Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Notification Solution, and Acme Packet Net-Net 6.2.0 with AT&T IP Flexible Reach Service using MIS/PNT or AVPN Transport – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya Notification Solution, and Acme Packet Net-Net (models 3800, 4250, or 4500) with the AT&T IP Flexible Reach service using **MIS/PNT** or **AVPN** transport connection.

The AT&T IP Flexible Reach service is one of several SIP-based Voice over IP (VoIP) services offered to enterprises for a variety of voice communications needs. The AT&T IP Flexible Reach service allows enterprises in the U.S.A. to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites. Avaya Notification Solution (ANS) provides real-time multimedia notification and response capabilities to many devices including IP Phones, Cellphones, and digital/analog phones. It can be applied to emergency broadcast and system alarming. An Acme Packet Net-Net is the point of connection between Avaya Notification Solution and the AT&T IP Flexible Reach service and is used to not only secure the SIP trunk, but also to make adjustments to the signaling for interoperability.

AT&T is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

TABLE OF CONTENTS

1. Introduction

These Application Notes describe the steps for configuring Avaya Notification Solution, and Acme Packet Net-Net (models 3800, 4250, or 4500) with the AT&T IP Flexible Reach service using **MIS/PNT** or **AVPN** transport connection. **Note that the configuration steps in these Application Notes are used for this reference configuration and are not meant to be prescriptive**.

The AT&T IP Flexible Reach service is one of several SIP-based Voice over IP (VoIP) services offered to enterprises for a variety of voice communications needs. The AT&T IP Flexible Reach service allows enterprises in the U.S.A. to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites.

Avaya Notification Solution (ANS) provides real-time multimedia notification and response capabilities to many devices including IP Phones, Cellphones, and digital/analog phones. It provides intelligent notification features such as notification cascading, acknowledgement gathering, and conference. It can be applied to emergency broadcast and system alarming.

An Acme Packet Net-Net (Acme SBC) is the point of connection between Avaya Notification Solution and the AT&T IP Flexible Reach service and is used to not only secure the SIP trunk, but also to make adjustments to the signaling for interoperability.

2. General Test Approach and Test Results

The test environment consisted of:

- A simulated enterprise site with ANS server and Acme Packet Session Border Controller (Acme SBC).
- A laboratory version of the AT&T IP Flexible Reach service, to which the simulated enterprise site was connected via MIS/PNT or AVPN transport connection.

The main test objectives were to verify the following features and functionality:

- Outbound calls from ANS server to notify the subscribers
- Outbound calls from ANS server to notify the subscribers to join a conference call
- Inbound call to ANS server to trigger an outbound notification
- Inbound call to ANS server to trigger a conference call notification to the subscribers
- Inbound and Outbound caller interaction with ANS, including prompting, and DTMF input
- Basic supplementary telephony features such as hold, resume, and conference
- G.729a and G.711 codec support
- Long duration calls using conferencing

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by

DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying call flows (see **Section 3.2** for sample call flows) between ANS, Acme Packet Net-Net, and the AT&T IP Flexible Reach service.

The compliance testing was based on a test plan provided by AT&T, for the functionality required for certification as a solution supported on the AT&T network. Calls were made to and from the PSTN across the AT&T network. The following features were tested as part of this effort:

- SIP trunking
- Passing of DTMF events and their recognition by navigating automated voice prompts
- ANS delivery of notifications to subscribers
- ANS and AT&T IP Flexible Reach service features such as hold, resume, and conference

2.2. Known Limitations/Test Results

1. ANS 1.2 does not support Answering Machine Detection leaving a voicemail
2. ANS 1.2 only supports a ptime of 20 msecs
3. ANS 1.2 does not support retrieving notifications from the ANS server
4. ANS 1.2 does not support transfer of calls to a help desk

The test objectives stated in **Section 2** with limitations as noted in this section were verified.

2.3. Support

AT&T customers may obtain support for the AT&T IP Flexible Reach service by calling (888) 288-8362.

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. In the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus. Customers may also use specific numbers (provided on http://support.avaya.com) to directly access specific support and consultation services based upon their Avaya support agreements.

3. Reference Configuration

The sample configuration used in these Application Notes is shown in **Figure 1** and consists of several components:

- Avaya Notification Solution provides notification service to its subscribers. Avaya Notification Solution consists of Text to Speech server. A single server is used for Avaya Notification Server and Text to Speech server.
- The Acme Packet Net-Net Session Director (SD) 3800[1] provides SIP Session Border Controller functionality between the AT&T IP Flexible Reach service and the enterprise internal network[2]. UDP transport protocol is used between the Acme Packet Net-Net SD and the AT&T IP Flexible Reach service.

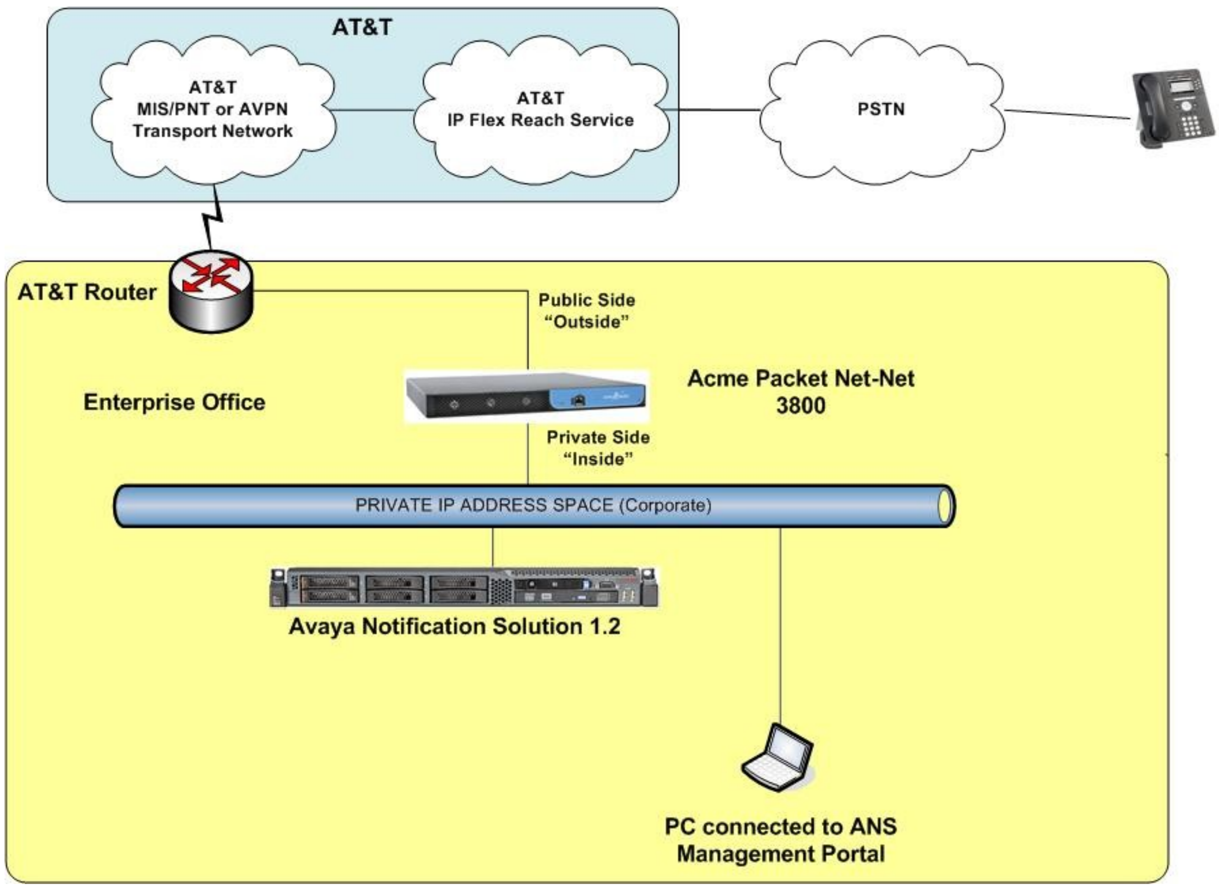


Figure 1: Reference Configuration

---

[1] Although an Acme Net-Net 3800 was used in the reference configuration, the 4250 and 4500 platforms are also supported.

[2] The AT&T IP Flexible Reach service uses SIP over UDP to communicate with enterprise edge SIP devices, e.g., the Acme Packet SBC in this reference configuration. In the reference configuration, Avaya Notification Solution uses SIP over TCP to communicate with the Acme Packet SBC.

3.1. Illustrative Configuration Information

The specific values listed in **Table 1** below and in subsequent sections are used in this reference configuration, and are **for illustrative purposes only**. Customers must obtain and use the specific values for their specific configurations.

Component	Illustrative Value in these Application Notes
Avaya Notification Solution	10.80.130.230
Acme Packet Session Border Controller	
IP Address of "Outside" Interface (connected to AT&T IP Flexible Reach Service)	192.168.62.51
IP Address of "Inside" Interface (connected to Avaya elements)	10.80.130.250
AT&T IP Flexible Reach Service	
Border Element IP Address	135.242.225.210

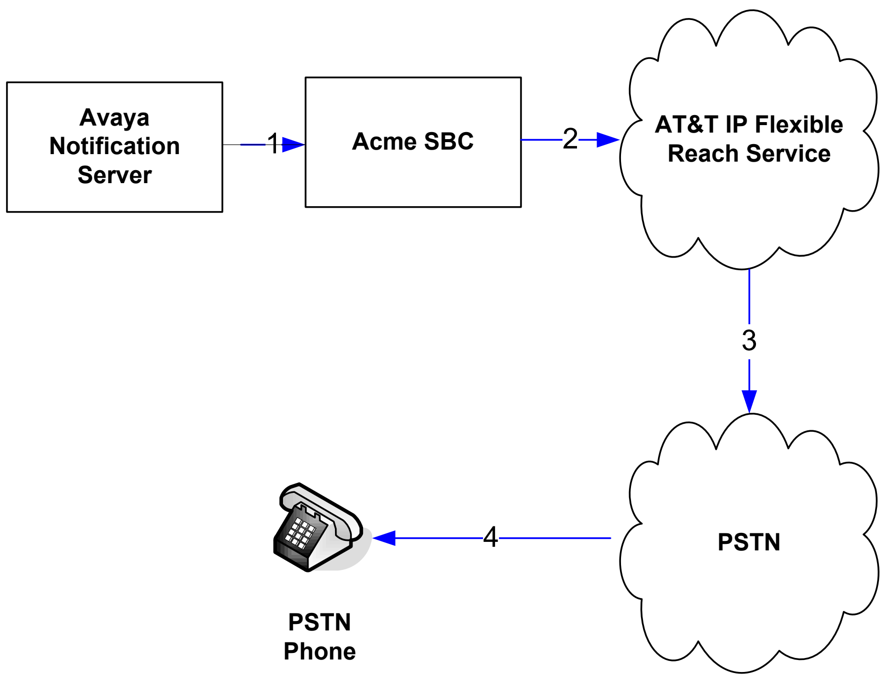
Table 1: Illustrative Values Used in this Reference Configuration

3.2. Call Flows

To understand how AT&T IP Flexible Reach calls are handled by ANS, several call flows are described in this section.

The first call scenario illustrated below is an outbound call originating from ANS to the subscriber/s on PSTN.

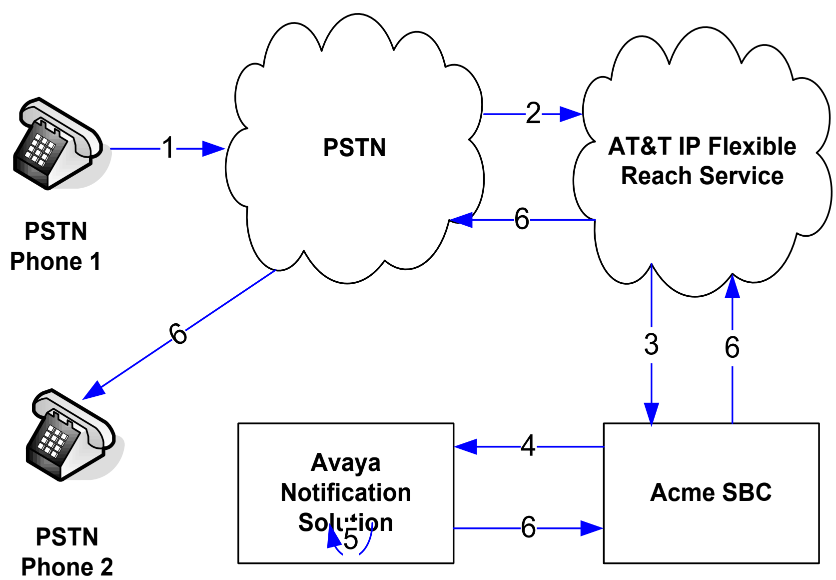
1. ANS originates a call to PSTN phone
2. Acme SBC performs any necessary SIP header modifications, and routes the call to the AT&T IP Flexible Reach Service
3. The AT&T IP Flexible Reach service routes the call to PSTN
4. PSTN delivers the notification call to a PSTN phone subscriber on ANS



Outbound Call from ANS

The second call scenario illustrated below is an inbound call to ANS to trigger a notification by ANS to its subscriber/s. A notification could be an invite to join a conference or provide information to the ANS subscriber/s.

1. PSTN phone 1 calls ANS DID
2. PSTN delivers call to AT&T Flexible Reach Service
3. AT&T Flexible Reach Service routes the call to Acme SBC at CPE.
4. Acme SBC performs any necessary SIP header modifications, and routes the call to ANS
5. Based upon the option entered by PSTN Phone 1, ANS may send a notification to ANS subscriber/s on ANS.
6. Same as Steps 1 to 4 in the first scenario



Inbound Call Handled by ANS to trigger an Outbound Notification to the ANS subscribers

4. Equipment and Software Validated

The following equipment and software was used for the sample configuration described in these Application Notes.

Component	Version
Avaya Notification Solution 1.2 running on VMWare Virtual Machine	VMware vSphere ESX4.0 running Avaya Notification Solution 1.2 on a 32-bit Redhat Enterprise Linux 5.4
Acme Packet Net-Net Session Director 3800	SCX6.2.0 MR-6 Patch 5 (Build 916)
AT&T IP Flexible Reach Service	VNI 23

Table 2: Equipment and Software Versions

5. Configure Avaya Notification Solution Server

These Application Notes assume that the necessary ANS licenses have been installed and basic ANS administration has already been performed. Consult [1] and **Error! Reference source not found.** for further details if necessary.

5.1. Background

ANS is a real-time multimodal notification system with a response gathering capability from the subscriber devices. These devices can be IP phones, cell phones, digital or analog phones. ANS broadcast text and audio messages to Avaya IP phones through IP without consuming any IP-PBX resources. ANS includes a Management Portal for creating notifications and checking their status. ANS stores user and group profiles locally and provides LDAP synchronization with external directory. ANS provides intelligent notification features such as escalation tree, and ad hoc conference. ANS can be used for mass notifications, emergency conferences and event notifications. ANS also has a Text-to-Speech server for converting the Text entered while creating a notification, to equivalent speech.

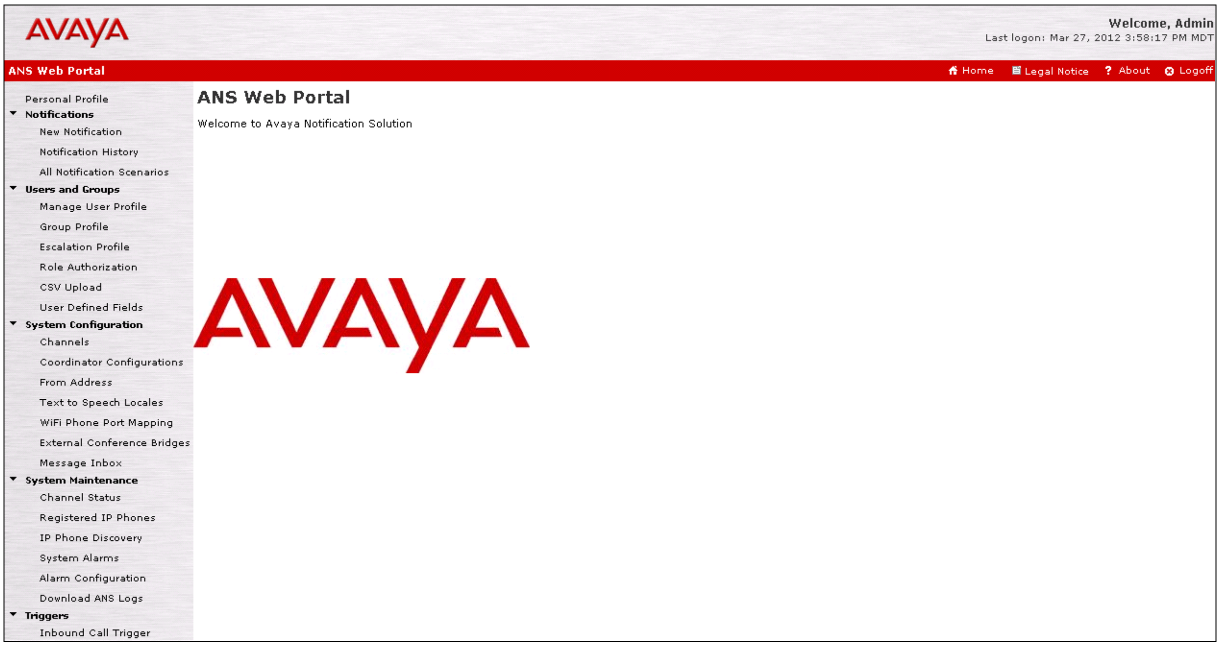
For this reference configuration, ANS was used to send notifications to its subscribers and trigger notifications for it subscribers by calling into the ANS system. Additionally, ad hoc conference feature for the ANS was tested by using inbound triggers or outbound notification for conference. When an inbound call arrives at ANS, it matches the user part of the **To** header in the INVITE to map to the appropriate notification. For outbound calls from ANS, its Management Portal is used to invoke the notification.

Note: The following sections only show the configuration for the values which were changed in this Reference configuration. For all other fields, default values were used. Additionally, the screens shown below are abridged for clarity.

5.2. VoIP Connection

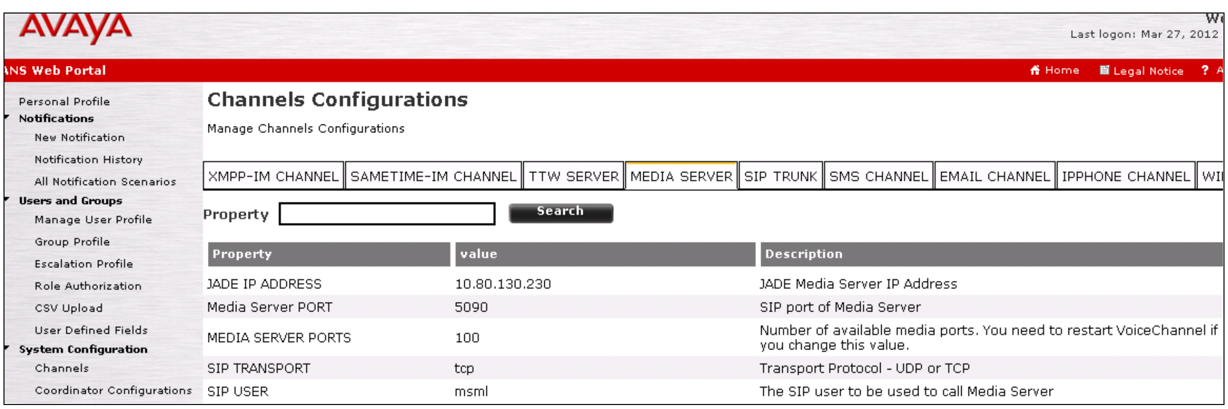
This section describes the steps to configure a SIP interface from ANS to the Acme SBC. **Note that only <u>ONE</u> SIP interface can be configured in ANS1.2**.

1. Launch a web browser, enter **https://<IP address of the ANS server>:8443/ManagementPortal** as the URL, and log in with the appropriate credentials to display the **ANS Web Portal** page.



ANS Web Portal

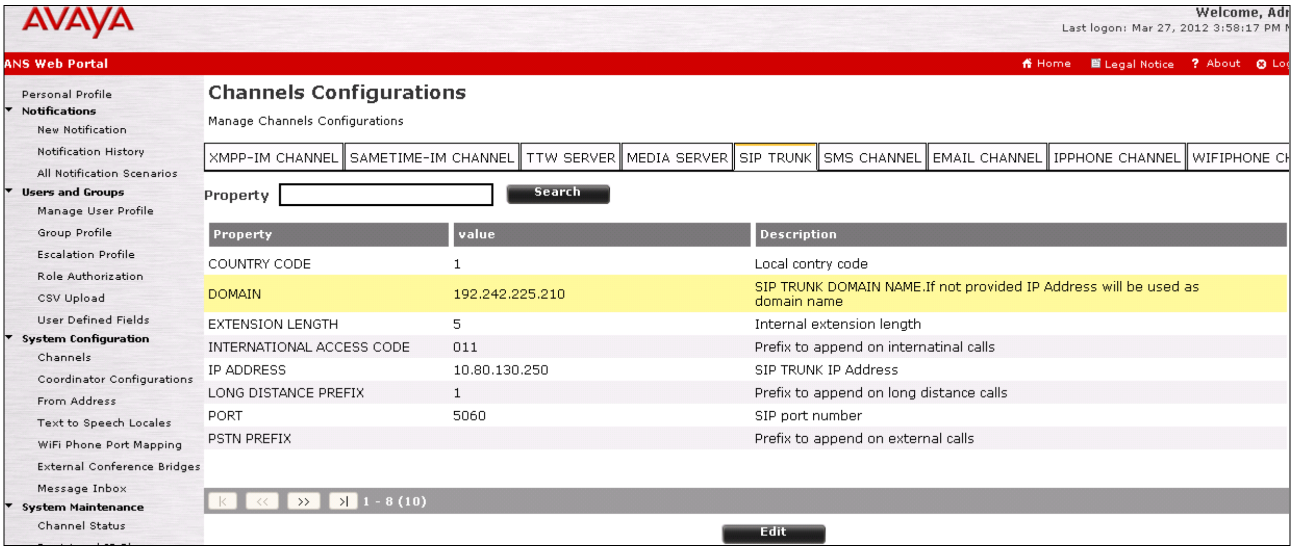
2. In the left pane, navigate to **System Configuration→Channels**. On the **Channels Configurations** page, select the **MEDIA SERVER** tab and verify **JADE IP ADDRESS** is set to the address of the ANS server, **Media Server PORT** field is set to **5090**, **MEDIA SERVER PORTS** is set to an appropriate value as per the number of licenses installed, **SIP TRANSPORT** is set to **tcp** and **SIP USER** is set to **msml**.



Channels Configurations – MEDIA SERVER

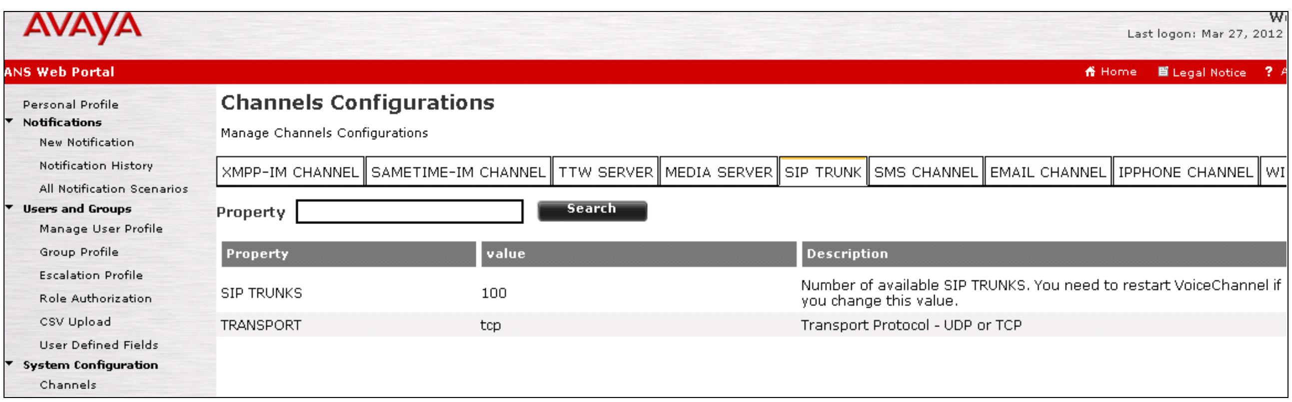
3. Select **SIP TRUNK** tab on the **Channels Configurations** page and configure as follows:
   - **DOMAIN** – Set to the AT&T Border Element IP Address. This domain is used in **From** and **To** headers. See **Section 6** for how the domain name is modified in the **From** header to the external interface of the Acme SBC.
   - **IP ADDRESS** – Set to IP Address of the Acme SBC internal interface
   - **PORT** – Set to **5060**
   - Click [>>] to display more entries on the **SIP TRUNK** form

Note: To change a particular property, highlight the field and click **Edit**



Channels Configurations Page – SIP TRUNK

4. On the page displayed below, set the **SIP TRUNKS** field to the number of available licenses and set the **TRANSPORT** field to **tcp**

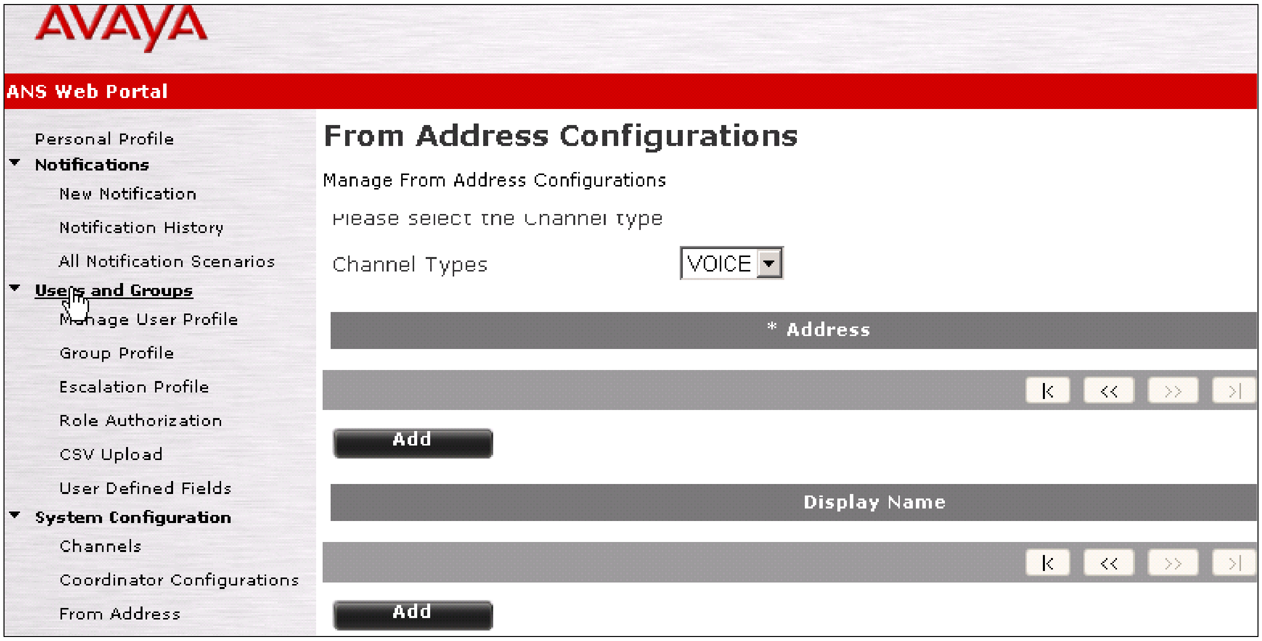


Channels Configurations Page – SIP TRUNK (cont.)

5.3. From Address Configuration

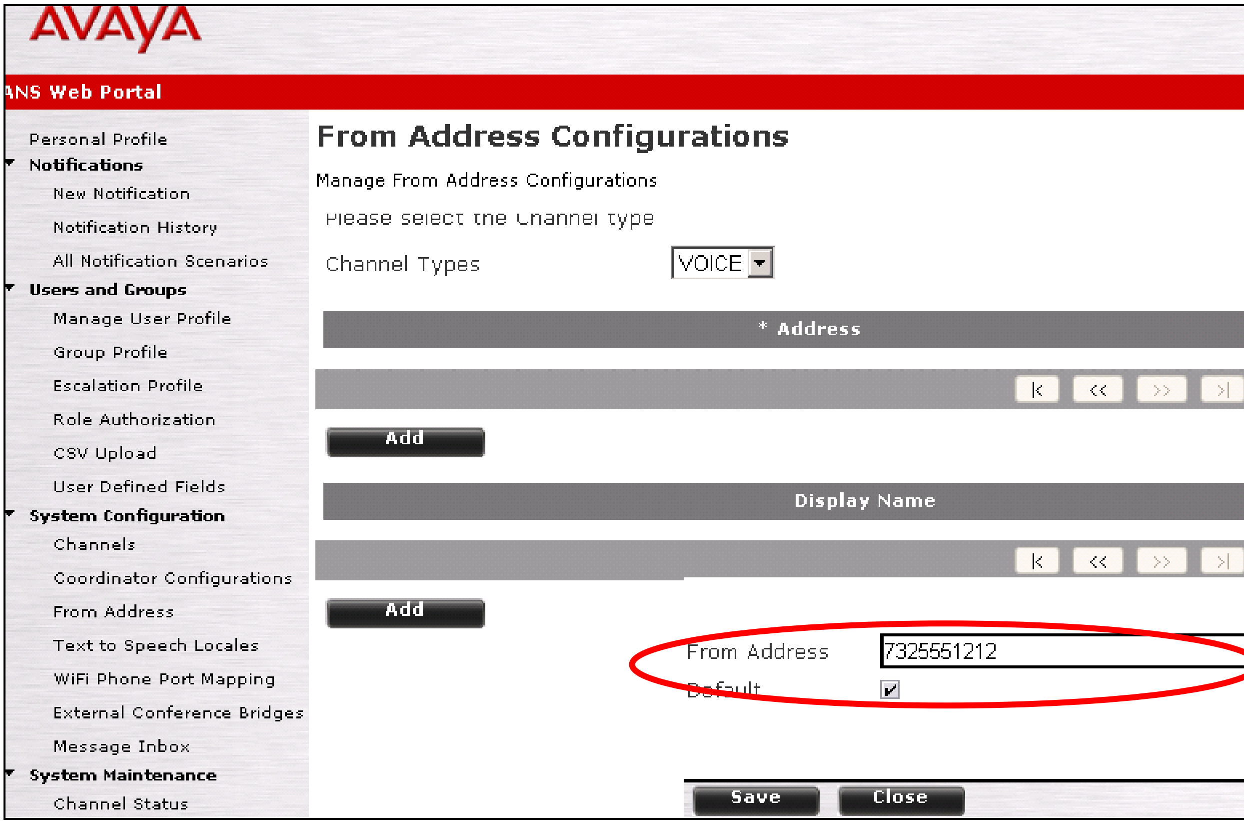
This section describes steps to configure the user part for the **From** header to be sent in an outbound call.

1. Navigate to **System Configuration→From Address** and select **VOICE** in **Channel Types** drop-down box.



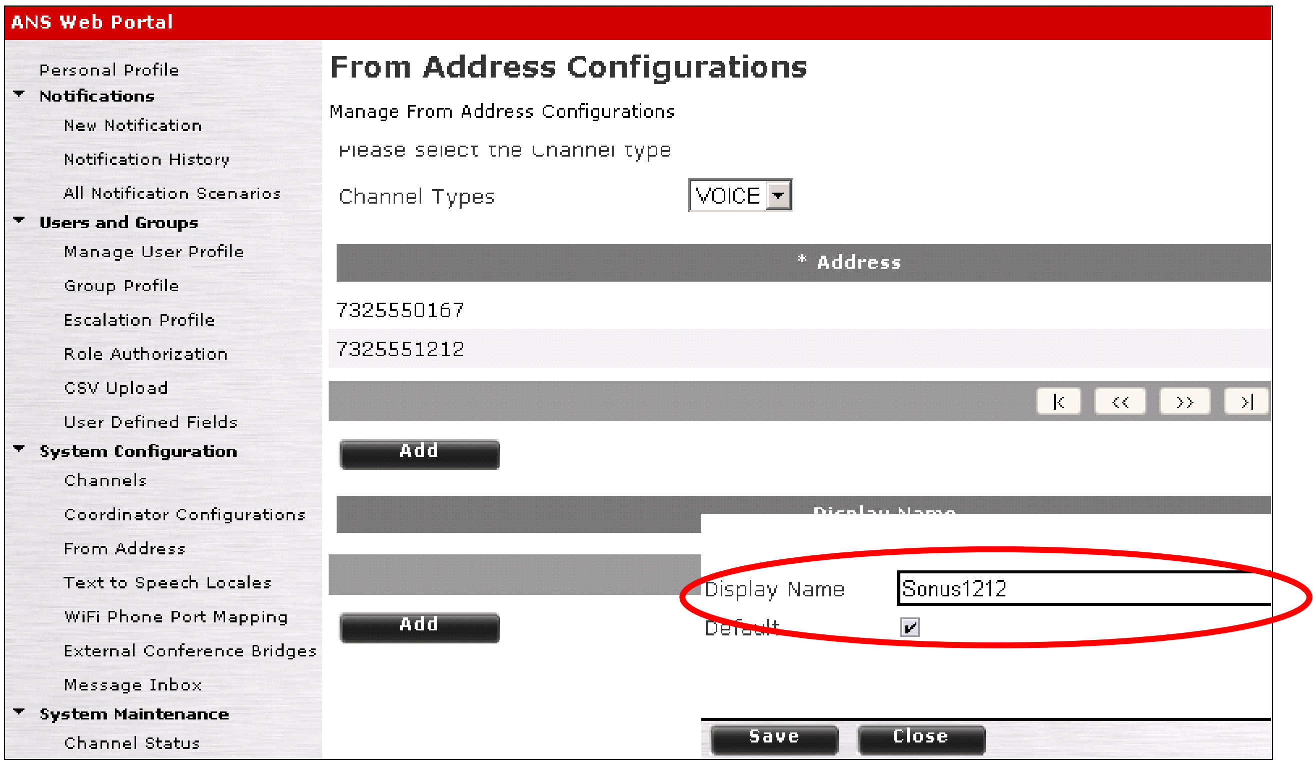
From Address Configurations

2. Click **Add** in the **Address** section of the **From Address Configurations** page, and in the pop-up screen displayed, enter the phone number in the **From Address** field to be sent in the **From** header for an outbound call and click **Save**.



From Address Configuration page – Add Address

3. Click **Add** in the **Display Name** section of the **From Address Configurations** page and enter any value in the **Display Name** field and click **Save**. Mutliple Display names can be configured in this step.

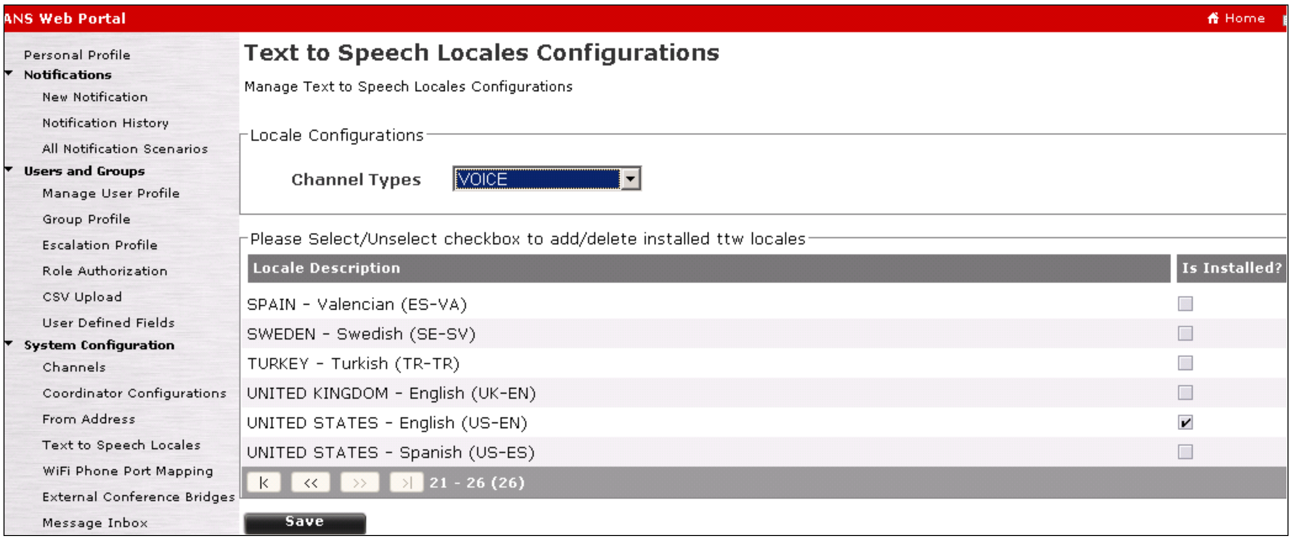


From Address Configuration – Add Display Name

5.4. Text To Speech Locales Configuration

ANS has a built-in Text to Speech service and configuration for this service is beyond the scope of these Application Notes. This section shows the step for configuring the right Locale for Text to Speech conversion on ANS.

- In the left pane, navigate to **System Configuration→Text to Speech Locales** and check the appropriate value in the **Is Installed** field. Click **Save**.



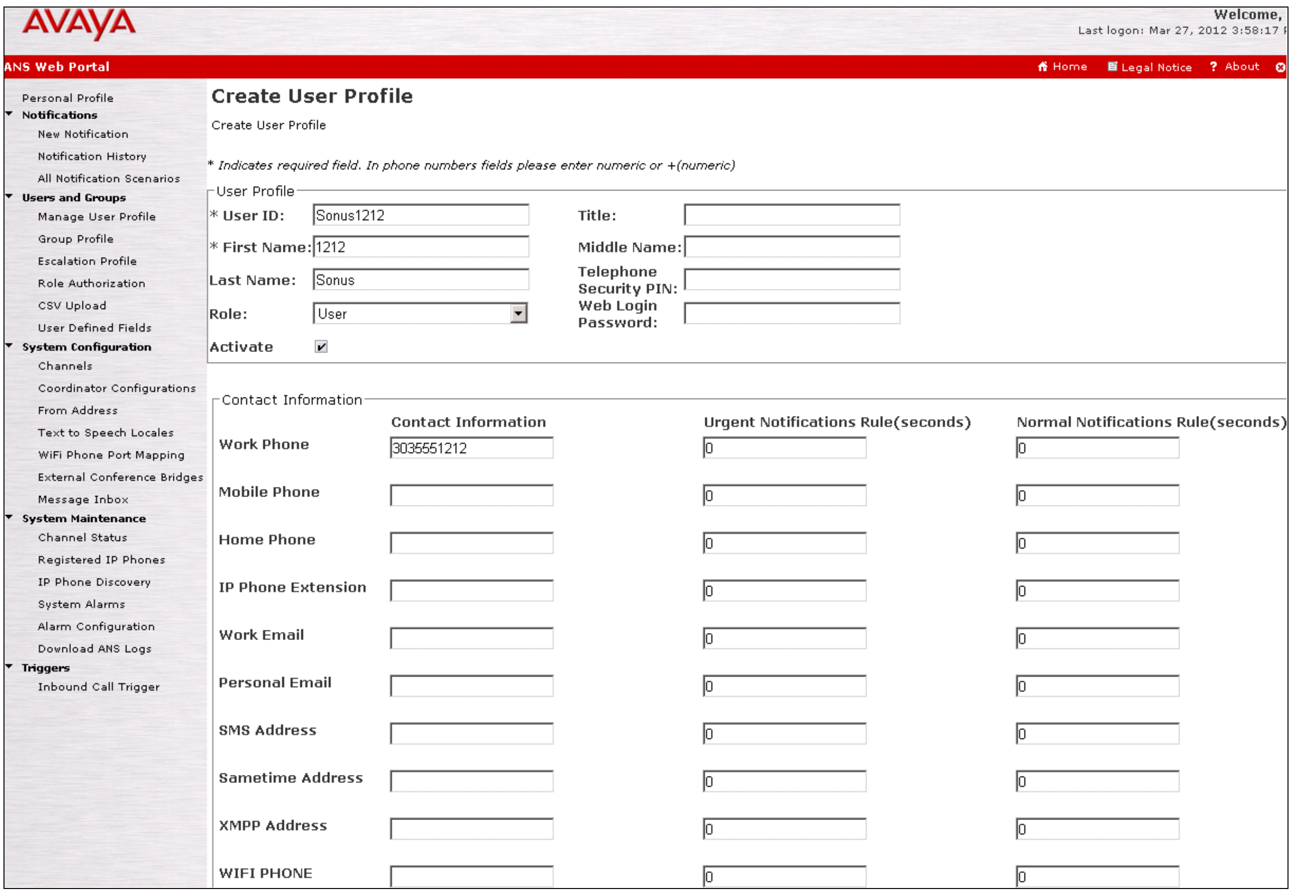
Text to Speech Locales Configurations Page

5.5. Manage User Profile

In the left pane, navigate to **Users and Groups→Manage User Profile** and click on **Add** on the **Manage User Profile** page (not shown). On the **Create User Profile** page shown below, configure as follows:

- **User ID** – Set to any descriptive value
- **First Name** – Set to any unique value
- **Last Name** – Set to any name
- **Work Phone** – Set to the phone number of a subscriber
- Click **Save** (not shown)

Note: If other phone numbers are entered then the notification will be sent simultaneously to the other phone numbers too.

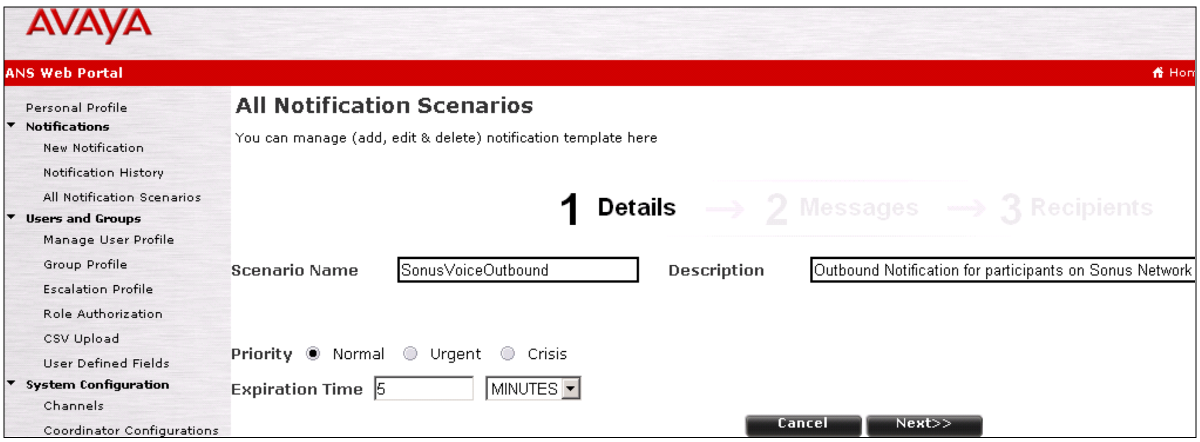


Create User Profile Page

5.6. Add Outbound Notifications

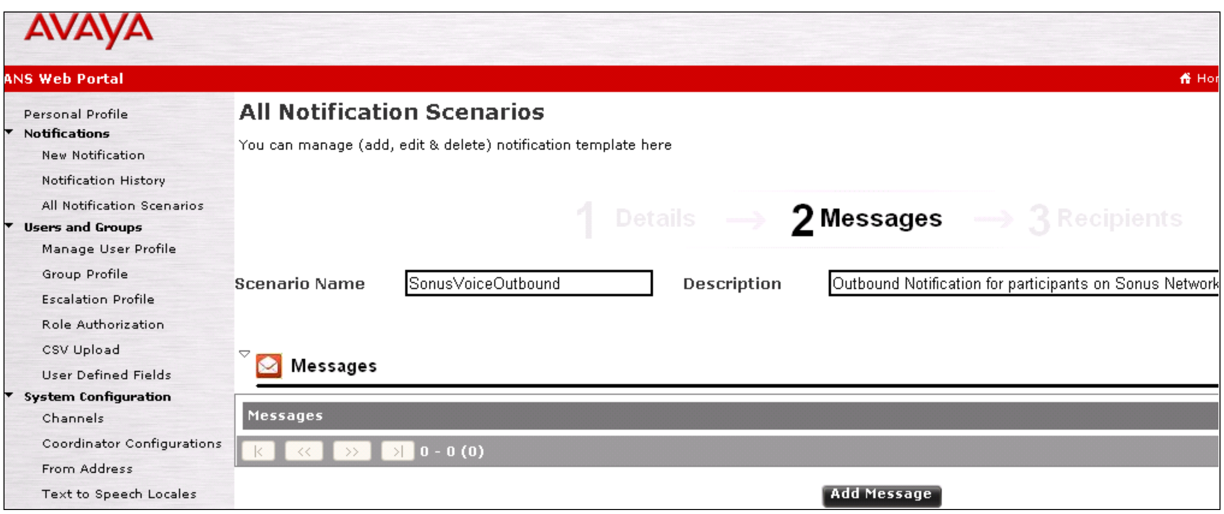
The following steps show the configuration of ANS for sending outbound notifications to its subscribers.

1. In the left pane, navigate to **Notifications→All Notifications Scenarios** and click **Add** on the **All Notification Scenarios** page (not shown). On the **Details** step shown below, configure as follows:
    - **Scenario Name** – Enter any descriptive name
    - **Description** – Enter description of the notification
    - **Priorty** – Set a valid priority
    - **Expiration Time** – Set the time for the notification to expire
    - Click **Next**



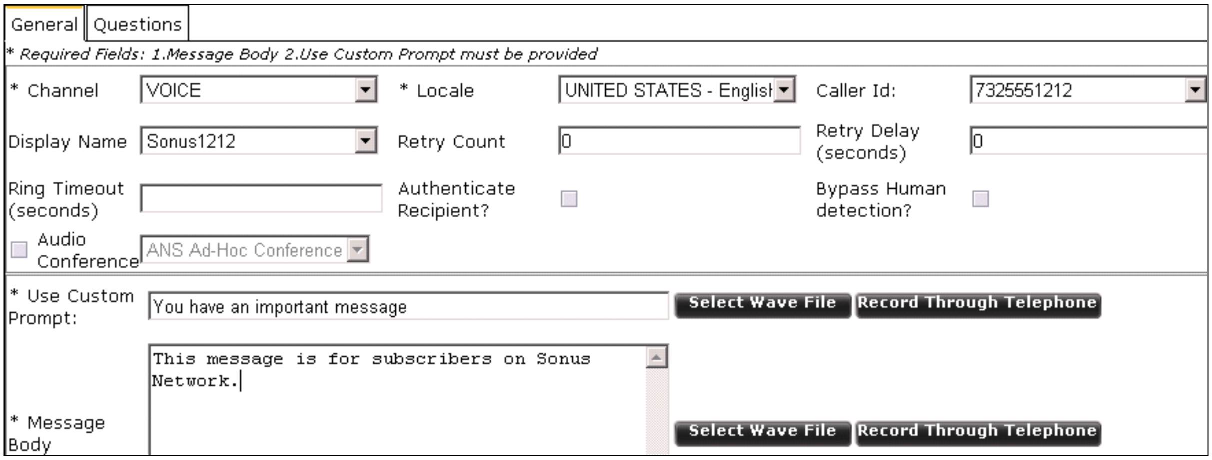
All Notification Scenarios – Details

2. Click **Add Message**



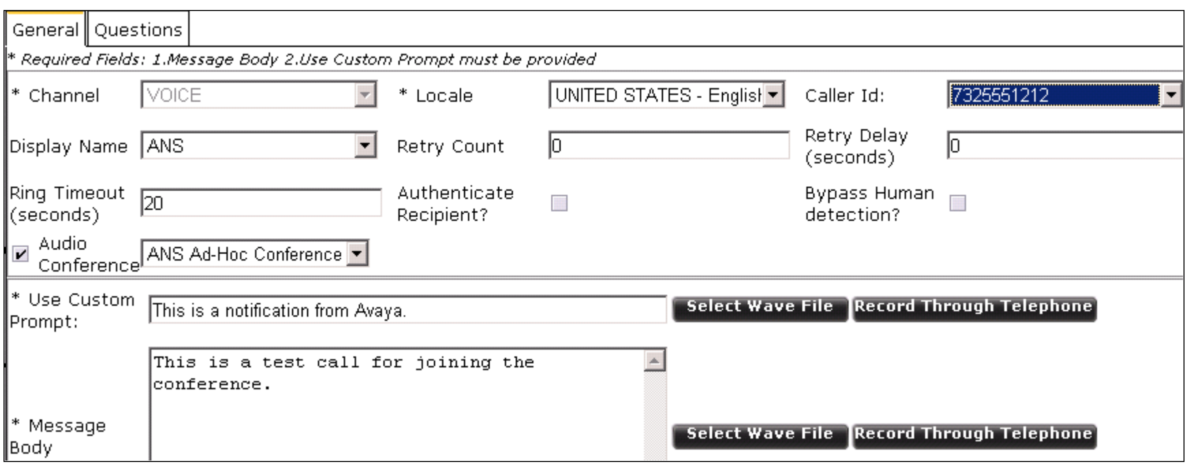
All Notification Scenarios – Message

3. Configure notification as follows:
    - **Channel** – Select **VOICE** from the drop-down box
    - **Caller Id** – Set to one of the values configured in **Section 5.3**, **Step 2**
    - **Display Name** – Set to one of the values configured in **Section 5.3**, **Step 3**
    - **User Custom Prompt** - Enter any text which is played by Text to Speech server when the subscriber picks up the phone
    - **Message Body** – Enter the message/notification to be delivered
    - Click **Save** at the bottom of the screen (not shown)



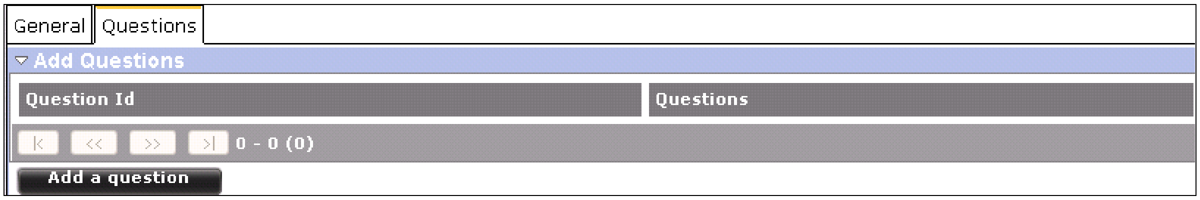
All Notification Scenarios – General

4. In case an adhoc conference is configured (which was done in this reference configuration), then the screen in previous step will look similar to the one shown below. Note that **Audio Conference** box is checked. Click **Questions**.



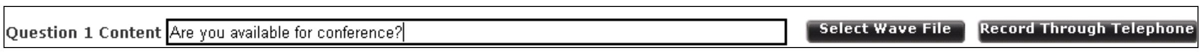
All Notification Scenarios – General (Audio Conference)

5. Click **Add a question**. Note that questions can be added for any notification scenario but in this reference configuration, it was only added for conferencing.



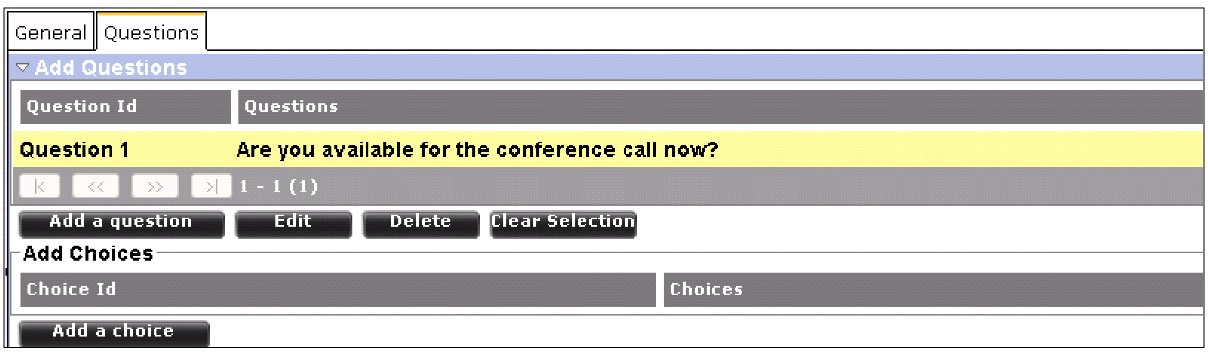
All Notification Scenarios – Question

6. Enter any relevant text in **Question 1 Content** field and click **Save** (not shown).



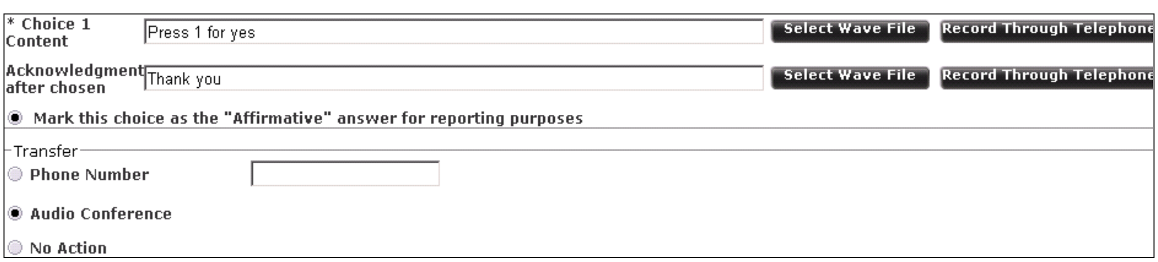
All Notification Scenarios – Add a Question

7. Highlight the question and click **Add a Choice**.



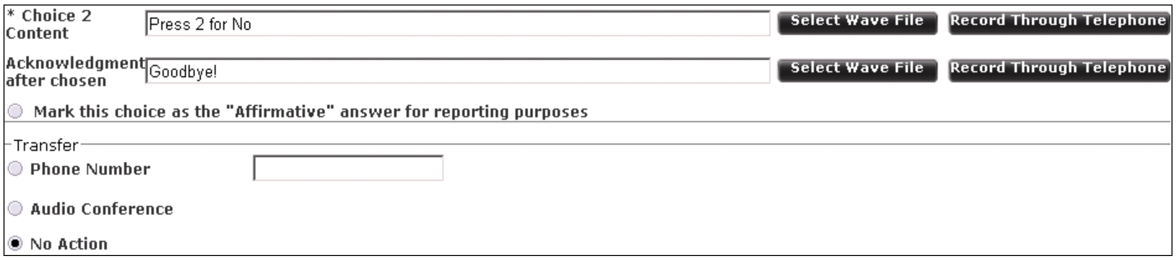
All Notification Scenarios – Add a Choice

8. In the choice details, text is entered for choice fields. In this reference configuration, only text was entered which is converted to speech using the TTS server on ANS. The following choice relates to a response from subscriber to join the conference.
   - **Choice 1 Content** – Enter any informative text
   - **Acknowledgement after chosen** – Enter any informative text
   - **Mark this choice as the "Affirmative" answer for reporting purposes** – Enabled
   - **Audio Conference** – Enabled
   - Click **Save** (not shown)



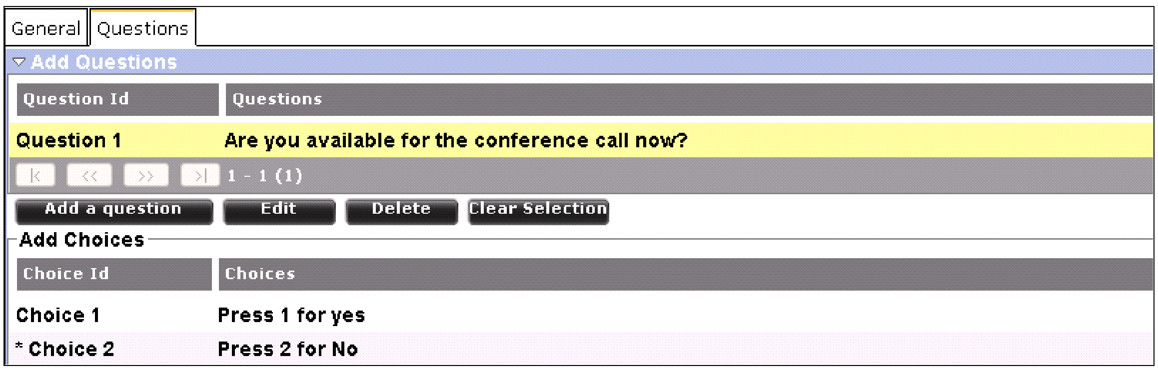
All Notification Scenarios – Add a Choice (Details)

9. The following screen displays another choice which gives the subscriber an opportunity to refuse to join the conference.



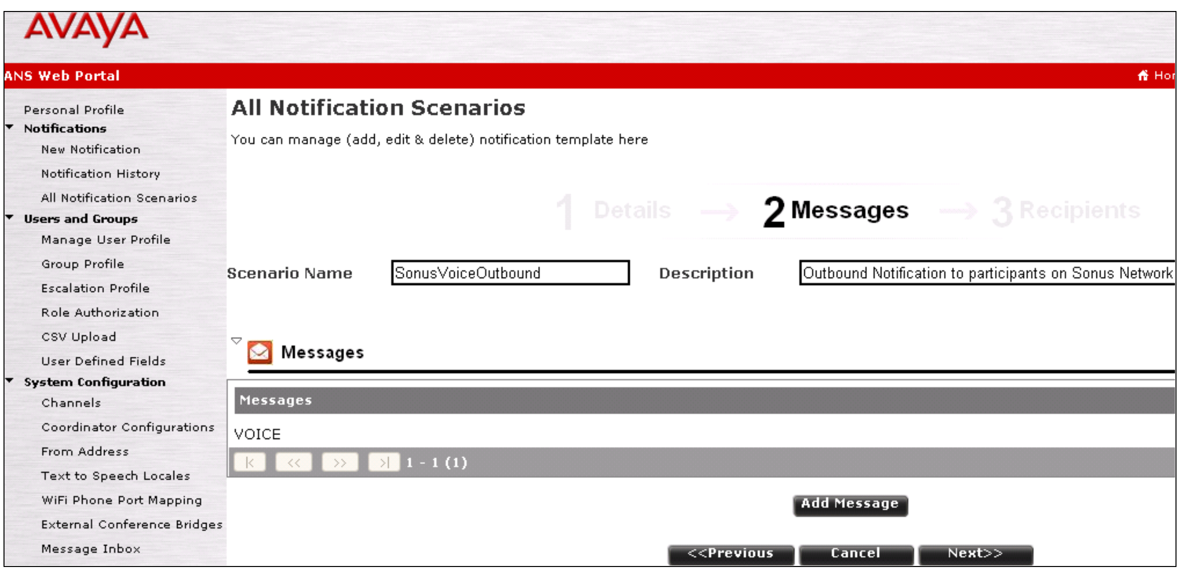
All Notification Scenarios – Add a Choice (Details)

10. The screen below shows the choice configured in previous steps. Click **Save** (not shown).



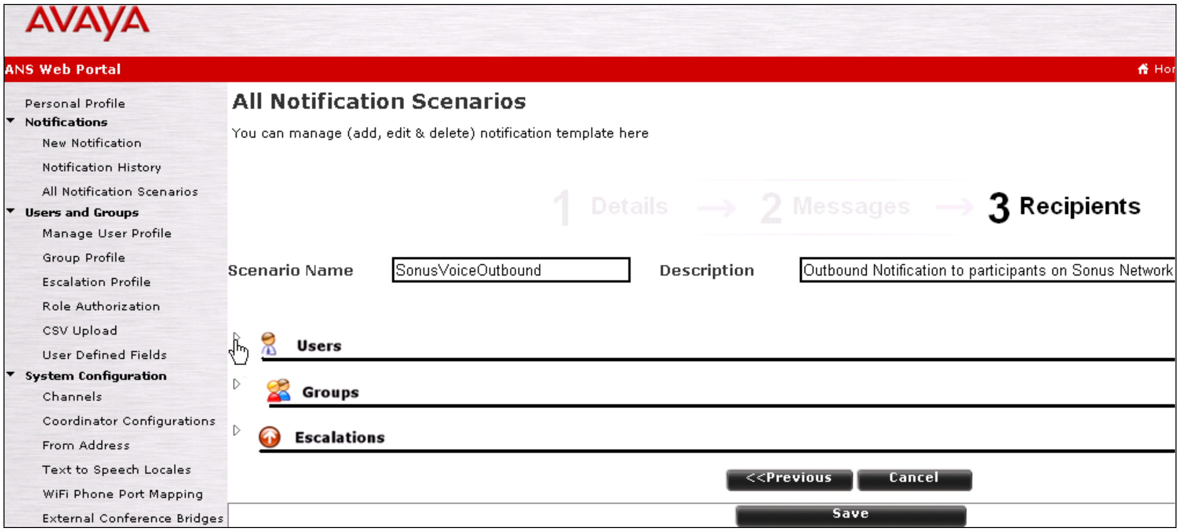
All Notification Scenarios – Choices (Final)

11. The screen below displays the configured message. Click **Next**.



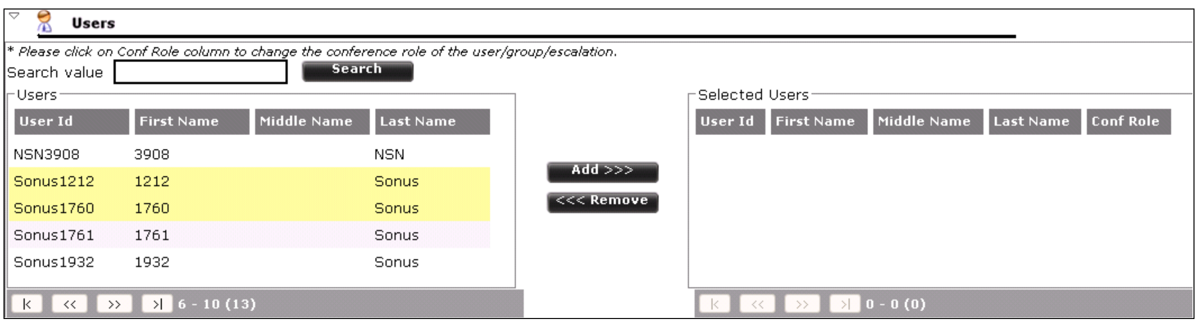
All Notification Scenarios – Message (Final)

12. Click on **Users** to add the recipients of this notification



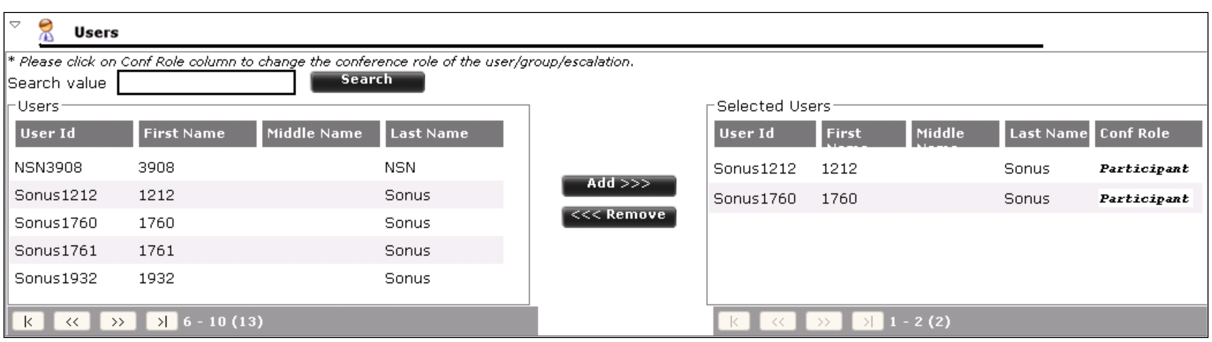
All Notification Scenarios – Recipients

13. Highlight the recipients in the **Users** area to send the notification and then click **Add** to move them to the **Selected Users** area



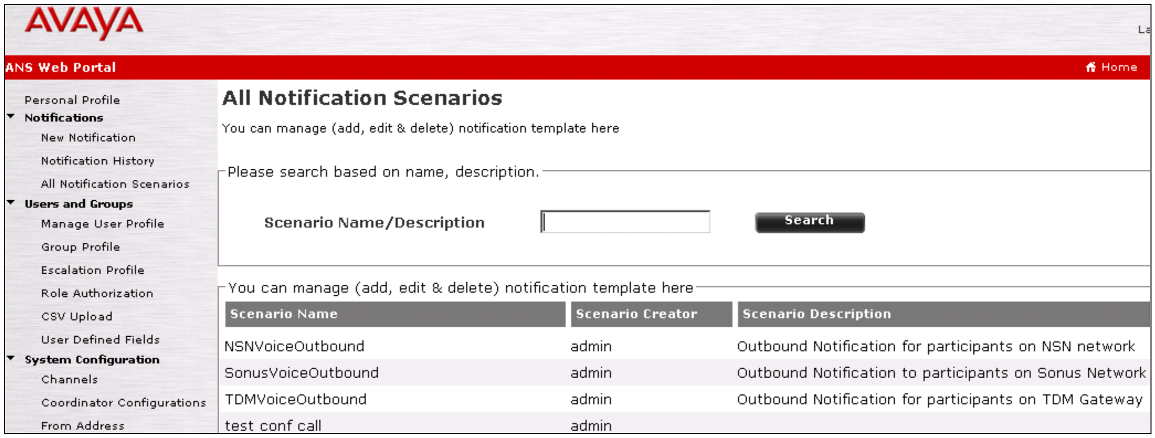
All Notification Scenarios – Recipients (Cont.)

14. The screen below shows the final screen with recepients. Click **Save** (not shown)



All Notification Scenarios – Recipients (Final)

15. The following screen shows all the notifications configured in this reference configuration

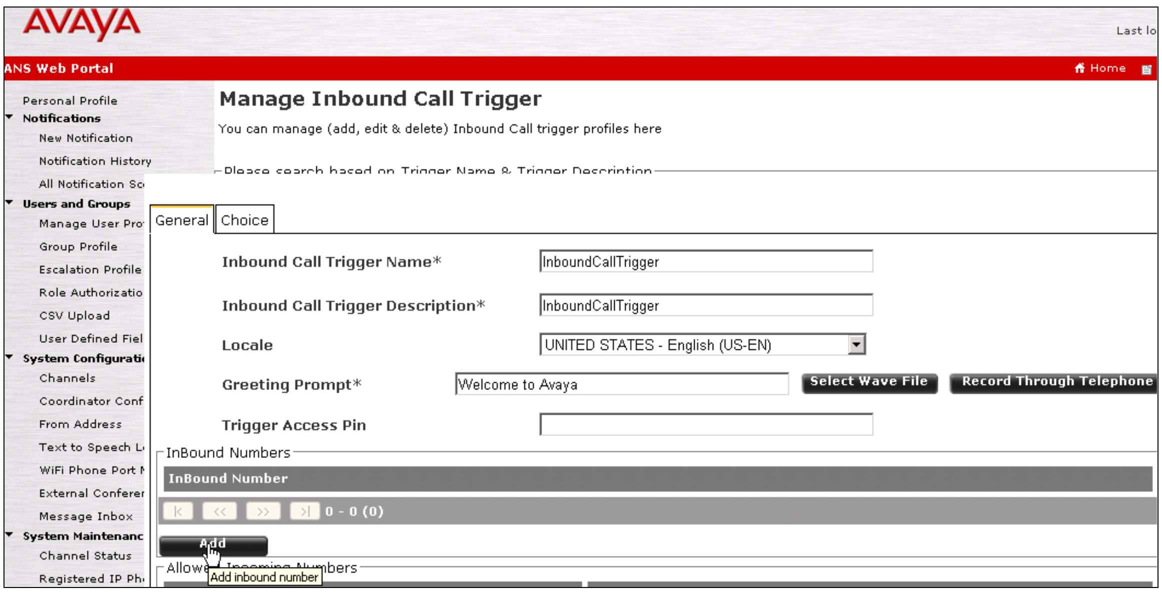


All Notification Scenarios configured

5.7. Add Inbound Triggers

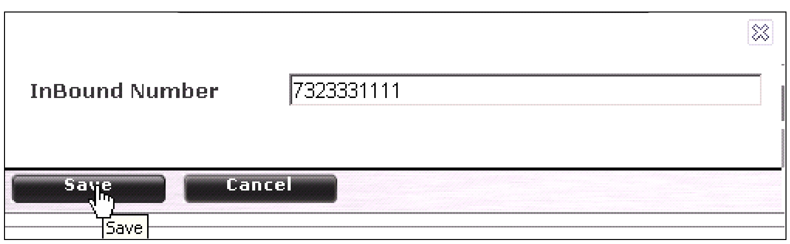
The following steps show the configuration of ANS adding triggers on an inbound call to generate outbound notifications based upon the choices entered by the caller.

1. In the left pane, navigate to **Triggers→Inbound Call Trigges** (not shown) and click on **Add** (not shown) on the **Manage Inbound Call Trigger** page (not shown). In the General section shown below, configure as follows:
   - **Inbound Call Trigger Name** – Enter any descriptive value
   - **Inbound Call Trigger Description** – Enter any descriptive string
   - **Locale** – Select **UNITED STATES – English(US-EN)** from the drop-down list
   - **Greeting Prompt** – Enter any text which is converted to speech and played to the caller when inbound call is received by ANS
   - Click **Add** to add an inbound number



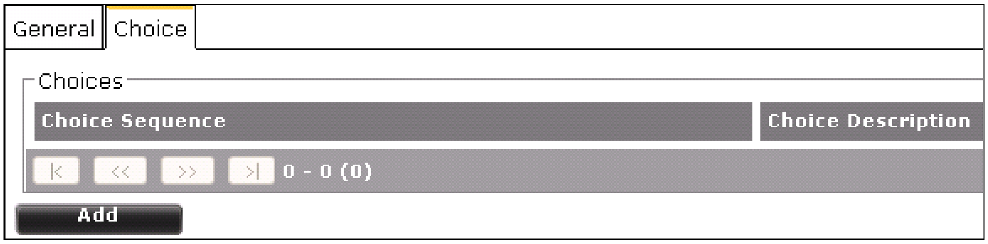
Manage Inbound Call – General

2. Enter a valid phone number in the **InBound Number** field and click **Save**.



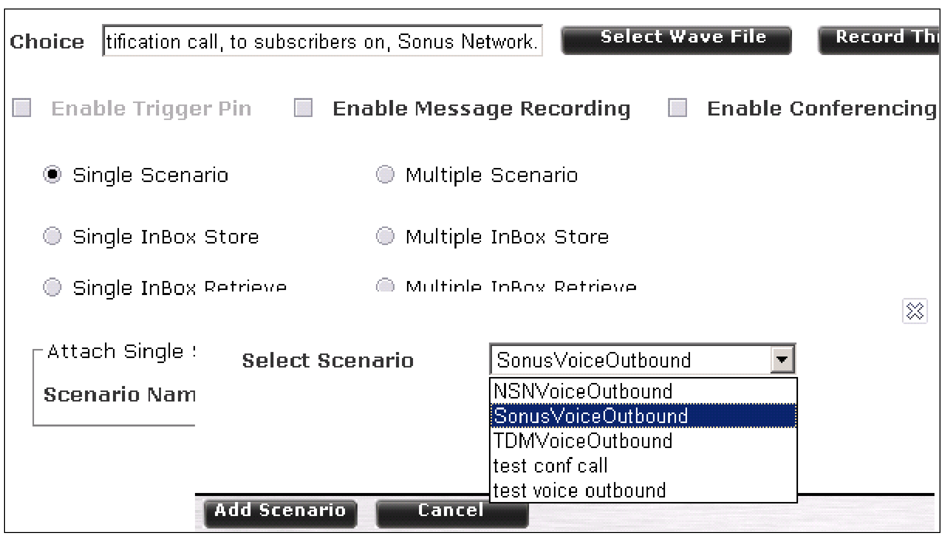
Manage Inbound Call – Inbound Number

3. Select **Choice** and click **Add**



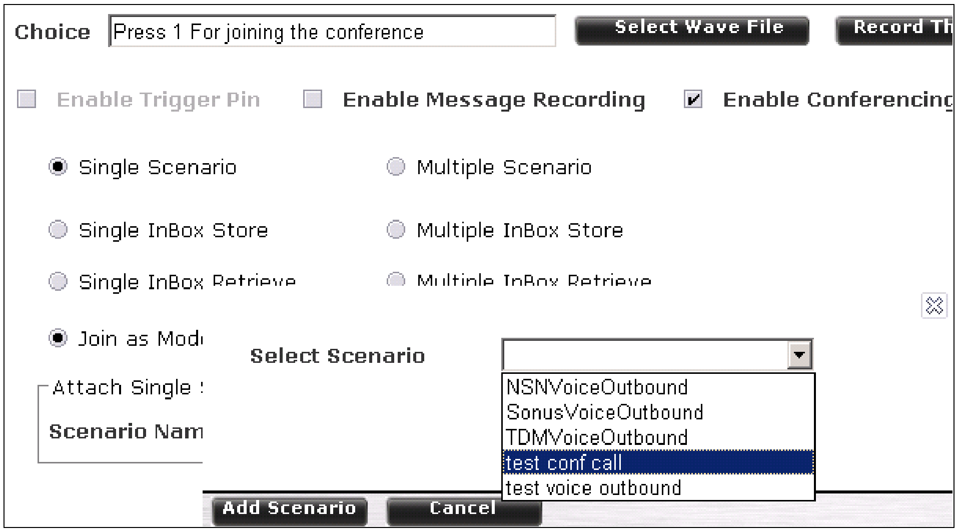
Manage Inbound Call – Choice

4. On the Choice pop-up screen, configure as follows:
   - Choice – Enter any descriptive string which is converted into speech when an inbound call comes into ANS
   - Single Scenario – Select this option
   - Click on **Select** next to the **Select Scenario** (not shown) and select the corresponding Notification to be triggered from the drop-down list. These notifications were configured in **Section 5.6**.
   - Click **Add Scenario**
   - Click **Save** (not shown)



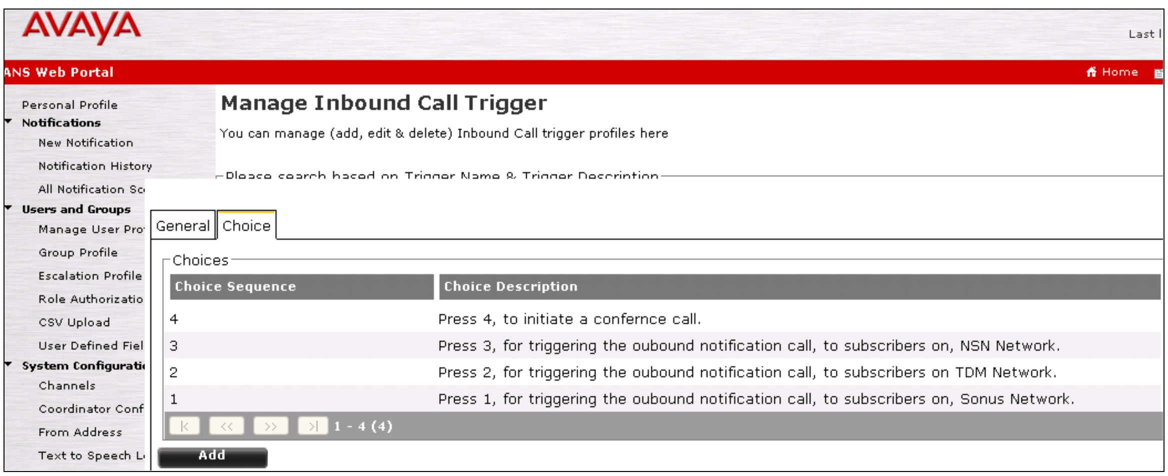
Manage Inbound Call – Choice to trigger Outbound Notification

5. Following screen shows the Choice configured for conferencing and sending a conference notification to the subscriber.



Manage Inbound Call – Choice to trigger Outbound Conference Notification

6. Following screen shows all the choices configured for the Inbound Trigger in this reference configuration



Manage Inbound Call – Choice (Final)

5.8. Configuring Codec and RTP ports Offered by Avaya Notification Solution

This configuration is required to change the codecs and payload type offered and their order by ANS. Additionally, AT&T requires the RTP port range of 16384 to 32767.

When ANS sends an outbound notification, AT&T IP Flexible Reach service prefers a G729 codec.

- Access the ANS via the command line interface and navigate to the **/opt/rhel48/usr/Avaya/MediaServer/config** directory
- Edit the **audioPreferences.cfg** file
- Change the order of the codec and their corresponding payload types

Configure the RTP ports in the range of 16384 to 32767 as follows:

- Access the ANS via the command line interface and navigate to the **/opt/rhel48/usr/Avaya/MediaServer/config** directory
- Edit the **softMediaServer.cfg** file
- Search for **baseRtpPort** and change the value to **16384**
- Search for **maxChannels** and change the value to **5000** (Maximum allowed in ANS 1.2)
- Change the order of the codec and their corresponding payload types

After saving the file with the changes, enter the following commands:

- **/etc/init.d/acms stop**
- **/etc/init.d/acms start**

6. Configure Acme Packet Session Border Controller

The Acme SBC configuration used in the sample configuration is provided below as a reference. The notable settings are highlighted in bold and brief annotations are provided on the pertinent settings. Consult with Acme Packet Support [3] for further details and explanations on the configuration below.

ANNOTATION: The local policy below governs the routing of SIP messages from elements on the network on which the Avaya elements, e.g., Notification Solution, Communication Manager, etc., reside to the AT&T IP Flexible Reach service.

```
local-policy
      from-address
                                      *
      to-address
                                      *
      source-realm
                                      Enterprise
      description
      activate-time                   N/A
      deactivate-time                 N/A
      state                           enabled
      policy-priority                 none
      last-modified-by                admin@console
      last-modified-date              2011-08-12 10:25:23
      policy-attribute
            next-hop                        sag:SP_PROXY
            realm                           ATT
            action                          none
            terminate-recursion             disabled
            carrier
            start-time                      0000
            end-time                        2400
            days-of-week                    U-S
            cost                            0
            app-protocol                    SIP
            state                           enabled
            methods
            media-profiles
```

ANNOTATION: The local policy below governs the routing of SIP messages from the AT&T IP Flexible Reach service to Notification Solution.

```
local-policy
      from-address
                                      *
      to-address
                                      *
      source-realm
                                      ATT
      description
      activate-time                   N/A
      deactivate-time                 N/A
```

```
      state                          enabled
      policy-priority                none
      last-modified-by               admin@console
      last-modified-date             2011-08-12 10:25:23
      policy-attribute
            next-hop                       10.80.130.230
            realm                          Enterprise
            action                         none
            terminate-recursion            disabled
            carrier
            start-time                     0000
            end-time                       2400
            days-of-week                   U-S
            cost                           0
            app-protocol                   SIP
            state                          enabled
            methods
            media-profiles

media-manager
      state                          enabled
      latching                       enabled
      flow-time-limit                86400
      initial-guard-timer            300
      subsq-guard-timer              300
      tcp-flow-time-limit            86400
      tcp-initial-guard-timer        300
      tcp-subsq-guard-timer          300
      tcp-number-of-ports-per-flow   2
      hnt-rtcp                       disabled
      algd-log-level                 NOTICE
      mbcd-log-level                 NOTICE
      red-flow-port                  1985
      red-mgcp-port                  1986
      red-max-trans                  10000
      red-sync-start-time            5000
      red-sync-comp-time             1000
      media-policing                 enabled
      max-signaling-bandwidth        7752190
      max-untrusted-signaling        80
      min-untrusted-signaling        20
      app-signaling-bandwidth        0
      tolerance-window               30
      rtcp-rate-limit                0
      min-media-allocation           32000
      min-trusted-allocation         60000
      deny-allocation                32000
      anonymous-sdp                  disabled
      arp-msg-bandwidth              32000
      fragment-msg-bandwidth         0
      rfc2833-timestamp              disabled
      default-2833-duration          100
      rfc2833-end-pkts-only-for-non-sig enabled
      translate-non-rfc2833-event    disabled
      dnsalg-server-failover         disabled
```

```
      last-modified-by               admin@console
      last-modified-date             2010-09-08 10:22:03

network-interface
      name                           wancom0
      sub-port-id                    0
      description
      hostname
      ip-address                     192.9.230.221
      pri-utility-addr
      sec-utility-addr
      netmask                        255.255.255.0
      gateway                        192.9.230.254
      sec-gateway
      gw-heartbeat
            state                          disabled
            heartbeat                      0
            retry-count                    0
            retry-timeout                  1
            health-score                   0
      dns-ip-primary
      dns-ip-backup1
      dns-ip-backup2
      dns-domain
      dns-timeout                    11
        hip-ip-list
      ftp-address
        icmp-address
      snmp-address
      telnet-address
      last-modified-by               admin@console
      last-modified-date             2011-08-12 10:21:39
```

ANNOTATION: The network interface below defines the IP addresses on the interface connected to the network on which the Avaya elements reside.

```
network-interface
      name                           s0p0
      sub-port-id                    0
      description
      hostname
      ip-address                     10.80.130.250
      pri-utility-addr
      sec-utility-addr
      netmask                        255.255.255.0
      gateway                        10.80.130.1
      sec-gateway
      gw-heartbeat
            state                          disabled
            heartbeat                      0
            retry-count                    0
            retry-timeout                  1
            health-score                   0
      dns-ip-primary
      dns-ip-backup1
```

```
      dns-ip-backup2
      dns-domain                      attavaya.com
      dns-timeout                     11
        hip-ip-list                   10.80.130.250
      ftp-address
        icmp-address                  10.80.130.250
      snmp-address
      telnet-address
      last-modified-by                admin@console
      last-modified-date              2011-08-12 14:58:25
```

ANNOTATION: The network interface below defines the IP addresses on the interface connected to the network on which the AT&T IP Flexible Reach service resides.

```
network-interface
      name                            s1p0
      sub-port-id                     0
      description
      hostname
      ip-address                      192.168.62.51
      pri-utility-addr
      sec-utility-addr
      netmask                         255.255.255.128
      gateway                         192.168.62.1
      sec-gateway
      gw-heartbeat
            state                           disabled
            heartbeat                       0
            retry-count                     0
            retry-timeout                   1
            health-score                    0
      dns-ip-primary
      dns-ip-backup1
      dns-ip-backup2
      dns-domain
      dns-timeout                     11
        hip-ip-list                     192.168.62.50
      ftp-address
        icmp-address                    192.168.62.50
      snmp-address
      telnet-address
      last-modified-by                admin@console
      last-modified-date              2011-08-12 10:24:07
ntp-config
      server                          192.9.1.2
      last-modified-by                admin@console
      last-modified-date              2009-03-12 10:20:46

phy-interface
      name                            wancom0
      operation-type                  Control
      port                            2
      slot                            0
      virtual-mac
```

```
      wancom-health-score            9
      last-modified-by               admin@console
      last-modified-date             2011-08-12 10:21:30

phy-interface
      name                           s0p0
      operation-type                 Media
      port                           0
      slot                           0
      virtual-mac                    00:08:25:a0:f3:68
      admin-state                    enabled
      auto-negotiation               enabled
      duplex-mode                    FULL
      speed                          100
      last-modified-by               admin@console
      last-modified-date             2011-08-13 15:29:00
phy-interface
      name                           s1p0
      operation-type                 Media
      port                           0
      slot                           1
      virtual-mac                    00:08:25:a0:f3:6e
      admin-state                    enabled
      auto-negotiation               enabled
      duplex-mode                    FULL
      speed                          100
      last-modified-by               admin@console
      last-modified-date             2011-08-13 15:29:23
```

ANNOTATION: The realm configuration **ATT** below represents the external network on which the AT&T IP Flexible Reach service resides, and applies SIP manipulations **ModifyMaxptime.**

```
realm-config
      identifier                     ATT
      description
      addr-prefix                    0.0.0.0
      network-interfaces
                                     s1p0:0
      mm-in-realm                    enabled
      mm-in-network                  enabled
      mm-same-ip                     enabled
      mm-in-system                   enabled
      bw-cac-non-mm                  disabled
      msm-release                    disabled
      generate-UDP-checksum          disabled
      max-bandwidth                  0
      fallback-bandwidth             0
      max-priority-bandwidth         0
      max-latency                    0
      max-jitter                     0
      max-packet-loss                0
      observ-window-size             0
      parent-realm
      dns-realm
```

```
media-policy
in-translationid
out-translationid
in-manipulationid              modifyMaxptime
out-manipulationid             NAT_IP
manipulation-string
class-profile
average-rate-limit             0
access-control-trust-level     none
invalid-signal-threshold       4
maximum-signal-threshold       3000
untrusted-signal-threshold     10
nat-trust-threshold            0
deny-period                    60
ext-policy-svr
symmetric-latching             disabled
pai-strip                      disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching            none
restriction-mask               32
accounting-enable              enabled
user-cac-mode                  none
user-cac-bandwidth             0
user-cac-sessions              0
icmp-detect-multiplier         0
icmp-advertisement-interval    0
icmp-target-ip
monthly-minutes                0
net-management-control         disabled
delay-media-update             disabled
refer-call-transfer            disabled
codec-policy
codec-manip-in-realm           disabled
constraint-name
call-recording-server-id
stun-enable                    disabled
stun-server-ip                 0.0.0.0
stun-server-port               3478
stun-changed-ip                0.0.0.0
stun-changed-port              3479
match-media-profiles
qos-constraint
last-modified-by               admin@console
last-modified-date             2009-04-22 19:26:23
```

ANNOTATION: The realm configuration **Enterprise** below represents the internal network on which the Avaya elements reside.

```
realm-config
      identifier               Enterprise
      description
      addr-prefix              0.0.0.0
```

```
network-interfaces              s0p0:0
mm-in-realm                     enabled
mm-in-network                   enabled
mm-same-ip                      enabled
mm-in-system                    enabled
bw-cac-non-mm                   disabled
msm-release                     disabled
generate-UDP-checksum           disabled
max-bandwidth                   0
fallback-bandwidth              0
max-priority-bandwidth          0
max-latency                     0
max-jitter                      0
max-packet-loss                 0
observ-window-size              0
parent-realm
dns-realm
media-policy
in-translationid
out-translationid
in-manipulationid
out-manipulationid
manipulation-string
class-profile
average-rate-limit              0
access-control-trust-level      high
invalid-signal-threshold        0
maximum-signal-threshold        0
untrusted-signal-threshold      0
nat-trust-threshold             0
deny-period                     30
ext-policy-svr
symmetric-latching              disabled
pai-strip                       disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching             none
restriction-mask                32
accounting-enable               enabled
user-cac-mode                   none
user-cac-bandwidth              0
user-cac-sessions               0
icmp-detect-multiplier          0
icmp-advertisement-interval     0
icmp-target-ip
monthly-minutes                 0
net-management-control          disabled
delay-media-update              disabled
refer-call-transfer             disabled
codec-policy
codec-manip-in-realm            disabled
constraint-name
call-recording-server-id
```

```
      stun-enable                    disabled
      stun-server-ip                 0.0.0.0
      stun-server-port               3478
      stun-changed-ip                0.0.0.0
      stun-changed-port              3479
      match-media-profiles
      qos-constraint
      last-modified-by               admin@console
      last-modified-date             2011-08-12 19:50:37
```

ANNOTATION: The session agent below represents Notification Solution used in this reference configuration.

```
session-agent
      hostname                       ANS
      ip-address                     10.80.130.230
      port                           5060
      state                          enabled
      app-protocol                   SIP
      app-type
      transport-method               UDP+TCP
      realm-id                       Enterprise
      egress-realm-id
      description                    Avaya Notification Solution
      carriers
      allow-next-hop-lp              enabled
      constraints                    disabled
      max-sessions                   0
      max-inbound-sessions           0
      max-outbound-sessions          0
      max-burst-rate                 0
      max-inbound-burst-rate         0
      max-outbound-burst-rate        0
      max-sustain-rate               0
      max-inbound-sustain-rate       0
      max-outbound-sustain-rate      0
      min-seizures                   5
      min-asr                        0
      time-to-resume                 0
      ttr-no-response                0
      in-service-period              0
      burst-rate-window              0
      sustain-rate-window            0
      req-uri-carrier-mode           None
      proxy-mode
      redirect-action
      loose-routing                  enabled
      send-media-session             enabled
      response-map
      ping-method                    OPTIONS;hops=0
      ping-interval                  180
      ping-send-mode                 keep-alive
      ping-in-service-response-codes
      out-service-response-codes
      media-profiles
```

```
      in-translationid
      out-translationid
      trust-me                      disabled
      request-uri-headers
      stop-recurse
      local-response-map
      ping-to-user-part
      ping-from-user-part
      li-trust-me                   disabled
      in-manipulationid
      out-manipulationid
      manipulation-string
      p-asserted-id
      trunk-group
      max-register-sustain-rate     0
      early-media-allow
      invalidate-registrations      disabled
      rfc2833-mode                  none
      rfc2833-payload               0
      codec-policy
      enforcement-profile
      refer-call-transfer           disabled
      reuse-connections             TCP
      tcp-keepalive                 enabled
      tcp-reconn-interval           0
      max-register-burst-rate       0
      register-burst-window         0
      last-modified-by              admin@console
      last-modified-date            2011-08-17 17:36:26
```

ANNOTATION: The session agent below represents the AT&T IP Flexible Reach service border element.

```
session-agent
      hostname                      135.242.225.210
      ip-address                    135.242.225.210
      port                          5060
      state                         enabled
      app-protocol                  SIP
      app-type
      transport-method              UDP
      realm-id                      ATT
      egress-realm-id
      description                   AT&T Border Element
      carriers
      allow-next-hop-lp             enabled
      constraints                   disabled
      max-sessions                  0
      max-inbound-sessions          0
      max-outbound-sessions         0
      max-burst-rate                0
      max-inbound-burst-rate        0
      max-outbound-burst-rate       0
      max-sustain-rate              0
      max-inbound-sustain-rate      0
```

```
     max-outbound-sustain-rate      0
     min-seizures                   5
     min-asr                        0
     time-to-resume                 0
     ttr-no-response                0
     in-service-period              0
     burst-rate-window              0
     sustain-rate-window            0
     req-uri-carrier-mode           None
     proxy-mode
     redirect-action
     loose-routing                  enabled
     send-media-session             enabled
     response-map
     ping-method                    OPTIONS;hops=70
     ping-interval                  180
     ping-send-mode                 keep-alive
     ping-all-addresses             disabled
     ping-in-service-response-codes
     out-service-response-codes
     media-profiles
     in-translationid
     out-translationid
     trust-me                       disabled
     request-uri-headers
     stop-recurse
     local-response-map
     ping-to-user-part
     ping-from-user-part
     li-trust-me                    disabled
     in-manipulationid
     out-manipulationid
     manipulation-string
     p-asserted-id
     trunk-group
     max-register-sustain-rate      0
     early-media-allow
     invalidate-registrations       disabled
     rfc2833-mode                   none
     rfc2833-payload                0
     codec-policy
     enforcement-profile
     refer-call-transfer            disabled
     reuse-connections              NONE
     tcp-keepalive                  none
     tcp-reconn-interval            0
     max-register-burst-rate        0
     register-burst-window          0
     last-modified-by               admin@console
     last-modified-date             2011-08-17 17:36:20

session-agent
     hostname                       1.1.1.1
     ip-address                     1.1.1.1
     port                           5060
```

```
state                          disabled(Only enabled for failover testing)
app-protocol                   SIP
app-type
transport-method               UDP
realm-id                       ATT
egress-realm-id
description                    AT&T Failover
carriers
allow-next-hop-lp              enabled
constraints                    disabled
max-sessions                   0
max-inbound-sessions           0
max-outbound-sessions          0
max-burst-rate                 0
max-inbound-burst-rate         0
max-outbound-burst-rate        0
max-sustain-rate               0
max-inbound-sustain-rate       0
max-outbound-sustain-rate      0
min-seizures                   5
min-asr                        0
time-to-resume                 0
ttr-no-response                0
in-service-period              0
burst-rate-window              0
sustain-rate-window            0
req-uri-carrier-mode           None
proxy-mode
redirect-action
loose-routing                  enabled
send-media-session             enabled
response-map
ping-method                    OPTIONS;hops=70
ping-interval                  180
ping-send-mode                 keep-alive
ping-all-addresses             disabled
ping-in-service-response-codes
out-service-response-codes
media-profiles
in-translationid
out-translationid
trust-me                       disabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me                    disabled
in-manipulationid
out-manipulationid
manipulation-string
p-asserted-id
trunk-group
max-register-sustain-rate      0
early-media-allow
```

```
invalidate-registrations       disabled
rfc2833-mode                   none
rfc2833-payload                0
codec-policy
enforcement-profile
refer-call-transfer            disabled
reuse-connections              NONE
tcp-keepalive                  none
tcp-reconn-interval            0
max-register-burst-rate        0
register-burst-window          0
last-modified-by               admin@console
last-modified-date             2011-08-17 17:36:20
```

ANNOTATION: The session-group is used for testing the failover scenario. In this case, an OPTION is sent to 1.1.1.1 and when no response is received, the 135.242.225.210 is tried

```
session-group
      group-name                    SP_PROXY
      description
      state                         enabled
      app-protocol                  SIP
      strategy                      RoundRobin
      dest
                                    1.1.1.1
                                    135.242.225.210
      trunk-group
      sag-recursion                 enabled
      stop-sag-recurse              401,407
      last-modified-by              admin@135.9.62.155
      last-modified-date            2012-03-19 17:11:46
```

ANNOTATION: The sip-config defines global sip-parameters, including SIP timers, SIP options, which realm to send requests to if not specified elsewhere, and enabling the SD to collect statistics on requests other than REGISTERs and INVITEs.

```
sip-config
      state                         enabled
      operation-mode                dialog
      dialog-transparency           enabled
      home-realm-id                 Enterprise
      egress-realm-id               Enterprise
      nat-mode                      None
      registrar-domain
      registrar-host
      registrar-port                0
      register-service-route        always
      init-timer                    500
      max-timer                     4000
      trans-expire                  32
      invite-expire                 180
      inactive-dynamic-conn         32
      enforcement-profile
      pac-method
      pac-interval                  10
      pac-strategy                  PropDist
      pac-load-weight               1
      pac-session-weight            1
      pac-route-weight              1
      pac-callid-lifetime           600
      pac-user-lifetime             3600
      red-sip-port                  1988
      red-max-trans                 10000
      red-sync-start-time           5000
      red-sync-comp-time            1000
```

```
add-reason-header             disabled
sip-message-len               4096
enum-sag-match                disabled
extra-method-stats            enabled
registration-cache-limit      0
register-use-to-for-lp        disabled
options                       max-udp-length=0
                                set-inv-exp-at-100-resp
add-ucid-header               disabled
last-modified-by              admin@console
last-modified-date            2011-08-12 10:22:04
```

ANNOTATION: The SIP interface below is used to communicate with the AT&T IP Flexible Reach service.

```
sip-interface
      state                         enabled
      realm-id                      ATT
      description
      sip-port
            address                       192.168.62.51
            port                          5060
            transport-protocol            UDP
            tls-profile
            allow-anonymous               all
            ims-aka-profile
      carriers
      trans-expire                  0
      invite-expire                 0
      max-redirect-contacts         0
      proxy-mode
      redirect-action
      contact-mode                  none
      nat-traversal                 none
      nat-interval                  30
      tcp-nat-interval              90
      registration-caching          disabled
      min-reg-expire                300
      registration-interval         3600
      route-to-registrar            disabled
      secured-network               disabled
      teluri-scheme                 disabled
      uri-fqdn-domain
      trust-mode                    all
      max-nat-interval              3600
      nat-int-increment             10
      nat-test-increment            30
      sip-dynamic-hnt               disabled
      stop-recurse                  401,407
      port-map-start                0
      port-map-end                  0
      in-manipulationid
      out-manipulationid
      manipulation-string
      sip-ims-feature               disabled
      operator-identifier
      anonymous-priority            none
      max-incoming-conns            0
      per-src-ip-max-incoming-conns 0
      inactive-conn-timeout         0
      untrusted-conn-timeout        0
      network-id
      ext-policy-server
      default-location-string
      charging-vector-mode          pass
      charging-function-address-mode pass
      ccf-address
```

```
    ecf-address
    term-tgrp-mode                  none
    implicit-service-route          disabled
    rfc2833-payload                 101
    rfc2833-mode                    transparent
    constraint-name
    response-map
    local-response-map
    ims-aka-feature                 disabled
    enforcement-profile
    route-unauthorized-calls
    tcp-keepalive                   none
    add-sdp-invite                  disabled
    add-sdp-profiles
    last-modified-by                admin@console
    last-modified-date              2009-04-22 18:14:23
```

ANNOTATION: The SIP interface below is used to communicate with the Avaya elements.

```
sip-interface
    state                           enabled
    realm-id                        Enterprise
    description
    sip-port
        address                         10.80.130.250
        port                            5060
        transport-protocol              TCP
        tls-profile
        allow-anonymous                 all
        ims-aka-profile
    carriers
    trans-expire                    30
    invite-expire                   0
    max-redirect-contacts           0
    proxy-mode
    redirect-action
    contact-mode                    none
    nat-traversal                   none
    nat-interval                    30
    tcp-nat-interval                90
    registration-caching            disabled
    min-reg-expire                  300
    registration-interval           3600
    route-to-registrar              disabled
    secured-network                 disabled
    teluri-scheme                   disabled
    uri-fqdn-domain
    trust-mode                      all
    max-nat-interval                3600
    nat-int-increment               10
    nat-test-increment              30
    sip-dynamic-hnt                 disabled
    stop-recurse                    401,407
    port-map-start                  0
```

```
        port-map-end                   0
        in-manipulationid
        out-manipulationid
        manipulation-string
        sip-ims-feature                disabled
        operator-identifier
        anonymous-priority             none
        max-incoming-conns             0
        per-src-ip-max-incoming-conns  0
        inactive-conn-timeout          0
        untrusted-conn-timeout         0
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode           pass
        charging-function-address-mode pass
        ccf-address
        ecf-address
        term-tgrp-mode                 none
        implicit-service-route         disabled
        rfc2833-payload                101
        rfc2833-mode                   transparent
        constraint-name
        response-map
        local-response-map
        ims-aka-feature                disabled
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                  none
        add-sdp-invite                 disabled
        add-sdp-profiles
        last-modified-by               admin@console
        last-modified-date             2009-04-16 18:07:58
```

ANNOTATION: The sip-manipulation modifies the **maxptime** attribute to **ptime.**

```
sip-manipulation
        name                           modifyMaxptime
        description                    Modify maxptime attribute
        header-rule
                name                           ReplaceMaxptime
                header-name                    Content-Type
                action                         manipulate
                comparison-type                case-sensitive
                msg-type                       any
                methods                        INVITE
                match-value
                new-value
                element-rule
                        name                           modmline
                        parameter-name                 application/sdp
                        type                           mime
                        action                         find-replace-all
                        match-val-type                 any
```

```
                comparison-type                 case-sensitive
                match-value                     maxptime
                new-value                       ptime
      last-modified-by              admin@console
      last-modified-date            2011-10-22 19:25:08
```

ANNOTATION: The steering pools below defines the RTP port range on the respective realms.

```
steering-pool
      ip-address                    192.168.62.51
      start-port                    16384
      end-port                      32767
      realm-id                      ATT
      network-interface
      last-modified-by              admin@console
      last-modified-date            2011-08-25 19:11:47
steering-pool
      ip-address                    10.80.130.250
      start-port                    16384
      end-port                      32767
      realm-id                      Enterprise
      network-interface
      last-modified-by              admin@console
      last-modified-date            2011-08-12 10:25:12
system-config
      hostname                      Enterprise-Acme
      description
      location
      mib-system-contact
      mib-system-name
      mib-system-location
      snmp-enabled                  enabled
      enable-snmp-auth-traps        disabled
      enable-snmp-syslog-notify     disabled
      enable-snmp-monitor-traps     disabled
      enable-env-monitor-traps      disabled
      snmp-syslog-his-table-length  1
      snmp-syslog-level             WARNING
      system-log-level              WARNING
      process-log-level             NOTICE
      process-log-ip-address        0.0.0.0
      process-log-port              0
      collect
            sample-interval               5
            push-interval                 15
            boot-state                    disabled
            start-time                    now
            end-time                      never
            red-collect-state             disabled
            red-max-trans                 1000
            red-sync-start-time           5000
            red-sync-comp-time            1000
            push-success-trap-state       disabled
```

```
call-trace                    disabled
internal-trace                disabled
log-filter                    all
default-gateway               205.168.62.1
restart                       enabled
exceptions
telnet-timeout                0
console-timeout               0
remote-control                enabled
cli-audit-trail               enabled
link-redundancy-state         disabled
source-routing                enabled
cli-more                      disabled
terminal-height               24
debug-timeout                 0
trap-event-lifetime           0
last-modified-by              admin@console
last-modified-date            2011-08-12 10:20:46
```

7. Verification Steps

7.1. General

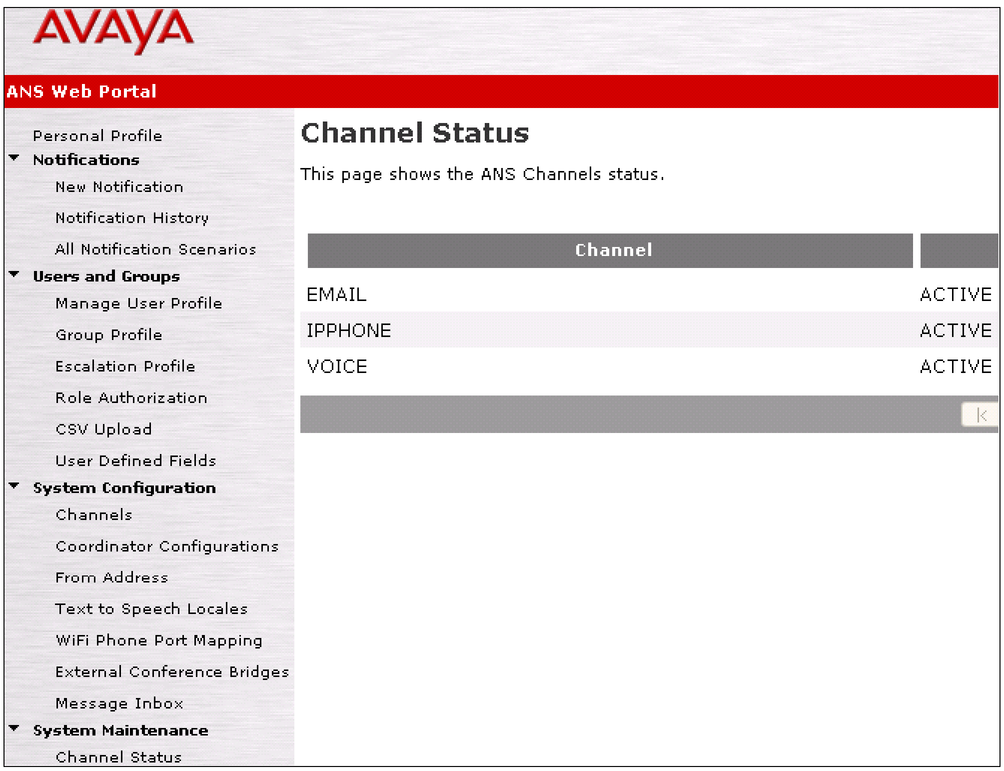
The following steps may be used to verify the configuration:

- Place an inbound call from PSTN to ANS, and verify that an announcement is played. Interact with the ANS prompts and verify that ANS responds properly to the DTMF digits entered.
- From the ANS web interface, trigger a notification and verify the notification is delivered to the subscriber and the participant is able to confirm the receipt of notification.

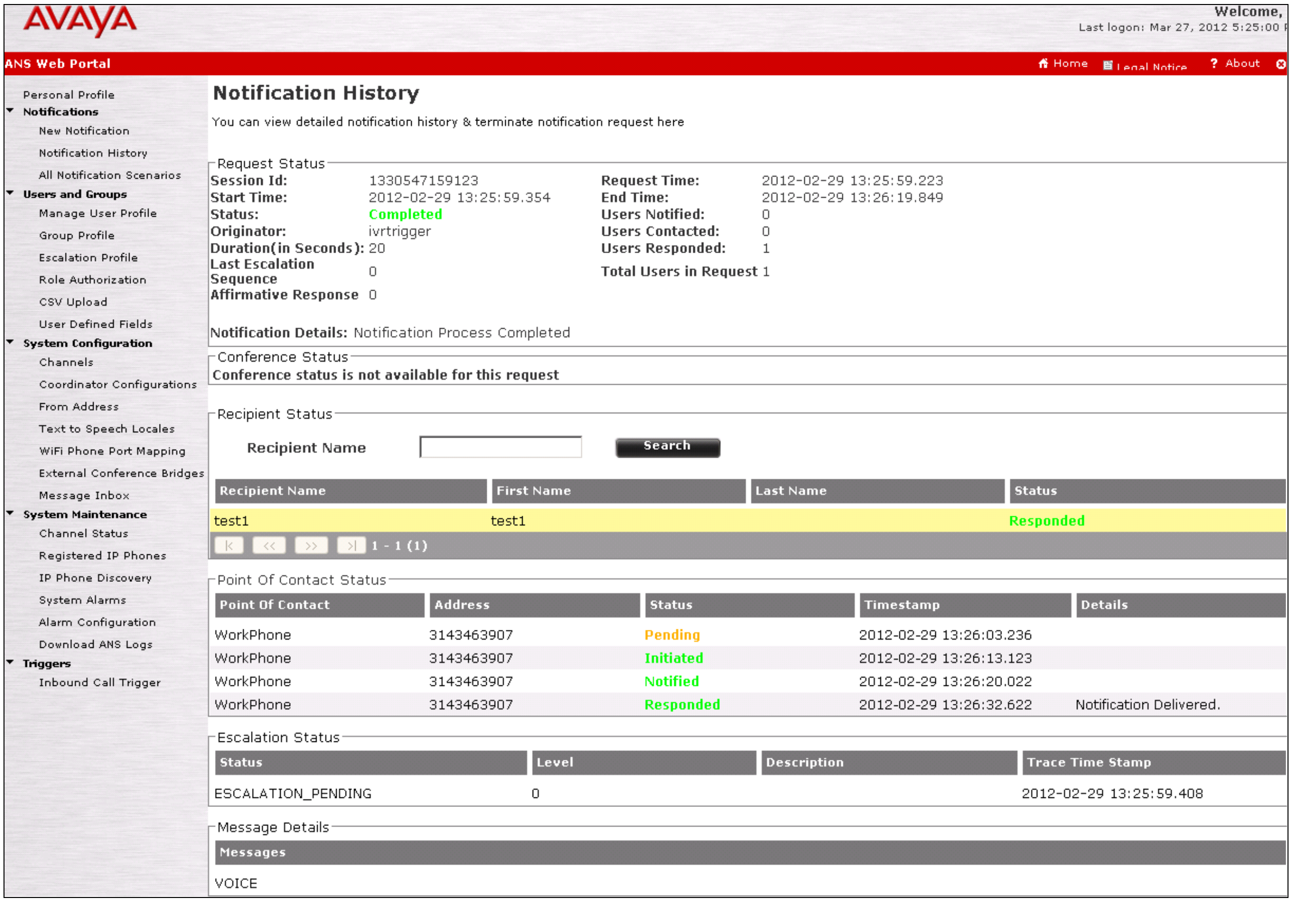
7.2. Avaya Notification Solution

The following commands are issued from the System Manager console.

1. Navigate to **System Maintenance→Channel Status** to verify the SIP trunk is properly configured. If **VOICE** shows **ACTIVE** status, then the configuration is good.



2. The following screen shows the notification sent by ANS was successfully delivered to the subscriber.



8. Conclusion

As illustrated in these Application Notes, ANS and the Acme SBC can be configured to interoperate successfully with the AT&T IP Flexible Reach service. This solution provides users of ANS the ability to send outbound notifications from the web interface, trigger outbound notification by dialing into ANS and initiate and hold adhoc conference calls.

The sample configuration shown in these Application Notes is representative of a basic enterprise customer configuration and is intended to provide configuration guidance to supplement other Avaya product documentation. It is based upon formal interoperability compliance testing as part of the Avaya DevConnect Service Provider program.

9. References

The Avaya product documentation is available at http://support.avaya.com.

[1] *ANS R1.2 Administration Guide*, April 2011
[2] *Avaya Notification Solution 1.2 SP1 Administration Guide*, August 2011

Acme Packet Support (login required):
[3] http://support.acmepacket.com

AT&T IP Flexible Reach Service Descriptions:
[4] *AT&T IP Flexible Reach*
http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ ip-flexible-reach-enterprise /

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.