Avaya Solution & Interoperability Test Lab

Application Notes for Configuring SIP Trunking Using SimpleSignal SIP Trunk Service and Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager – Issue 1.0

Abstract

These Application Notes describe steps to configure Session Initiation Protocol (SIP) trunking between the SimpleSignal Session Border Controller, EdgeMarc 4500, and an Avaya IP telephony solution. The Avaya solution consists of Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager, and various H.323 endpoints. These Application Notes correspond to SimpleSignal SIP Trunk Service offered using a network border switch in the network.

SimpleSignal 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.

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between SimpleSignal and an Avaya IP telephony solution. The Avaya solution consists of Avaya Aura™ Session Manager, Avaya Aura™ System Manager, Avaya Aura™ Communication Manager, and various H.323 endpoints. These Application Notes correspond to SimpleSignal SIP Trunk Service offered using a Session Border Controller, EdgeMarc 4500, in the network.

Customers using this Avaya IP telephony solution with the SimpleSignal SIP Trunk Service are able to place and receive PSTN calls via a dedicated broadband Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI. The text and coverage diagram below summarizes the SimpleSignal SIP Trunk Service at the time of writing these Application Notes. Please consult SimpleSignal for the most current description of capabilities.

1.1. SimpleSIgnal SIP Trunk

SimpleSignal offers SIP Trunking that is routed over the IP backbone of a carrier using VoIP technology. SIP Trunks are used in conjunction with an IP-PBX and are thought of as replacements for traditional PRI or analog circuits. The popularity of SIP Trunks is due primarily to the cost savings of SIP, along with the increased reliability as backed by the Service Level Agreement (SLAs) of SimpleSignal. SimpleSignal also offers Burstable SIP trunks.

1.2. Interoperability Compliance Testing

A simulated enterprise site using an Avaya IP telephony solution was connected to the public Internet using a dedicated broadband connection. The enterprise site was configured to use the commercially available SIP Trunk Service provided by SimpleSignal.

To verify SIP trunk interoperability between the SimpleSignal and an Avaya network, the following features and functionality were covered during the interoperability compliance test:

- Incoming calls to the enterprise site from the PSTN were routed to the DID numbers assigned by SimpleSignal. Incoming PSTN calls were made to H.323 (9600 and 4600 series), digital, and 16xx telephones at the enterprise.
- Outgoing calls from the enterprise site were completed via SimpleSignal to PSTN destinations. Outgoing calls from the enterprise to the PSTN were made from H.323 (9600 and 4600 series), digital, and 16xx telephones at the enterprise.
- Various call types were tested including: local, long distance, international, outbound toll-free, operator, directory assistance, and emergency.
- Calls using G.729A, G.711MU, and G.711A coders.
- DTMF transmission using RFC 2833 with successful vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, and conference.

- Off-net call forwarding and extension to cellular, when the call arrived from the SIP Trunk from SimpleSignal, or when the call forwarding destination and extension to cellular mobile number routed out the SIP Trunk to SimpleSignal, or both.
- Caller ID Presentation and Caller ID Restriction.
- Avaya IP Softphone in both "Road Warrior" and "Telecommuter" modes, where incoming PSTN calls arrived from SimpleSignal, or the telecommute number routed out the SIP Trunk to SimpleSignal, or both.

Please refer to Section 7 for complete test results, known limitations, observations and any necessary workarounds.

1.3. Support

For technical support on SimpleSignal SIP Trunk services can be obtained by contacting SimpleSignal Customer Service:

- URL - http://www.simplesignal.com/support.php
- Phone - (303) 242-8616

2. Reference Configuration

Figure 1 illustrates a sample Avaya IP telephony solution connected to the SimpleSignal SIP Trunk Service. This is the configuration used for DevConnect compliance testing.

The Avaya components used to create a simulated customer site included:

- Avaya S8720 Servers running Communication Manager
- Avaya G650 Media Gateway and associated hardware
- Avaya Aura™ System Manager
- Avaya Aura™ Session Manager
- Avaya 4600-Series IP telephones (configured for the H.323 protocol)
- Avaya 9600-Series IP telephones (configured for the H.323 protocol)
- Avaya 1600-Series IP telephones (configured for the H.323 protocol)
- Avaya IP Agent
- Avaya digital phones
- Fax machine

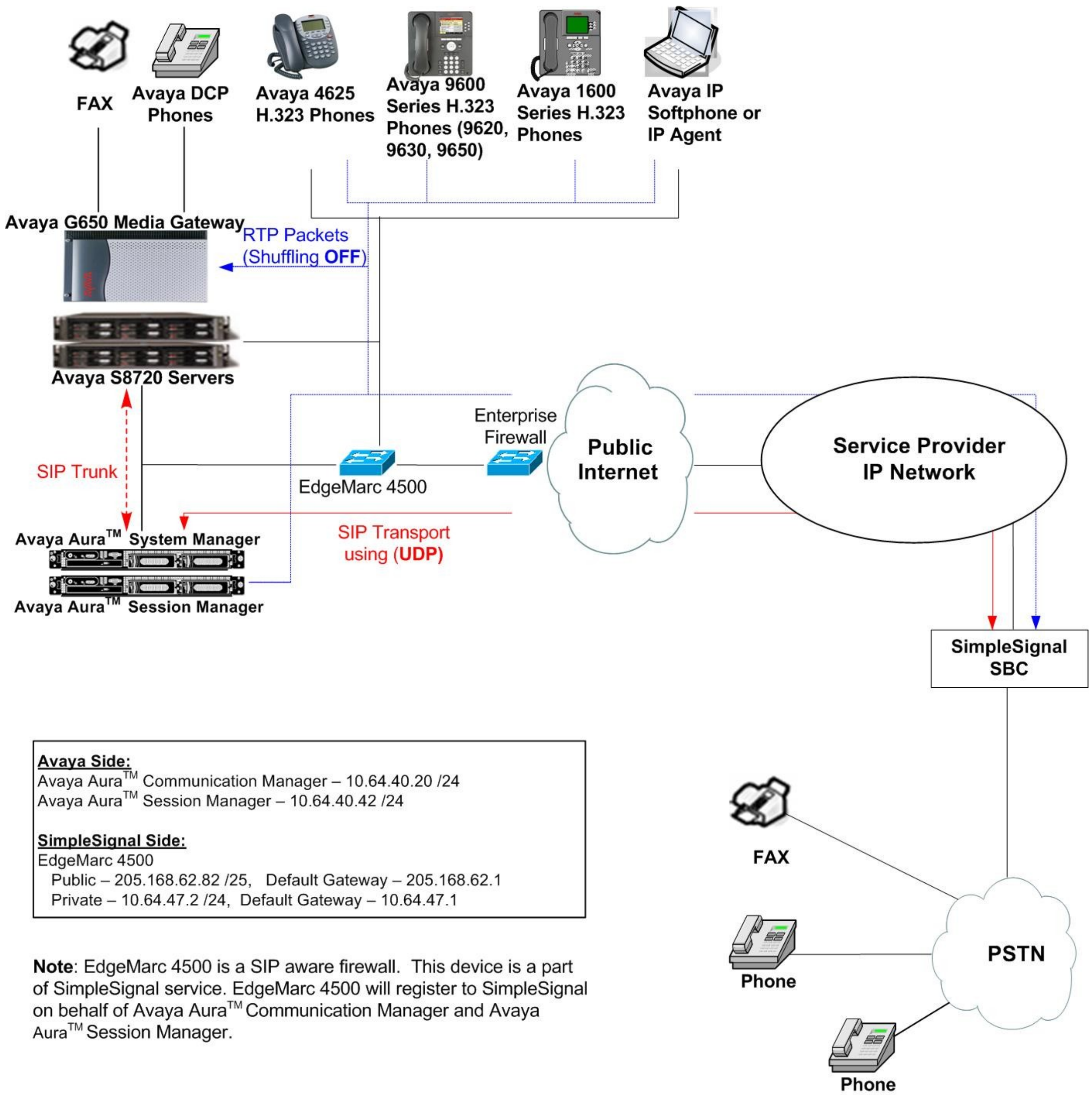


Figure 1: Avaya IP Telephony Network using SimpleSignal SIP Trunk Service

3. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura™ Communication Manager running on an Avaya S8720 Server (Element Manager)	5.2.1 (R015x.02.1.016.4)
Avaya G650 Media Gateway	
Avaya Aura™ Session Manager running on an Avaya S8500B Server	5.2.1.1
Avaya Aura™ System Manager running on an Avaya S8500B Server	5.2.1.1
Avaya 9600 IP Series Telephone (H.323) 9620 9630 9650	 3.1 3.1 3.1
Avaya 4600 Series IP Telephone 4625	 2.5
Avaya 1616 IP Telephone (H.323)	1.2.2
Avaya IP Agent	R7.0 SP7
SimpleSignal SIP Trunk Service Solution Components	
Component	Release
SimpleSignal SIP Trunk Service (EdgeMarc 4500)	9.12.2.yfl1

The specific configuration above was used for the compatibility testing. Note that this solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager, System Manager and Session Manager.

4. Configure Avaya Aura™ Communication Manager

This section describes the steps for configuring Communication Manager for SIP Trunking. A SIP trunk is established between Communication Manager and Session Manager. The trunk carries SIP signaling between Communication Manager and Session Manager.

It is assumed the general installation of Communication Manager, Avaya G650 Media Gateway and Session Manager has been previously completed and is not discussed here.

The Communication Manager configuration was performed using the System Access Terminal (SAT). This section summarizes the Communication Manager configuration in the test environment **prior** to adding SIP trunking to the SimpleSignal SIP Trunk Service.

4.1. Configure IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signaling group between Communication Manager and Session Manager. Use the **change node-names ip** command to create a mapping between a logical name and an IP address. In the test environment, node-name ***CLAN*** is mapped to IP address ***10.64.40.24***) and node name ***ASM*** is mapped to ***10.64.40.42*** (the IP address of Session Manager).

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
ASM                 10.64.40.42
CLAN                10.64.40.24
MEDPRO              10.64.40.26
default             0.0.0.0
```

4.2. Configure IP Network Regions

In the test environment, the Avaya S8720 Server, Avaya G650 Media Gateway, Session Manager, and IP (H.323) endpoints are located in a single IP network region. These components are located in the default IP network region 1. The **change ip-network-region 1** command was used to configure the region with the parameters described below.

- Set the **Authoritative Domain** field to match the domain name configured on Session Manager. In this configuration, the domain name is ***simplesignal.com***. This name appears in the "From" header of SIP messages originating from this IP region.
- Enter a descriptive name for the **Name** field.
- Set the **Codec Set** field to the IP codec set to be used for calls within this IP network region. In this case, IP codec set **1** was selected.
- Default values may be used for all other fields.

```
change ip-network-region 1                                        Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location:          Authoritative Domain: simplesignal.com
    Name:Avaya Devices
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: 65531
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

4.3. Configure Codecs

Use the **change ip-codec-set 1** command to define the codec(s) contained in this set which is used for calls within the enterprise as defined in the previous section. Which codecs are used and their order of preference is defined by the end customer. The example below uses only 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:
 3:
 4:
```

4.4. Signaling Group

The **add signaling-group** command was used to create a signaling group between Communication Manager and the Session Manager for use by intra-site traffic. For the compliance test, signaling group 301 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Set the **Transport Method** to the recommended default value of ***tcp.*** As a result, the **Near-end Listen Port** and **Far-end Listen Port** are automatically set to ***5060.***
- Set the **Near-end Node Name** to ***CLAN***. This node name maps to the IP address of the CLAN circuit pack in the Avaya G650 Media Gateway that terminates the SIP trunk. Node names are defined using the **change node-names ip** command.
- Set the **Far-end Node Name** to ***ASM***. This node name maps to the IP address of Session Manager as defined using the **change node-names ip** command.
- Set the **Far-end Network Region** to the IP network region defined **Section 4.2**.
- Set the **Far-end Domain** to **simplesignal.com**.
- Set **Direct IP-IP Audio Connections** to **n**[1]. This field will disable media shuffling on the SIP trunk. During the compliance test, shuffling was disabled.
- Set the **DTMF over IP** field to ***rtp-payload***. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Default values may be used for all other fields.

[1] Direct IP-IP Audio Connections, otherwise known as shuffling, did not work due to issues with incoming call scenarios; thus the recommendation was to turn the shuffling off.

```
add signaling-group 301                                         Page   1 of   1
                                SIGNALING GROUP

 Group Number: 301             Group Type: sip
                         Transport Method: tcp
  IMS Enabled? n



   Near-end Node Name: CLAN                      Far-end Node Name: ASM
 Near-end Listen Port: 5060                    Far-end Listen Port: 5060
                                            Far-end Network Region: 1
Far-end Domain: simplesignal.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? n
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? n
                                                  Alternate Route Timer(sec): 6
```

4.5. Configure Trunk Group

The **add trunk-group** command was used to create a trunk group for the signaling group created in the previous section. For the compliance test, trunk group 1 was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to ***tie***.
- Set the **Signaling Group** to the signaling group shown in the previous step.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous calls can be supported by this trunk. This value needs to match the capacity ordered from SimpleSignal for this Trunk.
- The default values were used for all other fields.

```
add trunk-group 301                                             Page   1 of  21
                                TRUNK GROUP

Group Number: 301                  Group Type: sip          CDR Reports: n
  Group Name: PSTN-via-SM                 COR: 1        TN: 1        TAC: 1031
   Direction: two-way         Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n

                                                        Signaling Group: 301
                                                      Number of Members: 10
```

4.6. SimpleSignal Specific Configuration

This section describes configuration specific for SimpleSignal SIP trunk service solution.

4.6.1. Configure System Features

Use the **change system-parameters feature** command to set the **Trunk-to-Trunk Transfer** field to ***all*** to allow incoming calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons, incoming calls should not be allowed to transfer back to the PSTN then leave the field set to ***none***.

```
change system-parameters features                               Page   1 of  18
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? y
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y
                             Music/Tone on Hold: none
              Music (or Silence) on Transferred Trunk Calls? no
                       DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n

             Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                     Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

4.6.2. Configure CPN Restriction

On **Page 9** of the **system-parameters features** form, verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the default value of ***Block*** for both fields**.**

```
change system-parameters features                               Page   9 of  18
                        FEATURE-RELATED SYSTEM PARAMETERS

CPN/ANI/ICLID PARAMETERS
   CPN/ANI/ICLID Replacement for Restricted Calls: Block
  CPN/ANI/ICLID Replacement for Unavailable Calls: Block

DISPLAY TEXT
                                       Identity When Bridging: principal
                                        User Guidance Display? n
 Extension only label for Team button on 96xx H.323 terminals? n

INTERNATIONAL CALL ROUTING PARAMETERS
                 Local Country Code:
          International Access Code:

ENBLOC DIALING PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n
```

On **Page 3** of the trunk-group form, set the **Numbering Format** field to ***public***. This field specifies the format of the calling party number (CPN) sent to the far-end. Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to ***y***. This will allow the CPN displayed on local endpoints to be replaced with the value set in this section, if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

```
change trunk-group 301                                          Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y

                     Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y
 Show ANSWERED BY on Display? y
```

4.6.3. Configure REFER Message

Enter the **display system-parameters customer-options** command. On **Page 4** of the form, verify the **ISDN/SIP Network Call Redirection** feature is enabled.

Note: *If a required feature is not enabled, contact an authorized Avaya sales representative to enable the feature.*

```
display system-parameters customer-options                      Page   4 of  11
                                OPTIONAL FEATURES

   Emergency Access to Attendant? n                                IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                           ISDN Feature Plus? n
                  Enhanced EC500? y        ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                             ISDN-BRI Trunks? n
       Enterprise Wide Licensing? n                                    ISDN-PRI? y
              ESS Administration? y              Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                    Malicious Call Trace? n
     External Device Alarm Admin? n                Media Encryption Over IP? y
  Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? y                Multifrequency Signaling? y
      Global Call Classification? n         Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y      Multimedia Call Handling (Enhanced)? n
 Hospitality (G3V3 Enhancements)? y              Multimedia IP SIP Trunking? n
                       IP Trunks? y

           IP Attendant Consoles? n
        (NOTE: You must logoff & login to effect the permission changes.)
```

When the **ISDN/SIP Network Call Redirection** field is enabled from the previous screen, the **Network Call Redirection** field on **Page 4** of the trunk-group form will be created. Set the **Network Call Redirection** field to **y**.

```
change trunk-group 301                                          Page   4 of  21
                              PROTOCOL VARIATIONS

                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
                 Network Call Redirection? y
                    Send Diversion Header? y
                  Support Request History? n
             Telephone Event Payload Type:
```

When the **Network Call Redirection** field is enabled, the **Service Type** has to be set to **public-ntwrk**.

```
change trunk-group 301                                          Page   1 of  21
                                TRUNK GROUP

Group Number: 301                  Group Type: sip           CDR Reports: n
  Group Name: PSTN-via-SM                 COR: 1        TN: 1        TAC: 1031
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: public-ntwrk           Auth Code? n

                                                        Signaling Group: 301
                                                      Number of Members: 10
```

4.6.4. Configure Fax Configuration

Use the **change ip-codec-set 1** command to define FAX Mode contained in this set. On **Page 2** of the ip-codec-set form, set the **Fax Mode** field to ***t.38-standard*** for allowing faxing to and from the SimpleSignal side. Retain the default values for the remaining fields, and submit these changes.

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n



                    Mode                 Redundancy
    FAX             t.38-standard           3
    Modem           off                     0
    TDD/TTY         US                      3
    Clear-channel   n                       0
```

4.6.5. Configure Diversion Header/History Info

On **Page 4** of the trunk-group form, set the **Send Diversion Header** and/or **Support Request History** field to ***y***. This field provides additional information to the destination party if the call has been re-directed. This is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

```
change trunk-group 301                                          Page   4 of  21
                              PROTOCOL VARIATIONS

                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
                 Network Call Redirection? n
                    Send Diversion Header? y
                  Support Request History? n
             Telephone Event Payload Type:
```

4.6.6. Configure Calling Party Information

Public unknown numbering defines the calling party number to be sent to the far-end. This calling party number is sent in the SIP "From" header. Use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID number will be one assigned by the SIP service provider. It is used to authenticate the caller.

In the sample configuration, three DID numbers were assigned for testing. These numbers were assigned to extensions 22001, 22003 and 71714. Thus, the same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these three extensions.

```
change public-unknown-numbering 0                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext              Trk       CPN          CPN
Len Code             Grp(s)    Prefix       Len
                                                     Total Administered: 3
 5  22001            301       7204571713   10          Maximum Entries: 9999
 5  22003            301       7204571715   10
 5  71714            301       72045        10
```

4.6.7. Configure Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise callers will dial 9 to reach an “outside line”. The common configuration is illustrated below with little elaboration. Use the **change dialplan analysis** command to define a dialed string beginning with 9 of length 1 as a feature access code (**fac**).

```
change dialplan analysis                                        Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location:  all          Percent Full:    2

       Dialed    Total  Call    Dialed    Total  Call     Dialed    Total  Call
       String    Length Type    String    Length Type     String    Length Type
     0             1    attd   2390         4    aar     4            5    ext
     10            4    dac    26           5    ext     5            5    ext
     11            3    dac    27           5    ext     6            5    ext
     12            3    fac    2800         5    ext     7            5    ext
     126           6    aar    2801         5    aar     8            1    fac
     13            3    fac    2802         5    ext     9            1    fac
     14            3    fac    2803         5    ext     *            3    fac
     15            3    fac    2804         5    ext     #            3    fac
     16            3    fac    2805         5    ext
     17            3    fac    2806         5    ext
     18            3    fac    2807         5    ext
     19            3    fac    2808         5    ext
     2             5    ext    2809         5    ext
     2000          5    ext    3            5    ext
```

Use the **change feature-access-codes** command to configure ***9*** as the **Auto Route Selection (ARS) – Access Code 1**.

```
change feature-access-codes                                     Page   1 of   8
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: *01
         Abbreviated Dialing List2 Access Code: *02
         Abbreviated Dialing List3 Access Code: *03
Abbreviated Dial - Prgm Group List Access Code: *04
                      Announcement Access Code: *05
                       Answer Back Access Code: #06

      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                Automatic Callback Activation: *09     Deactivation: #09
Call Forwarding Activation Busy/DA: #11     All: *10     Deactivation: #10
   Call Forwarding Enhanced Status:         Act:         Deactivation:
                        Call Park Access Code:
```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test including domestic long-distance calls. The highlighted section shown below describes the area code with 720 will go out through the route pattern 301. See **Section 7** for the complete list of call types tested.

```
change ars analysis 720                                         Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location:  all           Percent Full:    2

          Dialed           Total     Route     Call   Node  ANI
          String          Min  Max  Pattern    Type   Num   Reqd
    720                   10   10    301       hnpa          n
    732                   10   10    80        hnpa          n
```

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 301 during the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 301 was connected to SimpleSignal.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of ***0*** is the least restrictive level.
- **Pfx Mrk**: The prefix mark (**Pfx Mrk**) is left blank.

```
change route-pattern 301                                        Page   1 of   3
                    Pattern Number: 301 Pattern Name: To ASM
                             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: 301  0                                                               n   user
 2:                                                                      n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                        none
 2: y y y y y n  n            rest                                        none
```

4.6.8. Configure Inbound Routing

Incoming call handling treatment is applied to inbound calls to direct them to the proper destination. Use the **change inc-call-handling-trmt trunk-group *x*** command (where ***x*** is the service provider trunk group) to define the proper digit manipulation for each DID number to map it to an internal extension. The example below shows the DID numbers used in the compliance test.

```
change inc-call-handling-trmt trunk-group 301                    Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature         Len     Digits
 tie             10 7204571713       10  22001
 tie             10 7204571714       5
 tie             10 7204571715       10  22003
```

5. Configure Avaya Aura™ Session Manager

This section provides the procedures for configuring Session Manager as provisioned in the reference configuration. Session Manager is comprised of two functional components: the Session Manager server and the System Manager server. All SIP call provisioning for Session Manager is performed through the System Manager Web interface and is then downloaded into Session Manager.

The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

Session Manager is comprised of two main network components, the server itself and the SM-100 card.

The Session Manager server has two network interface ports with one being the port used for management/provisioning of Session Manager. This port must have network connectivity to System Manager.

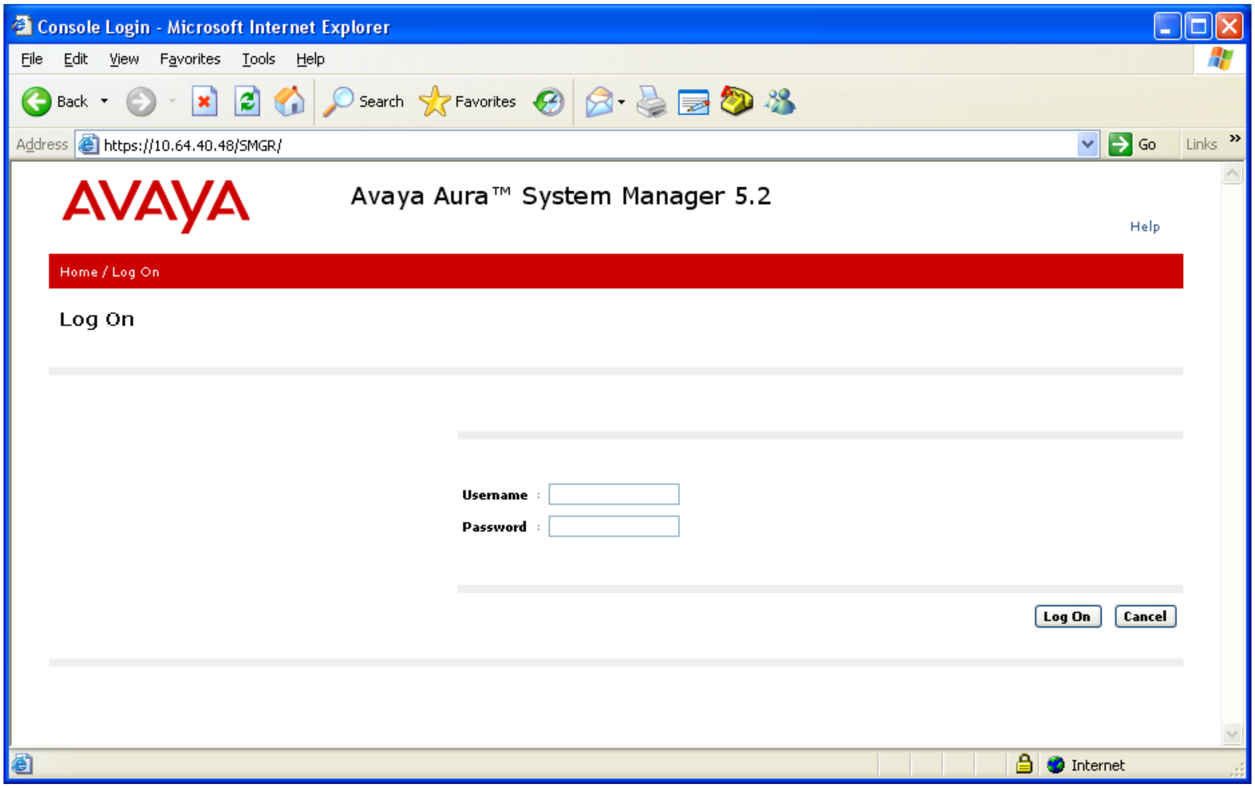
The Session Manager SM-100 card has four network interface ports, with one being the connection to the SIP VoIP network. This interface is used for all inbound and outbound SIP signaling and must have network connectivity to all provisioned SIP Entities.

In this section, the following topics are discussed:

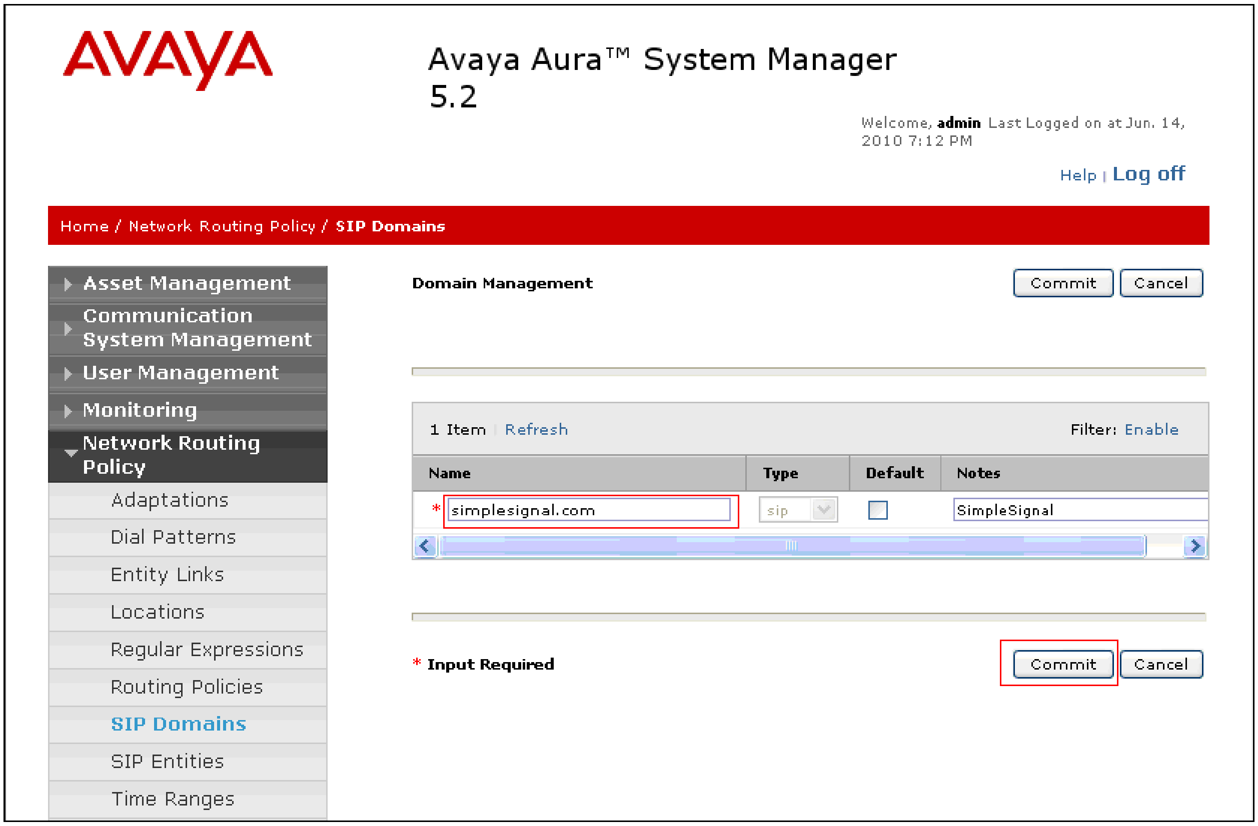
- SIP Domains
- Locations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policy
- Dial Patterns

5.1. Configure SIP Domain

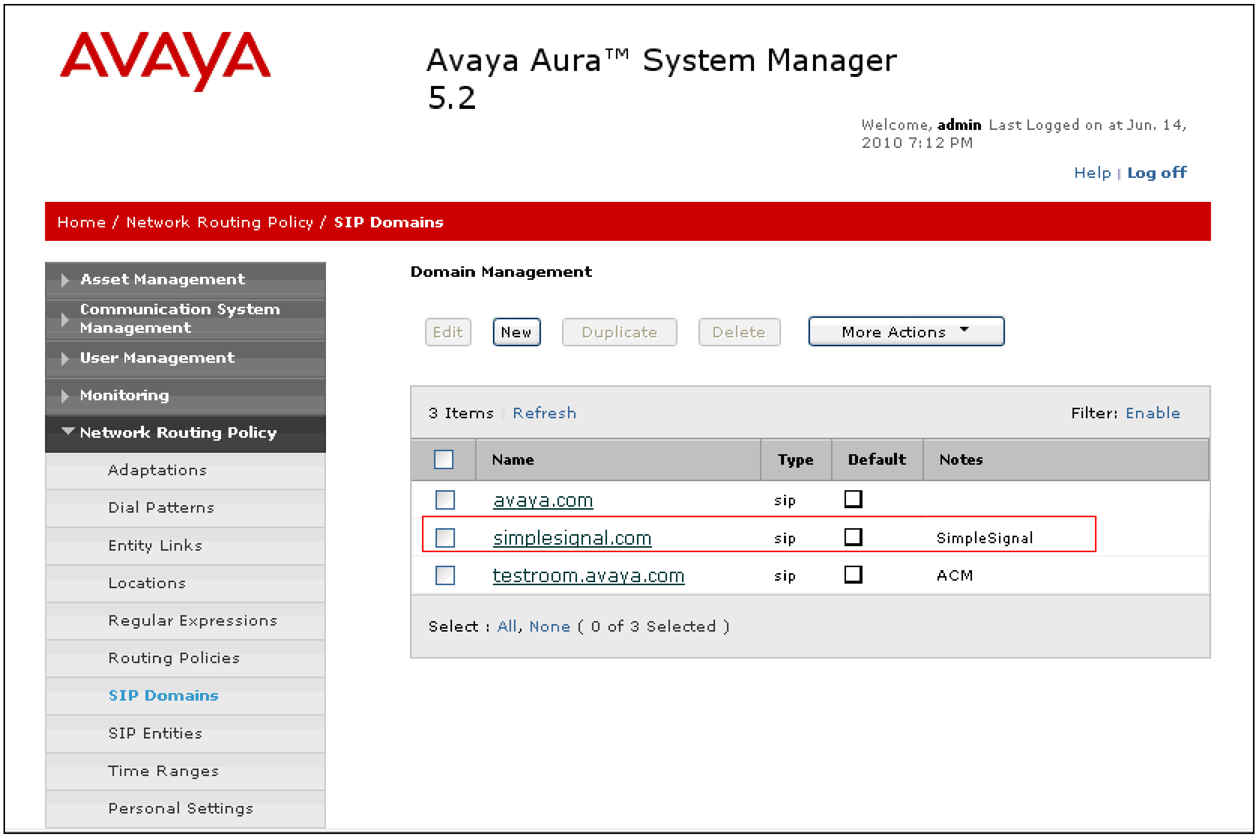
Launch a web browser, enter **http://<IP address of System Manager>/SMGR** in the URL, and log in with the appropriate credentials.



Navigate to **Network Routing Policy → SIP Domains**, and click on the **New** button to create a new SIP Domain. During the compliance test, **simplesignal.com** was utilized as a SIP Domain. Click on the **Commit** button.



The following screen shows the SIP Domain page used during the compliance test.

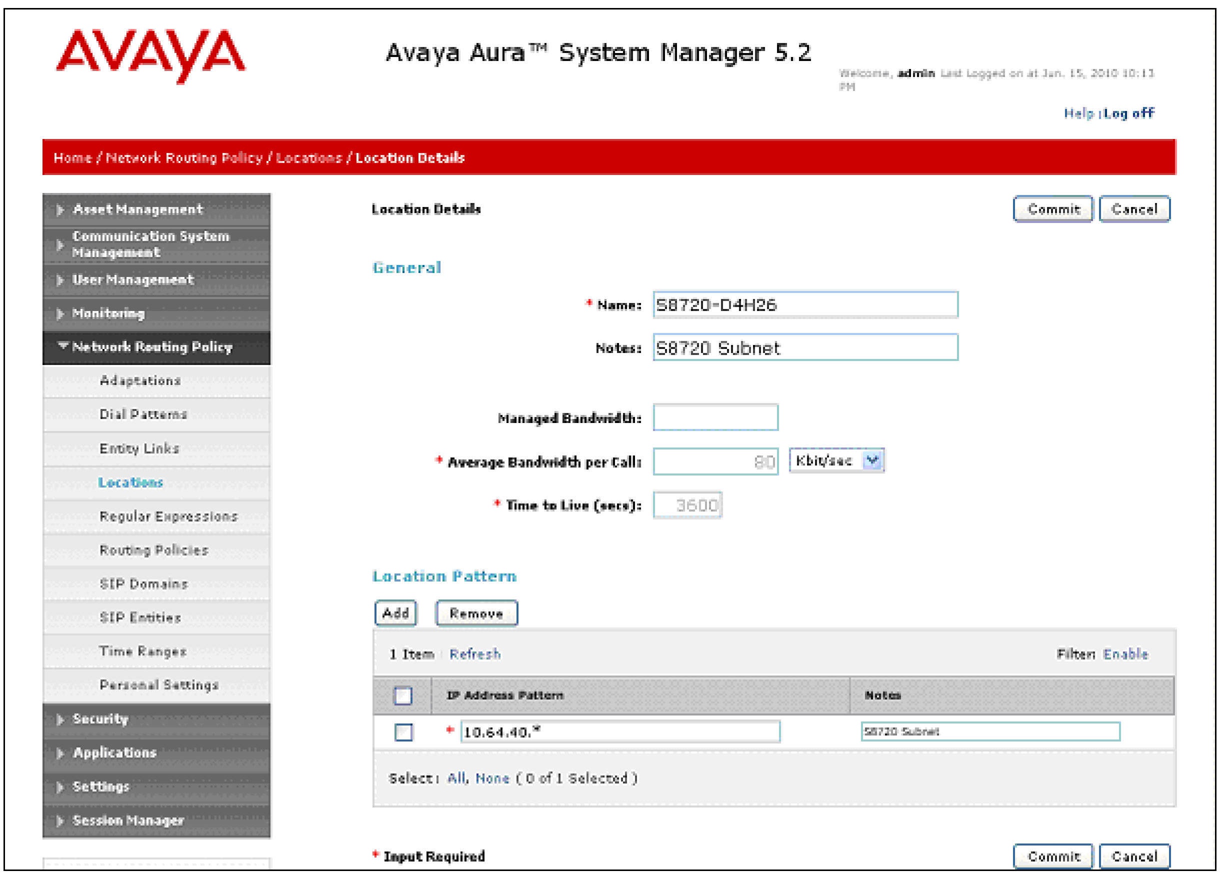


5.2. Configure Locations

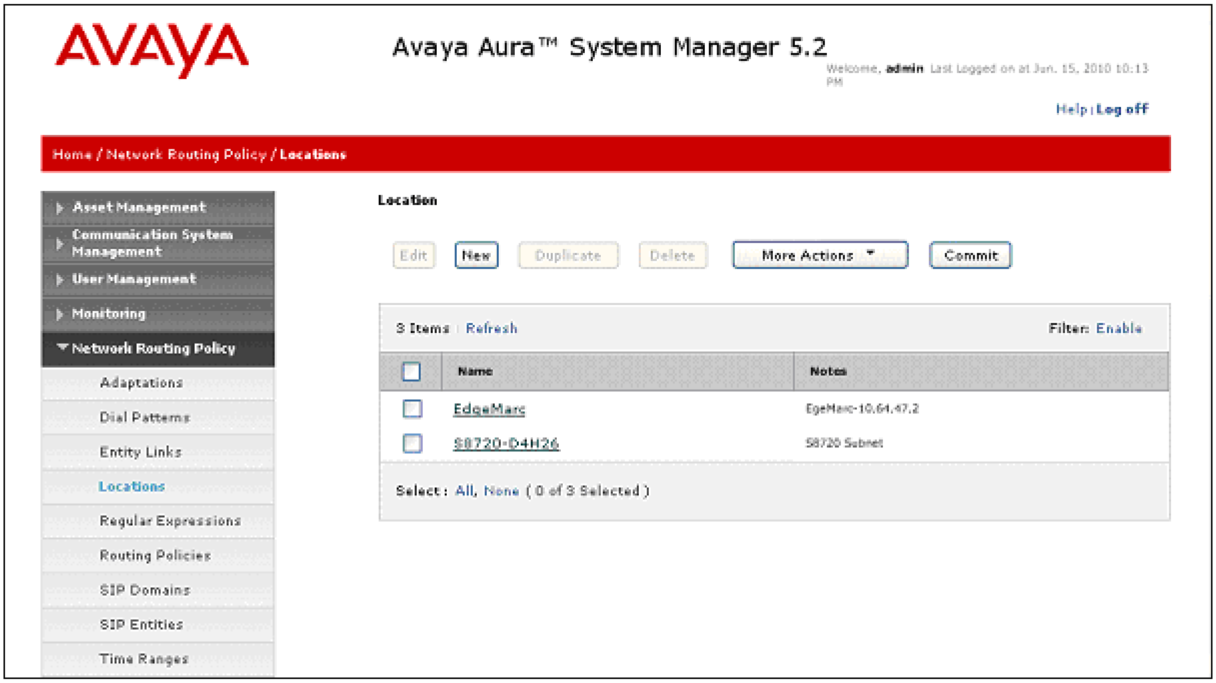
Locations are used to identify logical and/or physical locations where SIP Entities reside, by specifying the IP addressing for the locations as well as for purposes of bandwidth management if required. In the reference configuration, only the Avaya CPE site was defined as a Location.

To add a Location, select **Locations** in the left **Network Routing Policy** menu and click on the **New** button on the right. The screen shown below will open.

1. Enter a descriptive Location name in the Name field (e.g. **S8720-D4H26**).
2. Enter a description in the **Notes** field if desired.
3. Under the **Location Pattern** heading, click on **Add**.
4. Enter the IP address information for the Location (e.g. **10.64.40.***)
5. Enter a description in the **Notes** field if desired.
6. Repeat steps 3 thru 5 if the Location has multiple IP segments.
7. Modify the remaining values on the form, if necessary; otherwise, use all the default values.
8. Click on the **Commit** button.
9. Repeat all the steps for each new Location.



The following screen shows the Locations page used during the compliance test.



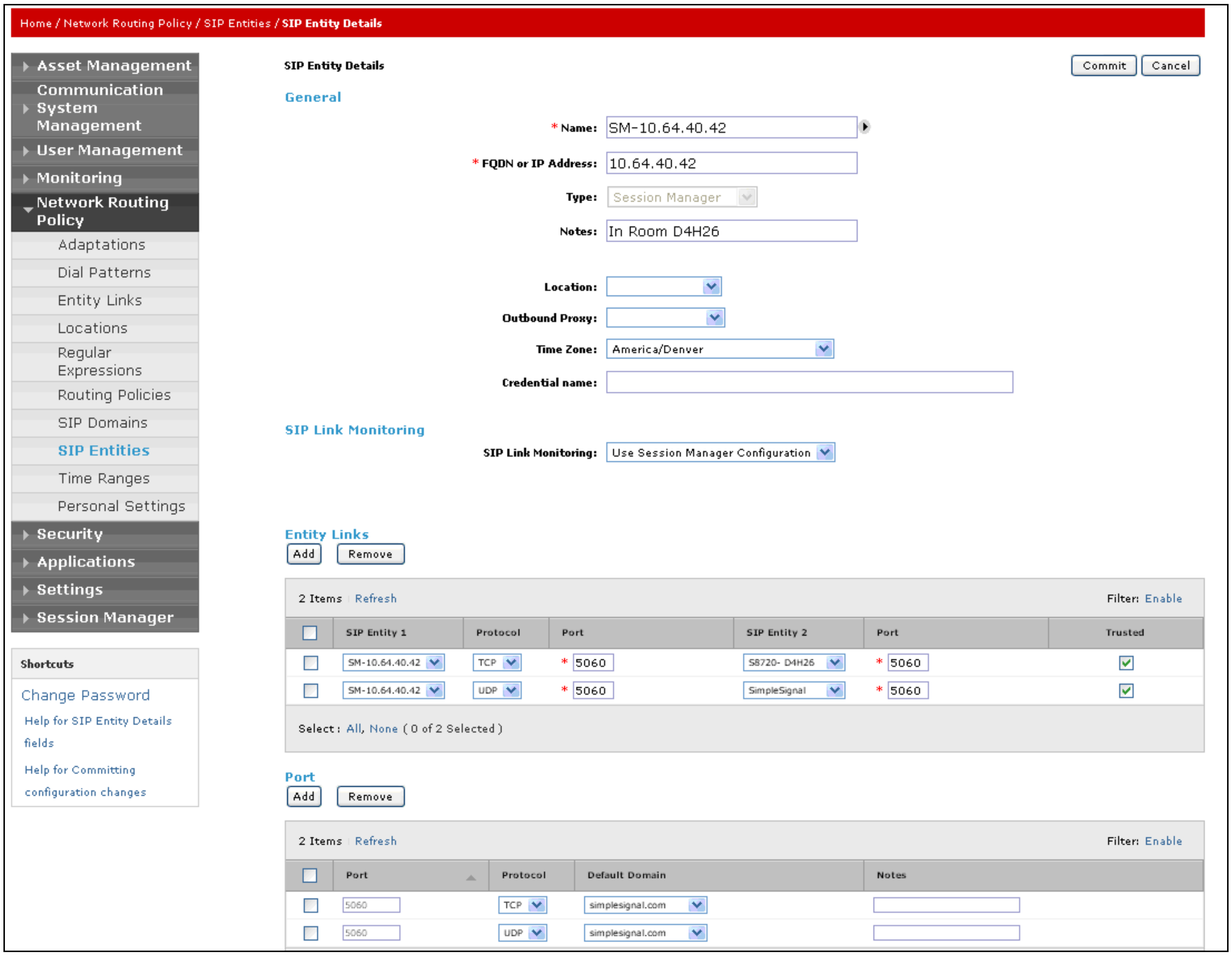
5.3. Configure SIP Entities

A SIP Entity must be added for Session Manager and for each network component that has a SIP trunk provisioned to Session Manager. During the compliance test, the following SIP Entities were configured:

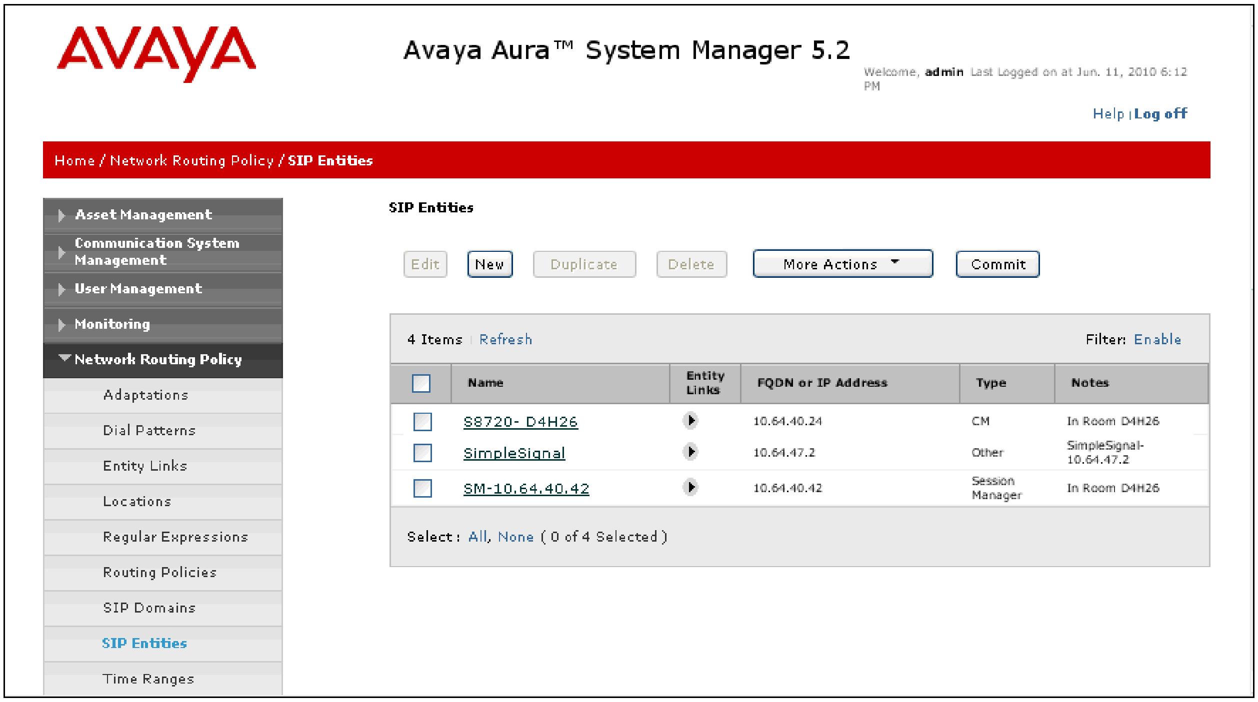
- Session Manager itself.
- Communication Manager
- SimpleSignal SBC (EdgeMarc 4500)

Navigate to **Network Routing Policy → SIP Entities**, and click on the **New** button to create a new SIP entity. Provide the following information:

1. **General** Section
    a. Enter a descriptive Location name in the **Name** field.
    b. Enter the IP address for the SIP Entity.
    c. From the **Type** drop down menu select a type that best matches the SIP Entity (e.g. **Session Manager**).
    d. Enter a description in the **Notes** field if desired.
    e. Select the appropriate time zone.
    f. Accept the other default values.
2. **Sip Link Monitoring** section
    a. Select the desired option.
3. **Port** section
    a. When defining a SIP Entity for Session Manager itself and **Session Manager** is selected from the **Type** drop down menu, an additional section called **Ports** will appear. Click **Add**, then edit the fields in the resulting new row:
        - Enter the **Port** number on which the system listens for SIP requests.
        - Select the transport **Protocol** to be used.
        - Select the SIP Domain configured in **Section 5.1** for the **Default Domain**.
    b. Repeat step 3 for each Port to be configured.
4. Click on **Commit**.
5. Repeat these steps for each SIP Entity.


Home / Network Routing Policy / SIP Entities / SIP Entity Details
Asset Management
Communication System Management
User Management
Monitoring
Network Routing Policy
Adaptations
Dial Patterns
Entity Links
Locations
Regular Expressions
Routing Policies
SIP Domains
SIP Entities
Time Ranges
Personal Settings
Security
Applications
Settings
Session Manager
Shortcuts
Change Password
Help for SIP Entity Details fields
Help for Committing configuration changes
SIP Entity Details
Commit
Cancel
General
* Name: SM-10.64.40.42
* FQDN or IP Address: 10.64.40.42
Type: Session Manager
Notes: In Room D4H26
Location:
Outbound Proxy:
Time Zone: America/Denver
Credential name:
SIP Link Monitoring
SIP Link Monitoring: Use Session Manager Configuration
Entity Links
Add
Remove
2 Items Refresh
Filter: Enable
SIP Entity 1
Protocol
Port
SIP Entity 2
Port
Trusted
SM-10.64.40.42
TCP
* 5060
S8720- D4H26
* 5060
SM-10.64.40.42
UDP
* 5060
SimpleSignal
* 5060
Select : All, None (0 of 2 Selected)
Port
Add
Remove
2 Items Refresh
Filter: Enable
Port
Protocol
Default Domain
Notes
5060
TCP
simplesignal.com
5060
UDP
simplesignal.com

The following screen shows the SIP Entities page used during the compliance test.



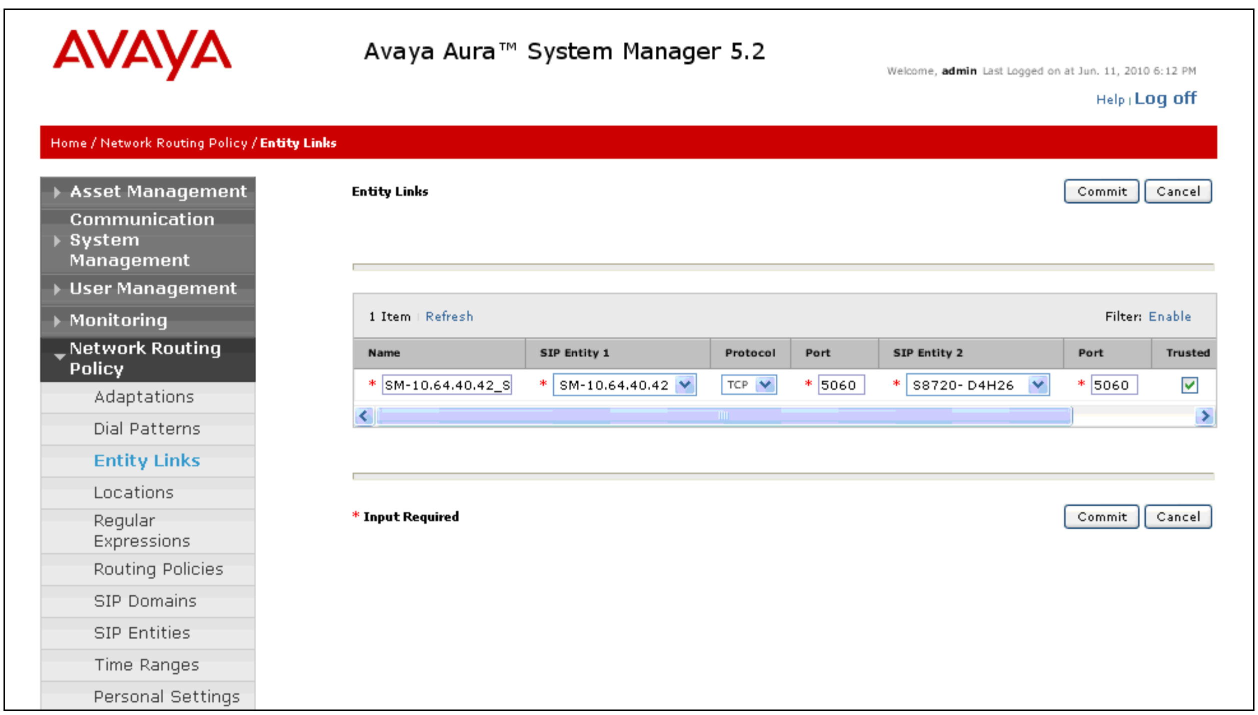
5.4. Configure Entity Links

Entity Links define the connections between the SIP Entities and Session Manager. In the reference configuration, Entity Links are defined between Session Manager and:

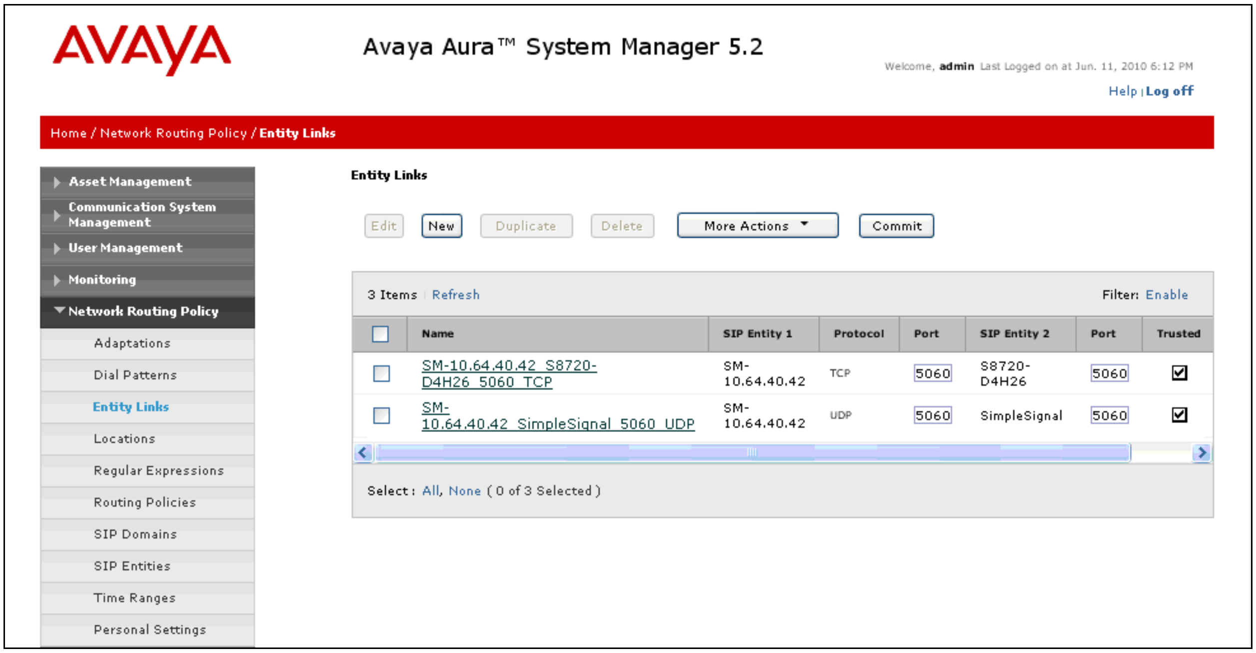
- Communication Manager
- SimpleSignal SBC (EdgeMarc 4500)

Navigate to **Network Routing Policy → Entity Links**, and click on the **New** button to create a new entity link. Provide the following information:

1. Enter a descriptive name in the **Name** field.
2. In the **SIP Entity 1** drop down menu, select the Session Manager SIP Entity created in **Section 5.3** (e.g. **SM-10.64.40.42**).
3. In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).
4. In the **SIP Entity 2** drop down menu, select one of the two entities in the bullet list above (which were created in **Section 5.3**).
5. In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).
6. Check the **Trusted** box.
7. In the **Protocol** drop down menu, select the protocol to be used.
8. Enter a description in the **Notes** field if desired (not shown).
9. Click on the **Commit** button.



The following screen shows the Entity Links page used during the compliance test.

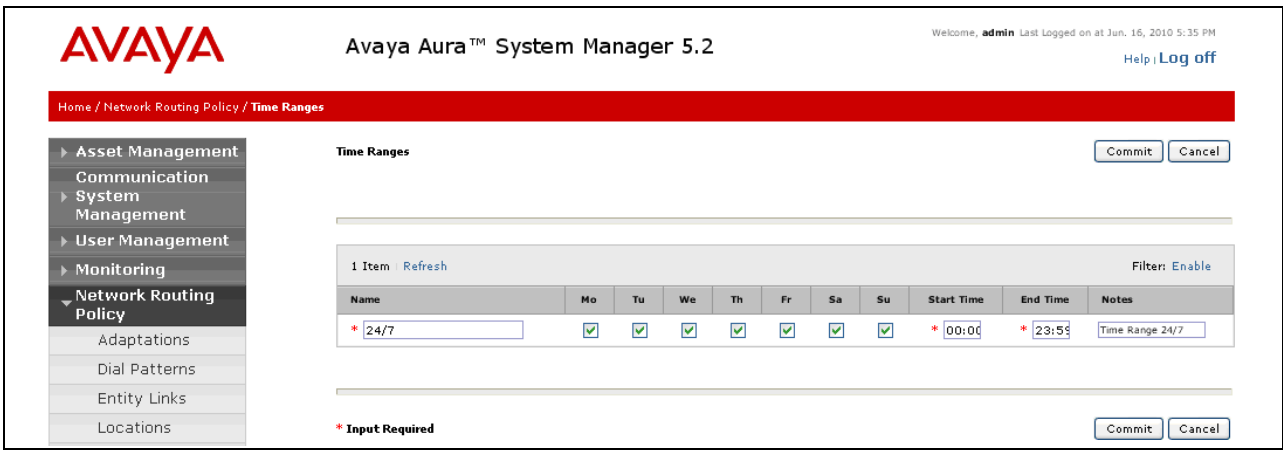


5.5. Time Ranges

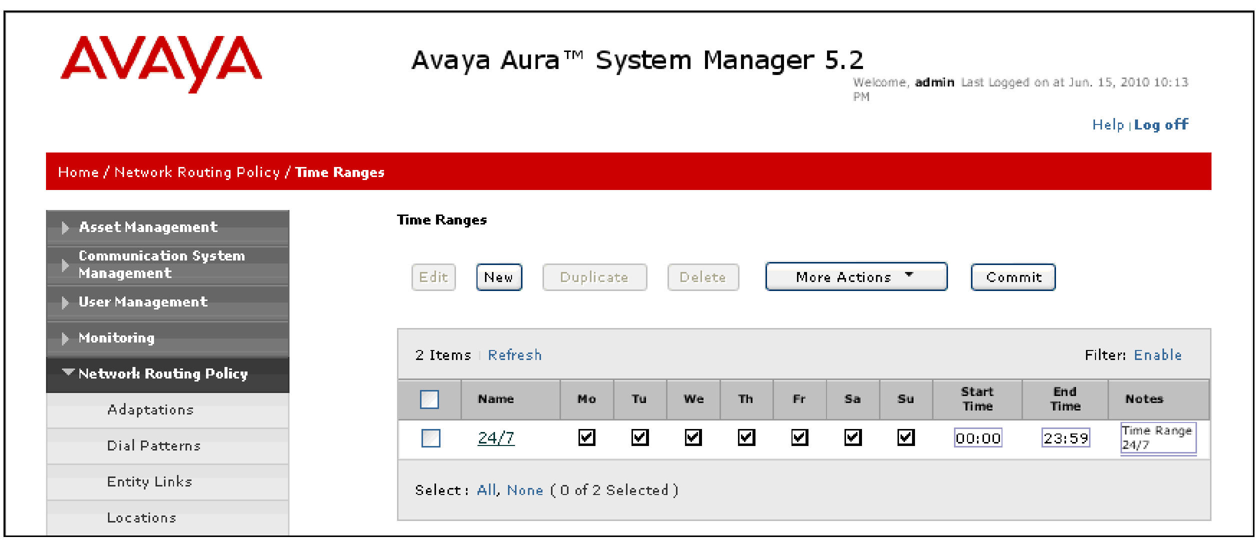
The Time Ranges form allows admission control criteria to be specified for Routing Policies (**Section 5.6**). In the reference configuration, no restrictions were used.

To add a Time Range, navigate to **Network Routing Policy → Time Ranges**, and click on the **New** button on the right. Provide the following information:

1. Enter a descriptive Location name in the **Name** field (e.g. **24/7**).
2. Check each day of the week.
3. In the **Start Time** field, enter **00:00**.
4. In the **End Time** field, enter **23:59**.
5. Enter a description in the **Notes** field if desired.
6. Click the **Commit** button.



The following screen shows the Time Range page used during the compliance test.



5.6. Configure Routing Policy

Routing Policies associate destination SIP Entities (**Section 5.3**) with Time of Day admission control parameters (**Section 5.5**) and Dial Patterns (**Section 5.7**). In the reference configuration, Routing Policies are defined for:

- Inbound calls to Communication Manager.
- Outbound calls to the SimpleSignal SBC (EdgeMarc 4500).

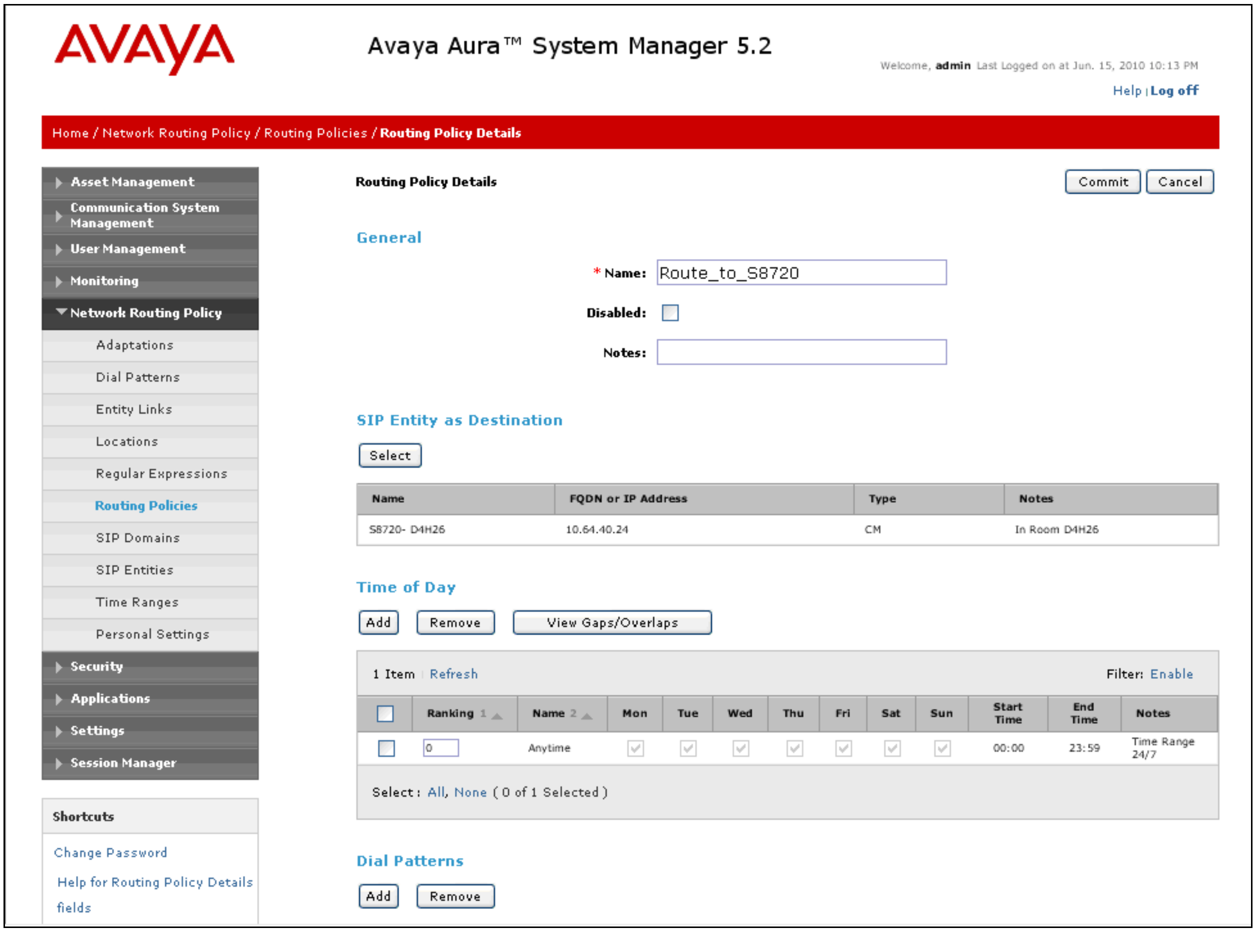
To add a Routing Policy, navigate to **Network Routing Policy → Routing Policy**, and click on the **New** button on the right. Provide the following information:

1. **General** section
   a. Enter a descriptive name in the **Name** field.
   b. Enter a description in the **Notes** field if desired.
2. **SIP Entity as Destination** section
   a. Click the **Select** button.
   b. Select the SIP Entity that will be the destination for this call.
   c. Click the **Select** button and return to the Routing Policy Details form.
3. **Time of Day** section
   a. Leave default values.

   Note – Multiple time ranges may be selected and a Ranking value applied (0 is the highest).
4. **Dial Pattern** section

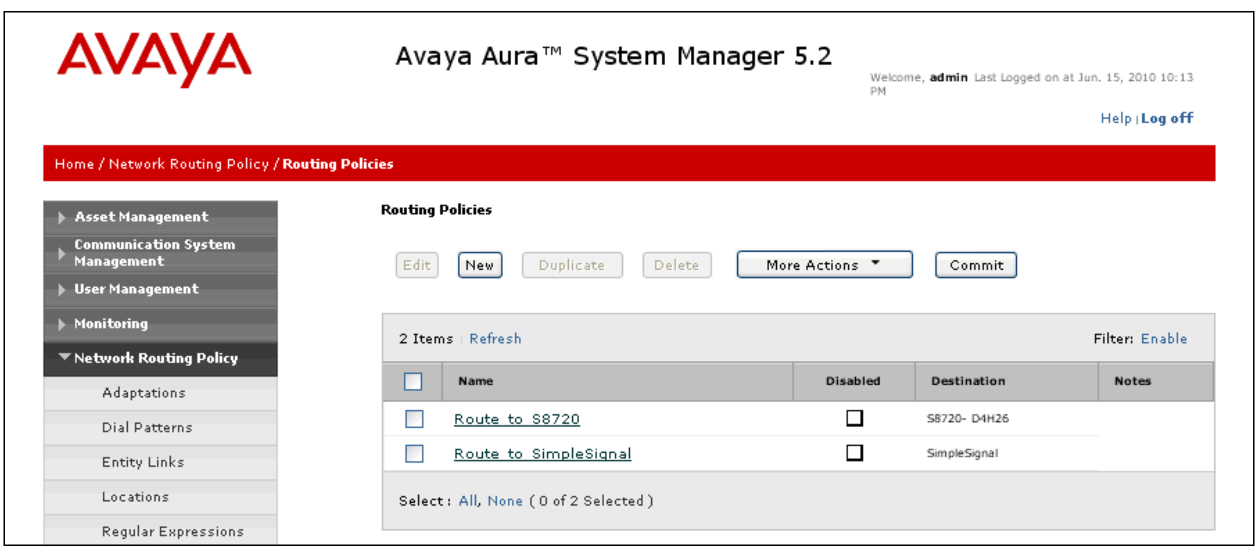
   Note – This step may be skipped. Dial Patterns will be mapped to Routing Policies in **Section 5.7**.

   a. Click the **Add** button and select the **Dial Pattern** for this Routing Policy.
   b. Click on **Select** and return to the Routing Policy Details form.



5. Click the **Commit** button.
6. Repeat steps 1 thru 5 for each Routing Policy.

The following screen shows the Routing Policy page used during the compliance test.

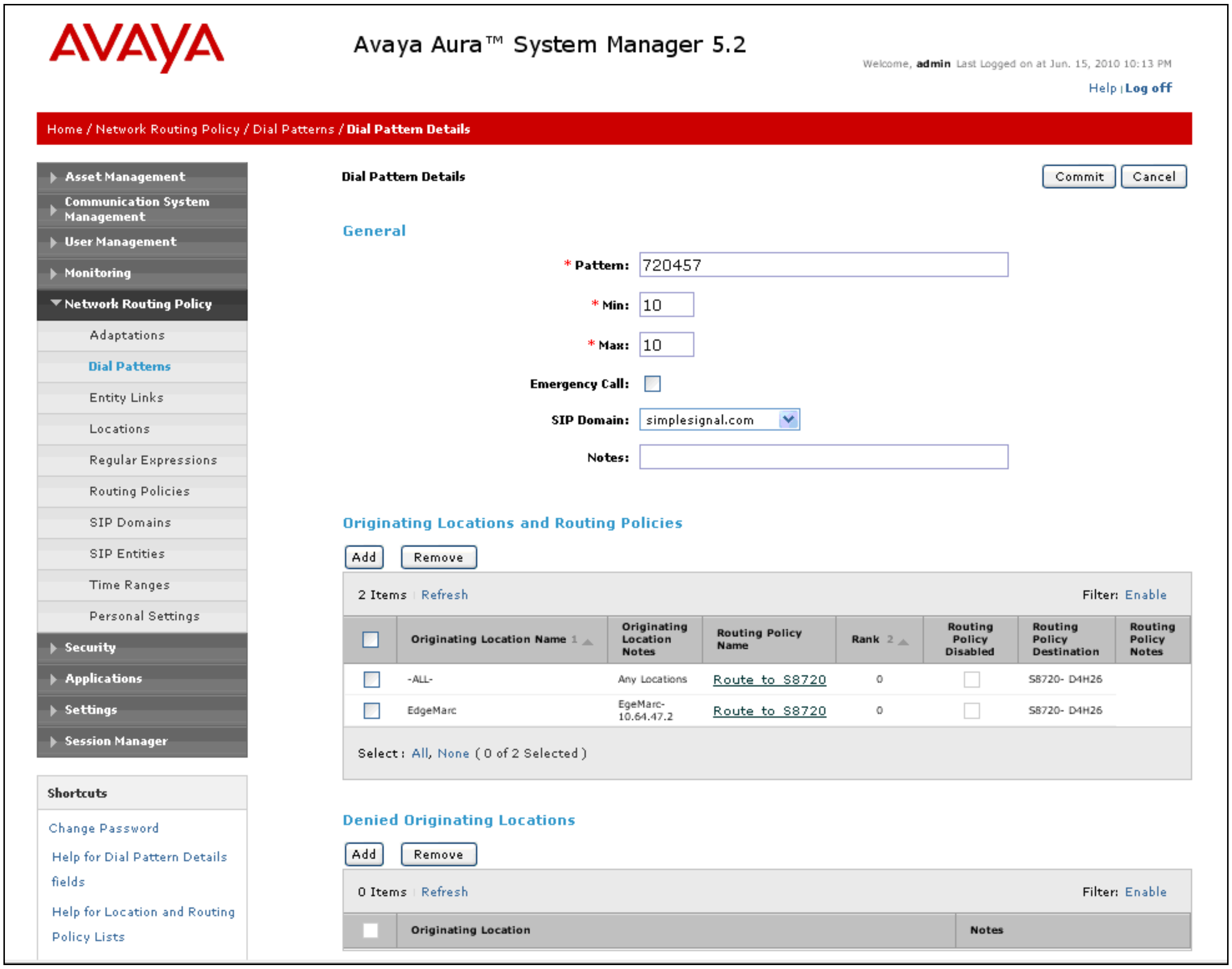


5.7. Dial Patterns

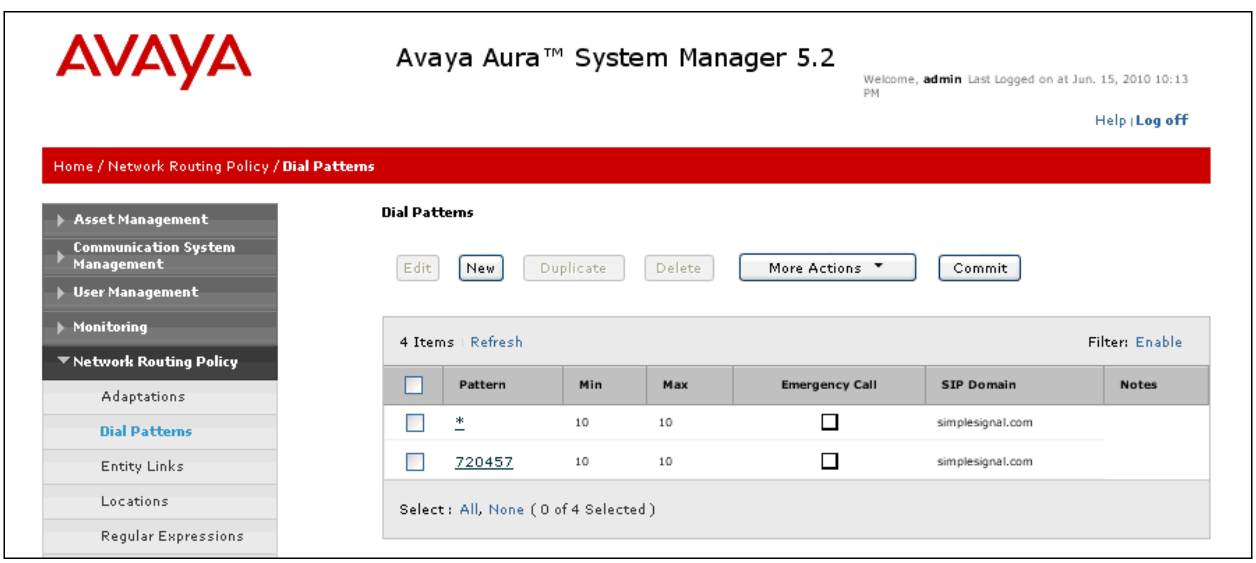
Dial Patterns define digit strings to be matched for inbound and outbound calls. In addition, the domain in the request URI is also examined.

To add a Dial Pattern, select **Network Routing Policy → Dial Patterns,** and click on the **New** button on the right. The screen shown below is displayed. In this example, a Request URI to a 10 digit number beginning with *720457xxxx*, and sent from SimpleSignal, is defined (this would be an inbound call to Communication Manager. Any other digit is sent to SimpleSignal SIP trunk service.

1. **General** section
    a. Enter a unique pattern in the **Pattern** field (e.g. **720457**).
    b. In the **Min** field enter the minimum number of digits (e.g. **10**).
    c. In the **Max** field enter the maximum number of digits (e.g. **10**).
    d. In the **SIP Domain** field drop down menu select the domain that will be contained in the Request URI *received* by Session Manager from Communication Manager.
    e. Enter a description in the **Notes** field if desired.
2. **Originating Locations and Routing Policies** Section
    a. Click on the **Add** button and a window will open (not shown).
    b. Click on the boxes for the appropriate Originating Locations (see **Section 5.2**), and Routing Policies (see **Section 5.6**) that pertain to this Dial Pattern.
        i. Location **10.64.40.0**.
        ii. Routing Policies **Route_to_S8720**.
    c. Click on the **Select** button and return to the Dial Pattern window.
3. Click the **Commit** button
4. Repeat steps 1 thru 3 for the remaining Dial Patterns.



The following screen shows the Dial Patterns page used during the compliance test.



6. SimpleSignal Services Configuration

To use SimpleSignal SIP Trunk Service, a customer must request service from SimpleSignal using their sales processes. The process can be started by contacting SimpleSignal via the corporate web site at http://www.simplesignal.com and requesting information via the online sales links or telephone numbers.

7. General Test Approach and Test Results

This section describes the interoperability compliance testing used to verify SIP trunk interoperability between the SimpleSignal SIP Trunk Service and an Avaya IP Telephony Solution.

A simulated enterprise site using an Avaya IP telephony solution was connected to the public Internet using a dedicated broadband connection. The enterprise site was configured to use the commercially available SIP Trunk Service provided by SimpleSignal.

The compliance test included the following:

- Incoming calls to the enterprise site from the PSTN were routed to the DID numbers assigned by SimpleSignal. Incoming PSTN calls were made to H.323, digital, and analog telephones at the enterprise.
- Outgoing calls from the enterprise site were completed via SimpleSignal to PSTN destinations. Outgoing calls from the enterprise to the PSTN were made from H.323, digital, and analog telephones.
- Various call types were tested including: local, long distance, international, outbound toll-free, operator, and directory assistance.
- Calls using G.729A, G.711MU, and G.711A coders.
- DTMF transmission using RFC 2833 with successful vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and extension to cellular, when the call arrived across the SIP Trunk from SimpleSignal, or when the call forwarding destination and extension to cellular mobile number routed out the SIP Trunk to SimpleSignal, or both.
- Caller ID Presentation and Caller ID Restriction.
- Avaya IP Softphone in both “Road Warrior” and “Telecommuter” modes, where incoming PSTN calls arrived from SimpleSignal, or the telecommute number routed out the SIP Trunk to SimpleSignal, or both.

Interoperability testing of the sample configuration was completed with successful results for the SimpleSignal Trunk Service. SimpleSignal provided the following services, and calls were made during the compliance test:

- CPN Block call
- Fax: T.38 fax is supported and tested by SimpleSignal.
- Inbound toll-free calls
- Outbound toll-free calls
- Operator Assisted call
- International call
- Emergency call
- Local Directory Assistance call

During the compliance test, the following limitation was observed:

- Direct IP-IP Audio Connections, otherwise known as shuffling, did not work due to issues with incoming call scenarios; thus the shuffling was turned off during the compliance test.

8. Verification Steps

This section provides verification steps that may be performed in the field to verify that the H.323, digital and analog endpoints can place outbound and receive inbound PSTN calls using the SimpleSignal SIP Trunk Service.

1. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
2. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active for more than 35 seconds.
3. Verify that the user on the PSTN can end an active call by hanging up.
4. Verify that an endpoint at the enterprise site can end an active call by hanging up.

9. Conclusion

These Application Notes describe the configuration necessary to connect Communication Manager and Session Manager to the SimpleSignal SIP Trunk Service. The SimpleSignal SIP Trunk Service is a SIP-based Voice over IP solution for customers ranging from small and midsize businesses to large enterprises. The SimpleSignal SIP Trunk Service provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunk lines.

During the DevConnect compliance test with the SimpleSignal SIP Trunk Service, Direct IP-IP Audio Connections, otherwise known as shuffling, did not work due to issues with incoming call scenarios; thus the recommendation was to turn shuffling off.

10. References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at http://support.avaya.com.

[1] *Administering Avaya Aura™ Communication Manager*, May 2009, Document Number 03-300509.

[2] *Administering Avaya Aura™ Session Manager,* March 2010, Document number 03-603324

[3] *Avaya Extension to Cellular and Off-PBX Station (OPS) Installation and Administration Guide*, June 2005, Document Number 210-100-500.

[4] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide,* November 2009, Document Number 16-300698

[5] RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information, http://www.ietf.org/

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.