Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager Server R6.0, Avaya Aura® Session Manager R6.1, and Avaya Session Border Controller for Enterprise R4.0.5 with Windstream – Issue 1.0

Abstract

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 6.1, Avaya Aura® Communication Manager Release 6.0.1, and Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 4.0.5 with the Windstream system.

The Windstream offer referenced within these Application Notes is designed for business customers with an Avaya SIP trunk solution. The service provides local and/or long distance PSTN calling via standards-based SIP trunks directly, without the need for additional TDM enterprise gateways or TDM cards and the associated maintenance costs.

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 Interoperability Test Lab, utilizing a Windstream circuit connection to the production Windstream Service.

©2012 Avaya Inc. All Rights Reserved.

Table of Contents

©2012 Avaya Inc. All Rights Reserved.

©2012 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 6.1, Avaya Aura® Communication Manager Release 6.0.1, and Avaya Session Border Controller for Enterprise Release 4.0.5 with the Windstream service. The Windstream Service provides local and/or long-distance calls (with PSTN endpoints) via standards-based SIP trunks.

2. General Test Approach and Test Results

Communication Manager connects to Avaya SBCE via Session Manager using a SIP connection. Avaya SBCE connects to the Windstream system using SIP signaling. Various call types were made between Communication Manager and the Windstream service to verify the interoperability.

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 scenarios for the configuration described in these Application Notes included the following:

- General call processing between Communication Manager and Windstream service including:
    - Codec/ptime (G.711 u-law / 20ms, G.729 / 20ms)
    - Hold/Retrieve on both ends
    - Caller ID (CLID) display
    - Ring-back tone
    - Talk path
    - Dial plan support
    - Advanced features (Call on Mute, Call Park, Call Waiting)
    - Abandoned Call
- Call redirection verification: all supported methods (blind transfer, consultative transfer, call forward, and conference) including CLID. Call redirection is performed from both ends
- UUI (User to User Information) - Call Redirect Capability
- DTMF in both directions
- SIP Transport UDP, TCP: Used TCP within CPE and UDP with Windstream
- Early Media Transmission

©2012 Avaya Inc. All Rights Reserved.

The following assumptions were made for this lab test configuration:

- Avaya Aura® Communication Manager is implemented R6.0.1 software and the latest service packs.
- Windstream provides support to setup, configure and troubleshoot on carrier switch during test execution.

During testing, the following activities were performed for each test scenario:

- Calls were checked for the correct call progress tones and cadences.
- During the ringing state, the ring back tone and destination ringing were verified.
- Calls were verified for both hands-free and handset mode due to internal Avaya requirement.
- Calls were verified for quality and talk path in both directions.
- The display(s) of the sets/ VoIP software phone involved were checked for consistent and expected CLID and redirection information both prior to answer and after call establishment.
- The Communication Manager maintenance terminal window was open during the test cases execution for the monitoring of BUG(s), ERR messages. Eg: Use command: list trace tac *010 to monitor the call.

2.2. Test Result

No limitations were found during testing.

2.3. Support

For technical support on the Avaya products described in these Application Notes visit http://support.avaya.com

For technical support on Windstream system, please contact Windstream technical support at:

- Toll Free: 1-800-843-9214
- http://www.windstreambusiness.com/support-center.html

©2012 Avaya Inc. All Rights Reserved.

3. Reference Configuration

Figure 1 illustrates the test configuration used during the compliance testing between Communication Manager and Windstream systems. For confidentiality and privacy purposes, actual public IP addresses used in this testing have been masked out and replaced with fictitious IP addresses throughout the document.

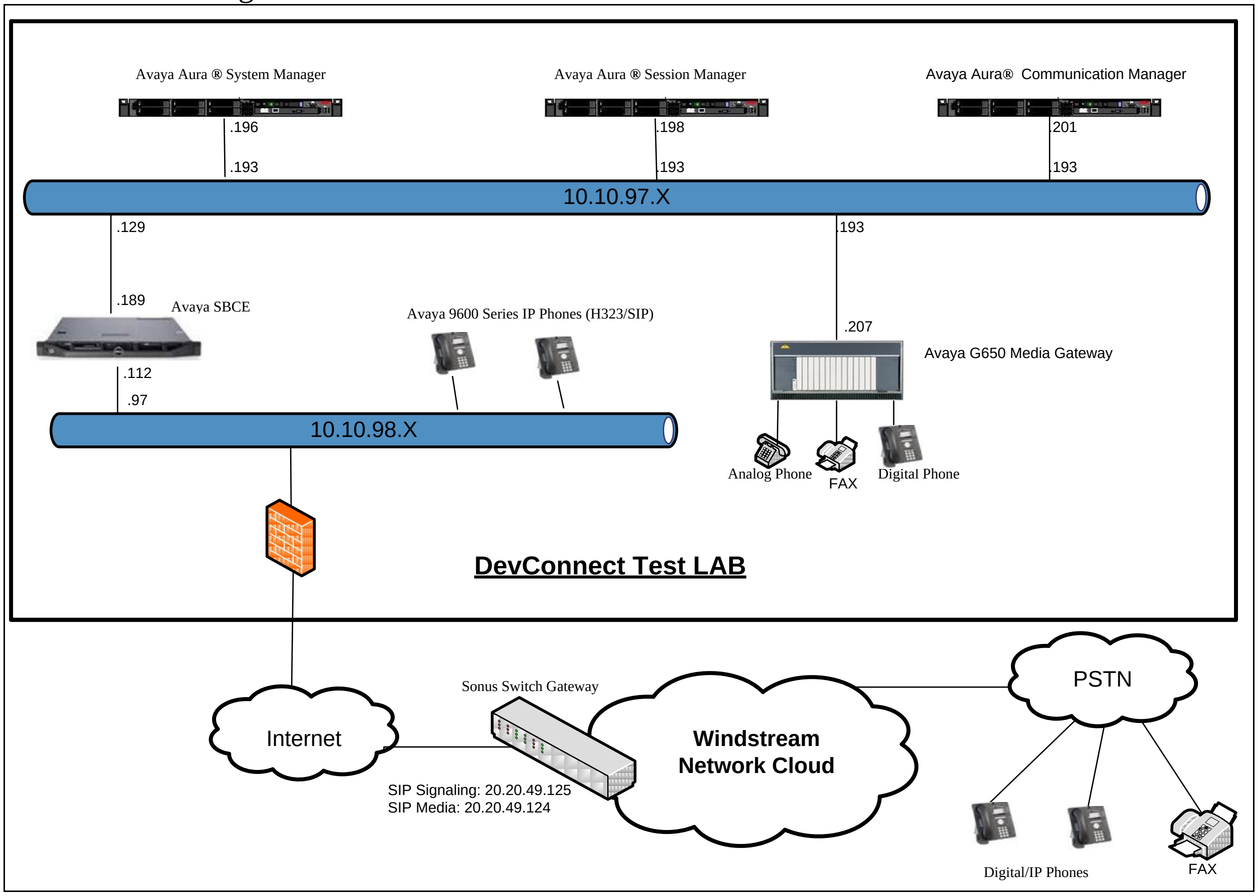


Figure 1- Reference Configuration

©2012 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

Avaya system:

Equipment	Release
Avaya S8800 Server	Avaya Aura® Communication Manager R6.0.1 (R016x00.1.510.1-19350
Avaya G650 Media Gateway TN2224B (Digital Line Card) TN793B (Analog Line Card) MediaPro	 HW12 HW6 FW95
Avaya S8800 Server	Avaya Aura® Session Manager R6.1.1.0.611023
Avaya S8800 Server	Avaya Aura ®System Manager R6.1.4.0 + SP0.r873
Avaya Dell R210 V2 Server	Avaya Session Border Controller for Enterprise R4.0.5 Q02
Avaya 9611 Phone (H323)	3.11
Avaya 96xx IP Phone (SIP)	6_0_3-120511
Avaya 9404 Digital Phone	N/A
Analog Phone	N/A

Windstream system:

Equipment	Software
Sonus Switch	7.3.5
Gateway	7.3.5

©2012 Avaya Inc. All Rights Reserved.

5. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring Communication Manager for SIP signaling. SIP trunks are established between Communication Manager and Session Manager. These SIP trunks will carry SIP signaling associated with Windstream SIP Trunk Service. For incoming calls, the Session Manager receives SIP messages from Windstream via Session Border Controller and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signaling is routed to Session Manager. Session Manager directs the outbound SIP messages to Windstream network via Session Border Controller. Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation.

5.1. Verify Licensed Features

The Communication Manager license file controls the maximum values for licensed features. Contact an authorized Avaya sales representative for assistance if a required feature needs to be enabled or there is insufficient capacity.

Use the **display system-parameters customer-options** command and on **Page 2,** verify that the **Maximum Administered SIP Trunks** are sufficient for the combination of trunks to the Windstream and any other SIP applications.

```
display system-parameters customer-options                      Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                                USED
                     Maximum Administered H.323 Trunks: 450   0
           Maximum Concurrently Registered IP Stations: 450   2
             Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
              Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 0     0
                        Maximum Video Capable Stations: 0     0
                   Maximum Video Capable IP Softphones: 0     0
                       Maximum Administered SIP Trunks: 450   75
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                             Maximum TN2501 VAL Boards: 0     0
                     Maximum Media Gateway VAL Sources: 0     0
           Maximum TN2602 Boards with 80 VoIP Channels: 0     0
          Maximum TN2602 Boards with 320 VoIP Channels: 0     0
   Maximum Number of Expanded Meet-me Conference Ports: 0     0
```


©2012 Avaya Inc. All Rights Reserved.

On **Page 3**, verify that **ARS** is set to **y**.

```
display system-parameters customer-options                     Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? n           Audible Message Waiting? n
        Access Security Gateway (ASG)? n               Authorization Codes? n
        Analog Trunk Incoming Call ID? n                        CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? n                          CAS Main? n
Answer Supervision by Call Classifier? n                 Change COR by FAC? n
                                  ARS? y   Computer Telephony Adjunct Links? n
                 ARS/AAR Partitioning? y      Cvg Of Calls Redirected Off-net? n
          ARS/AAR Dialing without FAC? y                       DCS (Basic)? n
          ASAI Link Core Capabilities? y                 DCS Call Coverage? n
          ASAI Link Plus Capabilities? y                DCS with Rerouting? n
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n     Digital Loss Plan Modification? n
              ATM WAN Spare Processor? n                           DS1 MSP? n
                                ATMS? n             DS1 Echo Cancellation? y
                  Attendant Vectoring? n
```

On **Page 5**, verify that **Private Networking** and **Processor Ethernet** are set to **y**.

```
display system-parameters customer-options                     Page   5 of  11
                                OPTIONAL FEATURES

                Multinational Locations? n                 Station and Trunk MSP? n
 Multiple Level Precedence & Preemption? n      Station as Virtual Extension? n
                     Multiple Locations? n
                                               System Management Data Transfer? n
          Personal Station Access (PSA)? y               Tenant Partitioning? n
                       PNC Duplication? n      Terminal Trans. Init. (TTI)? y
                   Port Network Support? n               Time of Day Routing? n
                        Posted Messages? n      TN2501 VAL Maximum Capacity? y
                   Uniform Dialing Plan? y
                     Private Networking? y    Usage Allocation Enhancements? y
                Processor and System MSP? n
                     Processor Ethernet? y                 Wideband Switching? n
                                                                   Wireless? n
                          Remote Office? n
          Restrict Call Forward Off Net? y
                  Secondary Data Module? y
```


©2012 Avaya Inc. All Rights Reserved.

5.2. Configure Dial Plan

In the sample configuration, the Avaya CPE environment uses **4** digits to dial the local extensions (**ext**), such as **45**xx. For outbound calls via SIP trunk to Windstream, the feature access code (**fac**) **9** is used to access the Automatic Route Selection (ARS) table. The dial plan illustrated here is not intended to be prescriptive; any valid dial plan may be used.

Use the **change dialplan analysis** command to make following changes:

- Enter the **Dialed String 45** with **Total Length 4**
- Enter the **Dialed String 9** with **Total Length 1**

```
change dialplan analysis                                           Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location:  all          Percent Full:    0

       Dialed   Total  Call    Dialed   Total  Call      Dialed   Total  Call
       String   Length Type    String   Length Type      String   Length Type
          0            3     fac
          1            3     fac
          45           4     ext
          3            5     ext
          4            10    ext
          6            10    ext
          8            1     fac
          9            1     fac
          *            2     fac
          *            3     fac
          *            4     dac
          #            2     fac
          #            3     fac
```


©2012 Avaya Inc. All Rights Reserved.

5.3. Configure IP Node Names

The node names are mappings of names to IP addresses that can be used in various screens. The following abridged **change node-names ip** output shows relevant node-names used in the sample configuration. The node name for Session Manager is **DevASM** with IP Address **10.10.97.198**. The node name and IP Address for the Processor Ethernet (procr) is **procr** and **10.10.97.201.** The **procr** is the interface that Communication Manager will use as the SIP signaling interface to Session Manager.

```
change node-names ip
                                  IP NODE NAMES
    Name              IP Address
DevASM                10.10.97.198
default               0.0.0.0
procr                 10.10.97.201
```

5.4. Configure IP Interface for procr

Use the **change ip-interface procr** command to change the Processor Ethernet (procr) parameters. The following screen shows the parameters used in the sample configuration. While the focus here is the use of the procr for SIP Trunk signaling, observe that the Processor Ethernet will also be used for registrations from H.323 IP Telephones. Ensure **Enable Interface** is **y** and **Network Region** is **1**

```
change ip-interface procr
                                  IP INTERFACES

                  Type: PROCR
                                                       Target socket load: 1700

      Enable Interface? y                           Allow H.323 Endpoints? y
                                                     Allow H.248 Gateways? y
        Network Region: 1                             Gatekeeper Priority: 5

                                 IPV4 PARAMETERS
             Node Name: procr                  IP Address: 10.10.97.201
           Subnet Mask: /26
```


©2012 Avaya Inc. All Rights Reserved.

5.5. Configure IP Network Regions for Gateway Telephones

Network regions provide a means to logically group resources. Use the **change ip-network-region 1** command to set the following values:

- The **Authoritative Domain** field is configured to match the domain name configured on Session Manager in **Section 7.1**. In this configuration, the domain name is **bvwdev7.com**.
- By default, **IP-IP Direct Audio** (both **Intra-** and **Inter-Region**) is set to **yes** to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources. The **Codec Set** is set to the number of the IP codec set to be used for calls within the IP network region. In this case, codec set **1** was used.

```
change ip-network-region 1                                  Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: bvwdev7.com
    Name: procr
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                  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
```

5.6. Configure IP Codec Set

The following screen shows the configuration for codec set to be used for local and external calls. In general, an IP codec set is a list of allowable codecs in priority order. Use the **change ip-codec-set** command for the codec set specified in the **IP Network Region 1** form above. Enter the list of audio codecs eligible to be used in order of preference. For the interoperability test, the codecs supported by Windstream were **G.711MU** and **G.729**

```
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.729             n                    2                 20
```


©2012 Avaya Inc. All Rights Reserved.

5.7. Configure SIP Signaling Groups

This section illustrates the configuration of the SIP Signaling Groups that will be used for inbound and outbound PSTN calls to Windstream Trunk Service. Use the **add signaling-group x** (**where x is the signaling-group number**) command to set the following values:

- **Group Type** is set to **sip**
- **Transport Method** is set to **tcp**
- **IMS Enabled** is set to **n**
- **Near-end Node Name** is set to **procr.** This value is taken from the IP Node Name form shown in **Section 5.3**
- **Far-end Node Name** is set to **DevASM** (Node name of the Session Manager entered in **Section 5.3**)
- **Near-end Listen Port** is set to **5060**
- **Far-end Listen Port** is set to **5060**
- **Far-end Network Region** is set to 1 (The IP Network Region is configured in **Section 5.5**)
- **Far-end domain** is set to **bvwdev7.com** (domain name as configured in **Section 5.5**) in **signaling group 1** for outbound calls and set to **blank** in **signaling group 2** for inbound calls
- **DTMF over IP** is set to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833
- **Enable Layer 3 Test** is set to **y** to enable Communication Manager to maintain heartbeat using the SIP OPTION method

```
add signaling-group 1
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n
     IP Video? n

   Near-end Node Name: procr                Far-end Node Name: DevASM
   Near-end Listen Port: 5060                      Far-end Listen Port: 5060
                                                   Far-end Network Region: 1
Far-end Domain: bvwdev7.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                       Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n           Alternate Route Timer(sec): 6
```


©2012 Avaya Inc. All Rights Reserved.

```
add signaling-group 2
                                SIGNALING GROUP

 Group Number: 2              Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n
     IP Video? n

   Near-end Node Name: procr                  Far-end Node Name: DevASM
   Near-end Listen Port: 5060                    Far-end Listen Port: 5060
                                                 Far-end Network Region: 1
Far-end Domain:

                                             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                     Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

5.8. Configure SIP Trunk Groups

This section illustrates the configuration of the SIP Trunks Groups corresponding to the SIP signaling groups from the previous section.

Use the **add trunk group x** (**where x is the trunk group number**) command to set the following values on **Page 1**:

- Choose a descriptive **Group Name**
- Specify a trunk access code (**TAC**) consistent with the dial plan, i.e. ***010**, ***011**
- The **Direction** is set to **outgoing** to allow outgoing calls and set to **incoming** to allow incoming calls
- The **Service Type** field should be set to **public-ntwrk** for the trunks that will handle calls with Windstream
- Specify the signaling group associated with this trunk group in the **Signaling Group** field as previously configured in **Section 5.7**
- Specify the **Number of Members** supported by this SIP trunk group

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

Group Number: 10                   Group Type: sip          CDR Reports: y
  Group Name: OUTSIDE CALL                COR: 1        TN: 1        TAC: *010
   Direction: outgoing        Outgoing Display? n
 Dial Access? n                                Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n

                                                      Signaling Group: 1
                                                    Number of Members: 50
```


©2012 Avaya Inc. All Rights Reserved.

On **Page 3** of the **trunk-group** screen set **Numbering Format** field 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
```

Use the **add trunk group 11** command to set the values of trunk group which will be used for PSTN calls to Windstream. Trunk group 11 is associated with **Signaling Group 2**.

```
add trunk-group 11                                                Page   1 of  21
                                TRUNK GROUP

Group Number: 11                   Group Type: sip          CDR Reports: y
  Group Name: INSIDE CALL                 COR: 1        TN: 1        TAC: *011
   Direction: incoming        Outgoing Display? n
 Dial Access? n                                 Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n

                                                      Signaling Group: 2
                                                    Number of Members: 15
```

On **Page3** of **trunk-group** form set **Numbering Format** to **private.**

```
change trunk-group 11                                                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
```


©2012 Avaya Inc. All Rights Reserved.

5.9. Configure Route Pattern

Use the **change route-pattern 1** command to route calls to the SIP trunk group described in **Section 5.8**. This allows route pattern 1 to destine the calls between the PSTN and the Windstream Service by using the SIP trunk group **10**. Digit manipulation can be performed on the called number, if needed, using the **No. Del Dgts** and **Inserted Digits** fields. Digit manipulation can also be performed by Session Manager.

```
change route-pattern 1                                              Page   1 of   3
                    Pattern Number: 1   Pattern Name: PSTN
                             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
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user
 6:                                                                     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
 3: y y y y y n  n            rest                                 none
 4: y y y y y n  n            rest                                 none
```


©2012 Avaya Inc. All Rights Reserved.

5.10. Configure Public Numbering

Use the **change public-unknown-numbering** command to define the format of numbers sent to Windstream in SIP headers such as the From and PAI headers. In general, the mappings of internal extensions to Windstream DID numbers may be done in Session Manager (via Digit Conversion in adaptations) or in Communication Manager (via public-unknown-numbering, and incoming call handling treatment for the inbound trunk group).

In the bolded rows shown in the example abridged output below, all Communication Manager extensions are mapped to a DID numbers by adding the sequence **864263** to the beginning of the number, when the call uses trunk group **10**. Alternatively, Communication Manager can send the extension to Session Manager by leaving the **CPN Prefix** field blank and setting the **CPN Len** to 4 and Session Manager can adapt the number to the Windstream DID.

```
change public-unknown-numbering 1                              Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext     Ext               Trk       CPN              CPN
Len     Code            Grp(s)    Prefix           Len
                                                                      Total
Administered: 8
 4      4500             10        864263           10        Maximum Entries: 240
 4      4501             10        864263           10
 4      4502             10        864263           10
 4      4503             10        864263           10
 4      4504             10        864263           10
```


©2012 Avaya Inc. All Rights Reserved.

5.11. Configure ARS Routing For Outbound Calls

Although not illustrated in these Application Notes, location-based routing may be configured so that users at different locations that dial the same telephone number can have calls choose different route-patterns. Various example scenarios for a multi-location network with failover routing are provided in reference [PE]. In these Application Notes, all locations table directs ARS calls to specific SIP Trunks to Session Manager. Appropriate ARS entries can be added to match the various dial patterns (e.g., long distance, service numbers, etc.) to be sent to Windstream.

Use the **change ars analysis 0** command to specify ARS configuration . For example if a user dials the ARS access code defined in **Section 5.2**, followed by the number beginning with **Dialed String 1** with a **length** of **11** digits and **Call Type** as **pubu**, the call will select **Route Pattern 1**.

```
change ars analysis 0                                        Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location:  all          Percent Full:    0

          Dialed           Total           Route       Call   Node   ANI
          String          Min  Max        Pattern      Type   Num   Reqd
           0              7    18          1            pubu          n
           011            13   24          1            intl          n
           1              11   11          1            pubu          n
           3              5     5          3            pubu          n
           4              10   10          1            pubu          n
           6              10   10          1            pubu          n
```

5.12. Configure Incoming Call Handling Treatment

In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion, and digit manipulation via Communication Manager incoming call handling table may not be necessary. If the DID number sent by Windstream is unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk-group 11. As an example, use the **change inc-call-handling-trmt trunk-group 11** to convert incoming DID numbers **864263**xxxx to 4 digit extension xxxx by deleting **6** of the incoming digit.

```
change inc-call-handling-trmt trunk-group 11                 Page   1 of   3
                       INCOMING CALL HANDLING TREATMENT
 Service/            Number     Number          Del  Insert
 Feature             Len        Digits
 public-ntwrk        10         864263            6
```


©2012 Avaya Inc. All Rights Reserved.

5.13. Configure Avaya Aura® Communication Manager Stations

In the sample configuration, four digit station extensions were used with the format 4xxx. Use the **add station 4500** command to add an Avaya H.323 IP telephone

```
add station 4500                                                      Page   1 of   5
                                     STATION

Extension: 4500                          Lock Messages? n              BCC: 0
     Type: 9620                          Security Code: 1234            TN: 1
     Port: S00021                      Coverage Path 1: 1              COR: 1
     Name: IP_4500                     Coverage Path 2:                COS: 1
                                       Hunt-to Station:
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 4500
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                           IP SoftPhone? n

                                                          IP Video? n


                                              Customizable Labels? Y
```

5.14. Save Avaya Aura® Communication Manager Configuration Changes

Use the **save translation all** command to save the configuration.

©2012 Avaya Inc. All Rights Reserved.

6. Avaya Aura® Communication Manager Configuration for UUI-Call Redirect Capability

This section describes the additional administration steps on Communication Manager necessary for supporting interaction with the Windstream Transfer Connect service. The steps are performed from the Communication Manager System Access Terminal (SAT) interface.

Note: In the following sections, only the highlighted parameters are applicable to these Application Notes. Other parameters shown should be considered informational.

6.1. Configure System Parameters

This section reviews the additional Communication Manager licenses and features that are required for supporting the interaction with the Windstream Transfer Connect service. For required parameters that are not enabled in the steps that follow, contact an authorized Avaya account representative to obtain the necessary licenses.

Enter the **display system-parameters customer-options** command. On **Page 4** of the system-parameters customer-options form, verify that the **ISDN/SIP Network Call Redirection?** field is set to **y**.

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

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

           IP Attendant Consoles? y
        (NOTE: You must logoff & login to effect the permission
```


©2012 Avaya Inc. All Rights Reserved.

On **Page 6** of the **system-parameters customer-options** form, verify that the vectoring features outlined below are set to **y.**

```
display system-parameters customer-options                      Page   6 of  11
                         CALL CENTER OPTIONAL FEATURES

                          Call Center Release: 5.0

                                ACD? y                         Reason Codes? n
                       BCMS (Basic)? n              Service Level Maximizer? n
         BCMS/VuStats Service Level? n            Service Observing (Basic)? y
  BSR Local Treatment for IP & ISDN? n     Service Observing (Remote/By FAC)? n
                  Business Advocate? n           Service Observing (VDNs)? y
                    Call Work Codes? n                          Timed ACW? n
      DTMF Feedback Signals For VRU? n                  Vectoring (Basic)? y
                   Dynamic Advocate? n              Vectoring (Prompting)? y
       Expert Agent Selection (EAS)? y          Vectoring (G3V4 Enhanced)? y
                            EAS-PHD? n           Vectoring (3.0 Enhanced)? y
                   Forced ACD Calls? n     Vectoring (ANI/II-Digits Routing)? y
               Least Occupied Agent? n     Vectoring (G3V4 Advanced Routing)? y
          Lookahead Interflow (LAI)? y                  Vectoring (CINFO)? y
Multiple Call Handling (On Request)? n      Vectoring (Best Service Routing)? y
    Multiple Call Handling (Forced)? n               Vectoring (Holidays)? y
  PASTE (Display PBX Data on Phone)? n              Vectoring (Variables)? y
```

6.2. Configure SIP Trunks

This section describes the steps for modifying the SIP trunk to the Avaya SBCE to support the interaction with the Windstream Transfer Connect service.

Enter the **change trunk-group 11** command, where **11** is the number of the trunk group administered in **section 5.8** for inbound Windstream service calls. On **Page 4** of the trunk-group form, set **Network Call Redirection** to **y**. Verify **Support Request History?** field is set to **n** and **Telephone Event Payload Type** field is set to **100**..

```
change trunk-group 11                                          Page   4 of  21
                              PROTOCOL VARIATIONS

                       Mark Users as Phone? n
             Prepend '+' to Calling Number? n
       Send Transferring Party Information? y
                  Network Call Redirection? y
                     Send Diversion Header? y
                   Support Request History? n
              Telephone Event Payload Type: 100
```

6.3. Configure Inbound Call Routing

This section describes the steps for routing inbound Windstream Transfer Connect service calls to reach Vector Directory Numbers (VDNs) with corresponding programmable vectors. These vectors contain steps that invoke the Communication Manager SIP Network Call Redirection (NCR) functionality (see **Section 6.2** above). Two different inbound call routing scenarios are described in these Application Notes:

1. Pre-Answer Redirection - An inbound Windstream Transfer Connect service call that invokes SIP NCR (using a SIP 302 message) prior to the call being answered.

©2012 Avaya Inc. All Rights Reserved.

2. Post-Answer Redirection - An inbound Windstream Transfer Connect service call that invokes SIP NCR (using a SIP REFER message) after the call has been answered by a vector.

These Application Notes provide rudimentary vector definitions to demonstrate and test the SIP NCR and UUI functionalities. In general, call centers will use vector functionality that is more complex and tailored to their individual needs. Call centers may also use customer hosts running applications used in conjunction with Avaya Application Enablement Services (AES) to define call routing and provide associated UUI. The definition and documentation of those complex applications and associated vectors are beyond the scope of these Application Notes.

6.3.1. Pre-Answer Redirection

This section provides an example of Pre-Answer Redirection. The following screen shots show how to route inbound Windstream Transfer Connect service calls to reach Vector Directory Numbers (VDNs) with corresponding programmable vector. The vector instructs Communication Manager to redirect the call to a designed number. In the example, the inbound call is routed to the **vdn 4503**, which invokes the **vector 22**.

```
change vdn 4503                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 4503
                                 Name*: 302
                           Destination: Vector Number        22


                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none

                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:
```

Note: The parameters for ASAI UUI variables A and B, and other vector variables are defined using the **change variables** command.

```
change variables                                                Page   1 of  39
                              VARIABLES FOR VECTORS

Var Description                     Type    Scope Length Start Assignment       VAC
A   UuiTest1                        asaiuui L     16     1
B   UuiTest2                        asaiuui L     16     17
C
```


©2012 Avaya Inc. All Rights Reserved.

The **vector 22** does the following:

- Plays ringback for 3 seconds (vector step **02**).
- Assigns the data **1234567890123456** to ASAI UUI variable **A** (vector step **05**).
- Redirects the call to the number **8642634504** (vector step **08**). Note that since this vector did not answer the call, the presence of the **~r** in the **route-to number** instructs Communication Manager to send a SIP 302 message with the number 8642634504 in the user part of the Contact header URI, e.g., 8642634504@<host/domain>, to the Windstream Transfer Connect service (via the Avaya SBCE)

```
change vector 22                                            Page   1 of   6
                                  CALL VECTOR

    Number: 22              Name: 302RingUUI
Multimedia? n                                                       Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? n
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 #    Ringing
02 wait-time    3   secs hearing ringback
03
04 #    Define UUI variable
05 set          A      = none   CATR  1234567890123456
06
07 #    Redirect
08 route-to     number ~r8642634504   with cov n if unconditionally
09 stop
10
11
12
```

6.3.2. Post-Answer Redirection

This section provides an example of Post-Answer Redirection. In this example, the inbound call is routed to the **vdn 4502**, which invokes the **vector 15**.

```
change vdn 4502                                             Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 4502
                                 Name*: REFER
                           Destination: Vector Number        15


                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none



                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:
```


©2012 Avaya Inc. All Rights Reserved.

The **vector 15** does the following:

- Assigns the data **1234567890123456** to ASAI UUI variable **B** (vector step **02**).
- Answers the call to play an **announcement 3003** (vector step **05**) and attempts to redirect the call to the number **8642634504** (vector step **08**). Note that since this vector answered the call, the presence of the **~r** in the **route-to number** instructs Communication Manager to send a SIP REFER message with the number **8642634504** in the user part of the Refer-header URI, e.g., **8642634504@<host/domain>** to the Windstream Transfer Connect service (via the Avaya SBCE).
- If the redirection fails (e.g. network denies the call), then **announcement 3004** (vector step **10**) is played to the caller.

```
change vector 15                                                   Page   1 of   6
                                  CALL VECTOR

    Number: 15               Name: Refer_UUI
Multimedia? n                                                              Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? n
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 #    Generate UUI
02 set          B      = none   CATR  1234567890123456
03
04 #    Play Refer announcement
05 announcement 3003
06
07 #    Refer occurs since this is post answer
08 route-to     number  ~r8642634504           with cov n if unconditionally
09 #    If Refer fails play announcement and disconnect
10 disconnect   after announcement 3004
11
12
```


©2012 Avaya Inc. All Rights Reserved.

6.3.3. Provision Station to display UUI

In order to display the UUI information defined in the **Sections 6.3.1** and **6.3.2** above, the Agent's station must have a UUI display button defined via the Communication Manager ***change station x*** form, where ***x*** is a station extension associated with the Agent. On **Page 4** of the **change station 4503** form, add the **uui-info** feature to any available button appearance (e.g. button appearance **4**).

```
change station 4503                                             Page   4 of   5
                                     STATION
 SITE DATA
       Room:                                             Headset? n
       Jack:                                             Speaker? n
      Cable:                                            Mounting: d
      Floor:                                         Cord Length: 0
   Building:                                           Set Color:

ABBREVIATED DIALING
     List1:                   List2:                   List3:




BUTTON ASSIGNMENTS
 1: call-appr                           4: uui-info
 2: call-appr                           5:
 3: call-appr                           6:
```

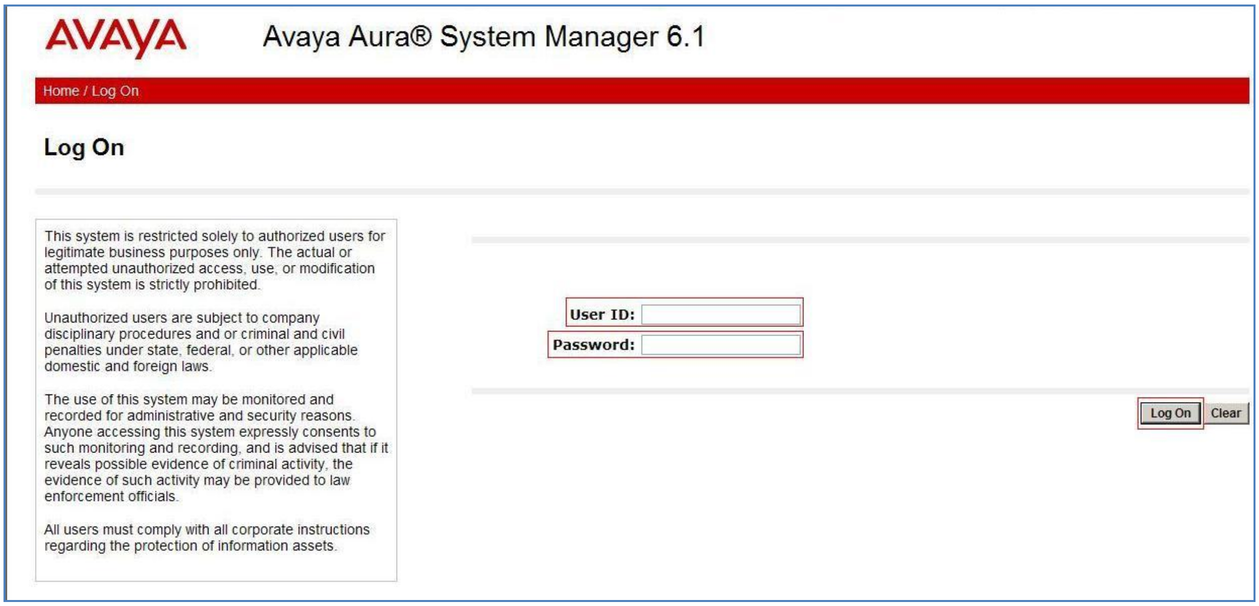

©2012 Avaya Inc. All Rights Reserved.

7. Configure Avaya Aura® Session Manager

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

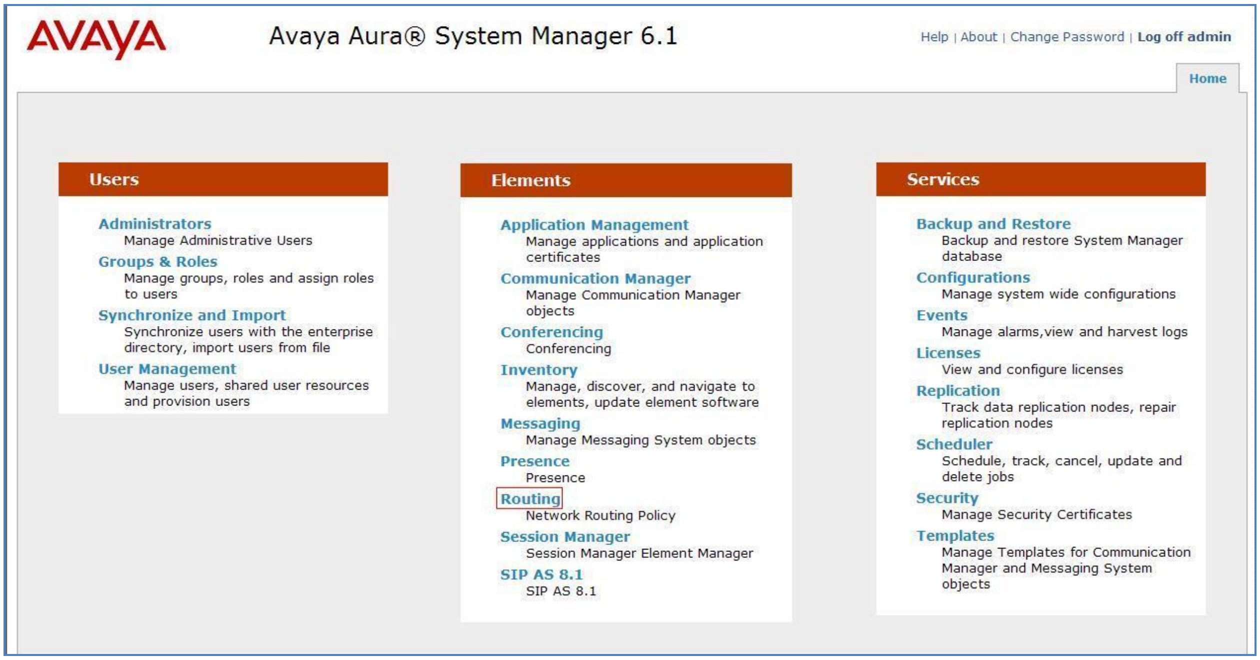
Note: The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two. For more information on Session Manager see **Section 11** of these Application Notes.

Session Manager is managed via System Manager. Using a web browser, access **https://<ip-addr of System Manager>/SMGR** In the **Log On** screen, enter appropriate **User ID** and **Password** and press the **Log On** button



©2012 Avaya Inc. All Rights Reserved.

Once logged in, a Home Screen is displayed as below:



When **Routing** is selected, the right side outlines a series of steps.

©2012 Avaya Inc. All Rights Reserved.

The sub-sections that follow are in the same order as the steps outlined under **Introduction to Network Routing Policy (NRP)** in the abridged screen shown below. In these Application Notes, all these steps are illustrated with the exception of **Step 3** and **Step 9**, since Regular Expressions were not used.

Introduction to Network Routing Policy

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.

The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).

Step 2: Create "Locations"

Step 3: Create "Adaptations"

Step 4: Create "SIP Entities"

- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"

Step 5: Create the "Entity Links"

- Between Session Managers
- Between Session Managers and "other SIP Entities"

Step 6: Create "Time Ranges"

- Align with the tariff information received from the Service Providers

Step 7: Create "Routing Policies"

- Assign the appropriate "Routing Destination" and "Time Of Day"

(Time Of Day = assign the appropriate "Time Range" and define the "Ranking")

Step 8: Create "Dial Patterns"

- Assign the appropriate "Locations" and "Routing Policies" to the "Dial Patterns"

Step 9: Create "Regular Expressions"

- Assign the appropriate "Routing Policies" to the "Regular Expressions"

Each "Routing Policy" defines the "Routing Destination" (which is a "SIP Entity") as well as the "Time of Day" and its associated "Ranking".

IMPORTANT: the appropriate dial patterns are defined and assigned afterwards with the help of the routing application "Dial patterns". That's why this overall routing workflow can be interpreted as

"Dial Pattern driven approach to define Routing Policies"

That means (with regard to steps listed above):

Step 7: "Routing Polices" are defined

Step 8: "Dial Patterns" are defined and assigned to "Routing Policies" and "Locations" (one step)

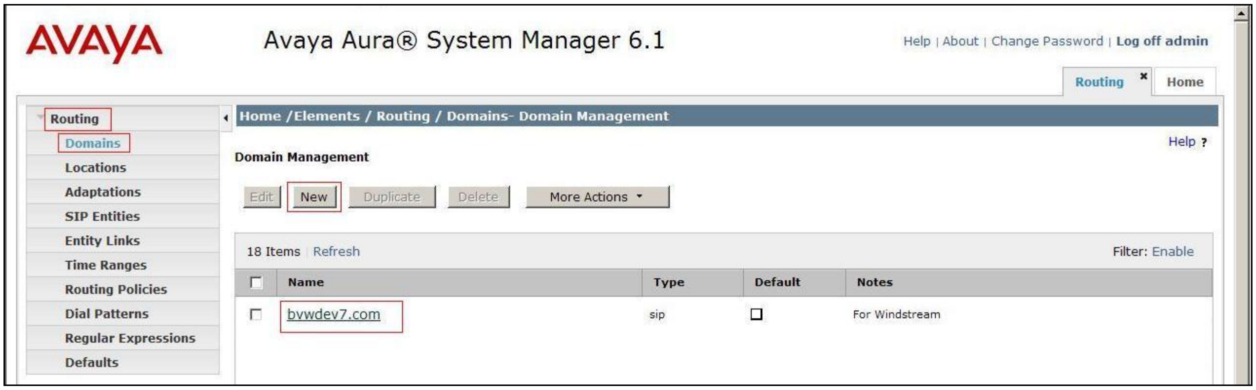
Step 9: "Regular Expressions" are defined and assigned to "Routing Policies" (one step)

©2012 Avaya Inc. All Rights Reserved.

7.1. Configure Domains

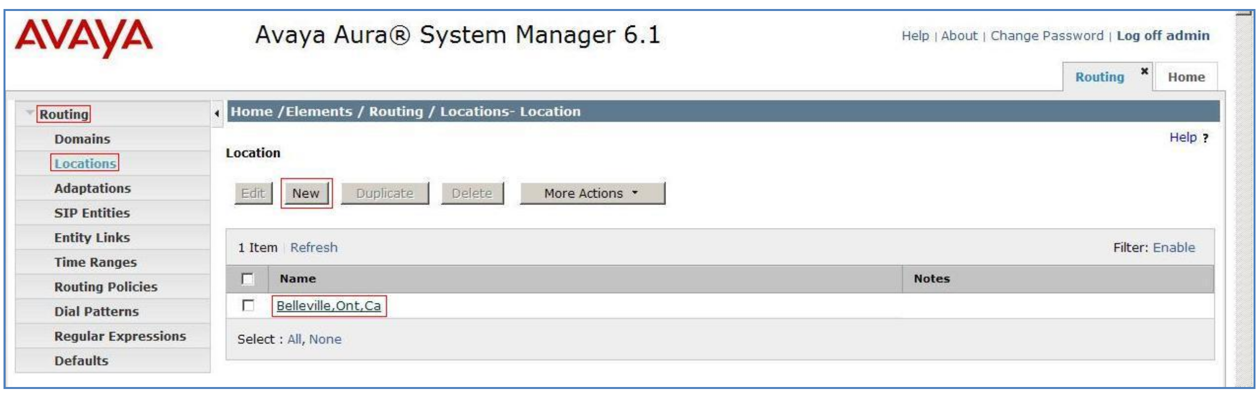
To add SIP domains that will be used with Session Manager, select **Routing → Domains**. Click the **New** button to add a new SIP domain entry. Click the Commit button after changes are completed.

The following screen shows the list of configured SIP domains. The domain **bvwdev7.com** is not known to the Windstream production service. The domain name should match the one used in the **ip-network-region** described in **Section 5.5.**



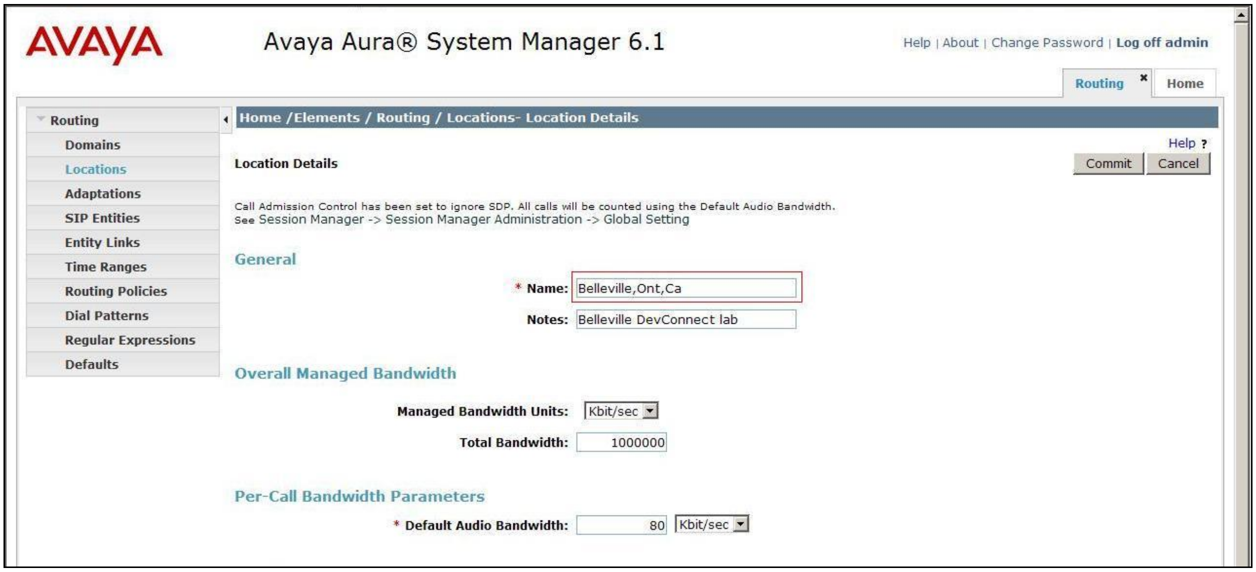
7.2. Configure Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside, for the purposes of bandwidth management. One location is added to the sample configuration for the enterprise SIP entities. To add locations, select **Routing → Locations**. The following screen shows an abridged list of configured locations. Click on the checkbox corresponding to the name of a configured location or Click on the **New** button to add a new location. Click the Commit button after changes are completed. Assigning unique locations can allow Session Manager to perform location-based routing, bandwidth management, and call admission control.



©2012 Avaya Inc. All Rights Reserved.

The following screen shows the location details for the location named **Belleville,Ont,Ca**, to be assigned to SIP Entities in **Section 7.3**.



7.3. Configure SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to the Session Manager. To add a SIP Entity, select **Routing → SIP Entities** and then click on the **New** button (not shown) and configure as follows:

Under **General:**

- In the **Name** field enter an informative name
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signaling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP entity and **Other** for the SBC SIP entity
- In the **Location** field select the appropriate location (configured in **section 7.2**) from the drop down menu
- In the **Time Zone** field enter the time zone where the SIP Entity is located

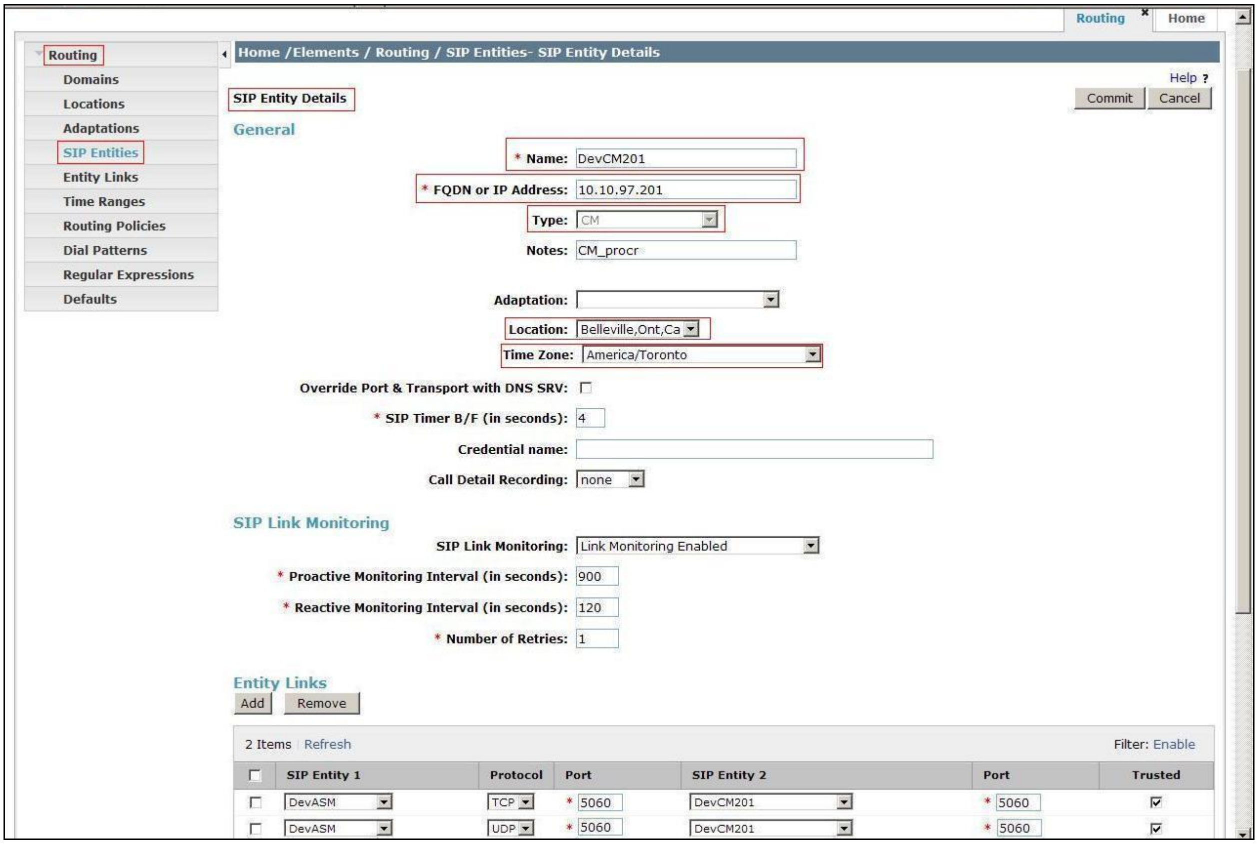
Following SIP Entities were configured for this reference configuration:

- Communication Manager SIP Entity
- Session Manager SIP Entity
- Session Border Controller SIP Entity

©2012 Avaya Inc. All Rights Reserved.

7.3.1. Configure Avaya Aura® Communication Manager SIP Entity

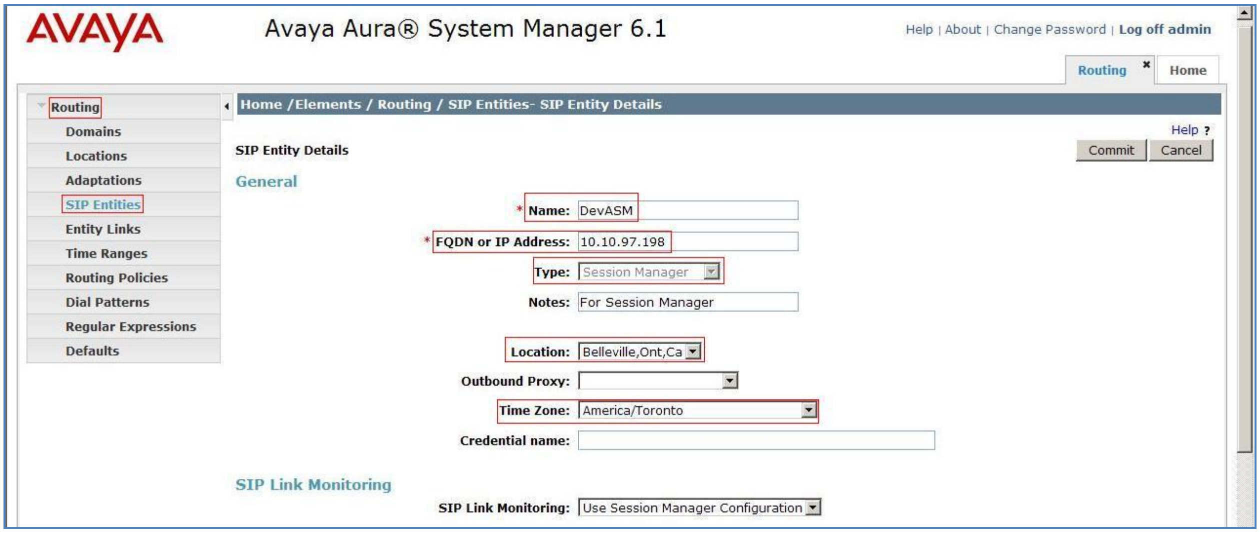
The following screen shows a portion of the **SIP Entity Details** corresponding to an Communication Manager SIP Entity named **DevCM201**. The **IP Address** field contains the IP Address of the processor ethernet (**10.10.97.201**). The **Type** field is set as **CM**. **Location** is set to **Belleville, Ont,Ca**. and **Time Zone** is set as **America/Toronto**.



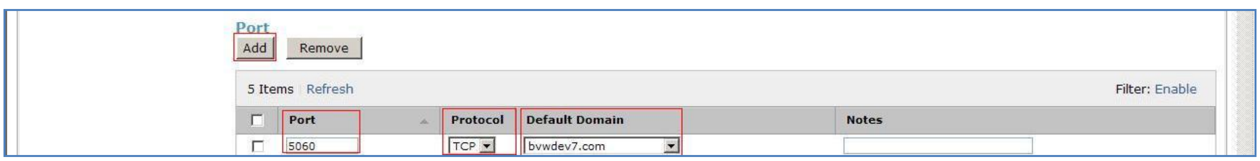
©2012 Avaya Inc. All Rights Reserved.

7.3.2. Configure Avaya Aura® Session Manager SIP Entity

The following screens show the SIP entity for Session Manager named **DevASM**. The **IP Address** field is set to the IP address **10.10.97.198** of the Session Manager SIP signaling interface. **Type** is set as **Session Manager**. **Location** is **Belleville, Ont,Ca**. **Time Zone** is **America/Toronto**



Click the **Add** button to configure a new port. **Protocol TCP** is used in the sample configuration for improved visibility during testing. **Port** is **5060** and **Default Domain** is **bvwdev7.com**.

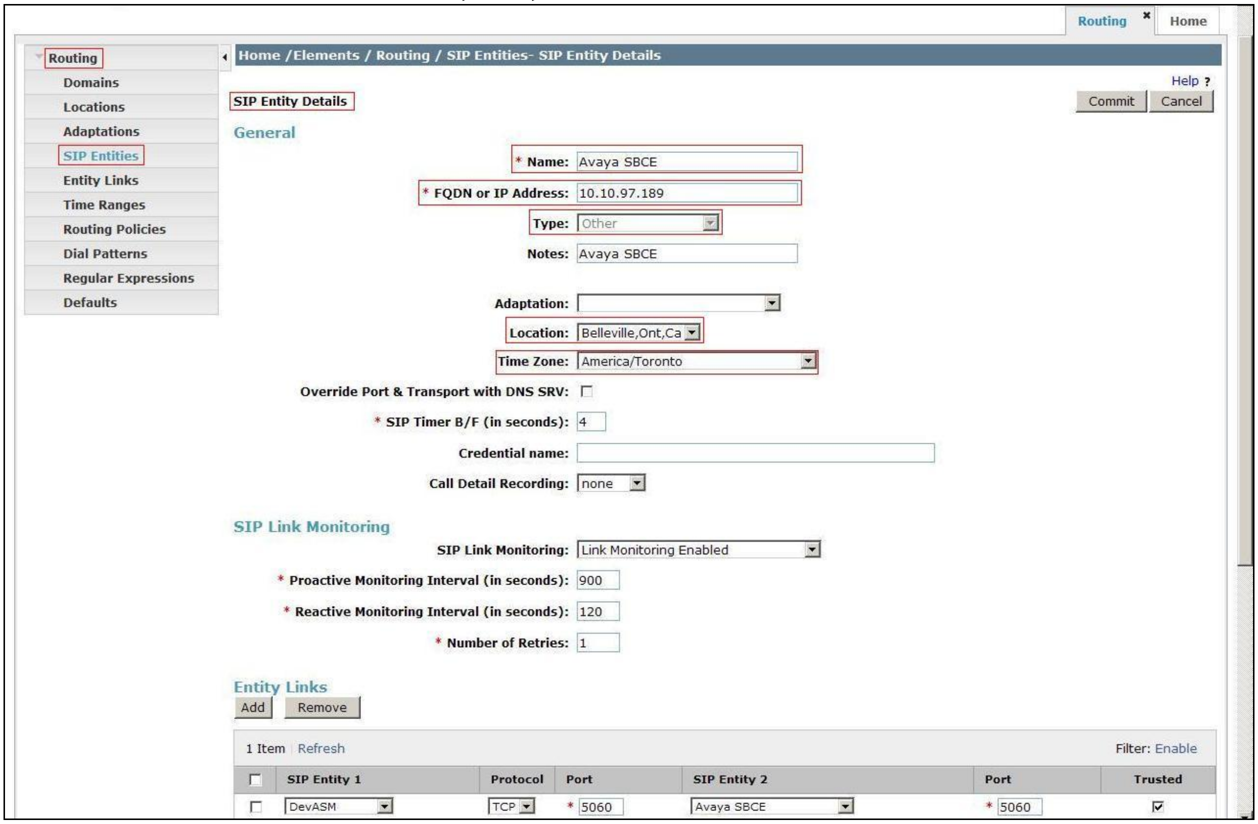


©2012 Avaya Inc. All Rights Reserved.

7.3.3. Configure Avaya SBCE SIP Entity

The following screen shows the **SIP Entity Details** for the Avaya SBCE.

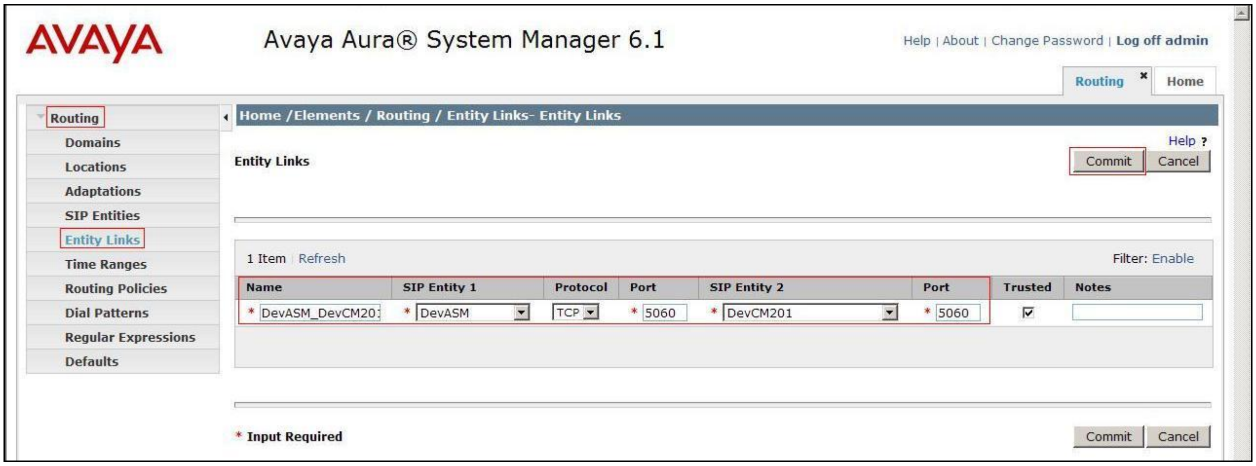
The **IP Address** field is set to the IP address **10.10.97.189** of the Avaya SBCE interface. **Type** is set as **Other**. **Location** is **Belleville, Ont,Ca**. and **Time Zone** is **America/Toronto**



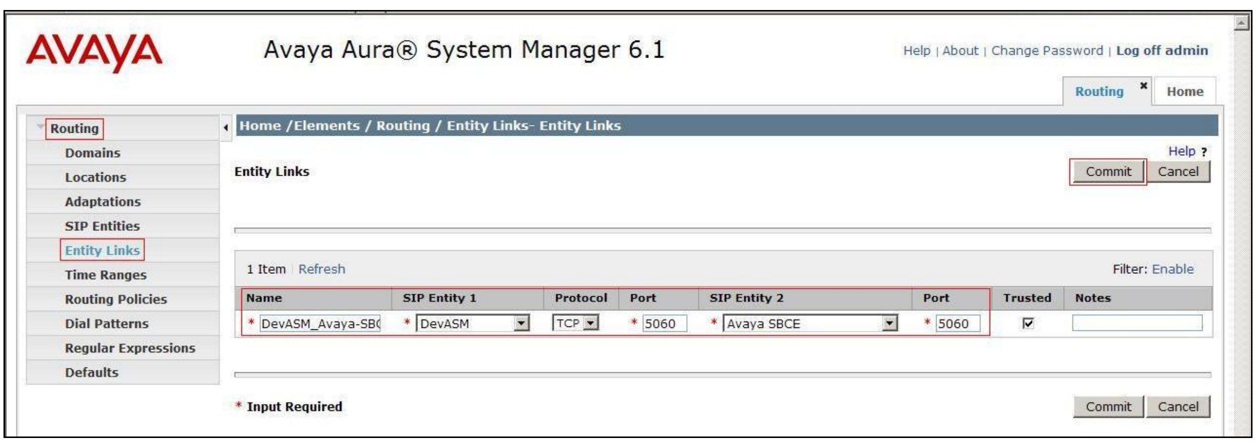
©2012 Avaya Inc. All Rights Reserved.

7.4. Configure Entity Links

A SIP trunk between a Session Manager and another system is described by an Entity Link. To add an Entity Link, select **Routing →Entity Links**. Click the **New** button to add a link for Communication Manager (not shown). Assign an appropriate **Name**, and select the Session Manager entity as **SIP Entity 1,** and the Communication Manager entity as **SIP Entity 2**. Assign the **Protocol** as **TCP**, select **Port 5060**, and click **Commit**.

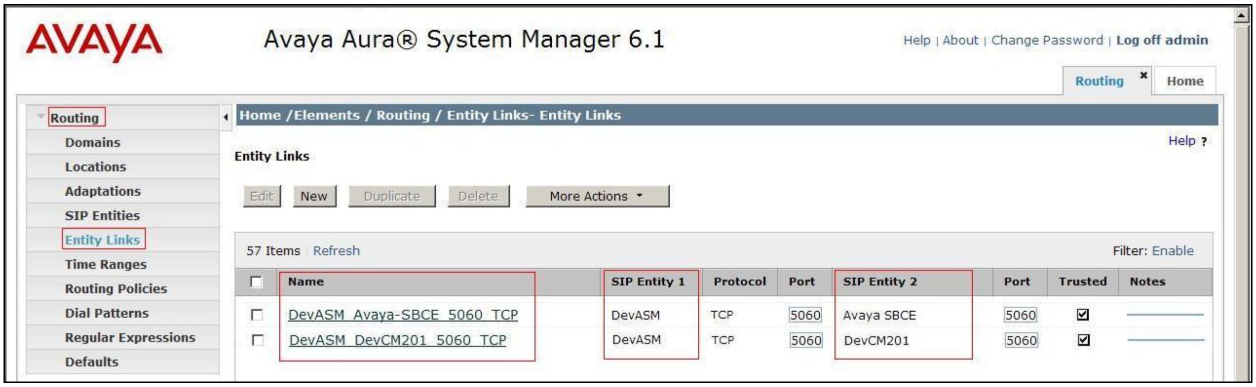


Click the **New** button to add a link for the Avaya SBCE (not shown). Assign an appropriate **Name**, and select the Session Manager entity as **SIP Entity 1,** and the Avaya SBCE entity as **SIP Entity 2**. Assign the **Protocol** as **TCP**, select **Port 5060**, and click **Commit**.



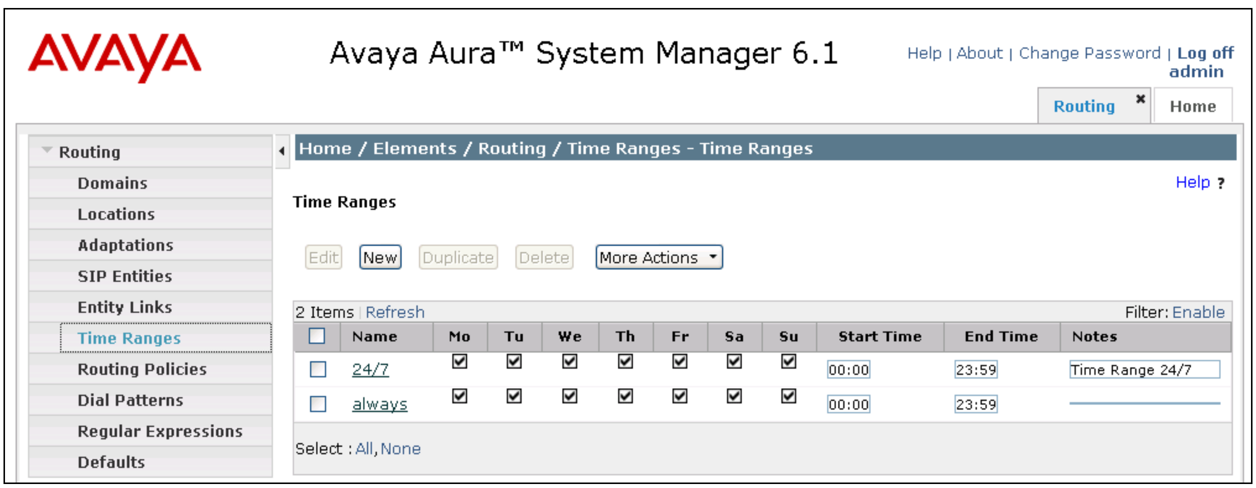
©2012 Avaya Inc. All Rights Reserved.

The following screen shows the list of configured entity links. Each of the links uses the entity named **DevASM** as SIP Entity 1, and the appropriate entity, such as **DevCM201**, **Avaya SBCE** for SIP Entity 2.



7.5. Configure Time Ranges

Time Ranges are configured for time-based-routing. In order to add a time range, select **Routing → Time Ranges** and then click **New** button. The Routing Policies shown subsequently will use the 24/7 range since time-based routing was not the focus of these Application Notes.



©2012 Avaya Inc. All Rights Reserved.

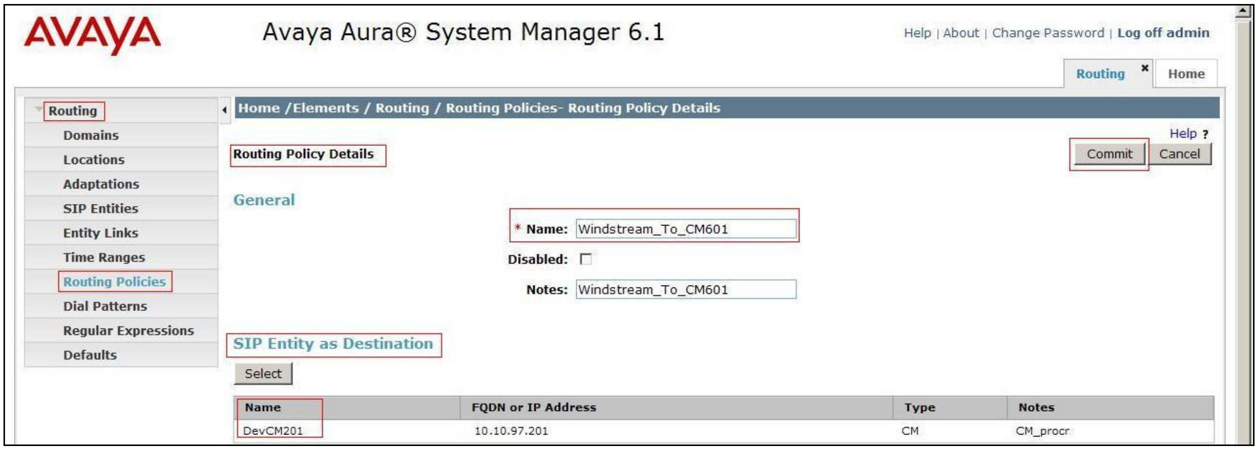
7.6. Configure Routing Policies

Routing policies must be created to direct how calls will be routed to a system. To add a new routing policy, select **Routing → Routing Policies** and then click on the **New** button to create a routing policy (not shown).

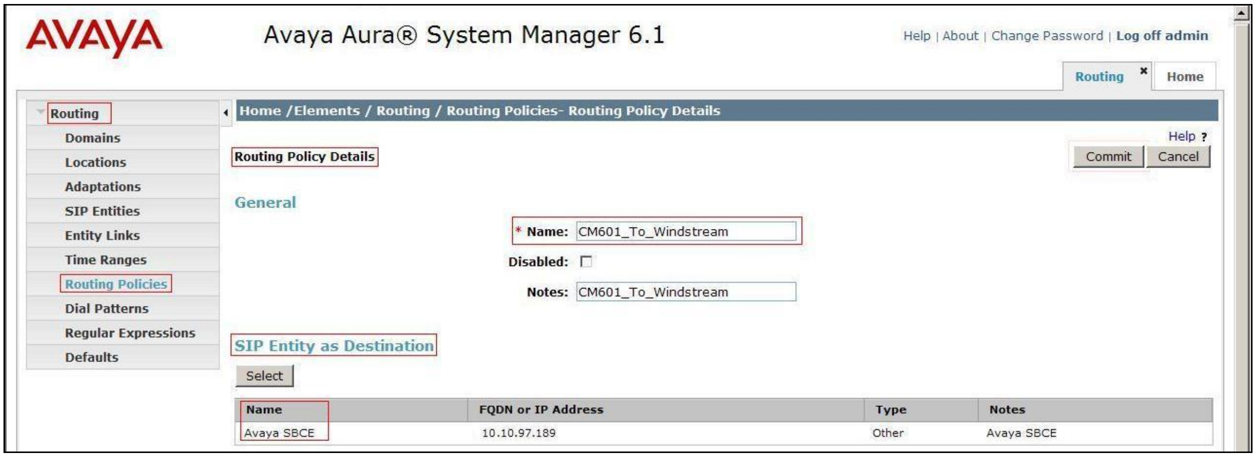
Under **General:**

- Enter an informative name in the **Name** field
- Under **SIP Entity as Destination**, click **Select**, and then select the appropriate SIP entity to which this routing policy applies

The following screen shows the **Routing Policy Details** for the policy named **Windstream_To_CM601** associated with incoming PSTN calls from Windstream to Communication Manager. Observe the **SIP Entity as Destination** is the entity named **DevCM201**.



The following screen shows the **Routing Policy Details** for the policy named **CM601_to_Windstream** associated with outgoing calls from Communication Manager to the PSTN via Windstream through the Avaya SBCE. Observe the **SIP Entity as Destination** is the entity named **Avaya SBCE**.



©2012 Avaya Inc. All Rights Reserved.

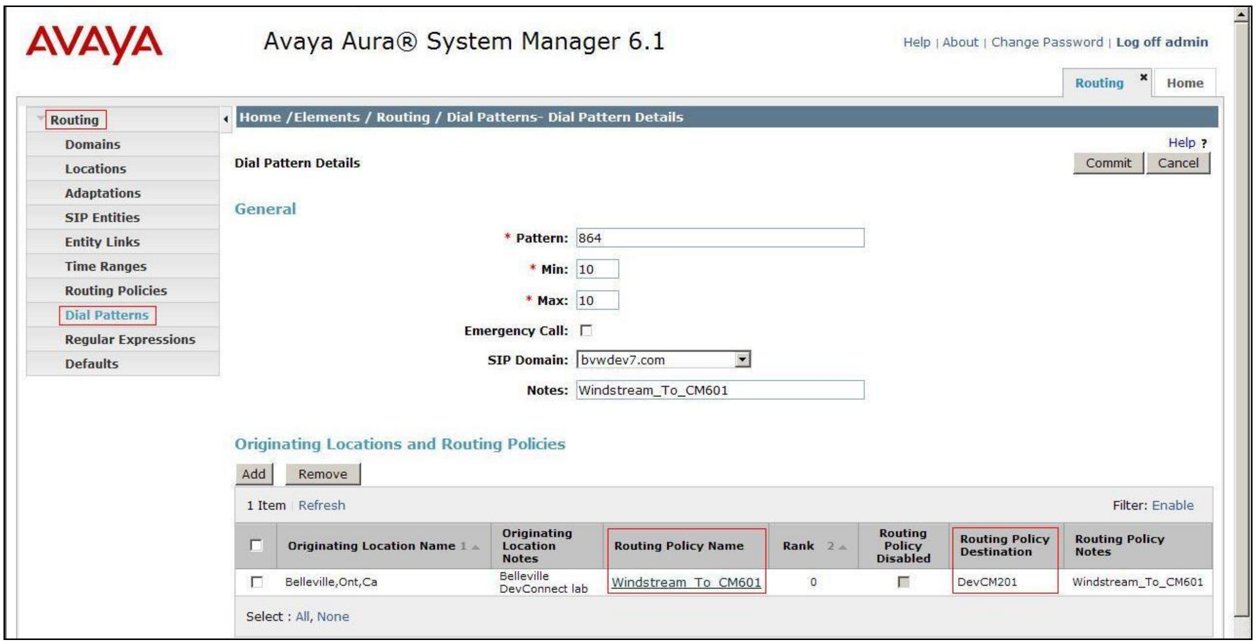
7.7. Configure Dial Patterns

A dial pattern must be defined to direct calls to the appropriate telephony system. To add a new dial pattern, select **Routing → Dial Patterns** and then click on the **New** button to create a dial pattern (not shown).

Under **General:**

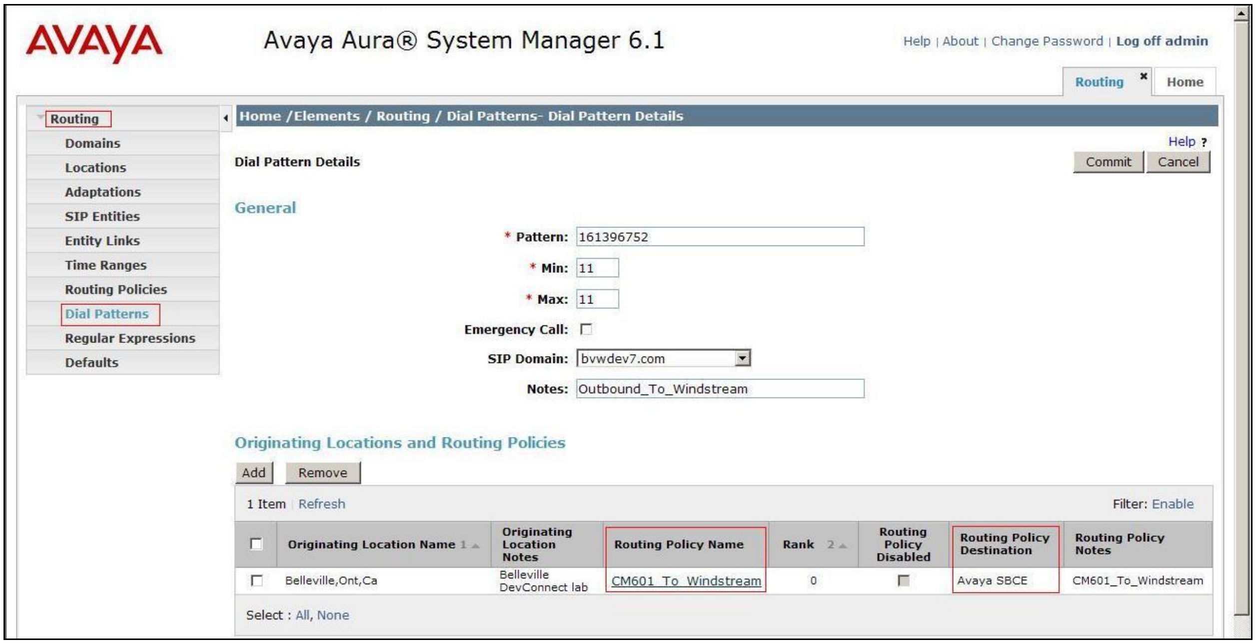
- In the **Pattern** field enter a dialed number or prefix to be matched
- In the **Min** field enter the minimum length of the dialed number
- In the **Max** field enter the maximum length of the dialed number
- In the **SIP Domain** field select the domain configured in **Section 7.1**

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise. When a user on the PSTN dials a number assigned to the Windstream Service, such as 8642634500, Windstream delivers the number to the enterprise, and the Avaya SBCE sends the call to Session Manager. Under **Originating Locations and Routing Policies**, the **Routing Policy Name Windstream_to_CM601** is selected, which sends the call to Communication Manager as described previously and **Routing Policy Destination** is set as **DevCM201**.

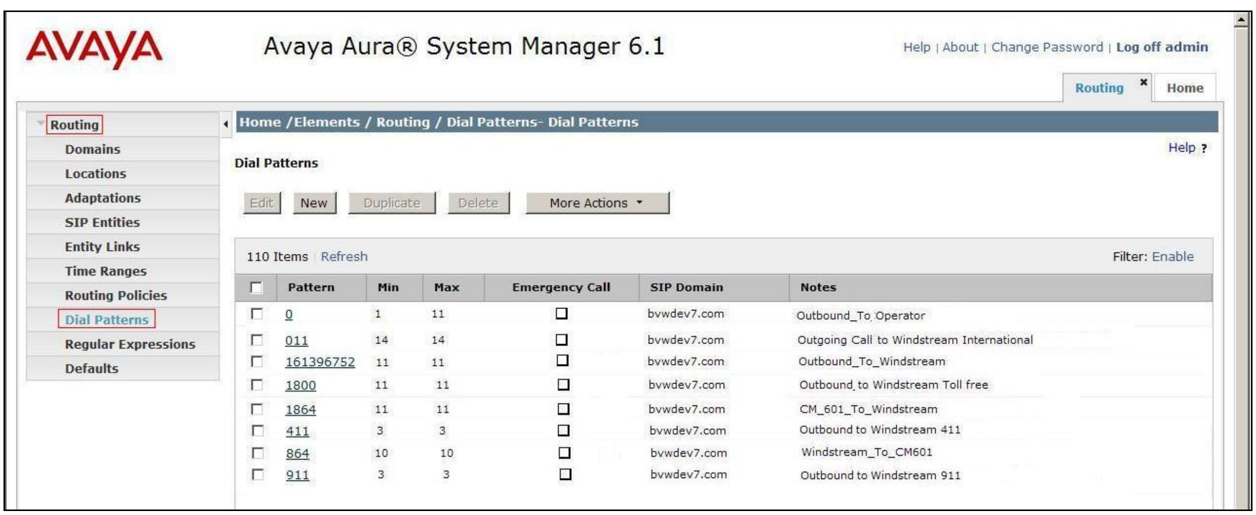


©2012 Avaya Inc. All Rights Reserved.

The following screen illustrates an example dial pattern used to verify outbound calls from the enterprise to the PSTN. When a Communication Manager user dials a PSTN number such as 1-613-967-5206, Communication Manager sends the call to Session Manager. Session Manager will match the dial pattern shown below and send the call to the Avaya SBCE via the **Routing Policy Name CM601_to_Windstream**. The **Routing Policy Destination** is set as **Avaya SBCE**.



The following screen shows the dial patterns used to verify inbound and outbound calls between the enterprise and the PSTN.



8. Configure Avaya SBCE

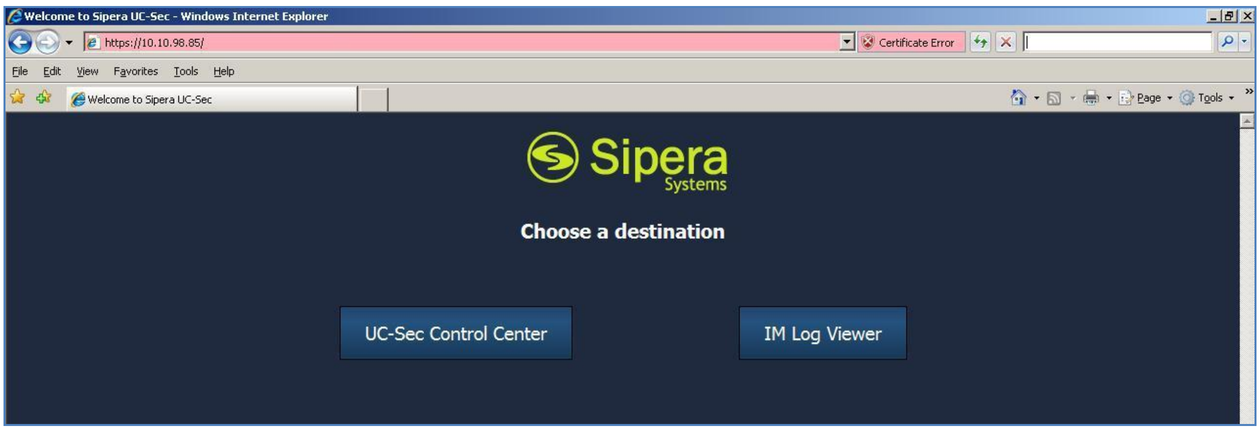
This section describes the configuration of the Avaya SBCE necessary for interoperability with the Avaya Session Manager and Windstream systems.

In this testing, according to the configuration reference **Figure 1**, the Avaya elements reside on the Private side and the Windstream system reside on the Public side of the network.

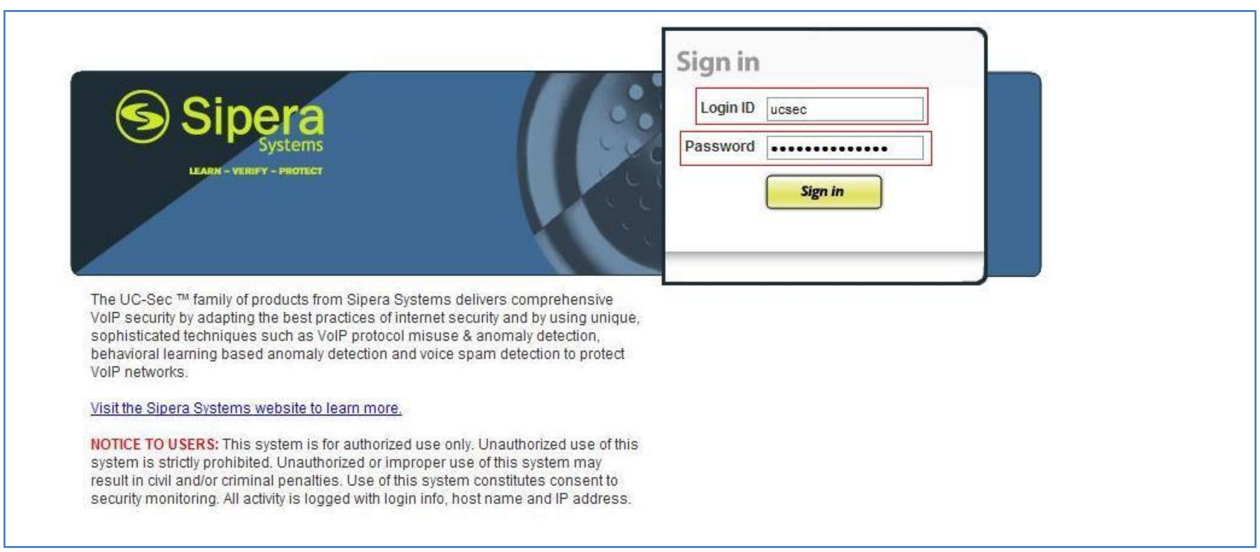
Note: The following section assumes that Avaya SBCE has been installed and that network connectivity exists between the systems. For more information on Avaya SBCE, see **Section 11** of these Application Notes.

8.1. Log in Avaya SBCE

Access the web interface by typing "**https://x.x.x.x**" (where x.x.x.x is the management IP Address of Avaya SBCE) and select **UC-Sec Control Center** from the screen below.



Enter the **Login ID** and **Password** in the screen below and click on **Sign in**.



©2012 Avaya Inc. All Rights Reserved.

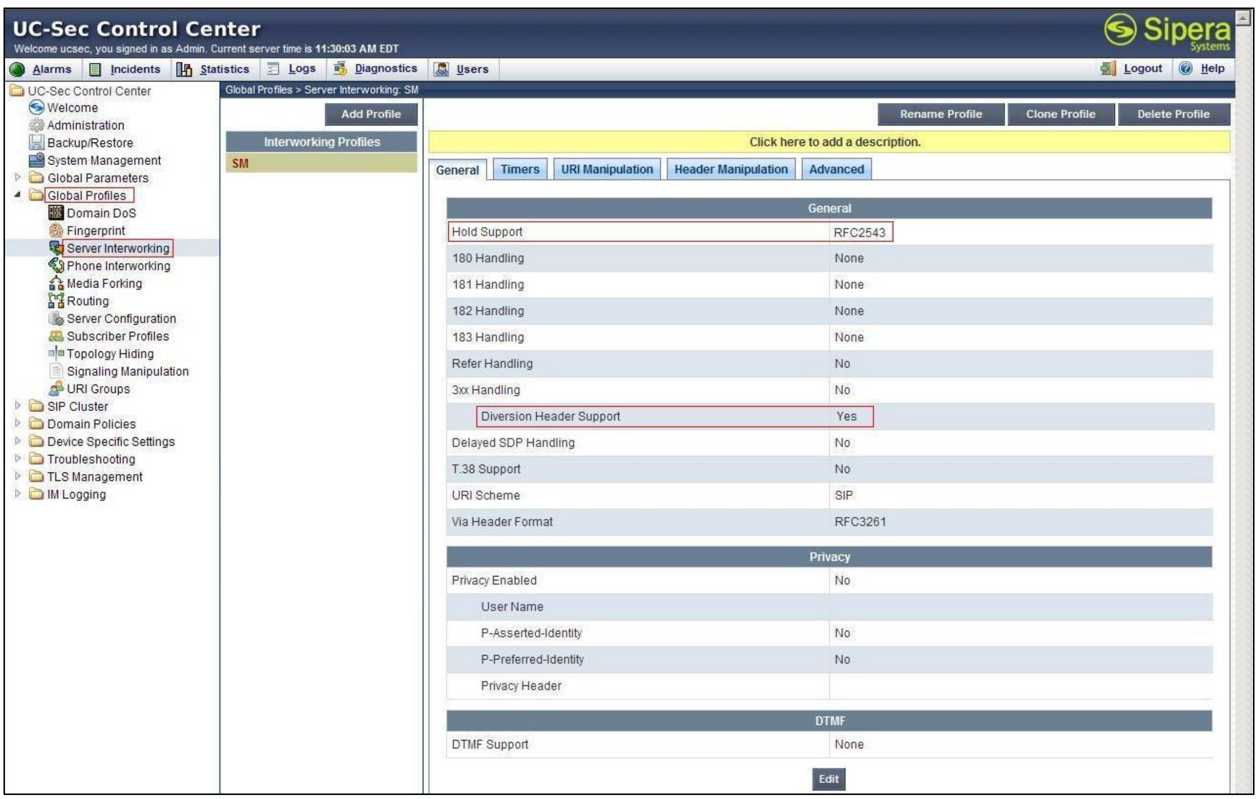
8.2. Global Profiles

When selected, Global Profiles allows for configuration of parameters across all UC-Sec appliances.

8.2.1. Configure Server Interworking - Avaya Side

Server Interworking allows users to configure and manage various SIP call server-specific capabilities such as call hold, etc.

- Select **Global Profiles** from the menu on the left-hand side
- Select the **Server Interworking**
- Select **Add Profile** and enter Internetworking profile **SM**
- In the **General** Tab:
  -
  - Check **Hold Support** as **RFC2543**
  - Check **Diversion Header Support** as **Yes**
  - All other options on the General Tab can be left at default
- In the **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** Tabs: All options can be left at default
- Click **Finish** (not shown)

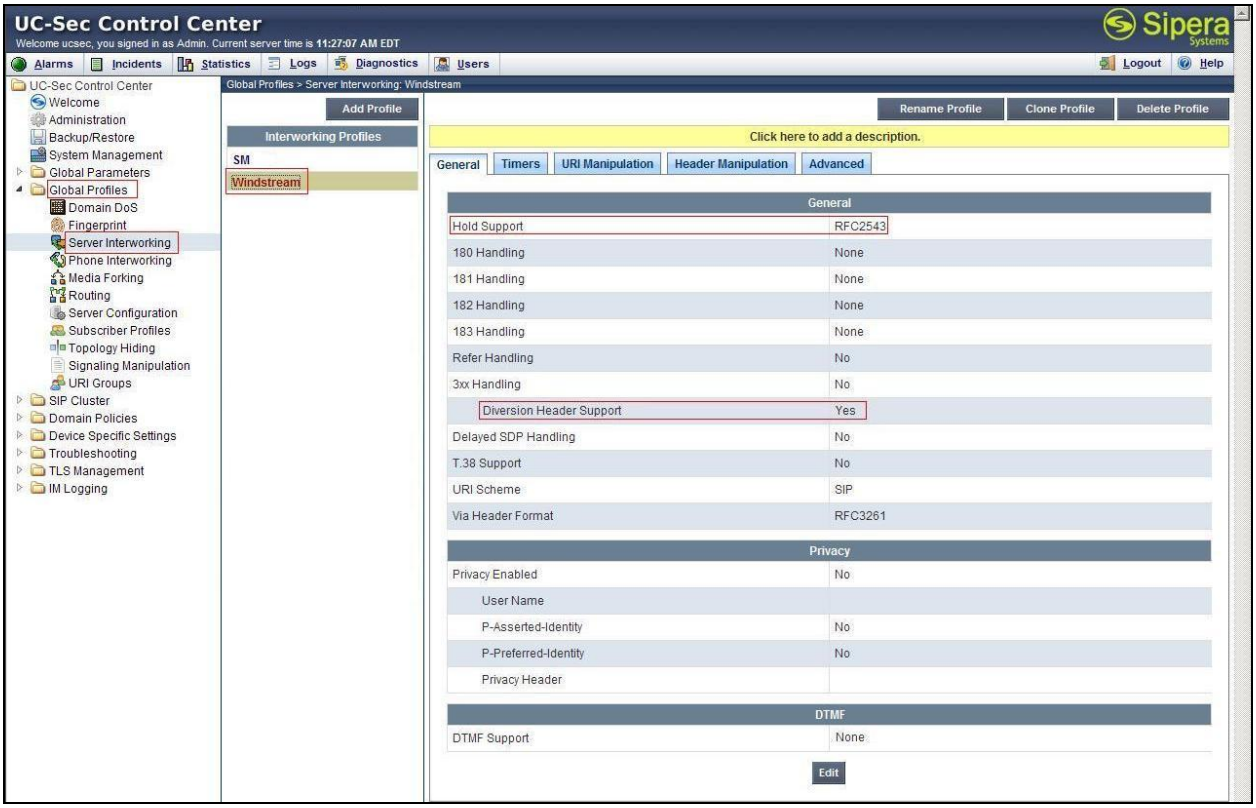


8.2.2. Configure Server Interworking – Windstream side

- Select **Global Profiles** from the menu on the left-hand side
- Select the **Server Internetworking**

©2012 Avaya Inc. All Rights Reserved.

- Select **Add Profile** and enter Internetworking profile **Windstream**
- In the **General** Tab:
  - Check **Hold Support** as **RFC2543**
  - Check **Diversion Header Support** as **Yes**
  - All other options in the General Tab can be left at default.
- In the **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** Tabs: All options can be left at default
- Click **Finish** (not shown)

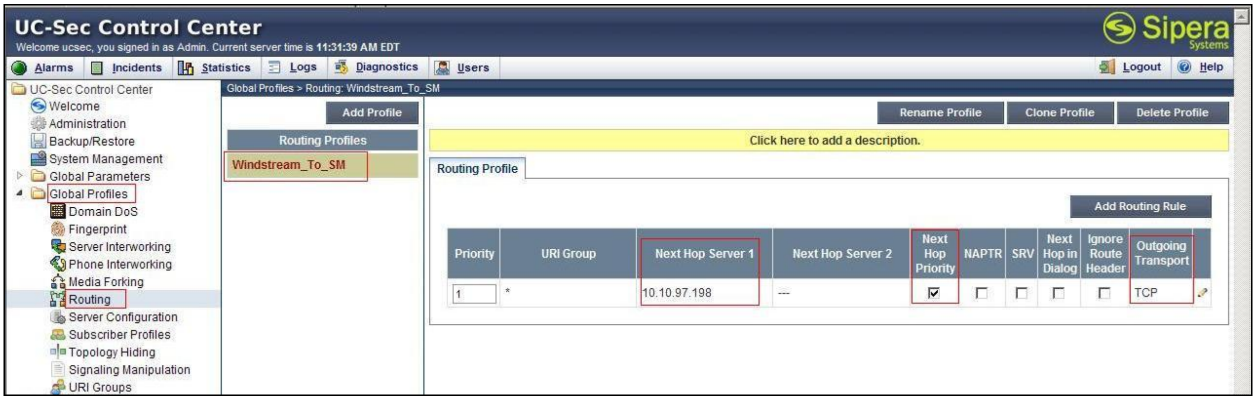


©2012 Avaya Inc. All Rights Reserved.

8.2.3. Configure Routing – Avaya side

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

- Select **Global Profiles** from the menu on the left-hand side
- Select the **Routing** tab
- Select **Add Profile** and enter Routing Profile **Windstream_To_SM**
  - **Next Hop Server 1**: **10.10.97.198 (Session Manager IP address)**
  - Check **Next Hop Priority**
  - **Outgoing Transport**: **TCP**
  - Click **Finish** (not shown)

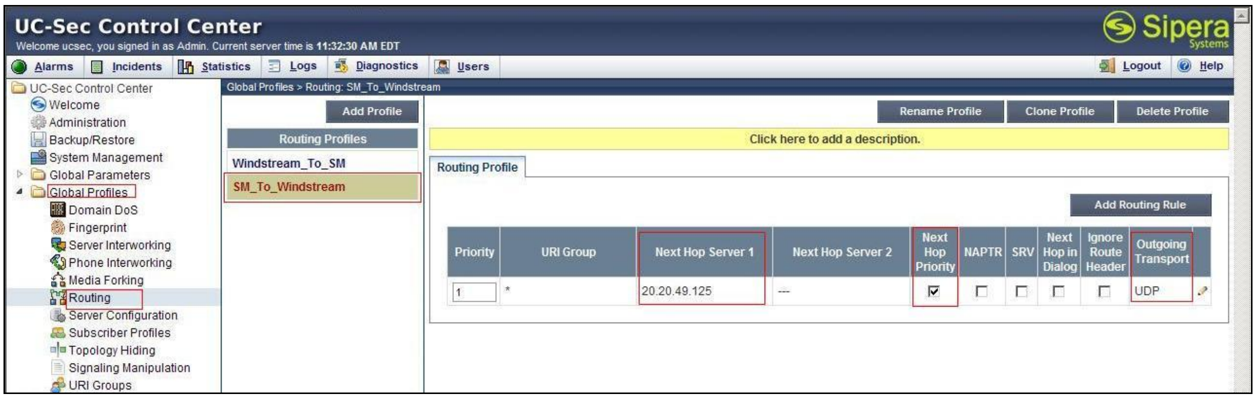


©2012 Avaya Inc. All Rights Reserved.

8.2.4. Configure Routing - Windstream side

The Routing Profile allows users to manage parameters related to routing SIP signaling messages.

- Select **Global Profiles** from the menu on the left-hand side
- Select the **Routing** tab
- Select **Add Profile** and enter Routing Profile **SM_To_Windstream**
  - **Next Hop Server 1**: **20.20.49.125** (IP Address provided by Windstream**)**
  - Check **Next Hop Priority**
  - **Outgoing Transport** as **UDP**

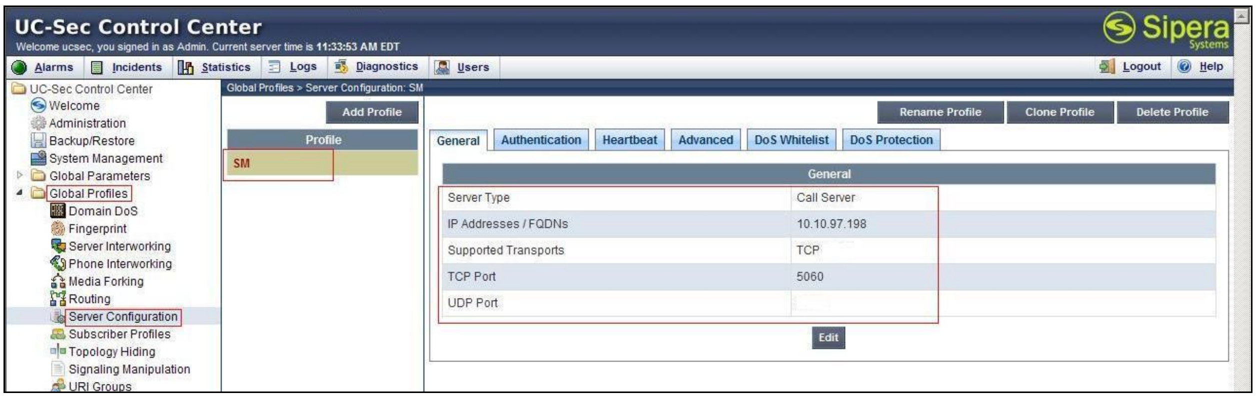


©2012 Avaya Inc. All Rights Reserved.

8.2.5. Configure Server – Avaya Session Manager

The Server Configuration screen contains four tabs: General, Authentication, Heartbeat, and Advanced. Together, these tabs are used to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signaling parameters and some advanced options.

- Select **Global Profiles** from the menu on the left-hand side
- Select the **Server Configuration**
- Select **Add Profile**, and enter Profile name **SM**
- On General tab:
  - **Server Type**: **Call Server**
  - **IP Address**: **10.10.97.198 (Session Manager IP Address)**
  - **Supported Transports**: Check **TCP**
  - **TCP Port**: **5060**



- On the **Advanced** Tab, select **SM** for **Interworking Profile**
- Click **Finish** (not shown)

©2012 Avaya Inc. All Rights Reserved.

8.2.6. Configure Server – Windstream Sonus Switch

- Select **Global Profiles** from the menu on the left-hand side
- Select the **Server Configuration**
- Select **Add Profile**, enter Profile:**Windstream**
- In General tab:
  - **Server Type**: **Trunk Server**
  - **IP Address: 20.20.49.125** (Windstream Trunk Server)
  - **Supported Transports**: Check **UDP**
  - **UDP Port**: **5060**

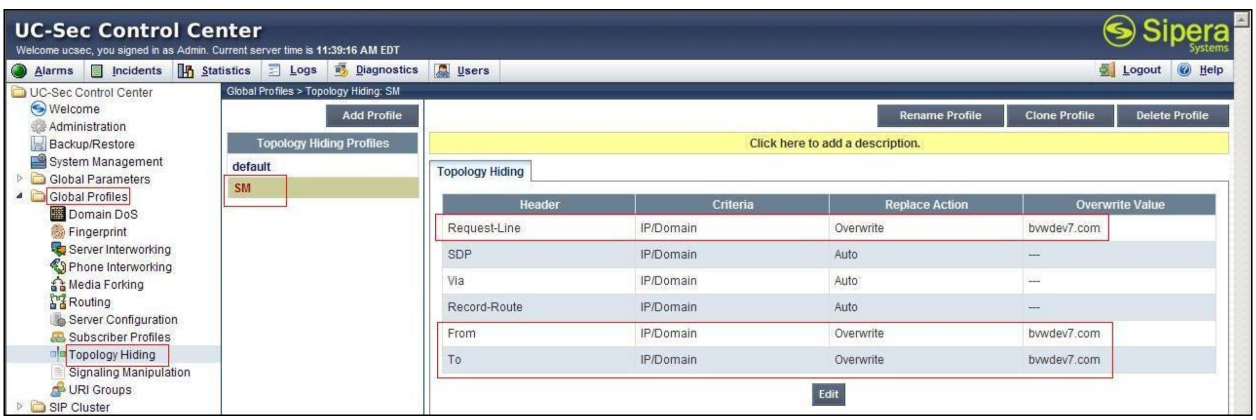
- On the **Advanced** Tab:
  - Select **Windstream** for **Interworking Profile**
  - Click **Finish** (not shown)

©2012 Avaya Inc. All Rights Reserved.

8.2.7. Configure Topology Hiding – Avaya side

The Topology Hiding screen shows how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

- Select **Global Profiles** from the menu on the left-hand side
- Select the **Topology Hiding**
- Click **Add Profile** and enter Topology Hiding Profile Name in the pop-up screen (not shown): **SM**, then click **Next** (not shown) to **Add Headers**.
- For the Header **To**,
    - In the **Criteria** column select **IP/Domain**
    - In the **Replace Action** column select: **Overwrite**
    - In the **Overwrite Value** column: **bvwdev7.com**
- For the Header **Request-Line**,
    - In the **Criteria** column select **IP/Domain**
    - In the **Replace Action** column select: **Overwrite**
    - In the **Overwrite Value** column: **bvwdev7.com**
- For the Header **From**,
    - In the **Criteria** column select **IP/Domain**
    - In the **Replace Action** column select: **Overwrite**
    - In the **Overwrite Value** column: **bvwdev7.com**



©2012 Avaya Inc. All Rights Reserved.

8.2.8. Configure Topology Hiding – Windstream side

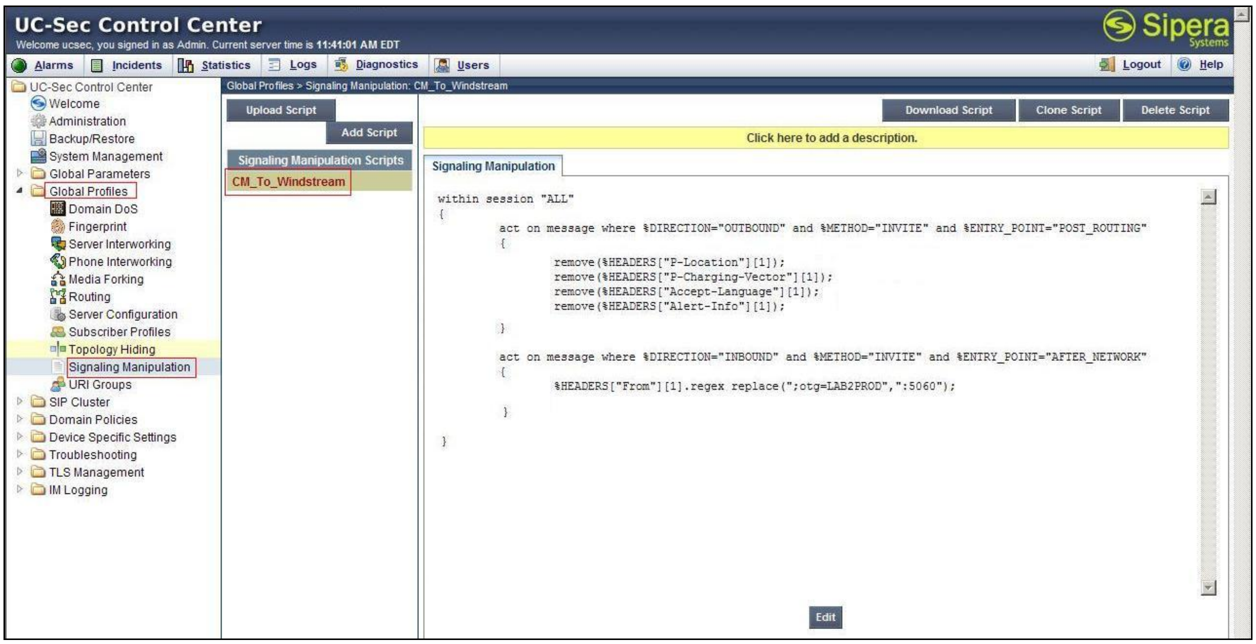
- Select **Global Profiles** from the menu on the left-hand side
- Select the **Topology Hiding**
- Click **Add Profile** and enter Topology Hiding Profile Name in the pop-up screen (not shown): **Windstream**, then click **Next** (not shown) to **Add Headers**.
- For the Header **To,**
    - In the **Criteria** column select **IP/Domain**
    - In the **Replace Action** column s**elect: Overwrite**
    - In the **Overwrite Value** column**: 20.20.49.125**
- For the Header **Request-Line,**
    - In the **Criteria** column select **IP/Domain**
    - In the **Replace Action** column select: **Overwrite**
    - In the **Overwrite Value** column: **20.20.49.125**

©2012 Avaya Inc. All Rights Reserved.

8.2.9. Configure Signaling Manipulation

Avaya SBCE SIP signaling header manipulation feature is used for the UC-Sec product. This feature provides the ability to add, change and delete any of the headers and other information in a SIP message

- Select **Global Profiles** from the menu on the left-hand side
- Select the **Signaling Manipulation**
- Select **Add Script** and enter Signaling Manipulation Script **CM_To_Windstream**
- Add the script to remove unwanted headers from the body of the SIP message
- Click **Save** (not shown)



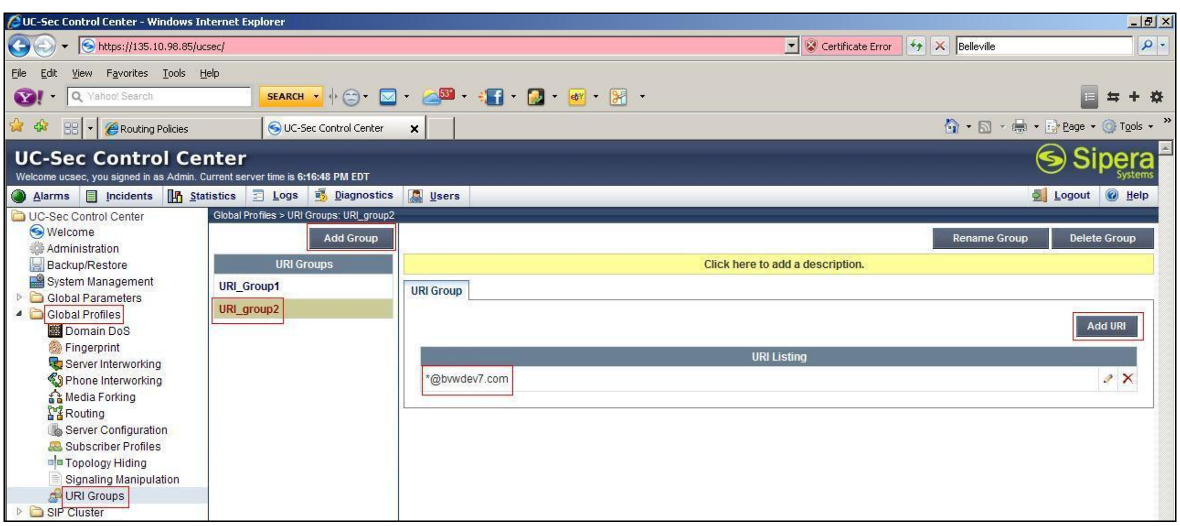
©2012 Avaya Inc. All Rights Reserved.

8.2.10. Configure URI Groups

The URI Group feature helps to create any number of logical URI groups that are comprised of individual SIP subscribers located in a particular domain or group.

- Select **Global Profiles** from the menu on the left-hand side
- Select **URI Groups**
- Select **Add Groups** and enter URI Group **URI Group1** in the next screen (not shown), then click **Next** (not shown)
- Select the **URI Type**: **Plain**
- Add **URI**: ***@bvwdev7.com**
- Click **Finish**

- Select Global Profiles from the menu on the left-hand side
- Select the **URI Groups**
- Select **Add Groups** and enter Group Name: **URI_group2** in the screen (not shown) and then click **Next**
- Select the **URI Type**: **Plain**
- Add **URI**: ***@bvwdev7.com**
- Click Finish (not shown)



©2012 Avaya Inc. All Rights Reserved.

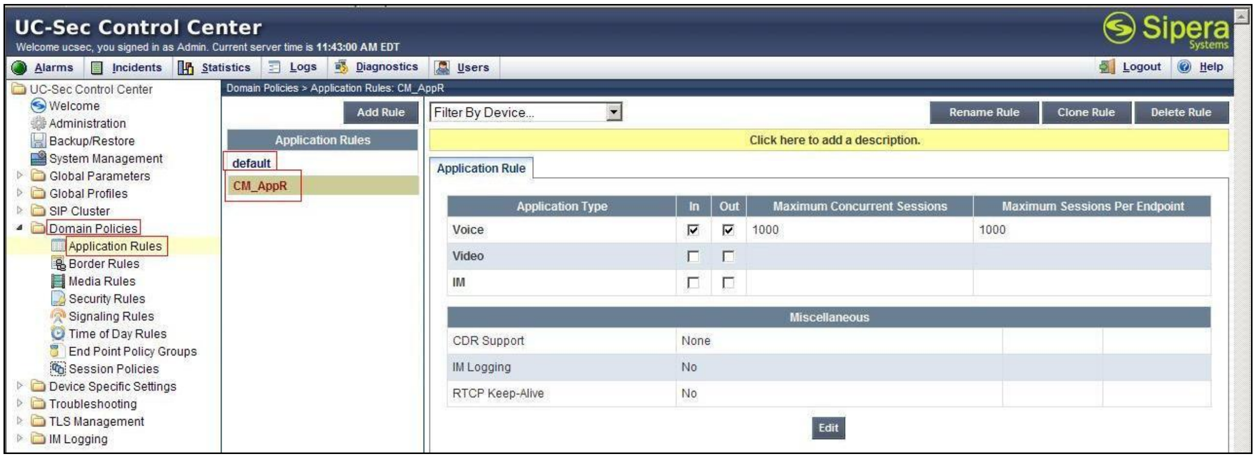
8.3. Domain Policies

The Domain Policies feature allows users to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criterion of communication sessions originating from or terminating at the enterprise. These criterion can be used to trigger different policies which will apply to call flows, change the behavior of the call, and make sure the call does not violate any of the policies. There are default policies available for use, or users can create custom domain policies.

8.3.1. Create Application Rules

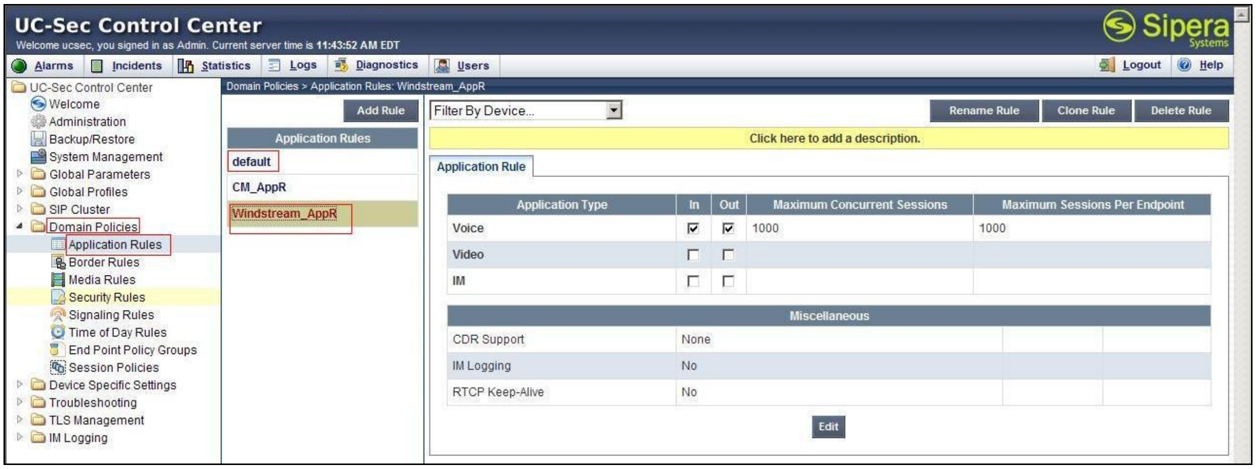
Application Rules allow users to define which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: voice, video, and/or Instant Messaging (IM). In addition, users can determine the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

- Select **Domain Policies** from the menu on the left-hand side
- Select the **Application Rules**
- Select the **default** Rule
- Select **Clone Rule** button
    - o Enter Clone Name: **CM_AppR**
    - o Click Finish (not shown)



©2012 Avaya Inc. All Rights Reserved.

- Select **Domain Policies** from the menu on the left-hand side
- Select the **Application Rules**
- Select the **default** Rule
- Select **Clone Rule** button
    - Enter Clone Name: **Windstream_AppR**
    - Click Finish (not shown)

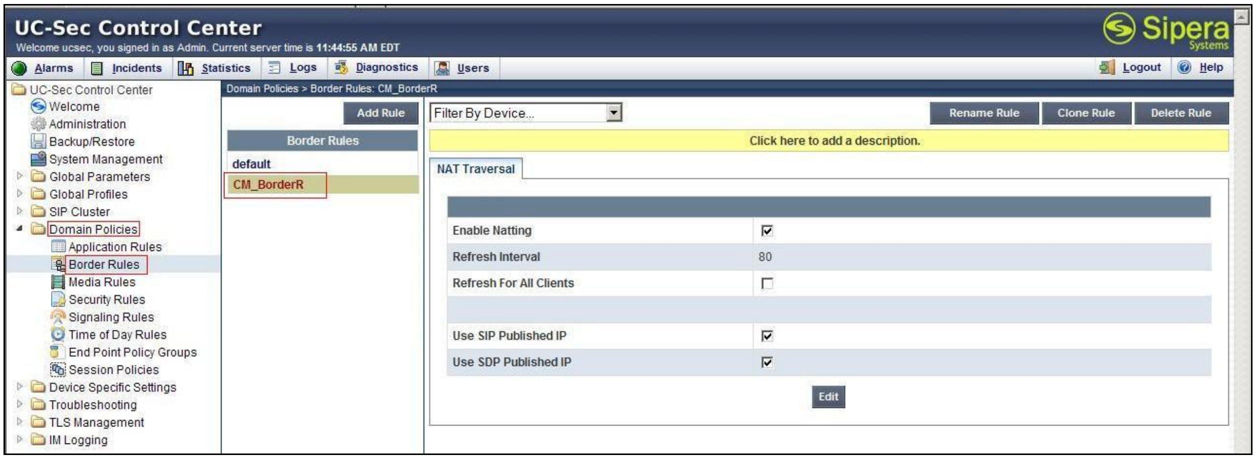


©2012 Avaya Inc. All Rights Reserved.

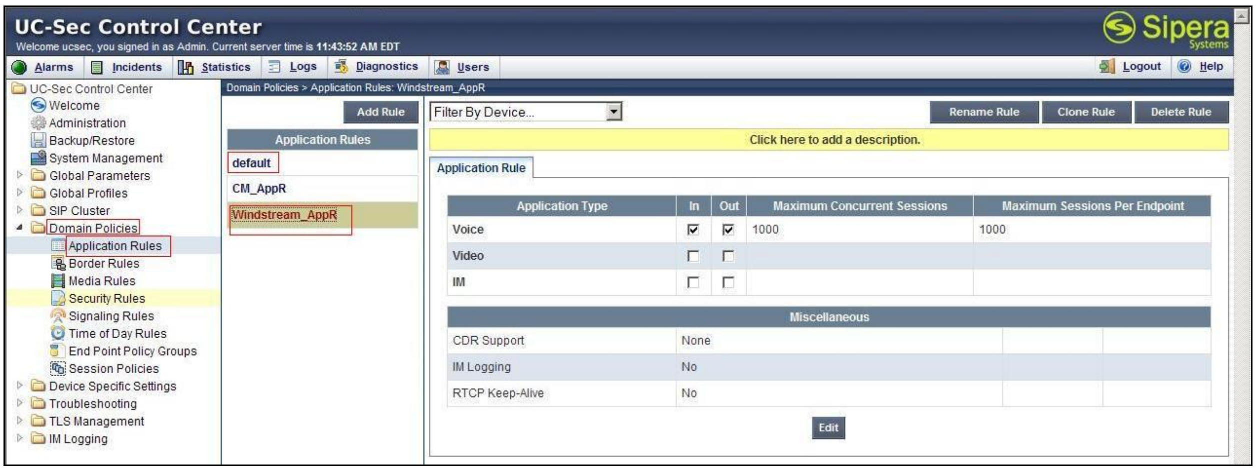
8.3.2. Create Border Rules

Border Rules allow control of NAT Traversal. The NAT Traversal feature determines whether or not call flowing through the DMZ needs to traverse a firewall and the manner in which pinholes are kept open in the firewall to accommodate traffic.

- Select **Domain Policies** from the menu on the left-hand side
- Select the **Border Rules**
- Select the **default** Rule
- Select **Clone Rule** button
    - Enter Clone Name: **CM_BorderR**
    - Click Finish (not shown)



- Select **Domain Policies** from the menu on the left-hand side
- Select the **Border Rules**
- Select the **default** Rule
- Select **Clone Rule** button
    - Enter Clone Name**: Windstream_BorderR**
    - Click Finish (not shown)

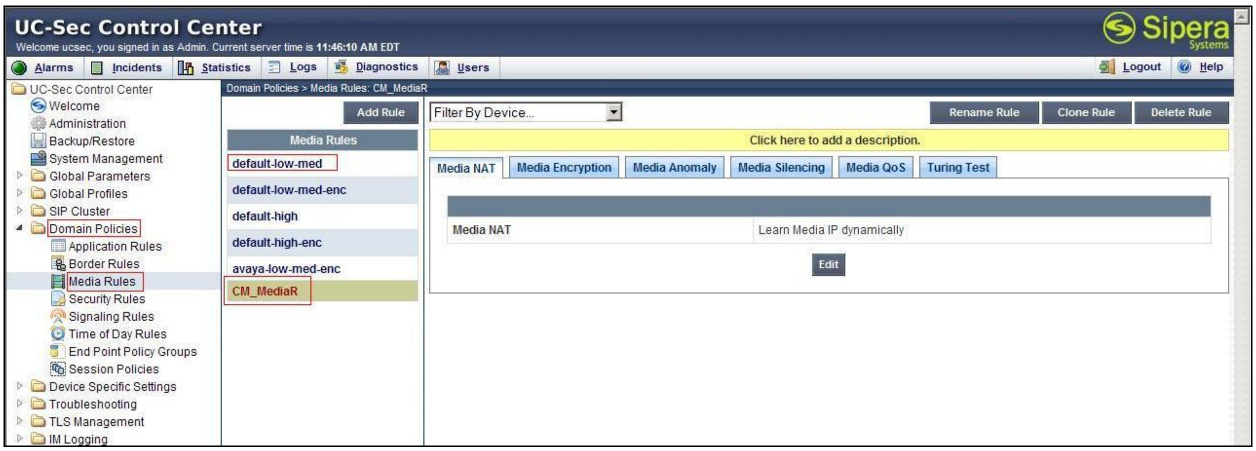


©2012 Avaya Inc. All Rights Reserved.

8.3.3. Create Media Rules

Media Rules allow definition of RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the UC-Sec security product

- Select **Domain Policies** from the menu on the left-hand side
- Select the **Media Rules**
- Select the **default-low-med** Rule
- Select **Clone Rule** button
    - Enter Clone Name**: CM_MediaR**
    - Click Finish (not shown**)**



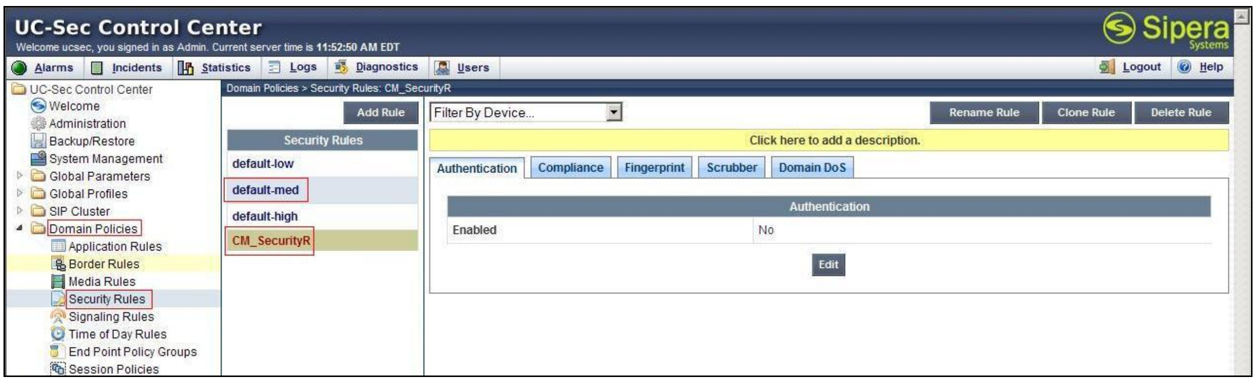
- Select **Domain Policies** from the menu on the left-hand side
- Select the **Media Rules**
- Select the **default-low-med** Rule
- Select **Clone Rule** button
    - Enter Clone Name: **Windstream_MediaR**
    - Click Finish (not shown)

©2012 Avaya Inc. All Rights Reserved.

8.3.4. Create Security Rules

Security Rules define which enterprise-wide VoIP and Instant Message (IM) security features will be applied to a particular call flow. Security Rules allows configuration of Authentication, Compliance, Fingerprinting, Scrubber, and Domain DoS. In addition to determining which combination of security features are applied, user can also define the security feature profile so that the feature is applied in a specific manner to a specific situation

- Select **Domain Policies** from the menu on the left-hand side
- Select the **Security Rules**
- Select the **default-med** Rule
- Select **Clone Rule** button
  - Enter Clone Name**: CM_SecurityR**
  - Click Finish (not shown)



- Select **Domain Policies** from the menu on the left-hand side
- Select the **Security Rules**
- Select the **default-med** Rule
- Select **Clone Rule** button
  - Enter Clone Name: **Windstream_SecurityR**
  - Click Finish (not shown)

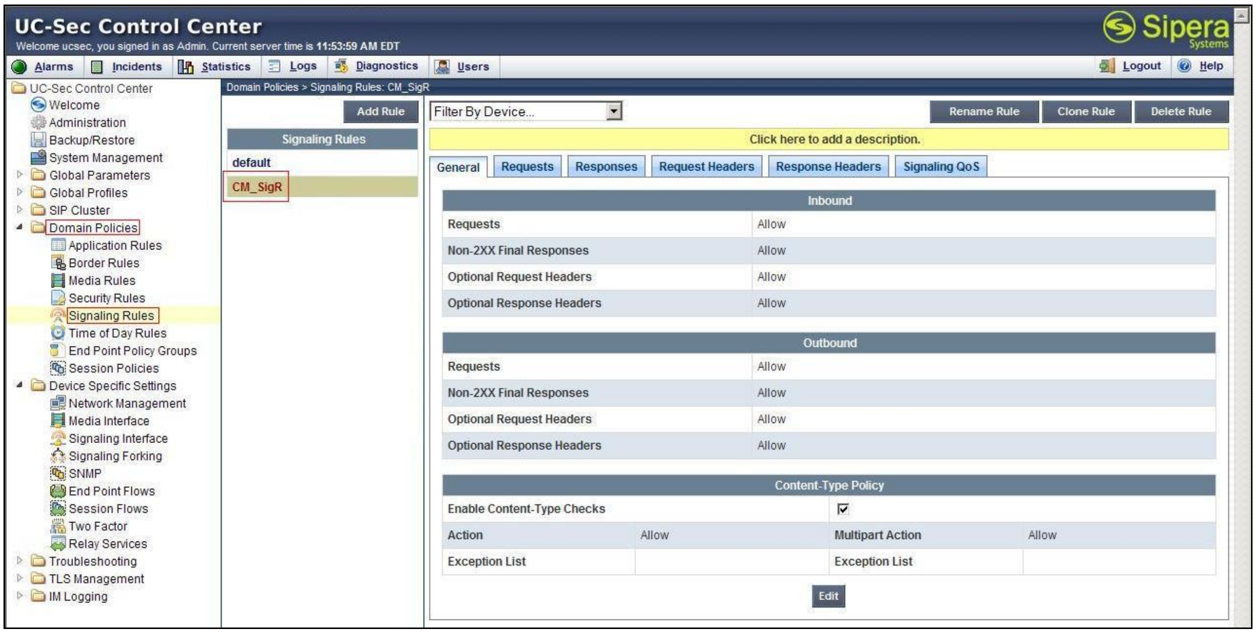
8.3.5. Create Signaling Rules

Signaling Rules define the action to be taken (*Allow*, *Block*, *Block with Response*, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are

©2012 Avaya Inc. All Rights Reserved.

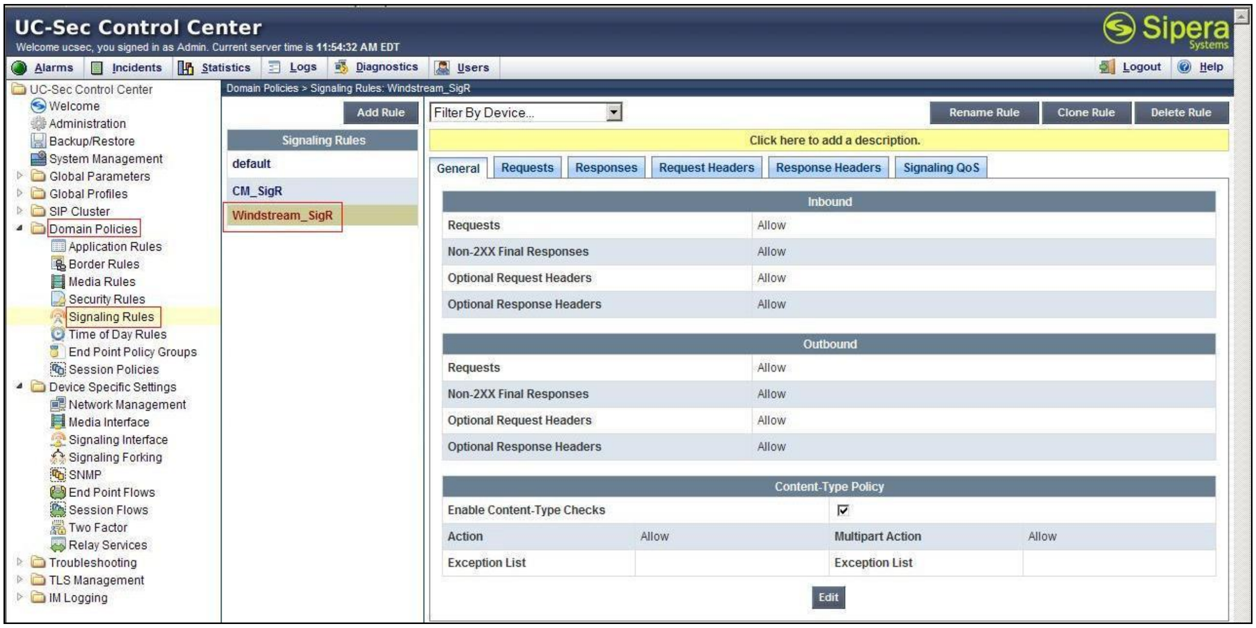
received by the UC-Sec, they are parsed and “patternmatched” against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching

- Select **Domain Policies** from the menu on the left-hand side
- Select the **Signaling Rules**
- Select the **default** Rule
- Select **Clone Rule** button
    - o Enter Clone Name: **CM_SigR**
- Click Finish (not shown)



©2012 Avaya Inc. All Rights Reserved.

- Select **Domain Policies** from the menu on the left-hand side
- Select the **Signaling Rules**
- Select the **default** Rule
- Select **Clone Rule** button
    - Enter Clone Name: **Windstream_SigR**
    - Click Finish (not shown)

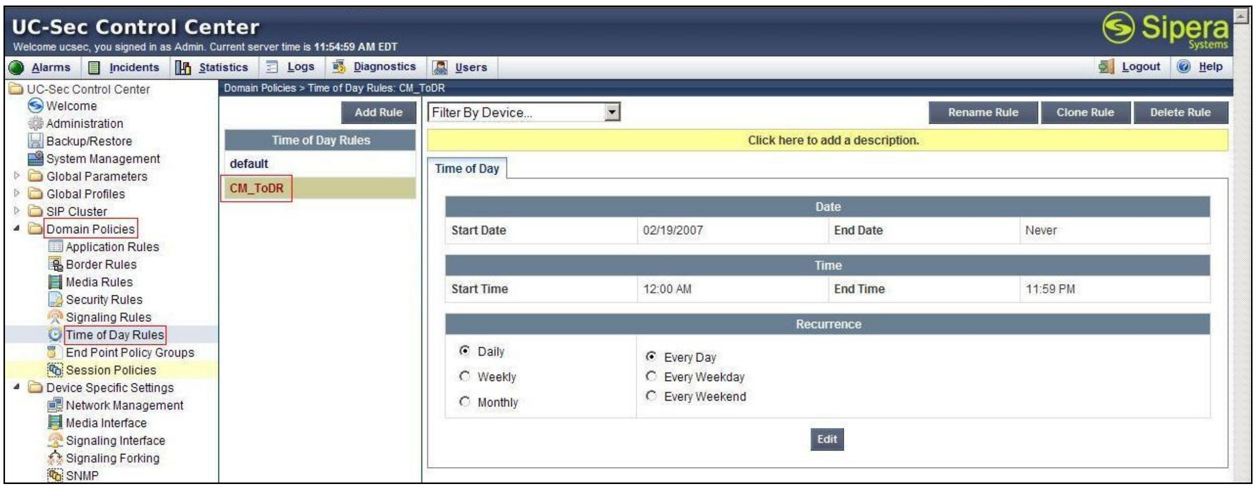


©2012 Avaya Inc. All Rights Reserved.

8.3.6. Create Time of Day Rules

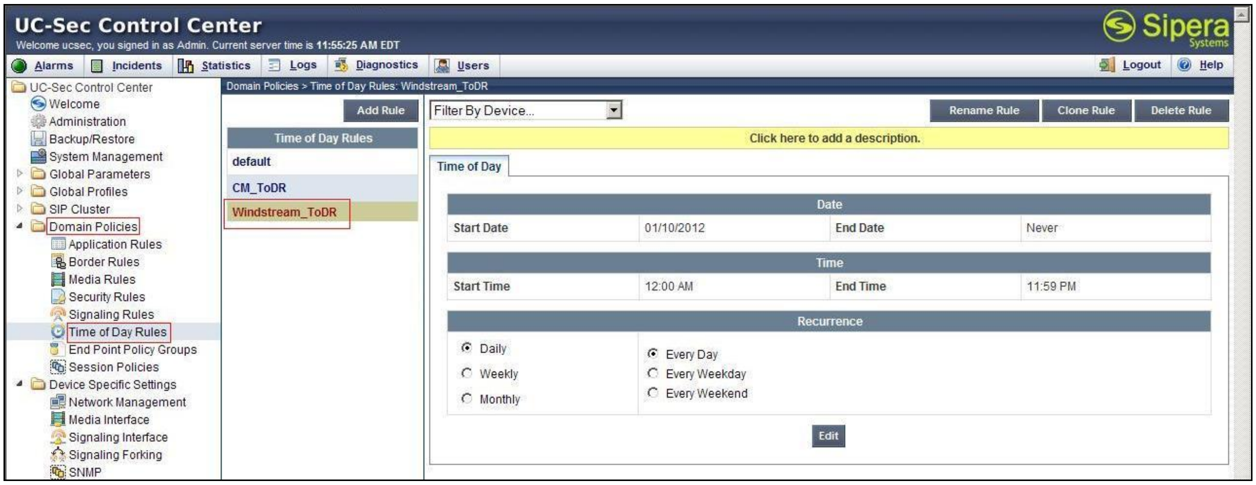
A Time-of-day (ToD) Rule allows to determine when the domain policy it is assigned to will be in effect. ToD rules provide complete flexibility to fully accommodate the enterprise by not only determining when a particular domain policy will be in effect, but also where it will apply to, and for how long it will remain in effect.

- Select **Domain Policies** from the menu on the left-hand side
- Select the **Time of Day Rules**
- Select the **default** Rule
- Select **Clone Rule** button
    - Enter Clone Name: **CM_ToDR**
    - Click Finish (not shown)



©2012 Avaya Inc. All Rights Reserved.

- Select **Domain Policies** from the menu on the left-hand side
- Select the **Time of Day Rules**
- Select the **default** Rule
- Select **Clone Rule** button
  - o Enter Clone Name: **Windstream_ToDR**
  - o Click Finish (not shown)

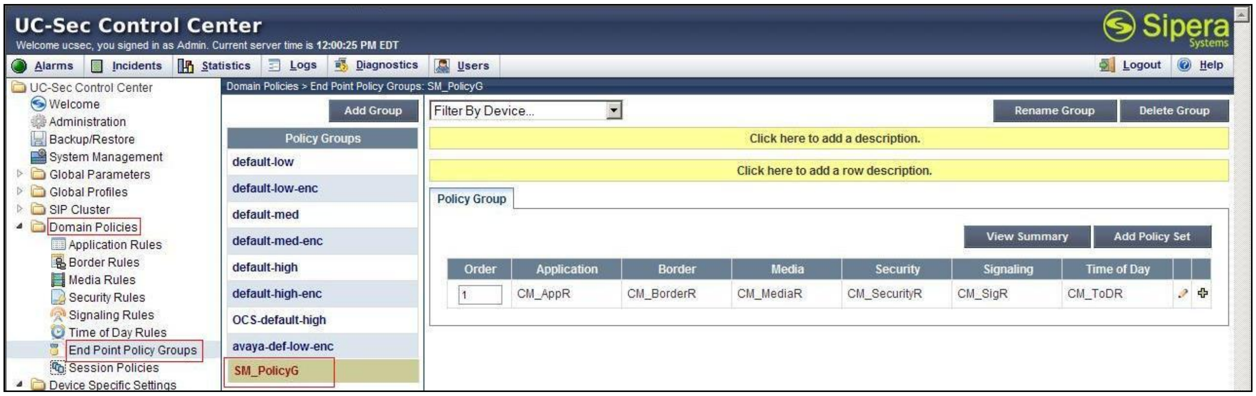


©2012 Avaya Inc. All Rights Reserved.

8.3.7. Create Endpoint Policy Groups

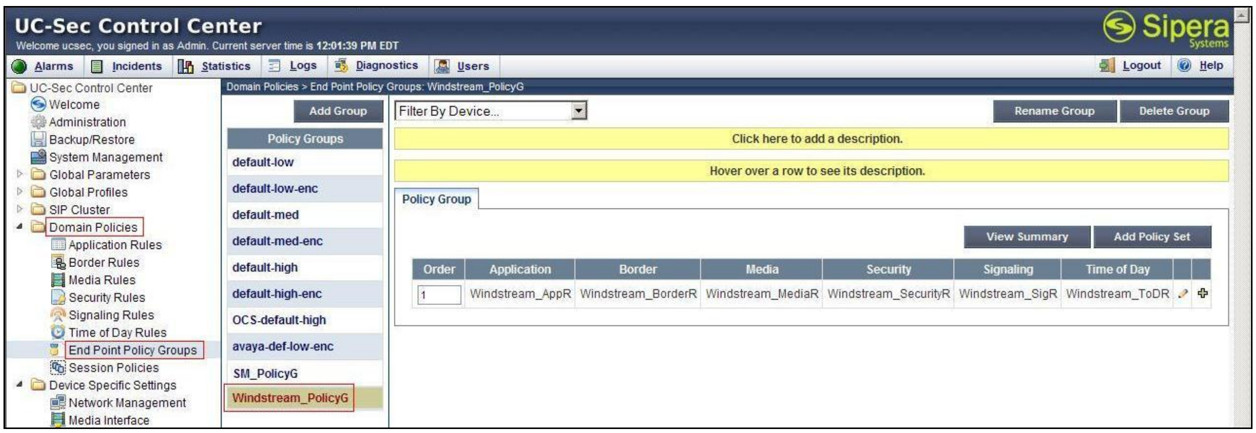
The End-Point Policy Group feature allows users to create **Policy Sets** and **Policy Groups**. A Policy Set is an association of individual, SIP signaling-specific security policies (rule sets): application, border, media, security, signaling, and ToD. (Each of which was creating using the procedures contained in the previous sections.) A Policy Group is comprised of one or more Policy Sets. The purpose of Policy Sets and Policy Groups is to increasingly aggregate and simplify the application of UC-Sec security features to very specific types of SIP signaling messages traversing through the enterprise

- Select **Domain Policies** from the menu on the left-hand side
- Select the **End Point Policy Groups**
- Select **Add Group**
- Enter **Group Name**: **CM_PolicyG**, in a pop-up screen (not shown) and then click **Next**
    - **Application Rule**: **CM_AppR**
    - **Border Rule**: **CM_BorderR**
    - **Media Rule**: **CM_MediaR**
    - **Security Rule**: **CM_SecurityR**
    - **Signaling Rule**: **CM_SigR**
    - **Time of Day: CM_ToDR**
    - Select Finish (not shown)



©2012 Avaya Inc. All Rights Reserved.

- Select **Domain Policies** from the menu on the left-hand side
- Select the **End Point Policy Groups**
- Select **Add Group**
- Enter **Group Name**: **Windstream_PolicyG**, in the pop-up window (not shown) and then click **Next**
    - **Application Rule**: **Windstream_AppR**
    - **Border Rule**: **Windstream_BorderR**
    - **Media Rule**: **Windstream_MediaR**
    - **Security Rule**: **Windstream_SecurityR**
    - **Signaling Rule**: **Windstream_SigR**
    - **Time of Day**: **Windstream_ToDR**
    - Select **Finish** (not shown)

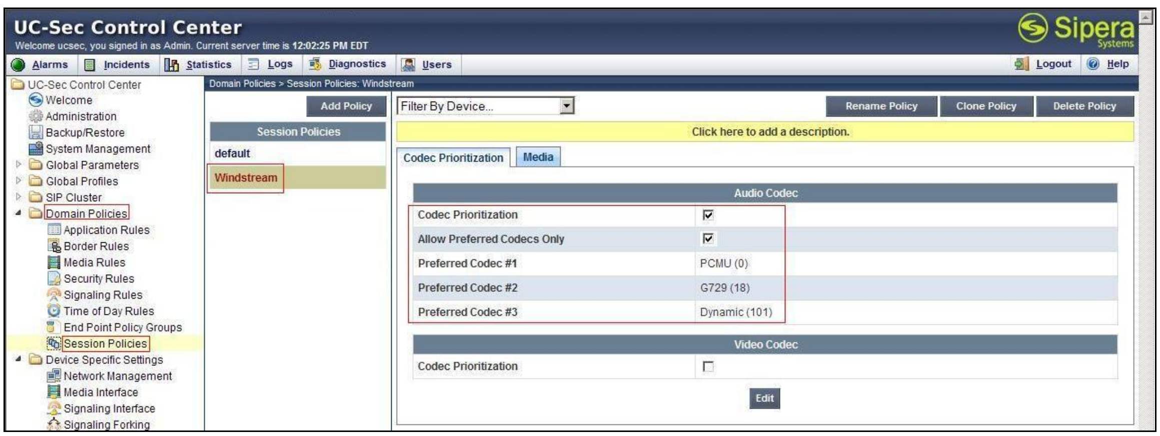


©2012 Avaya Inc. All Rights Reserved.

8.3.8. Create Session Policy

Session Policies allow users to define RTP media packet parameters such as codec types (both audio and video) and codec matching priority. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criterion will be handled by the UC-Sec security product.

- Select **Domain Policies** from the menu on the left-hand side
- Select the **Session Policies**
- Select **Add Policy**
- Enter **Policy Name**: **Windstream**, in the pop-up screen (not shown) and then click **Next**
    - Check **Codec Prioritization** and **Allow Preferred Codecs Only**
    - Set **Preferred Codec #1**: **PCMU (0)**
    - Set **Preferred Codec #2**: **G729 (18)**
    - Set **Preferred Codec #3**: **Dynamic (101)**
    - Select **Finish** (not shown)



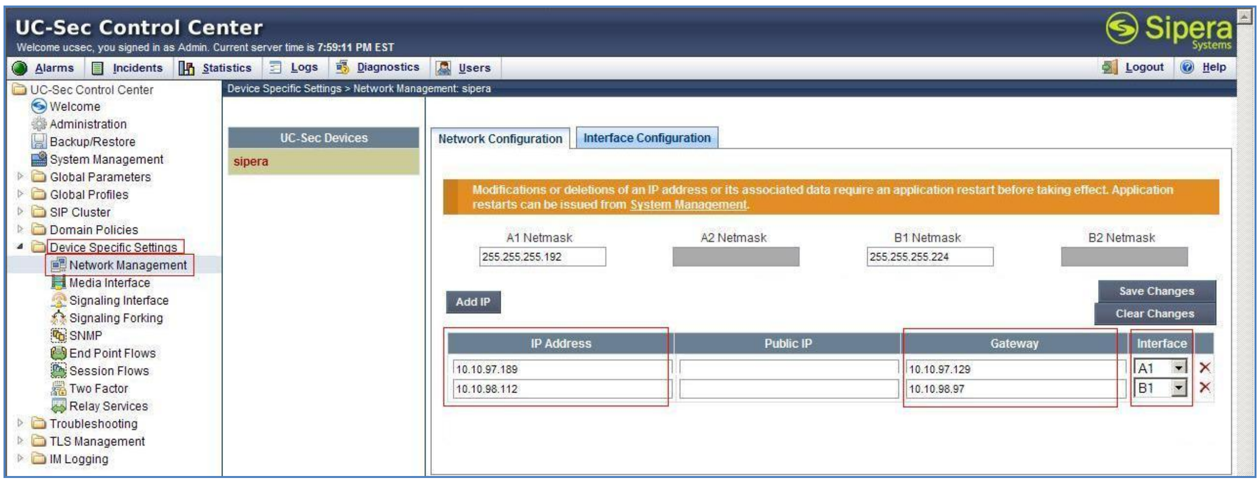
8.4. Device Specific Settings

The Device Specific Settings feature for SIP allows users to view aggregate system information, and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, users have the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows and Network Management.

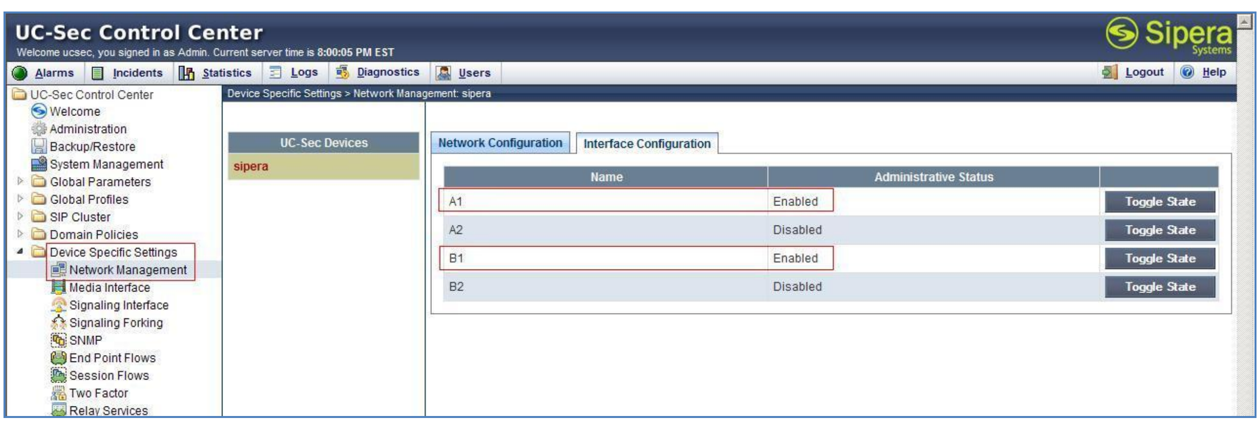
©2012 Avaya Inc. All Rights Reserved.

8.4.1. Manage Network Settings

- Select **Device Specific Settings** from the menu on the left-hand side
- Select **Network Management**
- Click **Add IP** and enter the **IP Address** and **Gateway Address** for both the Inside and the Outside interfaces:
  - **IP Address for Inside interface**: **10.10.97.189**; **Gateway**: **10.10.97.129**
  - **IP Address for Outside interface**: **10.10.98.112**; **Gateway**: **10.10.98.97**
- Select the physical interface used in the Interface column:
  - **Inside Interface**: **A1**
  - **Outside Interface**: **B1**



- Select the **Interface Configuration** Tab
- Toggle the State of the physical interfaces being used to enable them

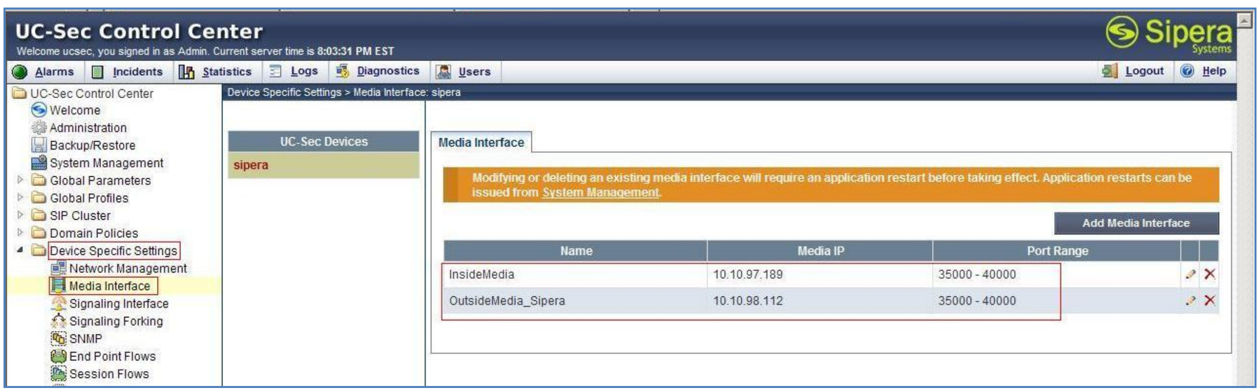


©2012 Avaya Inc. All Rights Reserved.

8.4.2. Create Media Interfaces

Media Interfaces define the type of signaling on the ports. The default media port range on the Avaya SBCE can be used for both inside and outside ports

- Select **Device Specific Settings** from the menu on the left-hand side
- Select **Media Interface**
- Select **Add Media Interface** and configure as follows:
  - **Name**: **InsideMedia**
  - **Media IP**: **10.10.97.189** (Internal Address toward Avaya Session Manager)
  - **Port Range**: **35000 - 40000**
  - Click Finish (not shown)
- Select **Add Media Interface** and configure as follows:
  - **Name**: **OutsideMedia_Avaya**
  - **Media IP**: **10.10.98.112** (External Internet Address toward Winstream trunk)
  - **Port Range**: **35000 - 40000**
  - Click Finish (not shown)



©2012 Avaya Inc. All Rights Reserved.

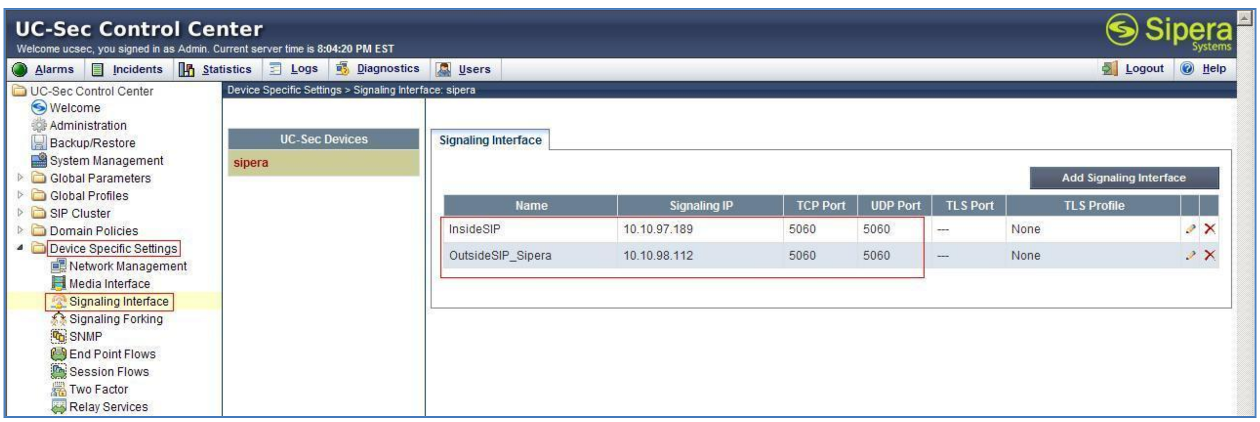
8.4.3. Create Signaling Interfaces

Signaling Interfaces define the type of signaling on the ports.
Inside SIP Avaya SBCE signaling interface was created as followings:

- Select **Device Specific Settings** from the menu on the left-hand side
- Select **Signaling Interface**
- Select **Add Signaling Interface**
  - **Name: InsideSIP**
  - **Media IP: 10.10.97.189** (Internal Address toward Avaya Session Manager)
  - **TCP Port: 5060**
  - **UDP Port: 5060**
  - Click Finish (not shown)

Similarly Outside SIP Avaya SBCE signaling interface was created as followings:

- Select **Device Specific Settings** from the menu on the left-hand side
- Select **Signaling Interface**
- Select **Add Signaling Interface**
  - **Name**: **OutsideSIP_Sipera**
  - **Media IP**: **10.10.98.112** (External Internet Address toward Windstream trunk)
  - **TCP Port**: **5060**
  - **UDP Port**: **5060**
  - Click Finish (not shown)



©2012 Avaya Inc. All Rights Reserved.

8.4.4. Configuration Server Flows

Server Flows allow users to categorize trunk-side signaling and apply a policy.

8.4.4.1 Create End Point Flows - To Avaya side

- Select **Device Specific Settings** from the menu on the left-hand side
- Select **End Point Flows**
- Select the **Server Flows** tab and click **Add Flow** (not shown). A pop-up screen (not shown) is displayed and configured as follows:
  - **Flow Name**: **Windstream_To_SM**
  - **Server Configuration**: **Windstream**
  - **URI Group**: *
  - **Transport**: *
  - **Remote Subnet**: *
  - **Received Interface**: **InsideSIP**
  - **Signaling Interface**: **OutsideSIP_SBCE**
  - **Media Interface**: **OutsideMedia_SBCE**
  - **End Point Policy Group**: **Windstream_PolicyG**
  - **Routing Profile**: **Windstream_To_SM**
  - **Topology Hiding Profile**: **Windstream**
  - **File Transfer Profile**: **None**
  - Click **Finish** (not shown)

8.4.4.2 Create End Point Flows – To Windstream side

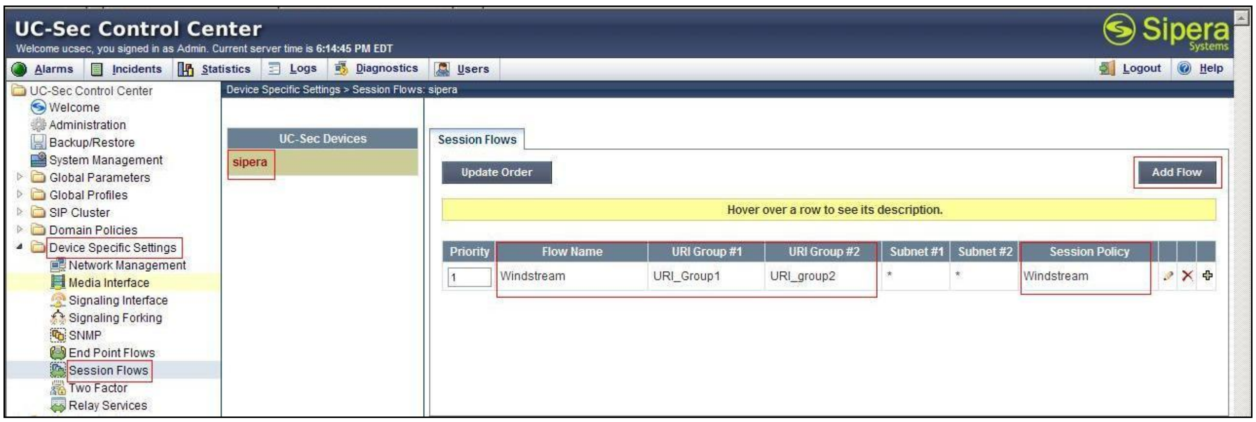
- Select **Device Specific Settings** from the menu on the left-hand side
- Select **End Point Flows**
- Select the **Server Flows** tab and click **Add Flow** (not shown). A pop-up window (not shown) is displayed and configured as follows:
    - **Flow Name**: **SM_To_Windstream**
    - **Server Configuration**: **SM**
    - **URI Group**: *****
    - **Transport**: *****
    - **Remote Subnet: ***
    - **Received Interface**: **OutsideSIP_SBCE**
    - **Signaling Interface: InsideSIP**
    - **Media Interface**: **InsideMedia**
    - **End Point Policy Group**: **SM_PolicyG**
    - **Routing Profile**: **SM_To_Windstream**
    - **Topology Hiding Profile**: **SM**
    - **File Transfer Profile**: **None**
    - Click Finish (not shown)

©2012 Avaya Inc. All Rights Reserved.

8.4.5. Create Session Flow

Session Flow determines the media (audio/video) sessions in order to apply the appropriate session policy

- Select **Device Specific Settings** from the menu on the left-hand side
- Select the **Session Flows**
- Select **Add Flow**(not shown) and in the pop-up window displayed (not shown) configure as follows:
    - **Flow Name**: **Windstream**
    - **URI Group#1**: **URI_Group1**
    - **URI Group#2**: **URI_group2**
    - **Session Policy**: **Windstream**
- Select **Finish** (not shown)



©2012 Avaya Inc. All Rights Reserved.

9. Verification Steps

The following steps may be used to verify the configuration.

9.1. General

Place an inbound or outbound call between a PSTN phone and an internal Avaya phone, answer the call, and verify that two-way speech path exists. Verify that the call remains stable for several minutes and disconnects properly.

9.1.1. Example for Inbound Call from PSTN via Windstream SIP Trunk

Incoming PSTN calls arrive from Windstream at the Avaya SBCE, which sends the call to Session Manager. Session Manager routes the call to Communication Manager via the entity link corresponding to the Communication Manager .On Communication Manager, the incoming call arrives via signaling group 2 and trunk group 11.

The following Communication Manager **list trace** output shows a an incoming call on trunk group 11. The PSTN telephone dialed 8642634500. The incoming call handling table for trunk group 11 converted the number to X4500. X4500 is a H323 Telephone with IP Address 10.10.97.137. Initially, the G650 Media Gateway (10.10.97.207) is used, but as can be seen in the final trace output, once the call is answered, the final RTP media path is ip-direct from the IP Telephone (10.10.97.137) to the inside of the Avaya SBCE (10.10.97.189).

```
list trace tac *011                                                    Page   1
                                LIST TRACEtime            data
16:25:51 SIP<INVITE sip:8642634500@bvwdev7.com  SIP/2.0
16:25:51     Call-ID: 658200e7-7533-122f-6b8e-00259010ee66
16:25:51     active trunk-group 11 member 1    cid 0xff
16:25:51 SIP>SIP/2.0 180 Ringing
16:25:51     Call-ID: 658200e7-7533-122f-6b8e-00259010ee66
16:25:51     dial 4500
16:25:51     ring station      4500 cid 0xff
16:25:51     G711MU ss:off ps:20
             rgn:1 [10.10.97.137]:4752
             rgn:1 [10.10.97.207]:4052
16:25:51     G711MU ss:off ps:20
             rgn:1 [10.10.97.189]:40414
             rgn:1 [10.10.97.207]:4054
16:25:51     xoip options: fax:Relay modem:PT tty:US  uid:0x50033
             xoip ip: [10.10.97.207]:4054

list trace tac *011                                                    Page   2
                                LIST TRACE
time            data
16:25:52 SIP>SIP/2.0 200 OK
16:25:52     Call-ID: 658200e7-7533-122f-6b8e-00259010ee66
16:25:52     active station      2057 cid 0xff
16:25:53 SIP>SIP/2.0 200 OK
16:25:53     Call-ID: 658200e7-7533-122f-6b8e-00259010ee66
16:25:54 SIP>SIP/2.0 200 OK
16:25:54     Call-ID: 658200e7-7533-122f-6b8e-00259010ee66
16:25:56     idle station      4500 cid 0xff
```


©2012 Avaya Inc. All Rights Reserved.

9.1.2. Example for Outbound Call to PSTN via Windstream SIP Trunk

The following trace shows an outbound ARS call from IP Telephone x4500 to the PSTN number 6139675206. The call is routed to route pattern 1 and trunk group 10. The call initially uses the gateway (10.10.97.207), but after the call is answered, the call is shuffled to become an ip-direct connection between the IP Telephone (10.10.97.137) and the inside of the Avaya SBCE (10.10.97.189)

```
list trace tac *010                                                  Page   1

                                LIST TRACE

time            data

16:27:18     dial 916139675206 route:ARS
16:27:18     route-pattern  1 preference 1 location 1/ALL  cid 0x101
16:27:18     seize trunk-group 10 member 13    cid 0x101
16:27:18     Calling Number & Name 4500 IP_4500
16:27:18 SIP>INVITE sip:16139675206@bvwdev7.com SIP/2.0
16:27:18     Call-ID: 04aa07143e115ec4eafd7dd00
16:27:18     Setup digits 16139675206
16:27:18     Calling Number & Name 6477252057 IP_4500
16:27:18 SIP<SIP/2.0 100 Trying
16:27:18     Call-ID: 04aa07143e115ec4eafd7dd00
16:27:18     Proceed trunk-group 10 member 13    cid 0x101
16:27:19 SIP<SIP/2.0 183 Session Progress
16:27:19     Call-ID: 04aa07143e115ec4eafd7dd00
16:27:19     G711MU ss:off ps:20
             rgn:1 [10.10.97.189]:40418
list trace tac *010                                                  Page   2

                  LIST TRACE

time            data
             rgn:1 [10.10.97.207]:4500
16:27:19     xoip options: fax:Relay modem:PT tty:US  uid:0x5000d
             xoip ip: [10.10.97.247]:4500
16:27:20 SIP<SIP/2.0 200 OK
16:27:20     Call-ID: 04aa07143e115ec4eafd7dd00
16:27:20 SIP>ACK sip:16139675206@135.10.97.189 5060;transport=udp SI
16:27:20 SIP>P/2.0
16:27:20     Call-ID: 04aa07143e115ec4eafd7dd00
16:27:20     active trunk-group 10 member 13    cid 0x101
16:27:20 SIP>INVITE sip:16139675206@135.10.97.189:5060;transport=udp
16:27:20 SIP> SIP/2.0
16:27:20     Call-ID: 04aa07143e115ec4eafd7dd00
16:27:20 SIP<SIP/2.0 100 Trying
16:27:20     Call-ID: 04aa07143e115ec4eafd7dd00
16:27:20 SIP<SIP/2.0 200 OK
16:27:20     Call-ID: 04aa07143e115ec4eafd7dd00
list trace tac *010                                                  Page   3

                                LIST TRACE

time            data
16:27:20     G711MU ss:off ps:20
             rgn:1 [10.10.97.137]:4752
             rgn:1 [10.10.97.184]:40418
16:27:20 SIP>ACK sip:16139675206@135.10.97.189:5060;transport=udp SI
16:27:20 SIP>P/2.0
```


©2012 Avaya Inc. All Rights Reserved.

```
16:27:20     Call-ID: 04aa07143e115ec4eafd7dd00
16:27:20     G711MU ss:off ps:20
             rgn:1 [10.10.97.184]:40418
             rgn:1 [10.10.97.137]:4752
16:27:23 SIP>BYE sip:16139675206@135.10.97.189:5060;transport=udp SI
16:27:23 SIP>P/2.0
16:27:23     Call-ID: 04aa07143e115ec4eafd7dd00
16:27:23     idle station      4500 cid 0x101
```


©2012 Avaya Inc. All Rights Reserved.

10. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager R6.0.1, Avaya Aura® Session Manager R6.1, and the Avaya SBCE R4.0.5 Q02 can be configured to interoperate successfully with Windstream. This solution allows Avaya Aura® Communication Manager and Avaya Aura® Session Manager customers to access the PSTN using a Windstream public SIP trunk service connection.

11. Additional References

Product services for Avaya SBCE may be found at:
http://www.sipera.com/products-services/esbc

Product documentation for Avaya, including the following, is available at:
http://support.avaya.com/

[1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.03, February 2011.

[2] *Administering Avaya Aura® System Platform*, Release 6, June 2010.

[3] *Administering Avaya Aura® Communication Manager*, Release 6.0, June 2010, Document Number 03-300509.

[4] *Avaya Aura® Communication Manager Feature Description and Implementation,* Release 6.0, June 2010, *D*ocument Number 555-245-205.

[5]*Installing and Upgrading Avaya Aura® System Manager*, Release 6.1, November 2010.

[6]*Installing and Configuring Avaya Aura® Session Manager*, Release 6.1, April 2011, Number 03-603473.

[7] *Administering Avaya Aura® Session Manager*, Release 6.1, May 2011, Document Number 03-603324.

[8] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, Release 3.1, November 2009, Document Number 16-300698.

[9]*Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide*, Release 2.6, June 2010, Document Number 16-601944.

[10] *Administering Avaya one-X® Communicator*, April 2011.

[11] *Using Avaya one-X® Communicator*, April 2011.

[12] *UC-Sec Install Guide (102-5224-400v1.01)*

[13] *UC-Sec Administration Guide (010-5423-400v106)*

[14] *RFC 3261 SIP: Session Initiation Protocol, http://www.ietf.org/*

[15] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method, http://www.ietf.org/*

[16] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, http://www.ietf.org/*

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

©2012 Avaya Inc. All Rights Reserved.

©2012 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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