



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Avaya Notification Solution 2.0, 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.....	3
2.	General Test Approach and Test Results.....	3
2.1.	Interoperability Compliance Testing.....	4
2.2.	Known Limitations/Test Results.....	4
2.3.	Support.....	4
3.	Reference Configuration.....	5
3.1.	Illustrative Configuration Information.....	6
3.2.	Call Flows.....	7
4.	Equipment and Software Validated.....	9
5.	Configure Avaya Notification Solution Server.....	10
5.1.	Background.....	10
5.2.	Logging in to ANS.....	10
5.3.	Security Configuration.....	11
5.4.	VoIP Connection.....	12
5.5.	Text To Speech Locales Configuration.....	14
5.6.	From Address Configuration.....	14
5.7.	TTW Server.....	16
5.8.	Permitted Driver IP Address.....	17
5.9.	Inbound Number.....	18
5.10.	Message Inbox.....	19
5.11.	Manage User Profile.....	20
5.12.	Add Outbound Notifications.....	21
5.13.	Add Inbound Triggers.....	28
5.14.	Avaya Media Server.....	32
6.	Configure Acme Packet Session Border Controller.....	34
7.	Verification Steps.....	52
7.1.	General.....	52
7.2.	Avaya Notification Solution.....	52
7.3.	Avaya Media Server.....	53
8.	Conclusion.....	53
9.	References.....	54

# 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, Voice Mail Detection, Notification Message retrieval and conference. It can be applied to emergency broadcast and system alarming.

An Acme Packet Net-Net (Acme Packet 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 Packet 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
- Outbound calls from ANS server to detect Voice Mail service and leave a message
- 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 call to ANS server to retrieve Message notification left for the subscribers
- Inbound call to ANS server to retrieve Conference notification and join the conference
- 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 2.0 does not support Compressed RTP (cRTP). So, cRTP was disabled on AT&T IP Flexible Reach service.
2. ANS 2.0 does not support G729 with annexb=yes as it is unable to detect Voice Mail service when silence suppression is enabled.
3. ANS 2.0 does not support transfer of calls to a help desk.

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

## 2.3. Support

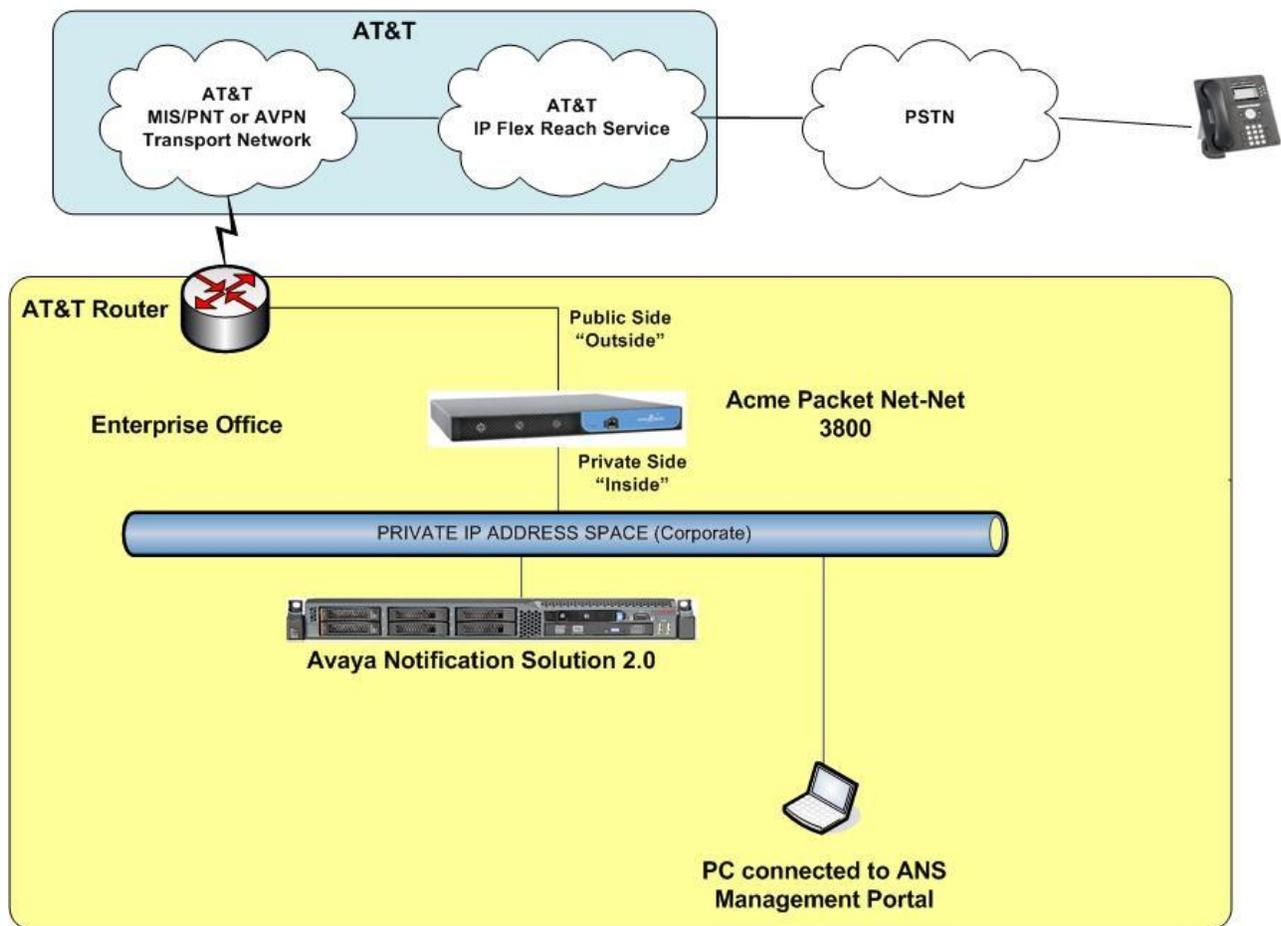
AT&T customers may obtain support for the AT&T IP Flexible Reach service by calling (888) 288-8362.

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<sup>1</sup> provides SIP Session Border Controller functionality between the AT&T IP Flexible Reach service and the enterprise internal network<sup>2</sup>. UDP transport protocol is used between the Acme Packet Net-Net SD and the AT&T IP Flexible Reach service.



**Figure 1: Reference Configuration**

<sup>1</sup> Although an Acme Net-Net 3800 was used in the reference configuration, the 4250 and 4500 platforms are also supported.

<sup>2</sup> 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.

<b>Component</b>	<b>Illustrative Value in these Application Notes</b>
Avaya Notification Solution with Avaya Media Server	10.80.130.230
<b>Acme Packet Session Border Controller</b>	
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
<b>AT&amp;T IP Flexible Reach Service</b>	
Border Element IP Address	135.242.225.210

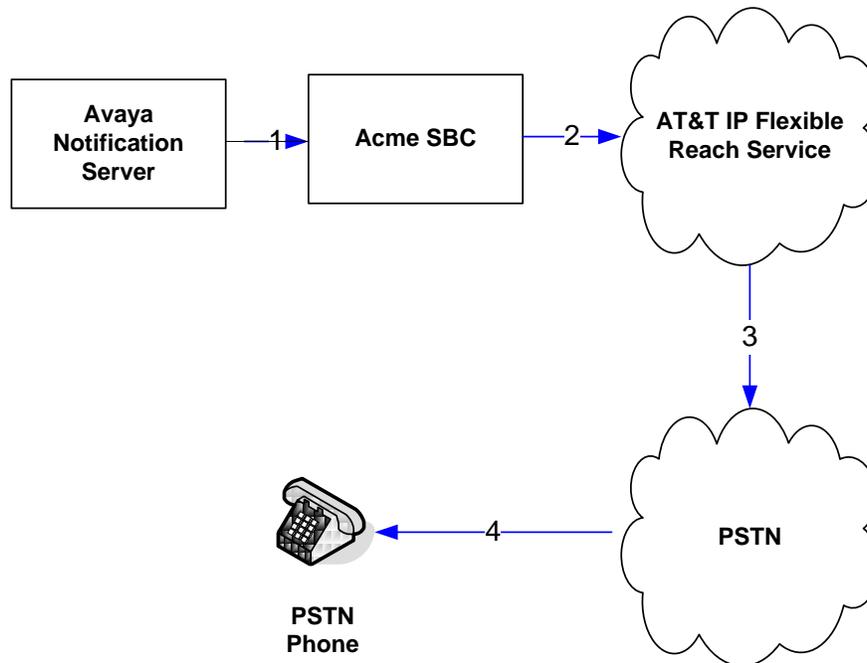
**Table 1: Illustrative Values Used in this Reference Configuration**

### 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.

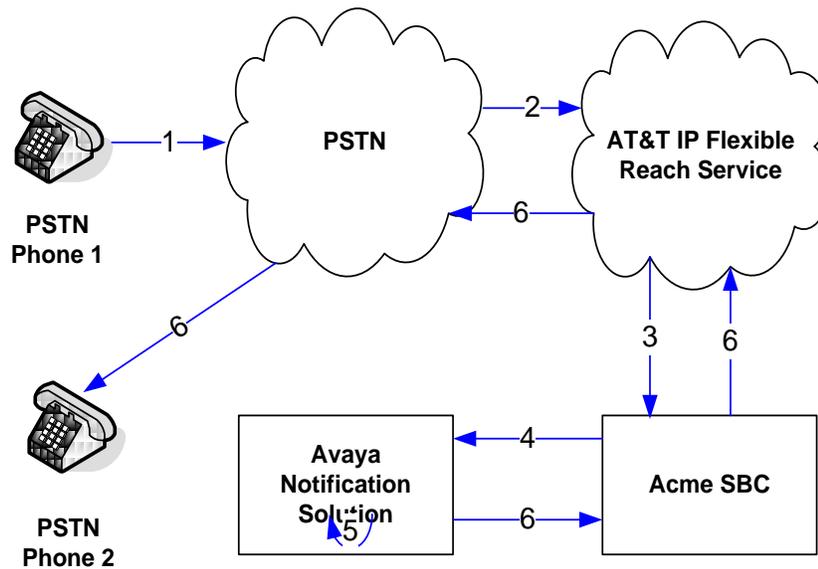
1. ANS originates a call to PSTN phone
2. Acme Packet SBC performs any necessary SIP header modifications, and routes the call to the AT&T IP Flexible Reach Service
3. The AT&T IP Flexible Reach service routes the call to PSTN
4. PSTN delivers the notification call to a PSTN phone subscriber on ANS. If the subscriber does not pick up the phone and a voicemail is detected, ANS leaves the notification message on subscriber's voicemail.



**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 Packet SBC at CPE
4. Acme Packet SBC performs any necessary SIP header modifications, and routes the call to ANS
5. Based upon the option entered by PSTN Phone 1, subscriber has an option to record a new message or retrieve a notification sent earlier or trigger an outbound notification
6. Same as Steps 1 to 4 in the first scenario and only performed if an outbound notification is triggered in **Step 5**



**Inbound Call Handled by ANS to record/retrieve message or trigger an Outbound Notification**

## 4. Equipment and Software Validated

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

<b>Component</b>	<b>Version</b>
Avaya Notification Solution 2.0	ANS2.0.3025 with InboundCallPatch3025
Avaya Media Server	Version 7.5.0.724
Avaya Notification Solution 2.0 running on VMWare Virtual Machine	VMware vSphere ESX4.0 running 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 [2] for further details if necessary. **Note** that in the following sections only the parameters used in this reference configuration are discussed. Default values are used for all other field configurations.

### 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 can detect voice mail system and leave a message for the subscriber on their voicemail. Subscribers can dial into ANS to retrieve the notification. 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 its 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. Additionally Voice Mail Detection and Notification retrieval functionality was also tested.

When an inbound call arrives at ANS, it matches the user part of the **To** header in the INVITE to map to the appropriate trigger. 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. Logging in to ANS

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

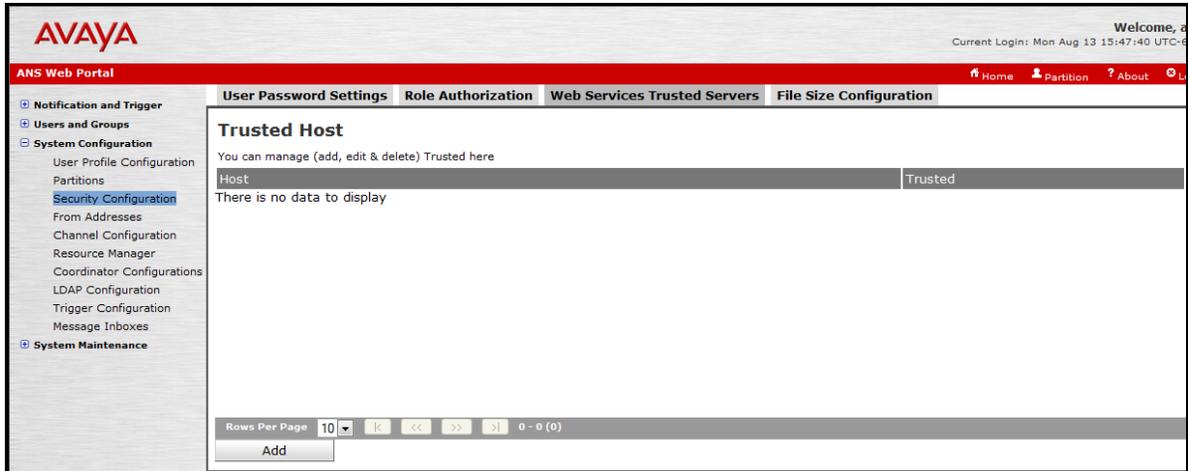


ANS Login Screen

### 5.3. Security Configuration

This section describes the steps to add ANS server as trusted host.

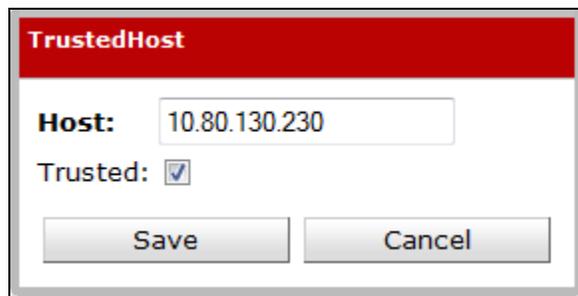
1. Navigate to **System Configuration**→**Security Configuration** and select **Web Services Trusted Servers** tab. Click **Add**.



Security Configuration – Trusted Host

On the pop-up screen **TrustedHost** shown below, configure as follows:

- **Host** – Enter IP address of ANS
- **Trusted** – Check the box
- Click **Save**

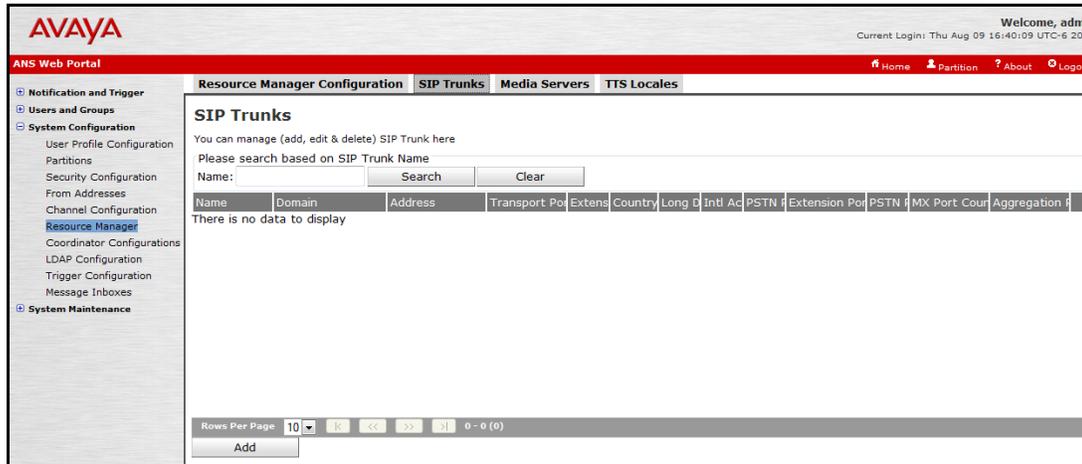


Security Configuration – TrustedHost

## 5.4. VoIP Connection

This section describes the steps required to configure a SIP trunk between ANS and Acme Packet SBC.

1. In the left pane, navigate to **System Configuration** → **Resource Manager** and select **SIP Trunks** tab. On the **SIP Trunks** page, click **Add**.



**Resource Manager – SIP Trunks**

On the pop-up screen **Add SIP Trunk** shown below, configure as follows:

- **Name** – Enter any informative string
- **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 Packet SBC
- **Address** – Set to IP Address of the Acme Packet SBC internal interface
- **Transport** – Set to **TCP** (used in this reference configuration)
- **Extension Length** – Set to any valid length (default **7**)
- **Extension Port Count** – Set to a valid number based upon the number of licenses
- **Transport Port No** – Set to **5060** (default)
- **PSTN Port Count** – Set to a valid number based upon the number of licenses
- **Aggregation Port Count** – Set to a valid number based upon the number of licenses
- Click **Save**

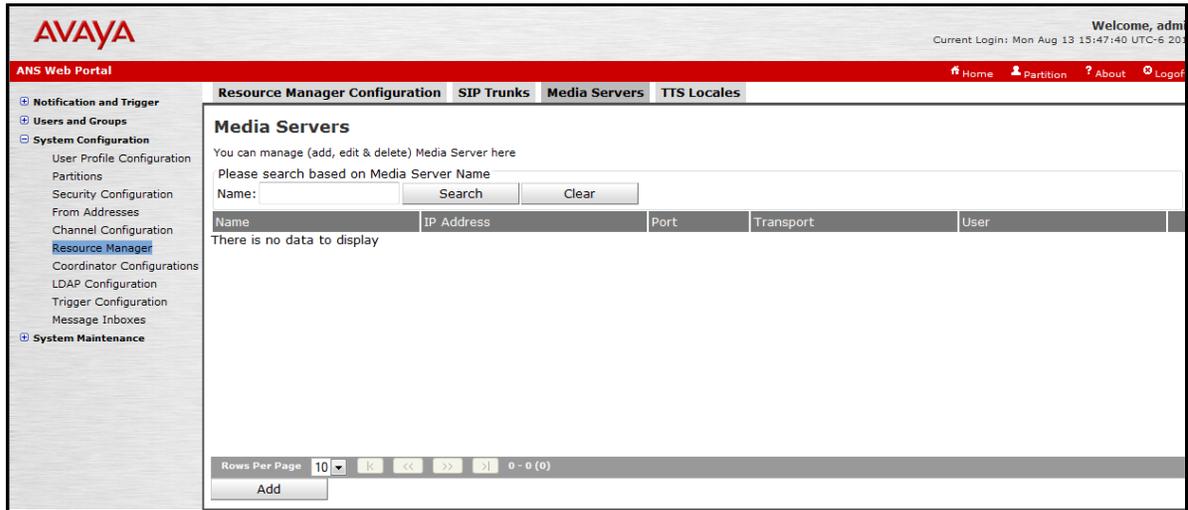
The screenshot shows the 'Add SIP Trunk' pop-up form. The form contains the following fields and values:

Name:	ToSBC	Domain:	135.242.225.210
Address:	10.80.130.250	Transport:	TCP
Extension Length:	7	Country Code:	
Long Distance Prefix:		Intl Access Code:	
PSTN Prefix:		Extension Port Count:	20
Transport Port No:	5060	PSTN Port Count:	20
Priority:	1	MX Port Count:	
Aggregation Port Count:	100		

At the bottom of the form are 'Save' and 'Cancel' buttons.

**Resource Manager – Add SIP Trunk**

- In the left pane, navigate to **System Configuration** → **Resource Manager** and select **Media Servers** tab. On the **Media Servers** page, click **Add**



### Resource Manager – Media Servers

On the pop-up screen **Add Media Server** shown below, configure as follows:

- **Name** – Enter any informative string
- **IP Address** – Set to IP Address of the of the Media Server which is **10.80.130.230** in this reference configuration
- Use default for all other fields and click **Save**

### Resource Manager – Add Media Server

## 5.5. 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** → **Resource Manager** and select the **TTS Locales** tab. Check the appropriate **Enable** box and click **Save**.

The screenshot shows the AVAYA ANS Web Portal interface. The left navigation pane is expanded to 'System Configuration' > 'Resource Manager'. The main content area is titled 'TTS Locales' and contains a table of locale configurations. The 'Channel Type' is set to 'Voice'. The table lists various locales with checkboxes for enabling them. The 'English-UNITE' checkbox is checked. The page also includes a 'Save' button and a 'Rows Per Page' dropdown set to 10.

Locale	Enable
English-UNITE	<input checked="" type="checkbox"/>
Catalan-SPAI	<input type="checkbox"/>
Portuguese-B	<input type="checkbox"/>
Valencian-SP	<input type="checkbox"/>
Spanish-COLC	<input type="checkbox"/>
Danish-DENM	<input type="checkbox"/>
Dutch-NEDER	<input type="checkbox"/>
English-UNITE	<input type="checkbox"/>
Finnish-FINLA	<input type="checkbox"/>
Chinese-Taiwan	<input type="checkbox"/>

Resource Manager – TTS Locales

## 5.6. From Address Configuration

This section describes steps to configure the user part for the **From** header to be sent in an outbound call. An address and display name are configured in the following steps.

1. Navigate to **System Configuration** → **From Address** and select **From Address** tab. On the **From Address** page, click **Add**.

The screenshot shows the AVAYA ANS Web Portal interface. The left navigation pane is expanded to 'System Configuration' > 'From Address'. The main content area is titled 'From Address' and contains a table of from address configurations. The 'Channel' is set to 'Voice'. The 'From' field is set to 'anonymous'. The 'Default Address' is set to 'Yes'. The 'Partition' is set to 'default'. The page also includes a 'Search' button and an 'Add' button.

Channel	From	Default Address	Partition
Email	admin@ans.com	Yes	default
Voice	anonymous	Yes	default

From Address - From Address

On the pop-up screen **Add From Address** shown below, configure as follows:

- **Channel** – Select **Voice** from a drop-down list
- **From** – Enter a valid telephone number
- **Default Address** – Check this box for at least one address
- Click **Save**
- Repeat this step to configure additional addresses

**From Address – Add From Address**

2. Navigate to **System Configuration** → **From Address** and select **From Display Name** tab. On the **From Display Name** page, click **Add**.

Channel	Display Name	Default Address	Partition
Email	admin	Yes	default
Voice	anonymous	Yes	default

**From Address– From Display Name**

On the pop-up screen **Add Display Name** shown below, configure as follows:

- **Channel** – Select **Voice** from drop-down list
- **Display Name** – Enter any informative string
- **Default Address** – Check this box for at least one address
- Click **Save**
- Repeat this step to configure additional display names

From Address– Add Display Name

## 5.7. TTW Server

This section describes steps to configure the TTW Server.

1. Navigate to **System Configuration** → **Channel Configuration** and select **TTW SERVER** from the drop-down list in the **Select the Channel/Component to configure** field.

Channel Configuration – Select Component

On the subsequent **Channel Configurations** screen, configure as follows:

- **TTW IP ADDRESS** – Set to the IP address of the ANS Server
- **TTW IP ADDRESS 2** – Set to the IP address of the ANS Server

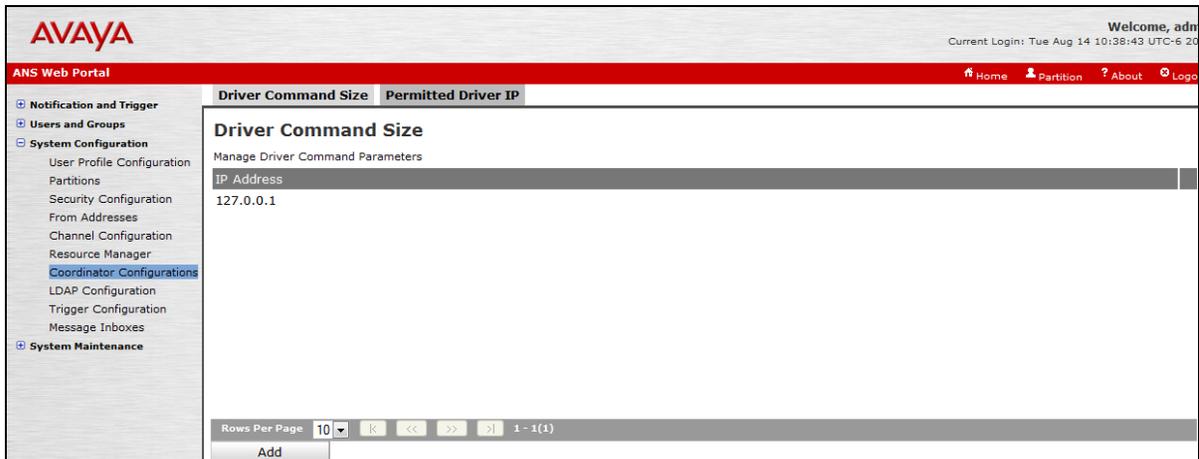
Property	Value	Description
TTW IP ADDRESS	10.80.130.230	TTW Service IP Address. Usually, TTW is installed c
TTW IP ADDRESS 2	10.80.130.230	TTW Service IP Address 2. Usually, TTW is instal
TTW PORT	1236	TTW Service port. (Default port is 1236)
TTW PORT 2	1236	TTW Service port 2. (Default port is 1236)

Channel Configuration – TTW Address

## 5.8. Permitted Driver IP Address

This section describes steps to configure the Permitted Driver IP Address.

1. Navigate to **System Configuration**→**Coordinator Configuration** and click **Add**.



**Coordinator Configuration – Permitted Driver IP**

On the pop-up screen **Add Driver IP Address** shown below set the **IP Address** field to ANS Server's IP address and click **Save**.

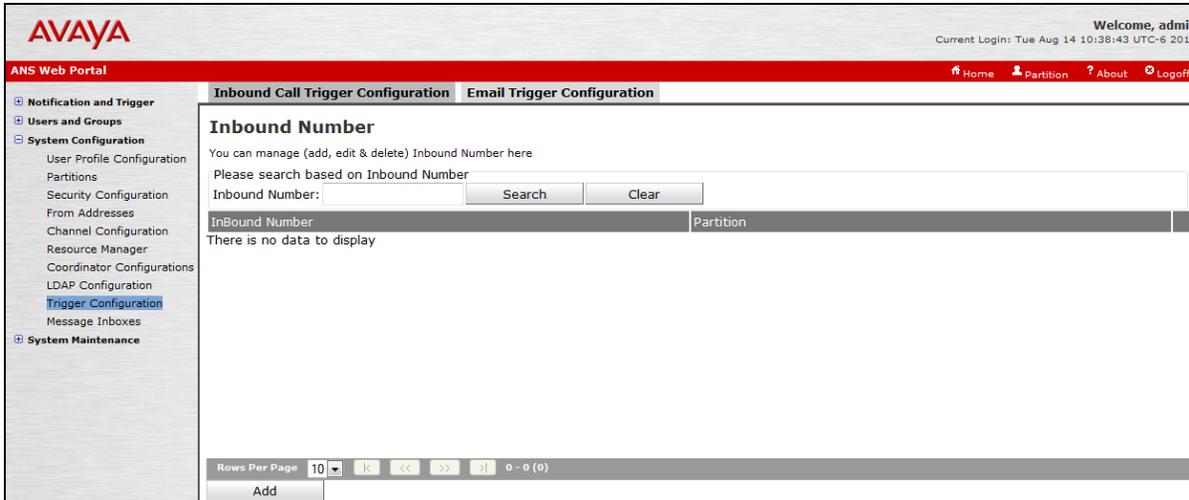


**Coordinator Configuration – Add Driver IP Address**

## 5.9. Inbound Number

ANS inspects the **To** header to determine the destination of the call. Inbound numbers are configured to determine which trigger is invoked when a call comes into ANS.

1. Navigate to **System Configuration**→**Trigger Configuration** and click **Add**.



**Trigger Configuration – Inbound Number**

On the pop-up screen **Add Inbound Number Data** shown below, configure as follows:

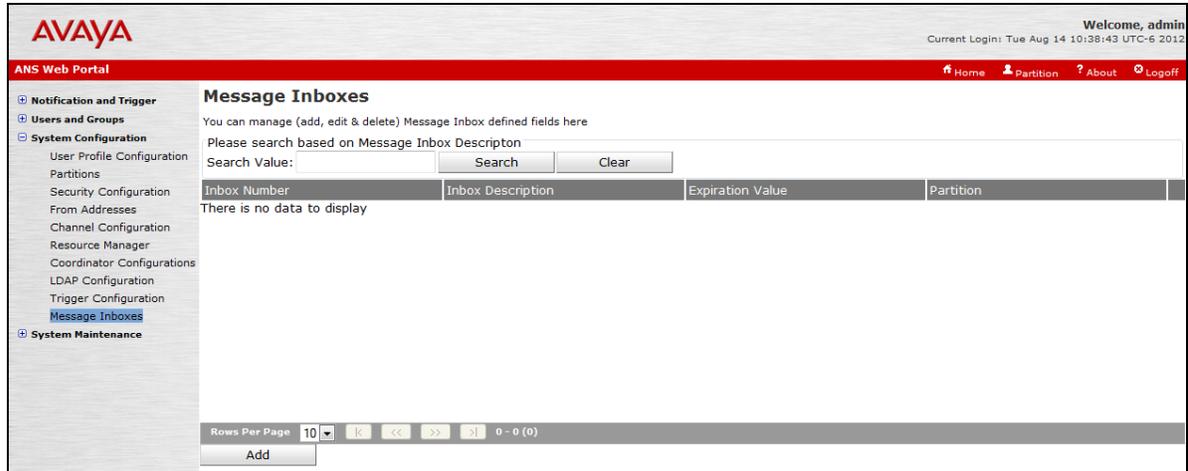
- **Inbound Number** – Set to a valid DID
- Click **Save**
- Repeat this step to configure additional inbound numbers

**Trigger Configuration – Add Inbound Number Data**

## 5.10. Message Inbox

Message inboxes are configured to store message notifications on ANS. Subscribers can call ANS to record or retrieve a message notification.

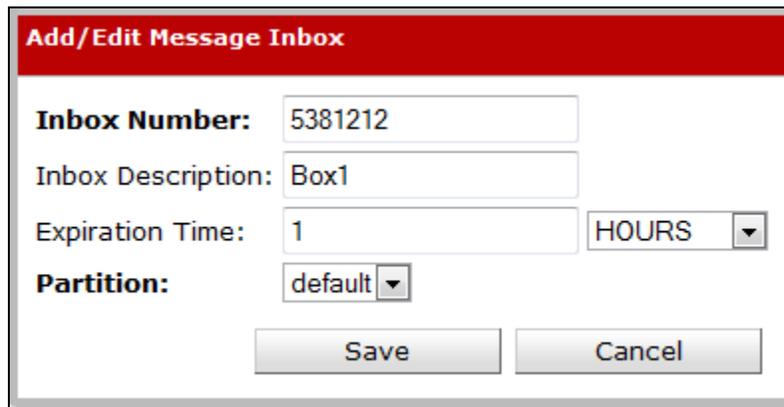
1. Navigate to **System Configuration**→**Message Inbox** and click **Add**.



Message Inboxes

On the pop-up screen **Add Inbound Number Data** shown below, configure as follows:

- **Inbox Number** – Set to any valid number
- **Inbox Description** – Enter any informative description
- Click **Save**
- Repeat this step to configure additional Message inboxes



Trigger Configuration – Add Inbound Number Data

## 5.11. Manage User Profile

The following steps show the subscriber configuration on ANS.

1. In the left pane, navigate to **Users and Groups** → **Users** and click **Add**.

The screenshot shows the 'Manage User Profile' page in the ANS Web Portal. The left navigation pane is expanded to 'Users and Groups' > 'Users'. The main content area has a heading 'Manage User Profile' and a sub-heading 'You can manage (add, edit & delete) user profile here'. Below this is a search bar with the text 'Please search based on User Id, First Name or Last Name.' and a 'Search Value:' input field. There are also dropdown menus for 'Role' (set to 'Select') and 'Active' (set to 'Ignore'). Below the search bar is a table with the following data:

User Id	First Name	Middle Name	Last Name
AUSER	Anonymous	AnsAdmin	Ans
admin	Admin	AnsAdmin	Ans

At the bottom of the table, there is a 'Rows Per Page' dropdown set to '10', navigation icons, and a '1 - 2(2)' indicator. Below the table are 'Add' and 'Remove All' buttons.

### Users – Manage User Profile

2. On the subsequent screen **Create User Profile** shown below, select the **User Details** tab and configure as follows:
  - **User Id** – Enter any valid id
  - **Time Zone** – Enter a valid timezone
  - **First Name** – Enter any informative string
  - **Last Name** – Enter any informative string
  - Click **Save**
  - Repeat this step to configure additional subscribers

The screenshot shows the 'Create User Profile' page in the ANS Web Portal, with the 'User Details' tab selected. The form contains the following fields:

- User Id:** PSTN1212
- Title:** (empty)
- Time Zone:** (UTC-06:00) - US/Mountain
- First Name:** 1212
- Last Name:** PSTN
- Middle Name:** (empty)
- Account Number:** (empty)
- Role:** User
- Telephone Security PIN:** (empty)
- Web Login Password:** (empty)
- Activate:**

At the bottom of the form are 'Save' and 'Cancel' buttons.

### Users – User Details

3. Select the **Contact Information** tab and enter valid contact information.

**Note:** Multiple contacts can be entered and Notification will be sent simultaneously to all the contacts.

**AVAYA** Current

ANS Web Portal Home

**Manage User Profile**  
You can manage (add, edit & delete) user profile here

**User Details** **Contact Information**

Point of Contact Information

	Contact Information	Urgent Notifications Rule		Normal Notifications Rule	
		Time Profile	Delay(s)	Time Profile	Delay(s)
Work Phone	3035381212	Anytime	0	Anytime	0
Mobile Phone		Anytime		Anytime	
Home Phone		Anytime		Anytime	
IP Phone Extension		Anytime		Anytime	
SMS Address		Anytime		Anytime	
Work Email		Anytime		Anytime	
Personal Email		Anytime		Anytime	
Sametime Address		Anytime		Anytime	
XMPP Address		Anytime		Anytime	

Save Cancel

**Users – Contact Information**

4. Repeat above step to configure additional subscribers.

## 5.12. 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 and Trigger** → **Notifications Scenarios** and click **Add**.

ANS Web Portal Home Partition About

**Notification Scenarios**  
You can manage (add, edit & delete) notification template here

Please search based on name, description

Scenario Name/Description:  Search Clear

Scenario Name	Description	Owner
There is no data to display		

Rows Per Page 10 |< << >> >| 0 - 0 (0)

Add

**Notification Scenarios**

2. On the subsequent screen, select **Details** tab and configure as follows:
  - **Scenario Name** – Enter any informative string
  - **Scenario Description** – Enter a description (Optional)

The screenshot shows the 'Notification Scenarios' configuration page in the ANS Web Portal. The left sidebar contains a navigation menu with 'Notification and Trigger' expanded, showing options like 'My Notification Scenarios', 'Notification Scenarios', 'My Notification History', 'Notification History', 'My Escalations', 'Escalations', 'Usage Report', 'Inbound Call Triggers', 'Email Trigger Configuration', and 'Conference Bridges'. Below this are 'Users and Groups', 'System Configuration', and 'System Maintenance'. The main content area is titled 'Notification Scenarios' and includes a sub-header 'You can manage (add, edit & delete) notification template here'. There are five tabs: 'Details', 'Message', 'Users', 'Groups', 'Escalations', and 'Trigger Permissions'. The 'Details' tab is active, showing the following fields:
 

- Scenario Name:** OutboundMessage
- Scenario Description:** messages to subscribers
- Owner:** admin (with a 'Select' button)
- Expiration Time:** 1 (with a dropdown menu set to 'HOURS')
- Priority:** Normal (selected), Urgent, Crisis

Notification Scenarios – Details

3. Select **Message** tab and click **Add Message**.

The screenshot shows the 'Notification Scenarios' configuration page in the ANS Web Portal, now with the 'Message' tab selected. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Notification Scenarios' and includes the same sub-header. The 'Message' tab is active, showing the following fields:
 

- Common Messages** section:
  - Text Message Subject:** (empty text input)
  - Text Message Body:** (empty text area)
  - Audio Message:** (empty text input with a 'Select W' button to its right)
- Messages** section:
  - A message: 'There is no data to display'
- Footer:**
  - Rows Per Page: 5 (dropdown)
  - Navigation buttons: <|, <<, >>, >|
  - Page info: 0 - 0 (0)
  - Add Message** button

Notification Scenarios – Message

On the pop-up screen **Add New Message** shown below, configure as follows:

- **Channel** – Select **VOICE** from the drop-down list
- **Caller ID** – Select one of the numbers configured in **Section 5.6, Step 1**
- **Display Name** - Select one of the values configured in **Section 5.6, Step 2**
- **Enable Inbound** – This field is enabled only if the notification needs to be saved in a Message Box configured in **Section 5.10** for subscribers to retrieve message later. Select one of the values configured in **Section 5.10, Step 1**
- **Greeting Prompt** – Enter any valid prompt which is played to the subscriber when the call is answered
- **Message Body** – Enter any valid message
- **Leave a message to voicemail** – Check this so that the message can be left on voicemail in case the subscriber is unavailable
- **Use same message body for voicemail** – Check this if the Voicemail Body is same as the Message Body. In this reference configuration, this field is checked
- Click **Save**

**Add New Message**

Messages Choice

Channel Messages  
Required Fields in bold: 1.Message Body 2.Greeting Prompt must be provided

**Channel:** VOICE **Locale:** en-US  
**Caller ID:** 7325551212 **Display Name:** ANS1212  
Retry Count: 0 Retry Delay(Seconds): 0 Ring Timeout(seconds):  
 Authenticate Recipient  Enable OutBound  Work Phone  
 Bypass Human Detection  Enable InBound 5381212  Mobile Phone  
 Audio Conference ANS Ad-Hoc Conference  Home Phone

**Greeting Prompt:** This is an important Message from Avaya Select Wave File Record Through Telephone

**Message Body:** emergency repairs. Please call 7325551212 for further details Select Wave File Record Through Telephone

Bypass Answer Machine Detection?  Leave a message to voicemail?  Use same message body for voicemail?

**Voicemail Body:** The building is closed today due to emergency rep Select Wave File Record Through Telephone

Save Cancel

**Notification Scenarios – Add New Message**

- In case an adhoc conference is configured (which is 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.

**Add New Message**

**Messages** **Choice**

Channel Messages  
Required Fields in bold: 1.Message Body 2.Greeting Prompt must be provided

**Channel:** VOICE **Locale:** en-US  
**Caller ID:** 7325551212 **Display Name:** ANS1212  
 Retry Count: 0 Retry Delay(Seconds): 0 Ring Timeout(seconds):  
 Authenticate Recipient  Enable OutBound  Work Phone  
 Bypass Human Detection  Enable InBound 5381212  Mobile Phone  
 Audio Conference ANS Ad-Hoc Conference  Home Phone

**Greeting Prompt:** This is an important Message from Avaya    
**Message Body:** This is a notification for joining the conference.

Bypass Answer Machine Detection?  Leave a message to voicemail?  Use same message body for voicemail?  
 Voicemail Body: The building is closed today due to emergency rep

**Notification Scenarios – Add New Message (Audio Conference)**

- Select the **Choice** tab and click **Add a question**

**Add New Message**

**Messages** **Choice**

▼ Add Questions

Question ID	Question
There is no data to display	

Rows Per Page 5     0 - 0 (0)

**Notification Scenarios – Choice (Audio Conference)**

- On the pop-up screen **Add Question** shown below, enter any informative string in **Question 1 Content** field and click **Save**

**Notification Scenarios – Add Question (Audio Conference)**

- On the next screen where the question is added, highlight the question and following screen appears. Click **Add a choice**

**Notification Scenarios – Add a choice (Audio Conference)**

On the pop-up screen **Add Question** shown below, configure as follows:

- Choice 1 Content** - Enter any informative text
- Acknowledgment after chose** – Enter any informative text
- Check the **Mark this choice as the “Affirmative” answer for reporting purposes** box
- Audio Conference** – Select this option
- Click **Save**

**Notification Scenarios – Choice to join the conference (Audio Conference)**

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

**Add Question**

Choice 2 Content:

Acknowledgment after chosen:

Mark this choice as the "Affirmative" answer for reporting purposes

Audio Conference

No Action

**Notification Scenarios – Refusal to join the conference (Audio Conference)**

- The screen below shows the choices configured in this step. Click **Save**

**Add New Message**

**Messages** **Choice**

▼ Add Questions

Question ID	Question
Question 1	Would you like the join the conference call?

Rows Per Page: 5 | 1 - 1(1)

Add Choices

Choice ID	Choice
Choice 1	Press 1 for joining the conference
Choice 2	Press 2 for No

Rows Per Page: 5 | 1 - 2(2)

**Notification Scenarios – Choices (Final)**

- Select the **Users** tab and highlight the subscriber/s to deliver the notification and click **Add**.

**Notification Scenarios**

You can manage (add, edit & delete) notification template here

Details Message **Users** Groups Escalations Trigger Permissions

Search Value:  Search Clear

First Name	Last Name	User Id	Middle Name		First Name	Last Name	User Id	Middle Name	Conference
Anonymous	Ans	AUSER	AnsAdmin	Add	There is no data to display				
Admin	Ans	admin	AnsAdmin	Remove					
1760	PSTN	PSTN1760							
1212	PSTN	PSTN1212							

Rows Per Page 10 1 - 4(4) Rows Per Page 10 0 - 0 (0)

Save Cancel

### Notification Scenarios – Add Users

- On the subsequent screen after the subscribers are added to receive notification, click **Save**

**Notification Scenarios**

You can manage (add, edit & delete) notification template here

Details Message **Users** Groups Escalations Trigger Permissions

Search Value:  Search Clear

First Name	Last Name	User Id	Middle Name		First Name	Last Name	User Id	Middle Name	Conference
Anonymous	Ans	AUSER	AnsAdmin	Add	1760	PSTN	PSTN1760		Participant
Admin	Ans	admin	AnsAdmin	Remove	1212	PSTN	PSTN1212		Participant

Rows Per Page 10 1 - 2(2) Rows Per Page 10 1 - 2(2)

Save Cancel

### Notification Scenarios – Users Added

- The following screen shows all the notifications configured for this reference configuration

**Notification Scenarios**

You can manage (add, edit & delete) notification template here

Please search based on name, description

Scenario Name/Description:  Search Clear

Scenario Name	Description	Owner
Conference	Notification to invite to join conference	admin
VoiceMailDetection	Notification to test voice mail detection	admin
OutboundMessage	Notification for subscribers on ANS	admin

### Notification Scenarios configured

## 5.13. 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 **Notification and Trigger**→**Inbound Call Trigger** and click **Add**.



**Inbound Call Triggers**

On the pop-up screen **Add Trigger** shown below, configure as follows:

- **Inbound Call Trigger Name** – Enter any informative string
- **Inbound Call Trigger Description** – Optional
- **Greeting Prompt** – Enter any informative string
- Scroll down and click **Add** (not shown) at the bottom of **Inbound Numbers** section

The screenshot shows the 'Add Trigger' pop-up window. It has two tabs: 'General' and 'Choice'. The 'General' tab is active. The form contains the following fields and controls:

- Inbound Call Trigger Name:** Text input field containing 'InboundCallTrigger'.
- Inbound Call Trigger Description:** Text input field containing 'essages, invoke triggers'.
- Locale:** Dropdown menu set to 'en-US'.
- Greeting Prompt:** Text input field containing 'Welcome to Avaya ANS'. To its right are two buttons: 'Select Wave File' and 'Record Through Telephone'.
- Trigger Access Pin:** Text input field.
- InBound Numbers:** A section with a table header 'InBound Number' and the message 'There is no data to display'.

At the bottom of the form, there is a pagination control showing 'Rows Per Page 5' and '0 - 0 (0)'. At the very bottom of the window are 'Save' and 'Cancel' buttons.

**Inbound Call Triggers – Add Trigger**

- On the pop-up screen **Add Inbound Number Data** shown below, select one of the numbers configured in **Section 5.9** and click **Save**

**Inbound Call Triggers – Add Inbound Number Data**

- Select the **Choice** tab and click **Add**

**Inbound Call Triggers – Choice**

- On the pop-up screen **Add Choice Data**, check the **Single Scenario** box and click **Select**

**Add Choice Data**

Choice: 1 for sending notification    Select Wave File    Record Through Telephone

Enable Trigger Pin     Enable Message Recording     Enable Conferencing     Enable User Account Authentication

Single Scenario     Multiple Scenario

Single InBox Store     Multiple InBox Store

Single InBox Retrieve     Multiple InBox Retrieve

Attach Single Scenario Scenario Name

Select

Save    Cancel

**Inbound Call Triggers – Add Choice Data**

- On the pop-up screen **Add Scenario**, select one of the notifications created in **Section 5.12**

**Add Scenario**

Select Scenario OutboundMessage    Select

Cancel

**Inbound Call Triggers – Add Scenario**

- Following screen shows all the choices configured for the Inbound Trigger in this reference configuration. Click **Save**

The screenshot shows a web-based configuration window titled "Add Trigger". It has two tabs: "General" and "Choice", with "Choice" selected. The main area contains a table with the following data:

Choice Sequence	Choice Description
1	Press 1 for sending notification
2	Press 2 for sending conference notification
3	Press 3 for recording notification message
4	Press 4 for retrieving notification message

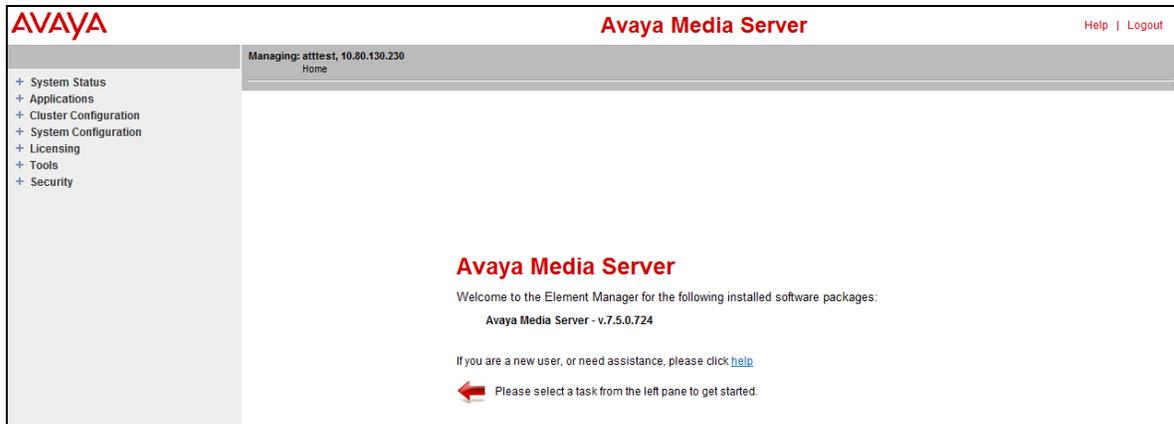
Below the table, there is a "Rows Per Page" dropdown set to 5, navigation buttons (back, first, last, forward), and a page indicator "1 - 4(4)". An "Add" button is located below the table. At the bottom right of the window are "Save" and "Cancel" buttons.

**Inbound Call Triggers – Add Trigger (Final)**

## 5.14. Avaya Media Server

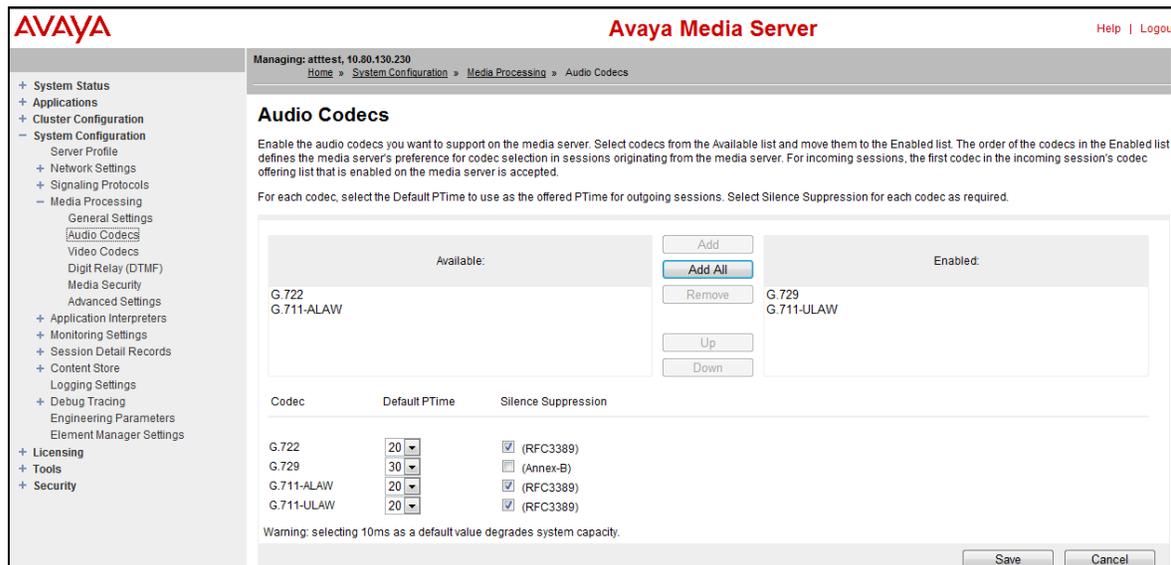
The installation of Avaya Media Server is beyond the scope of this document. For installation and basic system administration steps refer to [1, 2]. This section covers configuration related to IP Codec Set, Ptime, Dynamic Payload and RTP Port Range.

- Launch a web browser, enter **https://<IP address of the ANS server>:9443/** as the URL, and log in with the appropriate credentials to display Avaya Media Server (AMS) home page as shown below.



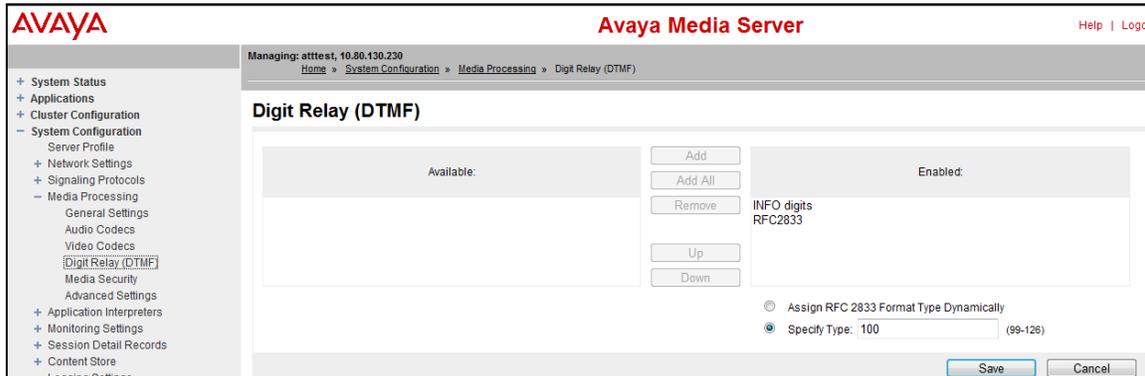
AMS Home Page

- Navigate to **System Configuration** → **Media Processing** → **Audio Codecs** and verify G729 codec is Enabled and on top of the list and the **Silence Suppression** box is unchecked for G729. See **Section 2.2, item 2** for further details.



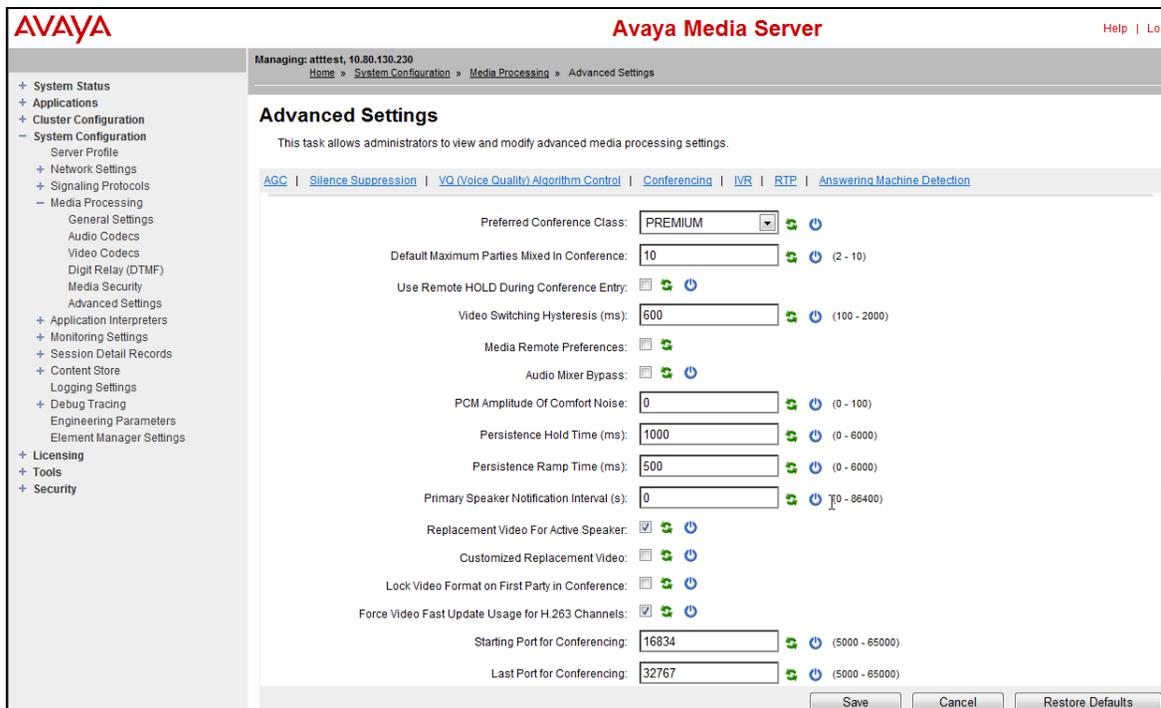
AMS Audio Codecs

- Navigate to **System Configuration**→**Media Processing**→**Digital Relay (DTMF)** and set Specify Type field to **100** and click **Save**



### AMS DTMF

- Navigate to **System Configuration**→**Media Processing**→**Advanced Settings** and set **Starting Port for Conferencing** field to **16834** and **Last Port for Conferencing** field to **32767** as required by AT&T IP Flexible Reach service and click **Save**



### AMS Advanced Setting for RTP ports

## 6. Configure Acme Packet Session Border Controller

These Application Notes assume that basic Acme Packet SBC administration has already been performed. The Acme Packet 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. Use **putty** or similar tool to access Acme Packet SBC for configuration. 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

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

<b>from-address</b>	*
<b>to-address</b>	*
<b>source-realm</b>	<b>ATT</b>

```

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
dnsgalg-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 slp0
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	
<b>in-manipulationid</b>	<b>modifyMaxptime</b>
<b>out-manipulationid</b>	<b>NAT_IP</b>
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**

<b>identifier</b>	<b>Enterprise</b>
description	
addr-prefix	0.0.0.0
<b>network-interfaces</b>	<b>s0p0:0</b>
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                UDP+TCP
  transport-method       Enterprise
  realm-id                Enterprise
  egress-realm-id        Enterprise
  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	
<b>ping-method</b>	<b>OPTIONS ;hops=70</b>
<b>ping-interval</b>	<b>180</b>
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**

<b>hostname</b>	1.1.1.1
<b>ip-address</b>	1.1.1.1
<b>port</b>	5060
<b>state</b>	disabled(Only enabled for failover testing)
<b>app-protocol</b>	SIP
<b>app-type</b>	
<b>transport-method</b>	UDP
<b>realm-id</b>	ATT
<b>egress-realm-id</b>	
<b>description</b>	AT&T Failover
<b>carriers</b>	
<b>allow-next-hop-lp</b>	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	
<b>ping-method</b>	<b>OPTIONS ;hops=70</b>
<b>ping-interval</b>	<b>180</b>
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
<b>extra-method-stats</b>	<b>enabled</b>
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**

<b>name</b>	<b>modifyMaxptime</b>
<b>description</b>	<b>Modify maxptime attribute</b>
<b>header-rule</b>	
<b>name</b>	<b>ReplaceMaxptime</b>
<b>header-name</b>	<b>Content-Type</b>

<b>action</b>	<b>manipulate</b>
<b>comparison-type</b>	<b>case-sensitive</b>
<b>msg-type</b>	<b>any</b>
<b>methods</b>	<b>INVITE</b>
<b>match-value</b>	
<b>new-value</b>	
<b>element-rule</b>	
<b>name</b>	<b>modmline</b>
<b>parameter-name</b>	<b>application/sdp</b>
<b>type</b>	<b>mime</b>
<b>action</b>	<b>find-replace-all</b>
<b>match-val-type</b>	<b>any</b>
<b>comparison-type</b>	<b>case-sensitive</b>
<b>match-value</b>	<b>maxptime</b>
<b>new-value</b>	<b>ptime</b>
last-modified-by	admin@console
last-modified-date	2011-10-22 19:25:08

**ANNOTATION:** The steering pools listed below define the RTP port range on the respective realms.

<b>steering-pool</b>	
<b>ip-address</b>	<b>192.168.62.51</b>
<b>start-port</b>	<b>16384</b>
<b>end-port</b>	<b>32767</b>
<b>realm-id</b>	<b>ATT</b>
network-interface	
last-modified-by	admin@console
last-modified-date	2011-08-25 19:11:47

<b>steering-pool</b>	
<b>ip-address</b>	<b>10.80.130.250</b>
<b>start-port</b>	<b>16384</b>
<b>end-port</b>	<b>32767</b>
<b>realm-id</b>	<b>Enterprise</b>
network-interface	
last-modified-by	admin@console
last-modified-date	2011-08-12 10:25:12

system-config	
<b>hostname</b>	<b>Enterprise-Acme</b>
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        192.168.62.1
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 ANS Web Portal.

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.

Channel	Present Status	IP Address
IP Phone	Active	10.80.130.230
Voice	Active	10.80.130.230
Email	Active	10.80.130.230

**Channel Status**

2. Navigate to **System Maintenance**→**Resource Manger Status** and make sure **Operational Status** of all the resource is **UP**.

Resource Name	IP Address	Priority	Capacity	Allocated Port	Failed Ports	Operational Status
ANS Media Server Ports		1	100	0	0	UP
ToSBC	10.80.130.250	1	100	0	0	UP
default		1	1000000	0	0	UP
attttest-VCD	10.80.130.230	1	600	0	0	UP
ANS Voice Notification Channel Ports		1	100	0	0	UP
ToSBC	10.80.130.250	1	100	0	0	UP
ToSBC-Extension	10.80.130.250	1	20	0	0	UP
ToSBC-PSTN	10.80.130.250	1	20	0	0	UP
ToSBC-Extension	10.80.130.250	1	20	0	0	UP
ToSBC-PSTN	10.80.130.250	1	20	0	0	UP

**Resource Status**

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

The screenshot shows the AVAYA ANS Web Portal interface. The top navigation bar includes 'Home', 'Partition', 'About', and 'Logoff'. The main content area is titled 'Notification History' and contains a table with the following data:

Request Status	Recipient Info	Escalation Status	Message Details
Session Id	1344277051017	Request Time	2012-08-06 12:17:31.107000000
Start Time	2012-08-06 12:17:32.512000000	End Time	2012-08-06 12:18:03.125000000
Status	<b>Completed</b>	Users Pending	0
Originator	admin	Users Initiated	0
Duration(in Seconds)	30	Users Notified	0
Last Escalation Sequence	0	Users Responded	1
Users Affirmatively Responded	0	Users Errored	0
Total Users in Request	1	Notification Details Notification Process Completed	

Notification History

### 7.3. Avaya Media Server

The following commands are issued from the ANS Web Portal.

- Navigate to **System Status** → **Element Status** and verify the **Element Status** is **Normal** for proper operation of Avaya Media Server.

The screenshot shows the AVAYA Avaya Media Server interface. The main content area is titled 'Element Status' and displays the following information:

- Managing: **attest, 10.80.130.230**
- Home > System Status > Element Status
- Click the element name to display the alarm viewer for this element.
- Buttons: Start, Stop, Restart, More Actions
- Refresh every: 5 seconds
- Element Name: [attest](#)
- UUID: 5b07a0e0-dfea-11e1-b8b8-005056aff75
- Server Address: 10.80.130.230
- Operating System: Linux
- Service Status: Started
- Operational State: Unlocked
- Element Status: **Normal**
- Alarm Description: No Alarm
- Installed Software Packages: Avaya Media Server - v.7.5.0.724

AMS Status

## 8. Conclusion

As illustrated in these Application Notes, ANS and the Acme Packet 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 R2.0 Installation and Administration Guide*

[2] *ANS 2.0 Operation Guide*

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/>

---

**©2012 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](mailto:devconnect@avaya.com).