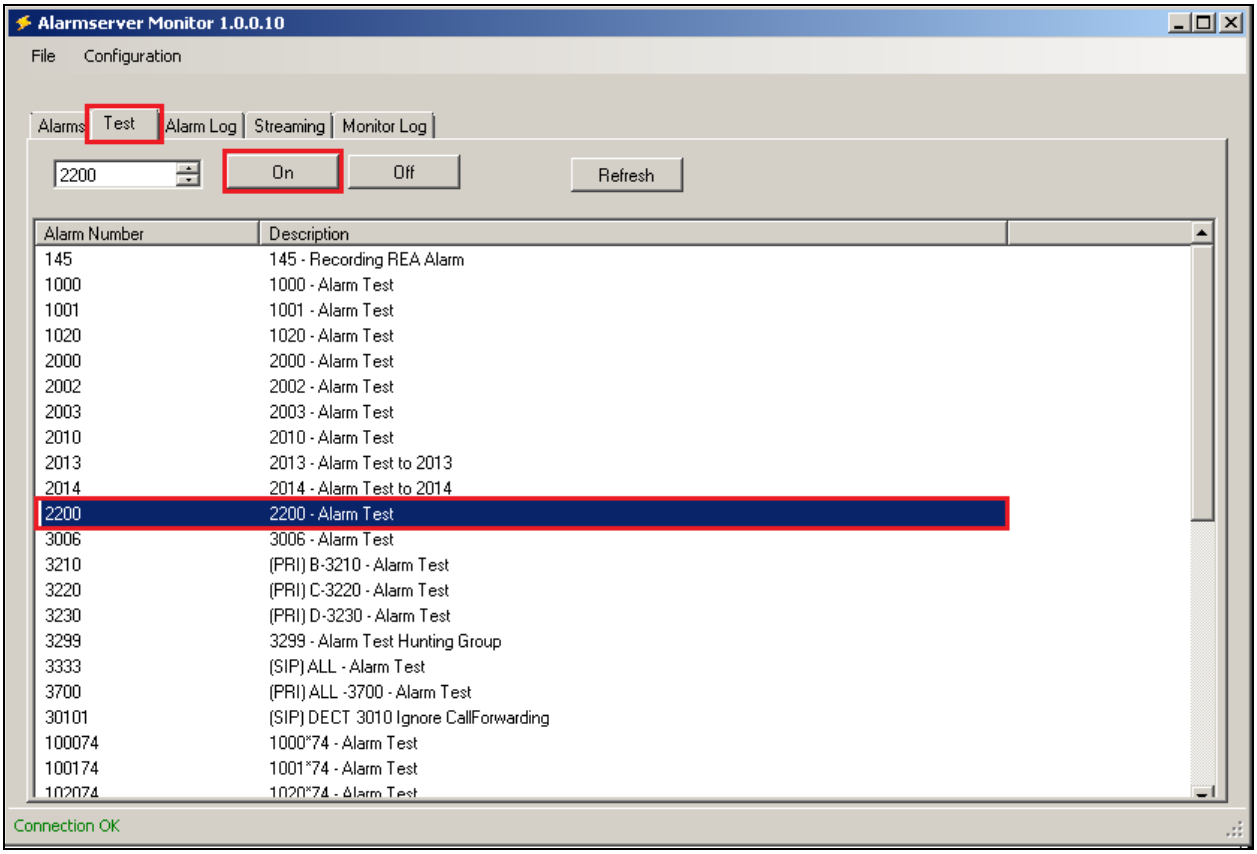
	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	AMX_Alarm	10.10.16.46	5060	UDP	FALSE	UP	200 OK	UP

8.2. Show alarm is sent on the AMX Alarm Server

Open the Alarm Server by clicking on the **AlarmServer** icon highlighted on the screen below.



Click on the **Test** tab and select the alarm event created in **Section 6.2.3**. Once selected click on the On button highlighted below and the extension associated with the event should ring allowing the alarm be heard correctly from that extension once answered.



9. Conclusion

These Application Notes describe the configuration steps required for ATT-AudioText Telecom AG Alarm Management Server to successfully interoperate with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager R7.0 by registering the Alarm with Avaya Aura® Session Manager as third-party SIP Trunk. Please refer to **Section 2.2** for test results and observations.

10. Additional References

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

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

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

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

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

Please refer to **Section 2.3** of these Application Notes for information on ATT support.

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.