Application Notes for Syn-Apps' SA-Announce with Avaya 9600 Series IP Deskphones – Issue 1.0

Abstract

These Application Notes describe a compliance-tested configuration consisting Avaya 9600 Series IP Deskphones and Syn-Apps SA-Announce.

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

1. Introduction

Syn-Apps' SA-Announce is an enhanced paging and mass notification solution that integrates with Avaya Aura and Avaya 9600 Series Deskphones; providing audio, text and graphic notifications across an organization. SA-Announce delivers real-time, pre-recorded or scheduled announcements to streamline critical situation communication and many operational processes.

Avaya 9600 Series IP Deskphones subscribe to Syn-Apps SA-Announce, to receive XML-based data pushed by SA-Announce. The data that is pushed by SA-Announce is in the form of Alerts. In addition, SA-Announce has the ability to send Multicast audio to Avaya 9600 Series IP Deskphones.

2. General Test Approach and Test Results

The compliance test focused on the interoperability between Avaya 9600 Series IP Deskphones and Syn-Apps SA-Announce.

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

2.1. Interoperability Compliance Testing

Compliance testing focused on receiving various types of Alerts and Notifications sent by SA-Announce to Avaya 9600 Series IP Deskphones. The following Alert Types were tested during Compliance test:

- Weather Alerts
- Amber Alerts
- Emergency Alerts
- RecordNPlay Notifications

Only Avaya 9600 Series H.323 phones were included in the test. Avaya 9600 Series SIP phones were not included due to the lack of support for Multicast audio. The following models were tested:

- 9611
- 9620
- 9621
- 9630
- 9640
- 9641
- 9670

2.2. Test Results

All executed test cases were passed and all objectives were met.

2.3. Support

Syn-Apps support can be contacted in the following ways:

Phone: 866-664-6071**Email**: support@syn-apps.com
Web Form: http://www.syn-apps.com/support/request/

3. Reference Configuration

Figure 1below displays a sample configuration that was tested during the compliance test.

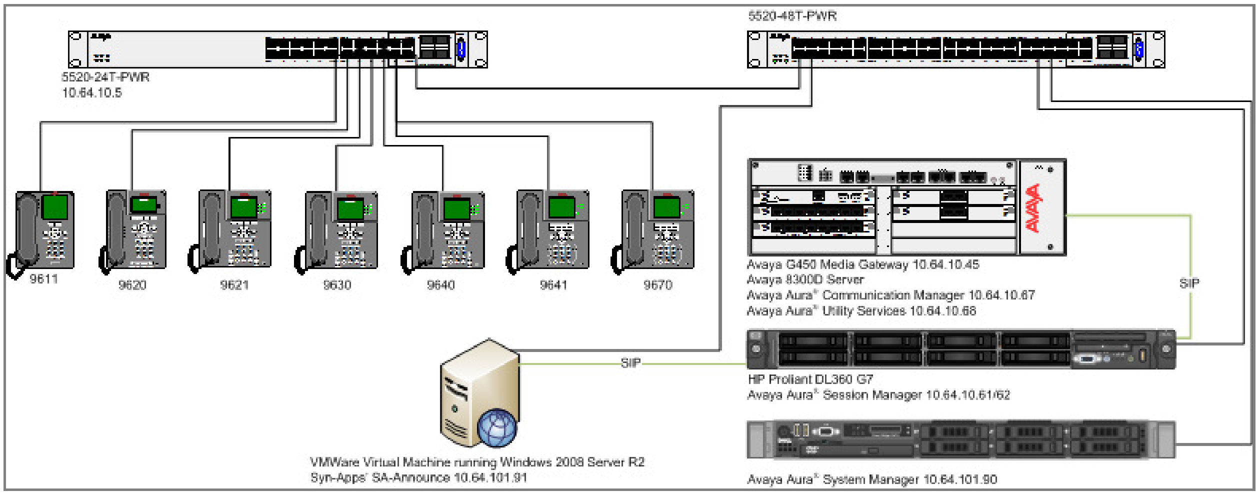

5520-48T-PWR
5520-24T-PWR
10.64.10.5
9611
9620
9621
9630
9640
9641
9670
Avaya G450 Media Gateway 10.64.10.45
Avaya 8300D Server
Avaya Aura® Communication Manager 10.64.10.67
Avaya Aura® Utility Services 10.64.10.68
SIP
SIP
HP Proliant DL360 G7
Avaya Aura® Session Manager 10.64.10.61/62
VMWare Virtual Machine running Windows 2008 Server R2
Syn-Apps' SA-Announce 10.64.101.91
Avaya Aura® System Manager 10.64.101.90

Figure 1: Reference Configuration

4. Equipment and Software Validated

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

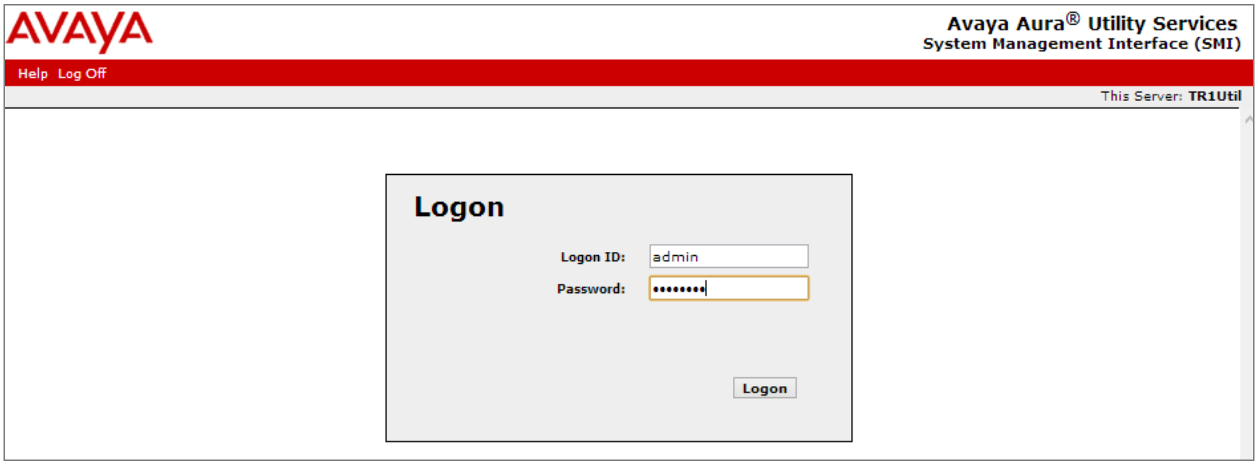
Equipment	Version
Avaya Aura® System Manager running on VMware EXSi 5.1 infrastructure	R6.2.12 Build 6.2.0.0.15669-6.2.12.408
Avaya Aura® Session Manager running on HP Proliant DL360 G7 server	6.2.3.0.622006
Avaya Aura® Communication Manager running on Avaya 8300D server	R6.2 build R016x.02.0.823.0
Avaya G450 Media Gateway	31.20.1
Avaya 96x1 Series H.323 Phones Avaya 96x0 Series H.323 Phones	6.2.4 3.10
Avaya Aura® Utility Services	6.2.0.0.15
Syn-Apps SA-Announce running on a Windows Server2008 R2 VMWare Virtual Machine	9.0.10

5. Configure Avaya Aura® Utility Server

Avaya 9600 Series IP Deskphones settings are controlled by 46xxsettings.txt file that is downloaded and parsed each time a phone resets/reboots. In order to interact with the phones, SA-Announce has to be "trusted" by the phones and the phones need to "subscribe" to SA-Announce. Furthermore, in order for a phone to receive and display content on the screen from a remote source, it needs to be configured for WML (Wireless Mark-up Language).

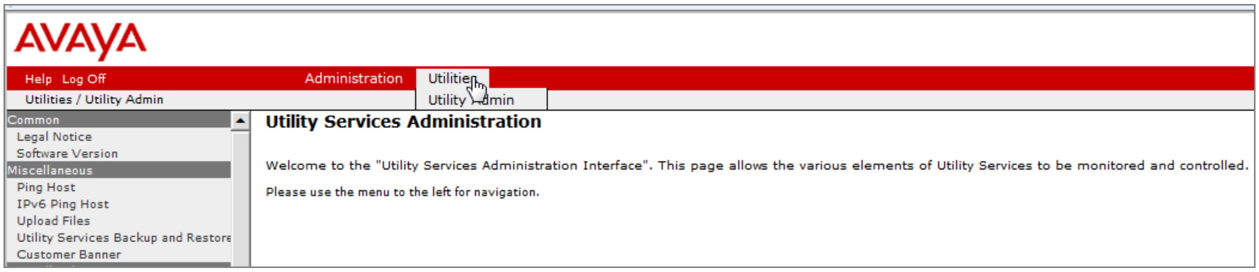
In the Interoperability Lab, Avaya Aura® Utility Server is used to manage Avaya 9600 Series IP Deskphones. All changes to the 46xxsetting.txt are made via Avaya Aura® Utility Services System Management Interface (SMI). Utility Service SMI can be reached via a web browser, http://<ip-address>/admin.html, where ip-address is the IP Address of Avaya Aura® Utility Services.

On the logon page, log in using appropriate credentials.


Avaya Aura® Utility Services
System Management Interface (SMI)
Help Log Off
This Server: TR1Util
Logon

Logon ID: admin
Password: ••••••••

Once logged in, navigate to **Utilities → Utilities Admin**.

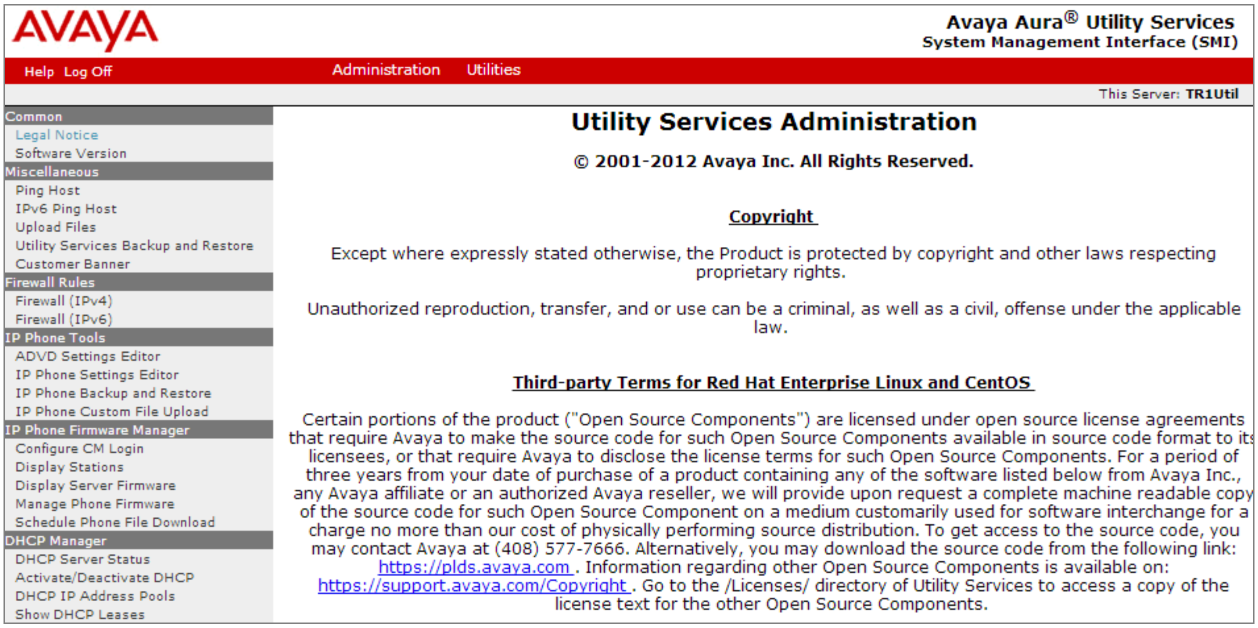


Utility Services Administration

Welcome to the "Utility Services Administration Interface". This page allows the various elements of Utility Services to be monitored and controlled.

Please use the menu to the left for navigation.

Then, navigate to **IP Phone Tools → IP Phone Settings Editor.**



Utility Services Administration

© 2001-2012 Avaya Inc. All Rights Reserved.

Copyright

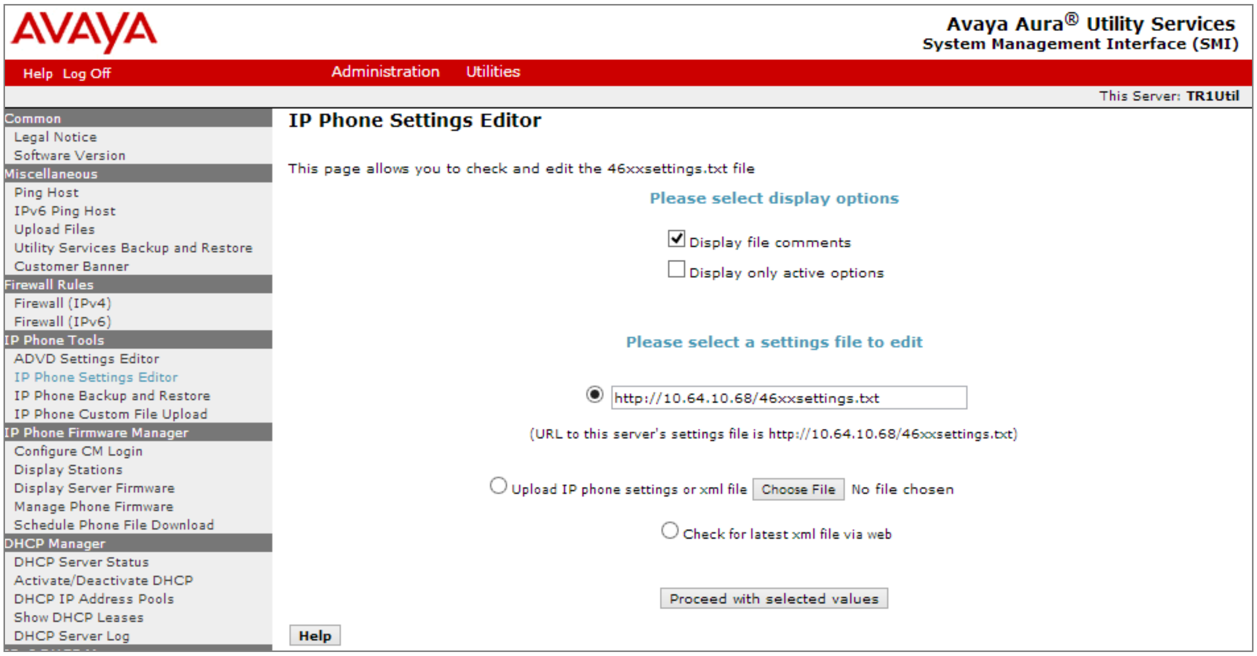
Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party Terms for Red Hat Enterprise Linux and CentOS

Certain portions of the product ("Open Source Components") are licensed under open source license agreements that require Avaya to make the source code for such Open Source Components available in source code format to its licensees, or that require Avaya to disclose the license terms for such Open Source Components. For a period of three years from your date of purchase of a product containing any of the software listed below from Avaya Inc., any Avaya affiliate or an authorized Avaya reseller, we will provide upon request a complete machine readable copy of the source code for such Open Source Component on a medium customarily used for software interchange for a charge no more than our cost of physically performing source distribution. To get access to the source code, you may contact Avaya at (408) 577-7666. Alternatively, you may download the source code from the following link: https://plds.avaya.com . Information regarding other Open Source Components is available on: https://support.avaya.com/Copyright . Go to the /Licenses/ directory of Utility Services to access a copy of the license text for the other Open Source Components.

On the **IP Phone Settings Editor**, Select **Proceed with Selected Values**.



IP Phone Settings Editor

This page allows you to check and edit the 46xxsettings.txt file

Please select display options

☑ Display file comments

□ Display only active options

Please select a settings file to edit

● http://10.64.10.68/46xxsettings.txt

(URL to this server's settings file is http://10.64.10.68/46xxsettings.txt)

○ Upload IP phone settings or xml file Choose File No file chosen

○ Check for latest xml file via web

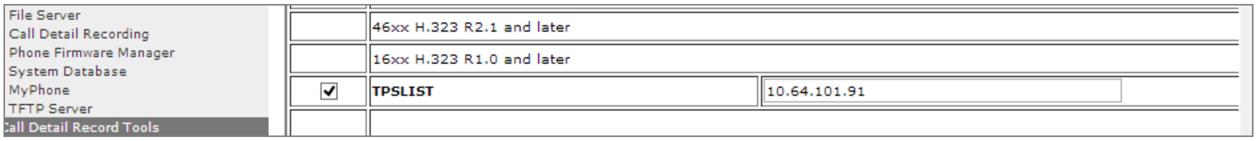
Enable the following options by selecting the check box in front of the options and setting their fields as follows:

- **TPSLIST**: Set it to the IP Address of SA-Announce server
- **SUBSCRIBELIST**: Set it to the following URL
    - http://<ip-address>/SA-Announce/PhoneServices/AvayaPhoneRegistration.aspx

Note: ip-address is the IP Address of SA-Announce server

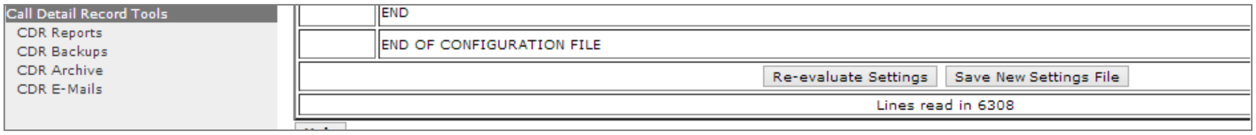
- **WMLHOME**: Configure with a suitable URL as a home page
- **PUSHCAL**: Set it to 22222

Below is a screen capture of configuring TPSLIST, other options are not shown.



	46xx H.323 R2.1 and later	
	16xx H.323 R1.0 and later	
☑	TPSLIST	10.64.101.91

Once done, select **Save New Setting File** at the bottom of the page.

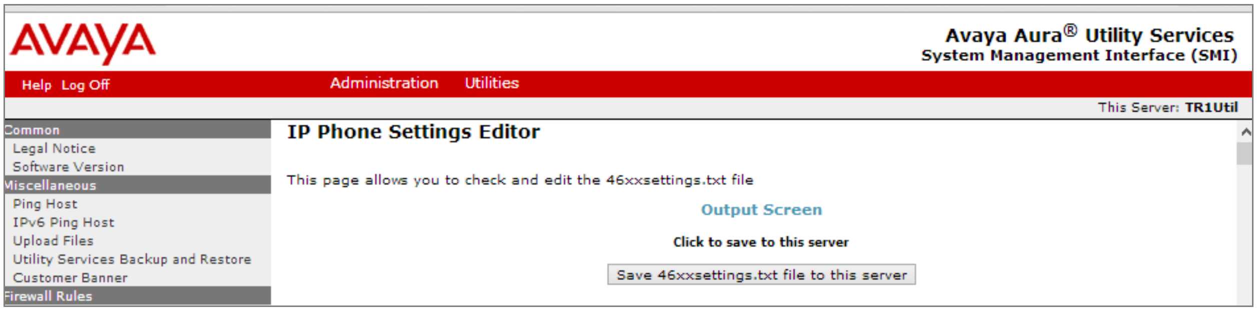


END

END OF CONFIGURATION FILE

Lines read in 6308

Verify the values of the options above on the **Output Screen**, and select **Save 46xxsetting.txt file to this server**.

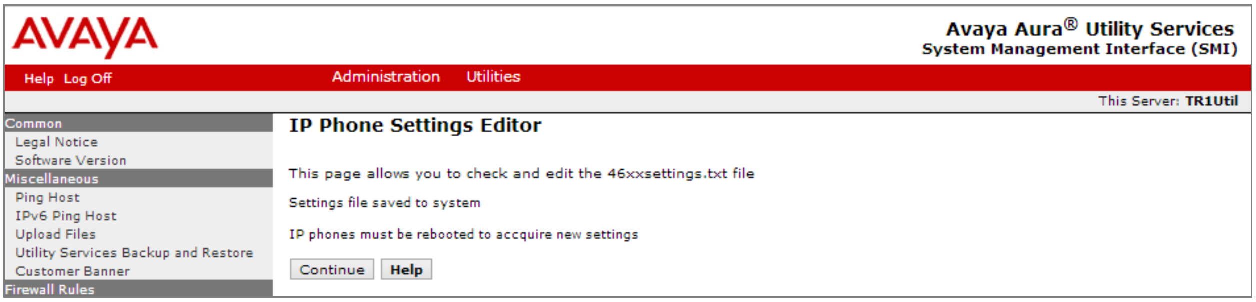


IP Phone Settings Editor

This page allows you to check and edit the 46xxsettings.txt file

Click to save to this server

On the next page, select **Continue**.



IP Phone Settings Editor

This page allows you to check and edit the 46xxsettings.txt file

Settings file saved to system

IP phones must be rebooted to accquire new settings

Reboot the Avaya 9600 Series IP Deskphones to update the settings.

6. Configure Avaya Aura® Communication Manager

Avaya Aura® Communication Manager allows for routing calls to SA-Announce via Avaya Aura® Session Manager using SIP trunks. In order for Avaya 9600 Series IP Deskphones to be able to dial a number to activate a SA-Announce group, a SIP trunk must be created that communicates with Session Manager. Another SIP trunk will be created on Session Manager to communicate to SA-Announce. The following information allows for a SIP connection between the Communication Manager and Session Manager.

6.1. Configure IP Network Region

Use the **change ip-network-region *n*** command to configure a network region, where ***n*** is an existing network region. Configure this network region as follows:

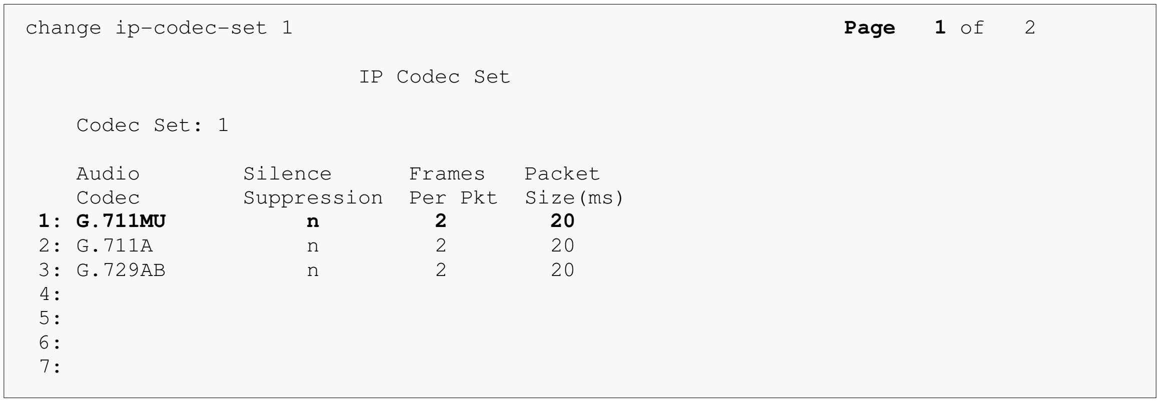
- Set **Location** to **1**
- Set **Codec Set** to **1**
- Set **Intra-region IP-IP Direct Audio** to **yes**
- Set **Inter-region IP-IP Direct Audio** to **yes**
- Enter and **Authoritative Domain**, e.g. avaya.com

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

6.2. Administer IP Codec Set

Use the **change ip-codec-set *n*** command to configure IP codec set, where ***n*** is an existing codec set number. Configure this codec set as follows, on **Page 1**:

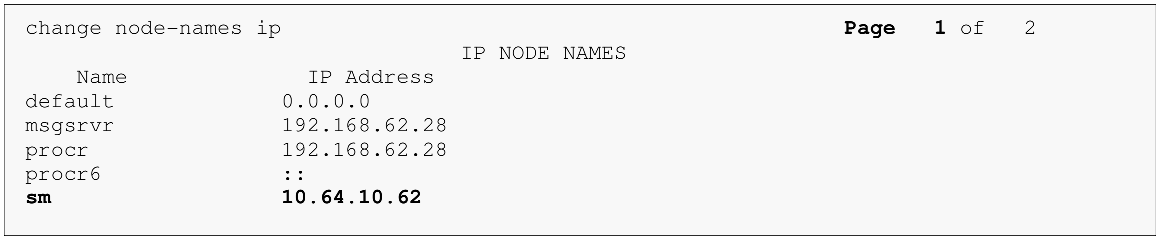
- Set **Audio Codec 1** to **G.711MU**



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

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU          n          2        20
 2: G.711A           n          2        20
 3: G.729AB          n          2        20
 4:
 5:
 6:
 7:
```

6.3. Administer IP Node Names

Use the **change node-names ip** command to add an entry for Session Manager. For compliance testing, **sm** and **10.64.10.62** entry was added.

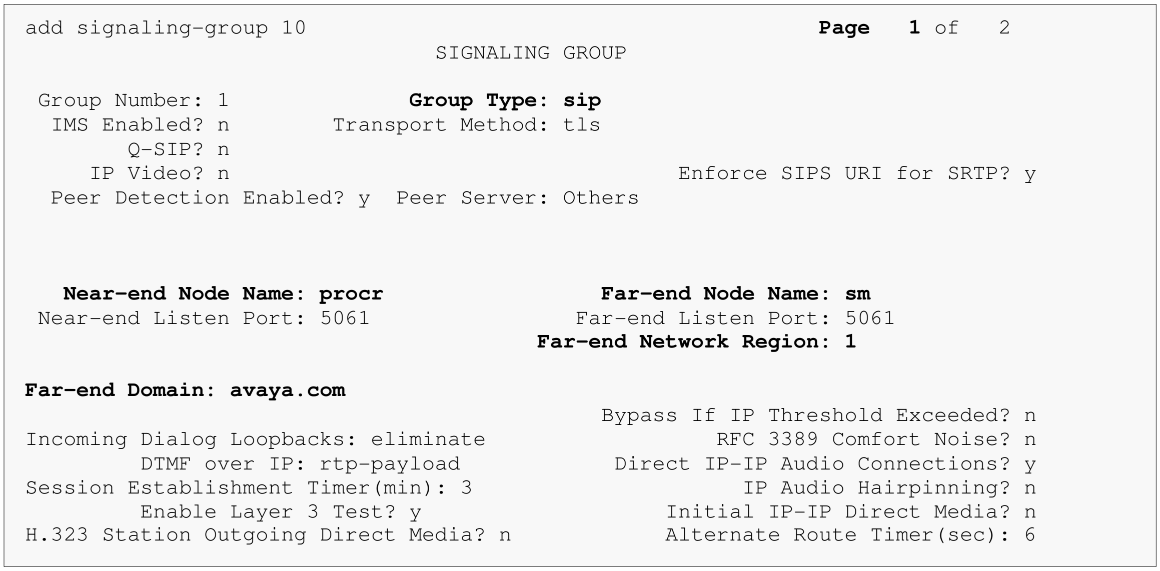


```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
default             0.0.0.0
msgsrvr             192.168.62.28
procr               192.168.62.28
procr6              ::
sm                  10.64.10.62
```

6.4. Administer SIP Signaling Group

Use the **add signaling-group *n*** command to add a new signaling group, where ***n*** is an available signaling group number. Configure this signaling group as follows:

- Set **Group Type** to **sip**
- Set **Near-end Node Name** to **procr**
- Set **Far-end Node Name** to the configured Session Manager in **Section 6.3**, i.e. sm
- Set **Far-end Network region** to the configured region in **Section 6.1**, i.e. 1
- Enter a **Far-end Domain,** e.g. avaya.com

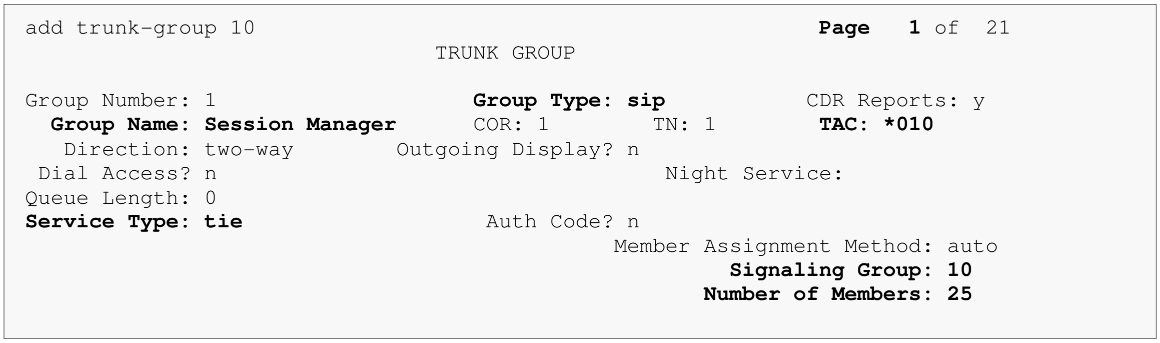


```
add signaling-group 10                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: Others



   Near-end Node Name: procr                 Far-end Node Name: sm
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1

Far-end Domain: avaya.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

6.5. Administer SIP Trunk Group

Use the **add trunk-group *n*** command to add a trunk group, where ***n*** is an available trunk group number. Configure this trunk group as follows, on **Page 1**:

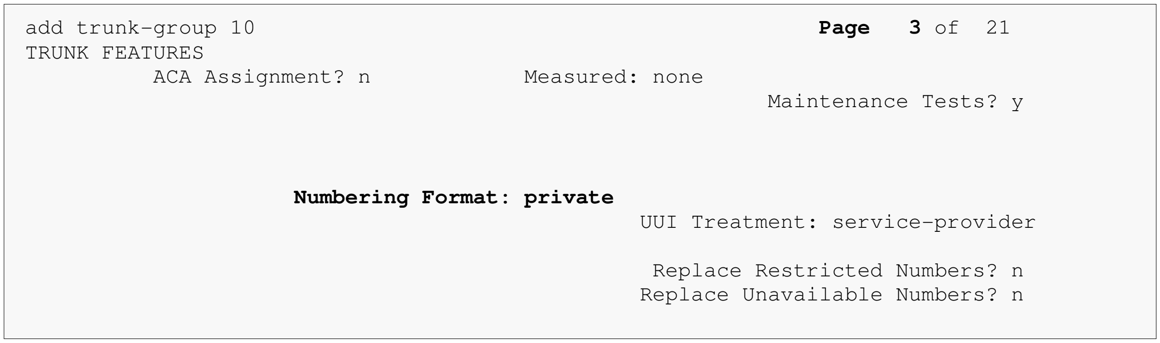
- Set **Group Type** to **sip**
- Enter a **Group Name**
- Enter a valid **TAC**, e.g. *010
- Set **Service Type** to **tie**
- Enter **Signaling Group** value to the signaling group configured in **Section 6.4**, i.e. 10
- Enter a desired number in **Number of Members** field



```
add trunk-group 10                                             Page   1 of  21
                                TRUNK GROUP

Group Number: 1                   Group Type: sip          CDR Reports: y
  Group Name: Session Manager      COR: 1        TN: 1        TAC: *010
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n
                                            Member Assignment Method: auto
                                                     Signaling Group: 10
                                                   Number of Members: 25
```

On **Page 3**:

- Set **Number Format** to private



```
add trunk-group 10                                             Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
```

6.6. Administer Route Pattern

Use the **change route-pattern *n*** command to configure a route pattern, where ***n*** is an available route patterns. Configure this route pattern as follows:

- Type a name in **Pattern Name** field
- For line 1, set **Grp No** to the trunk group configured in **Section 6.5**, i.e. 10
- For line 1, set **FRL** to **0**

```
change route-pattern 10                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: Voice and Fax
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 10   0                                                              n   user
 2:                                                                     n   user
```

6.7. Administer AAR Analysis

Use the **change aar analysis *n*** command to configure routing for extensions starting with ***n***. For compliance testing, extensions starting with 26 were used to route calls to SA-Announce:

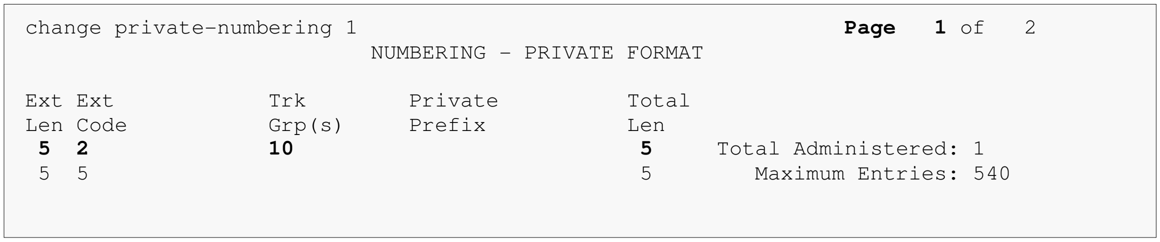
- Set **Dialed String** to starting digits of extensions that will be used, e.g. 26
- Set **Min** and **Max** to 5 for 5 digit extensions
- Set **Route Pattern** to pattern configured in **Section 6.6**, i.e. 10
- Set **Call Type** to **aar**

```
change aar analysis 26                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 1

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    26                    5    5     10       aar          n
    27                    5    5     21       aar          n
    275                   5    5     10       aar          n
    29                    5    5     10       aar          n
    3                     7    7     254      aar          n
    4                     5    5     2        aar          n
    45000                 5    5     30       aar          n
    5                     5    5     32       aar          n
```

6.8. Administer Private Numbering

Use the **change private-numbering 1** command to define the calling party number to send to Session Manager.
Configure private numbering as follows:

- During the compliance test, extensions starting with 2 and were 5 digits long were used; calls from these extension were made to SA-Announce via trunk group configured in **Section 6.5.**



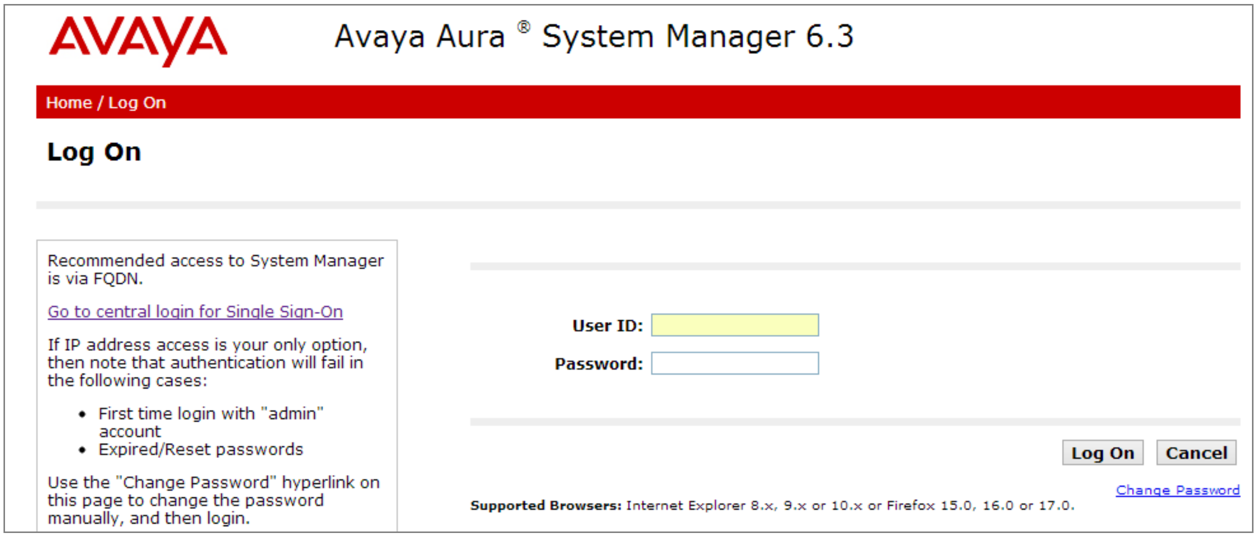
```
change private-numbering 1                                     Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext              Trk        Private          Total
Len Code             Grp(s)     Prefix           Len
 5  2                10                           5     Total Administered: 1
 5  5                                             5        Maximum Entries: 540
```

6.9. Administer Dial Plan Analysis and Stations

Administration of Dial Plan Analysis and Avaya Stations/Extensions in Communication Manager is not shown in this document. Please refer to document [1] in reference section of this document.

7. Configure Avaya Aura® Session Manager

Access the Session Manager Administration web interface by entering https://<ip-address>/SMGR URL in a web browser, where <ip-address> is the IP address of System Manager. Log in using appropriate credentials.



Avaya Aura ® System Manager 6.3

Home / Log On

Log On

Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

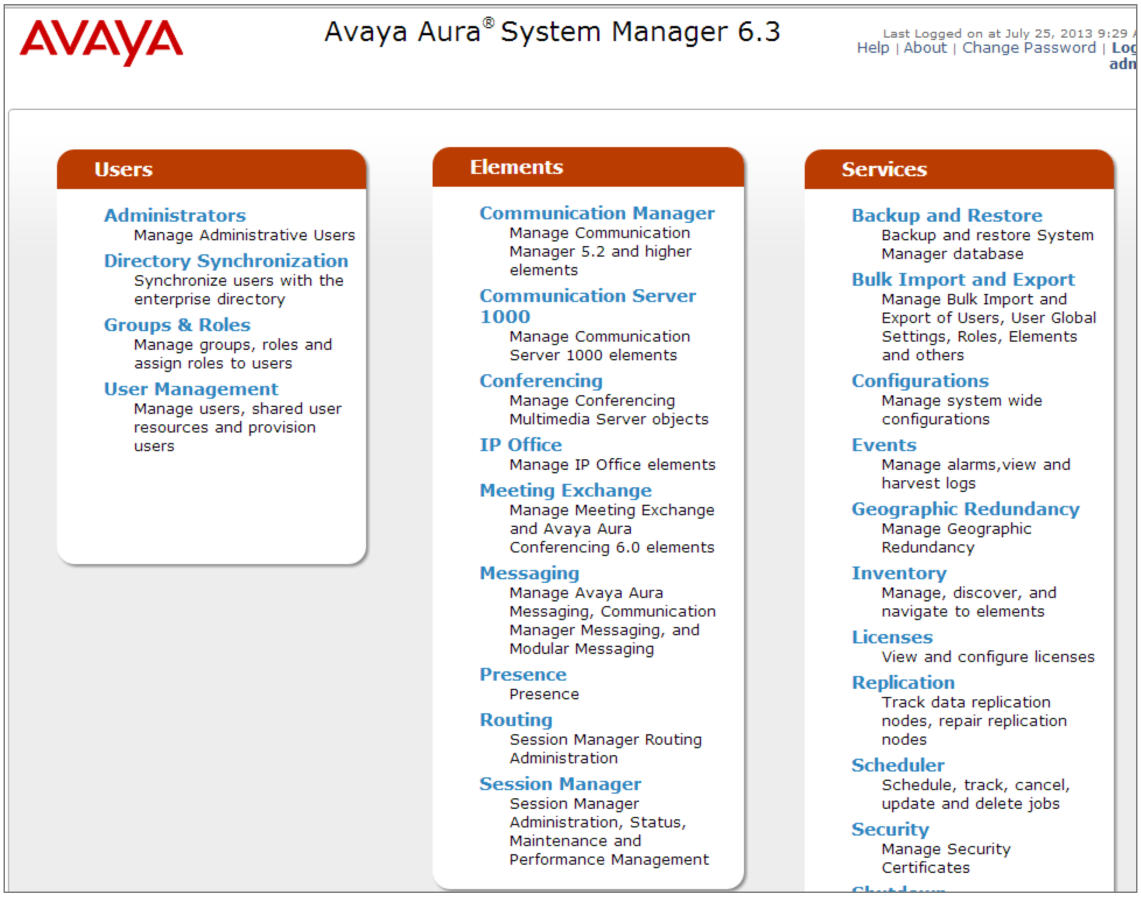
Use the "Change Password" hyperlink on this page to change the password manually, and then login.

User ID:

Password:

Supported Browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 15.0, 16.0 or 17.0.

Once logged in, the dashboard is displayed.



Avaya Aura® System Manager 6.3

Last Logged on at July 25, 2013 9:29

Help | About | Change Password | Log

adn

Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the enterprise directory

Groups & Roles
Manage groups, roles and assign roles to users

User Management
Manage users, shared user resources and provision users

Elements

Communication Manager
Manage Communication Manager 5.2 and higher elements

Communication Server 1000
Manage Communication Server 1000 elements

Conferencing
Manage Conferencing Multimedia Server objects

IP Office
Manage IP Office elements

Meeting Exchange
Manage Meeting Exchange and Avaya Aura Conferencing 6.0 elements

Messaging
Manage Avaya Aura Messaging, Communication Manager Messaging, and Modular Messaging

Presence
Presence

Routing
Session Manager Routing Administration

Session Manager
Session Manager Administration, Status, Maintenance and Performance Management

Services

Backup and Restore
Backup and restore System Manager database

Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Geographic Redundancy
Manage Geographic Redundancy

Inventory
Manage, discover, and navigate to elements

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

Scheduler
Schedule, track, cancel, update and delete jobs

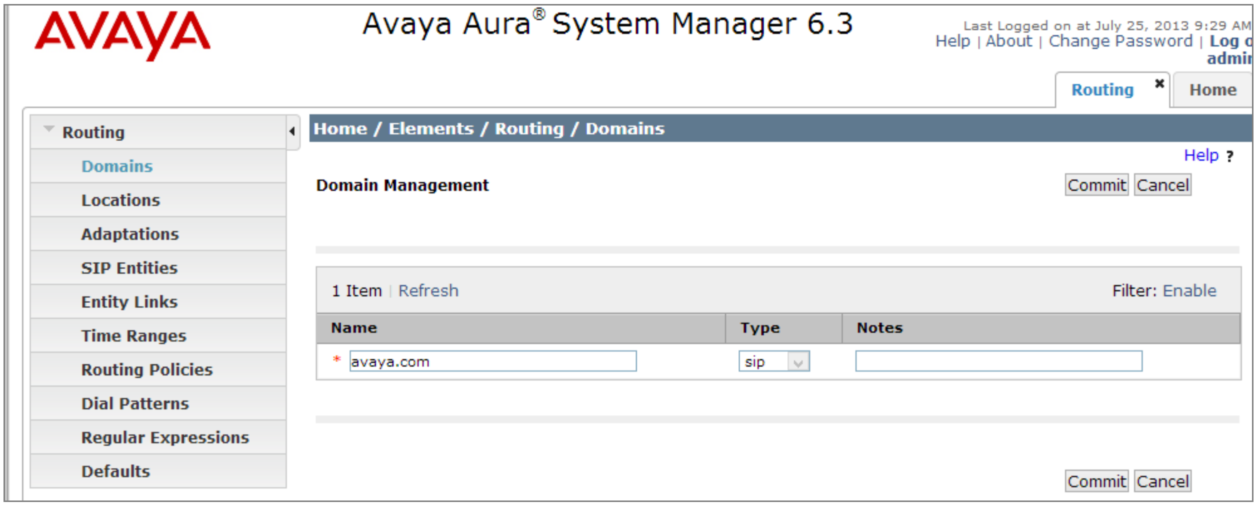
Security
Manage Security Certificates

7.1. Add SIP Domain

Navigate to **Home → Elements → Routing → Domains**, click on **New** button (not shown) and configure as follows:

- In **Name** field type in a domain (authoritative domain used in **Section 6.1**) i.e. avaya.com
- Set **Type** to **sip**

Click **Commit** to save changes.



Domain Management

Name	Type	Notes
* avaya.com	sip	

7.2. Add Location

Navigate to **Home → Elements → Routing → Location**, click on **New** button (not shown) and configure as follows:

Under **General**:

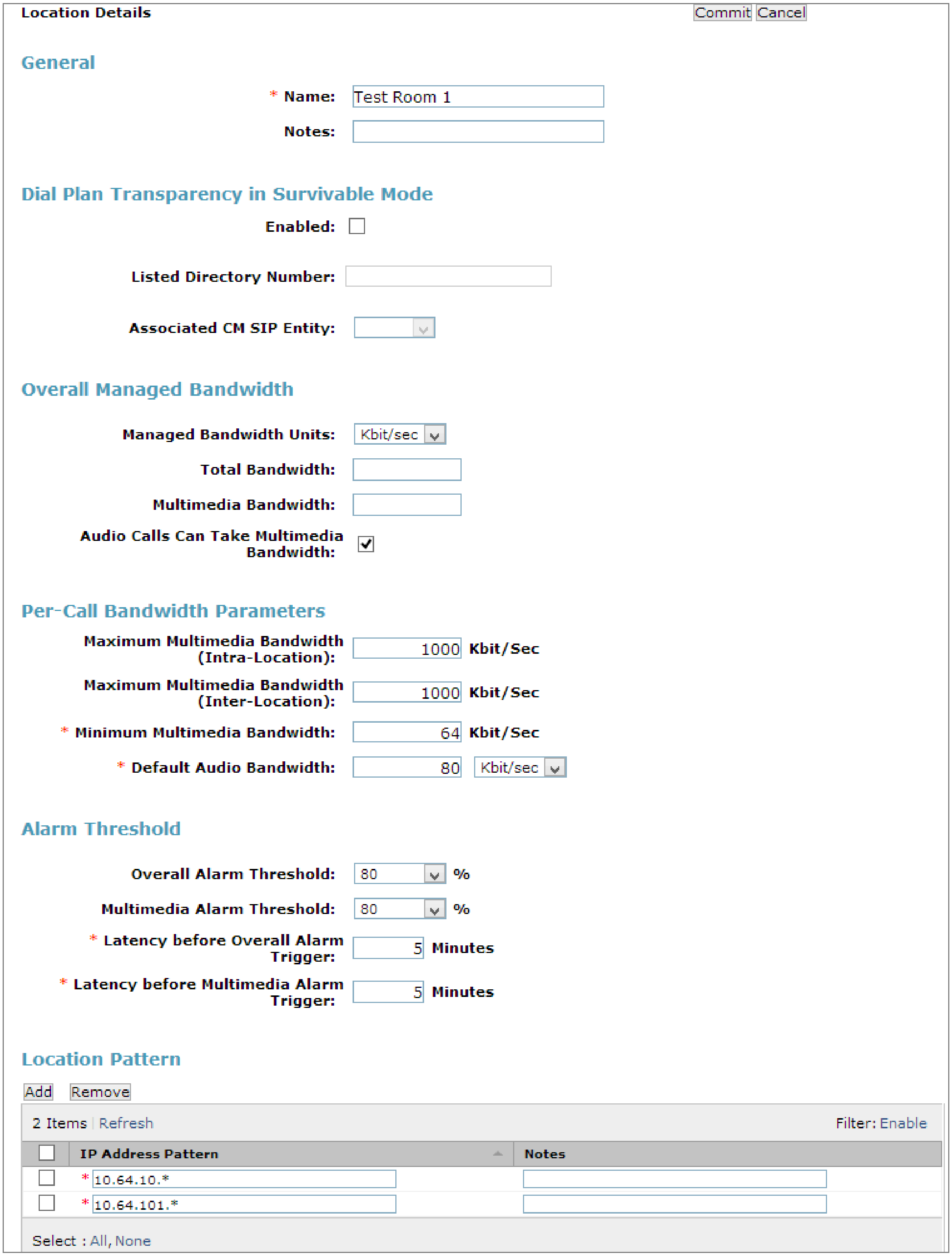
- Type in a descriptive **Name**

Under **Location Pattern** click on **Add** (not shown):

- Type in an **IP Address Pattern**, e.g. 10.64.10.*

Note: During compliance test, IP addresses in 10.64.10.* and 10.64.101.* were used. Also, the "*" refers to wildcard indicating a range.

Click **Commit** to save changes. Screen shot shown on next page.



Location Details

General

* Name: Test Room 1

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

2 Items | Refresh Filter: Enable

□	IP Address Pattern	Notes
□	* 10.64.10.*	
□	* 10.64.101.*	

Select : All, None

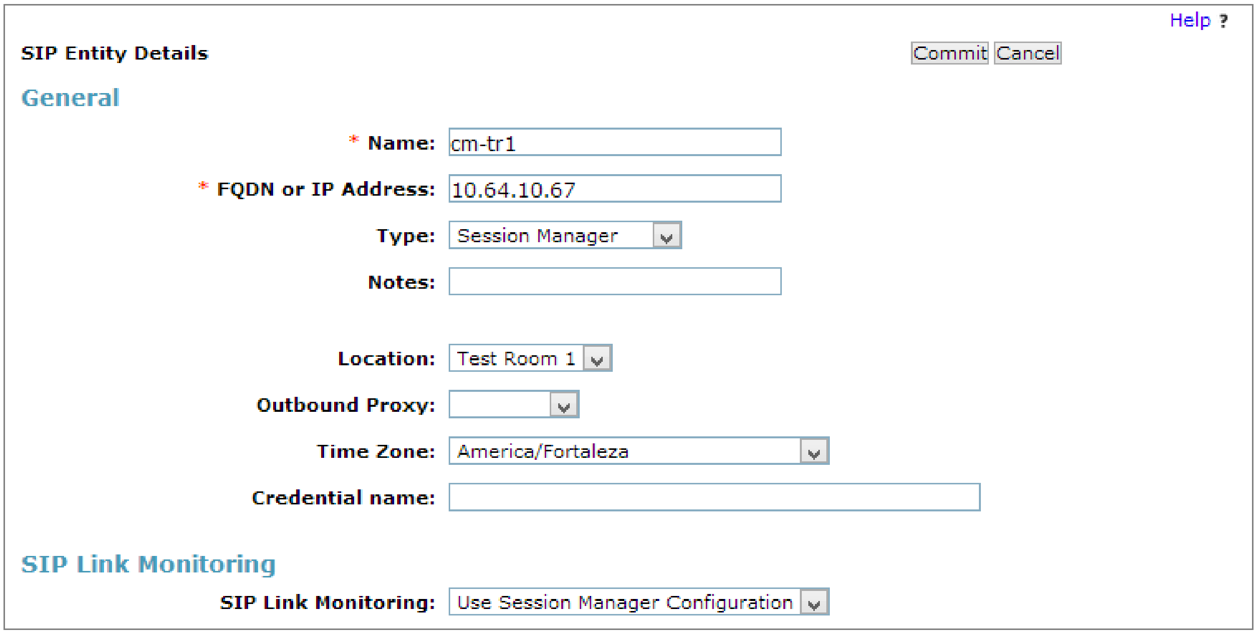
7.3. Add SIP Entity – Communication Manager

Each SIP device that communicates with the Session Manager over a SIP trunk, requires a SIP Entity configuration. Add Communication Manager as a SIP Entity. Navigate to **Home → Elements → Routing → SIP Entities,** click on **New** (no shown) and configure as follows:

- Type in a descriptive name in **Name** field
- Type in the FQDN or IP address of the Communication Manager in **FQDN or IP Address** field.
- Set **Type** to **CM**
- Set **Location** to the location configured in **Section 7.2**

Click **Commit** to save changes.

Note: It is assumed that SIP Entity for Session Manager has been already configured.



SIP Entity Details

General

* Name:	cm-tr1
* FQDN or IP Address:	10.64.10.67
Type:	Session Manager
Notes:	
Location:	Test Room 1
Outbound Proxy:	
Time Zone:	America/Fortaleza
Credential name:	

SIP Link Monitoring

SIP Link Monitoring:	Use Session Manager Configuration

7.4. Add Adaptation

Adaptations are used to manipulate digits (via Digit Conversion) and SIP URIs (Via Module and Egress Parameters) for incoming and outgoing calls. Navigate to **Home → Elements → Routing → Adaptation**, click **New** (not shown) and configure as follows:

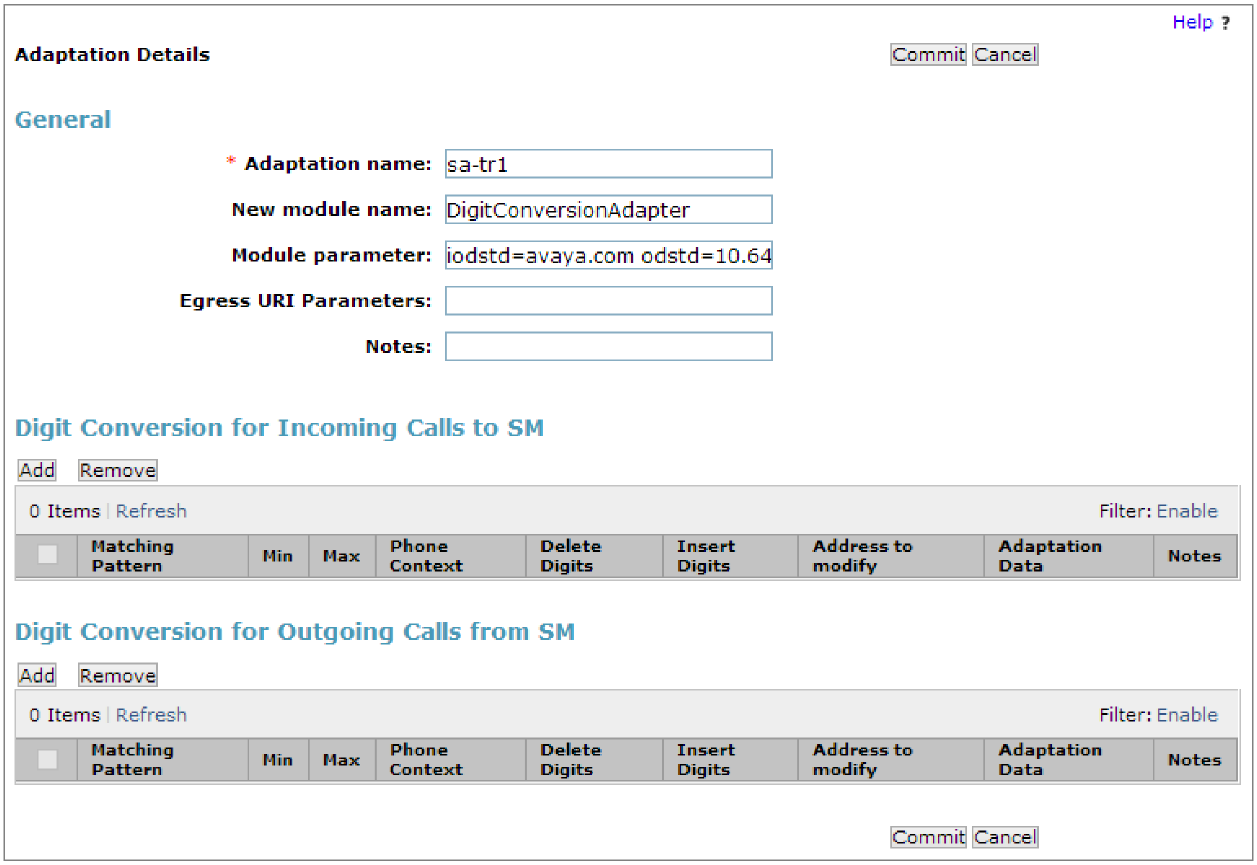
- Type in a descriptive name in **Adaptation Name** field
- Type in **DigitConversionAdapter** in **New Module Name** field
- In the **Module Parameter** field type in the following:
  - iodstd=avaya.com odstd=**ip-address** fromto=true

  Note: ip-address is the IP Address of SA-Announce.

Note: Module Parameters used during this test performed the following function.

- **fromto**: Modifies From and To headers of a SIP message.
- **idstd** (overrideDestinationDomain): Replaces the domain in Request-URI, To header, Refer-To header, and Notify/message-summary body with the given value for egress only. Egress refers to call routing out of Session Manager.
- **iodstd** (ingressOverrideDestinationDomain) : Replaces the domain in Request-URI, To header, and Notify/message-summary body with the given value for ingress only. Ingress refers to calls arriving into Session Manager.

Click **Commit** to save the changes.



Adaptation Details

General

* Adaptation name:	sa-tr1
New module name:	DigitConversionAdapter
Module parameter:	iodstd=avaya.com odstd=10.64
Egress URI Parameters:	
Notes:	

Digit Conversion for Incoming Calls to SM

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

Digit Conversion for Outgoing Calls from SM

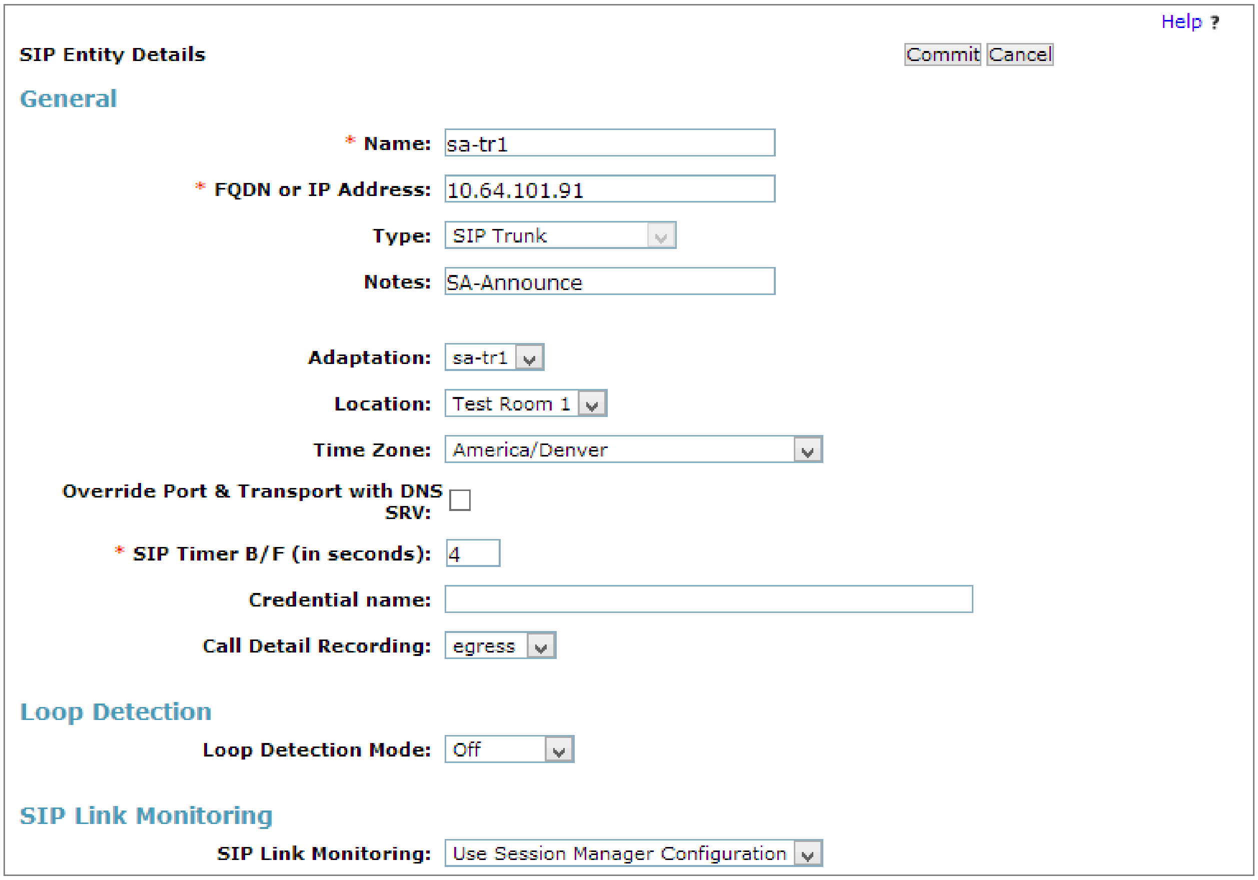
□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes

7.5. Add SIP Entity – SA-Announce

Add SA-Announce as a SIP Entity. Navigate to **Home → Elements → Routing → SIP Entities,** click on **New** (no shown) and configure as follows:

- Type in a descriptive name in **Name** field
- Type in the FQDN or IP address of the SA-Announce server in **FQDN or IP Address** field
- Set **Type** to **SIP Trunk**
- Set **Adaptation** to the one configured in previous section
- Set **Location** to the location configured in **Section 7.2**

Click **Commit** to save the changes.



SIP Entity Details

General

* Name:	sa-tr1
* FQDN or IP Address:	10.64.101.91
Type:	SIP Trunk
Notes:	SA-Announce
Adaptation:	sa-tr1
Location:	Test Room 1
Time Zone:	America/Denver
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	egress

Loop Detection

Loop Detection Mode:	Off

SIP Link Monitoring

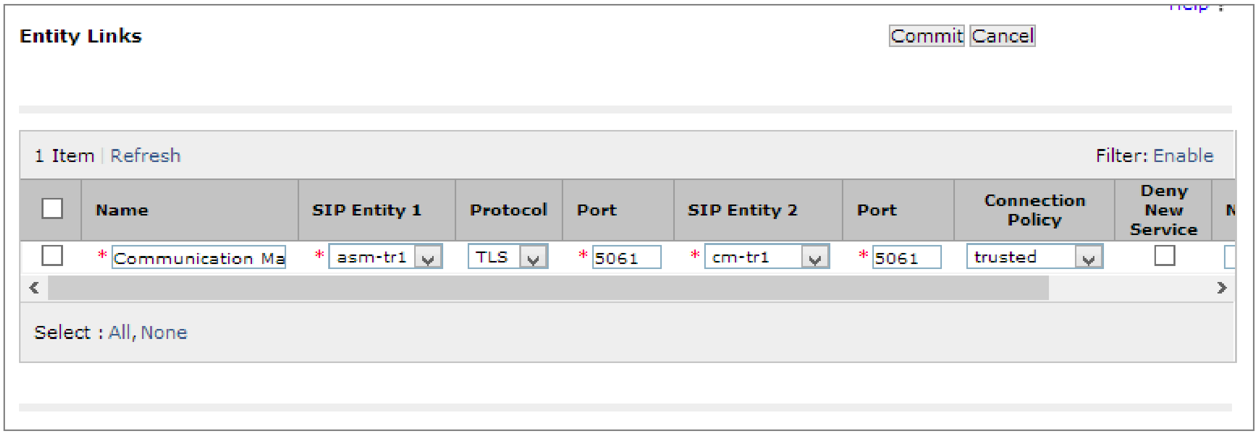
SIP Link Monitoring:	Use Session Manager Configuration

7.6. Add Entity Link – Communication Manager

A SIP Trunk between a Session Manager and another SIP entity is described by an Entity Link. Navigate to **Home → Elements → Routing → Entity Links**, click on **New** (not shown) and configure as follows:

- Type in a descriptive name in **Name** field
- Set **SIP Entity 1** to the name of Session Manager SIP Entity
- Set **SIP Entity 2** to Communication Manager SIP Entity configured in **Section 7.3**

Click **Commit** to save changes.



□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	N
□	* Communication Ma	* asm-tr1	TLS	* 5061	* cm-tr1	* 5061	trusted	□	

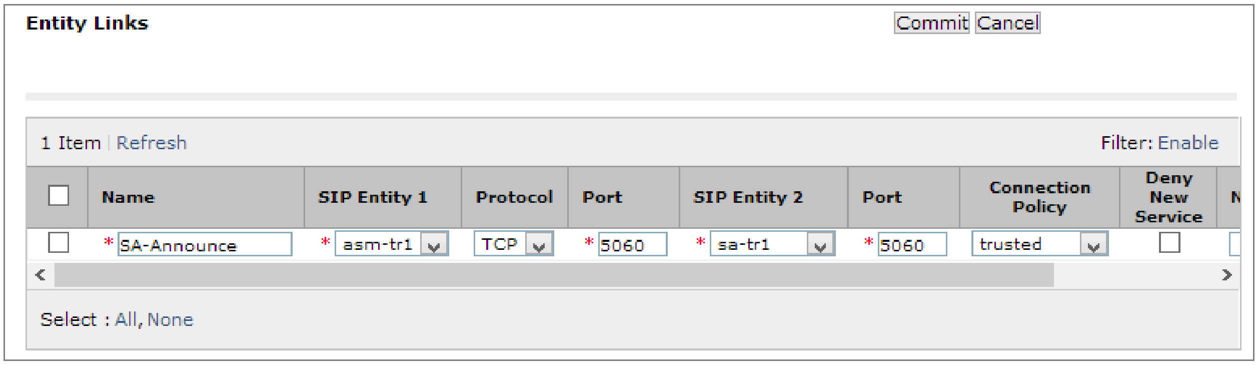
7.7. Add Entity Link – SA-Announce

Navigate to **Home → Elements → Routing → Entity Links**, click on **New** (not shown) and configure as follows:

- Type in a descriptive name in **Name** field
- Set **SIP Entity 1** to the name of Session Manager SIP Entity
- Set **Protocol** to **TCP**
- Set **SIP Entity 2** to Communication Manager SIP Entity configured in **Section 7.5**

Note: SA-Announce only supports **TCP**.

Click **Commit** to save changes.



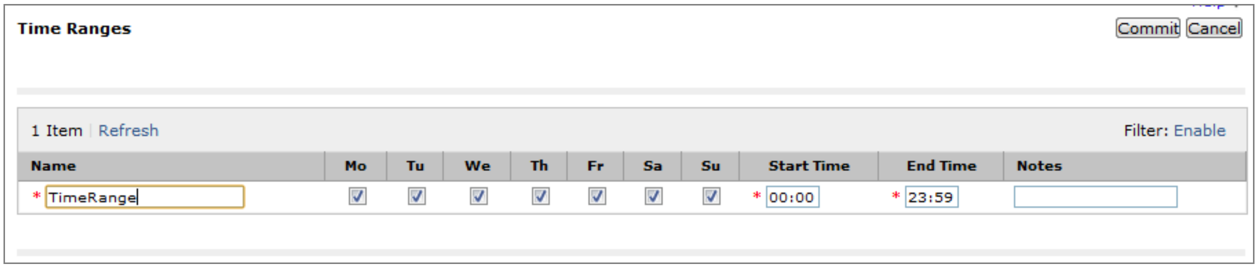
□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	N
□	* SA-Announce	* asm-tr1	TCP	* 5060	* sa-tr1	* 5060	trusted	□	

7.8. Add Time Ranges

Navigate to **Home → Elements → Routing → Time Ranges**, click on **New** (now shown) and configure as follows:

- Type in a descriptive name in **Name** field

Click **Commit** to save changes.



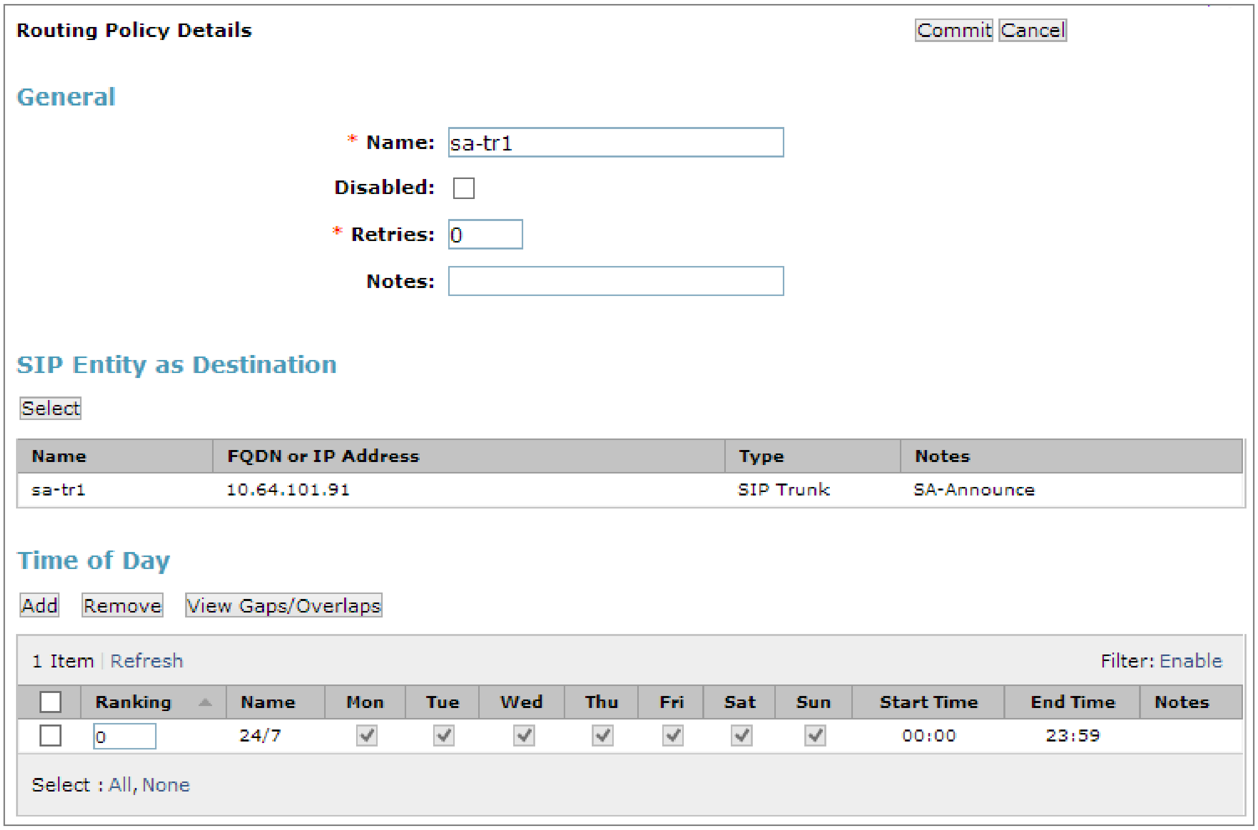
Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
* TimeRange	☑	☑	☑	☑	☑	☑	☑	* 00:00	* 23:59	

7.9. Add Routing Policy

Session Manager uses the data configured in the Routing Policy to find the best match against a number or address of the called party configured in a Dial Pattern. Dial pattern is configured once a Routing Policy is added. Navigate to **Home → Elements → Routing → Routing Policies**, click on **New** (not shown) and configure as follows:

- Type in a descriptive name in **Name** field
- Under **SIP Entity as Destination**, click on **Select** (not shown):
  - Select SA-Announce SIP entity added in **Section 7.5**
- Under **Time of Day**, click on **Add** (not shown):
  - Select time range added in previous step

Click **Commit** to save changes.



Routing Policy Details

General

* Name:	sa-tr1
Disabled:	□
* Retries:	0
Notes:	

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
sa-tr1	10.64.101.91	SIP Trunk	SA-Announce

Time of Day

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

7.10. Add Dial Patterns

Navigate to **Home → Elements → Routing → Dial Patterns**, click on **New** (not shown) and configure as follows:

Under **General:**

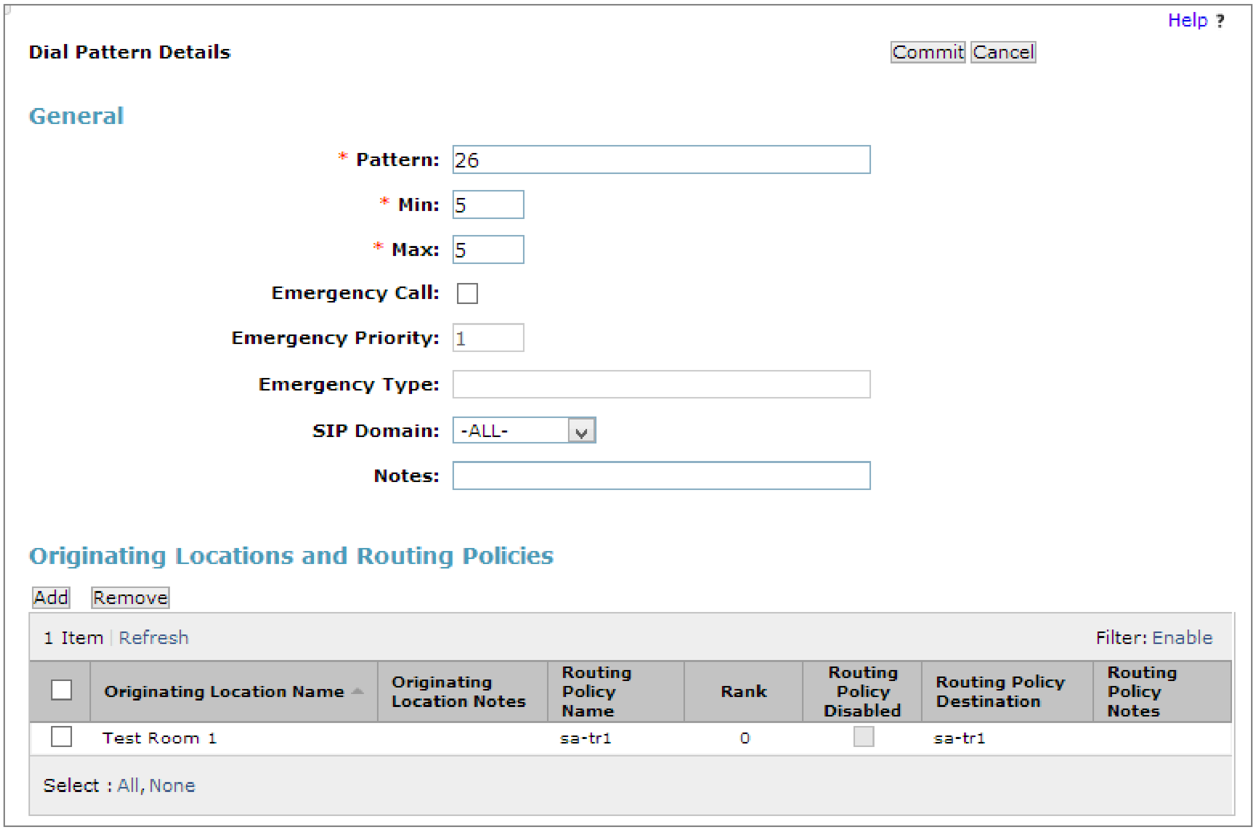
- Set **Pattern** to prefix of dialed number
- Set **Min** to minimum length of dialed number
- Set **Max** to maximum length of dialed number

During the compliance test, called numbers starting with digits 26 and 5 digits long were routed to SA-Announce.

Under **Originating Locations and Routing Policies:**

- Click **Add** and select originating location and SA-Announce routing policy as configured in **Section 7.9**

Click **Commit** to save changes.



Dial Pattern Details

General

* Pattern:	26
* Min:	5
* Max:	5
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	-ALL-
Notes:	

Originating Locations and Routing Policies

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Test Room 1		sa-tr1	0	□	sa-tr1	

8. Configure SA-Announce

SA-Announce is installed on a Windows Server platform. Windows Server 2008 R2 was used during compliance-testing. For other Windows Server configurations, please reference the SA-Announce Avaya User Guide. A link to the document has been provided in **Section 11**.

8.1. Server Requirements

The Windows Server requirements are as follows:

Server Requirement	**Description**
Manual Setup Requirement	**These require manual setup.**
Disabling Public Firewall	Firewall must be disabled or set to allow access on the required ports (see Firewall Ports).
Auto-Setup Requirement	**The installer should automatically complete these.**
Disabling IE Enhanced Security Configuration	IE Enhanced Security Configuration must be disabled to allow the website to function properly.
Creating ASPNET user account	
Installing Internet Information Service (IIS)	IIS is required for the product to function.
Installing ASP.NET	ASP.NET 4.0 is required for the product to function.
Recommended	**These are recommended items.**
Disabling User Account Control (UAC)	SA-Announce recommends disabling UAC.

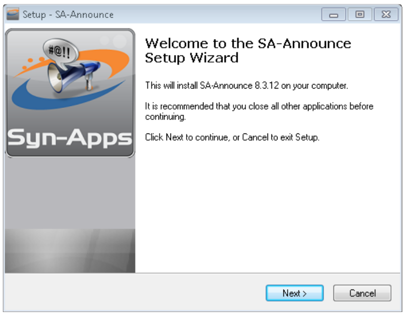
8.2. Network Requirements

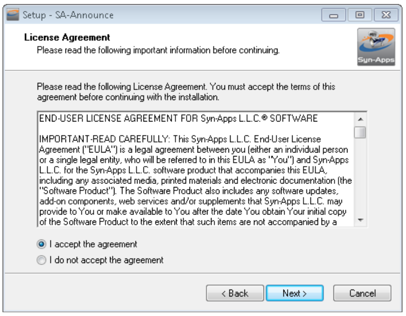
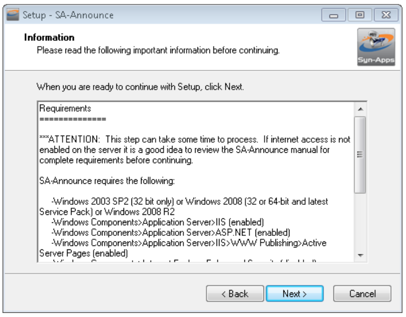
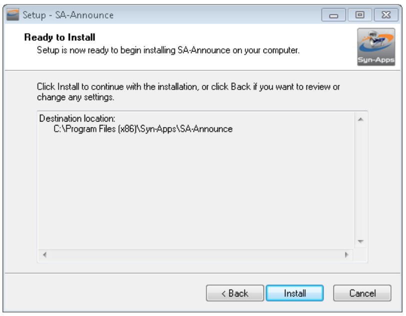
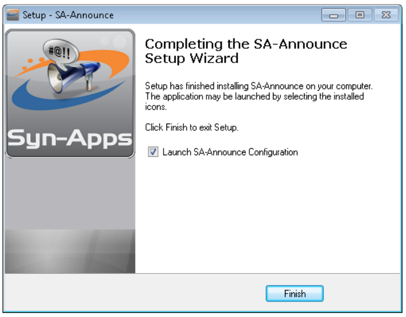
Firewall requirements/port usage:

Ports	Description
SA-Announce server to Avaya	*Protocol description*
5060	TCP – SIP – Session Initiation Protocol
SA-Announce Server to IP Phones:	*Protocol description*
80	TCP - HTTP
20480-32767	UDP - Real-Time Protocol (RTP)
20480-32767	UDP - Multicast Real-Time Protocol (RTP)
IP Phones to SA-Announce Server:	*Protocol description*
80	TCP - HTTP
20480-32767	UDP - Real-Time Protocol (RTP)
20480-32767	UDP - Multicast Real-Time Protocol (RTP)

8.3. SA-Announce Installation

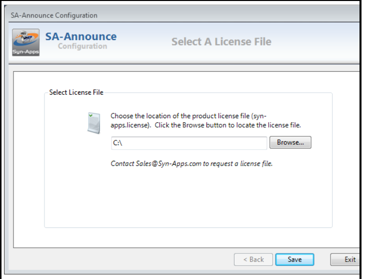
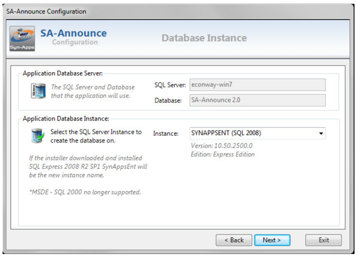
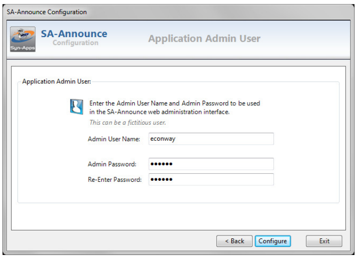
If the SA-Announce server does not have internet access, then please make sure the required components ASP.NET 4.0 and SQL Express 2008 R2 SP1 have been installed. See the SA-Announce Avaya User Guide for more information.

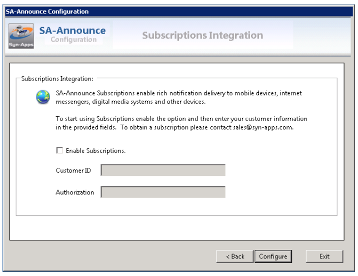
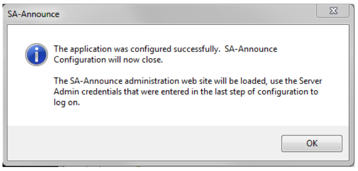
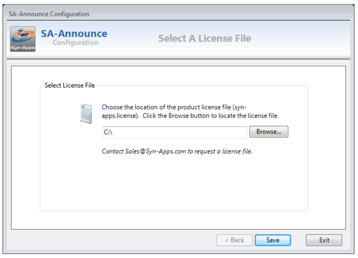
Installation Procedure	Description	Screenshot
Start the Installer	Start the SA-Announce setup program. The SA-Announce setup program welcome screen should appear. Click **Next** to proceed. Note: Download SA-Announce here: http://www.syn-apps.com/support/downloads/ A license file is required. Please contact sales@syn-apps.com to request one.	 Setup - SA-Announce Welcome to the SA-Announce Setup Wizard This will install SA-Announce 8.3.12 on your computer. It is recommended that you close all other applications before continuing. Click Next to continue, or Cancel to exit Setup.

Installation Procedure	**Description**	**Screenshot**
Accept License Agreement	The License Agreement page should appear. Read and accept the license terms by selecting clicking **I accept the agreement radio** button. Click **Next** to proceed.	 Setup - SA-Announce **License Agreement** Please read the following important information before continuing. Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation. END-USER LICENSE AGREEMENT FOR Syn-Apps L.L.C.® SOFTWARE IMPORTANT-READ CAREFULLY: This Syn-Apps L.L.C. End-User License Agreement ("EULA") is a legal agreement between you (either an individual person or a single legal entity, who will be referred to in this EULA as "You") and Syn-Apps L.L.C. for the Syn-Apps L.L.C. software product that accompanies this EULA, including any associated media, printed materials and electronic documentation (the "Software Product"). The Software Product also includes any software updates, add-on components, web services and/or supplements that Syn-Apps L.L.C. may provide to You or make available to You after the date You obtain Your initial copy of the Software Product to the extent that such items are not accompanied by a ● I accept the agreement ○ I do not accept the agreement
Requirement Information	Review and verify the server requirements. Click **Next** to proceed. *The system requirements will now be validated. Missing components will be downloaded from SA-Apps servers and installed if necessary. This could take some time depending on the system.	 Setup - SA-Announce **Information** Please read the following important information before continuing. When you are ready to continue with Setup, click Next. Requirements ============== ***ATTENTION: This step can take some time to process. If internet access is not enabled on the server it is a good idea to review the SA-Announce manual for complete requirements before continuing. SA-Announce requires the following: -Windows 2003 SP2 (32 bit only) or Windows 2008 (32 or 64-bit and latest Service Pack) or Windows 2008 R2 -Windows Components>Application Server>IIS (enabled) -Windows Components>Application Server>ASP.NET (enabled) -Windows Components>Application Server>IIS>WWW Publishing>Active Server Pages (enabled)
Ready to Install	Click **Install** to start the product installation.	 Setup - SA-Announce **Ready to Install** Setup is now ready to begin installing SA-Announce on your computer. Click Install to continue with the installation, or click Back if you want to review or change any settings. Destination location: C:\Program Files (x86)\Syn-Apps\SA-Announce
Install Complete	The installation is now complete.Make sure the **Launch SA-Announce Configuration** checkbox is checked. Click **Finish** to begin the SA-Announce Configuration Utility.	 Setup - SA-Announce Completing the SA-Announce Setup Wizard Setup has finished installing SA-Announce on your computer. The application may be launched by selecting the installed icons. Click Finish to exit Setup. ☑ Launch SA-Announce Configuration

8.4. SA-Announce Configuration Utility

The SA-Announce Configuration Utility will automatically run at the end of installation. It can also be started manually at any time from the **Start→All Programs→Syn-Apps→SA-Announce→SA-Announce Configuration** shortcut.

Config Step	Description	Screenshot
License Selection	In order to use the SA-Announce software, a valid license key must be obtained. Please contact sales@syn-apps.com to obtain a license. If the license file has already obtained, click **Browse** to locate it. The license file screen will only appear if the license file, Syn-Apps.license, does not exist in the program base directory (C:\Program Files\Syn-Apps\SA-Announce\). If you encounter problems with the browser, simply place your license in the program base directory and make sure it is copied there with the precise filename **Syn-Apps.license**. Click **Next** to proceed.	 Select License File Choose the location of the product license file (syn-apps.license). Click the Browse button to locate the license file. C:\ *Contact Sales@Syn-Apps.com to request a license file.* SA-Announce Configuration SA-Announce Configuration Syn-Apps Select A License File Browse... < Back Save Exit
Database Instance	If SQL Server Express 2008 R2 was installed along with this installation leave the default instance name as **SynAppsEnt**. If an existing local SQL server instance is to be used, select that instance name from the drop-down list. Click **Next** to proceed.	 Application Database Server: *The SQL Server and Database that the application will use.* SQL Server: econway-win7 Database: SA-Announce 2.0 Application Database Instance: Select the SQL Server Instance to create the database on. Instance: SYNAPPSENT (SQL 2008) *Version: 10.50.2500.0* *Edition: Express Edition* *If the installer downloaded and installed SQL Express 2008 R2 SP1 SynAppsEnt will be the new instance name.* **MSDE - SQL 2000 no longer supported.* SA-Announce Configuration SA-Announce Configuration Syn-Apps Database Instance < Back Next > Exit
Application Admin Credentials	Setup the SA-Announce application administrator user account credentials. This will be the system admin user for the SA-Announce notification system. It is not a Windows or Domain account. Click **Next** to proceed.	 Application Admin User: Enter the Admin User Name and Admin Password to be used in the SA-Announce web administration interface. *This can be a fictitious user.* Admin User Name: econway Admin Password: •••••• Re-Enter Password: •••••• SA-Announce Configuration SA-Announce Configuration Syn-Apps Application Admin User < Back Configure Exit

Config Step	Description	Screenshot
Subscriptions Integration	SA-Announce Subscription Services include various cloud messaging methods such as Smartphone and SMS notifications. This compliance test did not include testing of the Subscription Services. Please contact sales@syn-apps.com for more information. Click **Configure** to start the configuration process.	 SA-Announce Configuration SA-Announce Configuration Syn-Apps Subscriptions Integration Subscriptions Integration: < Back Configure Exit SA-Announce Subscriptions enable rich notification delivery to mobile devices, internet messengers, digital media systems and other devices. To start using Subscriptions enable the option and then enter your customer information in the provided fields. To obtain a subscription please contact sales@syn-apps.com. ☐ Enable Subscriptions. Customer ID Authorization
Configuration Complete	When the application is configured you will see a success window. Click **OK** to proceed.	 The application was configured successfully. SA-Announce Configuration will now close. The SA-Announce administration web site will be loaded, use the Server Admin credentials that were entered in the last step of configuration to log on.
License Activation	If the license has not been activated, the Activation Wizard will appear. Select **Online** if the SA-Announce server has access to the Internet. Click **Next** to activate the license. Select **By Email** if the SA-Announce server does not have access to the Internet. Click **Next**. Further instructions will be provided in this case.	 SA-Announce Configuration SA-Announce Configuration Syn-Apps Select A License File Select License File Browse... < Back Save Exit Choose the location of the product license file (syn-apps.license). Click the Browse button to locate the license file. C:\ *Contact Sales@Syn-Apps.com to request a license file.*

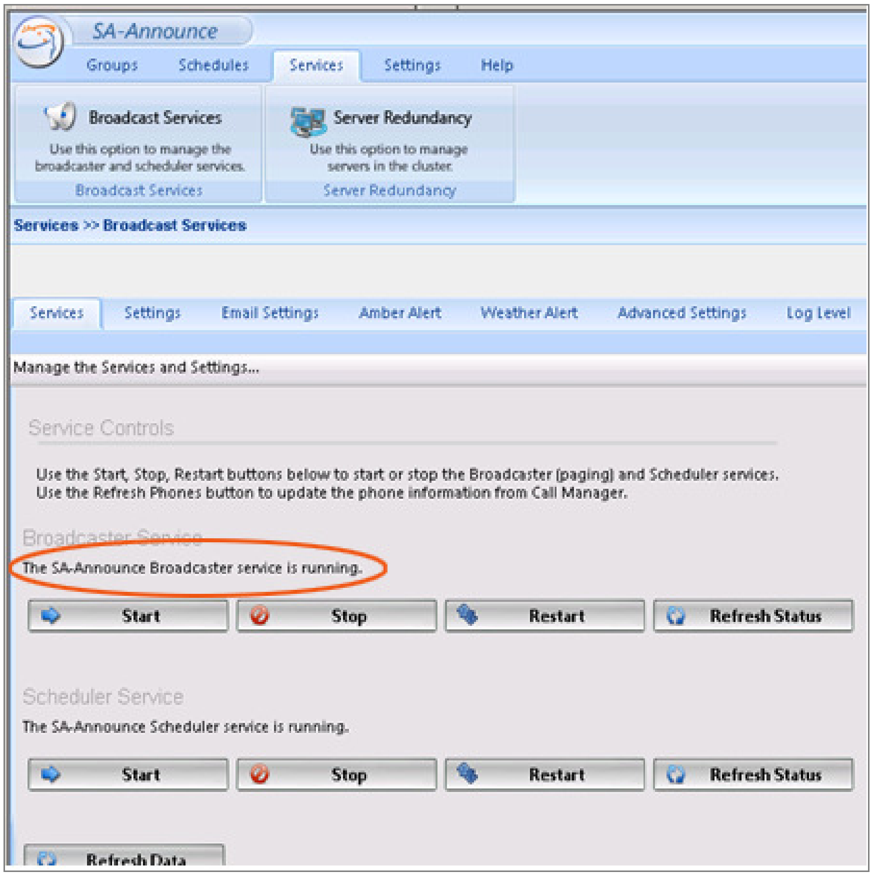
When the Configuration Wizard has completed the installation a shortcut will be placed on the desktop labeled **SA-Announce**, use this to access the SA-Announce web administration program. It is also possible to directly access the SA-Announce administration web pages from any machine on the network, by browsing to **http://<application-server-ip>/SA-Announce**, where application-server-ip address is the ip address of SA-Announce server.

The SA-Announce web page should be displayed automatically when the configuration program completes. The opening page reviews the settings necessary all SA-Announce to communicate with Avaya Communications Manager and Phones.

Note: When SA-Announce is installed it will automatically enable SIP traffic for port 5060 using TCP.

8.5. SA-Announce Paging Basics

Ensure the SA-Announce Broadcaster Service is running prior to testing paging. Open the **Services→Broadcast Services** page. The Services tab shows the service status and contains buttons to start, stop, and restart the service. The Broadcaster Service should be running as shown in the screen capture below.



Manage the Services and Settings...

Service Controls

Use the Start, Stop, Restart buttons below to start or stop the Broadcaster (paging) and Scheduler services.
Use the Refresh Phones button to update the phone information from Call Manager.

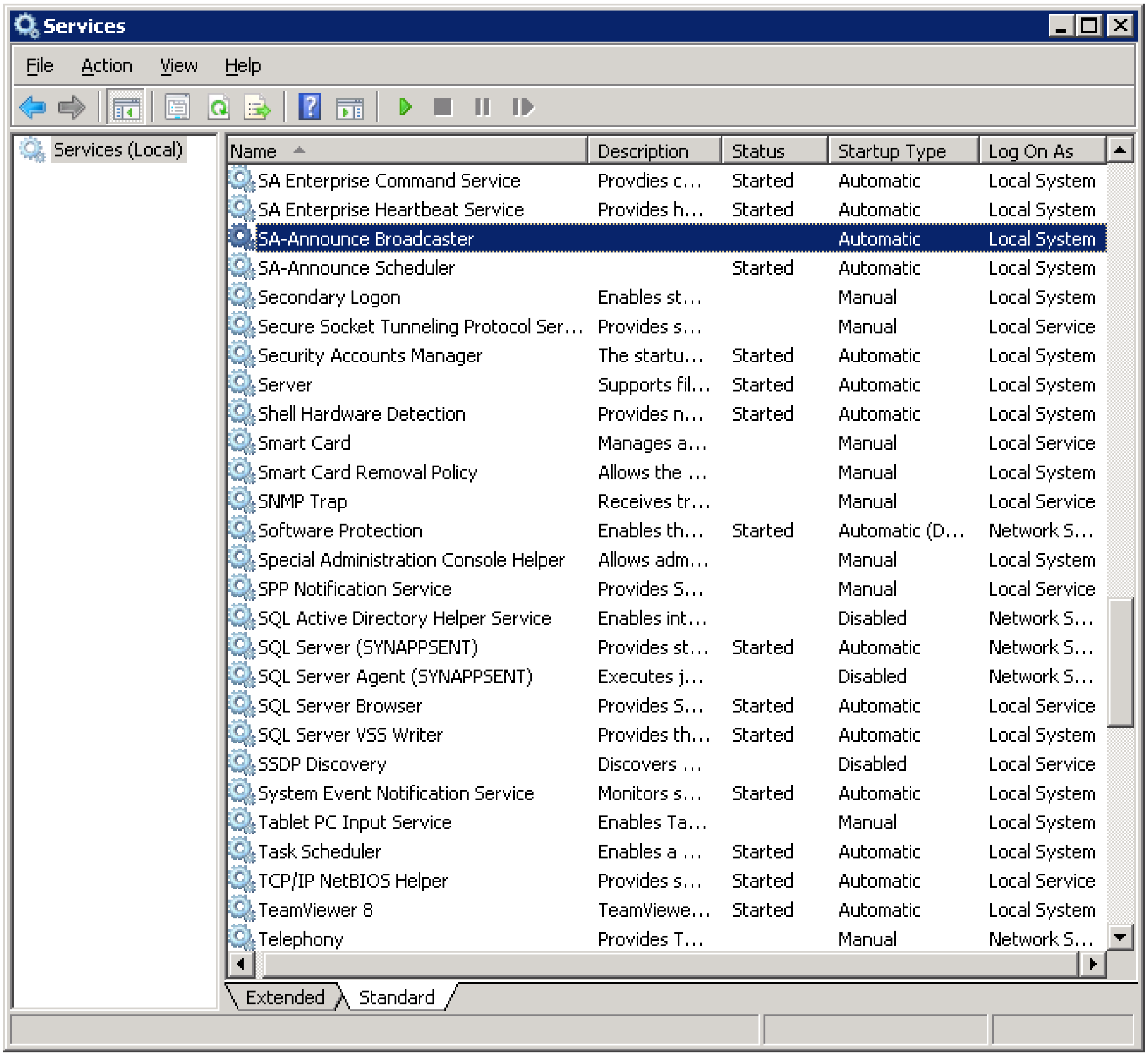
Broadcaster Service

The SA-Announce Broadcaster service is running.

Scheduler Service

The SA-Announce Scheduler service is running.

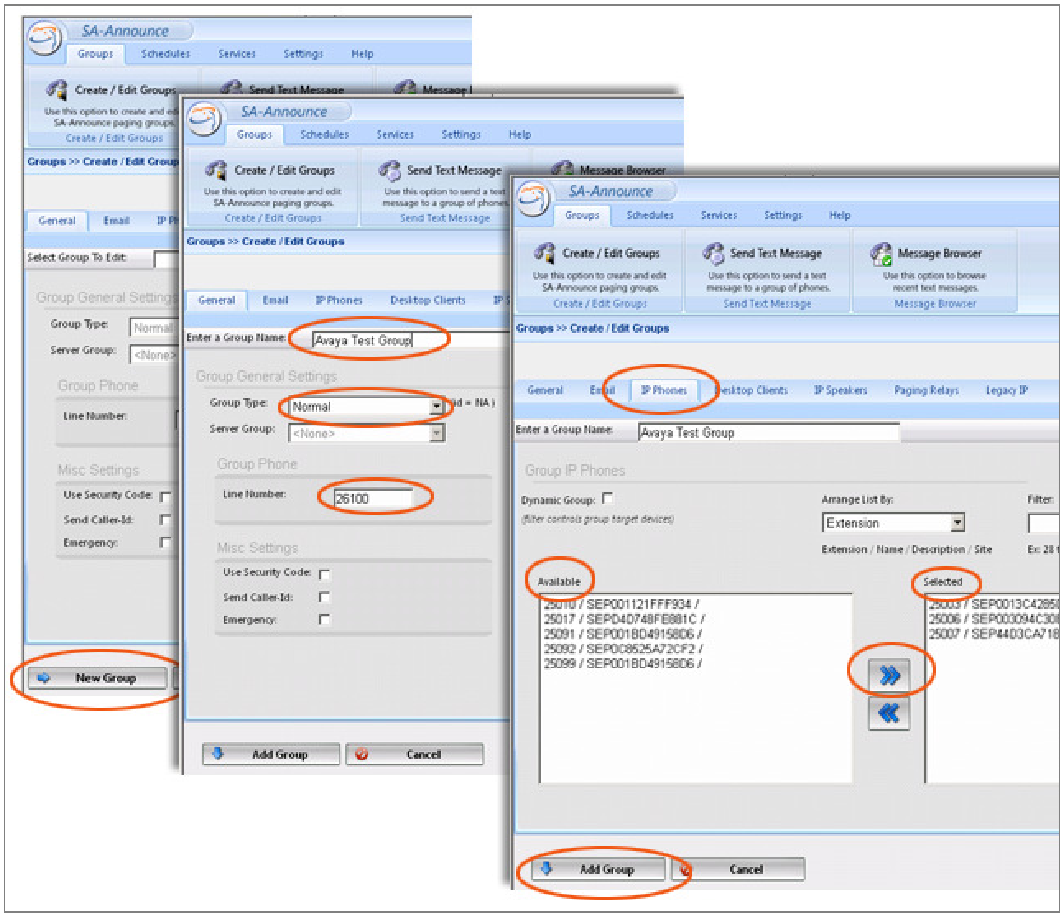
The SA-Announce services can also be controlled from the Windows Program Services Console (Services.msc). To control the SA-Announce broadcaster services, look for **SA-Announce Broadcaster** services in **Services.msc**.



Name	Description	Status	Startup Type	Log On As
SA Enterprise Command Service	Provdies c…	Started	Automatic	Local System
SA Enterprise Heartbeat Service	Provides h…	Started	Automatic	Local System
SA-Announce Broadcaster			Automatic	Local System
SA-Announce Scheduler		Started	Automatic	Local System
Secondary Logon	Enables st…		Manual	Local System
Secure Socket Tunneling Protocol Ser…	Provides s…		Manual	Local Service
Security Accounts Manager	The startu…	Started	Automatic	Local System
Server	Supports fil…	Started	Automatic	Local System
Shell Hardware Detection	Provides n…	Started	Automatic	Local System
Smart Card	Manages a…		Manual	Local Service
Smart Card Removal Policy	Allows the …		Manual	Local System
SNMP Trap	Receives tr…		Manual	Local Service
Software Protection	Enables th…	Started	Automatic (D…	Network S…
Special Administration Console Helper	Allows adm…		Manual	Local System
SPP Notification Service	Provides S…		Manual	Local Service
SQL Active Directory Helper Service	Enables int…		Disabled	Network S…
SQL Server (SYNAPPSENT)	Provides st…	Started	Automatic	Network S…
SQL Server Agent (SYNAPPSENT)	Executes j…		Disabled	Network S…
SQL Server Browser	Provides S…	Started	Automatic	Local Service
SQL Server VSS Writer	Provides th…	Started	Automatic	Local System
SSDP Discovery	Discovers …		Disabled	Local Service
System Event Notification Service	Monitors s…	Started	Automatic	Local System
Tablet PC Input Service	Enables Ta…		Manual	Local System
Task Scheduler	Enables a …	Started	Automatic	Local System
TCP/IP NetBIOS Helper	Provides s…	Started	Automatic	Local Service
TeamViewer 8	TeamViewe…	Started	Automatic	Local System
Telephony	Provides T…		Manual	Network S…

To create a simple Paging Group to test, go to the **Groups→Create/Edit Groups** page.

- Click the **New Group** button at the bottom of the page
- Enter a Paging **Group name**
- Select the **Normal** as **Group Type**
- Enter a **Line Number** (Extension) for the the group
- Click the **IP Phones** tab
- Select phones from the **Available** list and move them to the Selected list by clicking the **double right arrow button**
- Click the **Add Group** button to complete the process



Enter a Group Name: Avaya Test Group

Group Type: Normal

Server Group: <None>

Line Number: 26100

Dynamic Group: □

Arrange List By: Extension

Available:
25010 / SEP001121FFF934 /
25017 / SEP0D4D748FE881C /
25091 / SEP001BD49158D6 /
25092 / SEP0C8625A72CF2 /
25099 / SEP001BD49158D6 /

Selected:
25003 / SEP0013C4285
25006 / SEP003094C30
25007 / SEP44D3CA718

Once the group is saved, test the group by dialing the line number of the group (26100 in the example above). An audible tone should be heard the source phone's speaker. After hearing the tone, start speaking. The message should then be heard on the selected destination phones.

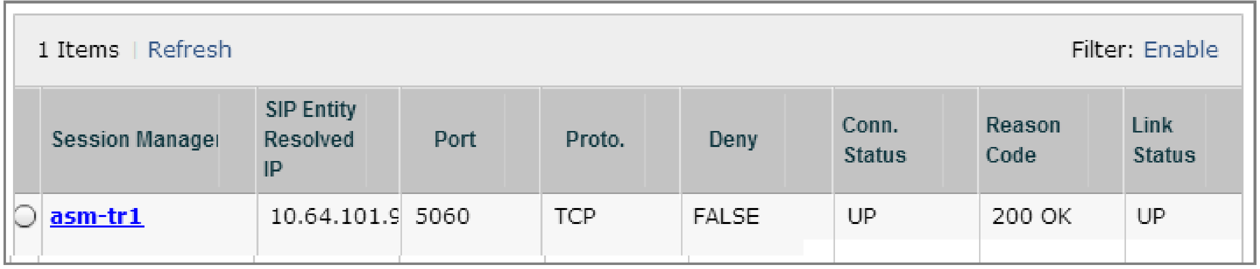
For more information on Group Types and Advanced Group configuration and testing, please reference the SA-Announce Avaya User Guide. A link to the document has been provided in Section 11.

9. Verification Steps

9.1. Avaya Aura® Session Manager

From the System Manager web page, navigate to **Session Manager → System Status → SIP Entity Monitoring**. Under the **All Monitoring SIP Entities**, select SA-Announce SIP entity that was configured in this document (not shown).

Ensure that **Conn. Status** is **UP**, and **Reason Code** is **200 OK**. This will verify that the connection between Session Manager and SA-Announce server is successful.



1 Items | Refresh   Filter: Enable

	Session Manage	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	asm-tr1	10.64.101.9	5060	TCP	FALSE	UP	200 OK	UP

Additionally, a test call can be made to a group configured in **Section 8.5** to verify that the group is active.

10. Conclusion

Syn-apps' SA-Announce was able to successfully interoperate with Avaya 9600 Series IP Deskphones. All executed test cases were passed.

11. Additional References

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

[1] Administering Avaya Aura® Communication Manager, Release 6.3, Document 03-300509, Issue 8 May 2013

[2] Administering Avaya Aura® Session Manager, Release 6.3, June 2013

Product information for Syn-Apps SA-Announce can be found at the following URL:

[3] SA-Announce Notification System User Manual Version 8.0.0

http://www.syn-apps.com/downloads/Install-Guides/SA-Announce%20Avaya%20User%20Guide.pdf

Note: The document used to Install and configured SA-Announce is for Version 8.0.0. Document for Version 9.0.0 will be published at a later time. Please contact Syn-apps to obtain the latest version of the document.

The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.