Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Notification Solution 2.0, Avaya Aura® Session Manager 6.3 and Avaya Session Border Controller for Enterprise 6.2.1, with AT&T IP Flexible Reach - Enhanced Features Service SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya Notification Solution 2.0, Avaya Aura® Session Manager 6.3, and the Avaya Session Border Controller for Enterprise 6.2.1 with the AT&T IP Flexible Reach - Enhanced Features service, using AT&T's **AVPN** or **MIS/PNT** transport connections.

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

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

TABLE OF CONTENTS

1. Introduction

These Application Notes describe the steps for configuring Avaya Notification Solution 2.0 (referred to in the remainder of this document as ANS), Avaya Aura® Session Manager 6.3 (referred to in the remainder of this document as Session Manager), and the Avaya Session Border Controller for Enterprise 6.2.1 (referred to in the remainder of this document as Avaya SBCE) with the AT&T IP Flexible Reach-Enhanced Features SIP trunking service (referred to in the remainder of this document as IPFR-EF). The AT&T IP Flexible Reach-Enhanced Features SIP trunking service utilizes AVPN or MIS/PNT transport connections.

Avaya Notification Solution 2.0 provides real-time multimedia notification and response capabilities to many devices including IP Phones, Cell phones, 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. ANS can detect voice mail system and leave a message for the subscriber in their mailbox. Subscribers can dial into ANS to retrieve missed notifications. The Avaya Notification Solution 2.0 platform includes the Avaya Media Server (AMS 7.5) application, running as a co-resident program. ANS also includes the Loquendo Text-to-Speech application, (licensed separately), for converting text to speech to create notification announcements. Alternatively, if Loquendo is not licensed, ANS can call out to a designated telephone to record notification announcements. For the reference configuration, ANS was used to send notifications to it subscribers via inbound call triggering, or triggered locally on ANS. Additionally, an ANS ad hoc conference feature was tested via inbound triggers or outbound notification for conferences. Notification via voicemail, and voicemail retrieval functionalities were also tested.

Avaya Aura® Session Manager 6.3 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® System Manager 6.3 is used to provision and manage Avaya Aura® Session Manager.

The Avaya Session Border Controller for Enterprise 6.2.1 is the point of connection between Avaya Aura® Session Manager and the AT&T IP Flexible Reach-Enhanced Features service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

The AT&T Flexible Reach service is one of the many SIP-based Voice over IP (VoIP) services offered to enterprises for their voice communication needs. The AT&T IP Flexible Reach-Enhanced Features service is a SIP based service which includes additional network based features to the IP Flexible Reach service.

2. General Test Approach and Test Results

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.

The interoperability compliance testing focused on verifying inbound call flows from IPFR-EF to the Customer Premises Equipment (CPE) containing the Avaya platforms (see **Section 3.2** for call flow examples).

The test environment described in these Application Notes consisted of:

- A simulated enterprise with ANS (including Avaya Media Server, running as a co-resident program), System Manager, Session Manager, and the Avaya SBCE.
- An IPFR-EF production circuit, to which the simulated enterprise was connected via AVPN transport.

2.1. Interoperability Compliance Testing

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 IPFR-EF network. Calls were made from the PSTN across the IPFR-EF network, to the CPE.

Note – Avaya Notification Solution utilizes customer provisioned Notification Scenarios to define interactive capabilities (e.g., announcements, menus, call routing, etc). The programming and testing of such scenarios are beyond the scope of this document.

The following features were tested and verified as part of this effort:

- Verification of SIP Trunking between ANS, System Manager, Session Manager, Avaya SBCE, and the IPFR-EF service.
- ANS inbound and outbound call processing via SIP trunks.
- Inbound and outbound caller interaction with ANS, including prompting, caller DTMF input, and announcements.
- ANS ad hoc conference.
- G.729A, and G.711mu codec support.

Note – Many IPFR-EF network features require DTMF interaction with the caller for these features to be activated. The ANS environment used during testing did not have outbound DTMF capability. Therefore, the following IPFR-EF service features were not accessed by ANS as part of this testing effort:

- Network based Simultaneous Ring.
- Network based Sequential Ring (Locate Me).
- Network based Call Forwarding Always (CFA/CFU).

- Network based Call Forwarding Ring No Answer (CF-RNA).
- Network based Call Forwarding Busy (CF-Busy).
- Network based Call Forwarding Not Reachable (CF-NR).

Note – Documents used to provision the test environment are listed in **Section 10**. References to these documents are indicated by the notation **[x]**, where *x* is the document reference number.

2.2. Test Results

The test objectives stated in **Section 2.1**, with limitations as noted below, were verified.

1. **Removal of unnecessary SIP headers.** In an effort to reduce packet size (or block headers containing private CPE information), the Avaya SBCE is provisioned to remove SIP headers not required by AT&T. The following headers are removed; *P-Location, Alert-Info, Endpoint-View, AV-Correlation-ID, Remote-Party-ID, AV-Global-Session-ID,* and *P-AV-Message-ID* (see **Section 7.4.3**).

2. **Use of G.729 and G.711mu codecs** – The AT&T IPFR-EF service recommends that G.729 be specified as the primary codec offering, with G.711mu as the secondary choice. However the ANS installation guide recommends that a G.711 codec be used to ensure the highest voice quality for generated announcements. The use of G.729 as the primary codec, (with G.711mu as secondary), is shown in these application notes. However G.711mu was tested successfully as the primary codec.

3. **Setting G.729 with silence suppression (AnnexB=Yes) on ANS is not recommended**. The ANS installation guide recommends that G.729 with silence suppression not be used. This is due to issues negotiating with some message answering systems, should ANS notifications cover to voicemail or answering machines. During testing it was found that with ANS using G.729B, notifications *did not* cover successfully to voicemail.

4. **AT&T restrictions on high capacity auto-dialer platforms –** Except as explicitly authorized in a written agreement between the customer and AT&T, the use of predictive dialers, auto-dialers, or other devices that generate automated outbound calls in conjunction with AT&T IP Flexible Reach is strictly prohibited. AT&T IP Flexible Reach calls may be blocked and/or AT&T IP Flexible Reach service may be terminated immediately for abuse or misuse of Service should customers use any such device.

5. **Emergency 911/E911 Services Limitations and Restrictions** – Although AT&T provides 911/E911 calling capabilities, AT&T does not warrant or represent that the equipment and software (e.g., IP PBX) documented in these Application Notes will properly operate with AT&T IP Flexible Reach to complete 911/E911 calls; therefore, it is the customer's responsibility to ensure proper operation with the equipment/software vendor.

While AT&T IP Flexible Reach services support E911/911 calling capabilities under certain Calling Plans, there are circumstances when the E911/911 service may not be available, as stated in the Service Guide for AT&T IP Flexible Reach found at http://new.serviceguide.att.com. Such circumstances include, but are not limited to, relocation of the end user's CPE, use of a non-native or virtual telephone number, failure in the broadband connection, loss of electrical power, and delays that may occur in updating the Customer's location in the automatic location information database. Please review the AT&T IP Flexible Reach Service Guide in detail to understand the limitations and restrictions**.**

2.3. Support

For more information on the AT&T IP Flexible Reach service visit: http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ip-flexible-reach-enterprise/. AT&T customers may obtain support for the AT&T IP Flexible Reach service by calling (877) 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.

3. Reference Configuration

The reference Customer Premises Equipment (CPE) configuration used in these Application Notes is shown in **Figure 1** and consists of several components:

- **Avaya Notification Solution 2.0** is a centrally located message broadcast and notification system providing real-time multimedia notification (e.g., emergency broadcast and system alarming), and response capabilities.
- **Avaya Media Server 7.5**, running as a co-resident program with ANS.
- **Session Manager 6.3** provides core SIP routing and integration services that enables communication between disparate SIP-enabled entities, (e.g., PBXs, SIP proxies, gateways, adjuncts, trunks, applications, etc.) across the enterprise.
- **System Manager 6.3** provides a common administration interface for centralized management of Session Manager.
- **Avaya SBCE 6.2.1** provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation between the IPFR-EF service and the enterprise internal network.
- UDP and TCP transport protocols are used in the reference configuration. The IPFR-EF service specifies SIP over UDP to communicate with enterprise edge SIP devices, (e.g., the Avaya SBCE). In the reference configuration, SIP over TCP was used to communicate between ANS, Session Manager, and the Avaya SBCE. ANS does not support TLS, and TCP was used between the other platforms to facilitate protocol trace analysis.
- Inbound and outbound calls were placed via an IPFR-EF production AVPN circuit.

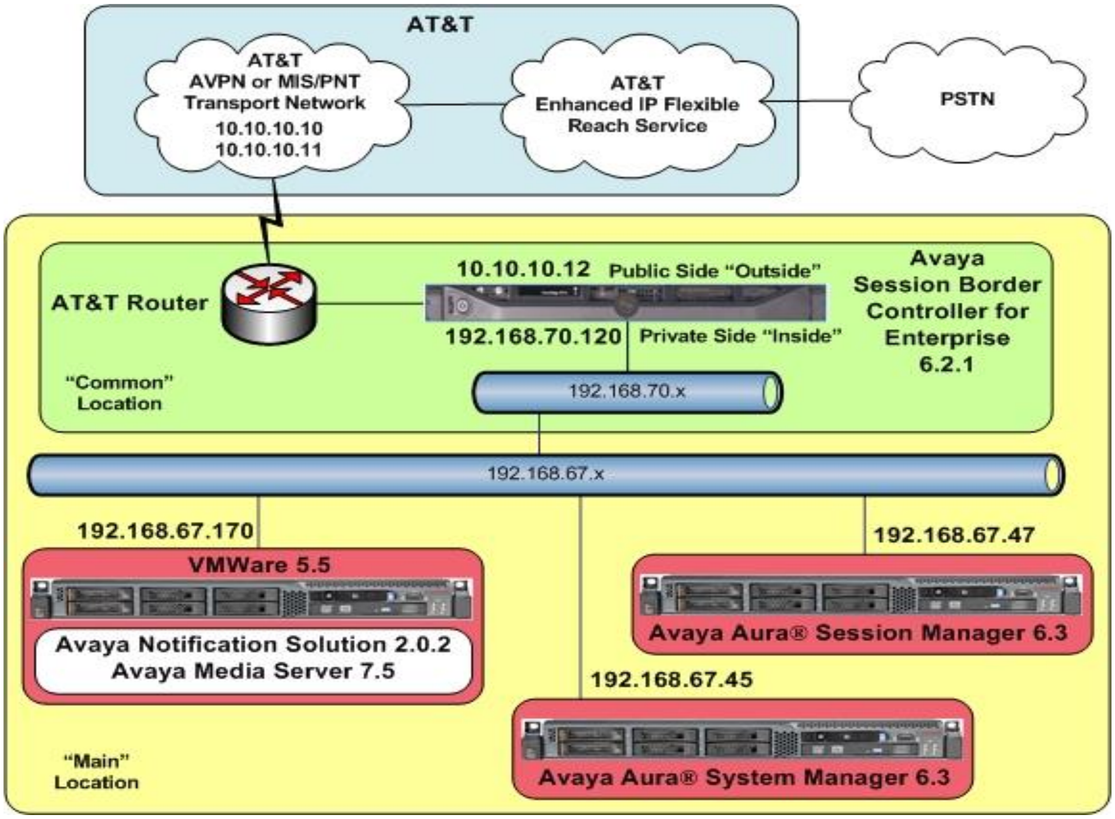


Figure 1: Reference configuration

3.1. Illustrative Configuration Information

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

Component	Illustrative Value in these Application Notes
Main Site	
Avaya Aura® System Manager	
IP Address	192.168.70.45
Avaya Aura® Session Manager	
Management IP Address	192.168.67.46
Network IP Address	192.168.67.47
Avaya Notification Solution/Avaya Media Server	
Network IP Address	192.168.67.170
Common Site	
Avaya Session Border Controller for Enterprise (SBCE)	
IP Address of Outside (Public) Interface	10.10.10.12 (see note below)
IP Address of Inside (Private) Interface	192.168.70.120

Table 1: Illustrative Values Used in these Application Notes

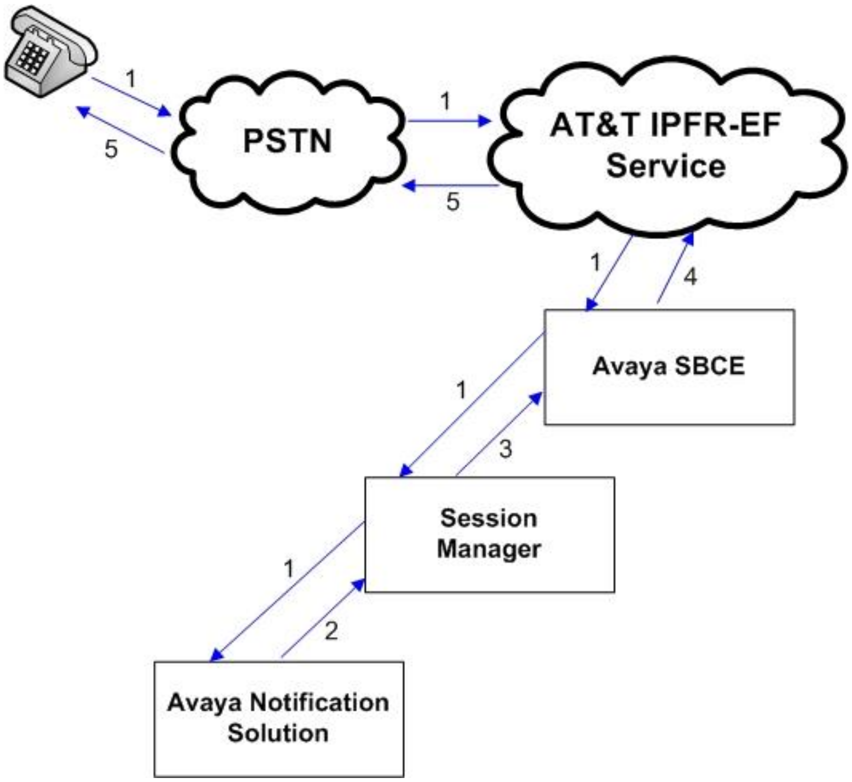
NOTE – The Avaya SBCE Outside interface communicates with AT&T Border Elements (BEs) located in the AT&T IPFR-EF network. For security reasons, the IP addresses of the AT&T BEs are not included in this document. However as placeholders in the following configuration sections, the IP addresses **10.10.10.12** (Avaya SBCE public interface), **10.10.10.10,** and **10.10.10.11** (AT&T BE IP addresses), are specified. In addition, AT&T DID/DNIS numbers shown in this document are examples as well. AT&T Customer Care will provide the actual Border Element IP addresses and DID/DNIS numbers as part of the IPFR-EF provisioning process.

3.2. Call Flows

To understand how IPFR-EF service calls are processed in an Avaya Notification Solution environment, several basic call flows are described in this section.

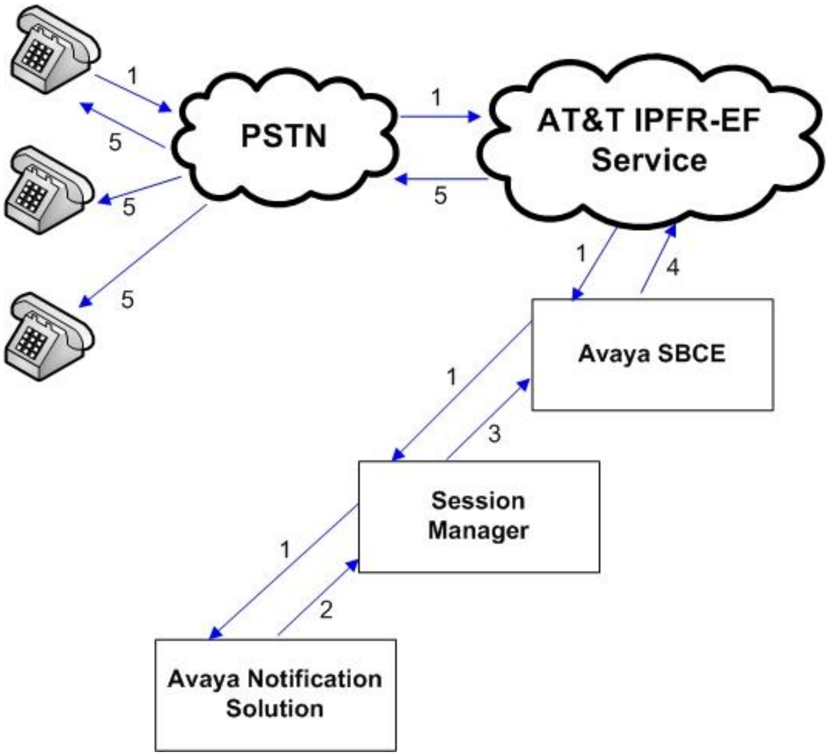
The first call scenario illustrated below is an outbound call originating from ANS to the subscriber(s) on PSTN.

1. The ANS notification may be triggered by an inbound call to ANS, or:
2. A notification is triggered locally from ANS. In either case, ANS sends the call to Session Manager.
3. Session Manager sends the call to the Avaya SBCE.
4. The Avaya SBCE performs any necessary SIP header modifications, and routes the call to the AT&T IP Flexible Reach Service.
5. The AT&T IP Flexible Reach service routes the call to the PSTN subscriber(s) defined in the ANS notification. If a subscriber does not pick up the phone and a voicemail is detected, ANS leaves the notification message on the subscriber’s voicemail.



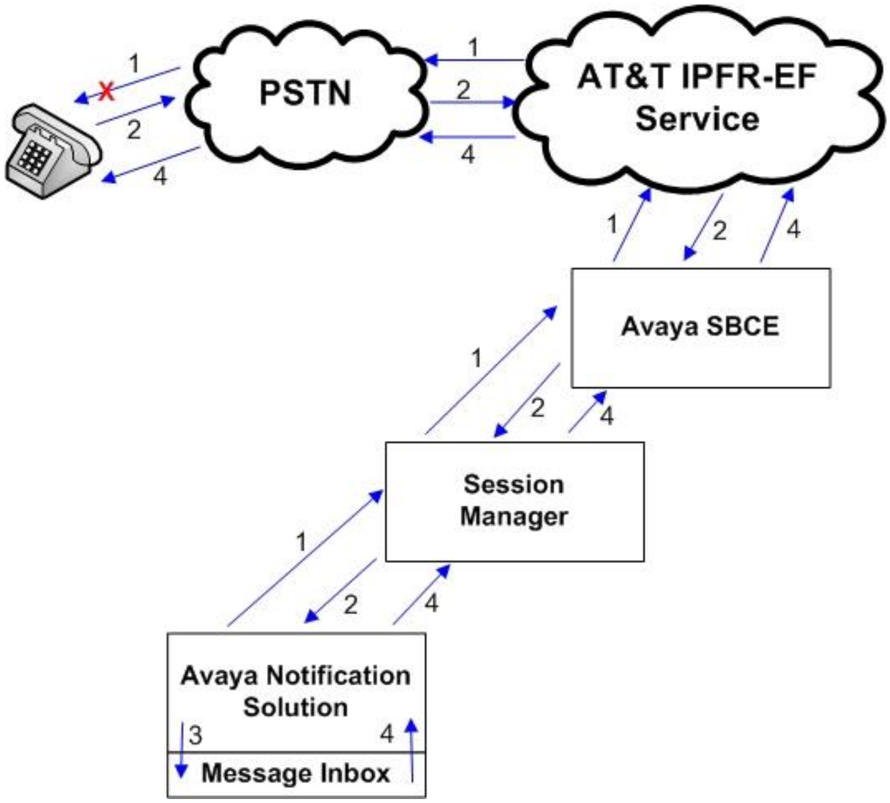
The second call scenario illustrated below is an ANS Ad Hoc conference. In this scenario ANS calls the subscribers, and via DTMF menus (e.g., conference access code, accept/decline invitation, etc.), subscribers join the conference.

1. The ANS Ad Hoc conference may be triggered by an inbound call to ANS from the conference host, or:
2. Calls to designated conference subscribers are initiated by ANS. In either case, ANS sends the calls to Session Manager.
3. Session Manager sends the calls to the Avaya SBCE.
4. The Avaya SBCE performs any necessary SIP header modifications, and routes the calls to the AT&T IP Flexible Reach Service.
5. The AT&T IP Flexible Reach service routes the calls to the PSTN subscriber(s) defined in the ANS notification. If a subscriber does not pick up the phone and a voicemail is detected, ANS leaves the notification message on the subscriber’s voicemail.



The third scenario describes a missed notification. Message inboxes may be defined on ANS. In the previous call scenarios, ANS may be provisioned to copy the notification announcement to a message inbox. If a subscriber misses the notification, they may call into that ANS message inbox and hear the notification. Access to the message inbox can be protected via an access code.

1. The ANS delivers a notification to a subscriber, but they miss the call.
2. The subscriber calls the designated ANS message inbox access number.
3. ANS connects the caller to the designated message inbox.
4. The missed notification is played back to the subscriber.



4. Equipment and Software Validated

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

Equipment/Software	Release/Version
HP Proliant DL360 G7 server • System Platform • Avaya Aura® System Manager	 • 6.3.0.0.18002 (with patch 08007) • 6.3.9 (r4602482)
IBM 8800 server • Avaya Aura® Session Manager	 • 6.3 SP9(6.3.9.0.639011)
Dell S8510 server • System Platform • Avaya Aura® Communication Manager	 • 6.3.0.0.18002 • 6.3 SP7 (03.0.124.0-21754)
HP Proliant DL120 G7 server • VMWare ESXi • Avaya Notification Solution ○ Avaya Media Server	 • 5.1.0 • 2.0.2.3807 • 7.5.0.1272
Dell R210 • Avaya Session Border Controller for Enterprise	 • 6.2.1 Q18

Table 2: Equipment and Software Versions

5. Configure Avaya Aura® Session Manager Release 6.3

This section illustrates relevant aspects of the Session Manager configuration used in the verification of these Application Notes.

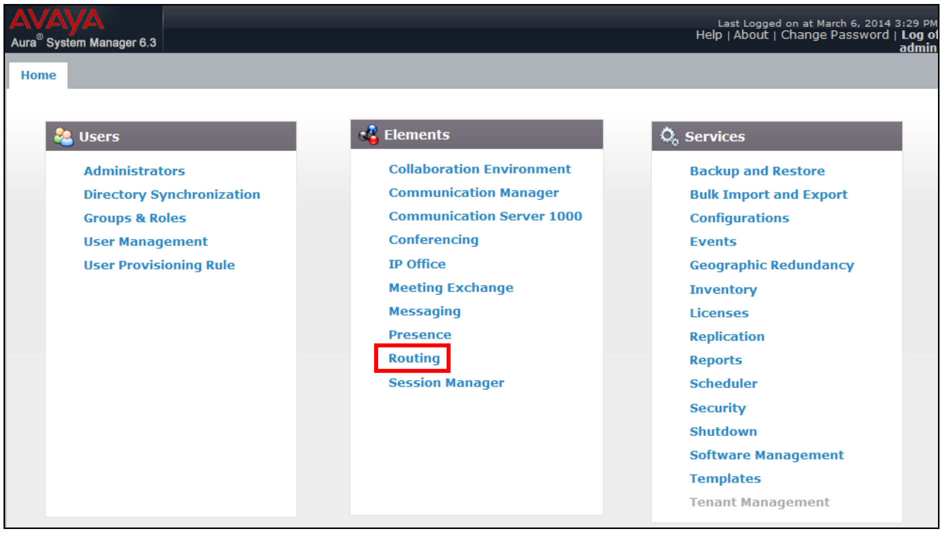
Note – These Application Notes assume that basic System Manager and Session Manager administration has already been performed. Consult documents **[3 & 4]** for further details if necessary.

This section provides the procedures for configuring Session Manager to receive calls from the AT&T IPFR-EF service (via the Avaya SBCE) and route these calls over the SIP trunks defined to ANS and the Avaya SBCE.

The following administration activities will be described:

- Define SIP Domain.
- Define Locations.
- Define SIP Entities corresponding to ANS and the Avaya SBCE.
- Define Entity Links between Session Manager and the SIP Entities.
- Define Routing Policies associated with ANS and the Avaya SBCE.
- Define Dial Patterns, which govern which routing policy will be selected for call routing.

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. In the **Log On** screen (not shown), enter appropriate **User ID** and **Password** and press the **Log On** button. Once logged in, **Home** screen is displayed. From the **Home** screen, under the **Elements** heading in the center, select **Routing**.



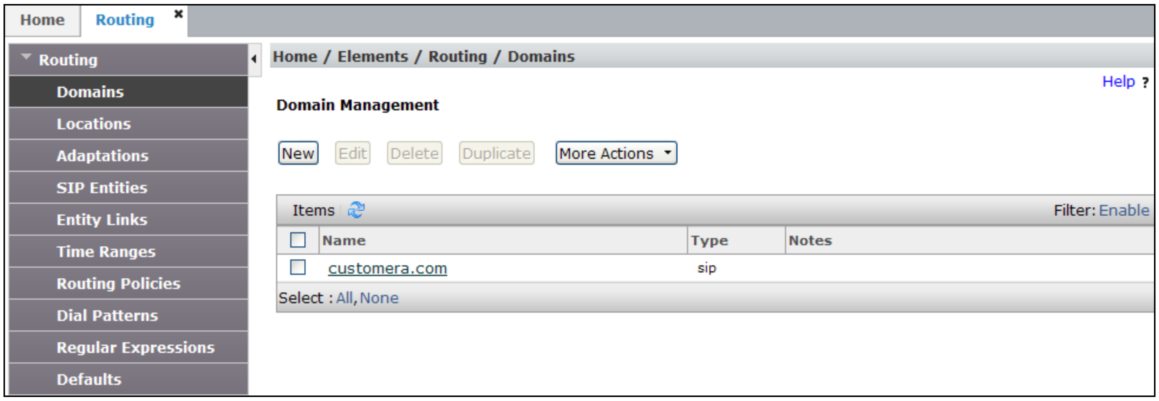
5.1. SIP Domain

Step 1 - Select **Domains** from the left navigation menu. In the reference configuration, domain **customera.com** was defined.

Step 2 - Click **New** (not shown)**.** Enter the following values and use default values for remaining fields**.**

- **Name:** Enter the enterprise SIP Domain Name. In the reference configuration, **customera.com** is used.
- **Type:** Verify **sip** is selected.
- **Notes:** Add a brief description.

Step 3 - Click **Commit** to save.



□	Name	Type	Notes
□	customera.com	sip	

5.2. Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. Location identifiers can be defined in a broad scope (e.g., 192.168.67.x for all devices on a particular subnet), or individual devices (e.g., 192.168.67.46 for a device's specific IP address). In the reference configuration, two Locations are specified:

- **Main** (**192.168.67.***) – The Location defining the majority of the CPE equipment (e.g., System Manager, Session Manager, and ANS).
- **Common** (**192.168.70.***) – The Location defining the Avaya SBCE.

Note – Two Locations are specified due to the specific network topology of the test reference configuration. A single Location, or more than two Locations, may be used as applicable.

5.2.1. Main Location

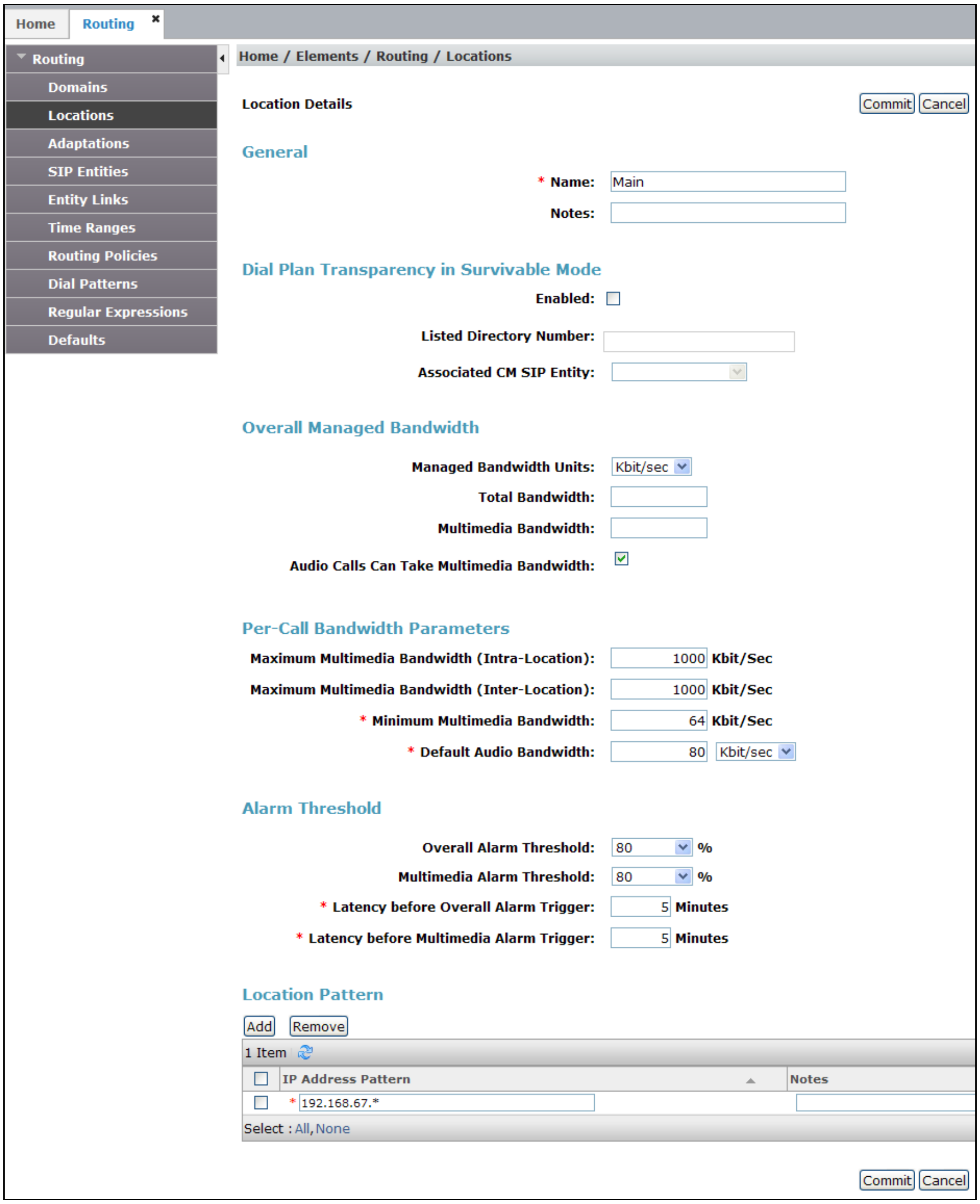
Step 1 - Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name for the Location (e.g., **Main**).
- **Notes:** Add a brief description.

Step 2 - In the **Location Pattern** section, click **Add** and enter the following values.

- **IP Address Pattern:** Enter the IP address of the CPE subnet (e.g., **192.168.67.***).
- **Notes:** Add a brief description if desired.

Step 3 - Click **Commit** to save.



Home / Elements / Routing / Locations

Location Details

General

* Name:	Main
Notes:	

Dial Plan Transparency in Survivable Mode

Enabled:	□
Listed Directory Number:	
Associated CM SIP Entity:	

Overall Managed Bandwidth

Managed Bandwidth Units:	Kbit/sec
Total Bandwidth:	
Multimedia Bandwidth:	
Audio Calls Can Take Multimedia Bandwidth:	☑

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):	1000 Kbit/Sec
Maximum Multimedia Bandwidth (Inter-Location):	1000 Kbit/Sec
* Minimum Multimedia Bandwidth:	64 Kbit/Sec
* Default Audio Bandwidth:	80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold:	80 %
Multimedia Alarm Threshold:	80 %
* Latency before Overall Alarm Trigger:	5 Minutes
* Latency before Multimedia Alarm Trigger:	5 Minutes

Location Pattern

1 Item

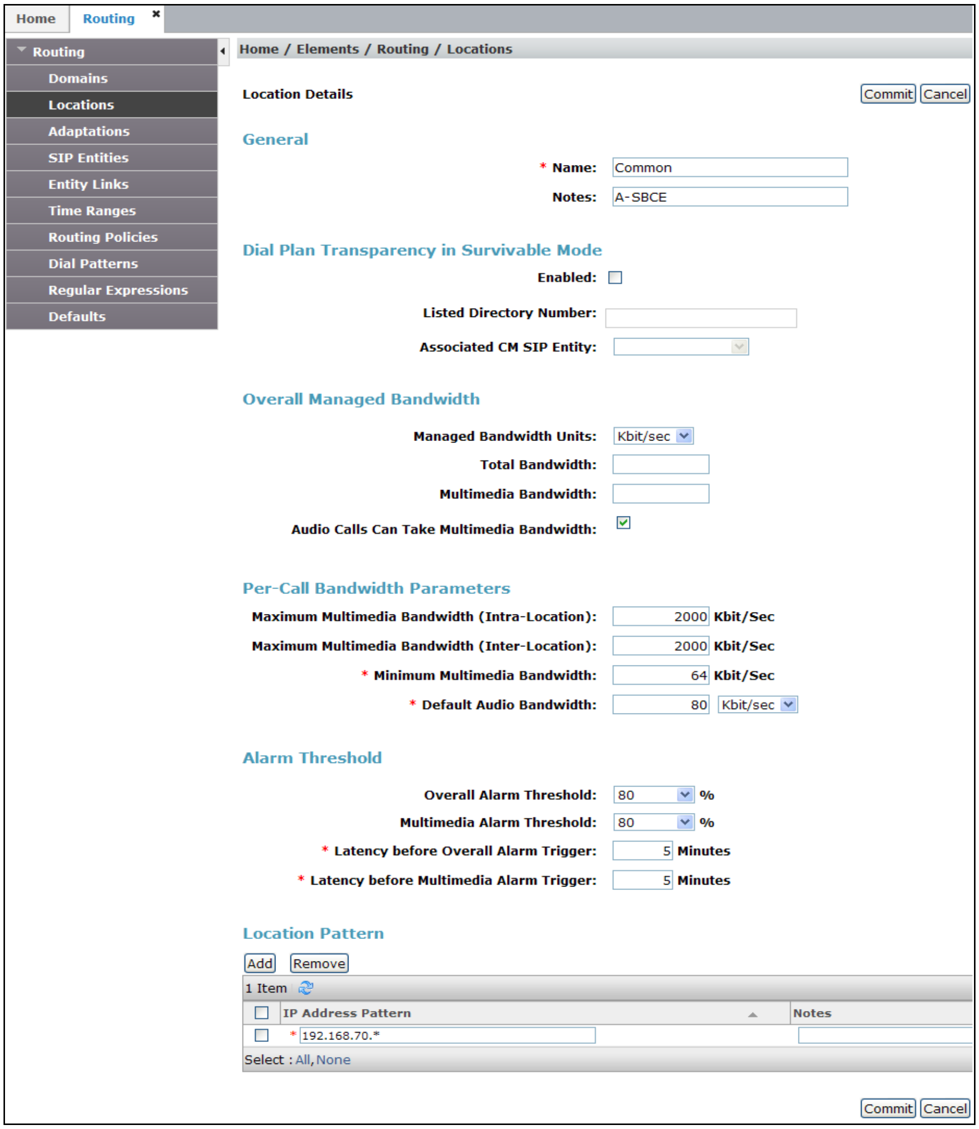
□	IP Address Pattern	Notes
□	* 192.168.67.*	

Select : All, None

5.2.2. Common Location

Repeat the steps from **Section 5.2.1** with the following changes:

- **Name:** Enter a descriptive name for the Location (e.g., **Common**).
- **IP Address Pattern:** Enter the IP address of the Branch subnet (e.g., **192.168.70.***).



Home / Elements / Routing / Locations

Location Details

General

* Name: Common

Notes: A-SBCE

Dial Plan Transparency in Survivable Mode

Enabled: □

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☑

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 2000 Kbit/Sec

* Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

* Latency before Overall Alarm Trigger: 5 Minutes

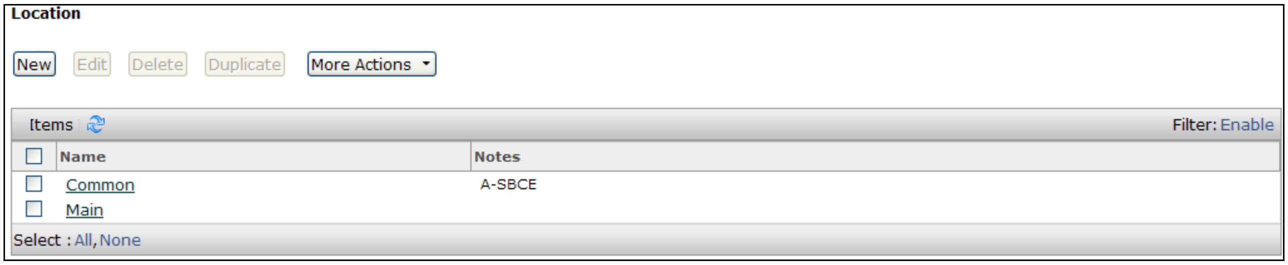
* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

1 Item

□	IP Address Pattern	Notes
□	* 192.168.70.*	

Select : All, None



Location

Items

□	Name	Notes
□	Common	A-SBCE
□	Main	

Select : All, None

5.3. Configure Adaptations

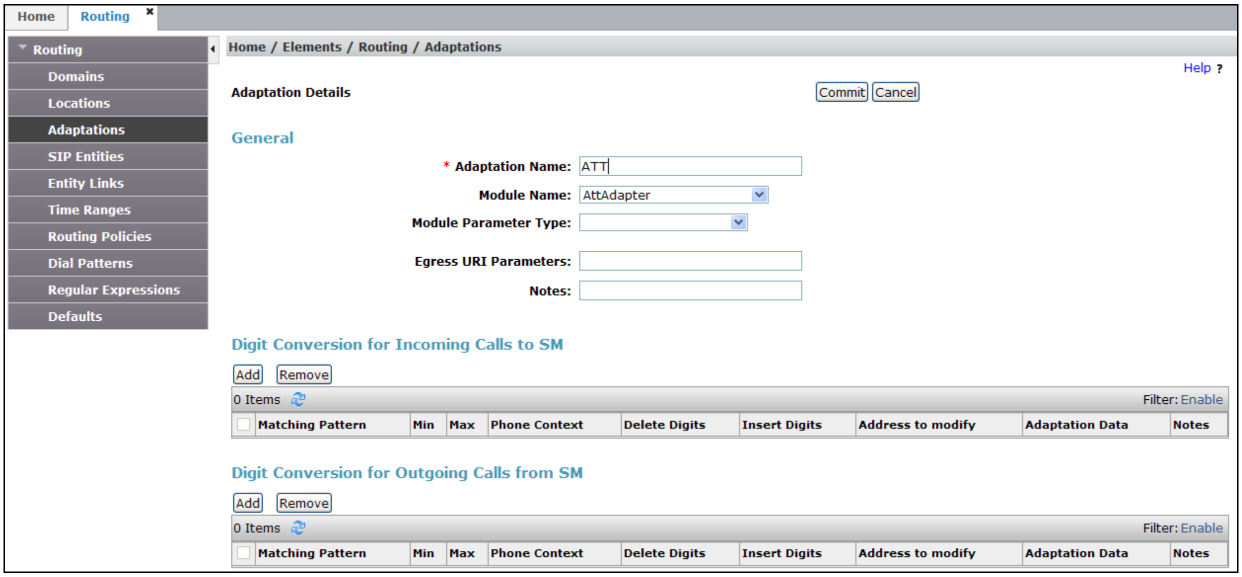
Session Manager can be configured to use Adaptation Modules to convert SIP headers sent to/from the AT&T IPFR-EF service. In the reference configuration the “AttAdapter” is used. This adaptation removes History-Info headers which are not supported by the IPFR-EF service.

Step 1 - Click on **Adaptations**. In the **Adaptations** page, click on **New** (not shown).
Step 2 - In the **Adaptation Details** page, enter:

1. A descriptive **Name**, (e.g., **ATT**).
2. Select **AttAdapter** from the **Module Name** drop down menu (if this module name is not present, select **<click to add module>** and enter **AttAdapter**).

Step 3 - Click on **Commit**.

Note – As shown in the screen below, no Incoming or Outgoing Digit Conversion was required in the reference configuration.



Adaptation Details

General

* Adaptation Name: ATT
Module Name: AttAdapter
Module Parameter Type:
Egress URI Parameters:
Notes:

Digit Conversion for Incoming Calls to SM

0 Items

□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes

Digit Conversion for Outgoing Calls from SM

0 Items

□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes

5.4. SIP Entities

In this section, SIP Entities are administered for the following SIP network elements:

- ANS (**Section 5.4.1**). This entity, and its associated Entity Link (using TCP with port 5060), is for calls to/from AT&T via the Avaya SBCE.
- Avaya SBCE (**Section 5.4.2**) - This entity, and it’s associated Entity Link (using TCP and port 5060), is for calls from AT&T (note that the connection between the Avaya SBCE and AT&T uses UDP/5060).
- Session Manager (**Section 5.4.3**). This section is normally populated during installation, but is shown here for completeness.

5.4.1. Avaya Notification Solution SIP Entity

Step 1- In the left pane under **Routing**, click on **SIP Entities**. In the **SIP Entities** page click on **New** (not shown).

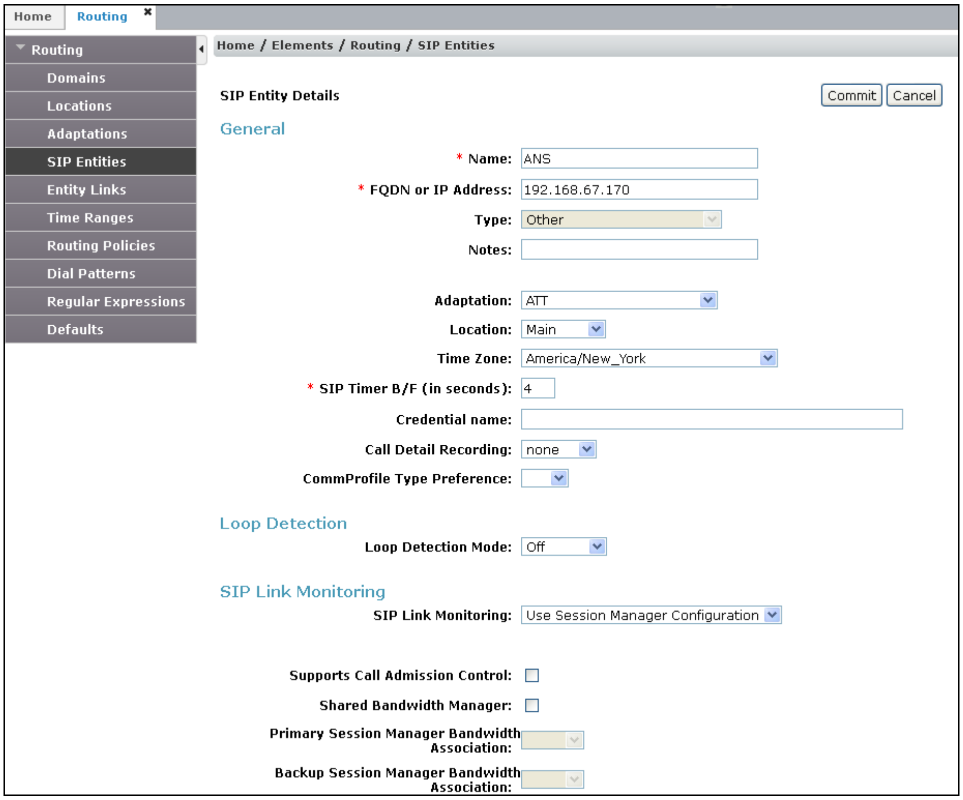
Step 2 - In the **General** section of the **SIP Entity Details** page, provision the following:

- **Name –** Enter a descriptive name (e.g. **ANS**).
- **FQDN or IP Address –** Enter the IP address of the ANS application (e.g. **192.168.67.170**).
- **Type –** Select **Other.**
- **Location** – Select location **Main** (**Section 5.2.1**).
- **Time Zone** – Select the time zone in which Session Manager resides.
- Note that this Entity has no Adaptation defined.

Step 3 - In the **SIP Link Monitoring** section of the **SIP Entity Details** page configure as follows:

- Select **Use Session Manager Configuration** for **SIP Link Monitoring** field.
- Use the default values for the remaining parameters.

Note – The **Entity Links** section of this form (not shown) will be automatically populated when the Entity Links are defined in **Section 5.5**. The **SIP Responses to an OPTIONS Request** section of the form is not used in the reference configuration.



SIP Entity Details

General

* Name: ANS

* FQDN or IP Address: 192.168.67.170

Type: Other

Notes:

Adaptation: ATT

Location: Main

Time Zone: America/New_York

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

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Supports Call Admission Control: □

Shared Bandwidth Manager: □

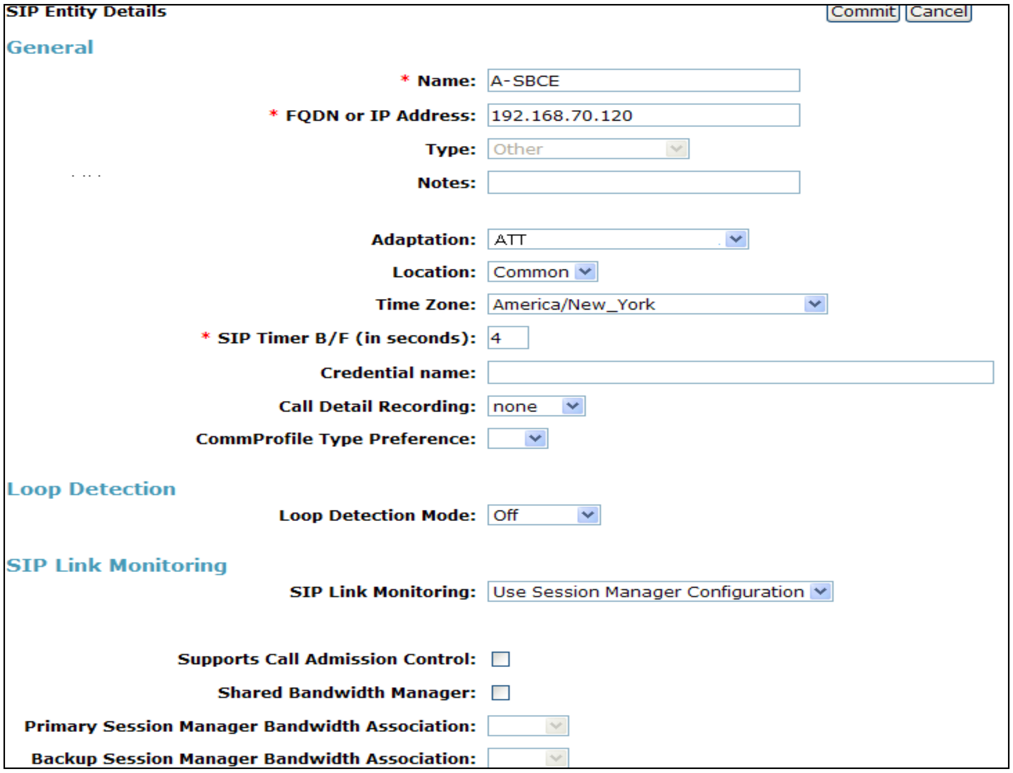
Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

5.4.2. Avaya Session Border Controller for Enterprise SIP Entity

To configure the Avaya SBCE SIP Entity, repeat the steps in **Section 5.4.1** with the following changes:

- **Name –** Enter a descriptive name (e.g., **A-SBCE**).
- **FQDN or IP Address –** Enter the IP address of the A1 (private) interface of the Avaya SBCE (e.g., **192.168.70.120**, see **Section 7.5.1**).
- **Type –** Verify **Other** is selected.
- **Adaptations –** Select Adaptation **ATT** (**Section 5.3**).
- **Location** – Select location **Common** (**Section 5.2.2)**.



General

* Name:	A-SBCE
* FQDN or IP Address:	192.168.70.120
Type:	Other
Notes:	
Adaptation:	ATT
Location:	Common
Time Zone:	America/New_York
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none
CommProfile Type Preference:	

Loop Detection

Loop Detection Mode:	Off

SIP Link Monitoring

SIP Link Monitoring:	Use Session Manager Configuration
Supports Call Admission Control:	□
Shared Bandwidth Manager:	□
Primary Session Manager Bandwidth Association:	
Backup Session Manager Bandwidth Association:	

5.4.3. Avaya Aura® Session Manager SIP Entity

Step 1- In the left pane under **Routing**, click on **SIP Entities**. In the **SIP Entities** page click on **New** (not shown).

Step 2 - In the **General** section of the **SIP Entity Details** page, provision the following:

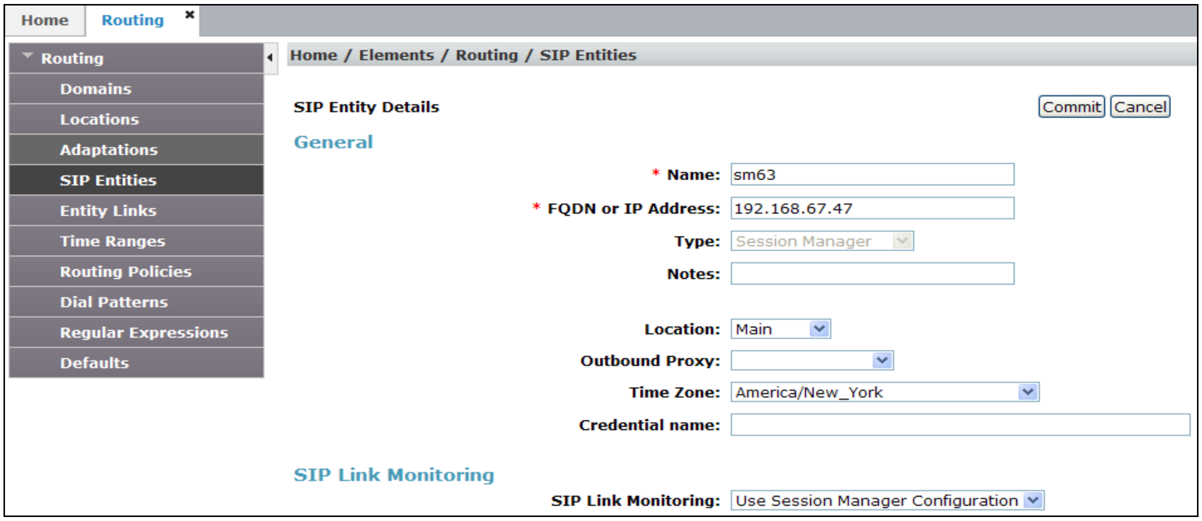
- **Name –** Enter a descriptive name (e.g., **sm63**).
- **FQDN or IP Address –** Enter the IP address of the Main Session Manager signaling interface, (*not* the management interface), provisioned during installation (e.g., **192.168.67.47**).
- **Type –** Verify **Session Manager** is selected.
- **Location** – Select location **Main** (**Section 5.2.1**).
- **Outbound Proxy** – (Optional) Leave blank or select another SIP Entity. For calls to SIP domains for which Session Manager is not authoritative, Session Manager

routes those calls to this **Outbound Proxy** or to another SIP proxy discovered through DNS if **Outbound Proxy** is not specified.

- **Time Zone** – Select the time zone in which Session Manager resides.

Step 3 - In the **SIP Monitoring** section of the **SIP Entity Details** page configure as follows:

- Select **Use Session Manager Configuration** for **SIP Link Monitoring** field.
- Use the default values for the remaining parameters.



SIP Entity Details

General

* Name: sm63

* FQDN or IP Address: 192.168.67.47

Type: Session Manager

Notes:

Location: Main

Outbound Proxy:

Time Zone: America/New_York

Credential name:

SIP Link Monitoring

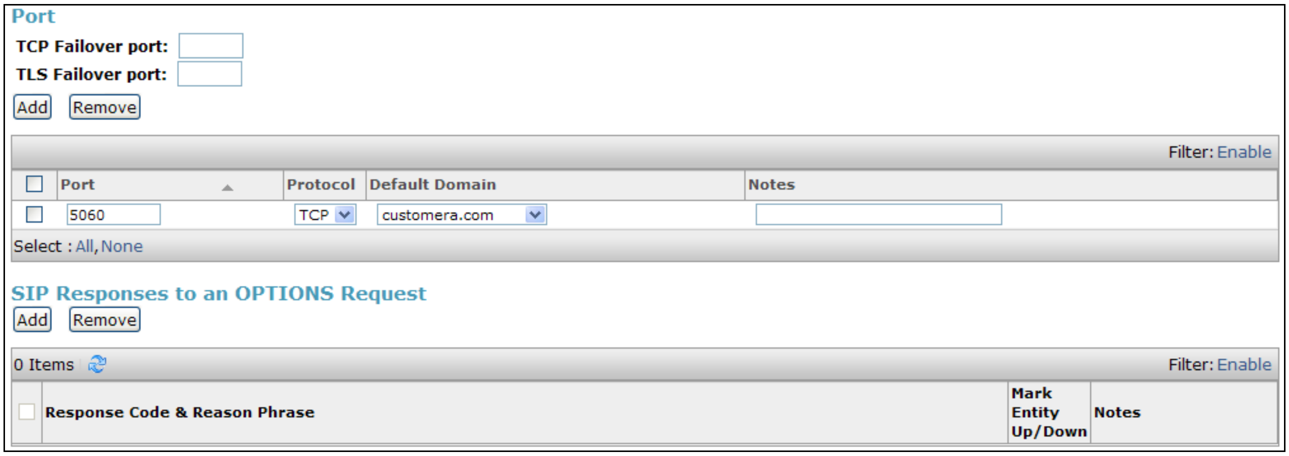
SIP Link Monitoring: Use Session Manager Configuration

Step 4 – Scrolling down to the **Port** section of the **SIP Entity Details** page (only the Session Manager Entity has the Port section), click on **Add** and provision entries as follow:

- **Port** – Enter **5060**.
- **Protocol** – Select **TCP**.
- **Default Domain –** Select a SIP domain administered in **Section 5.1** (e.g., **customera.com**).

Step 5 – Enter any notes as desired and leave all other fields on the page blank/default.

Step 6 - Click on **Commit**.



Port

TCP Failover port:

TLS Failover port:

☐	Port	Protocol	Default Domain	Notes
☐	5060	TCP	customera.com	

SIP Responses to an OPTIONS Request

☐	Response Code & Reason Phrase	Mark Entity Up/Down	Notes

5.5. Entity Links

In this section, Entity Links are administered for the following connections:

- Session Manager to ANS (**Section 5.5.1**).
- Session Manager to the Avaya SBCE (**Section 5.5.2**).

Note – Once the Entity Links have been committed, the link information will also appear on the associated SIP Entity pages configured in **Section 5.4**.

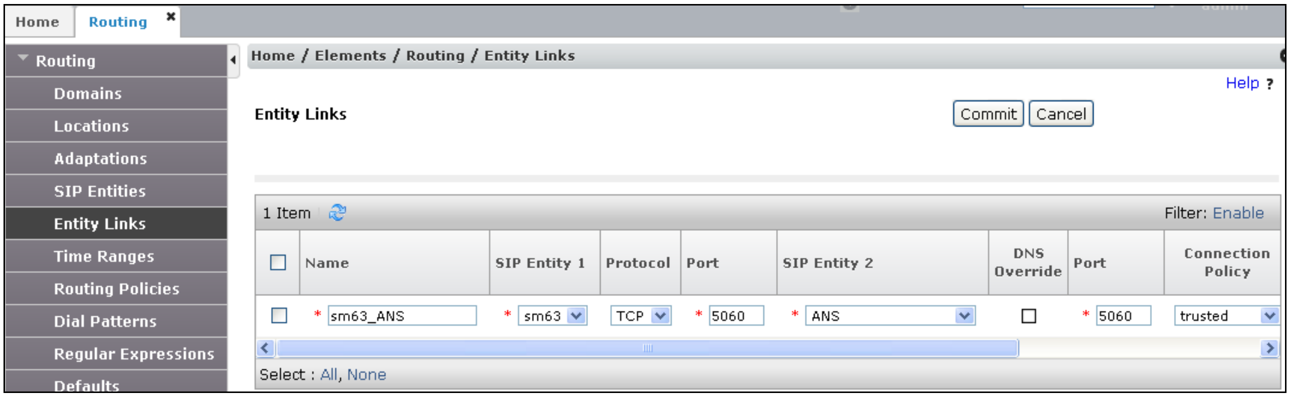
5.5.1. Avaya Aura® Session Manager Entity Link to Avaya Notification Solution

Step 1 - In the left pane under **Routing**, click on **Entity Links**, then click on **New** (not shown).

Step 2 - Continuing in the **Entity Links** page, provision the following:

- **Name** – Enter a descriptive name for this link to ANS (e.g., **sm63_ANS**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 5.4.3** for Session Manager (e.g., **sm63**).
- **SIP Entity 1 Port** – Enter **5060**.
- **Protocol** – Select **TCP**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.1** for the ANS entity (e.g., **ANS**).
- **SIP Entity 2 Port** - Enter **5060**.
- **Connection Policy** – Select **Trusted**.

Step 3 - Click on **Commit**.



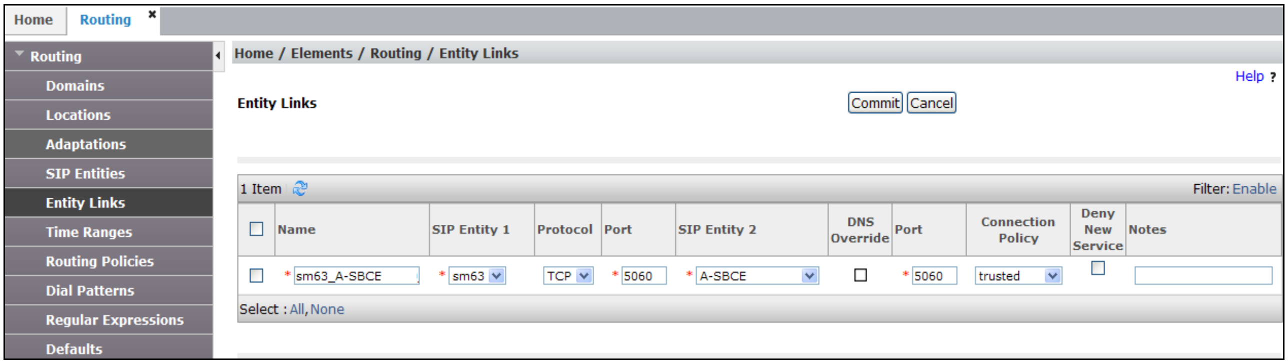
Entity Links

☐	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
☐	* sm63_ANS	* sm63	TCP	* 5060	* ANS	☐	* 5060	trusted

5.5.2. Avaya Aura® Session Manager Entity Link to the Avaya SBCE

To configure this Entity Link, repeat the steps in **Section 5.5.1**, with the following changes:

- **Name** – Enter a descriptive name for this link to the Avaya SBCE (e.g., **sm63_A-SBCE**).
- **SIP Entity 2** –Select the SIP Entity administered in **Section 5.4.2** for the Avaya SBCE (e.g., **A-SBCE**).



Entity Links

☐	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
☐	* sm63_A-SBCE	* sm63	TCP	* 5060	* A-SBCE	☐	* 5060	trusted	☐	

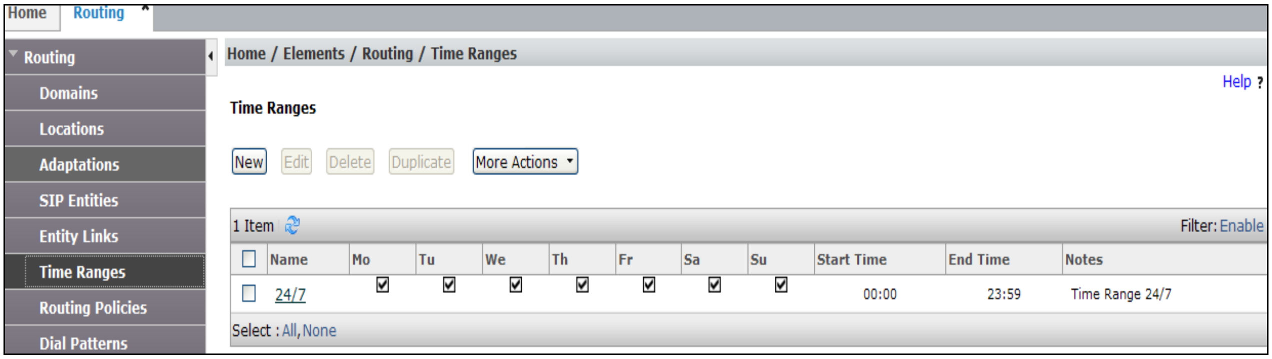
5.6. Time Ranges

Step 1 - In the left pane under **Routing**, click on **Time Ranges**. In the **Time Ranges** page click on **New** (not shown).

Step 2 - Continuing in the **Time Ranges** page, enter a descriptive **Name**, check the checkbox(s) for the desired day(s) of the week, and enter the desired **Start Time** and **End Time**.

Step 3 - Click on **Commit**.

Step 4 - Repeat **Steps 1 – 3** to provision additional time ranges.



Time Ranges

☐	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
☐	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

5.7. Routing Policies

In this section, the following Routing Policies are administered:

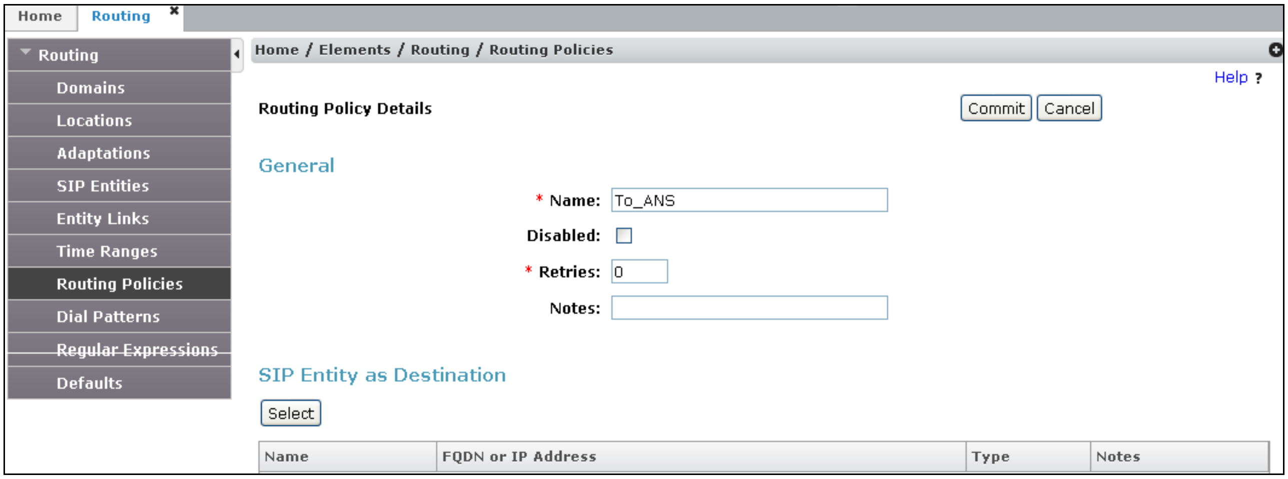
- Inbound calls to ANS from AT&T (**Section 5.7.1**).
- Outbound calls from ANS to AT&T (**Section 5.7.2**).

5.7.1. Routing Policy for AT&T Routing to Avaya Notification Solution

This Routing Policy is used for inbound calls from AT&T to ANS.

Step 1 - In the left pane under **Routing**, click on **Routing Policies**. In the **Routing Policies** page click on **New** (not shown).

Step 2 - In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing AT&T calls to ANS (e.g., **To_ANS** and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.



Routing Policy Details

General

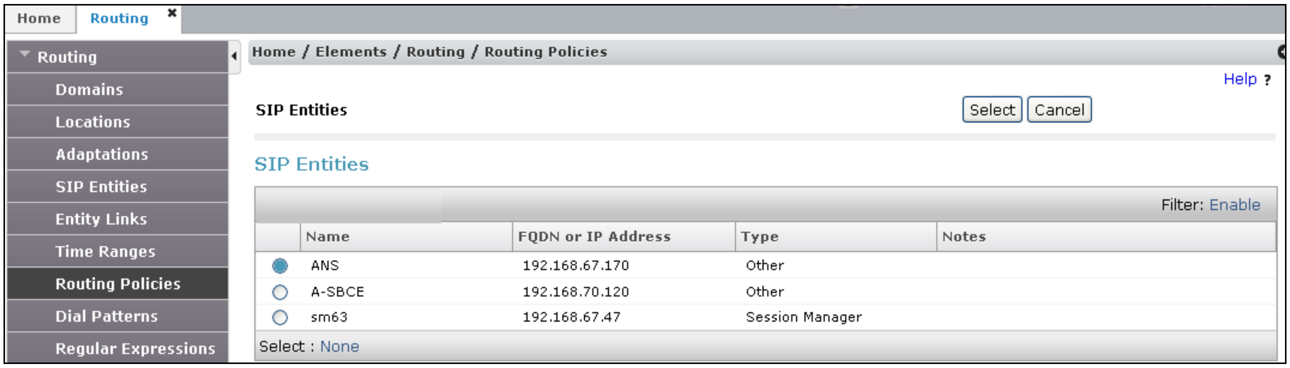
* Name:	To_ANS
Disabled:	□
* Retries:	0
Notes:	

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes

Step 3 – In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on **Select** and the SIP Entity list page will open.

Step 4 - In the **SIP Entities** page, select the SIP Entity administered in **Section 5.4.1** for the ANS SIP Entity (**ANS**), and click on **Select**.



SIP Entities

SIP Entities

	Name	FQDN or IP Address	Type	Notes
●	ANS	192.168.67.170	Other	
○	A-SBCE	192.168.70.120	Other	
○	sm63	192.168.67.47	Session Manager	

Select : None

Step 5 - Returning to the **Routing Policy Details** page in the **Time of Day** section (not shown), click on **Add**.

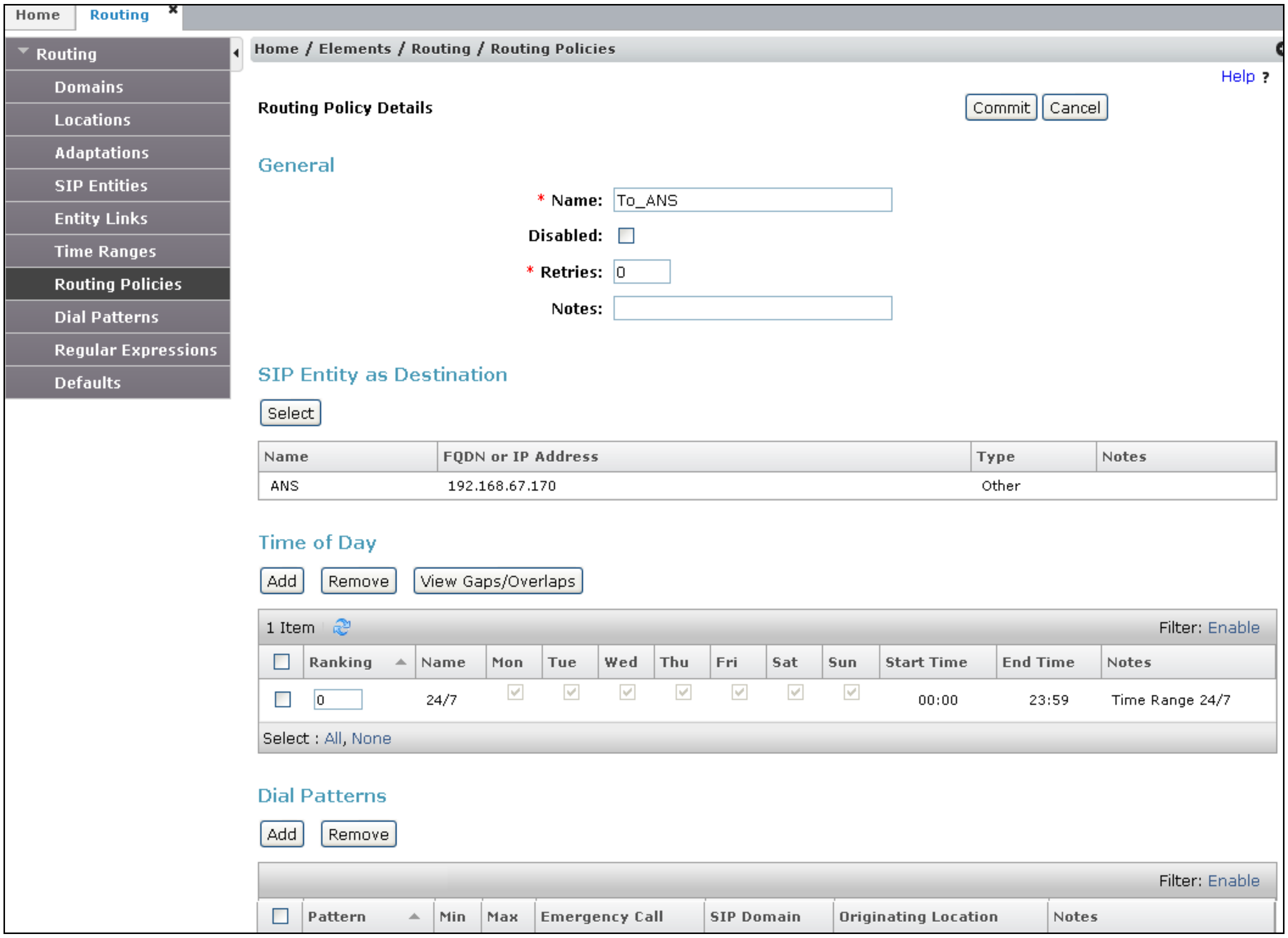
Step 6 - In the **Time Range List** page (not shown), check the checkbox(s) corresponding to one or more Time Ranges administered in **Section 5.6**, and click on **Select**.

Step 7 - Returning to the **Routing Policy Details** page in the **Time of Day** section, if multiple Time Ranges were selected, user may enter a **Ranking** (the lower the number, the higher the ranking) for each Time Range, and click on **Commit**.

Step 8 - No **Regular Expressions** were used in the reference configuration.

Step 9 - Click on **Commit**.

Note - Once the **Dial Patterns** are defined (**Section 5.8**) they will appear in the **Dial Pattern** section of this form.



Routing Policy Details

General

* Name:	To_ANS
Disabled:	□
* Retries:	0
Notes:	

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
ANS	192.168.67.170	Other	

Time of Day

1 Item   Filter: Enable

□	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Filter: Enable

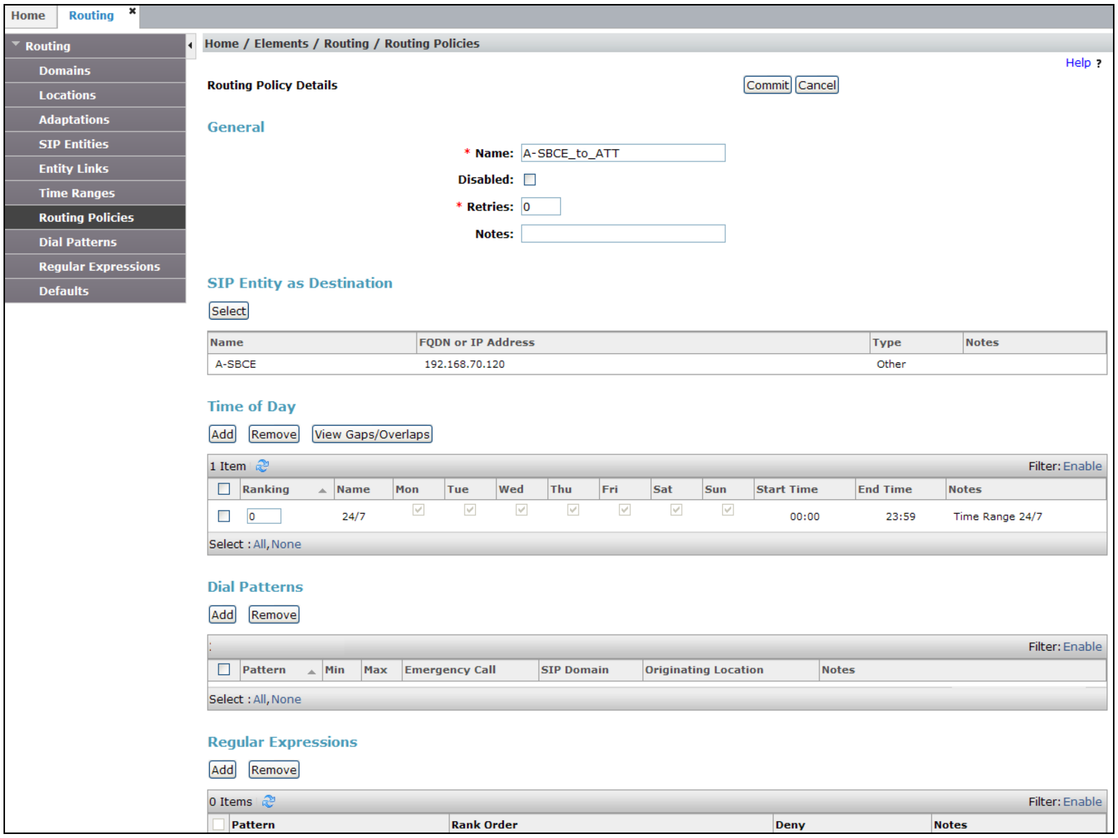
□	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes

5.7.2. Routing Policy for Avaya Notification Solution to AT&T

This Routing Policy is used for ANS outbound calls to AT&T. Repeat the steps in **Section 5.7.1** with the following changes:

- Enter a descriptive **Name** (e.g. **A-SBCE_to_ATT**) and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entity List** page, select the SIP Entity administered in **Section 5.4.2** for the Avaya SBCE (e.g. **A-SBCE**).
- In the **Time of Day** section, change the ranking number to **1**.

Note that once the **Dial Patterns** are defined (**Section 5.8**), they will appear in the **Dial Pattern** section.



Routing Policy Details

General

* Name: A-SBCE_to_ATT

Disabled: □

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
A-SBCE	192.168.70.120	Other	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

□	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Add Remove

Filter: Enable

□	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes

Select : All, None

Regular Expressions

Add Remove

0 Items Filter: Enable

□	Pattern	Rank Order	Deny	Notes

5.8. Dial Patterns

In this section, Dial Patterns are administered matching the following calls:

- Inbound PSTN calls to ANS (**Section 5.8.1**).
- Outbound calls from ANS to PSTN via AT&T (**Section 5.8.1**).

5.8.1. Matching Inbound PSTN Calls to ANS

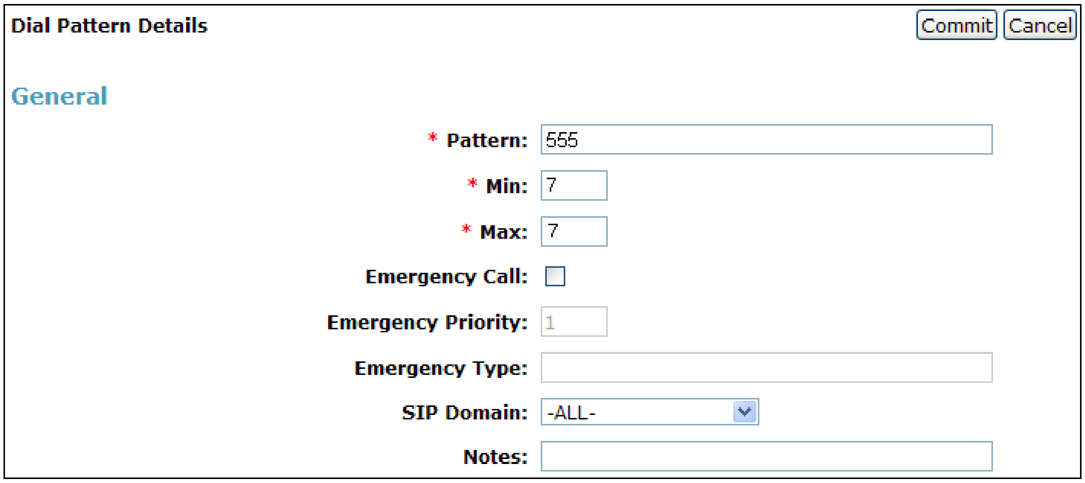
Note – Be sure to match on the DNIS digit string specified in the AT&T *Request URI*, not the DID digit string that is dialed, or the digit string in the *To* header. These may be different.

In the reference configuration, inbound calls from the AT&T IPFR-EF service used **7** digits in the SIP *Request URI*, using the format **555xxxx**, (the *To* headers contained 10 digits in the format xxx737xxxx).

Step 1 - In the left pane under **Routing**, click on **Dial Patterns**. In the **Dial Patterns** page click on **New** (not shown).

Step 2 - In the **General** section of the **Dial Pattern Details** page, provision the following:

- **Pattern** – To match the *Request URI* digit patterns sent by AT&T, enter **555**. ANS will map these digit strings to the appropriate notifications or mailboxes (see **Section 6.5**).
- **Min** - Enter **7.**
- **Max –** Enter **7**.
- **SIP Domain** – Select **-ALL-**, to select all of the administered SIP Domains.



Dial Pattern Details

General

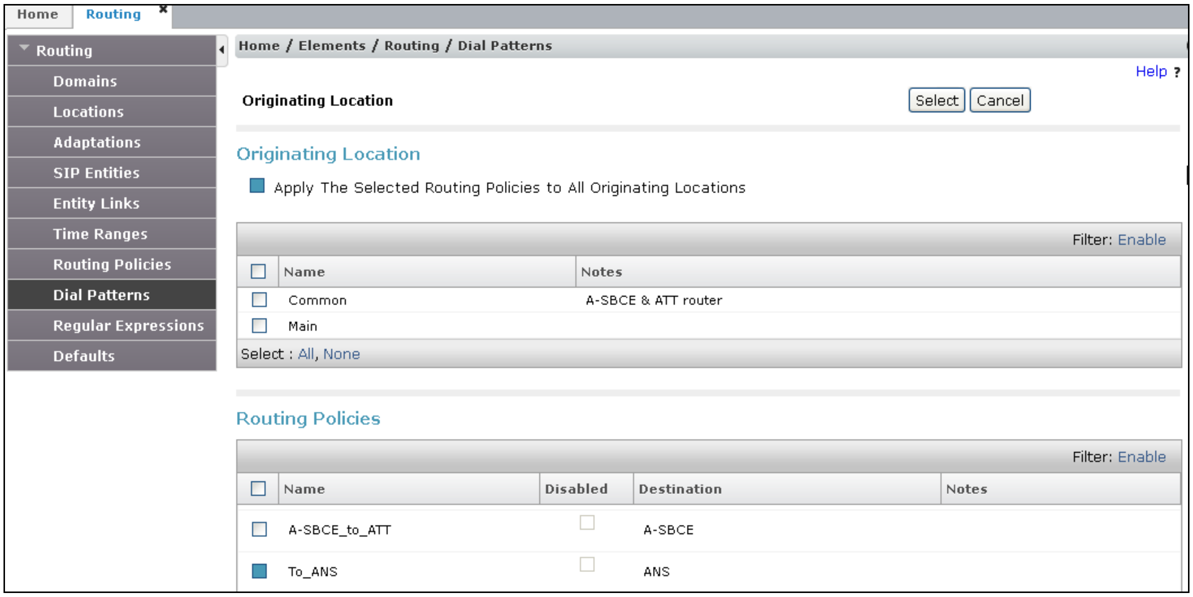
* Pattern:	555
* Min:	7
* Max:	7
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	-ALL-
Notes:	

Step 3 – Scrolling down to the **Originating Locations and Routing Policies** section of the **Dial Pattern Details** page (not shown), click on **Add**.

Step 4 - In the **Originating Location** section, select the box corresponding to "**All Originating Locations**".

Step 5 - In the **Routing Policies** section, select the box corresponding to the Routing Policy administered for routing calls to ANS in **Section 5.7.1** (e.g., **To_ANS**).

Step 6 – Click on **Select**.



Home / Elements / Routing / Dial Patterns

Originating Location

Originating Location

☑ Apply The Selected Routing Policies to All Originating Locations

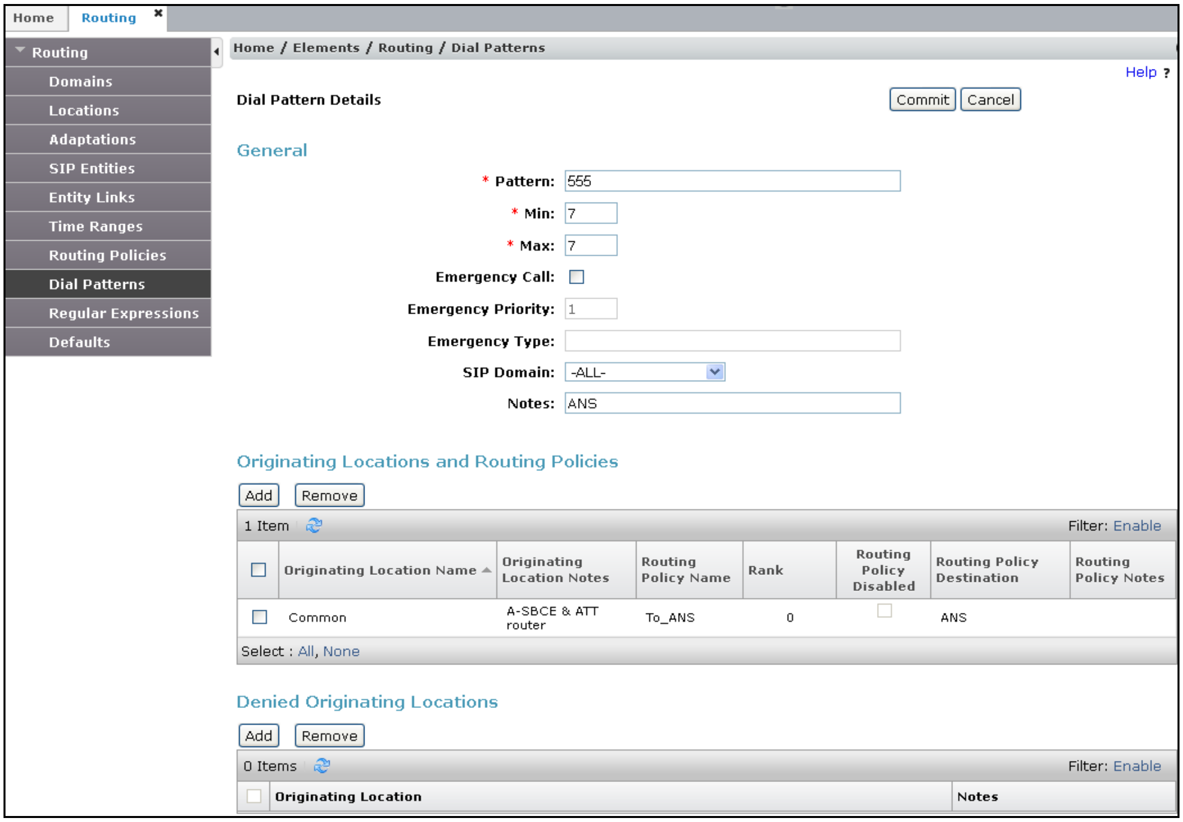
□	Name	Notes
□	Common	A-SBCE & ATT router
□	Main	

Select : All, None

Routing Policies

□	Name	Disabled	Destination	Notes
□	A-SBCE_to_ATT	□	A-SBCE	
☑	To_ANS	□	ANS	

Step 7 - Returning to the Dial Pattern Details page click on **Commit**.



Home / Elements / Routing / Dial Patterns

Dial Pattern Details

General

* Pattern: 555

* Min: 7

* Max: 7

Emergency Call: □

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes: ANS

Originating Locations and Routing Policies

1 Item

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Common	A-SBCE & ATT router	To_ANS	0	□	ANS	

Select : All, None

Denied Originating Locations

0 Items

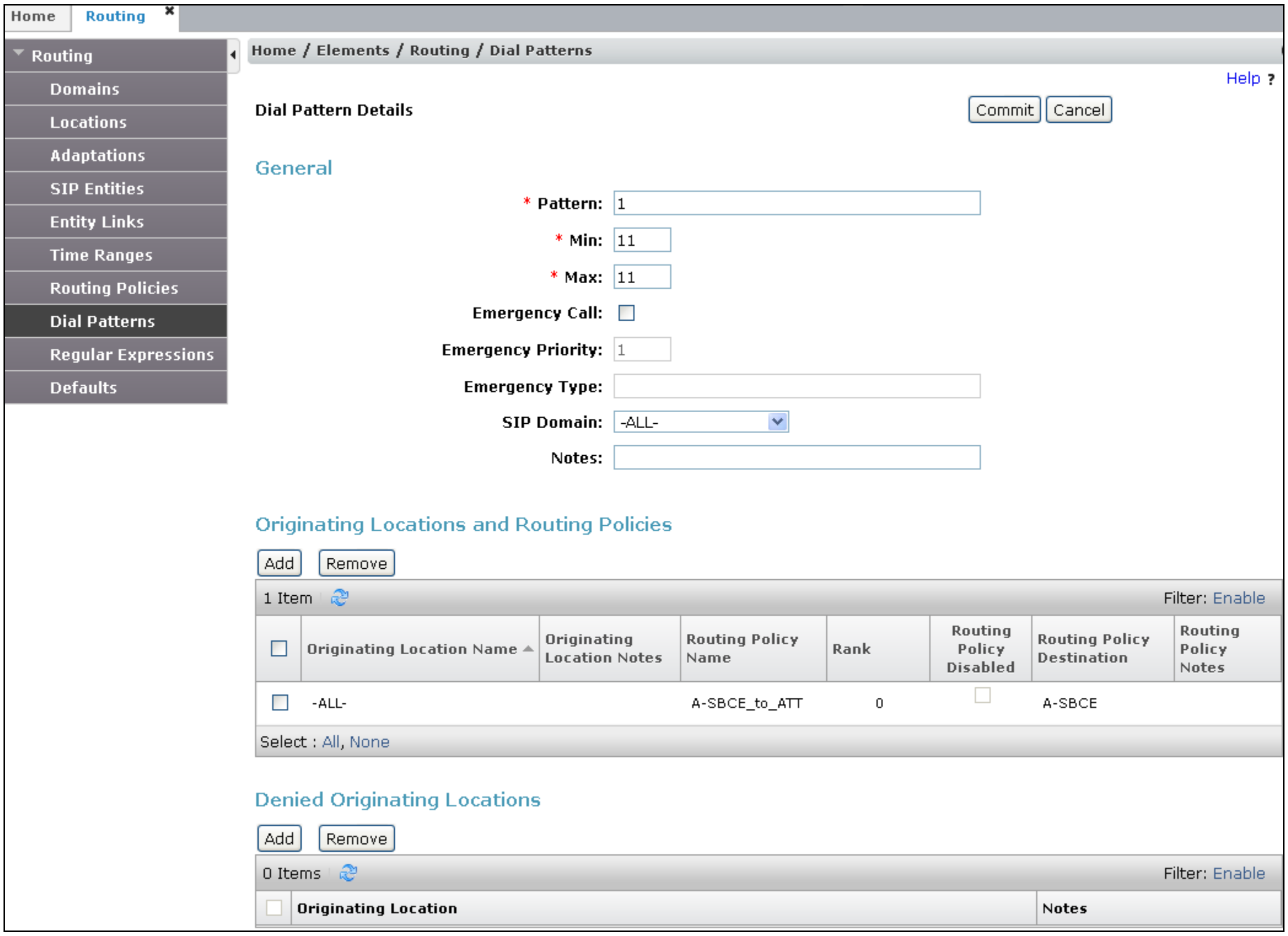
□	Originating Location	Notes

5.8.2. Matching Avaya Notification Solution Outbound Calls to AT&T

Note – In the reference configuration, outbound PSTN calls used an 11 digit North American format; 1-NPA-NXX-xxxx. Other formats may be specified.

Follow the steps shown in **Section 5.8.1**, with the following changes:

- **Pattern** – Enter **11**.
- **Min and Max** – Enter **11**.
- **Routing Policy Name** – Select **A-SBCE_to_ATT** (**Section 5.7.2**).



Dial Pattern Details

General

* Pattern:	1
* Min:	11
* Max:	11
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	-ALL-
Notes:	

Originating Locations and Routing Policies

1 Item

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		A-SBCE_to_ATT	0	□	A-SBCE	

Denied Originating Locations

0 Items

□	Originating Location	Notes

6. Configuring Avaya Notification Solution

In the following sections, the Avaya Notification Solution Web Portal and the Avaya Media Server applications are provisioned.

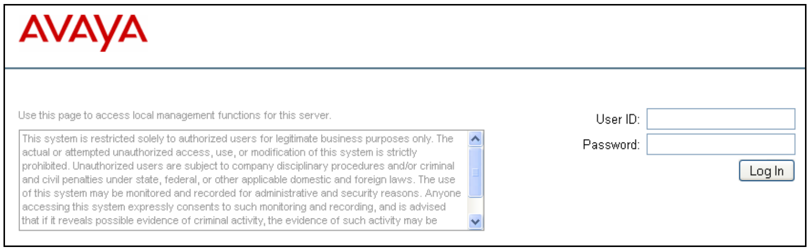
Note – A co-resident platform was used in the reference configuration. Therefore all ANS related applications share the same IP address.

6.1. Avaya Media Server Application

Note - The following sections show the configuration of parameters specific to interoperability in the reference configuration. The installation and basic configuration of AMS is beyond the scope of this document. See **[1 & 2]** for more information.

This section covers configurations related to audio codecs, ptime values, DTMF relay and RTP port ranges. Fields not specified below use the default settings.

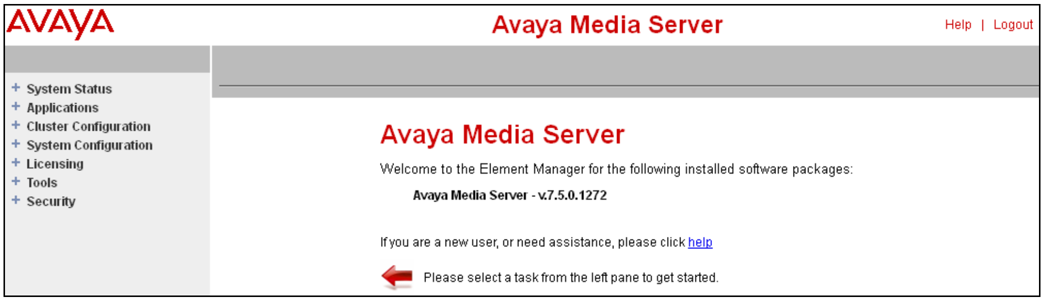
Step 1 - Launch a web browser, enter **https://<IP address of the ANS server>:9443/em** as the URL, enter the appropriate credentials, and click on **Log In**.



Use this page to access local management functions for this server.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and/or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws. The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be

The Avaya Media Server home page is displayed.



Avaya Media Server

Welcome to the Element Manager for the following installed software packages:

Avaya Media Server - v.7.5.0.1272

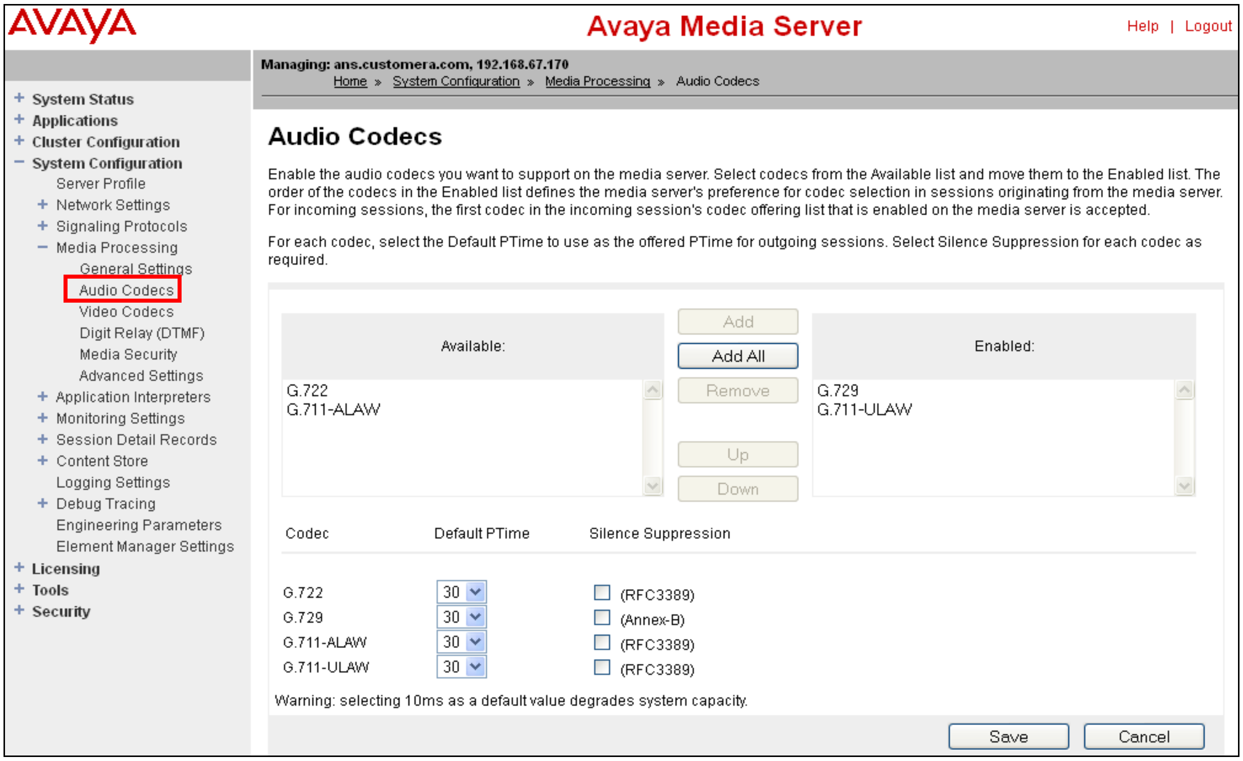
If you are a new user, or need assistance, please click help

Please select a task from the left pane to get started.

Step 2 - Navigate to **System Configuration→Media Processing→Audio Codecs** and provision as follows:

- Using the **Add/Remove** buttons select and move **G.729** and **G.711-ULAW** codecs into the **Enabled** column. Then use the **Up/Down** buttons, set the **G729** codec to the top of the list (see **Section 2.2**, **item 2)**.
- Set the **PTime** value for **G.729** and **G.711-ULAW** to **30**.

- Verify the **Silence Suppression** box in unchecked for **G729** (see **Section 2.2**, **item 3)**, and click on **Save**.



Audio Codecs

Enable the audio codecs you want to support on the media server. Select codecs from the Available list and move them to the Enabled list. The order of the codecs in the Enabled list defines the media server's preference for codec selection in sessions originating from the media server. For incoming sessions, the first codec in the incoming session's codec offering list that is enabled on the media server is accepted.

For each codec, select the Default PTime to use as the offered PTime for outgoing sessions. Select Silence Suppression for each codec as required.

Available: G.722, G.711-ALAW

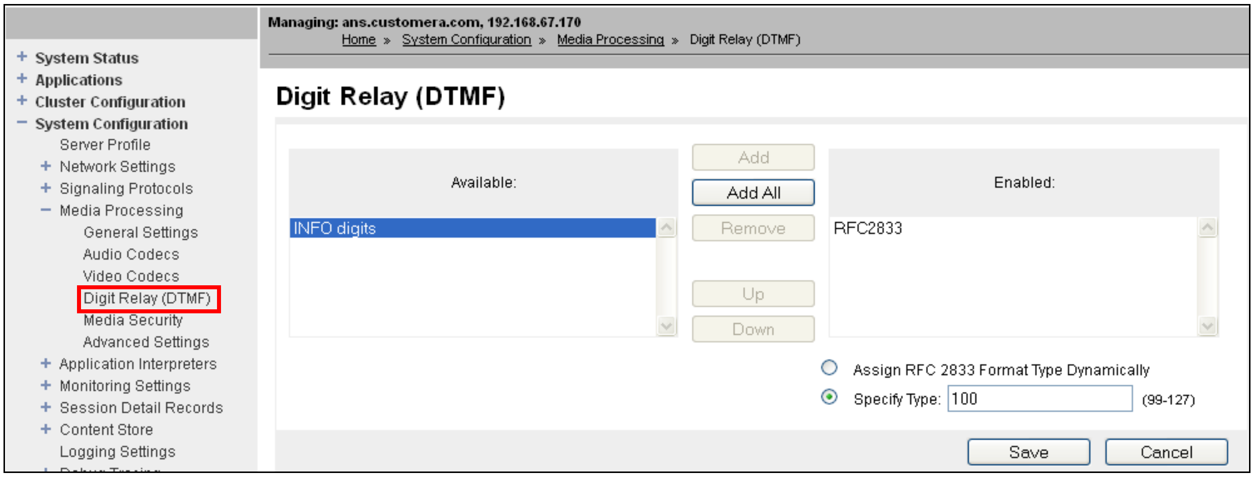
Enabled: G.729, G.711-ULAW

Codec	Default PTime	Silence Suppression
G.722	30	□ (RFC3389)
G.729	30	□ (Annex-B)
G.711-ALAW	30	□ (RFC3389)
G.711-ULAW	30	□ (RFC3389)

Warning: selecting 10ms as a default value degrades system capacity.

Step 4 - Navigate to **System Configuration→Media Processing→Digital Relay (DTMF)** and set the following:

- Verify that **RFC2833** is in the **Enabled** column. If not, use the **Add/Remove** buttons to set the value.
- Set the **Specify Type** field to **100** (value used by AT&T), and click **Save**.



Digit Relay (DTMF)

Available: INFO digits

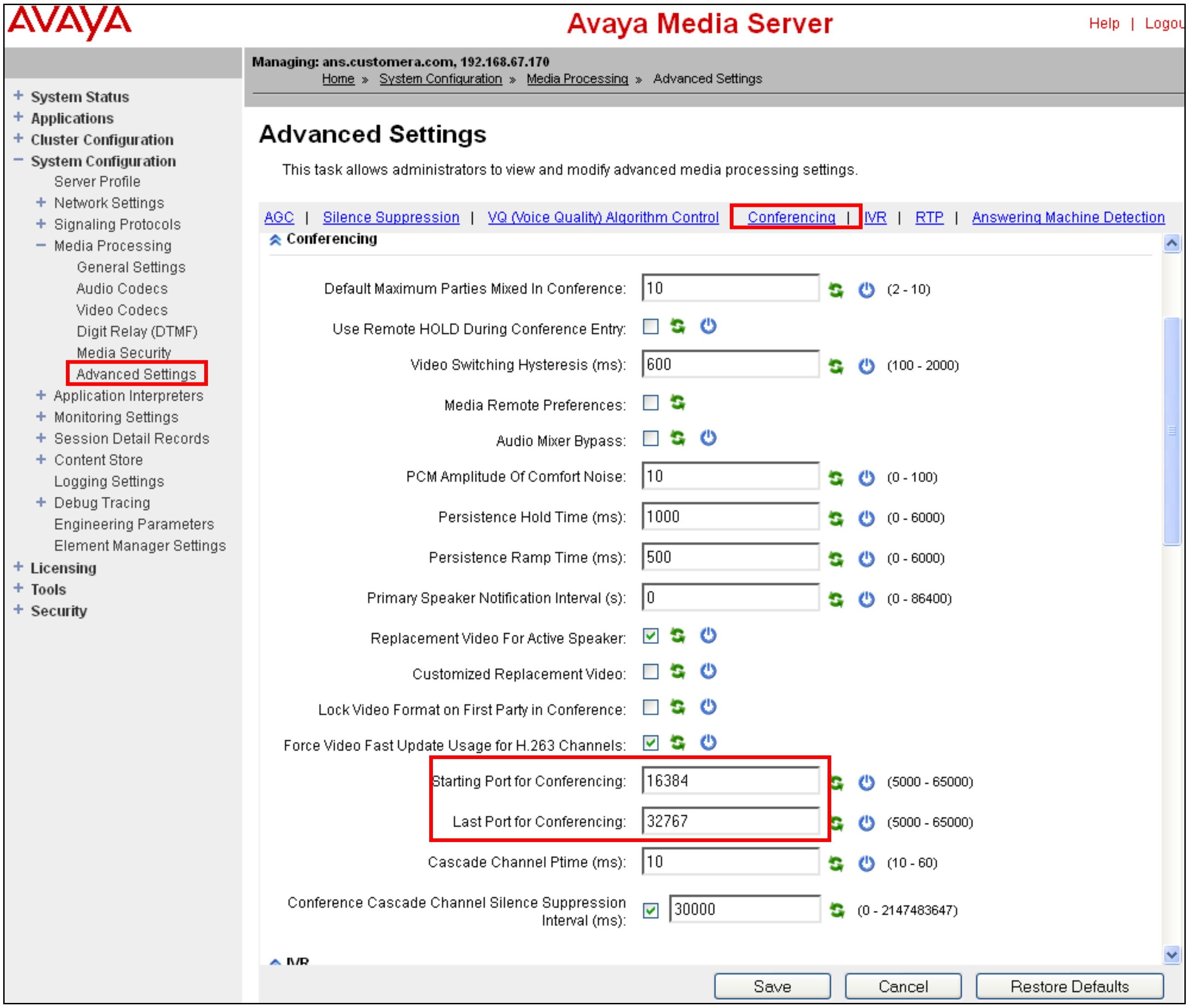
Enabled: RFC2833

○ Assign RFC 2833 Format Type Dynamically

● Specify Type: 100 (99-127)

Step 6 - Navigate to **System Configuration→Media Processing→Advanced Settings.** Select **Conferencing** from the upper menu and specify the following:

- Set **Starting Port for Conferencing** field to **16384** and **Last Port for Conferencing** field to **32767** as required by the AT&T IP Flexible Reach service, and click **Save**.



Advanced Settings

This task allows administrators to view and modify advanced media processing settings.

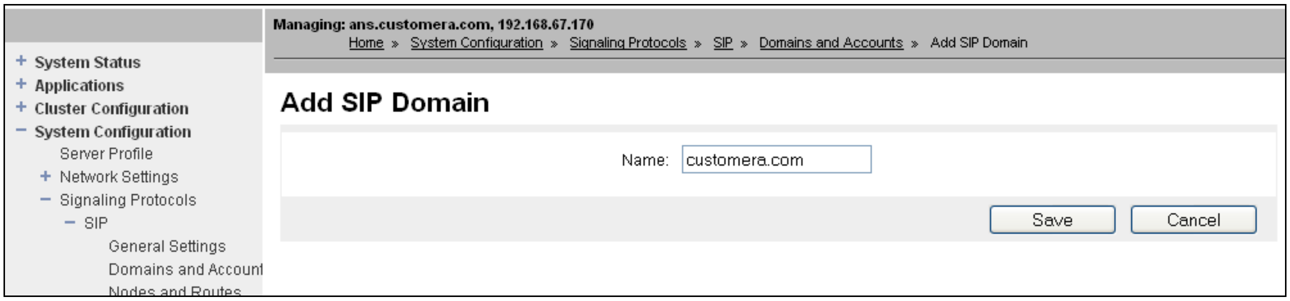
Conferencing

Default Maximum Parties Mixed In Conference:	10	(2 - 10)
Use Remote HOLD During Conference Entry:	☐	
Video Switching Hysteresis (ms):	600	(100 - 2000)
Media Remote Preferences:	☐	
Audio Mixer Bypass:	☐	
PCM Amplitude Of Comfort Noise:	10	(0 - 100)
Persistence Hold Time (ms):	1000	(0 - 6000)
Persistence Ramp Time (ms):	500	(0 - 6000)
Primary Speaker Notification Interval (s):	0	(0 - 86400)
Replacement Video For Active Speaker:	☑	
Customized Replacement Video:	☐	
Lock Video Format on First Party in Conference:	☐	
Force Video Fast Update Usage for H.263 Channels:	☑	
Starting Port for Conferencing:	16384	(5000 - 65000)
Last Port for Conferencing:	32767	(5000 - 65000)
Cascade Channel Ptime (ms):	10	(10 - 60)
Conference Cascade Channel Silence Suppression Interval (ms):	☑ 30000	(0 - 2147483647)

Step 8 - Navigate to **System Configuration→Signaling Protocols→SIP→Domains and Accounts**.

Step 9 – In the **Domains** section, click on **Add**, and enter the following:

- In the **Name** field enter the domain specified for Session Manager in **Section 5.1** (**customera.com**), then click on **Save**.



Add SIP Domain

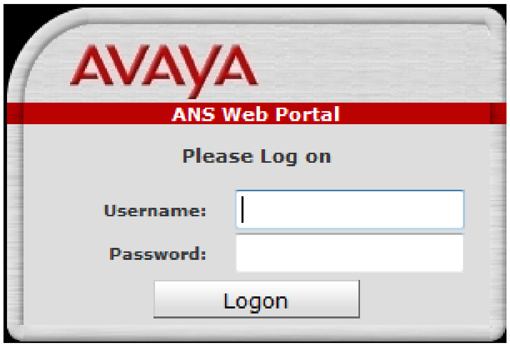
Name: customera.com

6.2. Avaya Notification Solution Application

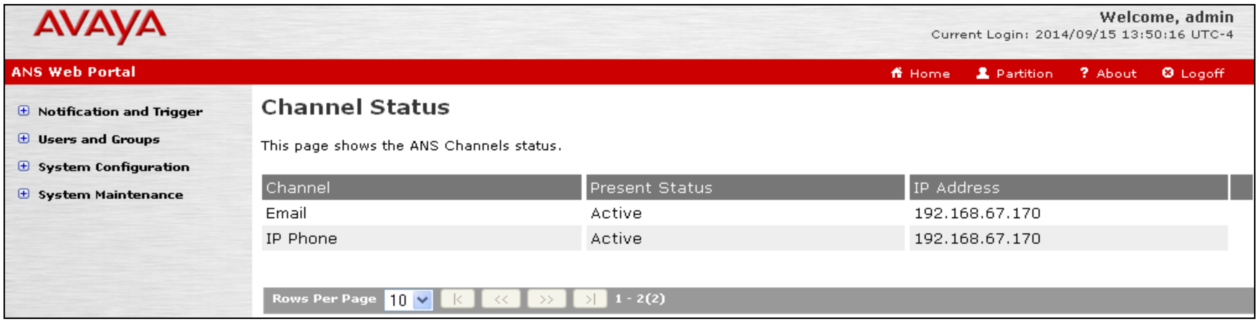
Note - The following sections show the configuration of parameters specific to interoperability in the reference configuration. The installation and basic configuration of ANS is beyond the scope of this document. See **[1 & 2]** for more information.

This section describes the provisioning of ANS to generate outbound notifications, ad hoc conferencing, as well as associated inbound call triggers, used to test SIP trunk interoperability with the IPFR-EF service. The following sections are not meant to be prescriptive, but are shown as provisioning examples.

Step 1 - Via a web browser, enter **https://<IP address of the ANS server>:8443/ANSWebPortal** as the URL, enter the appropriate credentials, and click on **Logon**.



The ANS Web Portal main page is displayed. Note that the screen shot shows provisioning performed during installation (192.168.67.170 is the IP address of the ANS server).



Channel Status

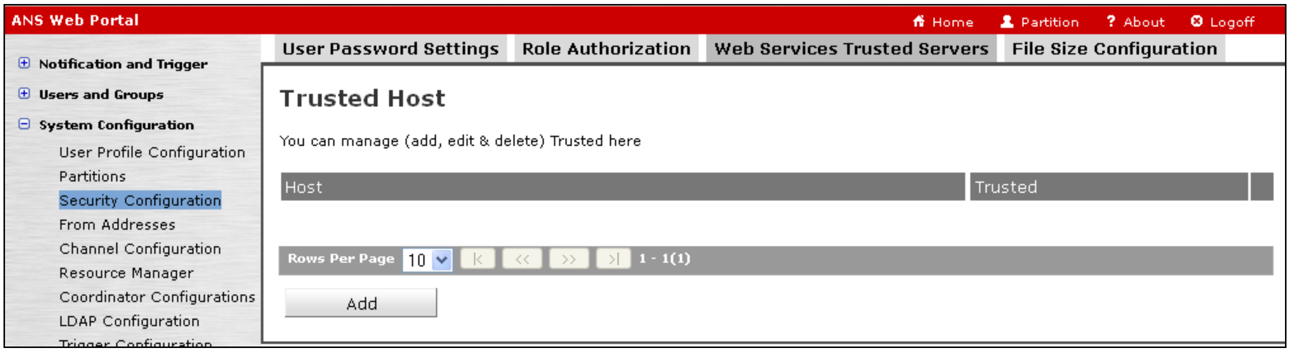
This page shows the ANS Channels status.

Channel	Present Status	IP Address
Email	Active	192.168.67.170
IP Phone	Active	192.168.67.170

6.2.1. Trusted Servers

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

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

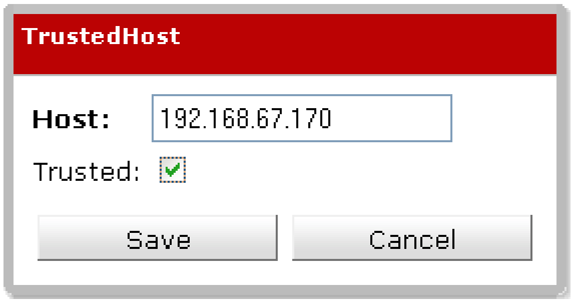


Trusted Host

You can manage (add, edit & delete) Trusted here

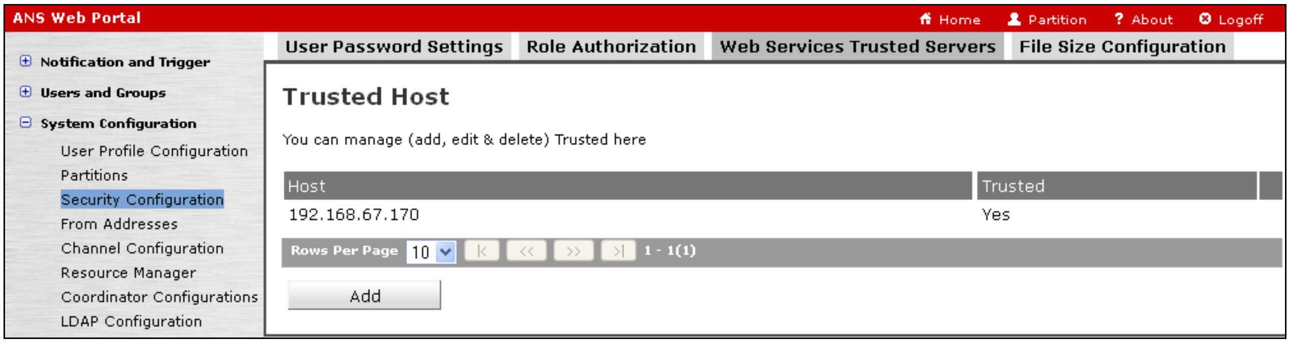
Host	Trusted

Step 2 – The **TrustedHost** window will open. Enter the IP address of the ANS server (e.g., **192.168.67.170**), and check the **Trusted** box. Click **Save**.



Host: 192.168.67.170

Trusted: ☑



Trusted Host

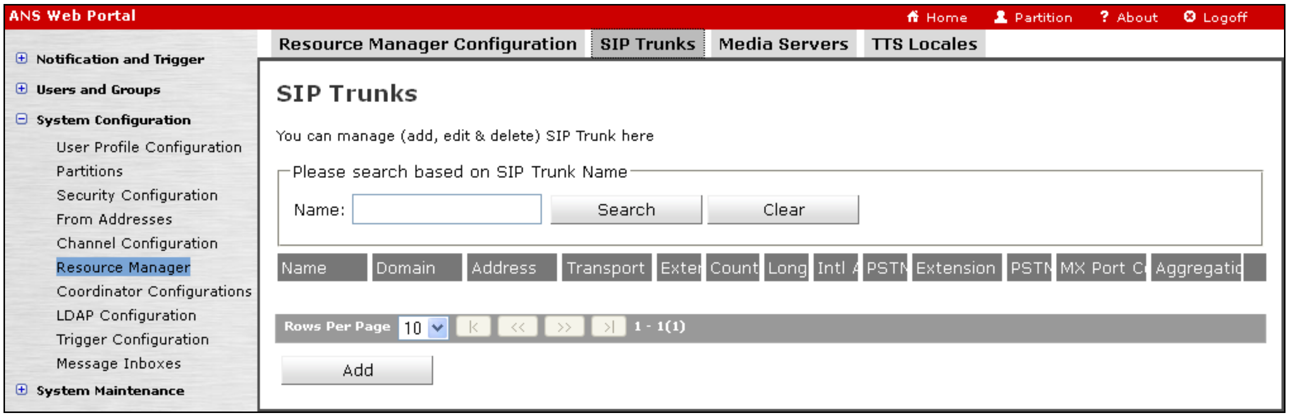
You can manage (add, edit & delete) Trusted here

Host	Trusted
192.168.67.170	Yes

6.2.2. VoIP Connection

This section describes the steps to configure a SIP trunk between ANS and Session Manager.

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



SIP Trunks

You can manage (add, edit & delete) SIP Trunk here

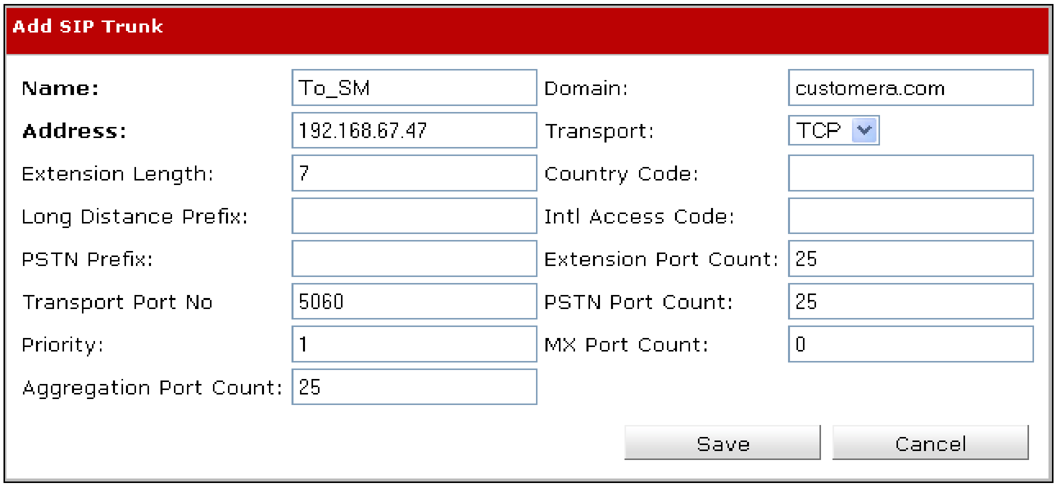
Please search based on SIP Trunk Name

Name:

Step 2 – The **Add SIP Trunk** window will open. Enter the following:

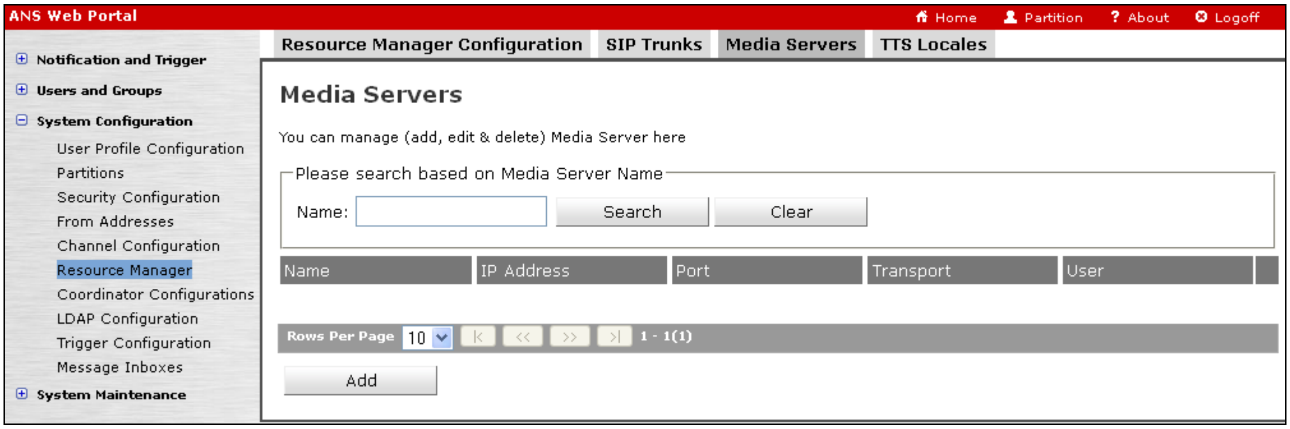
- **Name** – Enter a name (e.g., **To_SM**).
- **Domain** – Set to the SIP domain specified in **Sections 5.1** and **6.1** (e.g., **customera.com**).
- **Address** – Set to the IP Address of Session Manager (e.g., **192.168.67.47**, see **Section 5.4.3**).
- **Transport** – Set to **TCP** (used in the 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.

Step 3 - Click **Save**.



Name:	To_SM	Domain:	customera.com
Address:	192.168.67.47	Transport:	TCP
Extension Length:	7	Country Code:	
Long Distance Prefix:		Intl Access Code:	
PSTN Prefix:		Extension Port Count:	25
Transport Port No	5060	PSTN Port Count:	25
Priority:	1	MX Port Count:	0
Aggregation Port Count:	25		

Step 4 - In the left pane, navigate to **System Configuration→Resource Manager** and select **Media Servers** tab. On the **Media Servers** page, click **Add**.



Media Servers

You can manage (add, edit & delete) Media Server here

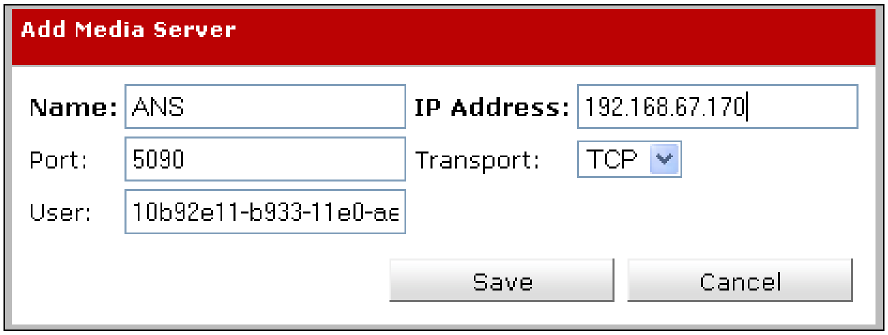
Please search based on Media Server Name

Name:

Name	IP Address	Port	Transport	User

Step 5 – The **Add Media Server** window will open. Enter the following:

- **Name** – Enter a name (e.g., **ANS**).
- **IP Address** – Enter the IP address of the ANS server (e.g., **192.168.67.170**).
- Use default for all other fields and click **Save**, (note that the **Transport** and **Port** fields are **TCP** & **5090**).



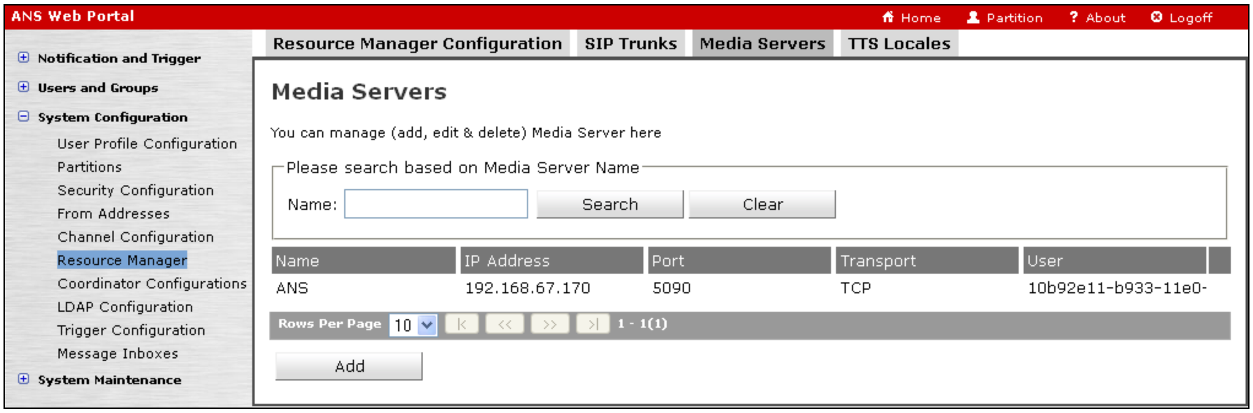
Name: ANS

IP Address: 192.168.67.170

Port: 5090

Transport: TCP

User: 10b92e11-b933-11e0-ae



Media Servers

You can manage (add, edit & delete) Media Server here

Please search based on Media Server Name

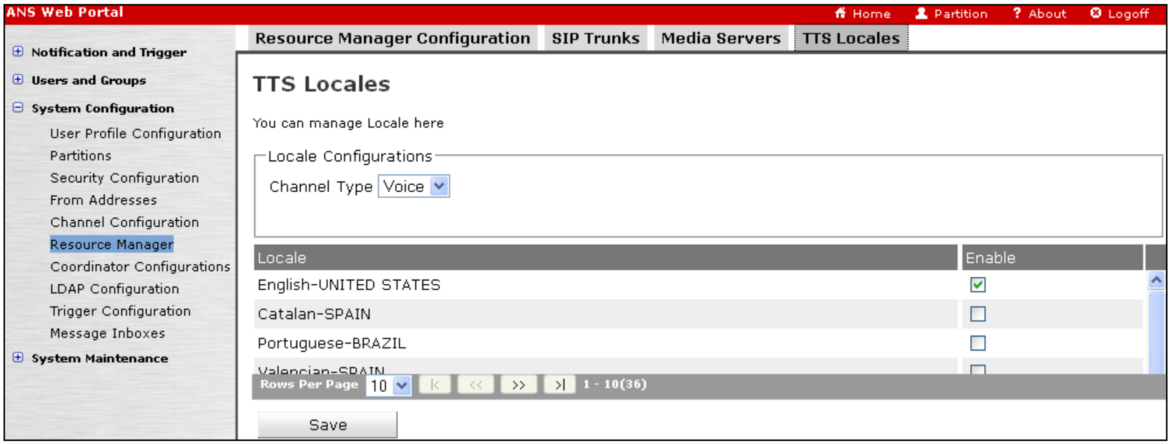
Name:

Name	IP Address	Port	Transport	User
ANS	192.168.67.170	5090	TCP	10b92e11-b933-11e0-

6.2.3. TTS Locales

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

Step 1 - In the left pane, navigate to **System Configuration→Resource Manager** and select the **TTS Locales** tab. Check the appropriate **Enable** box (e.g., **English-UNITED STATES**) and click **Save**.



TTS Locales

You can manage Locale here

Locale Configurations

Channel Type: Voice

Locale	Enable
English-UNITED STATES	☑
Catalan-SPAIN	☐
Portuguese-BRAZIL	☐
Valencian-SPAIN	☐

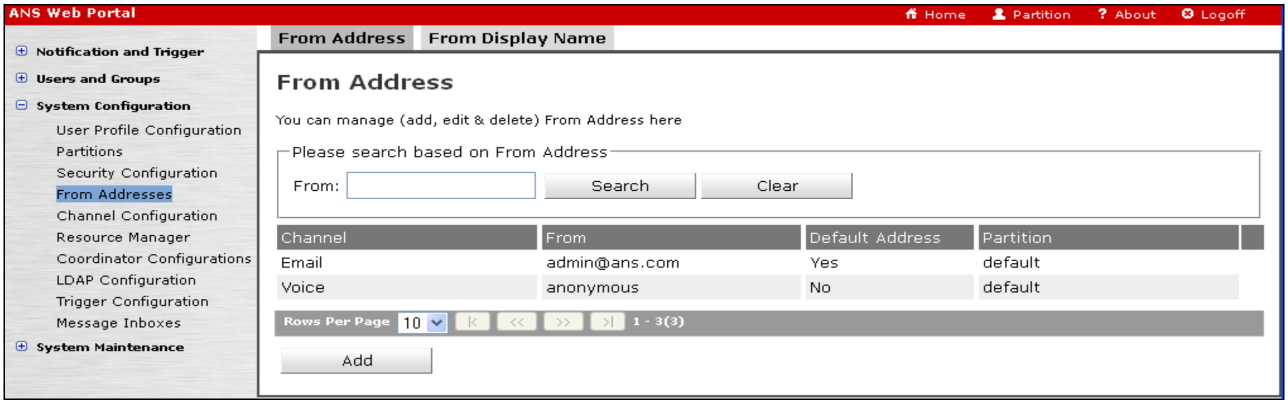
Rows Per Page 10 1 - 10(36)

6.2.4. From Address Configuration

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

Note – Default Email and Voice entries are created during ANS installation. A new Voice entry is added to be used for the testing.

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



From Address

You can manage (add, edit & delete) From Address here

Please search based on From Address

From:

Channel	From	Default Address	Partition
Email	admin@ans.com	Yes	default
Voice	anonymous	No	default

Rows Per Page 10 1 - 3(3)

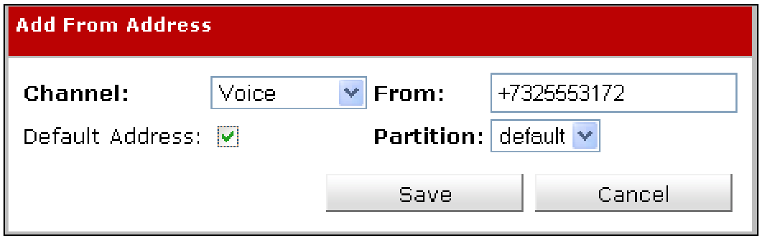
Step 2 – The **Add From Address** window will open. Enter the following:

- **Channel** – Select **Voice** from a drop-down list.
- **From** – Enter a valid telephone number (e.g., **+7325553172**).

Note – ANS requires that this entry begins with a "+" character.

- **Default Address** – Check this box for at least one Address entry.
- **Partition** – Use the **default** setting.

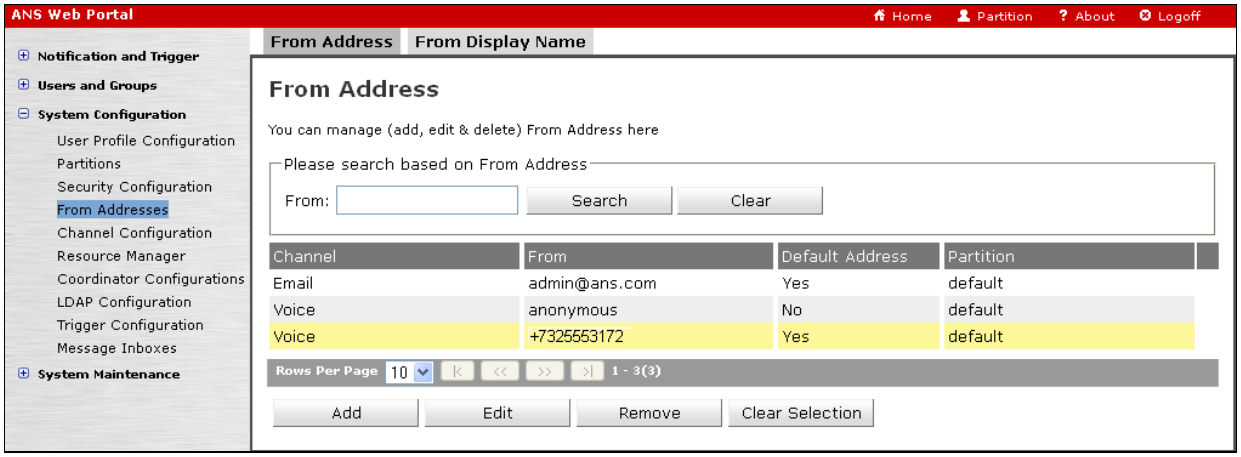
Step 3 - Click **Save**.



Add From Address

Channel: Voice **From:** +7325553172

Default Address: ☑ **Partition:** default



From Address

You can manage (add, edit & delete) From Address here

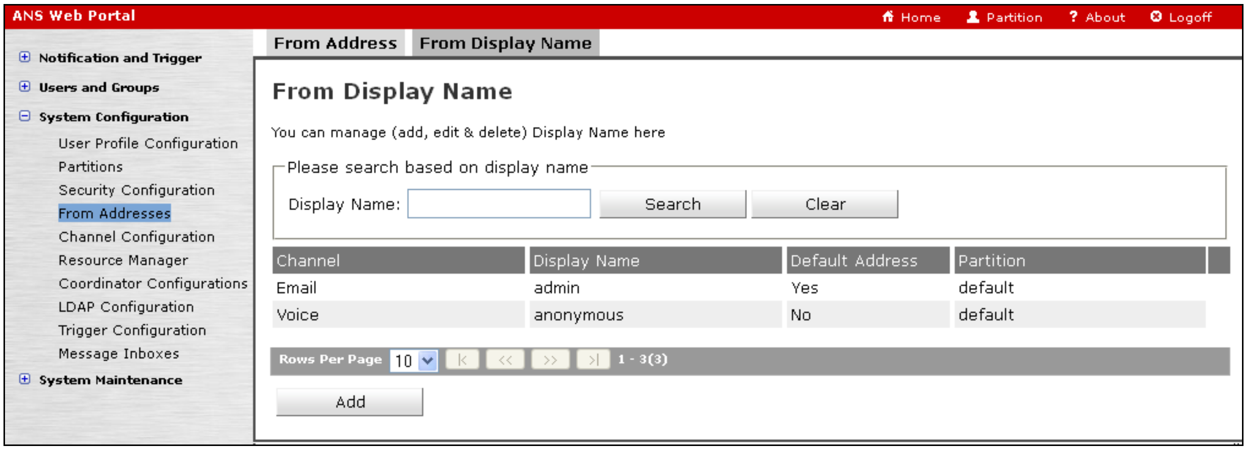
Please search based on From Address

From:

Channel	From	Default Address	Partition
Email	admin@ans.com	Yes	default
Voice	anonymous	No	default
Voice	+7325553172	Yes	default

Rows Per Page 10 1 - 3(3)

Step 4 – Click on the **From Display Name** tab. Click on **Add**.



From Display Name

You can manage (add, edit & delete) Display Name here

Please search based on display name

Display Name:

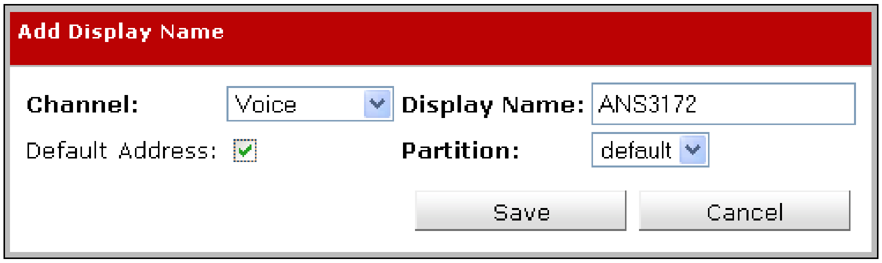
Channel	Display Name	Default Address	Partition
Email	admin	Yes	default
Voice	anonymous	No	default

Rows Per Page 10 1 - 3(3)

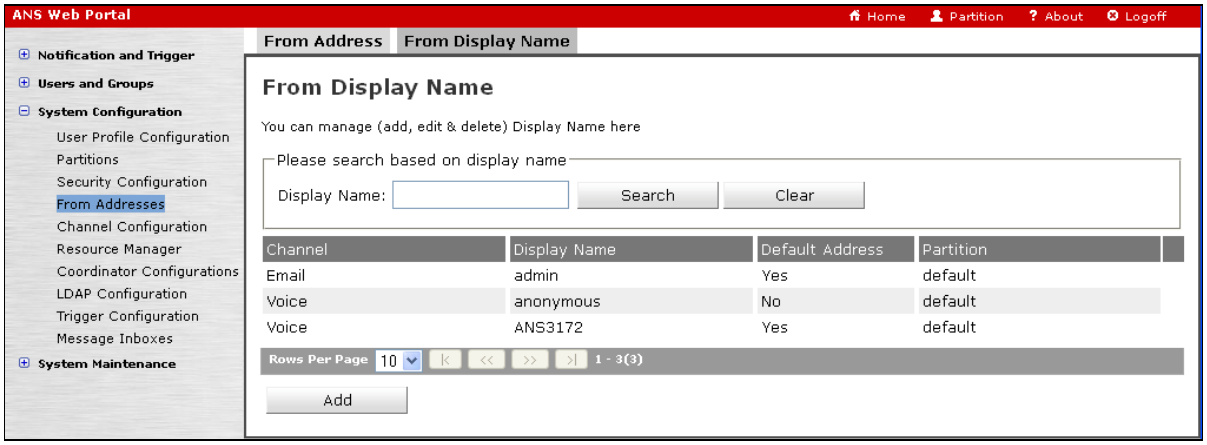
Step 5 – The Add Display Name window will open. Enter the following:

- **Channel** – Select **Voice** from drop-down list.
- **Display Name** – Enter a name (e.g., **ANS3172**).
- **Default Address** – Check this box for at least one Display Name entry.
- **Partition** – Use the **default** setting.

Step 6 - Click **Save**.



Channel:	Voice	**Display Name:**	ANS3172
Default Address:	☑	**Partition:**	default



From Display Name

You can manage (add, edit & delete) Display Name here

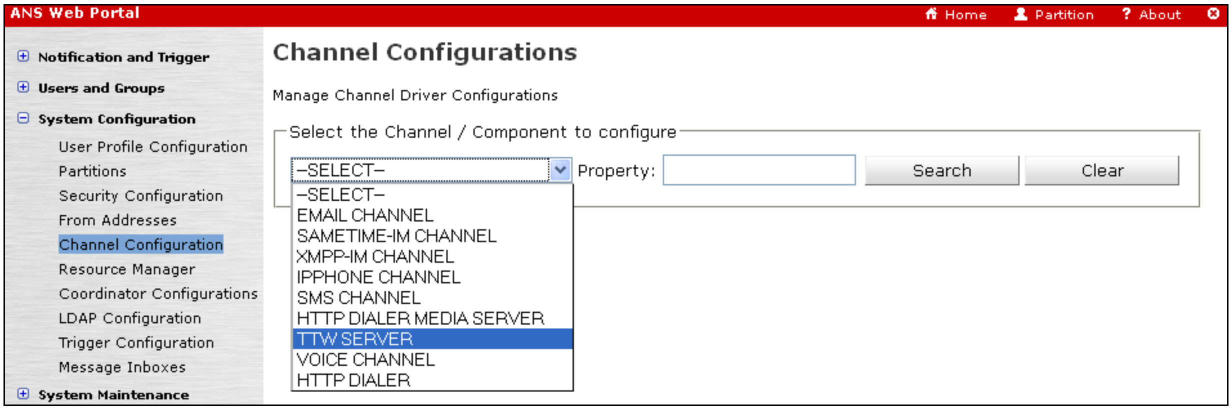
Please search based on display name

Display Name:

Channel	Display Name	Default Address	Partition
Email	admin	Yes	default
Voice	anonymous	No	default
Voice	ANS3172	Yes	default

6.2.5. TTW Server

Step 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.



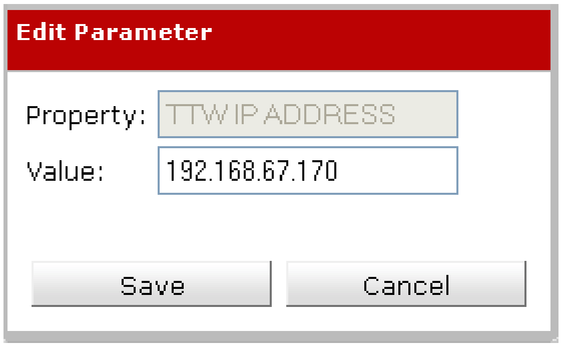
Channel Configurations

Manage Channel Driver Configurations

Select the Channel / Component to configure

Property:

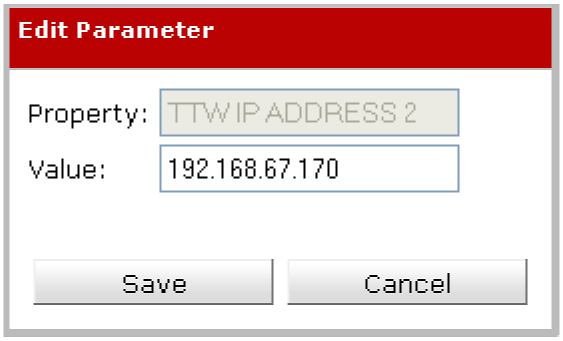
Step 2 – Select entries **TTW IP ADDRESS** and **TTW IP ADDRESS 2** and set them to the IP address of the ANS server (**192.168.67.170**), and click **Save**. Let other table entries default.



Edit Parameter

Property: TTW IP ADDRESS

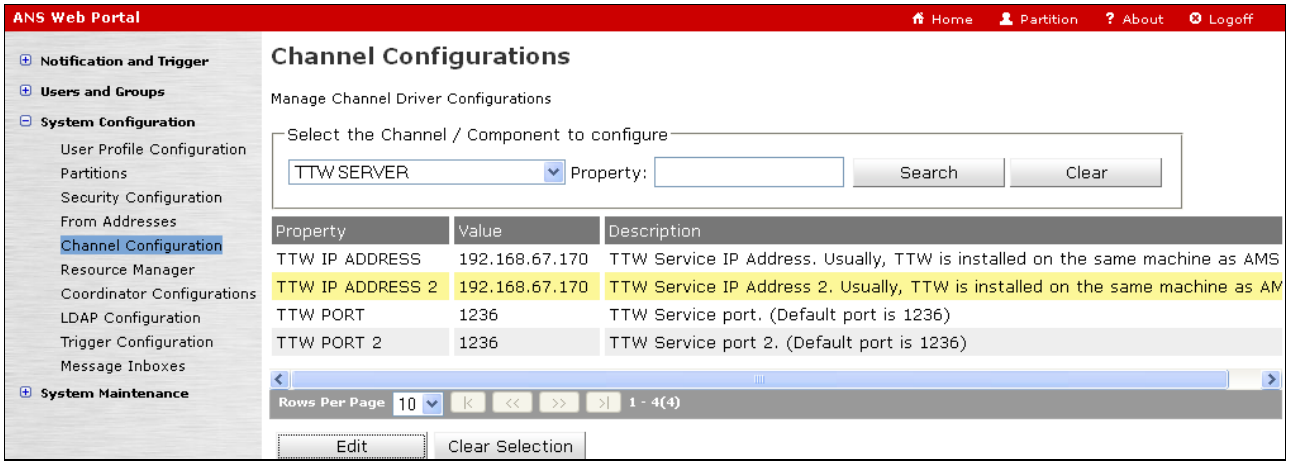
Value: 192.168.67.170



Edit Parameter

Property: TTW IP ADDRESS 2

Value: 192.168.67.170



Channel Configurations

Manage Channel Driver Configurations

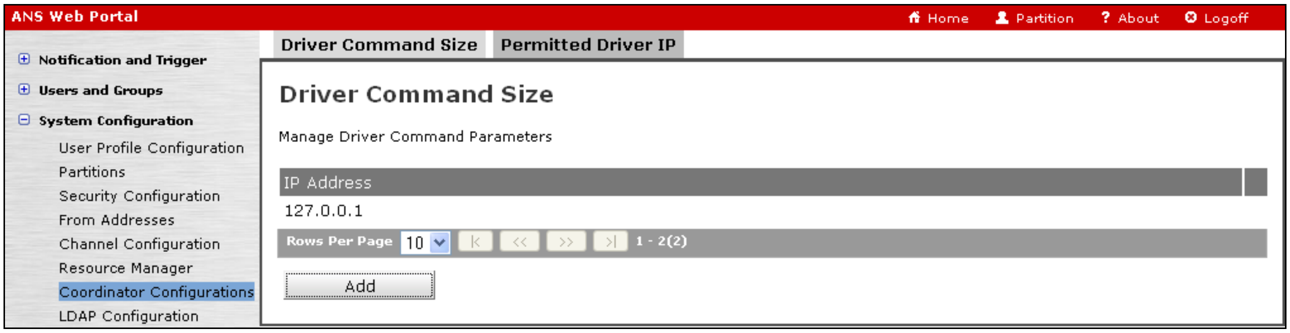
Select the Channel / Component to configure: TTW SERVER Property:

Property	Value	Description
TTW IP ADDRESS	192.168.67.170	TTW Service IP Address. Usually, TTW is installed on the same machine as AMS
TTW IP ADDRESS 2	192.168.67.170	TTW Service IP Address 2. Usually, TTW is installed on the same machine as AM
TTW PORT	1236	TTW Service port. (Default port is 1236)
TTW PORT 2	1236	TTW Service port 2. (Default port is 1236)

Rows Per Page 10 1 - 4(4)

6.2.6. Permitted Driver IP Addresses

Step 1 - Navigate to **System Configuration→Coordinator Configuration,** select the **Permitted Driver IP** tab, and click **Add**.



Driver Command Size

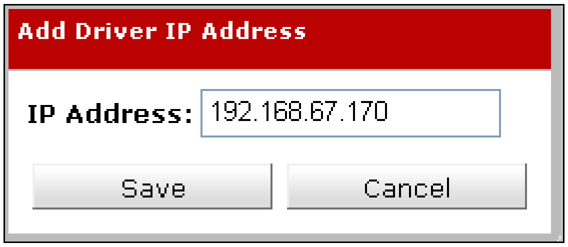
Manage Driver Command Parameters

IP Address
127.0.0.1

Rows Per Page 10 1 - 2(2)

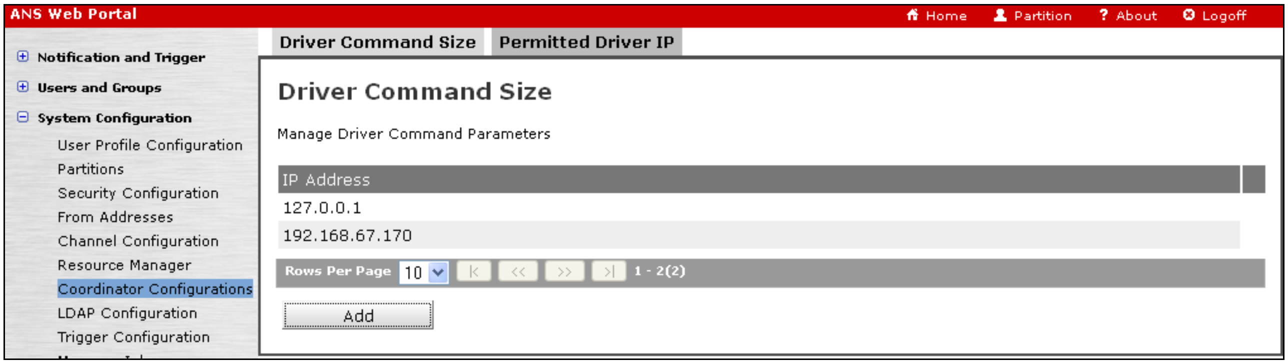
Step 2 – The **Add Driver IP Address** Window will open. Enter the following:

- IP Address – Enter the IP address of the ANS server (e.g., **192.168.67.170**). Click on **Save**.



Add Driver IP Address

IP Address: 192.168.67.170



Driver Command Size

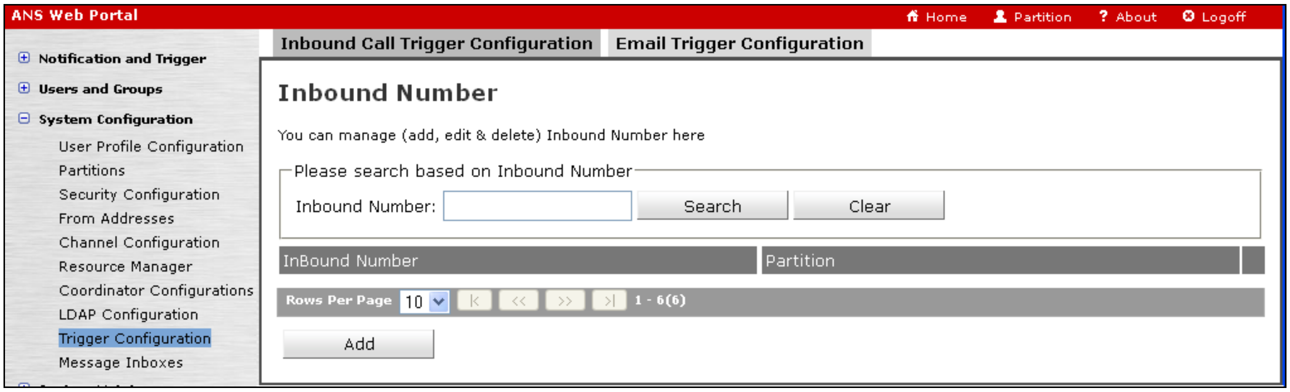
Manage Driver Command Parameters

IP Address
127.0.0.1
192.168.67.170

6.2.7. Inbound Number

ANS inspects the **To** header of inbound Invite messages to determine the acceptance/destination of a call. These inbound numbers are configured to determine which trigger is invoked when a call comes into ANS.

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



Inbound Number

You can manage (add, edit & delete) Inbound Number here

Please search based on Inbound Number

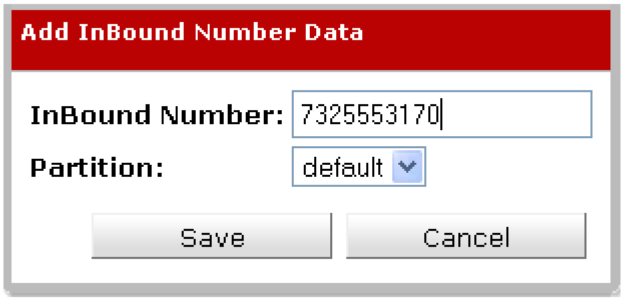
Inbound Number:

InBound Number	Partition

Step 2 – The **Add Inbound Number Data** window will open. Enter the following:

- **Inbound Number** – Set to a digit string that the IPFR-EF service *sends in the To header* of an inbound Invite message (e.g., **7325553170**).

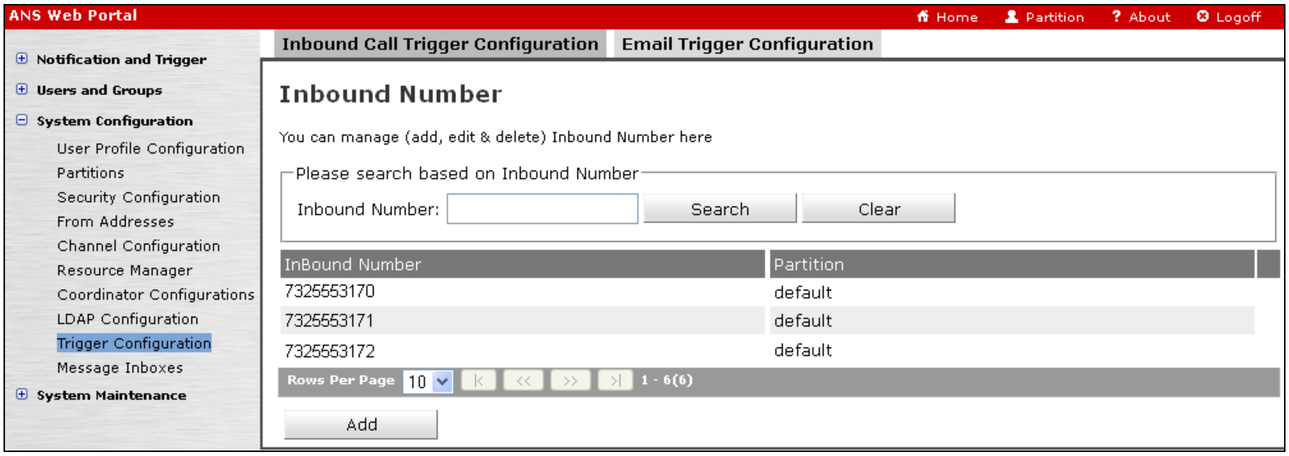
Step 3 - Click **Save.** Repeat **Steps 2 & 3** to configure additional inbound IPFR-EF service numbers as required.



Add InBound Number Data

InBound Number: 7325553170

Partition: default



Inbound Number

You can manage (add, edit & delete) Inbound Number here

Please search based on Inbound Number

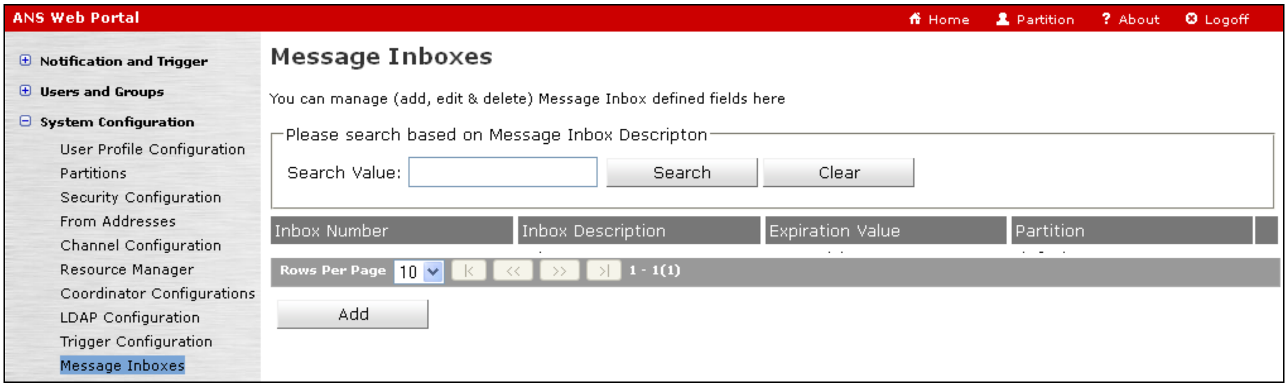
Inbound Number:

InBound Number	Partition
7325553170	default
7325553171	default
7325553172	default

6.2.8. Message Inbox

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

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



Message Inboxes

You can manage (add, edit & delete) Message Inbox defined fields here

Please search based on Message Inbox Descripton

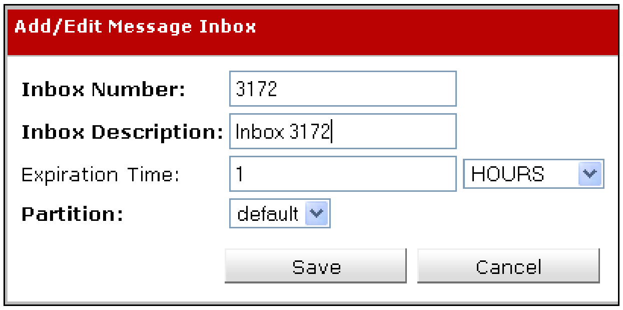
Search Value:

Inbox Number	Inbox Description	Expiration Value	Partition

Step 2- The Add/Edit Message Inbox window will open. Enter the following:

- **Inbox Number** – Set to any valid number (e.g., **3172**).
- **Inbox Description** – Enter a description (e.g., **Inbox 3172**).
- Use the default values for the **Expiration Time** and **Partition** fields.

Step 3 - Click **Save**.



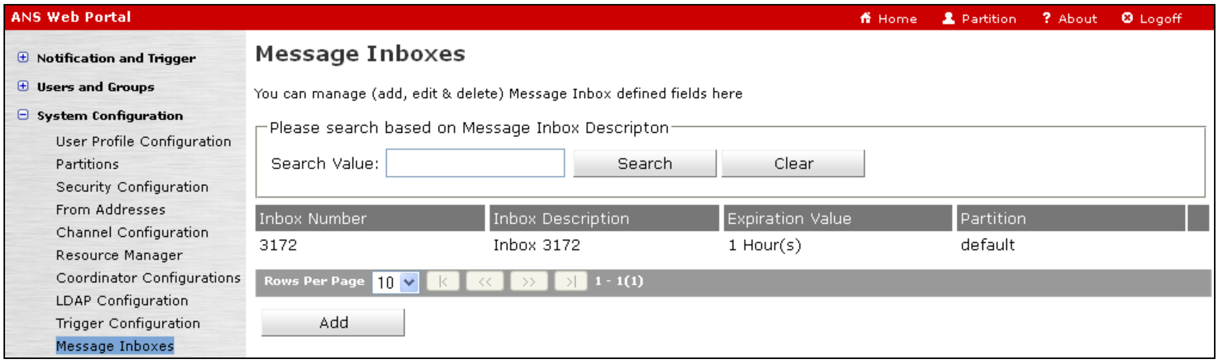
Add/Edit Message Inbox

Inbox Number: 3172

Inbox Description: Inbox 3172

Expiration Time: 1 HOURS

Partition: default



Message Inboxes

You can manage (add, edit & delete) Message Inbox defined fields here

Please search based on Message Inbox Descripton

Search Value:

Inbox Number	Inbox Description	Expiration Value	Partition
3172	Inbox 3172	1 Hour(s)	default

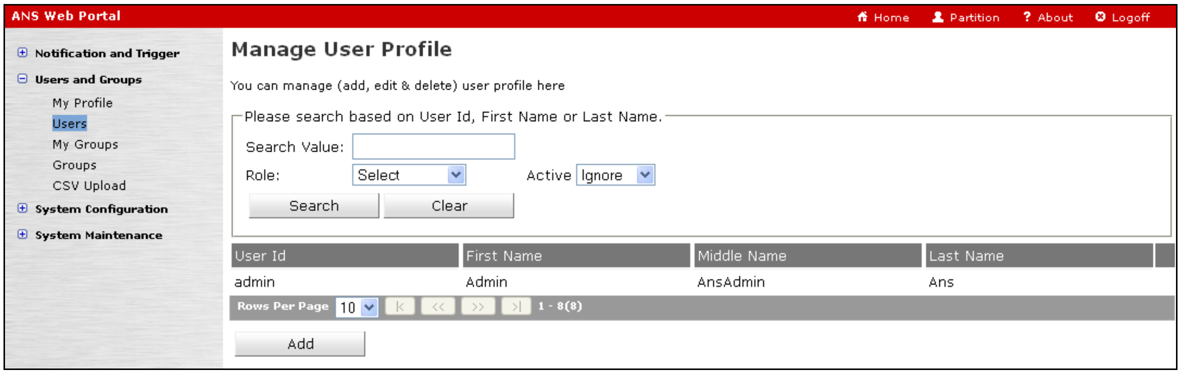
Rows Per Page 10 1 - 1(1)

Step 4 - Repeat **Steps 2** & **3** to configure additional Message inboxes as needed.

6.2.9. Manage User Profile

The following steps provision the subscribers on ANS.

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



Manage User Profile

You can manage (add, edit & delete) user profile here

Please search based on User Id, First Name or Last Name.

Search Value:

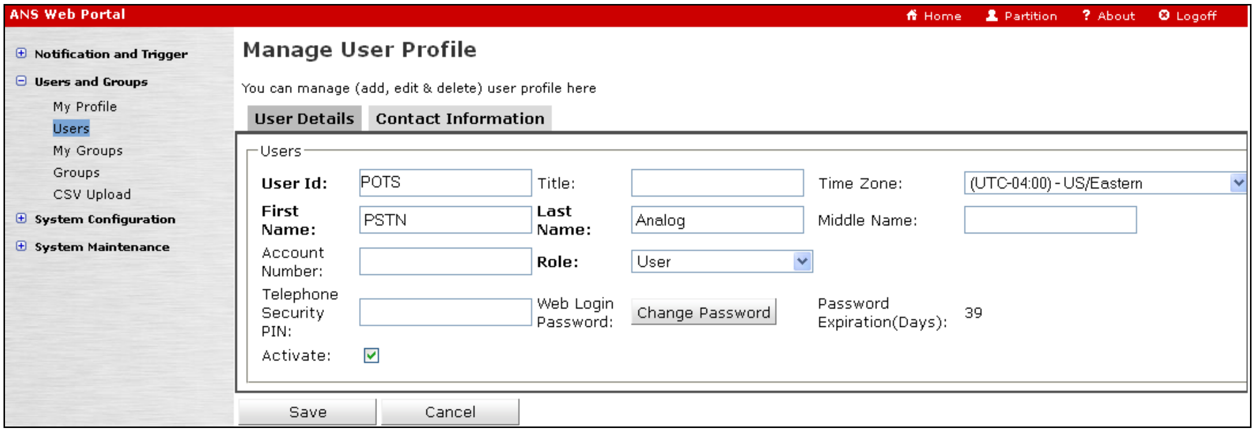
Role: Select Active Ignore

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

Rows Per Page 10 1 - 8(8)

Step 2 - On the subsequent screen, select the **User Details** tab and configure as follows:

- **User Id** – Enter any valid id (e.g., **POTS**).
- **Time Zone** – Enter a valid timezone (e.g., **US/Eastern**).
- **First Name** – Enter any string (e.g., **PSTN**).
- **Last Name** – Enter any string (e.g., **Analog**).
- Use default values for the remaining fields.



Manage User Profile

You can manage (add, edit & delete) user profile here

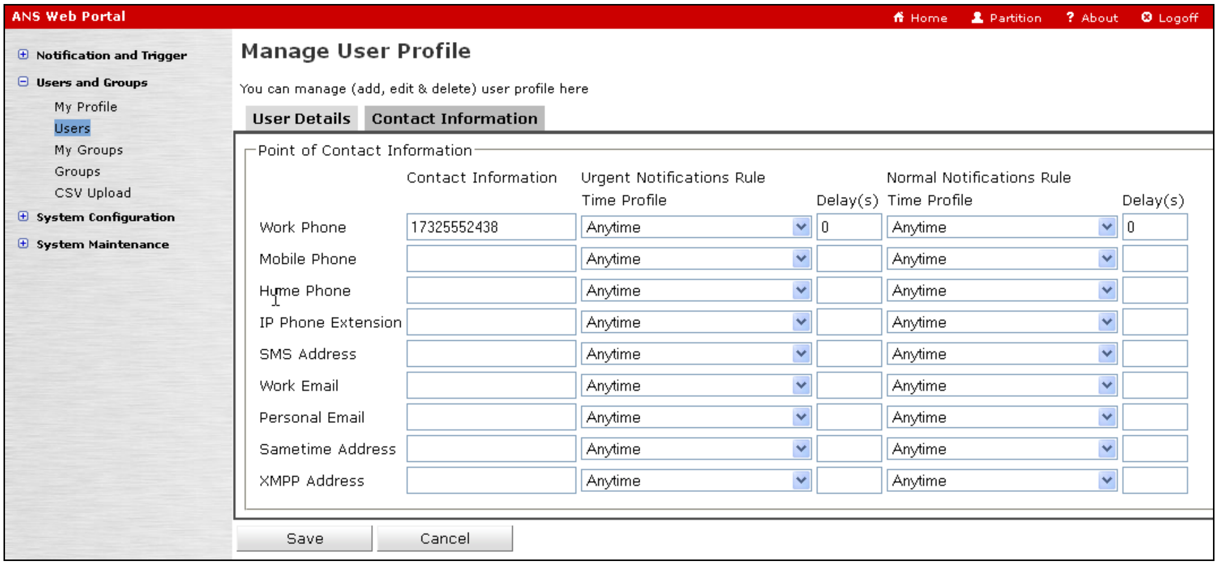
Users

User Id:	POTS	Title:		Time Zone:	(UTC-04:00) - US/Eastern
First Name:	PSTN	**Last Name:**	Analog	Middle Name:	
Account Number:		**Role:**	User		
Telephone Security PIN:		Web Login Password:	Change Password	Password Expiration(Days):	39
Activate:	☑				

Step 4 - Select the **Contact Information** tab and enter valid contact information for this user. In the example below a **Work Phone** number has been defined.

Note – If multiple are entered and the notifications will be simultaneously sent to all the contacts.

Step 5 - Click **Save**.



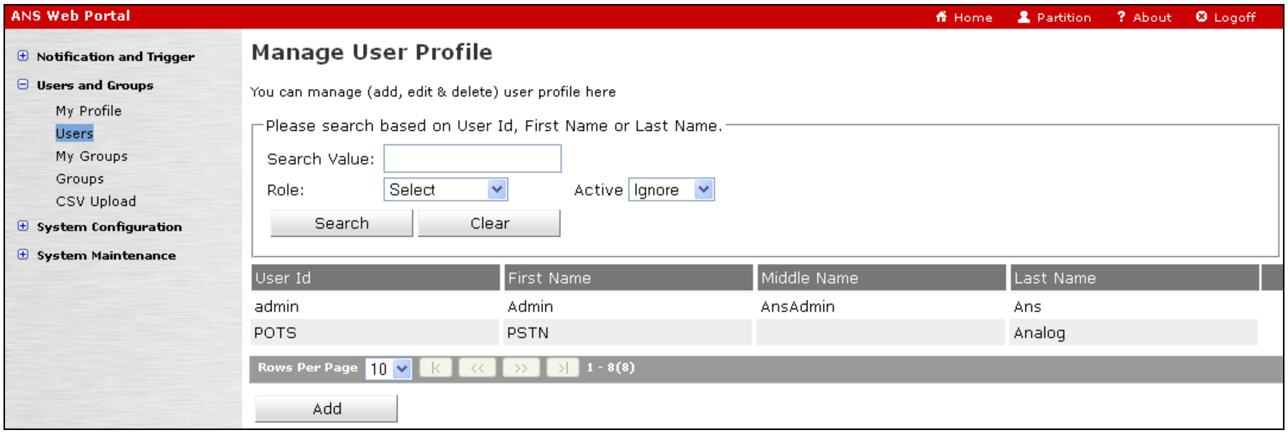
Manage User Profile

You can manage (add, edit & delete) user profile here

Point of Contact Information

	Contact Information	Urgent Notifications Rule Time Profile	Delay(s)	Normal Notifications Rule Time Profile	Delay(s)
Work Phone	17325552438	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	

Step 5 - Repeat **Steps 1-5** for any additional users.



Manage User Profile

You can manage (add, edit & delete) user profile here

Please search based on User Id, First Name or Last Name.

Search Value:

Role: Select

Active Ignore

User Id	First Name	Middle Name	Last Name
admin	Admin	AnsAdmin	Ans
POTS	PSTN		Analog

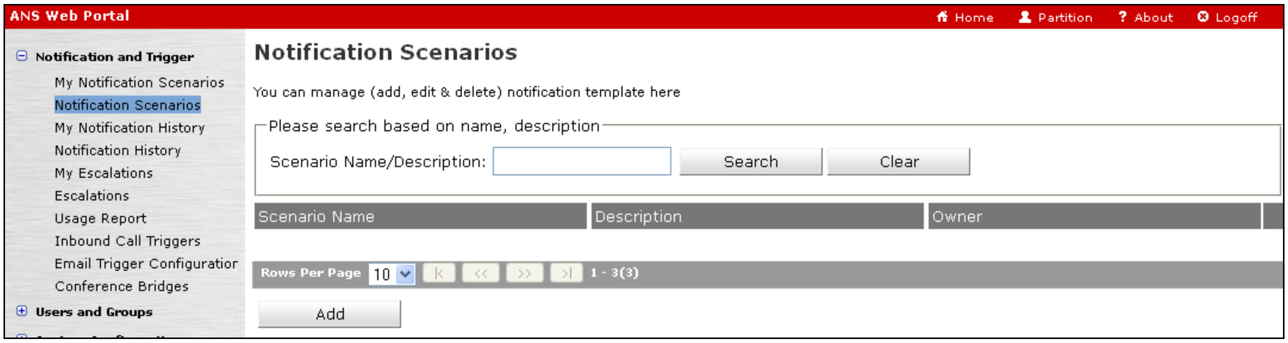
Rows Per Page 10

6.2.10. Outbound Notifications

The following sections show the configuration of an ANS outbound notification and an ANS Ad-Hoc conference, to selected subscribers.

6.2.10.1 Outbound Notification

Step 1 - In the left pane, navigate to **Notifications and Trigger → Notifications Scenarios** and click **Add**.



Notification Scenarios

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

Please search based on name, description

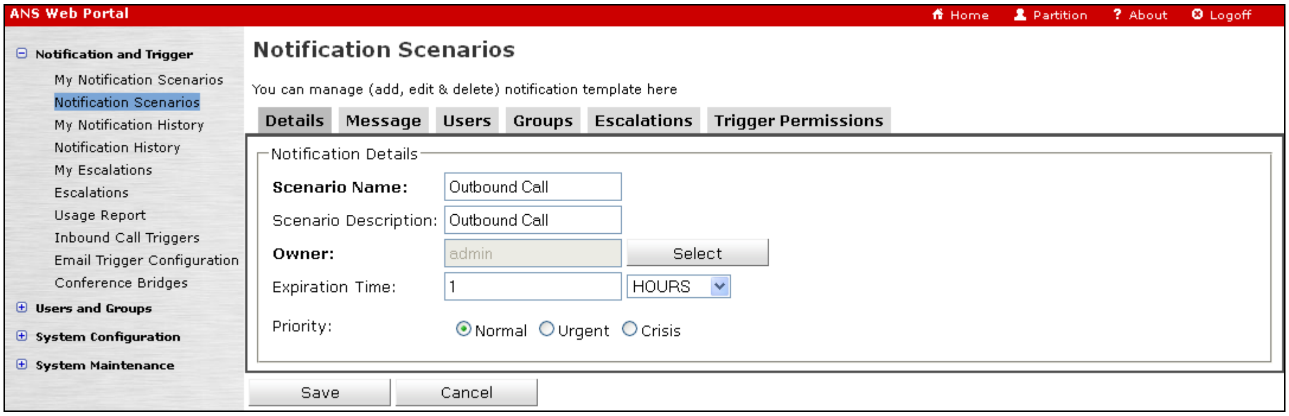
Scenario Name/Description:

Scenario Name	Description	Owner

Rows Per Page 10

Step 2 – The **Notification Scenarios** window will open. Select the **Details** tab and populate the fields as follows:

- **Scenario Name** – Enter a name for the scenario (e.g., **Outbound Call**).
- **Scenario Description** – Fill in a description if desired.
- **Owner** – Use the default **admin**.
- **Expiration Time** – This is the amount of time ANS will attempt to deliver the notification before abandoning the attempt. Set as desired (**1 Hour** is the default).
- **Priority** – Set as appropriate.



Notification Scenarios

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

Notification Details

Scenario Name: Outbound Call

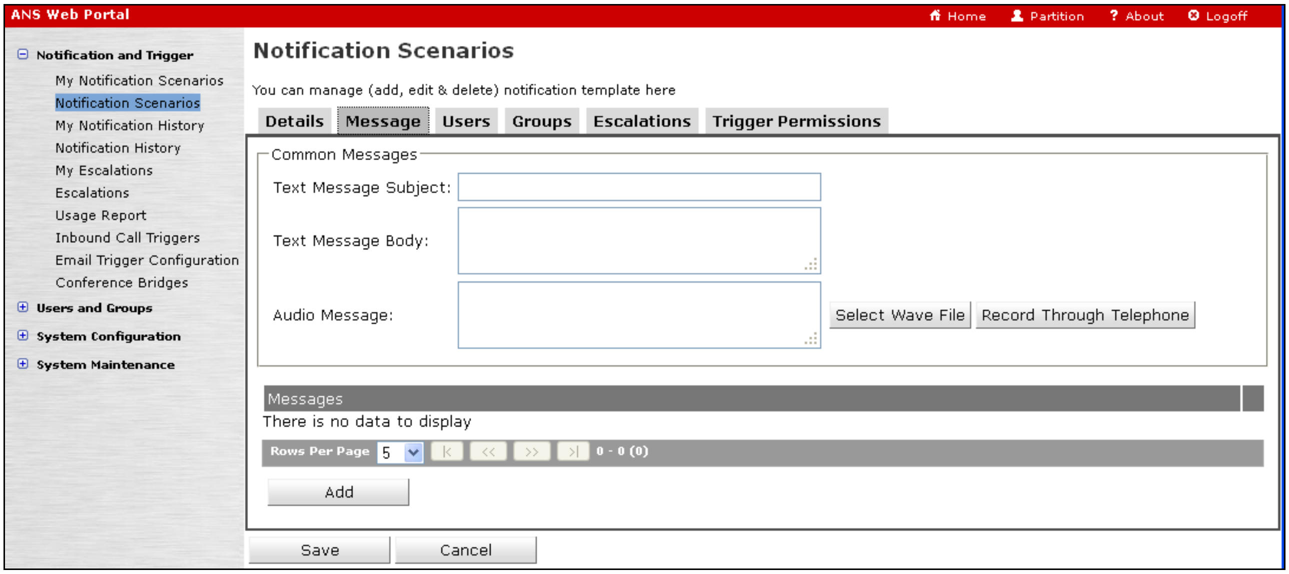
Scenario Description: Outbound Call

Owner: admin

Expiration Time: 1 HOURS

Priority: ● Normal ○ Urgent ○ Crisis

Step 3 – Select the **Message** tab and click on **Add** and enter the following:



Notification Scenarios

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

Common Messages

Text Message Subject:

Text Message Body:

Audio Message:

Messages

There is no data to display

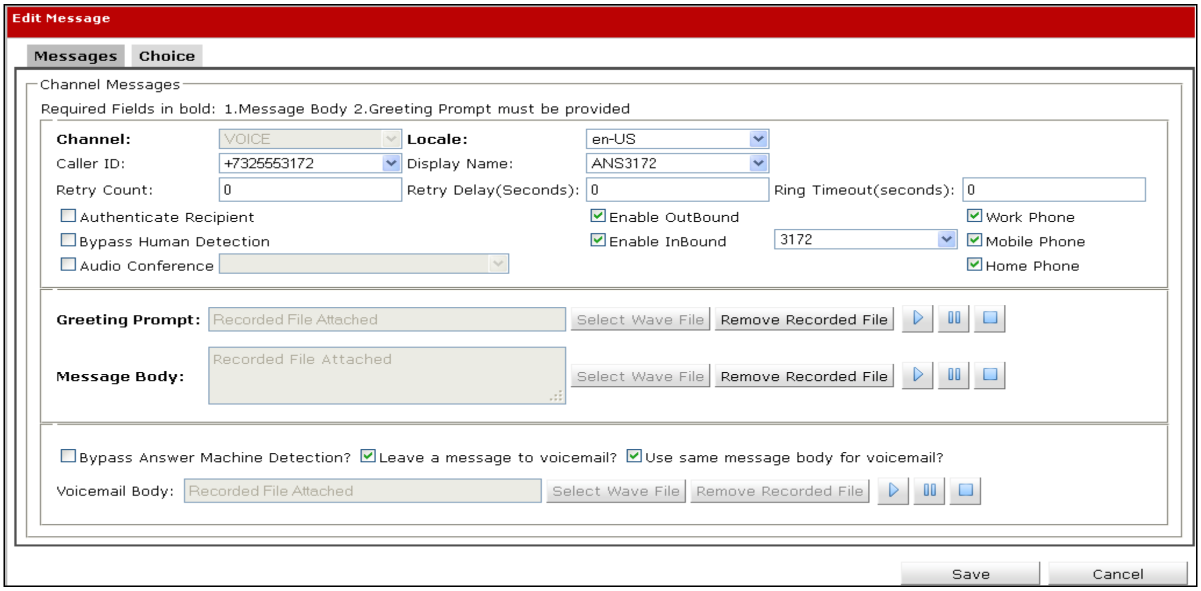
Step 4 – The **Add New Message** window will open. Select the **Messages** tab and enter the following:

- **Channel** – Select **VOICE** from the drop-down list.
- **Caller ID** – Select the number configured in **Section 6.2.4**, **Step 2** (e.g., **+7325553172**).
- **Locale –** Set as appropriate.
- **Display Name** - Select the name configured in **Section 6.2.4, Step 5** (e.g., **ANS3172**).
- **Enable Inbound** – This field is enabled only if the notification needs to be saved in an ANS Message Inbox configured in **Section 6.2.8**, so subscribers may retrieve the message later (e.g., **3172**).
- Select how the subscriber will be contacted from **Work Phone**, **Mobile Phone**, and **Home Phone options** as appropriate.
- **Greeting Prompt –** A greeting message is played to the subscriber when the call is answered. If Loquendo has been licensed, then enter the message in the text field. Loquendo

will convert it to speech. Alternatively, click on the **Select Wave File** or **Record Through Telephone** button.

Note - In the reference configuration, the **Record Through Telephone** option was used for all notification messages. See **Section 6.2.10.3** for the **Record Through Telephone** procedure.

- **Message Body –** Repeat the process used for the **Greeting Prompt** above to generate the notification message.
- **Leave a message to voicemail –** Check this so that the message can be left on the subscriber's voicemail in case the subscriber is unavailable.
- **Use same message body for voicemail –** Check this if the **Voicemail Body** message is same as the **Message Body**. Otherwise create a new message. In this reference configuration, this field is checked.
- Use the default values for the remaining fields.
- **Step 5 –** Click on **Save**, and the **Add New Message** window will close.



Edit 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: +7325553172 Display Name: ANS3172

Retry Count: 0 Retry Delay(Seconds): 0 Ring Timeout(seconds): 0

□ Authenticate Recipient ☑ Enable OutBound ☑ Work Phone

□ Bypass Human Detection ☑ Enable InBound 3172 ☑ Mobile Phone

□ Audio Conference ☑ Home Phone

Greeting Prompt: Recorded File Attached | Select Wave File | Remove Recorded File

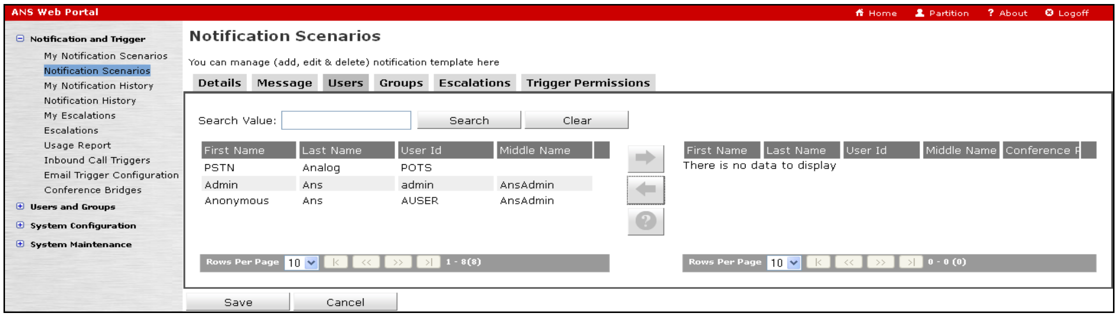
Message Body: Recorded File Attached | Select Wave File | Remove Recorded File

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

Voicemail Body: Recorded File Attached | Select Wave File | Remove Recorded File

Save | Cancel

Step 6 – Returning to the **Notifications Scenario** window, click on the **Users** tab.



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
PSTN	Analog	POTS	
Admin	Ans	admin	AnsAdmin
Anonymous	Ans	AUSER	AnsAdmin

Rows Per Page 10 1 - 8(8)

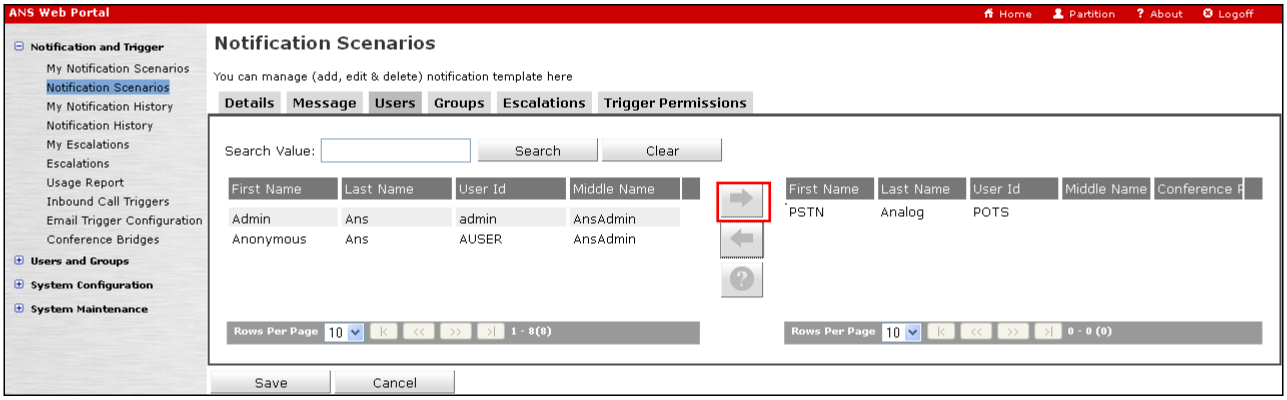
First Name	Last Name	User Id	Middle Name	Conference F

There is no data to display

Rows Per Page 10 0 - 0 (0)

Save | Cancel

Step 7 – From the list of users, click on the PSTN user created in **Section 6.2.9** (e.g., **PSTN**). Then using the right arrow button, move the user into the right hand column. ANS will send this notification to any user listed in this column. Click on **Save**.



Notification Scenarios

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

Search Value:

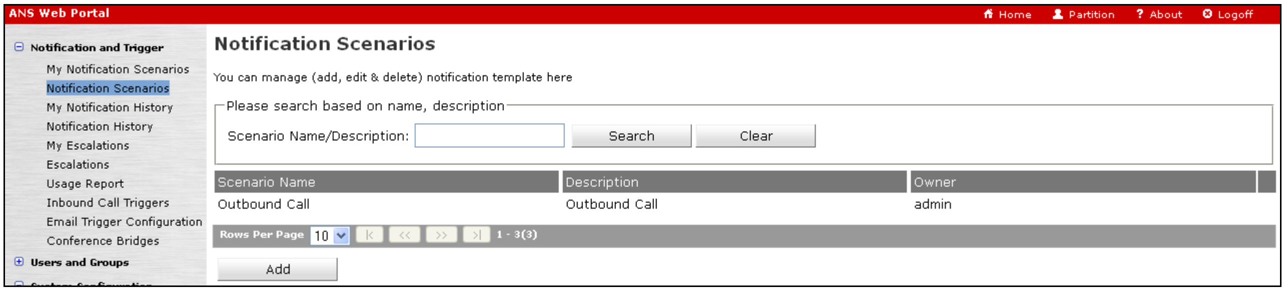
First Name	Last Name	User Id	Middle Name
Admin	Ans	admin	AnsAdmin
Anonymous	Ans	AUSER	AnsAdmin

Rows Per Page 10 1 - 8(8)

First Name	Last Name	User Id	Middle Name	Conference F
PSTN	Analog	POTS		

Rows Per Page 10 0 - 0 (0)

The **Outbound Call** scenario is created.



Notification Scenarios

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

Please search based on name, description

Scenario Name/Description:

Scenario Name	Description	Owner
Outbound Call	Outbound Call	admin

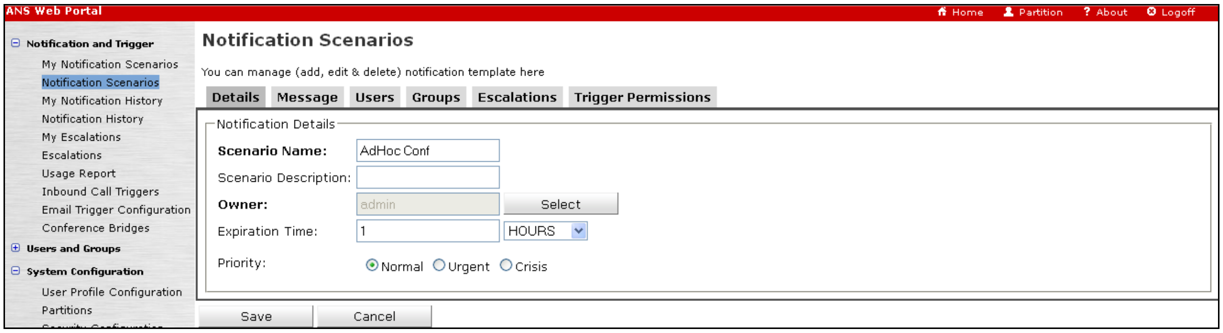
Rows Per Page 10 1 - 3(3)

6.2.10.2 Ad–Hoc Conference Notification

ANS may be configured to call out to subscribers and ask them to join an Ad-Hoc conference hosted by ANS.

Step 1 – The Ad-Hoc Conference notification scenario is created in a similar fashion to the notification scenario shown in **Section 6.2.10.1**. Repeat the steps shown in that section, with the following differences:

- In **Section 6.2.10.1**, **Step 2**,
    - **Scenario Name** – Enter a name for the scenario (e.g., **AdHoc Conf**).



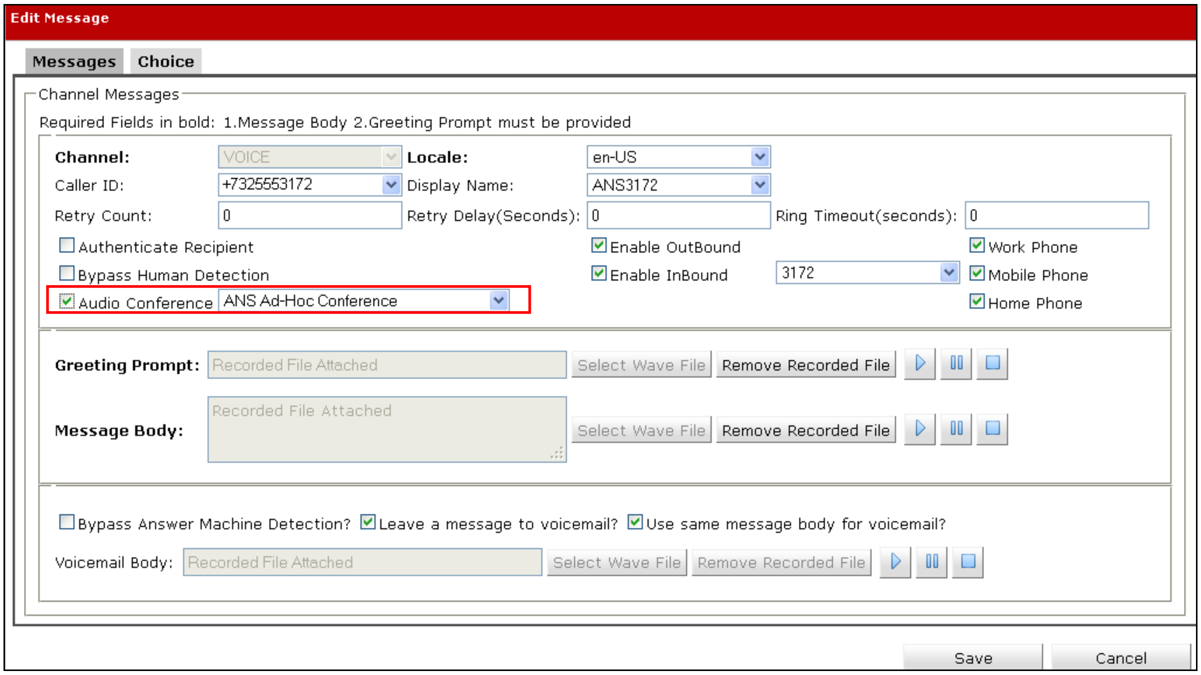
Notification Scenarios

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

Notification Details

Scenario Name:	AdHoc Conf
Scenario Description:	
Owner:	admin
Expiration Time:	1 HOURS
Priority:	● Normal ○ Urgent ○ Crisis

- In **Section 6.2.10.1**, **Step 4**,
    - Check the **Audio Conference** box and select **Ad-Hoc Conference** from the drop-down menu.



Edit 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: +7325553172 Display Name: ANS3172

Retry Count: 0 Retry Delay(Seconds): 0 Ring Timeout(seconds): 0

□ Authenticate Recipient ☑ Enable OutBound ☑ Work Phone

□ Bypass Human Detection ☑ Enable InBound 3172 ☑ Mobile Phone

☑ Audio Conference ANS Ad-Hoc Conference ☑ Home Phone

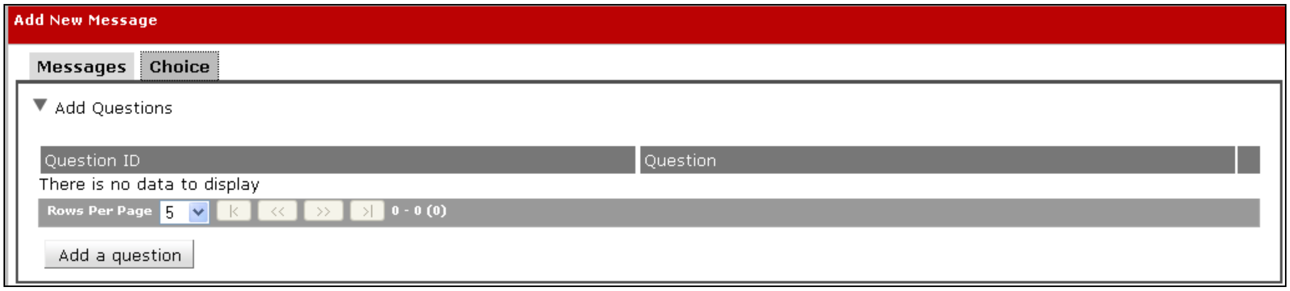
Greeting Prompt: Recorded File Attached

Message Body: Recorded File Attached

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

Voicemail Body: Recorded File Attached

Step 2 – Select the **Choice** tab, and click the **Add a question** button.



Add New Message

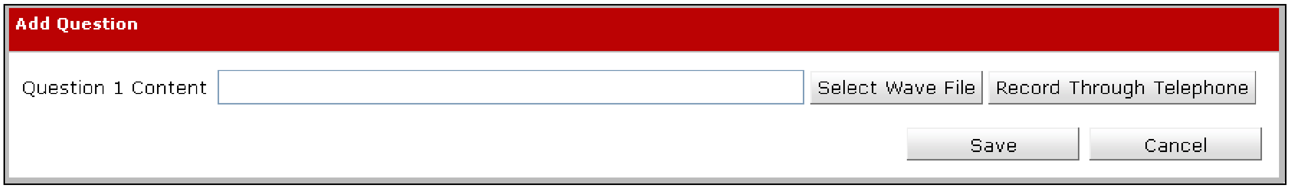
Messages | Choice

▼ Add Questions

Question ID	Question
There is no data to display	

Rows Per Page 5 0 - 0 (0)

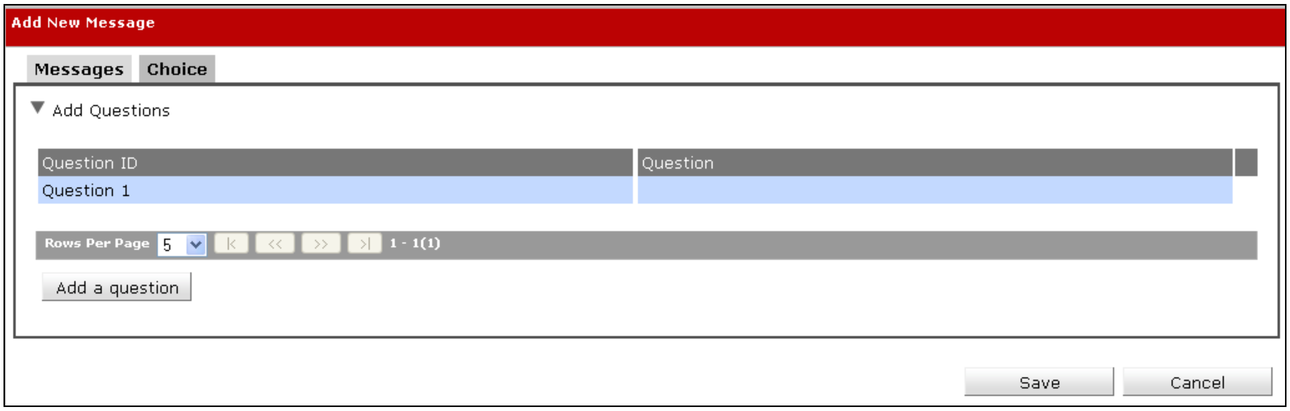
Step 3 – The **Add Question** window will open. Following the procedure in **Section 6.2.10.1**, **Step 4**, create a question for the caller (e.g., “Would you like to join the conference call?”), and click **Save**.



Add Question

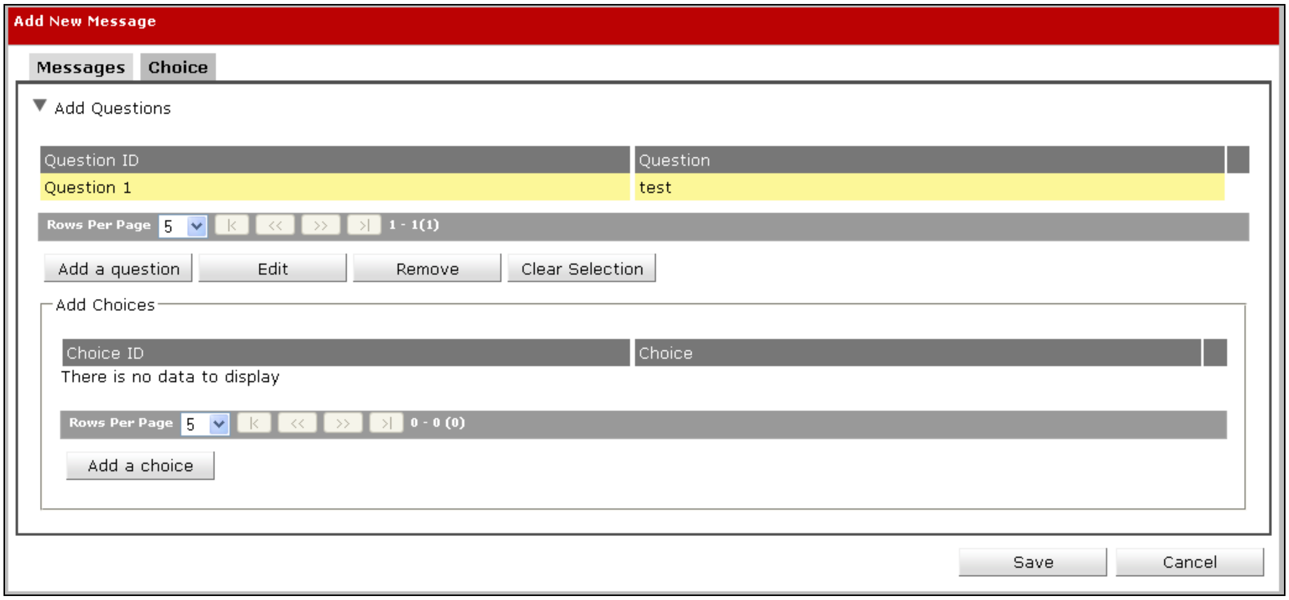
Question 1 Content

Step 4 – Returning to the **Add New Message** window, click on the question entry created in **Step 3** (e.g., **Question 1**).



Question ID	Question
Question 1	

Step 5 – The **Add Choices** section will open. Click **Add a choice.**



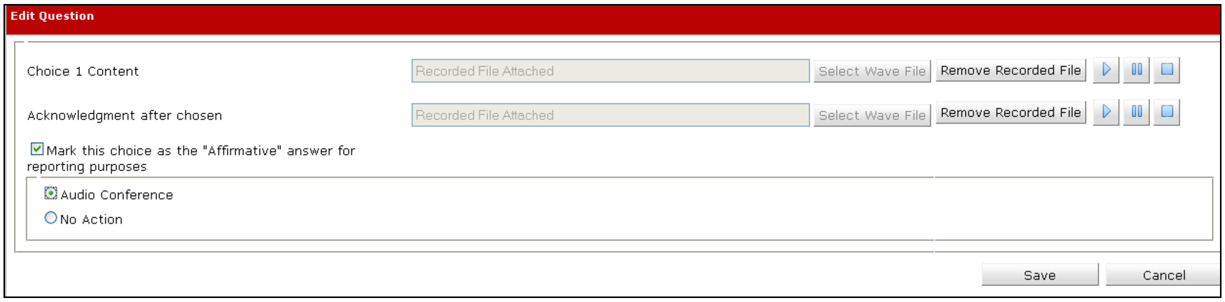
Question ID	Question
Question 1	test

Choice ID	Choice

There is no data to display

Step 6 - The **Add Question window will open.** Enter the following:

- **Choice 1 Content -** Following the procedure in **Section 6.2.10.1**, **Step 4**, create a choice for the caller (e.g., "Press 1 for yes.").
- **Acknowledgment after chose** – Following the procedure in **Section 6.2.10.1**, **Step 4**, create a response for the caller (e.g., "You are joining the conference.").
- Check the **Mark this choice as the "Affirmative" answer for reporting purposes** box.
- **Audio Conference** – Select this option.
- Click **Save**.



Edit Question

Choice 1 Content: Recorded File Attached

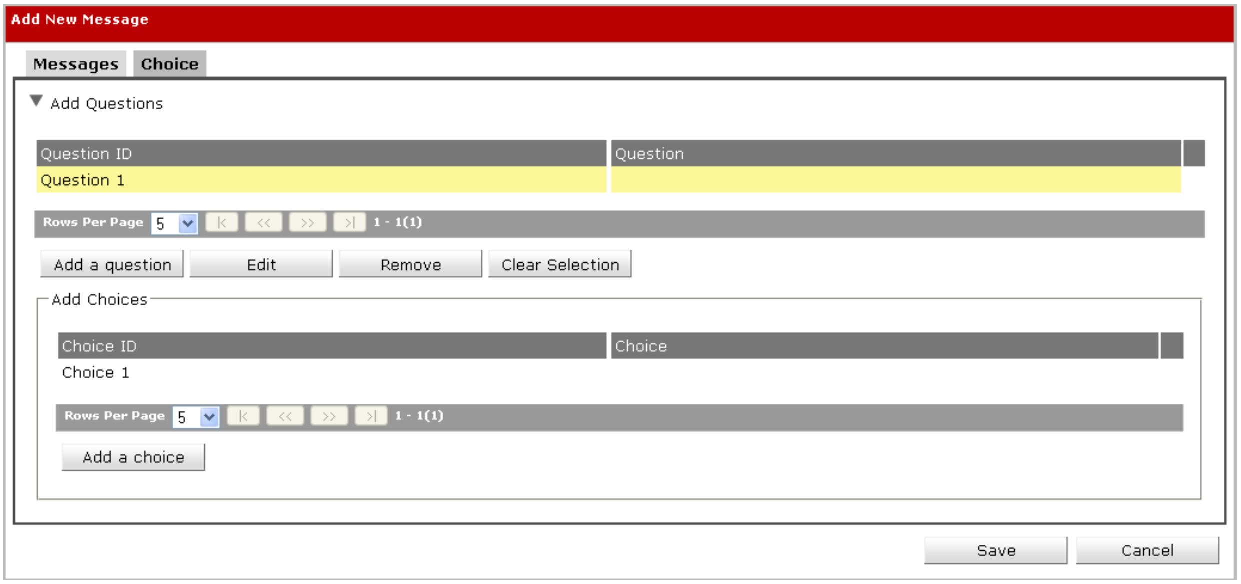
Acknowledgment after chosen: Recorded File Attached

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

● Audio Conference

○ No Action

Step 7 – Returning to the **Add New Message** window, additional choices may be added. Otherwise click on **Save**.



Add New Message

Add Questions

Question ID	Question
Question 1	

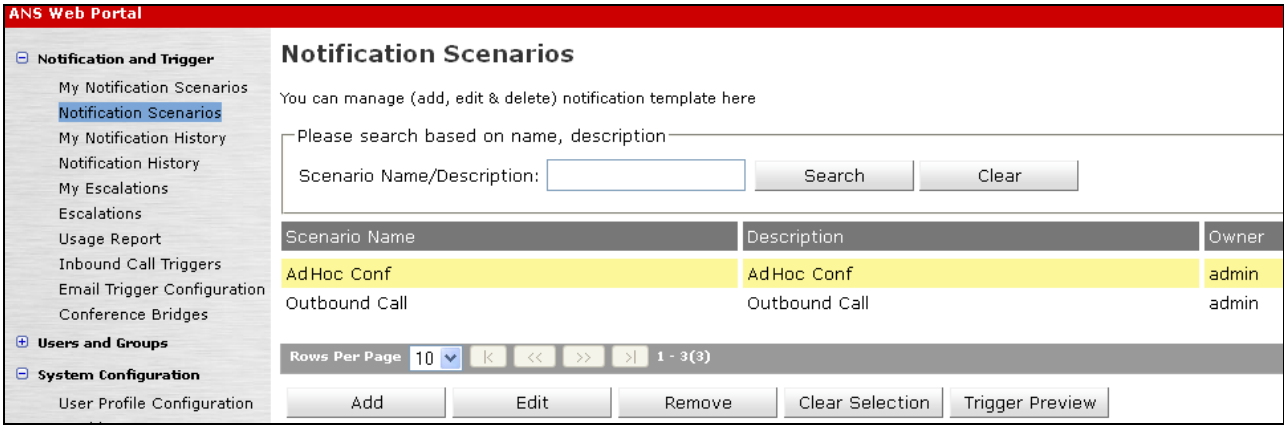
Rows Per Page 5 1 - 1(1)

Add Choices

Choice ID	Choice
Choice 1	

Rows Per Page 5 1 - 1(1)

Step 8 – Returning to the **Notifications Scenario** window, click on the **Users** tab and repeat the procedures in **Section 6.2.10.1**, **Steps 6** & **7**. The **Ad Hoc Conf** notification is created.



ANS Web Portal

Notification Scenarios

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

Please search based on name, description

Scenario Name/Description:

Scenario Name	Description	Owner
AdHoc Conf	AdHoc Conf	admin
Outbound Call	Outbound Call	admin

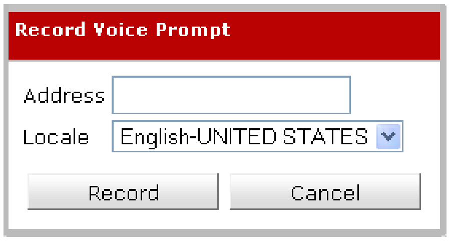
Rows Per Page 10 1 - 3(3)

6.2.10.3 Recording Notification Announcements via a Telephone

As described in **Section 6.2.10.1, Step 4**, by selecting the **Record Through Telephone** button, ANS announcements may be recorded via telephone. ANS calls out to the designated telephone number or local PBX extension to create the recording.

> **Note** – In the reference configuration, ANS calls are routed via Session Manager. Therefore, these numbers must be routable by Session Manager.

When the **Record Through Telephone** button is selected on one of the announcement windows, the **Record Voice Prompt** window is displayed.



Record Voice Prompt

Address:

Locale: English-UNITED STATES

Enter a telephone number or local PBX extension in the **Address** field, and click the **Record** button. ANS will call the specified number. ANS will prompt the caller through the recording process.

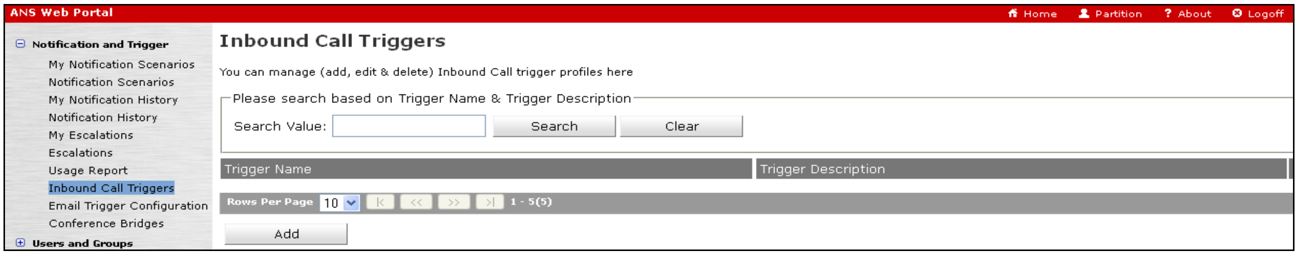
When the recoding is completed, ANS will close the **Record Voice Prompt** window, and the Record Through Telephone button on the associated announcement window, is replaced by Remove Recorded File ▷ ▯▯ □

6.2.11. Triggering Notifications

ANS notification scenarios may be initiated (triggered), via an inbound call to ANS, or locally from the ANS web portal.

6.2.11.1 Defining an Inbound Call Trigger

Step 1 - Navigate to **System Configuration→Inbound Call Trigger** and click **Add**.



Inbound Call Triggers

You can manage (add, edit & delete) Inbound Call trigger profiles here

Please search based on Trigger Name & Trigger Description

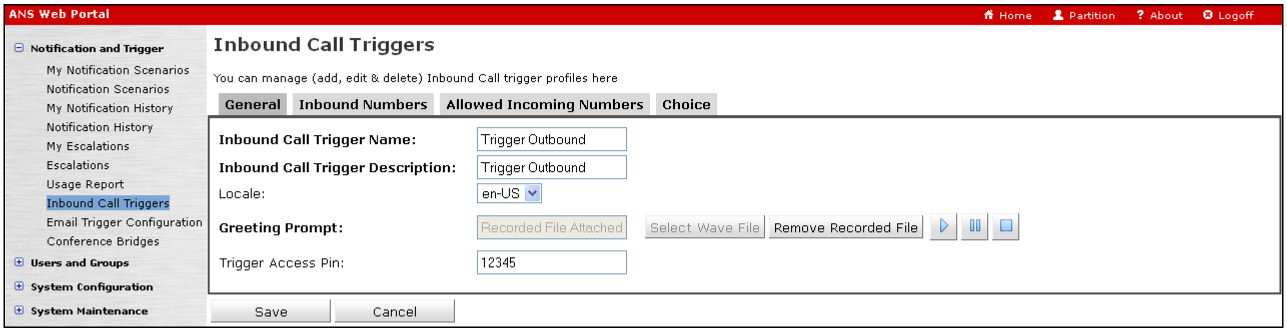
Search Value:

Trigger Name	Trigger Description

Rows Per Page 10 1 - 5(5)

Step 2 – The **Inbound Call Trigger** window will open. From the **General** tab, enter the following:

- **Inbound Call Trigger Name** – Enter a name for the trigger.
- **Inbound Call Trigger Description** – Enter a description if desired.
- **Locale** – Select as appropriate.
- **Greeting Prompt** – Enter/Record an ANS greeting (see **Sections 6.2.10.1 and 6.2.10.3**).
- **Trigger Access Pin** – Optionally, an access PIN may be provisioned to challenge the caller**.**



Inbound Call Triggers

You can manage (add, edit & delete) Inbound Call trigger profiles here

Inbound Call Trigger Name: Trigger Outbound

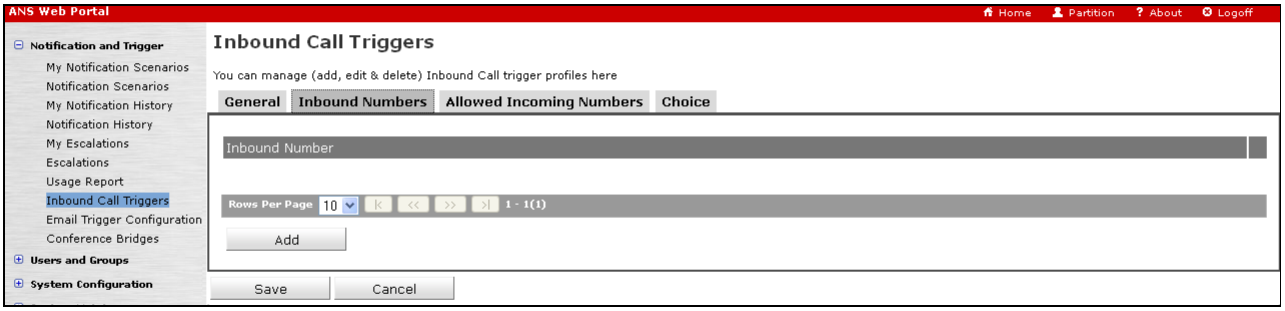
Inbound Call Trigger Description: Trigger Outbound

Locale: en-US

Greeting Prompt: Recorded File Attached

Trigger Access Pin: 12345

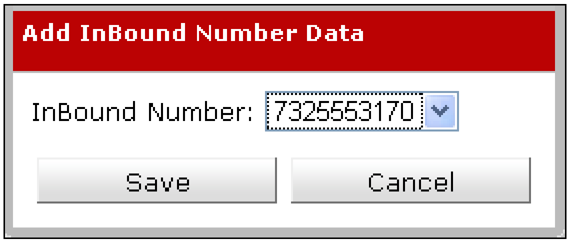
Step 3 – Select the **Inbound Numbers** tab, and click on the **Add** button.



Inbound Call Triggers

You can manage (add, edit & delete) Inbound Call trigger profiles here

Step 4 – The **Add Inbound Number Data** window will open. From the drop-down menu select from one of the inbound numbers defined in **Section 6.2.7** (e.g., **7325553170**). Click on **Save**.

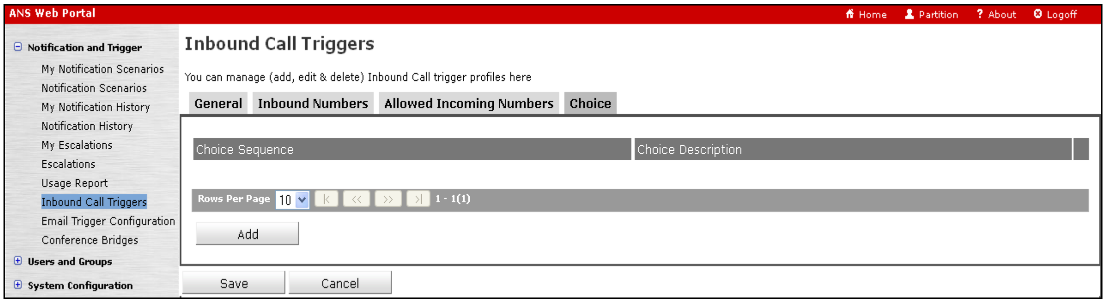


Add InBound Number Data

InBound Number: 7325553170

Note – Once an inbound number is selected for a trigger, that number is removed from the drop-down menu selection.

Step 5 – Returning to the Inbound **Call Triggers** page, select the **Choice** tab, and click **Add**.



Inbound Call Triggers

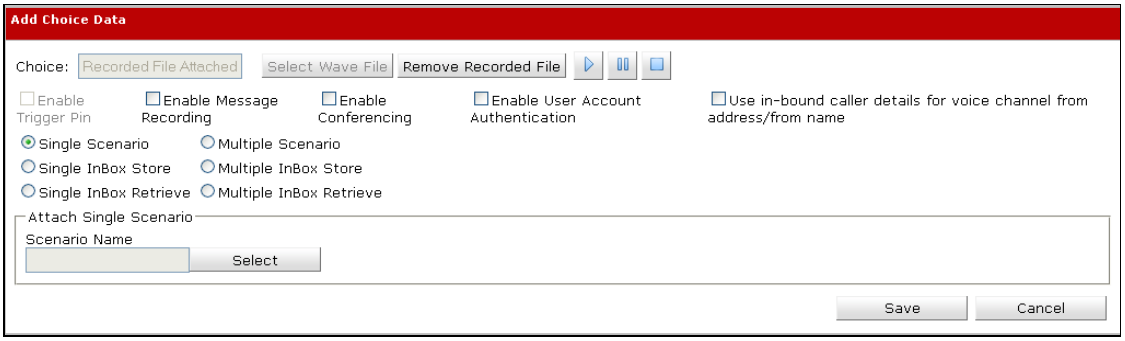
You can manage (add, edit & delete) Inbound Call trigger profiles here

Choice Sequence	Choice Description

Rows Per Page: 10

Step 6 – The **Add Choice Data** window will open. Enter the following:

- **Choice** – Create an announcement that ANS will play to the caller. See **Sections 6.2.10.1** and **6.2.10.3** regarding announcement creation**.**
- Select the **Single Scenario** option**.**
- In the **Attach Single Scenario** section, click on the **Select** button.



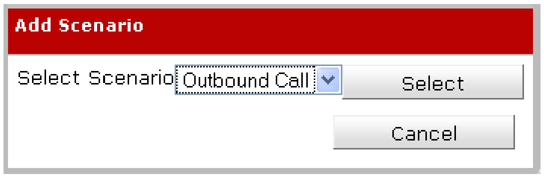
Choice: Recorded File Attached

□ Enable Trigger Pin
□ Enable Message Recording
□ Enable Conferencing
□ Enable User Account Authentication
□ Use in-bound caller details for voice channel from address/from name

● Single Scenario
○ Multiple Scenario
○ Single InBox Store
○ Multiple InBox Store
○ Single InBox Retrieve
○ Multiple InBox Retrieve

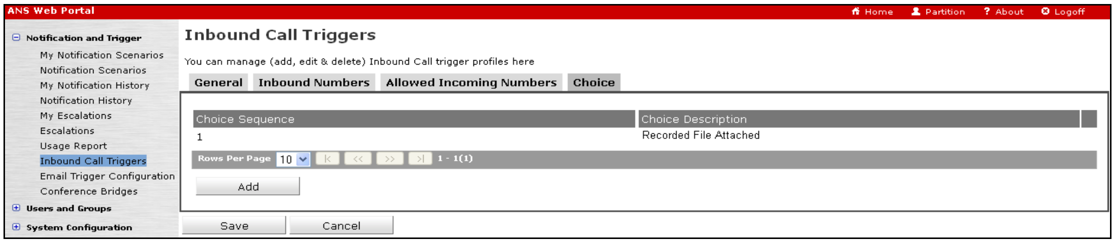
Scenario Name:

Step 7 – The **Add Scenario** window will open. From the drop-down menu, select a scenario created in **Section 6.2.10** (e.g., **Outbound Call**), then click on **Select**.



Select Scenario: Outbound Call

Step 8 – Returning to the Inbound **Call Triggers** window, select **Save.**



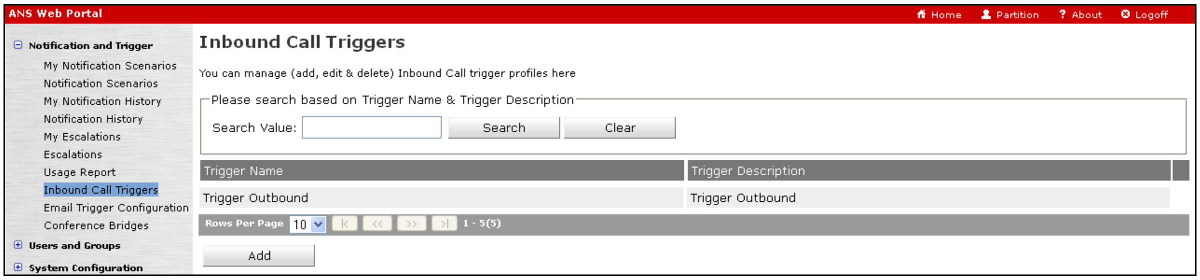
Inbound Call Triggers

You can manage (add, edit & delete) Inbound Call trigger profiles here

Choice Sequence	Choice Description
1	Recorded File Attached

Rows Per Page: 10

The inbound call trigger for the **Outbound Call** notification is created. Repeat **Steps 1-8** to create additional inbound call triggers.



Inbound Call Triggers

You can manage (add, edit & delete) Inbound Call trigger profiles here

Please search based on Trigger Name & Trigger Description

Search Value:

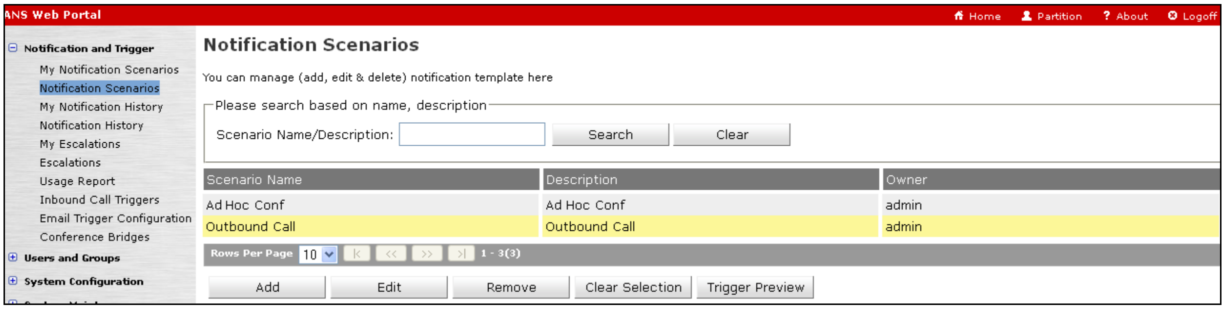
Trigger Name	Trigger Description
Trigger Outbound	Trigger Outbound

Rows Per Page 10 1 - 5(5)

6.2.11.2 Triggering a notification from Avaya Notification Solution

Step 1 - In the left pane, navigate to **Notifications and Trigger → Notifications Scenarios** and select a notification created in **Section 6.2.10** (e.g., **Outbound Call**).

Step 2 – Click on the **Trigger Preview** button.



Notification Scenarios

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

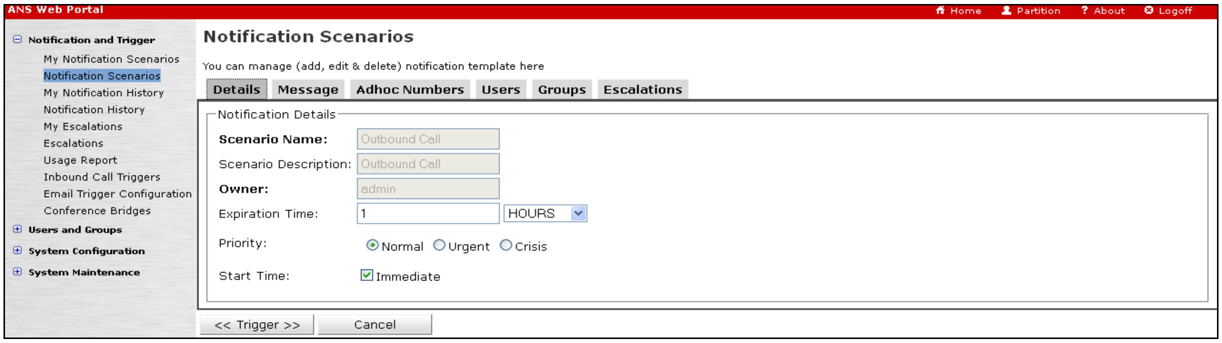
Please search based on name, description

Scenario Name/Description:

Scenario Name	Description	Owner
Ad Hoc Conf	Ad Hoc Conf	admin
Outbound Call	Outbound Call	admin

Rows Per Page 10 1 - 3(3)

Step 3 – The **Trigger Preview** window will open. Click on the **Trigger** button, and ANS will send the notification call to the subscribers configured in **Section 6.2.10.1, Steps 6** & **7**.



Notification Scenarios

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

Notification Details

Scenario Name: Outbound Call

Scenario Description: Outbound Call

Owner: admin

Expiration Time: 1 HOURS

Priority: ● Normal ○ Urgent ○ Crisis

Start Time: ☑ Immediate

7. Configure Avaya Session Border Controller for Enterprise

Note: Only the Avaya SBCE provisioning required for the reference configuration is described in these Application Notes. The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document. Refer to **[5 & 6]** for additional information.

7.1. Initial Installation/Provisioning

IMPORTANT! – During the Avaya SBCE installation, the Management interface of the Avaya SBCE must be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1). If this is not the case, contact your Avaya representative to get this condition resolved.

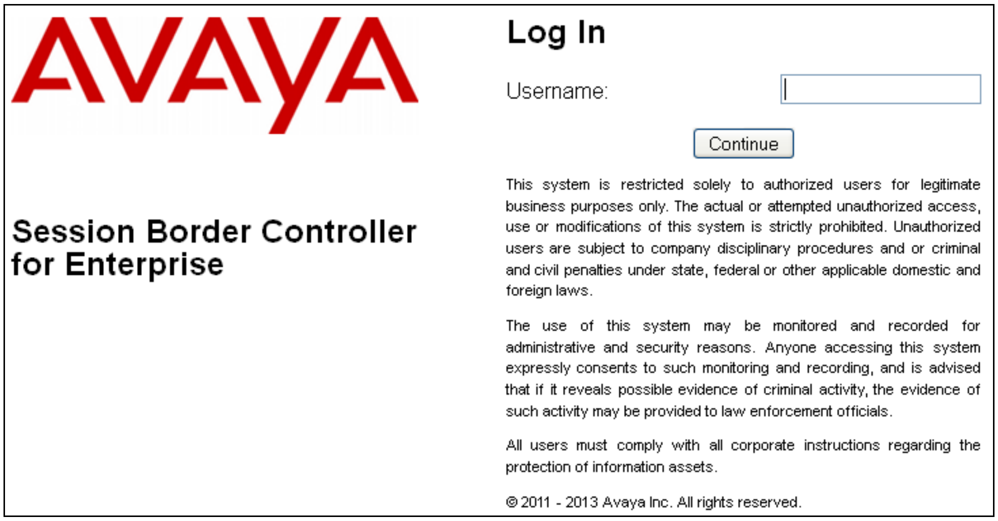
As described in **Section 3.1**, the reference configuration places the private interface (A1) of the Avaya SBCE in its own subnet (Common site, 192.168.70.x), with access to the Main site (192.168.67.x) subnet. The connection to AT&T uses the Avaya SBCE public interface B1 (IP address 10.10.10.12[1]).

7.2. Log into the Avaya SBCE

The follow provisioning is performed via the Avaya SBCE GUI interface, using the "M1" management LAN connection on the chassis.

Step 1 - Access the web interface by typing "**https://x.x.x.x**" (where x.x.x.x is the management IP address of the Avaya SBCE).

Step 2 - Enter the **Username** and click **Continue**.



This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

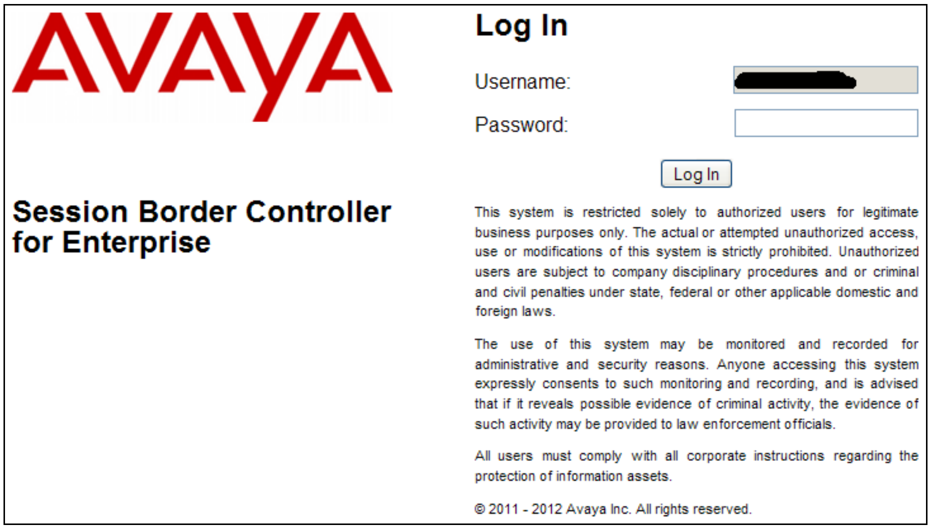
The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2013 Avaya Inc. All rights reserved.

[1] See **Section 3.1**.

Step 3 – Enter the **Password** and click **Log In**.



AVAYA

Session Border Controller for Enterprise

Log In

Username: [redacted]

Password:

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

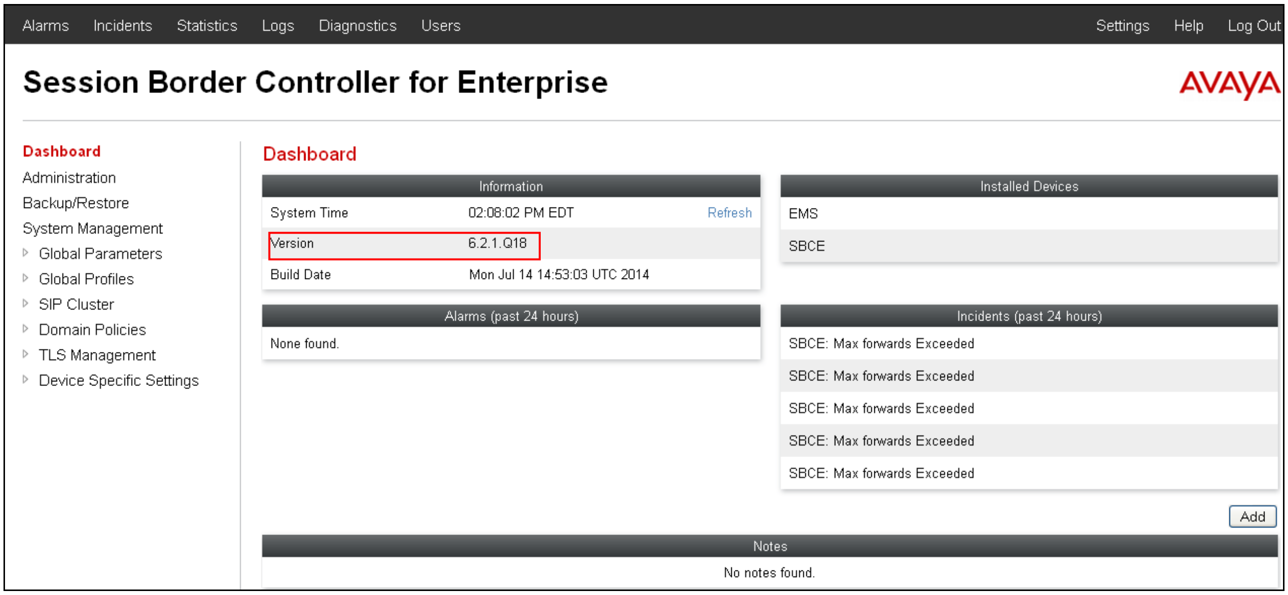
The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2012 Avaya Inc. All rights reserved.

Step 3 - The main menu window will open. Note that the installed software version is displayed.

Note – All page navigation described in the following sections will utilize the menu shown on the left pane of the screenshot below.



Session Border Controller for Enterprise

Dashboard

Information		
System Time	02:08:02 PM EDT	Refresh
Version	6.2.1.Q18	
Build Date	Mon Jul 14 14:53:03 UTC 2014	

Installed Devices
EMS
SBCE

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
SBCE: Max forwards Exceeded
SBCE: Max forwards Exceeded
SBCE: Max forwards Exceeded
SBCE: Max forwards Exceeded
SBCE: Max forwards Exceeded

Notes
No notes found.

7.3. Global Profiles

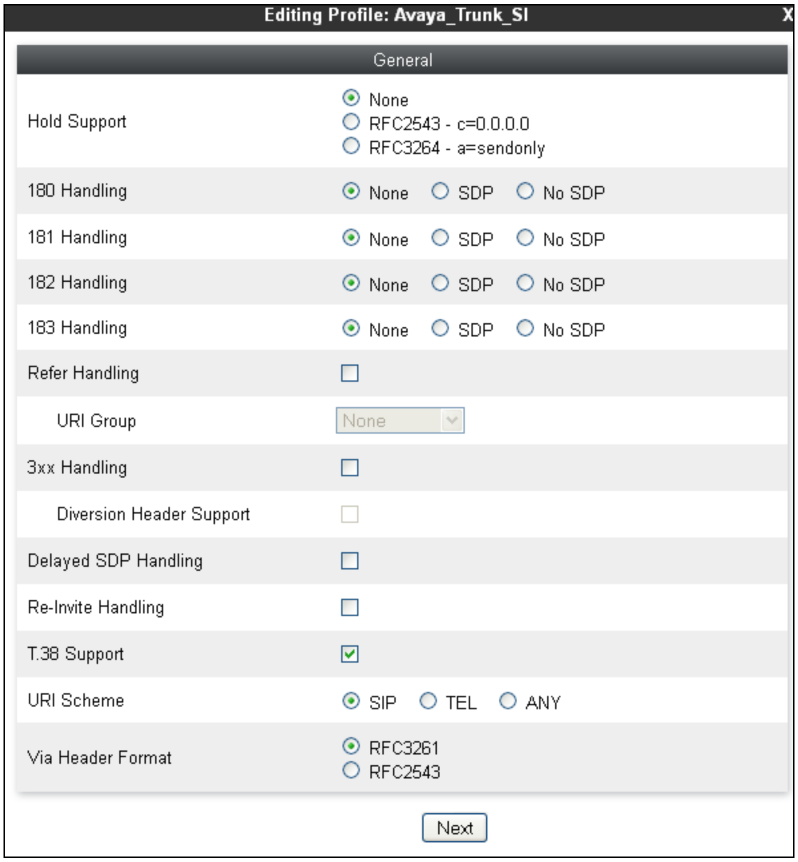
Global Profiles allow for configuration of parameters across the Avaya SBCE appliances.

7.3.1. Server Interworking – Avaya

Server Interworking allows users to configure and manage various SIP call server-specific capabilities.

Step 1 - Select **Global Profiles → Server Interworking** from the left-hand menu (not shown).
Step 2 - Select the default **avaya-ru** profile and click **Clone** button (not shown). The **Profile** name window will open (not shown).
Step 3 - Enter a profile name: (e.g., **Avaya_Trunk_SI**), and click **Next**.
Step 4 - The **General** screen will open.

- Verify that **Hold Support** is **None** (default).
- Set Verify that **Refer Handling** is *not* selected (default), and **URI Group** is set to **None** (default).
- Select **T38 Support**.
- All other options can be left with default values.
- Click **Next**.

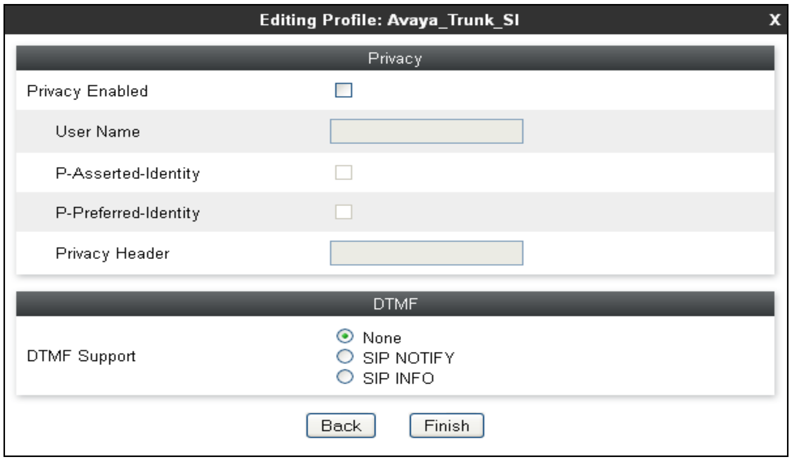


Editing Profile: Avaya_Trunk_SI

General

Hold Support	● None ○ RFC2543 - c=0.0.0.0 ○ RFC3264 - a=sendonly
180 Handling	● None ○ SDP ○ No SDP
181 Handling	● None ○ SDP ○ No SDP
182 Handling	● None ○ SDP ○ No SDP
183 Handling	● None ○ SDP ○ No SDP
Refer Handling	□
URI Group	None
3xx Handling	□
Diversion Header Support	□
Delayed SDP Handling	□
Re-Invite Handling	□
T.38 Support	☑
URI Scheme	● SIP ○ TEL ○ ANY
Via Header Format	● RFC3261 ○ RFC2543

Step 5 - On the **Privacy/DTMF** section select **Finish** to accept default values.



Editing Profile: Avaya_Trunk_SI

Privacy

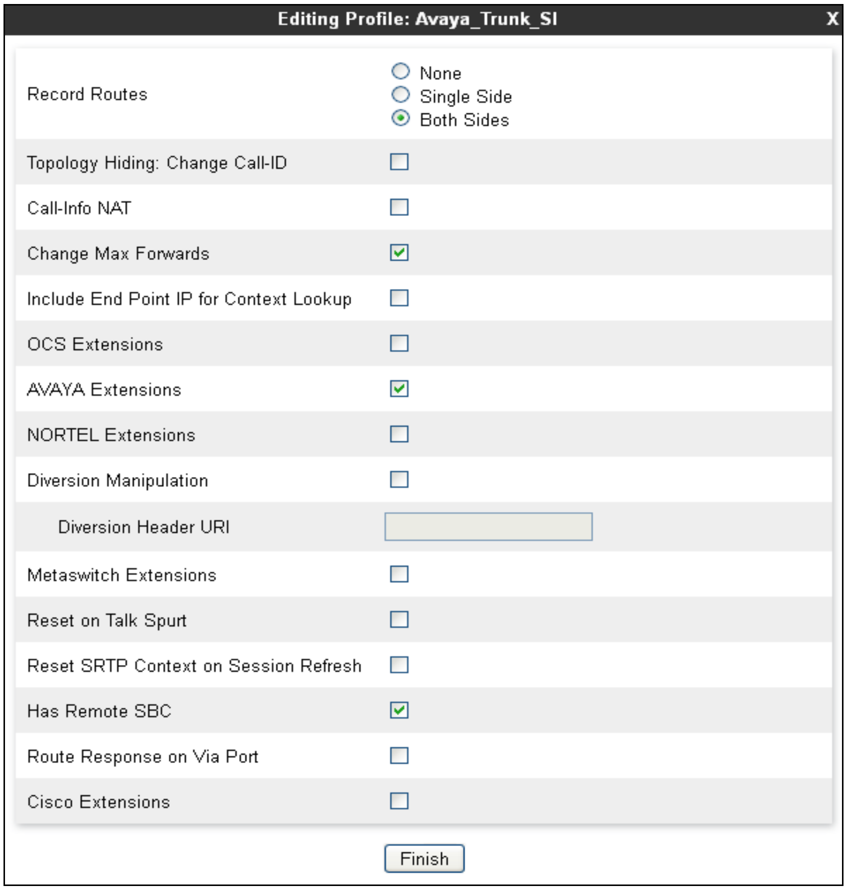
Privacy Enabled	□
User Name	
P-Asserted-Identity	□
P-Preferred-Identity	□
Privacy Header	

DTMF

DTMF Support	● None ○ SIP NOTIFY ○ SIP INFO

Step 6 - On the **SIP Timers/Transport Timers** tabs (not shown) select **Finish** to accept default values.

Step 7 - On the **Advanced** tab, verify the following settings, and click **Finish**.



Editing Profile: Avaya_Trunk_SI

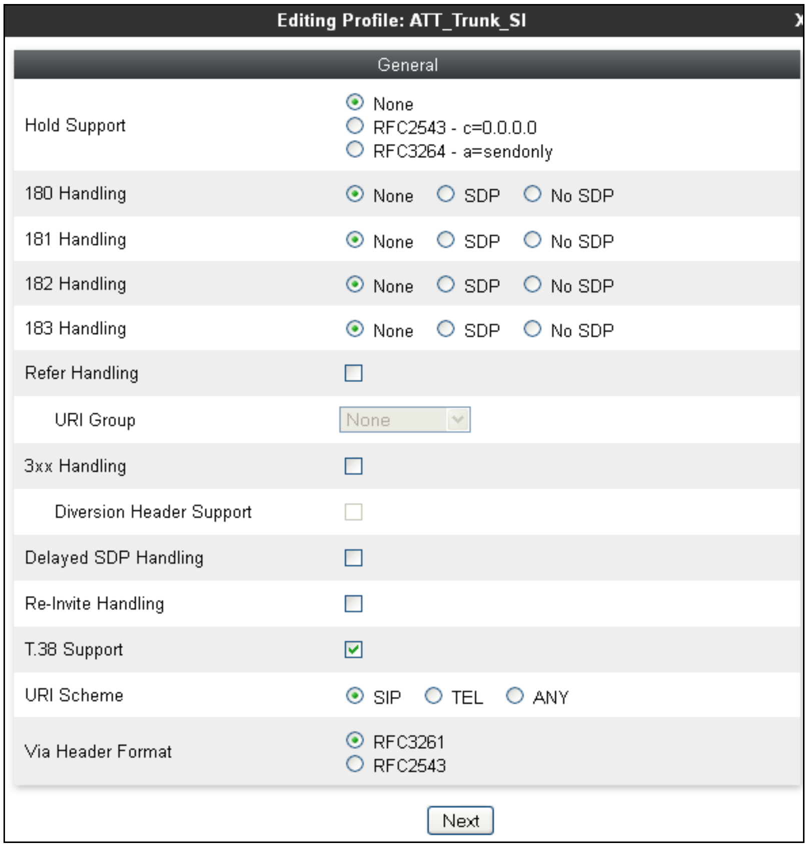
Record Routes	○ None ○ Single Side ● Both Sides
Topology Hiding: Change Call-ID	□
Call-Info NAT	□
Change Max Forwards	☑
Include End Point IP for Context Lookup	□
OCS Extensions	□
AVAYA Extensions	☑
NORTEL Extensions	□
Diversion Manipulation	□
Diversion Header URI	
Metaswitch Extensions	□
Reset on Talk Spurt	□
Reset SRTP Context on Session Refresh	□
Has Remote SBC	☑
Route Response on Via Port	□
Cisco Extensions	□

7.3.2. Server Interworking – AT&T

Add an Interworking Profile for the connection to AT&T via the public network.

Step 1 - Repeat the steps in **Section 7.3.1** with the following changes:

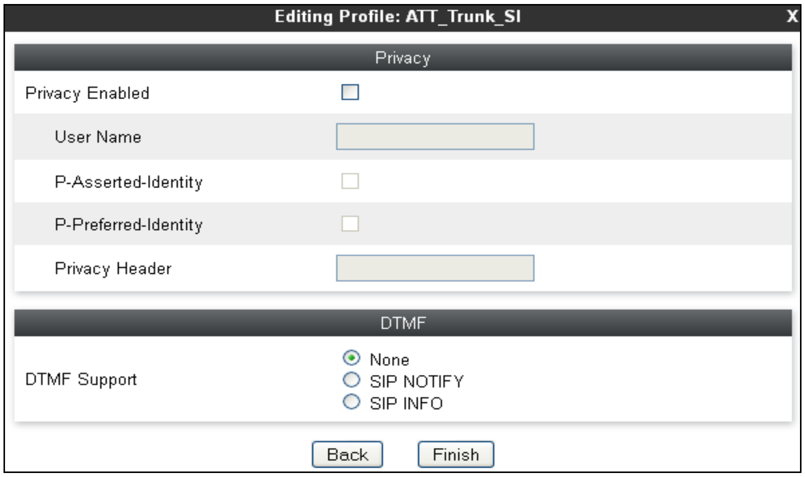
- Create a new profile by selecting **Add Profile** (not shown), and enter a profile name**:** (e.g., **ATT_Trunk_SI**).
- For the **General** tab (not shown) enter the follow, then click **Finish**:



Editing Profile: ATT_Trunk_SI

General

Hold Support	● None ○ RFC2543 - c=0.0.0.0 ○ RFC3264 - a=sendonly
180 Handling	● None ○ SDP ○ No SDP
181 Handling	● None ○ SDP ○ No SDP
182 Handling	● None ○ SDP ○ No SDP
183 Handling	● None ○ SDP ○ No SDP
Refer Handling	□
URI Group	None
3xx Handling	□
Diversion Header Support	□
Delayed SDP Handling	□
Re-Invite Handling	□
T.38 Support	☑
URI Scheme	● SIP ○ TEL ○ ANY
Via Header Format	● RFC3261 ○ RFC2543



Editing Profile: ATT_Trunk_SI

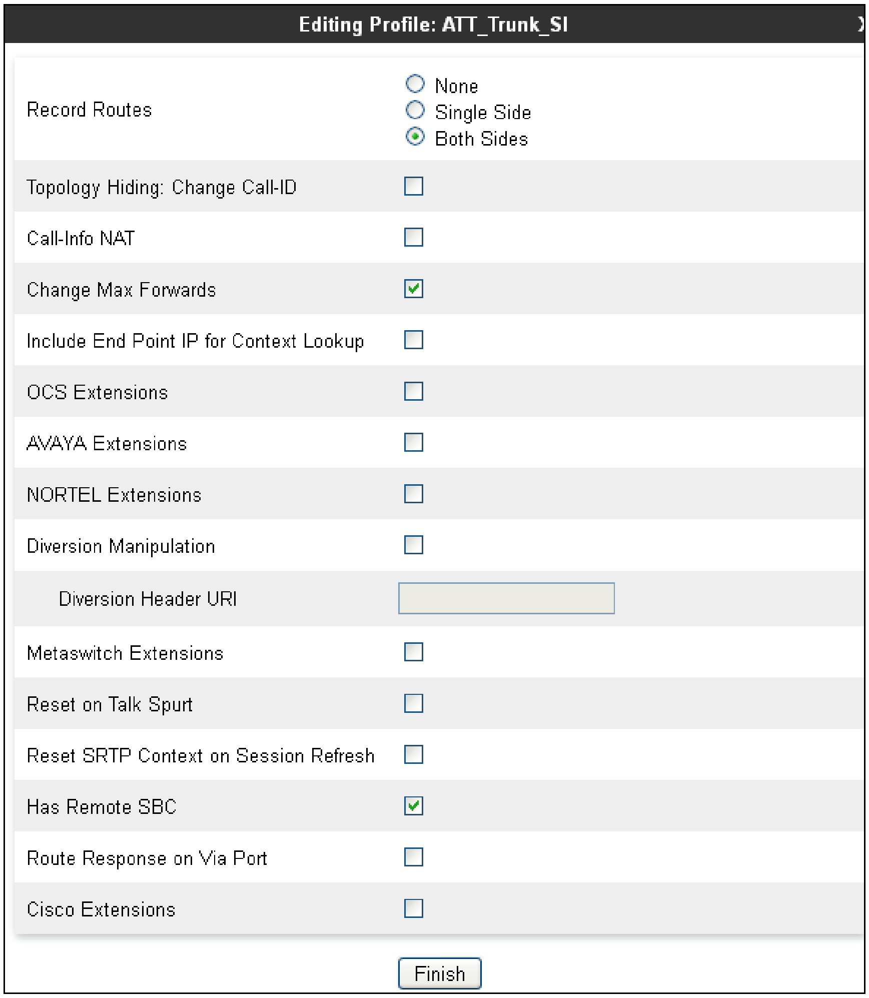
Privacy

Privacy Enabled	□
User Name	
P-Asserted-Identity	□
P-Preferred-Identity	□
Privacy Header	

DTMF

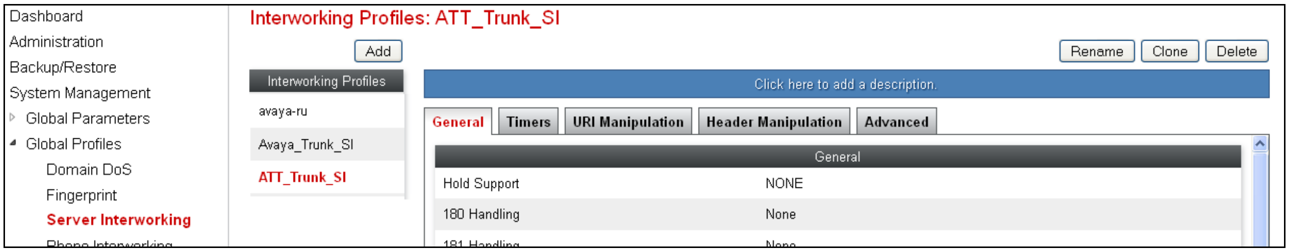
DTMF Support	● None ○ SIP NOTIFY ○ SIP INFO

Step 2 - For the **Advanced** Tab (not shown) use the following settings and click **Finish**:



Editing Profile: ATT_Trunk_SI

Record Routes	○ None ○ Single Side ● Both Sides
Topology Hiding: Change Call-ID	□
Call-Info NAT	□
Change Max Forwards	☑
Include End Point IP for Context Lookup	□
OCS Extensions	□
AVAYA Extensions	□
NORTEL Extensions	□
Diversion Manipulation	□
Diversion Header URI	
Metaswitch Extensions	□
Reset on Talk Spurt	□
Reset SRTP Context on Session Refresh	□
Has Remote SBC	☑
Route Response on Via Port	□
Cisco Extensions	□



Interworking Profiles: ATT_Trunk_SI

Interworking Profiles
- avaya-ru
- Avaya_Trunk_SI
- ATT_Trunk_SI

General

Hold Support	NONE
180 Handling	None
181 Handling	None

7.3.3. Routing – To Session Manager

The following routing profile provides routing to Session Manager.

Step 1 - Select **Global Profiles → Routing** from the menu on the left-hand side (not shown).

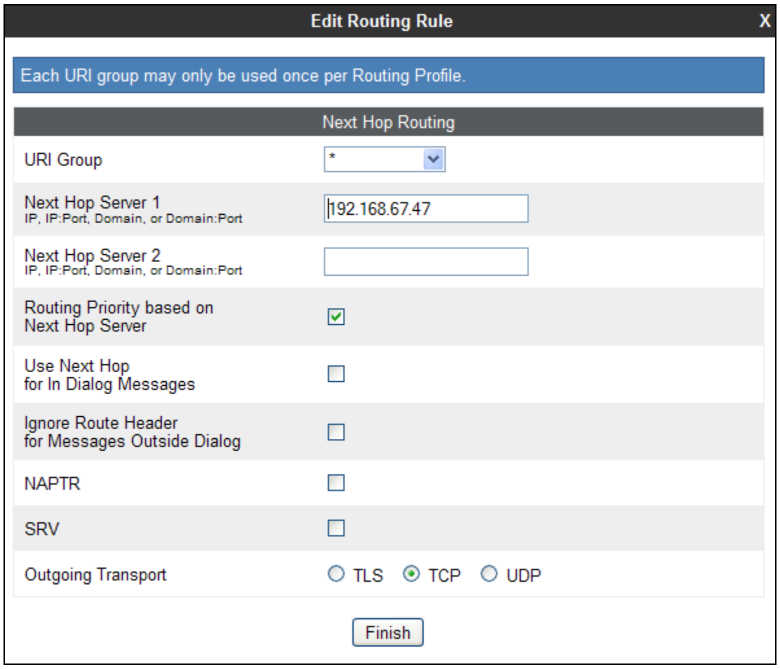
Step 2 - Select **Add Profile** (not shown).

Step 3 - Enter **Profile Name**: (e.g., **To_SM _RP)**.

Step 4 - Click **Next** and enter the following for regular inbound calls:

- In the **URI Group** field specify ***.**
- **Next Hop Server 1**: **192.168.67.47** (Session Manager).
- Verify **Routing Priority Based on Next Hop Server** is selected (default).
- **Outgoing Transport**: **TCP.**
- Accept remaining default values.

Step 5 - Click **Finish**.

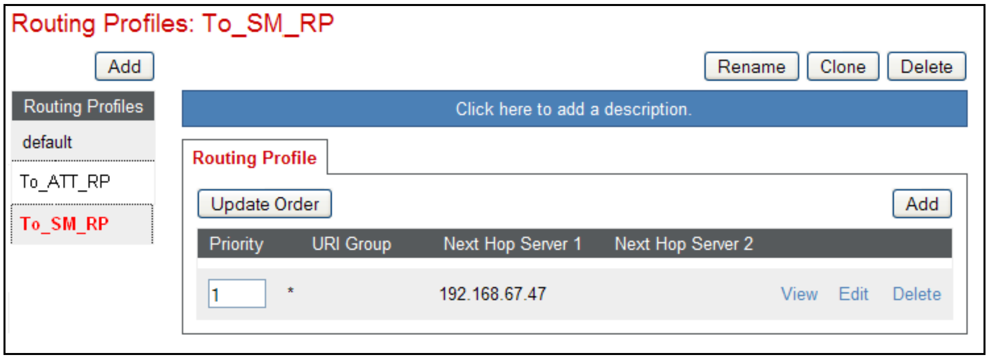


Edit Routing Rule

Each URI group may only be used once per Routing Profile.

Next Hop Routing

URI Group	*
Next Hop Server 1 IP, IP:Port, Domain, or Domain:Port	192.168.67.47
Next Hop Server 2 IP, IP:Port, Domain, or Domain:Port	
Routing Priority based on Next Hop Server	☑
Use Next Hop for In Dialog Messages	□
Ignore Route Header for Messages Outside Dialog	□
NAPTR	□
SRV	□
Outgoing Transport	○ TLS ● TCP ○ UDP



Routing Profiles: To_SM_RP

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	*	192.168.67.47		View Edit Delete

7.3.4. Routing – To AT&T

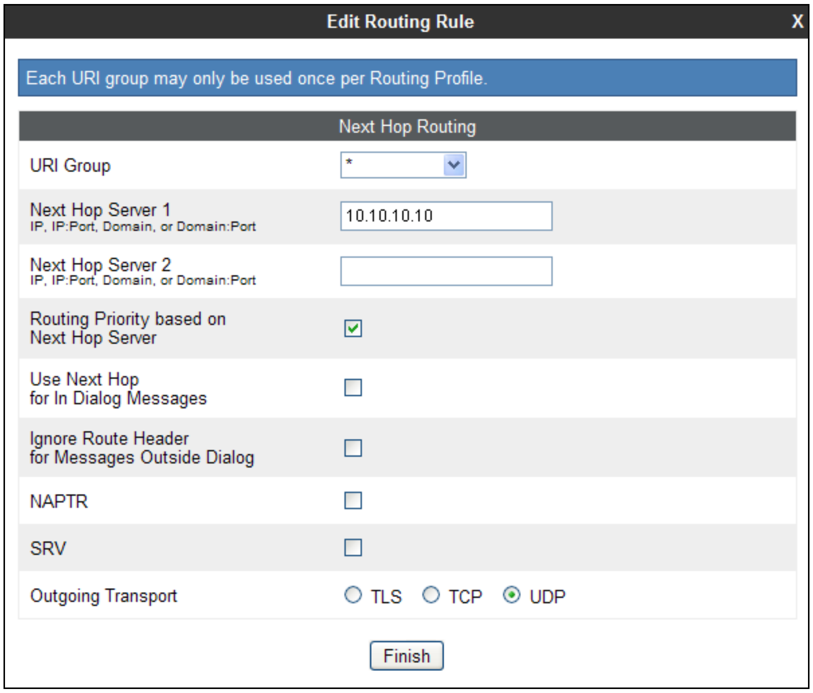
Repeat the steps in **Section 7.3.3**, with the following changes, to add a Routing Profile for the connection to AT&T.

Step 1 - Enter Profile Name: (e.g., **To_ATT_RP)**.

Step 2 - Click **Next**, then enter the following:

- **Next Hop Server 1: 10.10.10.10** (Primary AT&T Border Element IP address).
- Verify **Routing Priority Based on Next Hop Server** is selected (default).
- **Outgoing Transport**: **UDP.**

Step 3 - Click **Finish**.



Edit Routing Rule X

Each URI group may only be used once per Routing Profile.

Next Hop Routing	
URI Group	*
Next Hop Server 1 IP, IP:Port, Domain, or Domain:Port	10.10.10.10
Next Hop Server 2 IP, IP:Port, Domain, or Domain:Port	
Routing Priority based on Next Hop Server	☑
Use Next Hop for In Dialog Messages	□
Ignore Route Header for Messages Outside Dialog	□
NAPTR	□
SRV	□
Outgoing Transport	○ TLS ○ TCP ● UDP

7.3.5. Server Configuration – Session Manager

Step 1 - Select **Global Profiles → Server Configuration** from the menu on the left-hand side (not shown).

Step 2 - Select **Add Profile** and the **Profile Name** window will open (not shown). Enter a Profile Name (e.g., **SM_Trunk_SC**) and click **Next**.

Step 3 - The **Add Server Configuration Profile - General** window will open.

- Select **Server Type**: **Call Server**.
- **IP Address**: **192.168.67.47**.
- **Supported Transports**: Check **TCP**.
- **TCP Port**: **5060**.
- Select **Next**.

Step 4 - The **Add Server Configuration Profile - Authentication** window will open (not shown).

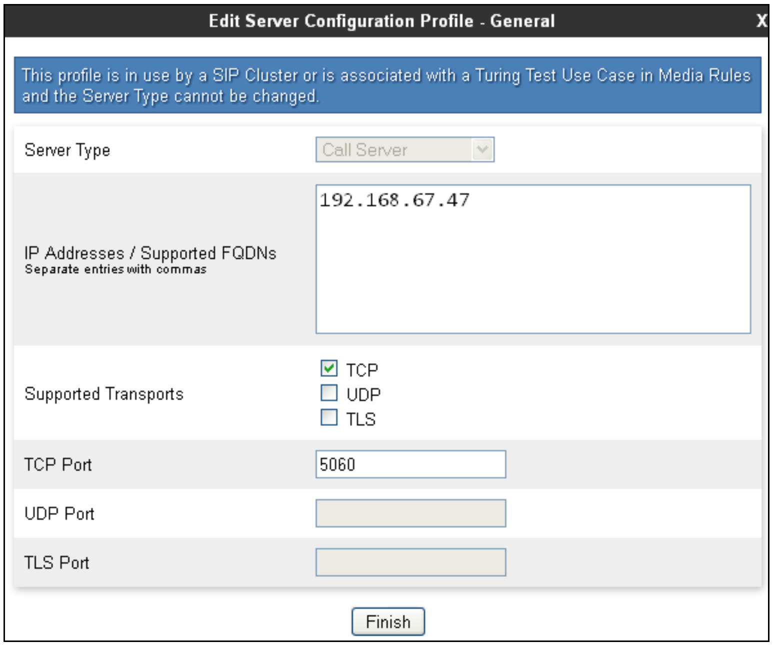
- Select **Next** to accept default values.

Step 5 - The **Add Server Configuration Profile - Heartbeat** window will open (not shown).

- Select **Next** to accept default values.

Step 6 - The **Add Server Configuration Profile - Advanced** window will open.

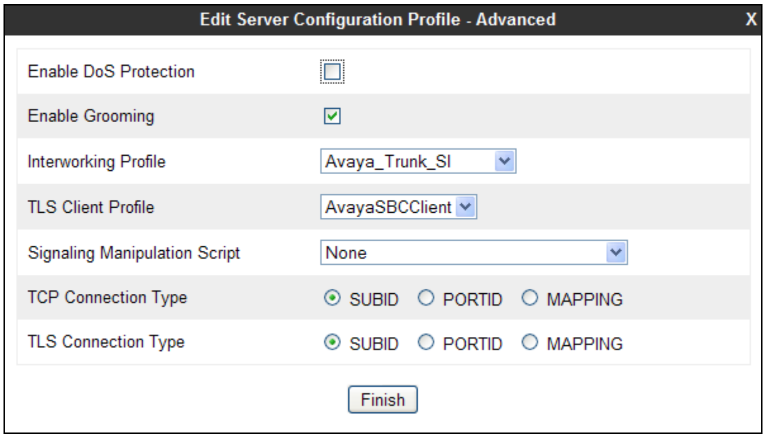
- Select **Avaya_Trunk_SI** (created in **Section 7.3.1**), for **Interworking Profile**.
- Select **AvayaSBCClient** for **TLS Client Profile**.
- **Verify the Signaling Manipulation Script field is set to None (default).**
- Select **Finish**.



Edit Server Configuration Profile - General

This profile is in use by a SIP Cluster or is associated with a Turing Test Use Case in Media Rules and the Server Type cannot be changed.

Server Type	Call Server
IP Addresses / Supported FQDNs Separate entries with commas	192.168.67.47
Supported Transports	☑ TCP ☐ UDP ☐ TLS
TCP Port	5060
UDP Port	
TLS Port	



Edit Server Configuration Profile - Advanced

Enable DoS Protection	☐
Enable Grooming	☑
Interworking Profile	Avaya_Trunk_SI
TLS Client Profile	AvayaSBCClient
Signaling Manipulation Script	None
TCP Connection Type	● SUBID ○ PORTID ○ MAPPING
TLS Connection Type	● SUBID ○ PORTID ○ MAPPING

7.3.6. Server Configuration – AT&T

Note – The AT&T IPFR-EF service may provide a Primary and Secondary Border Element. This section describes the connection to a single Border Element. See **Addendum 1** for information on configuring Primary & Secondary IPFR-EF Border Elements.

Repeat the steps in **Section 7.3.5**, with the following changes.

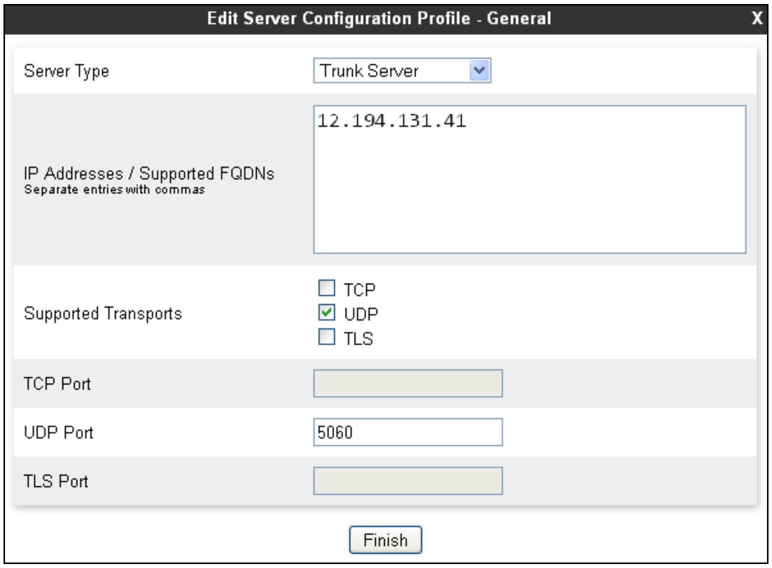
Step 1 - Enter a Profile Name (e.g., **ATT_SC**) and select **Next**.

Step 2 - The **Add Server Configuration Profile - General** window will open (not shown).

- Select Server Type**: Trunk Server.**
- **IP Address: 10.10.10.10** (AT&T Primary Border Element IP address).
- **Supported Transports**: Check **UDP.**
- **UDP Port: 5060.**
- Select **Next.**

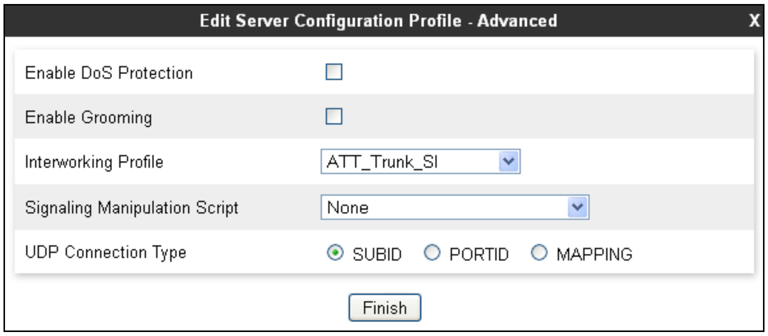
Step 3 - The **Add Server Configuration Profile - Advanced** window will open.

- Select **ATT_Trunk_SI** (created in **Section 7.3.2**), for **Interworking Profile**.
- In the **Signaling Manipulation Script** field select **None**.
- Select **Finish**.



Edit Server Configuration Profile - General

Server Type	Trunk Server
IP Addresses / Supported FQDNs Separate entries with commas	12.194.131.41
Supported Transports	□ TCP ☑ UDP □ TLS
TCP Port	
UDP Port	5060
TLS Port	



Edit Server Configuration Profile - Advanced

Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	ATT_Trunk_SI
Signaling Manipulation Script	None
UDP Connection Type	● SUBID ○ PORTID ○ MAPPING

7.3.7. Topology Hiding – Avaya Side

The **Topology Hiding** hides the topology of the enterprise network from external networks.

Step 1 - Select **Global Profiles → Topology Hiding** from the menu on the left-hand side (not shown).

Step 2 - Click **default** profile and select **Clone Profile** (not shown).

Step 3 - Enter Profile Name: (e.g., **Avaya_TH**)

Step 4 - For the Header **To**,

- In the **Criteria** column select **IP/Domain**.
- In the **Replace Action** column select **Overwrite**.
- In the **Overwrite Value** column enter **customera.com**.

Step 5 - For the Header **Request Line**,

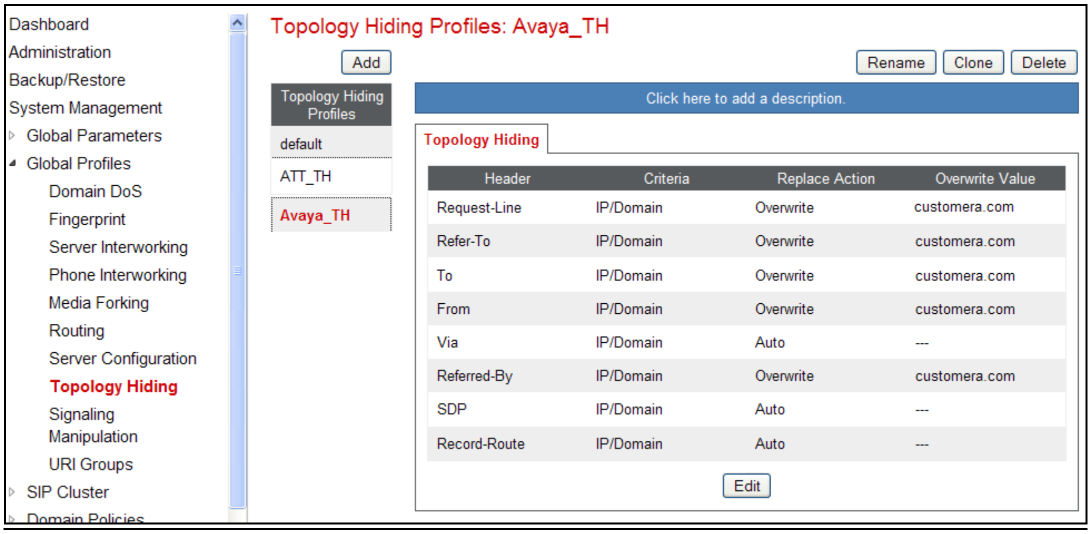
- In the **Criteria** column select **IP/Domain**.
- In the **Replace Action** column select **Overwrite**.
- In the **Overwrite Value** column enter **customera.com**.

Step 6 - For the Header **From**,

- In the **Criteria** column select **IP/Domain**.
- In the **Replace Action** column select **Overwrite**.
- In the **Overwrite Value** column enter **customera.com**.

Step 7 - Use default values for rest of the fields.

Step 8 - Click **Finish**.



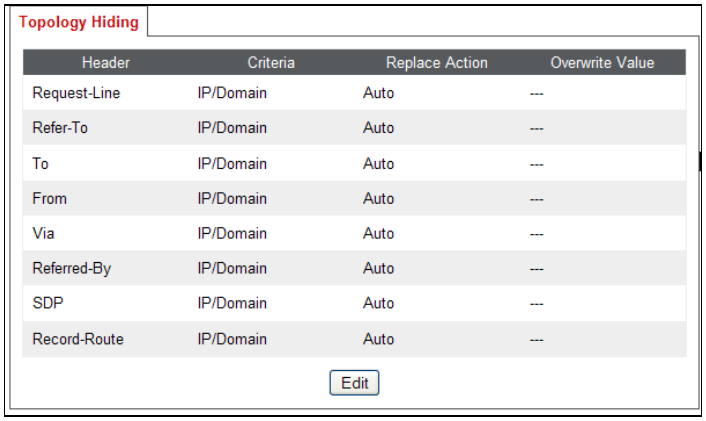
Topology Hiding Profiles: Avaya_TH

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Overwrite	customera.com
Refer-To	IP/Domain	Overwrite	customera.com
To	IP/Domain	Overwrite	customera.com
From	IP/Domain	Overwrite	customera.com
Via	IP/Domain	Auto	---
Referred-By	IP/Domain	Overwrite	customera.com
SDP	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---

7.3.8. Topology Hiding – AT&T Side

Step 1 - Repeat the steps in **Section 7.3.7,** with the following changes:

- Enter Profile Name: (e.g., **ATT_TH**).
- Leave all values at default.



Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
To	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---

7.3.9. Signaling Manipulations

The Avaya SBCE can manipulate inbound and outbound SIP headers through the use of Sigma scripts. However, in the reference configuration, no signaling manipulation scripts were required.

7.4. Domain Policies

The Domain Policies feature allows users to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise.

7.4.1. Application Rules

Step 1 - Select **Domain Policies → Application Rules** from the menu on the left-hand side (not shown).

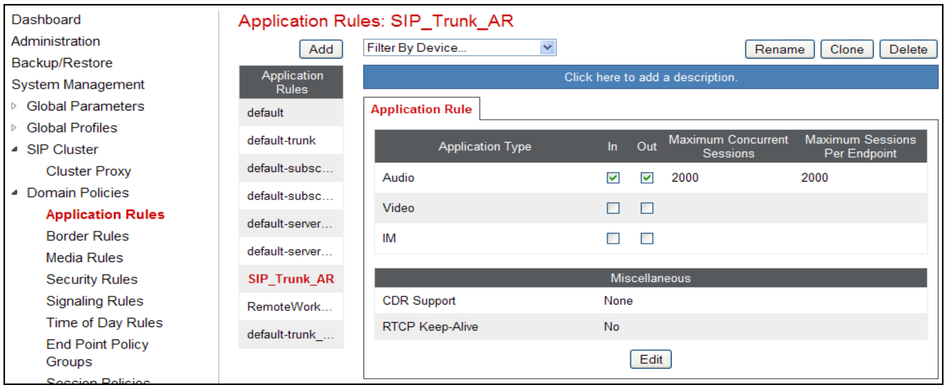
Step 2 - Select the **default** Rule (not shown).

Step 3 - Select the **Clone** button (not shown), and the **Clone Rule** window will open.

- In the **Clone Name** field enter **SIP_Trunk_AR**.
- Click **Finish**.

Step 4 - Select the **SIP_Trunk_AR** rule just created (not shown).

- Click the **Edit** button. The **Editing Rule** screen will be displayed.
- In the **Audio** row:
  - Change the **Maximum Concurrent Sessions** to **2000**.
  - Change the **Maximum Sessions per Endpoint** to **2000**.
- Click on **Finish**.



Application Rules: SIP_Trunk_AR

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	☑	☑	2000	2000
Video	□	□		
IM	□	□		

Miscellaneous	
CDR Support	None
RTCP Keep-Alive	No

7.4.2. Media Rules

The following Media Rule will be applied to both the Avaya and AT&T connections and therefore, only one rule is needed.

Step 1 - Select **Domain Policies → Media Rules** from the menu on the left-hand side menu (not shown).

Step 2 - The Media Rules window will open (not shown). From the Media Rules menu, select the **default-low-med** rule

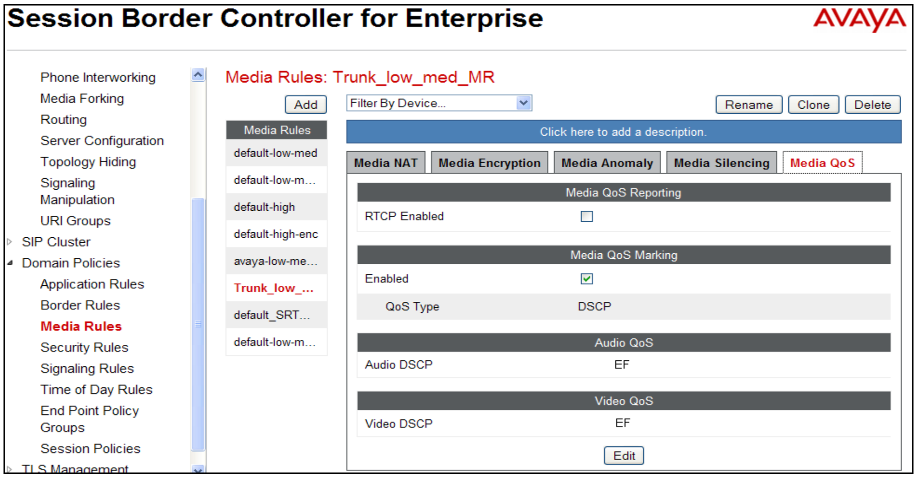
Step 3 - Select **Clone** button (not shown), and the **Clone Rule** window will open.

- In the **Clone Name** field enter **Trunk_low_med_MR.**
- Click **Finish.** The newly created rule will be displayed.

Step 4 - Highlight the **Trunk-low-med_MR** rule just created (not shown):

- Select the **Media QOS** tab.
- Click the **Edit** button and the **Media QOS** window will open.
- Check the **Media QOS Marking** field is **Enabled.**
- Select the **DSCP** box.
- **Audio**: Select **EF** from the drop-down.
- **Video**: Select **EF** from the drop-down.

Step 5 - Click **Finish.** The completed **Media Rules** screen is shown below.



Media Rules: Trunk_low_med_MR

Media QoS Reporting	
RTCP Enabled	□

Media QoS Marking	
Enabled	☑
QoS Type	DSCP

Audio QoS	
Audio DSCP	EF

Video QoS	
Video DSCP	EF

7.4.3. Signaling Rules

In the reference configuration, Signaling Rules are used to define QOS parameters, as well as to remove unwanted SIP headers (see **Section 2.2, Item 1**).

Note – SIP headers may also be blocked by the Signaling Manipulation function. However, Signaling Rules are a more efficient use of Avaya SBCE resources.

7.4.3.1 Avaya – Signaling QOS

Step 1 - Select **Domain Policies → Signaling Rules** from the menu on the left-hand side menu (not shown).

Step 2 - The Signaling Rules window will open (not shown). From the Signaling Rules menu, select the **default** rule.

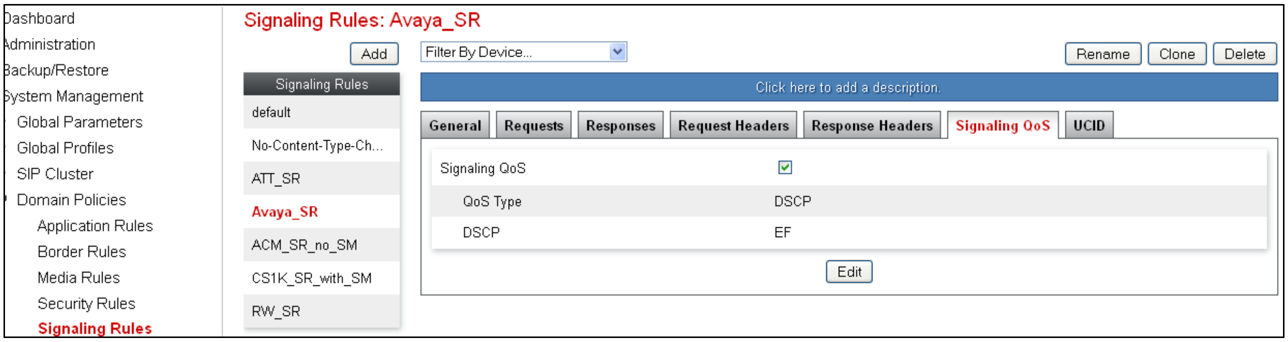
Step 3 - Select the **Clone** button and the **Clone Rule** window will open (not shown).

- In the **Rule Name** field enter **Avaya_SR.**
- Click **Finish.** The newly created rule will be displayed.

Step 4 - Highlight the **Avaya_SR** rule created in step **4** and enter the following:

- Select the **Signaling QOS** tab.
- Click the **Edit** button and the **Signaling QOS** window will open.
- Verify that **Signaling QOS** is selected.
- Select **DCSP**.
- Select **Value** = **EF**.

Step 5 - Click **Finish.** The completed **Signaling Rules** screen is shown below.



Signaling Rules: Avaya_SR

Signaling QoS	☑
QoS Type	DSCP
DSCP	EF

7.4.3.2 AT&T – Signaling QOS Tab

Step 1 - Repeat the steps in **Section 7.4.3.1**, with the following changes:

- After cloning the **default** rule (not shown), name the rule **(**e.g., **ATT_SR).**
- Specify the same parameters used in **Section 7.4.3.1**.

7.4.3.3 Avaya – Request Headers Tab – Removal of Unwanted SIP Headers

The following Signaling Rules remove SIP Request headers (e.g., Invites) sent by Communication Manager, (or other components of the CPE), that are either not supported or required by AT&T, or headers that may contain internal CPE information.

Note – In configurations that include Avaya Aura® Session Manager, History-Info headers are removed by Session Manager adaptations (see **Section 5.3**). Alternatively they may be removed here.

Use the following steps to remove the **P-Location** header from Invites:

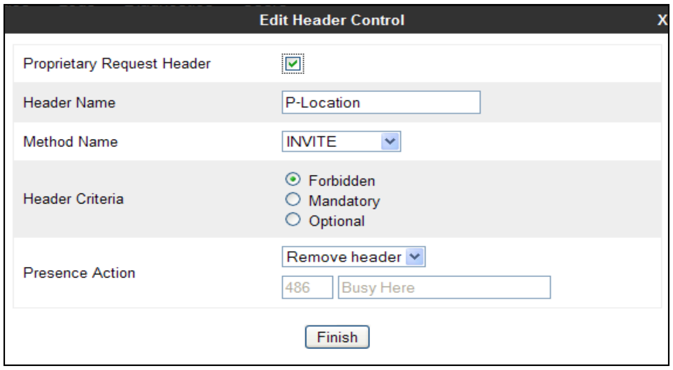
Step 1 - Select **Domain Policies** from the menu on the left-hand side menu (not shown).
Step 2 - Select **Signaling Rules** (not shown).
Step 3 - From the Signaling Rules menu, select the **default** rule.
Step 4 - Select **Clone Rule** button.

- Enter a name**: Avaya_SR.**
- Click **Finish.**

Step 5 - Highlight and edit the **Avaya_SR** rule created in **Step 4** and enter the following:

- Select the **Add In Header Control** button (not shown). The Add Header Control window will open.
- Select the **Request Headers** tab (not shown).
- Click the **Edit** button and the **Edit Header Control** window will open.
- Check the **Proprietary Request Header** box.
- In the **Header Name** field, enter **P-Location**.
- From the **Method Name** menu select **Invite**.
- For **Header Criteria** select **Forbidden**.
- From the **Presence Action** menu select **Remove Header**.

Step 6 - Click **Finish.**



Edit Header Control

Proprietary Request Header	☑
Header Name	P-Location
Method Name	INVITE
Header Criteria	● Forbidden ○ Mandatory ○ Optional
Presence Action	Remove header 486 Busy Here

Step 7 - Repeat **Steps 5** through **6** to create a rule to remove the **P-Location** header from ACKs.

- Verify the **Proprietary Request Header** box is *checked*.
- From the **Header Name** menu select **Alert-Info.**
- From the **Method Name** menu select **Ack**.

Step 8 - Repeat **Steps 5** through **6** to create a rule to remove the **Alert-Info** header.

- Verify the **Proprietary Request Header** box is *unchecked*.
- From the **Header Name** menu select **Alert-Info.**

Step 9 - Repeat **Steps 5** through **6** to create a rule to remove the **Endpoint-View** header.

- Check the **Proprietary Request Header** box.
- In the **Header Name** field, enter **Endpoint-View.**

Step 10 - Repeat **Steps 5** through **6** to create a rule to remove the **AV-Correlation-ID** header.

- Check the **Proprietary Request Header** box.
- In the **Header Name** field enter **AV-Correlation-ID**.

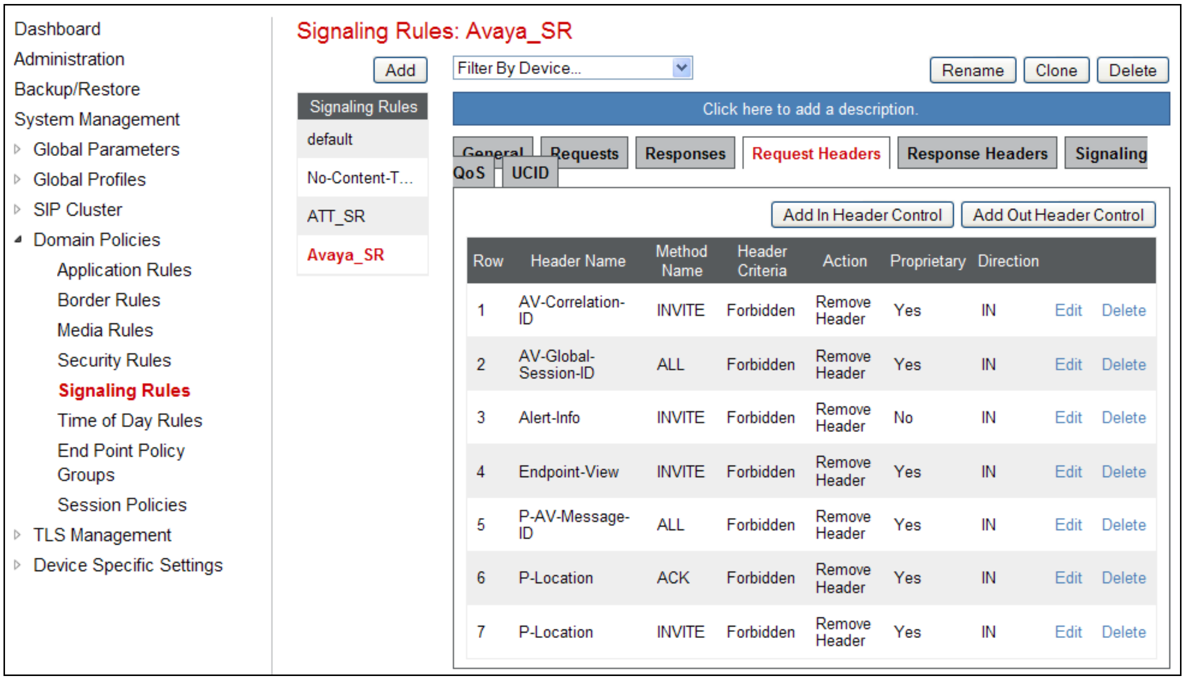
Step 11 - Repeat **Steps 5** through **6** to create a rule to remove the **AV-Global-Session-ID** header.

- Check the **Proprietary Request Header** box.
- In the **Header Name** field enter **AV-Global-Session-ID.**
- From the **Method Name** menu select **ALL**.

Step 12 - Repeat **Steps 5** through **6** to create a rule to remove the P-**AV-Message-ID** header.

- In the **Header Name** field enter **P-AV-Message-ID.**
- From the **Method Name** menu select **ALL**.

The completed **Request Headers** form is shown below. Note that the **Direction** column says **IN**.



Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction		
1	AV-Correlation-ID	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	AV-Global-Session-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	Alert-Info	INVITE	Forbidden	Remove Header	No	IN	Edit	Delete
4	Endpoint-View	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-AV-Message-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	P-Location	ACK	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-Location	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete

7.4.3.4 Avaya – Response Headers Tab – Removal of Unwanted SIP Headers

The following Signaling Rules remove SIP Response headers (e.g., 1xx and/or 200ok) sent by ANS that are either not supported or required by AT&T, or are headers that may contain internal CPE information.

Step 1 - Highlight the **Avaya_SR** rule created in **Section 7.4.3.1**, and using the same procedures shown in **Section 7.4.3.3** remove the **P-Location** header from **1xx** responses:

- Select the **Response Headers** tab (not shown).
- Check the **Proprietary Request Header** box.
- In the **Header Name** field, enter **P-Location**.
- From the **Response Code** menu select **1xx**.
- From the **Method Name** menu select **Invite**.
- For **Header Criteria** select **Forbidden**.
- From the **Presence Action** menu select **Remove Header**.
- Click **Finish.**

Step 2 - Repeat **Step 1** to create a rule to remove the **P-Location** header from **2xx** responses.

- From the **Response Code** menu select **2xx**.

Step 3 - Repeat **Step 1** to create a rule to remove the **Endpoint-View** header from **1xx** responses.

- In the **Header Name** field, enter **Endpoint-View**.
- From the **Response Code** menu select **1xx**.

Step 4 - Repeat **Step 3** to remove **Endpoint-View** headers from **2xx** responses.

- From the **Response Code** menu select **2xx**.

Step 5 - Repeat **Step 1** to create a rule to remove the P-**AV-Message-ID** header from **1xx** responses.

- In the **Header Name** field, enter **Endpoint-View**.
- From the **Response Code** menu select **1xx**.
- From the **Method Name** menu select **ALL**.

Step 6 - Repeat **Step 5** to remove P-**AV-Message-ID** headers from **2xx** responses.

- From the **Response Code** menu select **2xx**.

Step 7 - Repeat **Step 1** to create a rule to remove the **AV-Global-Session-ID** header from **1xx** responses.

- In the **Header Name** field, enter **Endpoint-View**.
- From the **Response Code** menu select **1xx**.
- From the **Method Name** menu select **ALL**.

Step 8 - Repeat **Step 7** to remove **AV-Global-Session-ID** headers from **2xx** responses.

- From the **Response Code** menu select **2xx**.

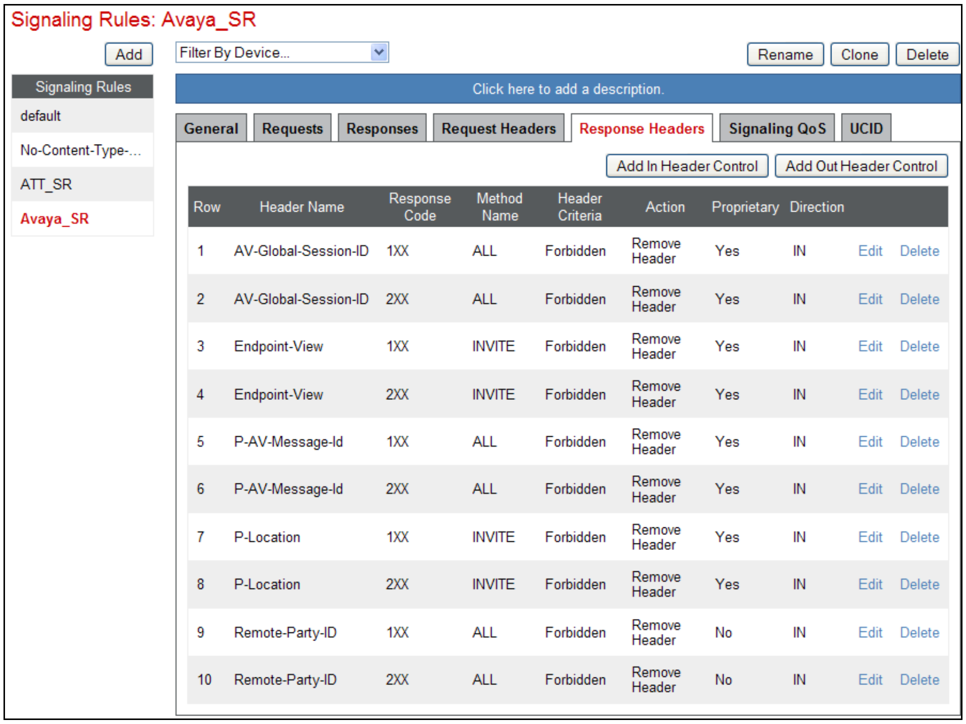
Step 9 - Repeat **Step 1** to remove **Remote-Party-ID** headers from **1xx** and **2xx** responses.

- *Do not* check the **Proprietary Request Header** box.
- In the **Header Name** field, enter **Remote-Party-ID**.
- From the **Response Code** menu select **1xx**.
- From the **Method Name** menu select **ALL**.

Step 10- Repeat **Step 9** to remove **Remote-Party-ID** headers from **2xx** responses.

- From the **Response Code** menu select **2xx**.

The completed **Response Headers** form is shown below. Note that the **Direction** column says **IN**.



Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	AV-Global-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	AV-Global-Session-ID	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	Endpoint-View	1XX	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	Endpoint-View	2XX	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-AV-Message-Id	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	P-AV-Message-Id	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-Location	1XX	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
8	P-Location	2XX	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
9	Remote-Party-ID	1XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
10	Remote-Party-ID	2XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete

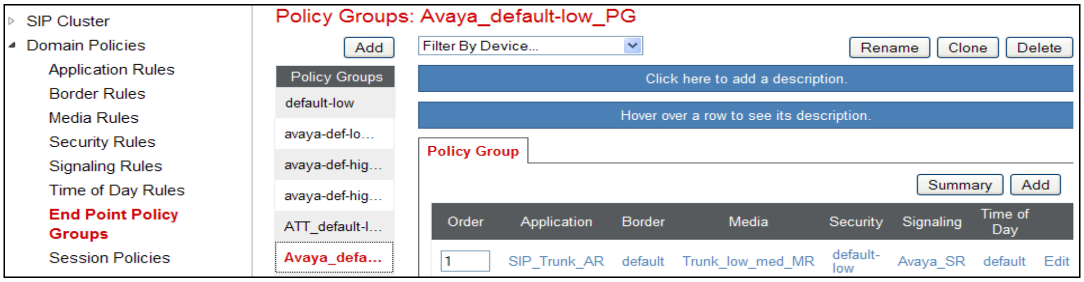
7.4.4. Endpoint Policy Groups – Avaya Connection

Step 1 - Select **Domain Policies** → **End Point Policy Groups** from the menu on the left-hand side (not shown).

Step 2 - Select **Add Group**, and enter the following:

- **Name**: **Avaya_default-low_PG.**
- **Application Rule**: **SIP_Trunk_AR** (created in **Section 7.4.1**).
- **Border Rule**: **default**.
- **Media Rule**: **Trunk_low_med_MR** (created in **Section 7.4.2**).
- **Security Rule**: **default-low**.
- **Signaling Rule**: **Avaya_SR** (created in **Section 7.4.3**).
- **Time of Day**: **default**.

Step 3 - Select **Finish** (not shown).



Policy Groups: Avaya_default-low_PG

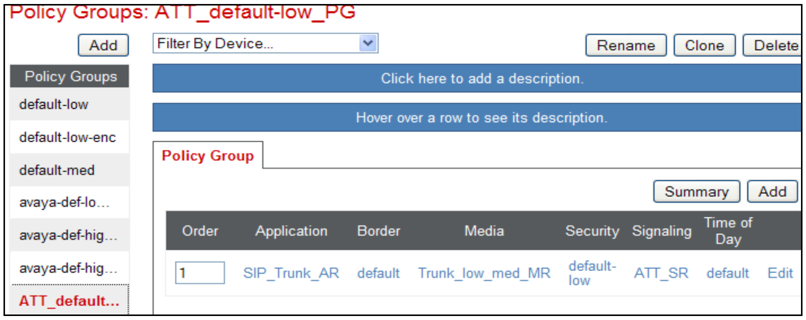
Order	Application	Border	Media	Security	Signaling	Time of Day	
1	SIP_Trunk_AR	default	Trunk_low_med_MR	default-low	Avaya_SR	default	Edit

7.4.5. Endpoint Policy Groups – AT&T Connection

Step 1 - Repeat steps **1** through **4** from **Section 7.4.4** with the following changes:

- **Group Name**: **ATT_default-low_PG**.
- **Signaling Rule**: **ATT_SR** (created in **Section 7.4.3**).

Step 2 - **Select Finish** (not shown).



Policy Groups: ATT_default-low_PG

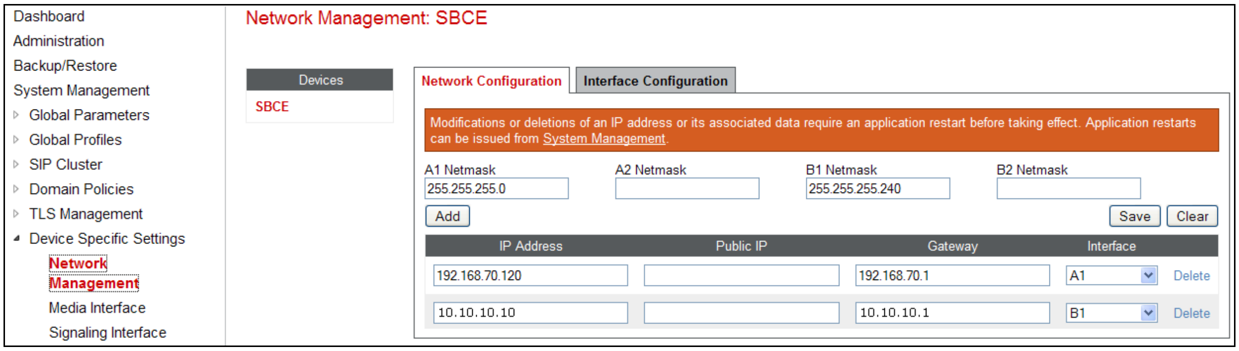
Order	Application	Border	Media	Security	Signaling	Time of Day	
1	SIP_Trunk_AR	default	Trunk_low_med_MR	default-low	ATT_SR	default	Edit

7.5. Device Specific Settings

7.5.1. Network Management

Step 1 - Select **Device Specific Settings** from the menu on the left-hand side.

Step 2 - Select **Network Management** and the **Network Configuration** tab. The network interfaces are defined during installation. However they may be modified, via this tab.



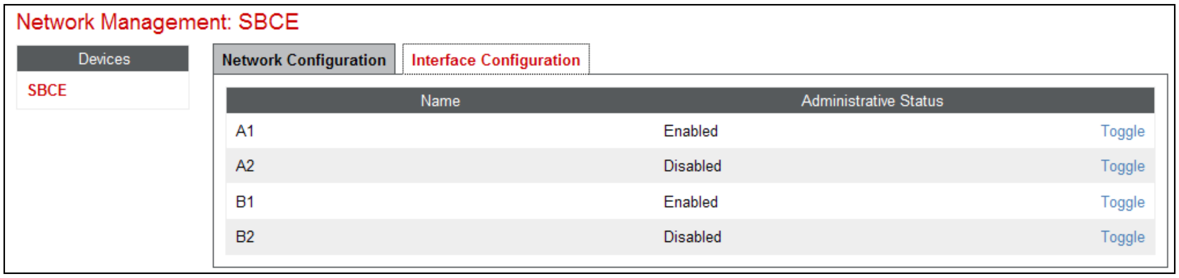
Network Management: SBCE

Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.

A1 Netmask: 255.255.255.0
A2 Netmask:
B1 Netmask: 255.255.255.240
B2 Netmask:

IP Address	Public IP	Gateway	Interface	
192.168.70.120		192.168.70.1	A1	Delete
10.10.10.10		10.10.10.1	B1	Delete

Step 3 - In addition, the provisioned interfaces may be enabled/disabled via the **Interface Configuration** tab (note that the A2 and B2 interfaces are not supported at this time).



Network Management: SBCE

Name	Administrative Status	
A1	Enabled	Toggle
A2	Disabled	Toggle
B1	Enabled	Toggle
B2	Disabled	Toggle

7.5.2. Advanced Options

In **Section 7.5.3**, the media UDP port ranges required by AT&T are set (**16384 – 32767**). By default part of this range is already allocated by the Avaya SBCE for internal use (22000 - 31000). The following steps reallocate the port ranges used by the Avaya SBCE so the range required by AT&T can be used.

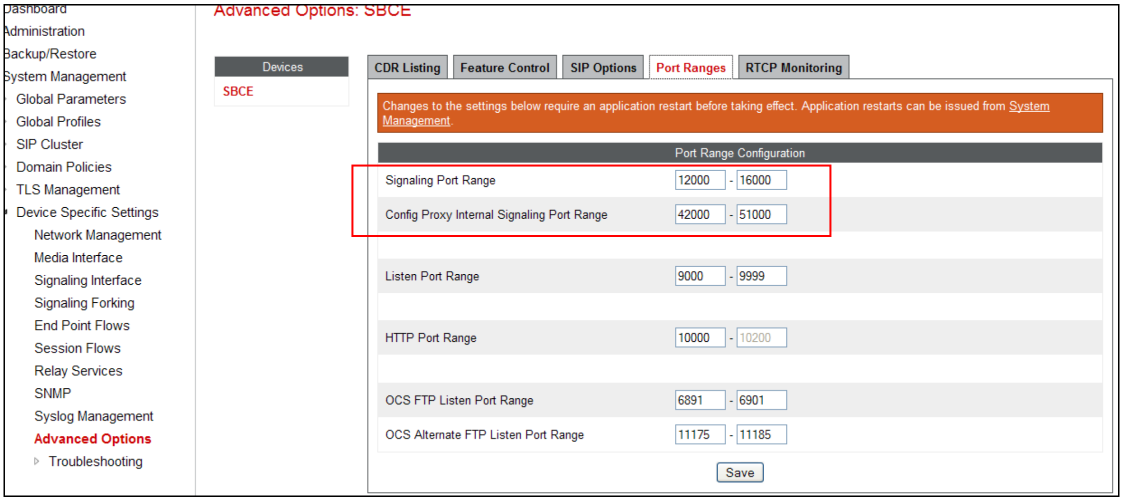
Step 1 - Select **Device Specific Settings → Advanced Options** from the menu on the left-hand side (not shown).

Step 2 - Select the **Port Ranges** tab.

Step 3 – In the **Signaling Port Range** row, change the range to **12000 – 16000**.

Step 4 - In the **Config Proxy Internal Signaling Port Range** row, change the range to **42000 – 51000**.

Step 4 - Scroll to the bottom of the window and select **Save** (not shown).



Advanced Options: SBCE

Changes to the settings below require an application restart before taking effect. Application restarts can be issued from System Management.

Port Range Configuration

Signaling Port Range	12000	16000
Config Proxy Internal Signaling Port Range	42000	51000
Listen Port Range	9000	9999
HTTP Port Range	10000	10200
OCS FTP Listen Port Range	6891	6901
OCS Alternate FTP Listen Port Range	11175	11185

7.5.3. Media Interfaces

The AT&T IPFR-EF service specifies that customers use RTP ports in the range of **16384 – 32767**. Both inside and outside ports have been changed to this range, but only the outside is required by the AT&T IPFR-EF service.

Step 1 - Select **Device Specific Settings → Media Interface** from the menu on the left-hand side (not shown).

Step 2 - Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:

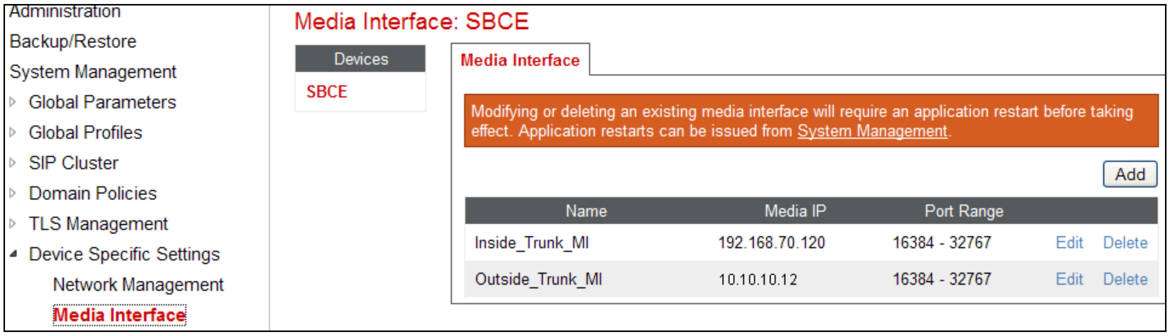
- **Name**: **Inside_Trunk_MI.**
- **IP Adrress**: **192.168.70.120** (Avaya SBCE A1 address).
- **Port Range**: **16384 – 32767.**

Step 3 - Click **Finish** (not shown).

Step 4 - Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:

- **Name**: **Outside_Trunk_MI.**
- **IP Address**: **10.10.10.12** (Avaya SBCE B1 address).
- **Port Range**: **16384 – 32767.**

Step 5 - Click **Finish** (not shown).



Media Interface: SBCE

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Name	Media IP	Port Range		
Inside_Trunk_MI	192.168.70.120	16384 - 32767	Edit	Delete
Outside_Trunk_MI	10.10.10.12	16384 - 32767	Edit	Delete

7.5.4. Signaling Interface

Step 1 - Select **Device Specific Settings → Signaling Interface** from the menu on the left-hand side (not shown).

Step 2 - Select **Add** (not shown) and enter the following:

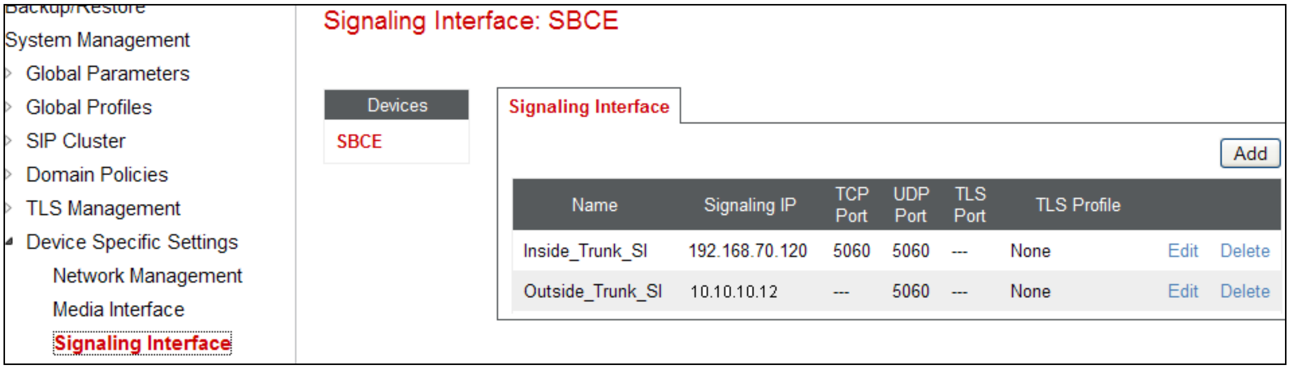
- **Name**: **Inside_Trunk_SI**.
- **IP Address**: **192.168.70.120** (Avaya SBCE A1 address).
- **TCP Port**: **5060.**

Step 3 - Click **Finish** (not shown).

Step 4 - Select **Add** again, and enter the following:

- **Name**: **Outside_Trunk_SI**.
- **IP Address**: **10.10.10.12** (Avaya SBCE B1 address).
- **UDP Port**: **5060.**

Step 5 - Click **Finish** (not shown).

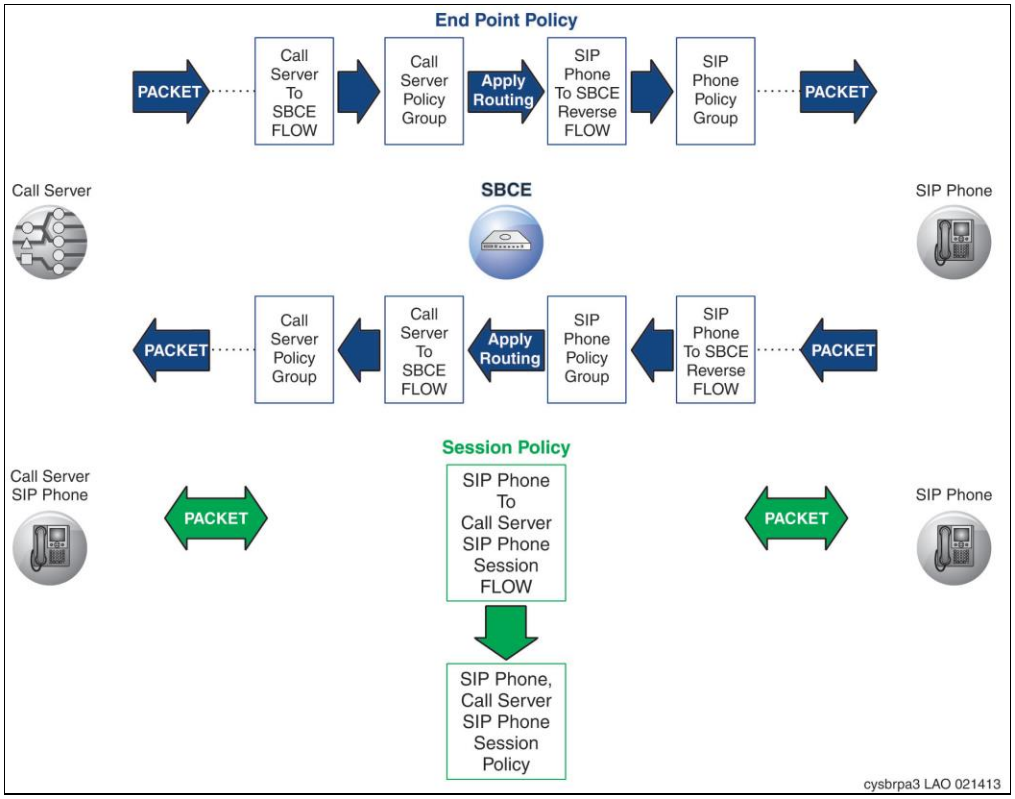


Signaling Interface: SBCE

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Inside_Trunk_SI	192.168.70.120	5060	5060	---	None	Edit	Delete
Outside_Trunk_SI	10.10.10.12	---	5060	---	None	Edit	Delete

7.6. Endpoint Flows

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy group which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following diagram illustrates the call flow through the Avaya SBCE.



7.6.1.1 Endpoint Flows – Avaya

Step 1 - Select **Device Specific Settings → Endpoint Flows** from the menu on the left-hand side (not shown).

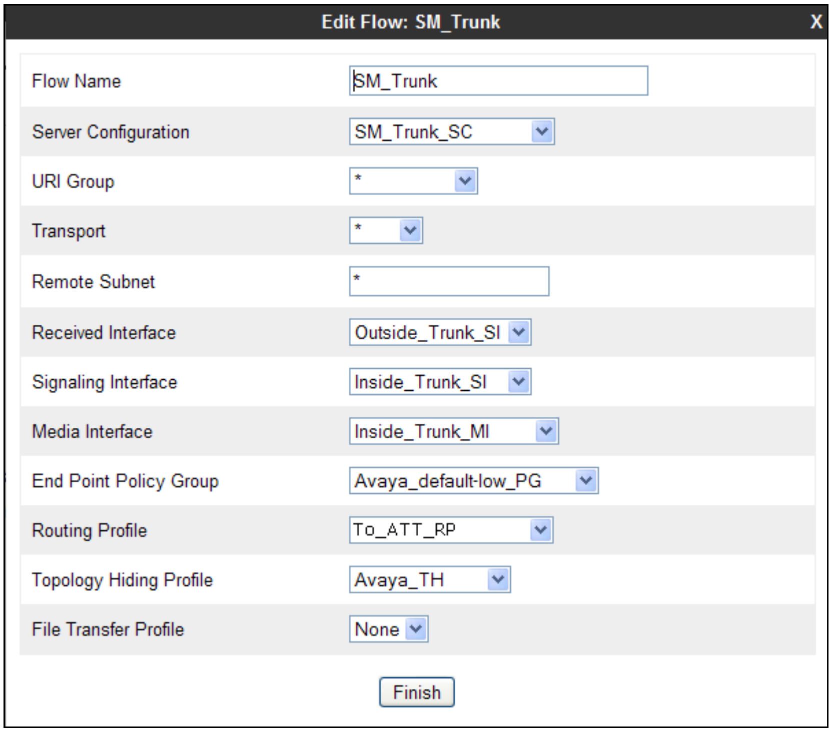
Step 2 - Select the **Server Flows** tab (not shown).

Step 3 - Select **Add**, (not shown) and enter the following:

- **Name**: **SM_Trunk.**
- **Server Configuration**: **SM_Trunk_SC** (**Section 7.3.5**).
- **URI Group**: ***.**
- **Transport**: ***.**
- **Remote Subnet**: ***.**
- **Received Interface**: **Outside_Trunk_SI (Section 7.5.4**).
- **Signaling Interface**: **Inside_Trunk_SI** (**Section 7.5.4**).

- **Media Interface**: **Inside_Trunk_MI** (**Section 7.5.3**).
- **End Point Policy Group**: **Avaya_default-low_PG** (**Section 7.4.4**).
- **Routing Profile**: **To_ATT _RP** (**Section 7.3.4**).
- **Topology Hiding Profile**: **Avaya_TH** (**Section 7.3.7**).
- **File Transfer Profile**: **None.**

Step 4 - Click **Finish**.



Edit Flow: SM_Trunk

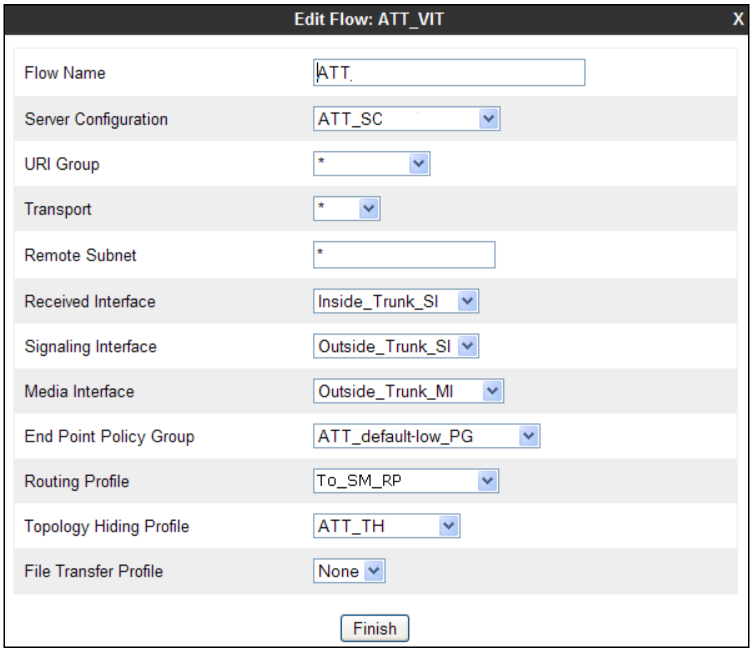
Flow Name	SM_Trunk
Server Configuration	SM_Trunk_SC
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Outside_Trunk_SI
Signaling Interface	Inside_Trunk_SI
Media Interface	Inside_Trunk_MI
End Point Policy Group	Avaya_default-low_PG
Routing Profile	To_ATT_RP
Topology Hiding Profile	Avaya_TH
File Transfer Profile	None

7.6.1.2 Endpoint Flows – AT&T

Step 1 - Repeat steps **1** through **4** from **Section 7.6.1.1**, with the following changes:

- **Name**: **ATT.**
- **Server Configuration**: **ATT_ SC** (**Section 7.3.6**).
- **URI Group**: ***.**
- **Transport**: ***.**
- **Remote Subnet**: ***.**
- **Received Interface**: **Inside_Trunk_SI** (**Section 7.5.4**).
- **Signaling Interface**: **Outside_Trunk_SI (Section 7.5.4**).
- **Media Interface**: **Outside_Trunk_MI** (**Section 7.5.3**).
- **End Point Policy Group**: **ATT_default-low_PG** (**Section 7.4.5**).
- **Routing Profile**: **To_SM_RP (Section 7.3.3**).
- **Topology Hiding Profile**: **ATT_TH** (**Section 7.3.8**).
- **File Transfer Profile**: **None.**

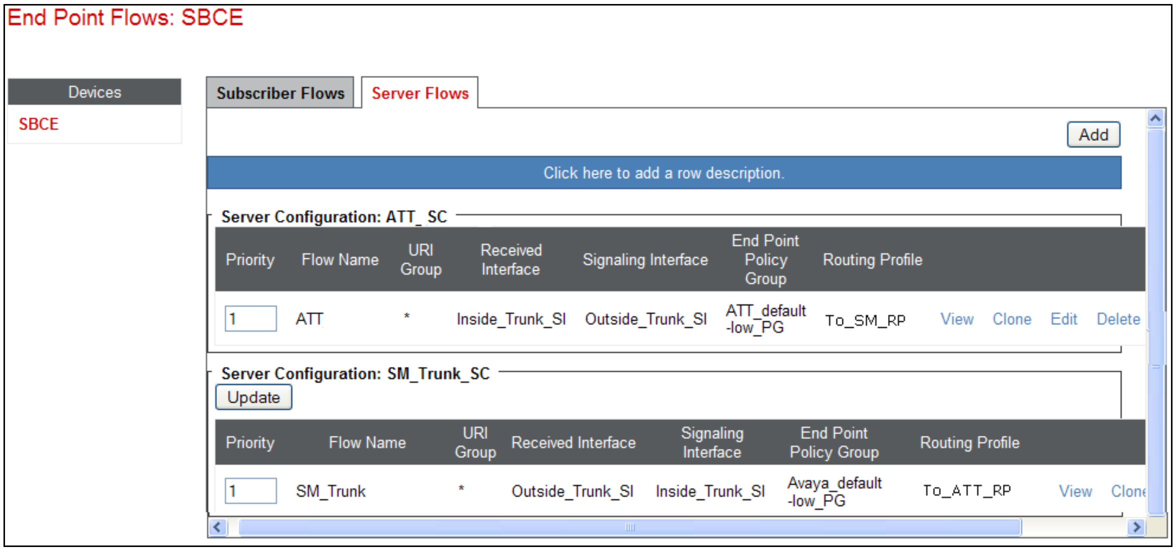
Step 2 - Click **Finish**.



Edit Flow: ATT_VIT

Flow Name	ATT
Server Configuration	ATT_SC
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Inside_Trunk_SI
Signaling Interface	Outside_Trunk_SI
Media Interface	Outside_Trunk_MI
End Point Policy Group	ATT_default-low_PG
Routing Profile	To_SM_RP
Topology Hiding Profile	ATT_TH
File Transfer Profile	None

The completed **End Point Flows** screen is shown below.



End Point Flows: SBCE

Server Configuration: ATT_ SC

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	ATT	*	Inside_Trunk_SI	Outside_Trunk_SI	ATT_default -low_PG	To_SM_RP	View	Clone	Edit	Delete

Server Configuration: SM_Trunk_SC

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile		
1	SM_Trunk	*	Outside_Trunk_SI	Inside_Trunk_SI	Avaya_default -low_PG	To_ATT_RP	View	Clone

8. Verification Steps

The following steps may be used to verify the call flow via the reference configuration:

8.1. Avaya Notification Solution Related Telephony

1. Place an inbound trigger call to ANS. Interact with the ANS prompts and verify that the call quality is good and that it disconnect properly.
2. Verify that ANS issues the correct notification as triggered, and that the appropriate subscribers are called. Verify any DTMF interactions as well as call quality, and that the call disconnects properly when the notification has completed.
3. Use local ANS triggering to launch a notification. Verify that ANS issues the correct notification as triggered, and that the appropriate subscribers are called. Verify any DTMF interactions as well as call quality, and that the call disconnects properly when the notification has completed.
4. Trigger an ANS notification to a subscriber with voicemail. Verify that the notification is recorded on the subscriber's voicemail system, and can be retrieved successfully.
5. Call into an ANS message inbox associated with a notification, and verify that the notification can be retrieved.

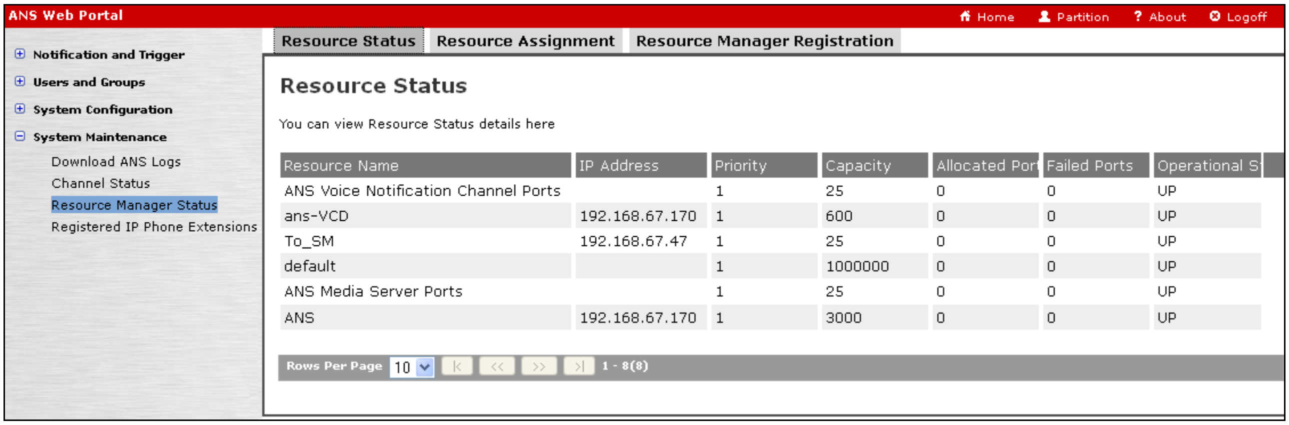
8.2. Avaya Notification Solution Status and Logs

The ANS Web Portal and the Avaya Media Server both provide access to various system status and troubleshooting capabilities. Refer to **[5 & 6]** for more information on these capabilities; however a few system status and logging examples are shown in the following sections.

8.2.1. Avaya Notification Solution Web Portal

Connect to the ANS Web Portal by entering **https://<*ANS IP address*>:8443/ANSWebPortal**, entering the appropriate credentials, and logging on.

Navigate to **System Maintenance → Resource Manager Status.** This display shows the state of the various ANS components.

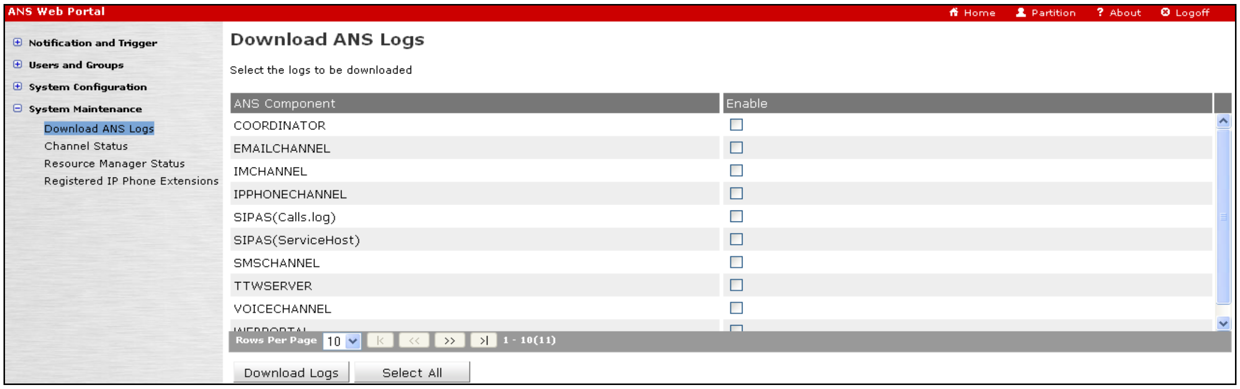


Resource Status

You can view Resource Status details here

Resource Name	IP Address	Priority	Capacity	Allocated Port	Failed Ports	Operational S
ANS Voice Notification Channel Ports		1	25	0	0	UP
ans-VCD	192.168.67.170	1	600	0	0	UP
To_SM	192.168.67.47	1	25	0	0	UP
default		1	1000000	0	0	UP
ANS Media Server Ports		1	25	0	0	UP
ANS	192.168.67.170	1	3000	0	0	UP

Navigate to **System Maintenance → Download ANS Logs.** Select the ANS component(s) from the **Enable** column and click on **Download Logs**.



Download ANS Logs

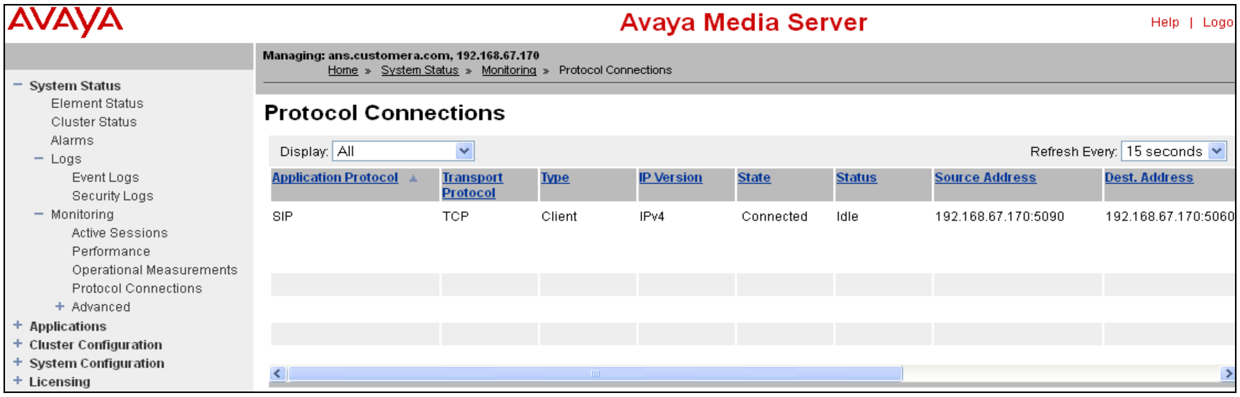
Select the logs to be downloaded

ANS Component	Enable
COORDINATOR	□
EMAILCHANNEL	□
IMCHANNEL	□
IPPHONECHANNEL	□
SIPAS(Calls.log)	□
SIPAS(ServiceHost)	□
SMSCHANNEL	□
TTWSERVER	□
VOICECHANNEL	□
WEBPORTAL	□

8.2.2. Avaya Media Server

Connect to the Avaya Media Server by entering **https://<ANS IP address>:9443/em**, entering the appropriate credentials, and logging on.

Navigate to **System Status → Monitoring → Protocol Connections.** This display shows the status of the SIP trunk.



Managing: ans.customera.com, 192.168.67.170

Home » System Status » Monitoring » Protocol Connections

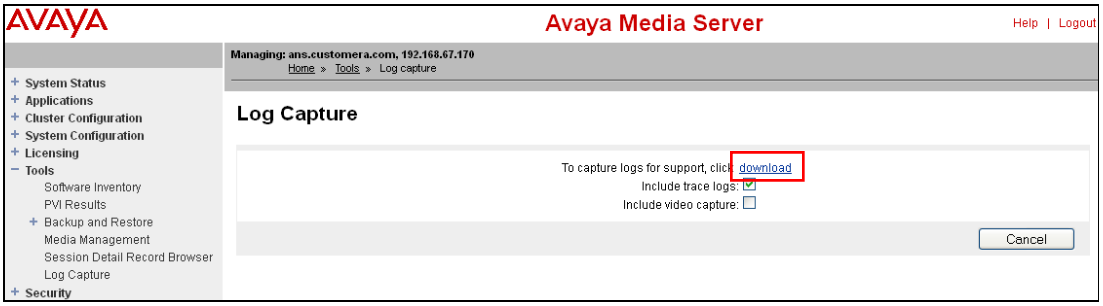
Protocol Connections

Display: All

Refresh Every: 15 seconds

Application Protocol	Transport Protocol	Type	IP Version	State	Status	Source Address	Dest. Address
SIP	TCP	Client	IPv4	Connected	Idle	192.168.67.170:5090	192.168.67.170:5060

Navigate to **Tools → Log Capture.** Click on **download**.



Managing: ans.customera.com, 192.168.67.170

Home » Tools » Log capture

Log Capture

To capture logs for support, click download

Include trace logs: ☑

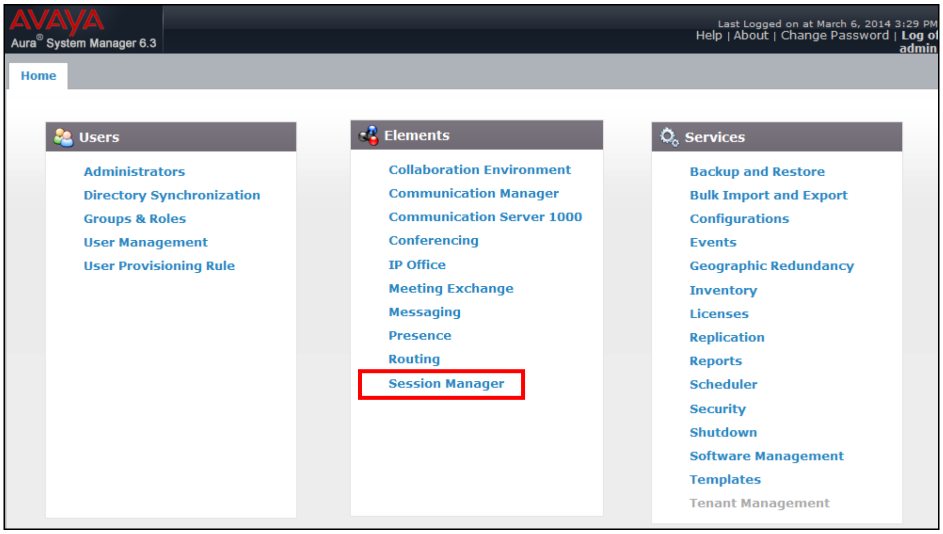
Include video capture: □

8.3. Avaya Aura® Session Manager

The Main and Branch Session Manager configurations may be verified via System Manager.

8.3.1. Session Manager Status

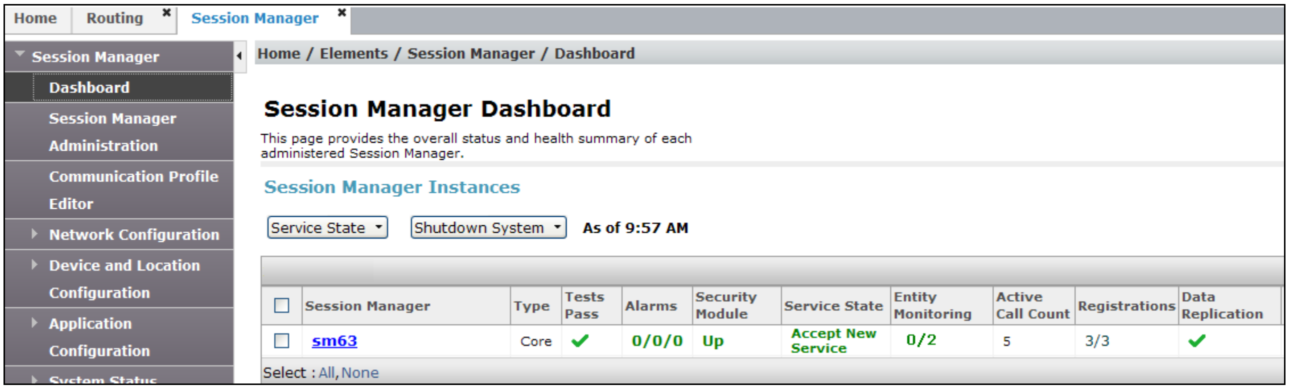
Step 1 – Using the procedures described in **Section 5**, access the System Manager GUI. From the **Home** screen, under the **Elements** heading, select **Session Manager**.



Step 2 – The Session Manager Dashboard is displayed. In the example below, Session Manager instance **sm63** is displayed.

Note that for Session Manager **sm63**, the **Test Passed**, **Alarms**, **Service State**, and **Data Replication** columns, all show good status.

In the **Entity Monitoring Column**, the Session Manager **sm63** shows that there are **0** (zero) alarms out of the **2** Entities defined.


Home
Routing
Session Manager
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
Home / Elements / Session Manager / Dashboard
Service State
Shutdown System

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

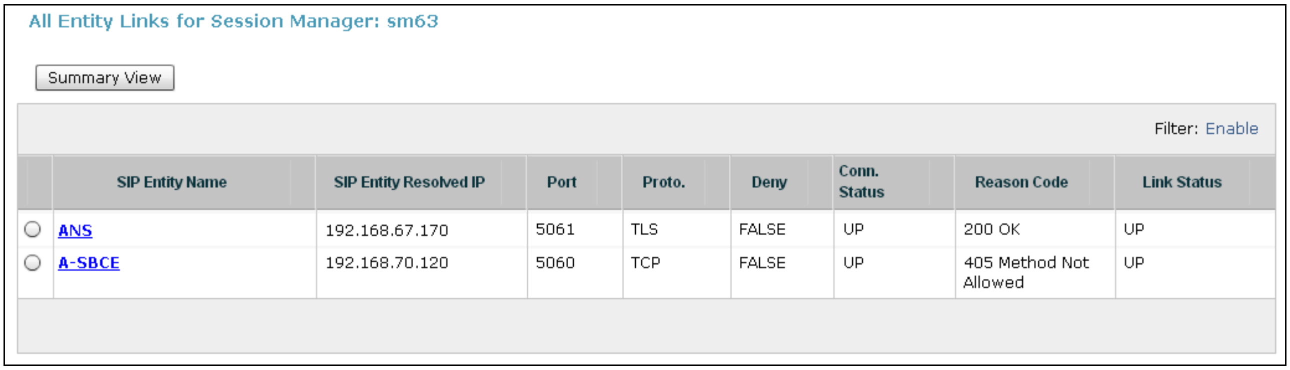
Session Manager Instances

As of 9:57 AM

□	Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication
□	sm63	Core	✓	0/0/0	Up	Accept New Service	0/2	5	3/3	✓

Select : All, None

Step 3 - Clicking on the **0/2** entry in the **Entity Monitoring** column for Session Manager **sm63**, results in the following display.



All Entity Links for Session Manager: sm63

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	ANS	192.168.67.170	5061	TLS	FALSE	UP	200 OK	UP
○	A-SBCE	192.168.70.120	5060	TCP	FALSE	UP	405 Method Not Allowed	UP

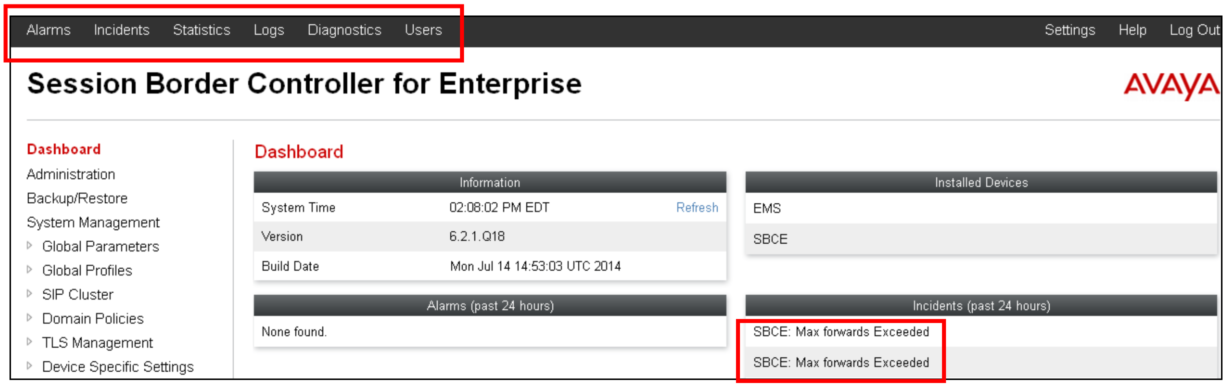
Note - The **A-SBCE** Entity **Reason Code** column indicates that Session Manager has received a SIP **405 Method Not Allowed** response to the SIP OPTIONS it has sent to the Avaya SBCE. The Avaya SBCE sends the Session Manager generated OPTIONS on to the AT&T Border Element. It is the AT&T Border Element that is generating the 405, which the Avaya SBCE sends back to Session Manager. This AT&T response is normal in the reference configuration test environment, and is sufficient for SIP Link Monitoring to consider the link up.

8.4. Avaya Session Border Controller for Enterprise

8.4.1. System Status

Various system conditions monitored by the Avaya SBCE may be displayed as follows.

Step 1 – Log into the Avaya SBCE as shown in **Section 7.2**. Across the top of the display are options to display **Alarms**, **Incidents**, **Logs**, and **Diagnostics**. In addition, the most recent Incidents are listed in the lower right of the screen.



Information	
System Time	02:08:02 PM EDT
Version	6.2.1.Q18
Build Date	Mon Jul 14 14:53:03 UTC 2014

Installed Devices
EMS
SBCE

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
SBCE: Max forwards Exceeded
SBCE: Max forwards Exceeded

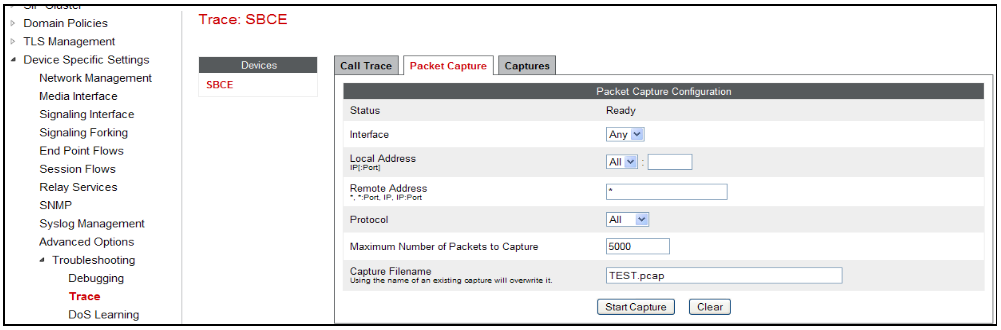
8.4.2. Protocol Traces

The Avaya SBCE can take internal traces of specified interfaces.

Step 1 - Navigate to UC-Sec Control Centre → Troubleshooting → Trace Settings

Step 2 - Select the **Packet Capture** tab and select the following:

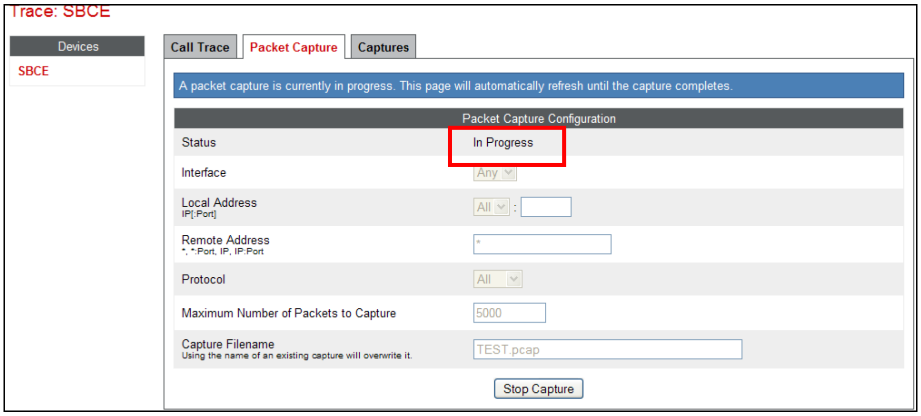
- Select the desired **Interface** from the drop down menu. Selecting **Any** will result in a trace showing activity on both the A1 (inside) and B1 (outside) interfaces.
- Specify the **Maximum Number of Packets to Capture** (e.g., **5000**). Note that the number specified should be a best guess based on the duration of the test.
- Specify a **Capture Filename**.
- Click **Start Capture** to begin the trace.



Trace: SBCE

Packet Capture Configuration	
Status	Ready
Interface	Any
Local Address IP[:Port]	All :
Remote Address *, *:Port, IP, IP:Port	*
Protocol	All
Maximum Number of Packets to Capture	5000
Capture Filename Using the name of an existing capture will overwrite it.	TEST.pcap

The capture process will initialize and then display the following status window. Note that the **Status** will change to **In Progress** when the trace begins, and the screen will begin to refresh.



Trace: SBCE

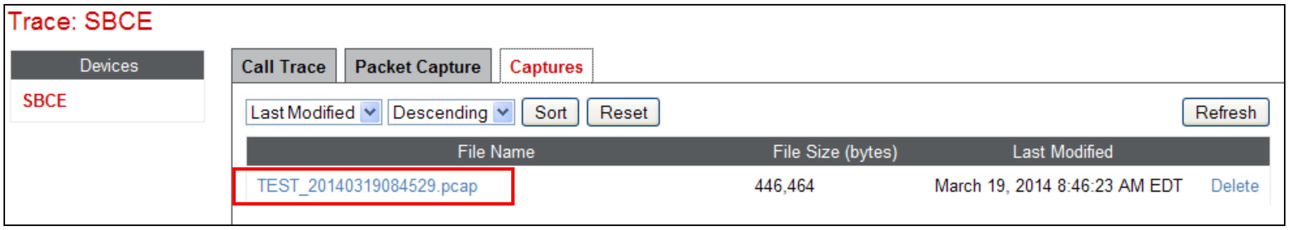
A packet capture is currently in progress. This page will automatically refresh until the capture completes.

Packet Capture Configuration	
Status	In Progress
Interface	Any
Local Address IP[:Port]	All :
Remote Address *, *:Port, IP, IP:Port	*
Protocol	All
Maximum Number of Packets to Capture	5000
Capture Filename Using the name of an existing capture will overwrite it.	TEST.pcap

Step 3 – Run the test. At the conclusion of the test, select the **Stop Capture** button shown above.

Step 5 - Click on the **Captures** tab and the packet capture is listed as a *.pcap* file with the date and time added to filename specified in **Step 2**.

Step 6 - Click on the **File Name** link to download the file and use Wireshark to open the trace.



Trace: SBCE

File Name	File Size (bytes)	Last Modified	
TEST_20140319084529.pcap	446,464	March 19, 2014 8:46:23 AM EDT	Delete

9. Conclusion

As illustrated in these Application Notes, Avaya Notification Solution 2.0, Avaya Aura® Session Manager 6.3, and the Avaya Session Border Controller for Enterprise 6.2.1 can be configured to interoperate successfully with the AT&T IP Flexible Reach - Enhanced Features service, within the limitations described in **Section 2.2**.

The reference 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.

10. References

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

Avaya Notification Solution

[1] **Avaya Notification Solution Installation and Administration guide,** Release 2.0.1, January 2013

[2] **Avaya Notification Solution Operations guide,** Release 2.0, July 2012

Avaya Aura® Session Manager/System Manager

[3] **Administering Avaya Aura® Session Manager,** Release 6.3, Issue 3, October 2013

[4] **Administering Avaya Aura® System Manager,** Release 6.3, Issue 3, October 2013

Avaya Session Border Controller for Enterprise

[5] **Installing Avaya Session Border Controller for Enterprise,** Release 6.2, Issue 3, June 2013

[6] **Administering Avaya Session Border Controller for Enterprise,** Release 6.2, Issue 2, January 2014

AT&T IP Flexible Reach-Enhanced Features Service Descriptions:

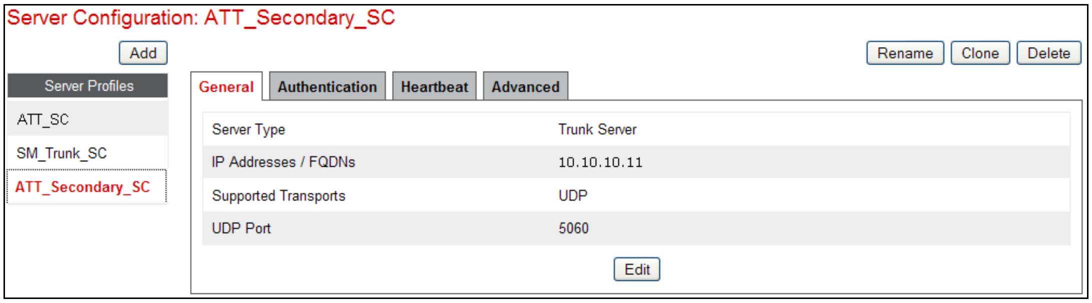
[7] AT&T IP Flexible Reach - Enhanced Features Service description - http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ip-flexible-reach-enterprise/

11. Addendum 1 – Redundancy to Multiple AT&T Border Elements

The AT&T IPFR-EF service may provide multiple network Border Elements for redundancy purposes. The Avaya SBCE can be provisioned to support this redundant configuration. Given two AT&T Border Elements **10.10.10.10** and **10.10.10.11** (see the note in **Section 3.1**) the Avaya SBCE is provisioned as follows to include the secondary trunk connection to 10.10.10.11 (the primary AT&T trunk connection to 10.10.10.10 is defined in **Section 7.3.6**).

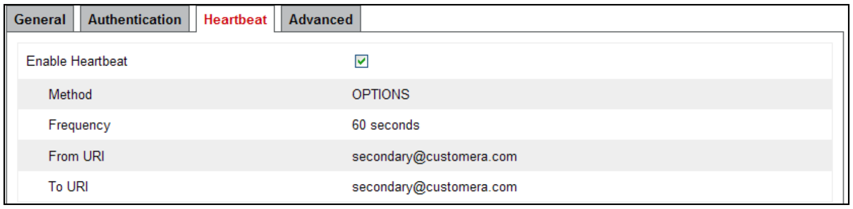
11.1. Configure the Secondary Location in Server Configuration

1. Select **Global Profiles → Server Configuration** from the menu on the left (not shown).
2. Select **Add Profile**
   a) **Name: ATT_Secondary_SC.**
   b) On the **General** tab , select **Server Type: Trunk Server**
   c) **IP Address: 10.10.10.11** (sample address for a secondary location).
   d) **Supported Transports**: Check **UDP** and **UDP Port: 5060.**
   e) Select **Finish** (not shown). The completed **General** tab is shown below.



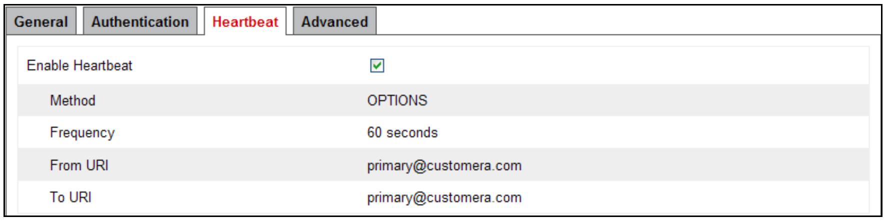
Server Type	Trunk Server
IP Addresses / FQDNs	10.10.10.11
Supported Transports	UDP
UDP Port	5060

3. On the **Authentication** tab:
   a) Select **Next** (not shown)
4. On the **Heartbeat** tab:
   a) Check **Enable Heartbeat.**
   b) **Method: OPTIONS.**
   c) **Frequency:** As desired (e.g., 60 seconds).
   d) **From URI** and **To URI : secondary@customera.com.**
   e) Select **Next** (not shown).
5. On the **Advanced** Tab:
   a) Click **Finish** (not shown). The completed Heartbeat tab is shown below.



Enable Heartbeat	☑
Method	OPTIONS
Frequency	60 seconds
From URI	secondary@customera.com
To URI	secondary@customera.com

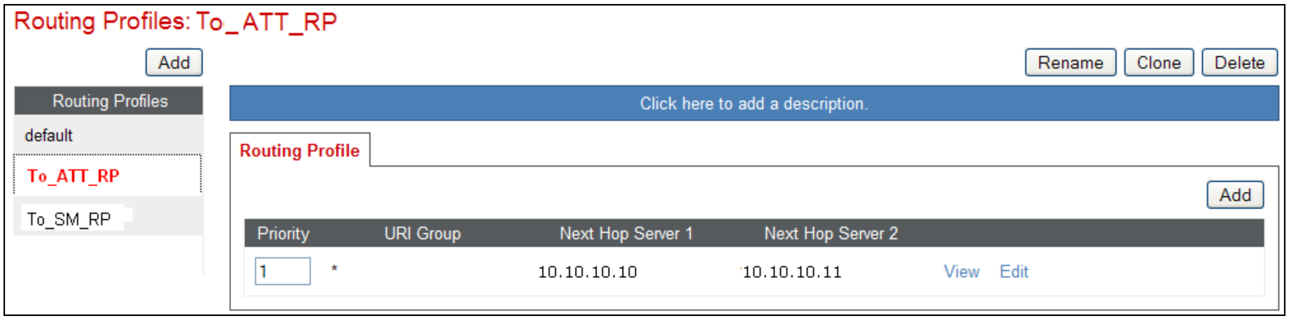
6. Select the **Server Configuration** created in **Section 7.3.6** (e.g., **ATT_ SC**).
7. Select the **Heartbeat Tab** and select **Edit.**
8. Repeat **Steps 6 – 7,** using the information shown below, and then click **Finish** (not shown).



Enable Heartbeat	☑
Method	OPTIONS
Frequency	60 seconds
From URI	primary@customera.com
To URI	primary@customera.com

11.2. Add Secondary IP Address to Routing

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Routing.**
3. Select the routing profile created in **Section 7.3.4** (e.g., **To_ATT _RP**).
4. Click the pencil icon at the end of the line to edit (not shown).
   a) Enter the IP Address of the secondary location in the **Next Hop Server 2** (e.g., **10.10.10.11**).
5. Click **Finish** (not shown).



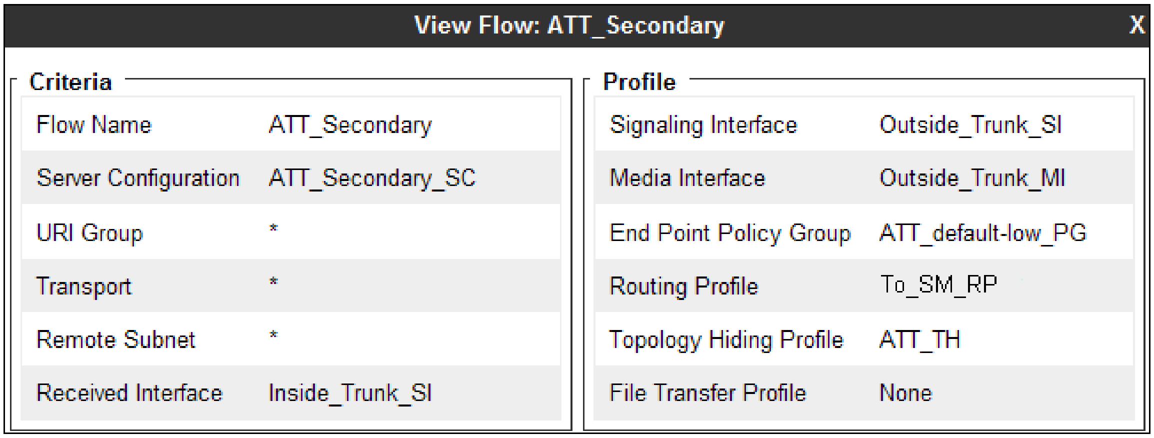
Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	*	10.10.10.10	10.10.10.11	View Edit

11.3. Configure End Point Flows – Server Flow - ATT_Secondary

1. Select **Device Specific Settings** from the menu on the left-hand side.
2. Select **Endpoint Flows.**
3. Select the **Server Flows** Tab.
4. Select **Add Flow:**
   a) **Name: ATT_Secondary.**
   b) **Server Configuration: ATT_Secondary _SC.**
   c) **URI Group: *.**
   d) **Transport: *.**
   e) **Remote Subnet: *.**
   f) **Received Interface: Inside_Trunk_SI** (**Section 7.5.4**).
   g) **Signaling Interface: Outside_Trunk_ SI** (**Section 7.5.4**).
   h) **Media Interface: Outside_trunk_MI** (**Section 7.5.3**).
   i) **End Point Policy Group**: **ATT_default-low_PG** (**Section 7.4.5**).

j) **Routing Profile: To_SM _RP** (**Section 7.3.3**).
k) **Topology Hiding Profile: ATT_TH** (**Section 7.3.8**).
l) **File Transfer Profile: None.**

5. Click **Finish** (not shown).



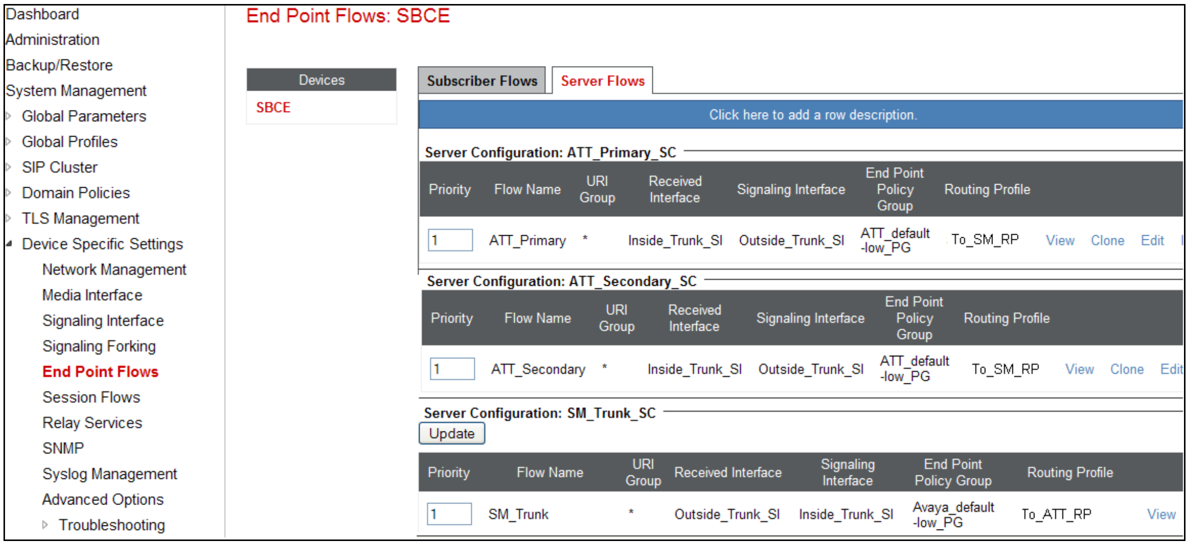
View Flow: ATT_Secondary

Criteria

Flow Name	ATT_Secondary
Server Configuration	ATT_Secondary_SC
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Inside_Trunk_SI

Profile

Signaling Interface	Outside_Trunk_SI
Media Interface	Outside_Trunk_MI
End Point Policy Group	ATT_default-low_PG
Routing Profile	To_SM_RP
Topology Hiding Profile	ATT_TH
File Transfer Profile	None



End Point Flows: SBCE

Server Configuration: ATT_Primary_SC

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile			
1	ATT_Primary	*	Inside_Trunk_SI	Outside_Trunk_SI	ATT_default -low_PG	To_SM_RP	View	Clone	Edit

Server Configuration: ATT_Secondary_SC

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile			
1	ATT_Secondary	*	Inside_Trunk_SI	Outside_Trunk_SI	ATT_default -low_PG	To_SM_RP	View	Clone	Edit

Server Configuration: SM_Trunk_SC

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SM_Trunk	*	Outside_Trunk_SI	Inside_Trunk_SI	Avaya_default -low_PG	To_ATT_RP	View

When completed, the Avaya SBCE will issue OPTIONS messages to the primary (10.10.10.10) and secondary (10.10.10.11) Border Elements.

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.