

Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Communication Server 1000E R7.5, Avaya Aura® Session Manager R6.2, Avaya Session Border Controller for Enterprise R4.0.5 to support Cable & Wireless Storm SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describes the steps to configure Session Initiation Protocol (SIP) Trunking between Storm SIP Trunk Service and an Avaya SIP enabled Enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Session Border Controller for Enterprise and Avaya Communication Server 1000E.

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

©2012 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Cable & Wireless Storm SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Communication Server 1000E (CS1000E) connected to Storm SIP Trunk Service via an Avaya Session Border Controller for Enterprise (Avaya SBCE). Customers using this Avaya SIP-enabled Enterprise Solution with Storm SIP Trunk Service are able to place and receive PSTN calls via SIP protocol over a dedicated internet connection. This converged network solution is an alternative to traditional PSTN trunks. This approach normally results in lower cost for the enterprise.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of Session Manager, Avaya SBCE and CS1000E. The enterprise site was configured to use the SIP Trunk to Storm SIP Trunk Service. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1.**

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

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming PSTN calls were made to Unistim, SIP, Digital and Analog telephones at the enterprise
- Incoming calls to the enterprise site from the PSTN routed to the DDI numbers assigned by Storm
- Outgoing calls from the enterprise to the PSTN were made from Unistim, SIP, Digital and Analog telephones
- Outgoing calls from the enterprise site completed via Storm to PSTN destinations
- Calls using the G.711A codec supported by Storm
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls
- User features such as hold and resume, transfer, conference, call forwarding, etc
- Caller ID Presentation and Caller ID Restriction
- Call coverage and call forwarding for endpoints at the enterprise site
- Mobile-X call features
- Off-net call forwarding and mobility (extension to mobile)

©2012 Avaya Inc. All Rights Reserved.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Storm SIP Trunk with the following observations:

- As Storm do not support SIP UPDATE, the CS1000E default configuration will not allow a blind transfer to be executed if the parties involved do not support the SIP UPDATE method. With the installation of plugin 501 on the CS1000E, the blind transfer will be allowed and the call will be completed. The limitation of this plugin is that no ringback is provided to the originator of the call for the duration that the destination set is ringing. In addition to plugin 501, it is required that **VTRK SU version "cs1000-vtrk-7.50.17.16-15.i386.000.ntl"** or higher be used on all SSG signaling servers to ensure proper operation of the blind transfer feature. The use of plugin 501 does not restrict the use of the SIP UPDATE method of blind transfer to other parties that do happen to support the UPATE method, but rather extend support to those parties that do not
- 181 handling with SDP needs to be enabled on the Avaya SBCE as Storm SIP trunk service use this status code to indicate that the call is being forwarded to a different set of destinations. See **Section 7.2.1** and **Section 7.2.2** for this configuration
- Storm had Symmetric-Latching configured on their ACME-Packet SBC resulting in one-way ringback and no speech path during CallForward Off-Net testing. Storm disabled Symmetric latching on their Acme-Packet SBC and the CallForward Off-Net test case passed successfully
- T.38 fax transmission is not supported
- All unwanted MIME was stripped on outbound calls using the Adaptation Module in Session Manager
- No inbound toll free numbers were tested as none were available from the Service Provider
- No Emergency Services numbers tested as test calls to these numbers should be pre-arranged with the Operator

2.3. Support

Cable&Wireless Worldwide
Service Management Centre (Dublin)
Unit B, Willsborough Ind. Est.
Clonshaugh
Dublin 17
Ireland
Tel: 0035314040321
Service.ireland@cw.com

©2012 Avaya Inc. All Rights Reserved.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the Storm SIP Trunks Service. Located at the enterprise site are Session Manager, Avaya SBCE and CS1000E. Endpoints are Avaya 1140 series IP telephones, Avaya 1200 series (not shown in **Figure 1**) IP telephones (with Unistim and SIP firmware), Avaya IP Softphones (SMC3456, 2050 and Avaya one-X® Communicator), Avaya Digital telephone, Analog telephone and fax machine. For security purposes, any public IP addresses or PSTN routable phone numbers used in the compliance test are not shown in these Application Notes.

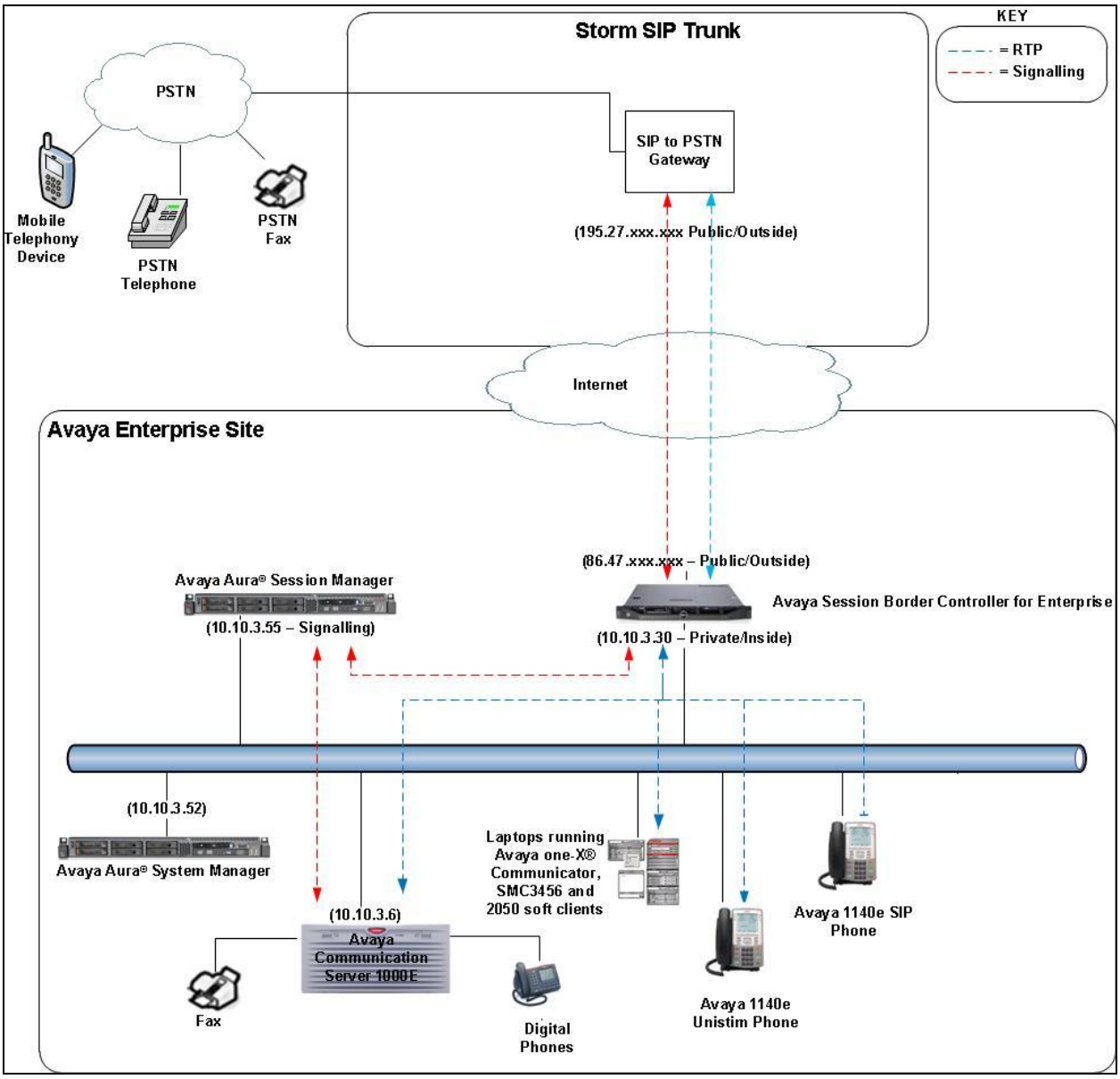


Figure 1: Test Setup Storm SIP Trunk Service to Avaya Enterprise

©2012 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Session Manager running on Avaya S8800 server	R6.2 Build: 6.2.2.0.622005
Avaya Aura® System Manager running on Avaya S8800 server	R6.2 Load: 6.2.0.0.15669 Service Pack 2
Avaya Communication Server 1000E running on CP+PM server as co-resident configuration	R7.5, Version 7.50.17 Service Update: 7.50_16Jul12 Deplist: X21 07.50Q
Avaya Session Border Controller for Enterprise on Dell R210 V2 server	Build: 4.0.5.Q09
Avaya Communication Server 1000E Media Gateway	CSP Version: MGCC CD02 MSP Version: MGCM AB01 APP Version: MGCA BA07 FPGA Version: MGCF AA18 BOOT Version: MGCB BA15 DSP1 Version: DSP1 AB04
Avaya 1140e and 1230 Unistim Telephones	FW: 0625C8A
Avaya 1140e and 1230 SIP Telephones	FW: 04.01.13.00.bin
Avaya SMC 3456	Version 2.6 build 53715
Avaya one-X® Communicator	Version cs6.1.0.10
Avaya Analog Telephone	N/A
Avaya M3904 Digital Telephone	N/A
Cable & Wireless Storm SIP Trunk Service	
DNX-400	RTPerformer Version 6

5. Configure Avaya Communication Server 1000E

This section describes the steps required to configure CS1000E for SIP Trunking and also the necessary configuration for terminals (analog, SIP and IP phones). SIP trunks are established between CS1000E and Session Manager. These SIP trunks carry SIP Signaling associated with Storm SIP Trunk Service. For incoming calls, the Session Manager receives SIP messages from the Avaya SBCE; through which Storms SIP Service directs incoming SIP messages to CS1000E (see **Figure 1**). Once a SIP message arrives at CS1000E, 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 CS1000E and may be first subject to outbound features such as route selection, digit manipulation and class of service restrictions. Once CS1000E selects a SIP trunk, the SIP signaling is routed to the Session Manager. The Session Manager directs the outbound SIP messages to the Avaya SBCE and on to Storms network. Specific CS1000E configuration was performed using Element Manager and the system terminal interface. The general installation of the CS1000E, System Manager and Session Manager is presumed to have been previously completed and is not discussed here.

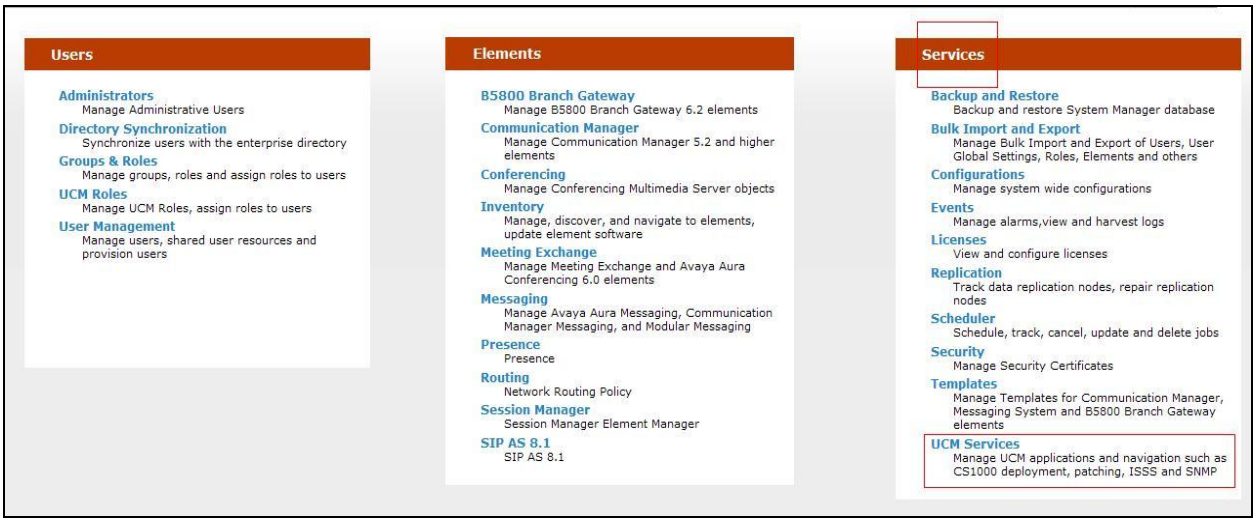
©2012 Avaya Inc. All Rights Reserved.

5.1. Log in to the Avaya Communication Server 1000E

Configuration on the CS1000E will be performed by using both SSH Putty session and Avaya Unified Communications Management GUI.

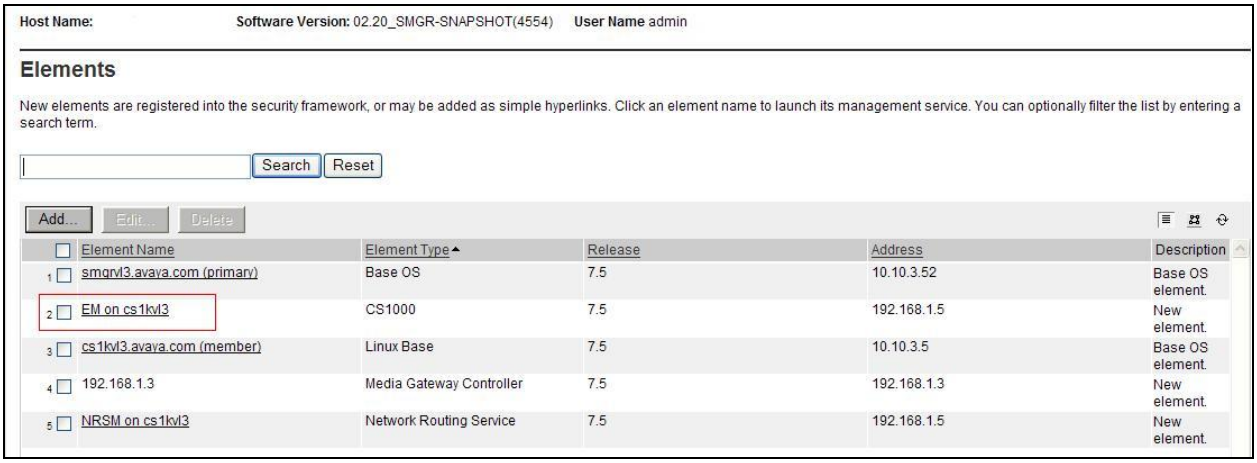
Log in using SSH to the ELAN IP address of the Call Server using a user with correct privileges. Once logged in type **csconsole,** this will take the user into the vxworks shell of the call server. Next type **login**, the user will then be asked to login with correct credentials. Once logged in the user can then progress to load any overlay.

Log in using the web based Avaya Unified Communications Management GUI. The Avaya Unified Communications Management GUI may be launched by accessing the browser-based GUI of System Manager, using the URL https://<ip-address>/SMGR, where <ip-address> is the IP address of System Manager. Log in with the appropriate credentials and click on **Log On** (not shown). Navigate to **Services-> UCM Services** as per thescreenshot below.



©2012 Avaya Inc. All Rights Reserved.

The Avaya Unified Communications Management Elements page will be used for configuration. Click on the Element Name corresponding to CS1000E in the Element Type column. In the abridged screen below, the user would click on the Element Name **EM on cs1kvl3**.



©2012 Avaya Inc. All Rights Reserved.

5.2. Confirm System Features

The keycode installed on the Call Server controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity. Use the CS1000E system terminal and manually load overlay 22 to print the System Limits (the required command is **SLT**), and verify that the number of **SIP Access Ports** reported by the system is sufficient for the combination of trunks to Storms network, and any other SIP trunks needed. See the following screenshot for a typical System Limits printout. The value of **SIP ACCESS PORTS** defines the maximum number of SIP trunks for the CS1000E.

```
System type is - Communication Server 1000E/CPPM Linux
CPPM - Pentium M 1.4 GHz

IPMGs Registered:               1
IPMGs Unregistered:             0
IPMGs Configured/unregistered:  0

TRADITIONAL TELEPHONES 32767    LEFT 32766    USED     1
DECT USERS             32767    LEFT 32767    USED     0
IP USERS               32767    LEFT 32744    USED    23
BASIC IP USERS         32767    LEFT 32766    USED     1
TEMPORARY IP USERS     32767    LEFT 32767    USED     0
DECT VISITOR USER      10000    LEFT 10000    USED     0
ACD AGENTS             32767    LEFT 32752    USED    15
MOBILE EXTENSIONS      32767    LEFT 32767    USED     0
TELEPHONY SERVICES     32767    LEFT 32767    USED     0
CONVERGED MOBILE USERS 32767    LEFT 32767    USED     0
NORTEL SIP LINES       32767    LEFT 32765    USED     2
THIRD PARTY SIP LINES  32767    LEFT 32761    USED     6
SIP CONVERGED DESKTOPS 32767    LEFT 32767    USED     0
SIP CTI TR87           32767    LEFT 32767    USED     0
SIP ACCESS PORTS        2000    LEFT 1970     USED    30
```

Load **overlay 21**, and confirm the customer is setup to use **ISDN** trunks (see below).

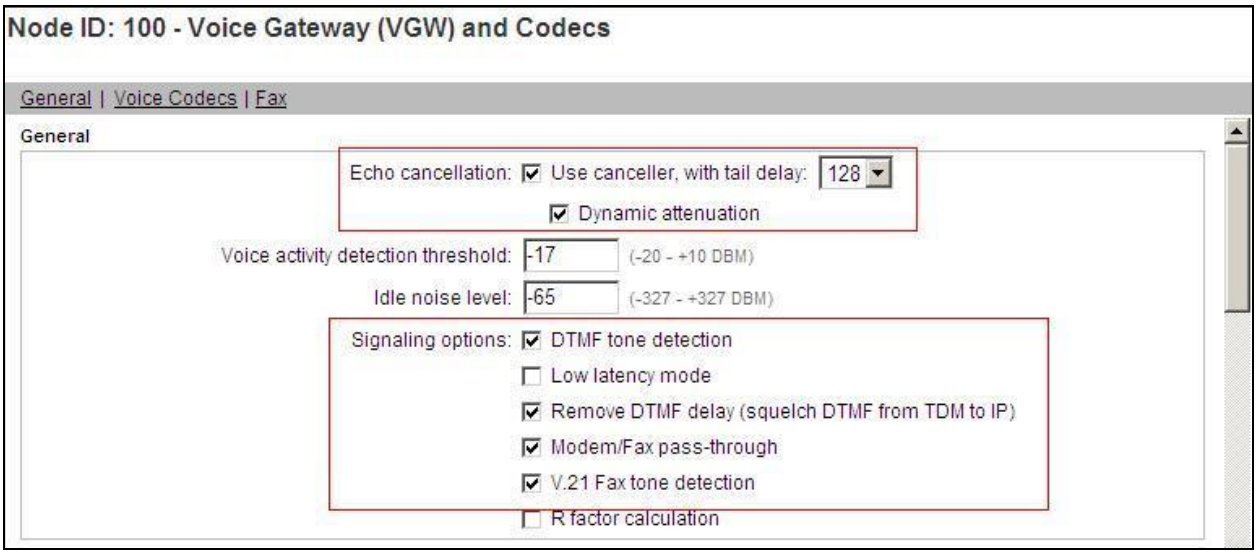
```
REQ: prt
TYPE: net
TYPE NET_DATA
CUST 0

TYPE NET_DATA
CUST 00
OPT RTD
AC1 INTL NPA SPN NXX LOC
AC2
FNP YES
ISDN YES
```

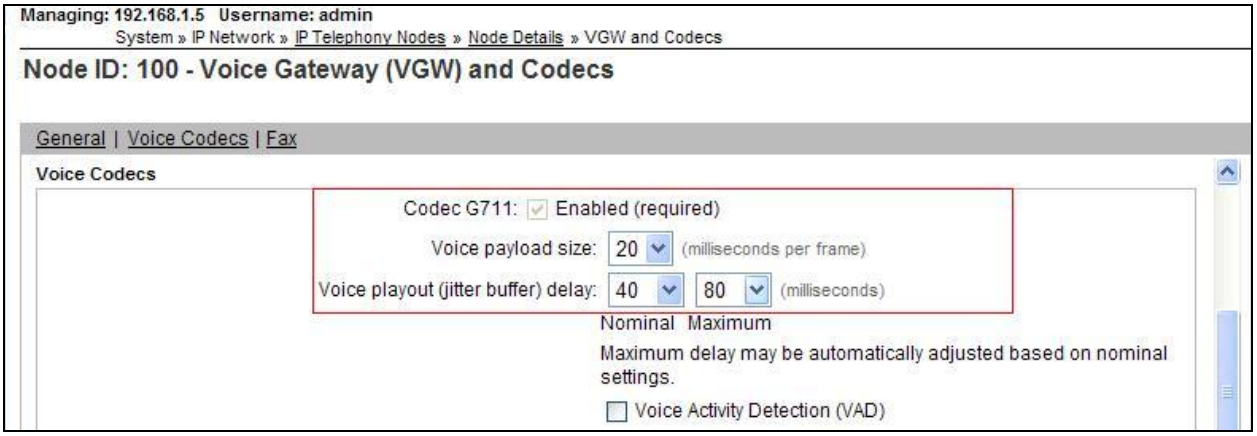

©2012 Avaya Inc. All Rights Reserved.

5.3. Configure Codec's for Voice and FAX Operation

Storms SIP Trunk service supports G.711A and modem pass-through FAX transmissions. Using the CS1000E element manager sidebar, navigate to the **IP Network → IP Telephony Nodes → Node Details → VGW Gateway (VGW) and Codec's** property page and configure the CS1000E General codec settings as in the next screenshot.

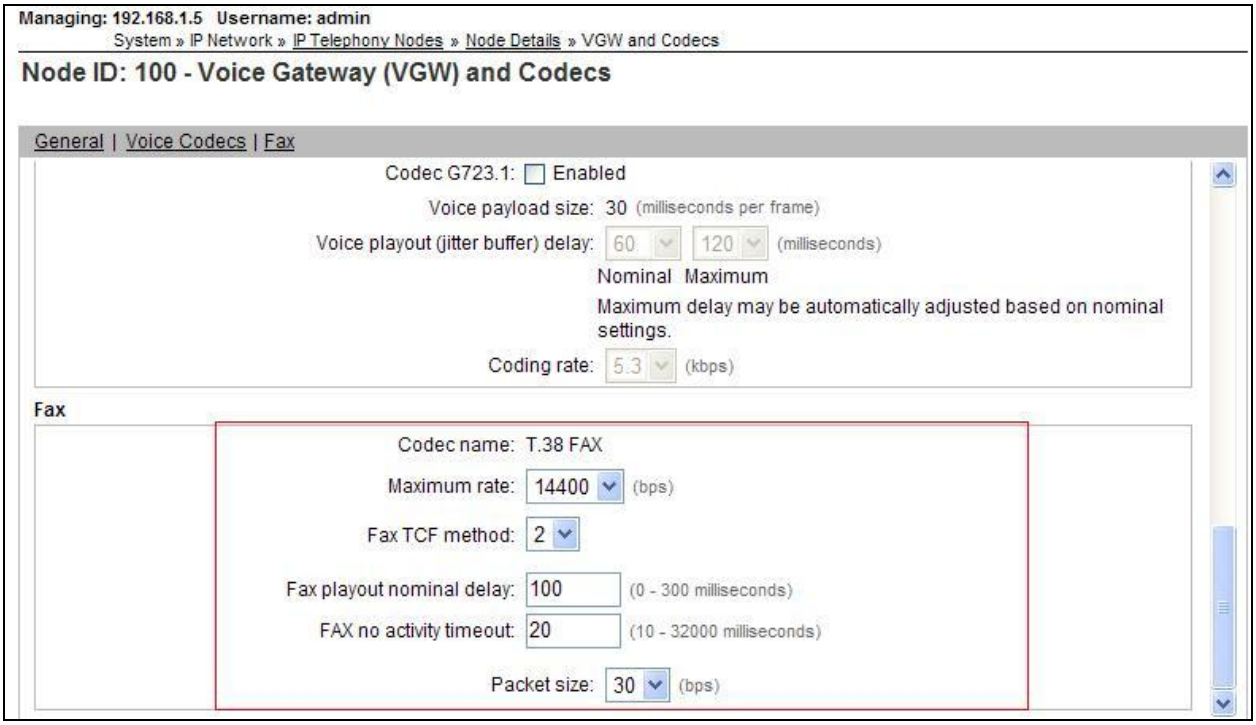


Next, scroll down and configure the **Codec G.711**. The relevant settings are highlighted in the following screenshot.



©2012 Avaya Inc. All Rights Reserved.

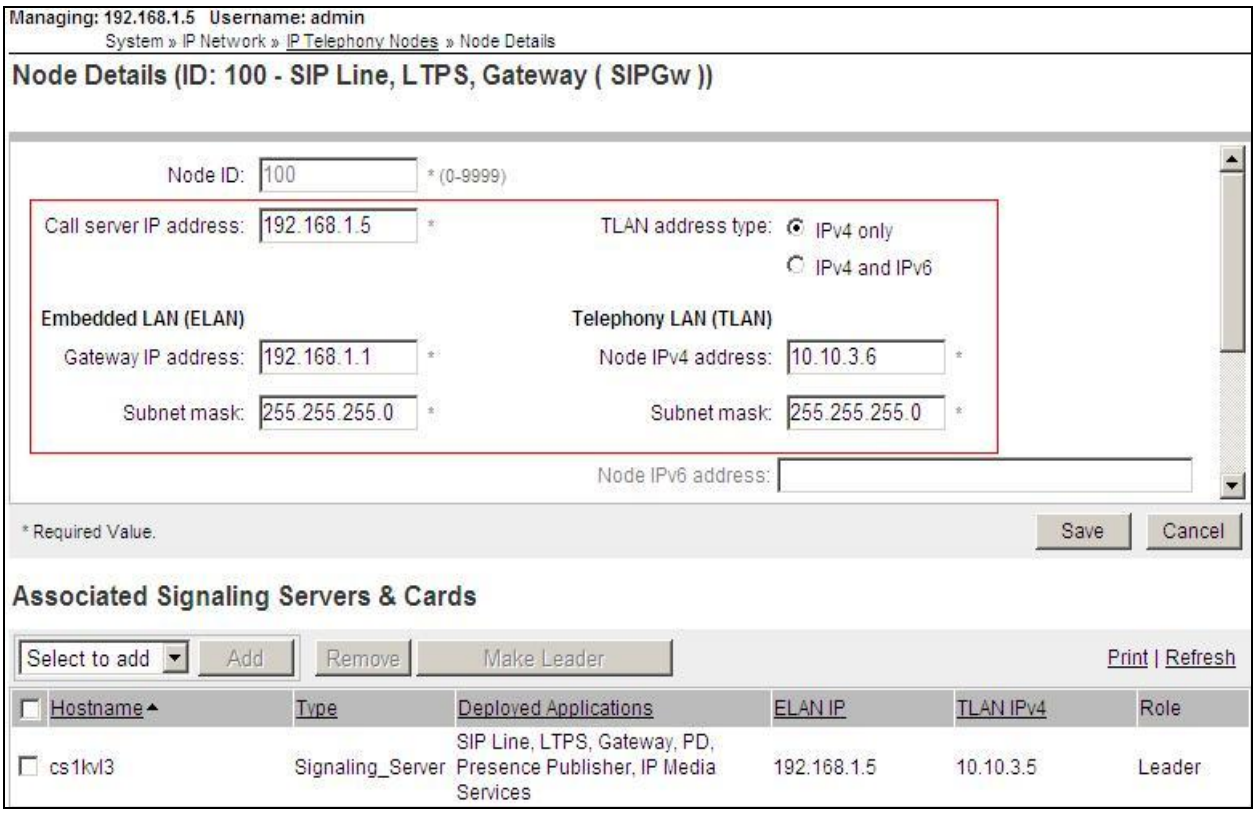
Finally, configure the **Fax** settings as in the highlighted section of the next screenshot.



©2012 Avaya Inc. All Rights Reserved.

5.4. Virtual Trunk Gateway Configuration

Use CS1000E Element Manager to configure the system node properties. Navigate to the **System → IP Networks → IP Telephony Nodes → Node Details** and verify the highlighted section is completed with the correct IP addresses and subnet masks of the Node. At this stage the call server has an IP address and so too does the signalling server. The Node IP is the IP address that the IP phones use to register. This is also where the SIP trunk connection is made to the Session Manager. When an entity link is added in Session Manager for the CS1000E it is the Node IP that is used (please see **Section 6.5** – Define SIP Entities for more details).

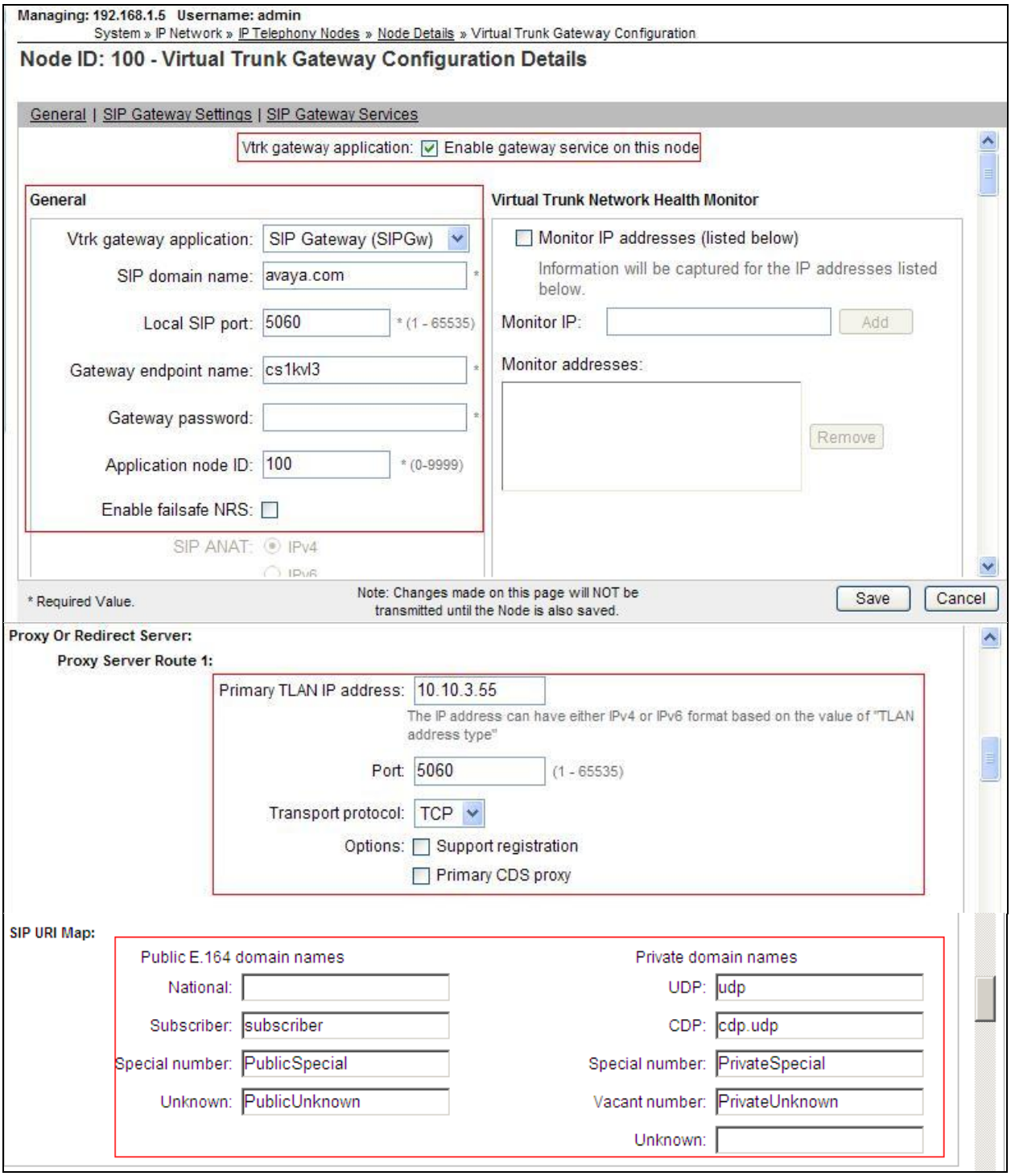


©2012 Avaya Inc. All Rights Reserved.

The next two screenshots show the SIP Virtual Trunk Gateway configuration, navigate to **System → IP Networks → IP Telephony Nodes → Node Details → Gateway (SIPGW) Virtual Trunk Configuration Details** and fill in the highlighted areas with the relevant settings.

- **Vtrk gateway application:** Provides option to select Gateway applications. The three supported modes are **SIP Gateway (SIPGw)**, **H.323Gw**, and **SIPGw.**
- **SIP domain name:** The SIP Domain Name is the SIP Service Domain. The SIP Domain Name configured in the Signaling Server properties must match the Service Domain name configured in the Session Manager
- **Local SIP port:** The Local SIP Port is the port to which the gateway listens. The default value is **5060**
- **Gateway endpoint name:** This field cannot be left blank so a value is needed here. This field is used when a Network Routing Server is used for registration of the endpoint. In this network a Session Manager is used so any value can be put in here and will not be used
- **Application node ID:** This is a unique value that can be alphanumeric and is for the new Node that is being created, in this case **100**
- **Proxy or Redirect Server:** Primary TLAN IP address is the Security Module IP address of the Session Manager. The **Transport protocol** used for **SIP**, in this case is TCP
- **SIP URI Map: Public National** and **Private Unknown** are left blank. All other fields in the SIP URI Map are left with default values.

©2012 Avaya Inc. All Rights Reserved.

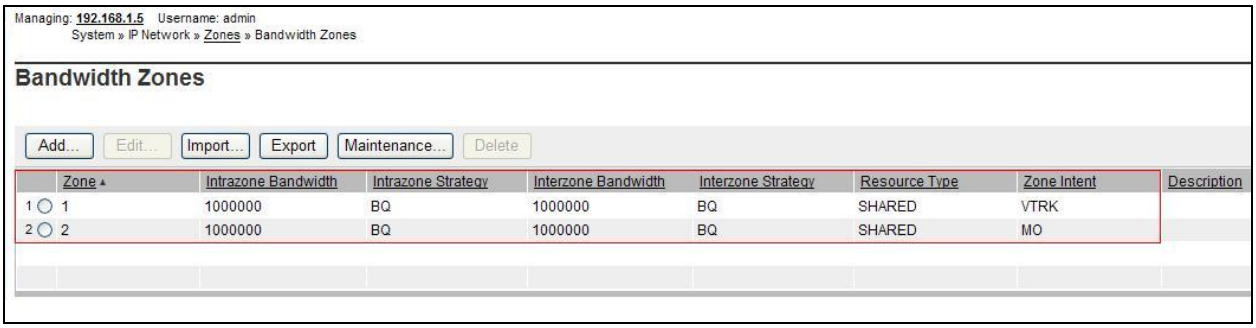


©2012 Avaya Inc. All Rights Reserved.

5.5. Configure Bandwidth Zones

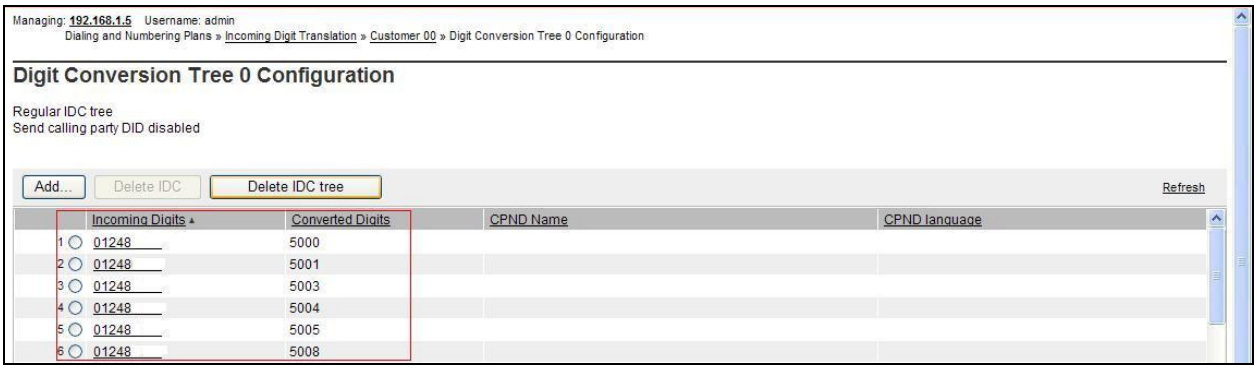
Bandwidth Zones are used for alternate call routing between IP stations and for Bandwidth Management. SIP trunks require a unique zone, not shared with other resources and best practice dictates that IP telephones and Media Gateways are all placed in separate zones. In the sample configuration SIP trunks use zone 1 and IP Telephones use zone 2, system defaults were used for each zone other than the parameter configured for **Zone Intent**. For SIP Trunks (zone 01), **VTRK** is configured for **Zone Intent**. For IP, SIP Telephones (zone 02), **MO** is configured for **Zone Intent**.

Use Element Manager to define bandwidth zones as in the following highlighted example. Use Element Manager and navigate to **System → IP Network → Zones → Bandwidth Zones** and add new zones as required.



5.6. Configure Incoming Digit Conversion Table

A limited number of Direct Dial Inwards (DDI) numbers were available. The IDC table was configured to translate incoming PSTN numbers to five digit local telephone extension numbers. The digits of the actual PSTN DDI number are obscured for security reasons. The following screenshot shows the incoming PSTN numbers converted to local extension numbers. These were altered during testing to map to various SIP, Analog, Digital or Unistim telephones depending on the particular test case being executed.



©2012 Avaya Inc. All Rights Reserved.

5.7. Configure SIP Trunks

CS1000E virtual trunks will be used for all inbound and outbound PSTN calls to Storms SIP Trunk Service. Six separate steps are required to configure CS1000E virtual trunks.

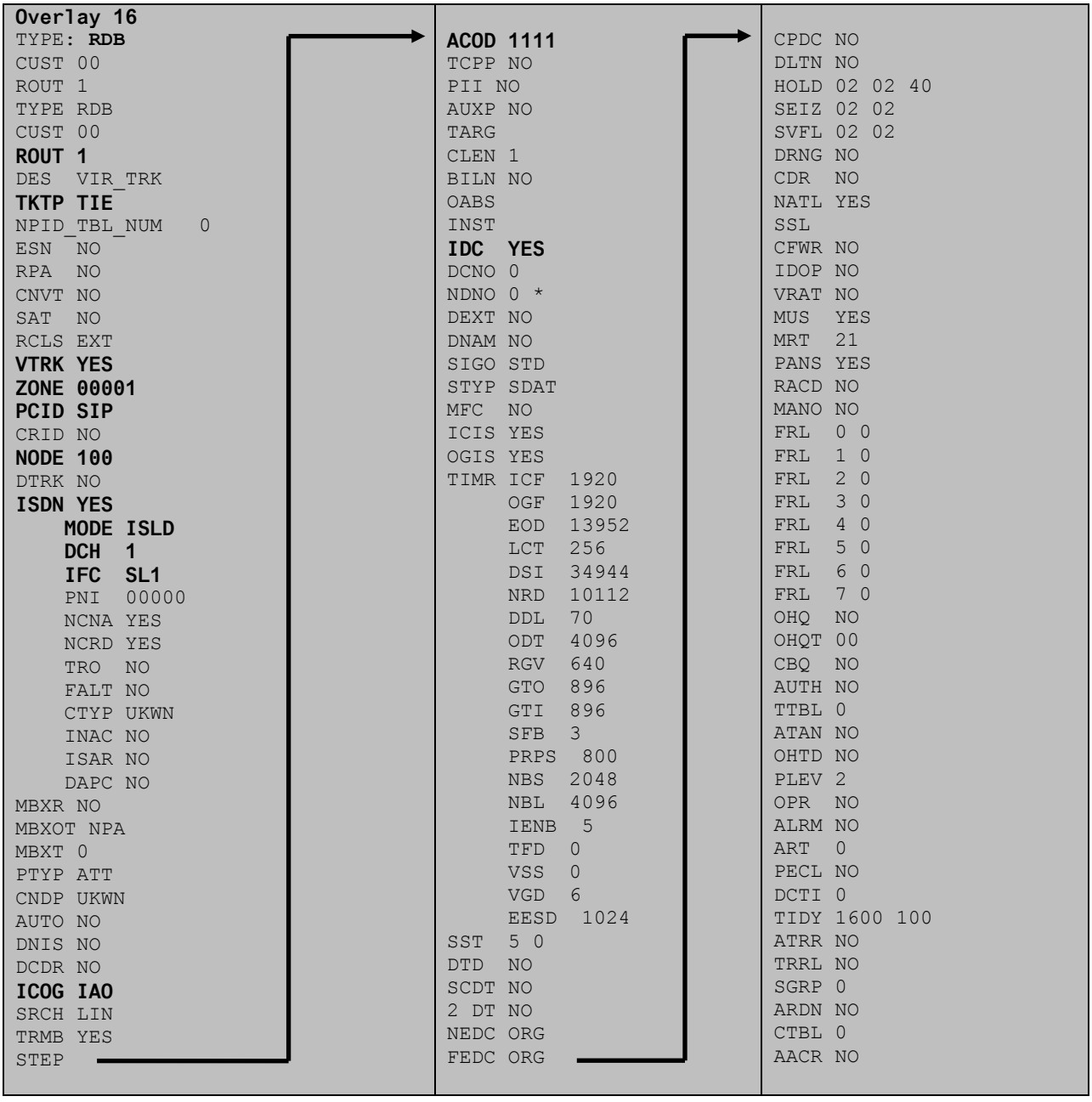
- Configure a D-Channel Handler (**DCH**); configure using the CS1000E system terminal and overlay 17
- Configure a SIP trunk Route Data Block (**RDB**); configure using the CS1000E system terminal and overlay 16
- Configure SIP trunk members; configure using the CS1000E system terminal and overlay 14
- Configure a Digit Manipulation Data Block (**DGT**), configure using the CS1000E system terminal and overlay 86
- Configure a Route List Block (**RLB**); configure using the CS1000E system terminal and overlay 86
- Configure Co-ordinated Dialling Plan(s) (**CDP**); configure using the CS1000E system terminal and overlay 87

The following is an example DCH configuration for SIP trunks. Load **Overlay 17** at the CS1000E system terminal and enter the following values. The highlighted entries are required for correct SIP trunk operation. Exit overlay 17 when completed.

```
Overlay 17
ADAN     DCH 1
  CTYP DCIP
  DES  VIR_TRK
  USR  ISLD
  ISLM 4000
  SSRC 3700
  OTBF 32
  NASA YES
  IFC  SL1
  CNEG 1
  RLS  ID  4
  RCAP ND2
  MBGA NO
  H323
    OVLR NO
    OVLS NO
```


©2012 Avaya Inc. All Rights Reserved.

Next, configure the SIP trunk Route Data Block (RDB) using the CS1000E system terminal and overlay 16. Load **Overlay 16**, enter **RDB** at the prompt, press return and commence configuration. The value for **DCH** is the same as previously entered in overlay 17. The value for **NODE** should match the node value in **Section 5.4**. The value for **ZONE** should match that used in **Section 5.5** for **SIP_VTRK**. The remaining highlighted values are important for correct SIP trunk operation.



©2012 Avaya Inc. All Rights Reserved.

Next, configure virtual trunk members using the CS1000E system terminal and **Overlay 14**. Configure sufficient trunk members to carry both incoming and outgoing PSTN calls. The following example shows a single SIP trunk member configuration. Load **Overlay 14** at the system terminal and type **new X**, where X is the required number of trunks. Continue entering data until the overlay exits. The **RTMB** value is a combination of the **ROUT** value entered in the previous step and the first trunk member (usually 1). The remaining highlighted values are important for correct SIP trunk operation.

```
Overlay 14
TN   100 0 0 0
DATE
PAGE
DES  VIR_TRK
TN   100 0 00 00  VIRTUAL
TYPE IPTI
CDEN 8D
CUST 0
XTRK VTRK
ZONE 00001
TIMP 600
BIMP 600
AUTO_BIMP NO
NMUS NO
TRK  ANLG
NCOS 0
RTMB 1 1
CHID 1
TGAR 1
STRI/STRO IMM IMM
SUPN YES
AST  NO
IAPG 0
CLS  UNR DIP CND ECD WTA LPR APN THFD XREP SPCD MSBT
     P10 NTC
TKID
AACR NO
```


©2012 Avaya Inc. All Rights Reserved.

Next, configure a Digit Manipulation data block (DGT) in overlay 86. Load **Overlay 86** at the system terminal and type **new**. The following example shows the values used. The value for **DMI** is the same as when inputting the **DMI** value during configuration of the Route List Block.

```
Overlay 86
CUST 0
FEAT dgt
DMI  10
DEL  0
ISPN NO
CTYP NPA
```

Configure a Route List Block (RLB) in overlay 86. Load **Overlay 86** at the system terminal and type **new**. The following example shows the values used. The value for **ROUT** is the same as previously entered in overlay 16. The **RLI** value is unique to each RLB.

```
Overlay 86
CUST 0
FEAT rlb
RLI  10
ELC  NO
ENTR 0
LTER NO
ROUT 1
TOD  0 ON  1 ON  2 ON  3 ON
     4 ON  5 ON  6 ON  7 ON
VNS  NO
SCNV NO
CNV  NO
EXP  NO
FRL  0
DMI  10
CTBL 0
ISDM 0
```

```
FCI  0
FSNI 0
BNE  NO
DORG NO
SBOC NRR
PROU 1
IDBB DBD
IOHQ NO
OHQ  NO
CBQ  NO

ISET 0
NALT 5
MFRL 0
OVLL 0
```

Next, configure Co-ordinated Dialling Plan(s) (CDP) which users will dial to reach PSTN numbers. Use the CS1000E system terminal and **Overlay 87**. The following are some example CDP entries used. The highlighted **RLI** value previously configured in overlay 86 is used as the Route List Index (**RLI**), this is the default PSTN route to the SIP Trunk service.

```
TSC  00353
FLEN 0
RRPA NO
RLI  10
CCBA NO
```

```
TSC  18
FLEN 0
RRPA NO
RLI  10
CCBA NO
```

```
TSC  800
FLEN 0
RRPA NO
RLI  10
CCBA NO
```

```
TSC  08
FLEN 0
RRPA NO
RLI  10
CCBA NO
```


©2012 Avaya Inc. All Rights Reserved.

5.8. Configure Analog, Digital and IP Telephones

A variety of telephone types were used during the testing, the following is the configuration for the Avaya 1140e Unistim IP telephone. Load **Overlay 20** at the system terminal and enter the following values. A unique four digit number is entered for the **KEY 00** and **KEY 01** value. The value for **CFG_ZONE** is the same value used in **Section 5.5** for **VIRTUALSETS**.

```
Overlay 20 IP Telephone configuration
DES  1140
TN   100 0 01 0  VIRTUAL
TYPE 1140
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00002
CUR_ZONE 00002
ERL  0
ECL  0
FDN  0
TGAR 0
LDN  NO
NCOS 0
SGRP 0
RNPG 1
SCI  0
SSU
LNRS 16
XLST
SCPW
SFLT NO
CAC_MFC 0
CLS  UNR FBA WTA LPR PUA MTD FNA HTA TDD HFA CRPD
     MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
     POD SLKD CCSD SWD LNA CNDA
     CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBD
     ICDA CDMD LLCN MCTD CLBD AUTR
     GPUD DPUD DNDA CFXA ARHD FITD CLTD ASCD
     CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
     UDI RCC HBTA AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
     DRDD EXR0
     USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
     FDSD NOVD VOLA VOUD CDMR PRED RECA MCDD T87D SBMD KEM3 MSNV FRA  PKCH MUTA MWTD

---continued on next page----
```


©2012 Avaya Inc. All Rights Reserved.

```
---continued from previous page----

DVLD CROD CROD
CPND_LANG ENG
RCO  0
HUNT 0
LHK  0
PLEV 02
PUID
DANI NO
AST  00
IAPG 1
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY  00 MCR 5000 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME IP1140
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     01 MCR 5000 0
        CPND
          CPND_LANG ROMAN
            NAME IP1140
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     02
     03 BSY
     04 DSP
     05
     06
     07
     08
     09
     10
     11
     12
     13
     14
     15
     16
     17 TRN
     18 AO6
     19 CFW 16
     20 RGA
     21 PRK
     22 RNP
     23
     24 PRS
     25 CHG
     26 CPN
```


©2012 Avaya Inc. All Rights Reserved.

Digital telephones are configured using the **Overlay 20**, the following is a sample **3904** digital set configuration. Again, a unique number is entered for the **KEY 00** and **KEY 01** value.

```
Overlay 20 - Digital Set configuration
TYPE: 3904
DES  3904
TN   04 0 02 00  VIRTUAL
TYPE 3904
CDEN 8D
CTYP XDLC
CUST 0
MRT
ERL  0
FDN  0
TGAR 0
LDN  NO
NCOS 0
SGRP 0
RNPG 1
SCI  0
SSU
LNRS 16
XLST
SCPW
SFLT NO
CAC_MFC 0
CLS  UNR FBD WTA LPR PUA MTD FND HTD TDD HFA GRLD CRPA STSD
     MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
     POD SLKD CCSD SWD LNA CNDA
     CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBD
     ICDA CDMA LLCN MCTD CLBD AUTU
     GPUD DPUD DNDA CFXA ARHD FITD CNTD CLTD ASCD
     CPFA CPTA ABDA CFHD FICD NAID BUZZ AGRD MOAD
     UDI RCC HBTD AHA IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
     DRDD EXR0
     USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
     FDSD NOVD CDMR PRED RECA MCDD T87D SBMD PKCH CROD CROD
CPND_LANG ENG
RCO  0
HUNT
PLEV 02
PUID
DANI NO
SPID NONE
AST
IAPG 1
AACS
ACQ
ASID
SFNB
SFRB
USFB
CALB
FCTB
ITNA NO
DGRP
PRI  01
MLWU_LANG 0

---continued on next page----
```


©2012 Avaya Inc. All Rights Reserved.

```
---continued from previous page----

MLNG ENG
DNDR 0
KEY  00 MCR 5008 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME Digital Set
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     01 MCR 5008 0
        CPND
          CPND_LANG ROMAN
            NAME Digital Set
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     02
     03
     04
     05
     06
     07
     08
     09
     10
     11
     12
     13
     14
     15
     16
     17 TRN
     18 AO6
     19 CFW 16
     20 RGA
     21 PRK
     22 RNP
     23
     24 PRS
     25 CHG
     26 CPN
     27 CLT
     28 RLT
     29
     30
     31
```


©2012 Avaya Inc. All Rights Reserved.

Analog telephones are also configured using **Overlay 20**, the following example shows an analog port configured for Plain Ordinary Telephone Service (POTS) and also configured to allow pass through fax transmission. A unique value is entered for **DN**, this is the extension number. **DTN** is required if the telephone uses DTMF dialing. Values **FAXD** and **MPTA** configure the port for pass through fax transmissions.

```
Overlay 20 - Analog Telephone Configuration
DES  500
TN   04 0 03 00
TYPE 500
CDEN 4D
CUST 0
MRT

ERL 00000
WRLS NO
DN   5015
AST  NO
IAPG 0
HUNT
TGAR 0
LDN  NO
NCOS 0
SGRP 0
RNPG 0
XLST
SCI  0
SCPW
SFLT NO
CAC_MFC 0
CLS  UNR DTN FBD XFD WTA THFD FND HTD ONS
     LPR XRD AGRD CWD SWD MWD RMMD SMWD LPD XHD SLKD CCSD LND TVD
     CFTD SFD MRD C6D CNID CLBD AUTU
     ICDD CDMD LLCN EHTD MCTD
     GPUD DPUD CFXD ARHD OVDD AGTD CLTD LDTD ASCD SDND
     MBXD CPFA CPTA UDI RCC HBTD IRGD  DDGA NAMA MIND
     NRWD NRCD NROD SPKD CRD PRSD MCRD
     EXR0 SHL SMSD ABDD CFHD DNDY DNO3
     CWND USMD USRD CCBD BNRD OCBD RTDD RBDD RBHD FAXD CNUD CNAD PGND FTTC
     FDSD NOVD CDMR PRED MCDD T87D SBMD PKCH MPTA
PLEV 02
PUID
AACS NO
MLWU_LANG 0
FTR  DCFW 4
```


©2012 Avaya Inc. All Rights Reserved.

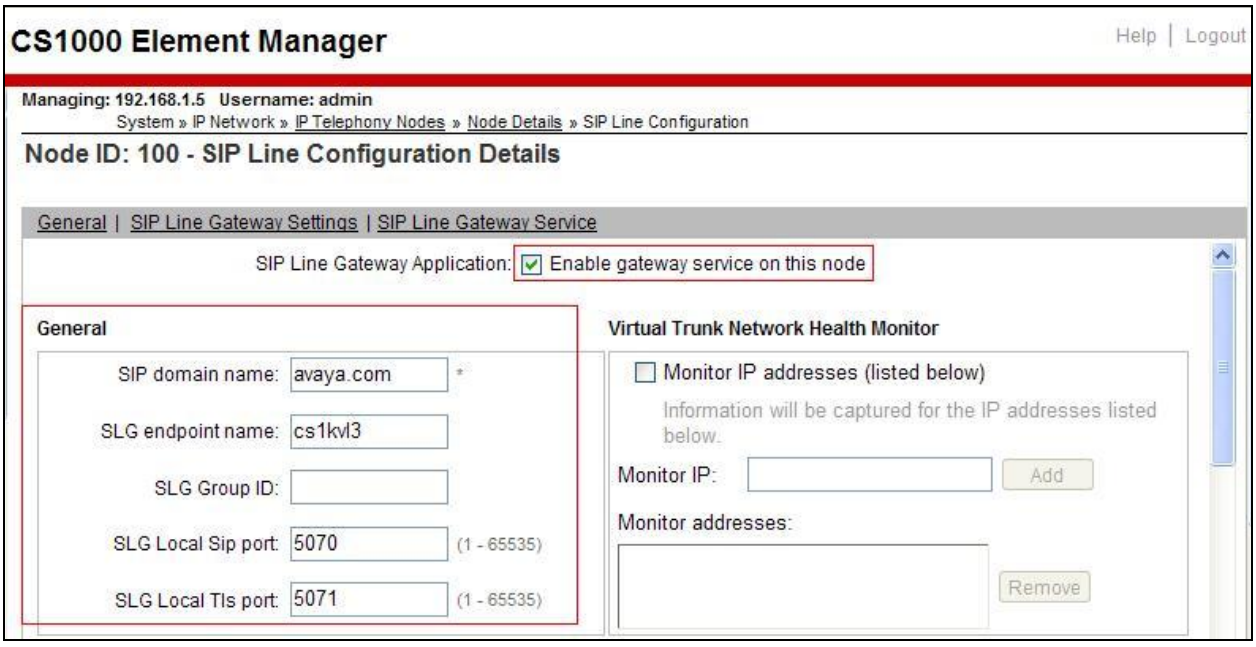
5.9. Configure the SIP Line Gateway Service

SIP terminal operation requires the Communication Server node to be configured as a SIP Line Gateway (SLG) before SIP telephones can be configured. Prior to configuring the SIP Line node properties, the SIP Line service must be enabled in the customer data block. Use the CS1000E system terminal and **Overlay 15** to activate SIP Line services, as in the following example where **SIPL_ON** is set to **YES**.

```
SLS_DATA
  SIPL_ON YES
  UAPR 11
  NMME NO
```

If a numerical value is entered against the **UAPR** setting, this number will be pre appended to all SIP Line configurations, and is used internally in the SIP Line server to track SIP terminals. Use Element Manager and navigate to the **IP Network → IP Telephony Nodes → Node Details → SIP Line Gateway Configuration** page. See the following screenshot for highlighted critical parameters.

- **SIP Line Gateway Application:** Enable the SIP line service on the node, check the box to enable
- **SIP Domain Name:** The value must match that configured in **Section 6.2**
- **SLG endpoint name:** The endpoint name is the same endpoint name as the SIP Line Gateway and will be used for SIP gateway registration
- **SLG Local Sip port:** Default value is **5070**
- **SLG Local TLS port:** Default value is **5071**



©2012 Avaya Inc. All Rights Reserved.

5.10. Configure SIP Line Telephones

When SIP Line service configuration is completed, use the CS1000E system terminal and **Overlay 20** to add a Universal Extension (UEXT). See the following example of a SIP Line extension. The value for **UXTY** must be **SIPL**. This example is for an Avaya SIP telephone, so the value for **SIPN** is 1. The **SIPU** value is the username, **SCPW** is the logon password and these values are required to register the SIP telephone to the SLG. The value for **CFG_ZONE** is the value set for **SIPLINEZONE** in **Section 5.5**. A unique telephone number is entered for value **KEY 00**. The value for **KEY 01** is comprised of the **UAPR** (set in **Section 5.8**) value and the telephone number used in **KEY 00**.

```
Overlay 20 – SIP Telephone Configuration
DES  SIPD
TN   100 0 01 10  VIRTUAL
TYPE UEXT
CDEN 8D
CTYP XDLC
CUST 0
UXTY SIPL
MCCL YES
SIPN 1
SIP3 0
FMCL 0
TLSV 0
SIPU 5003
NDID 100
SUPR NO
SUBR DFLT MWI RGA CWI MSB
UXID
NUID 100
NHTN 100 0 01 10
CFG_ZONE 00002
CUR_ZONE 00002
ERL  0
ECL  0
VSIT NO
FDN
TGAR 0
LDN  NO
NCOS 0
SGRP 0
RNPG 0
SCI  0
SSU
XLST
SCPW 1234
SFLT NO
CAC_MFC 0
CLS  UNR FBD WTA LPR MTD FNA HTA TDD HFD CRPD
     MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
     POD SLKD CCSD SWD LND CNDA
     CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBD
     ICDD CDMD LLCN MCTD CLBD AUTU
     GPUD DPUD DNDA CFXA ARHD FITD CLTD ASCD
     CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD

---continued on next page---
```


©2012 Avaya Inc. All Rights Reserved.

```
---continued from previous page---

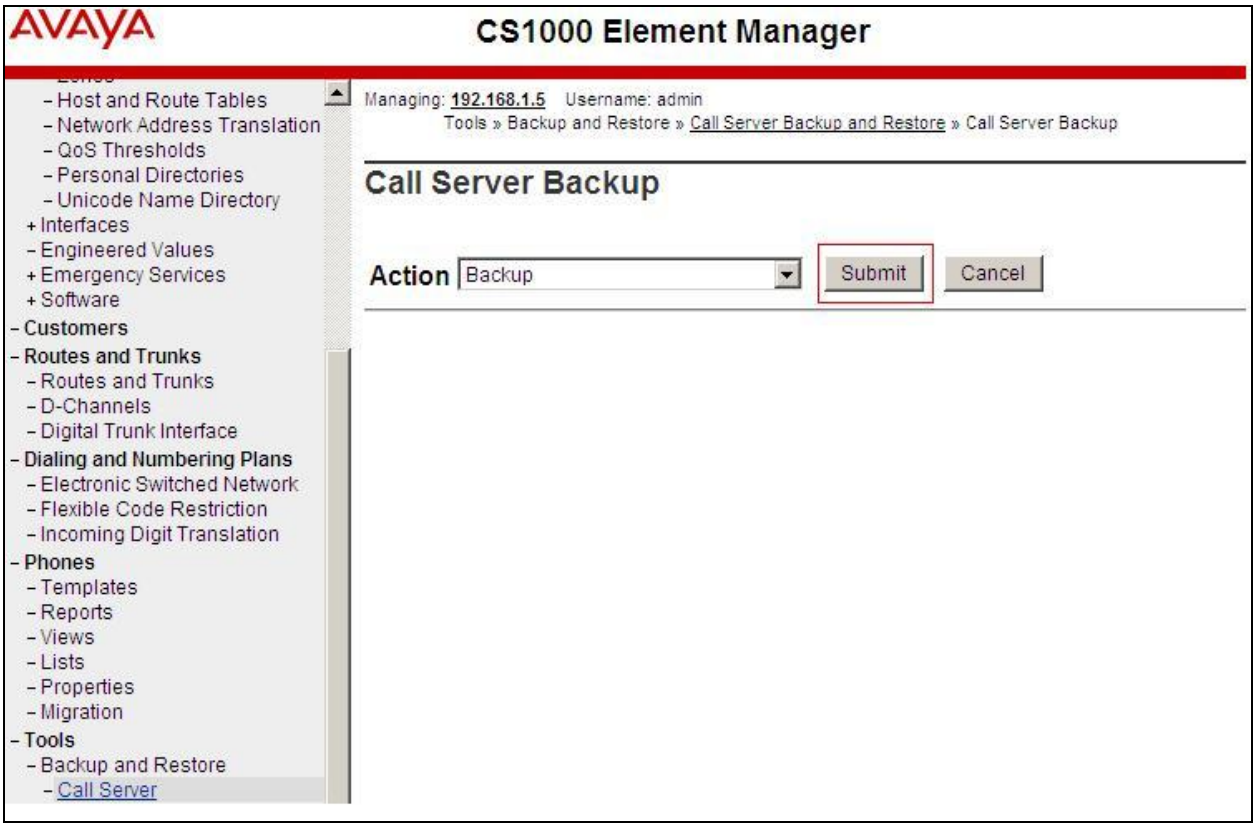
     UDI RCC HBTD AHA IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
     DRDD EXR0
     USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
     FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD ELMD MSNV FRA  PKCH MWTD DVLD
CROD CROD
CPND_LANG ENG
RCO  0
HUNT
LHK  0
PLEV 02
PUID
DANI NO
AST
IAPG 0 *

AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY  00 SCR 5003 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME Sigma 1140
            XPLN 11
            DISPLAY_FMT FIRST,LAST*
     01 HOT U 115003 MARP 0
     02
     03
     04
     05
     06
     07
     08
     09
     10
     11
     12
     13
     14
     15
     16
     17 TRN
     18 AO6
     19 CFW 16
     20 RGA
     21 PRK
     22 RNP
     23     *
     24 PRS
     25 CHG
     26 CPN
     27
     28
     29
     30
     31
```


©2012 Avaya Inc. All Rights Reserved.

5.11. Save Configuration

Expand **Tools → Backup and Restore** on the left navigation panel and select **Call Server.** Select **Backup** and click **Submit** to save configuration changes as shown below.



Backup process will take several minutes to complete. Scroll to the bottom of the page to verify the backup process completed successfully as shown below.



Configuration of CS1000E is complete.

©2012 Avaya Inc. All Rights Reserved.

6. Configure Avaya Aura® Session Manager

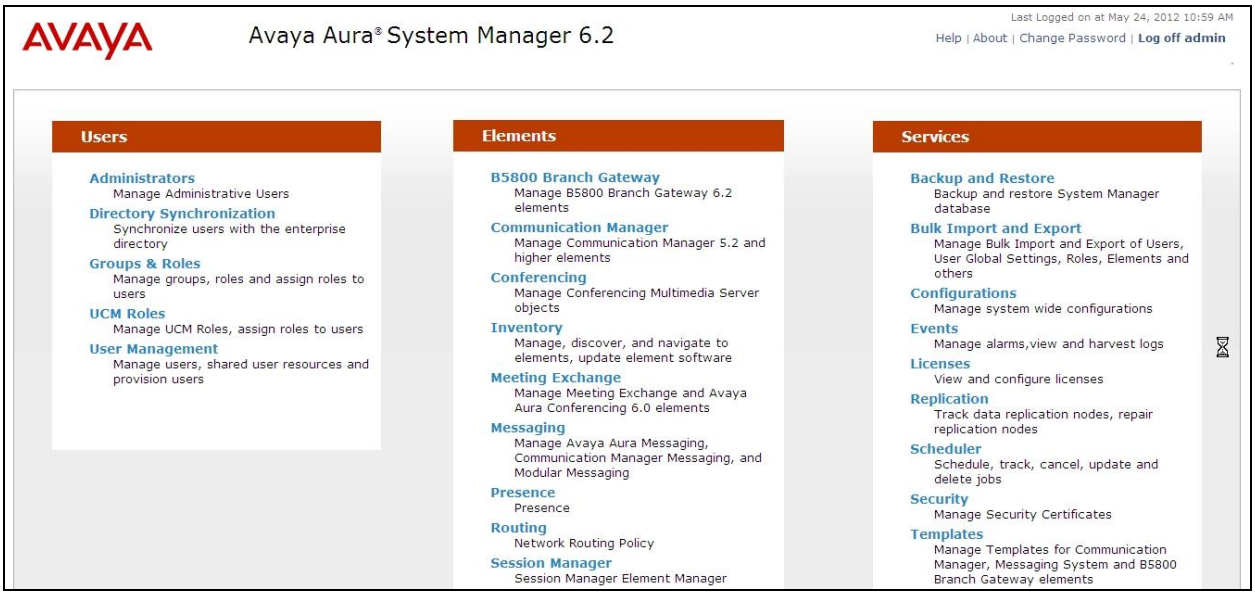
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- SIP Entities corresponding to CS1000E, Avaya SBCE and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Session Manager Instance, corresponding to the Session Manager server to be administered in System Manager

It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

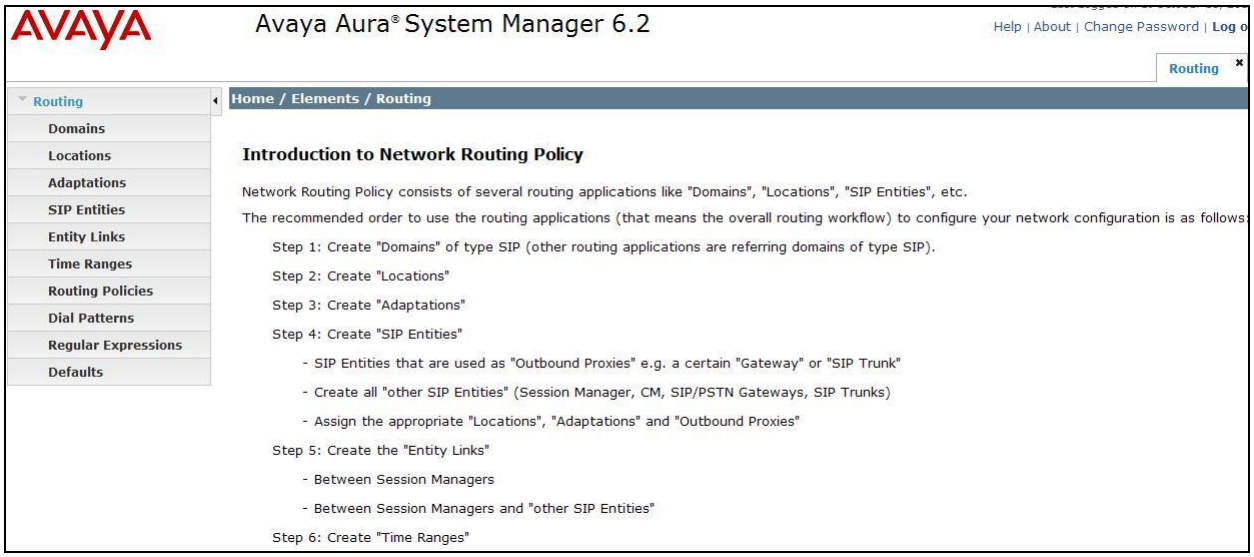
6.1. Avaya Aura® System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL https://<ip-address>/SMGR, where <ip-address> is the IP address of System Manager. Log in with the appropriate credentials and click on **Log On** (not shown). The screen shown below is then displayed.



©2012 Avaya Inc. All Rights Reserved.

Most of the configuration items are performed in the Routing Element. Click on **Routing** in the Elements column shown above to bring up the Introduction to Network Routing Policy screen.

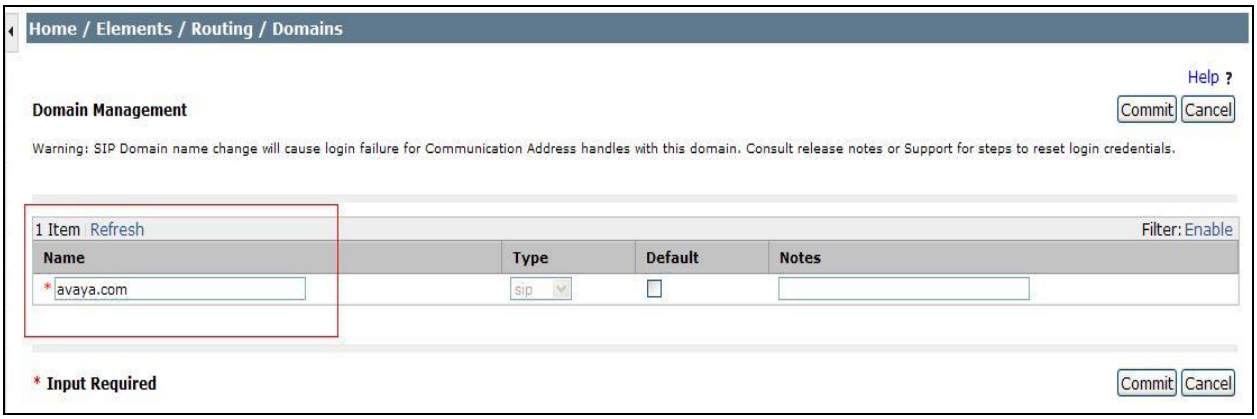


6.2. Define SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. Expand **Elements → Routing** and select **Domains** from the left navigation menu, click **New** (not shown)**.** Enter the following values and use default values for remaining fields**.**

- **Name** Enter the Domain Name specified for the SIP Gateway in **Section 5.4.** In the sample configuration, **avaya.com** was used
- **Type** Verify **SIP** is selected
- **Notes** Add a brief description [Optional]

Click **Commit** to save. The screen below shows the SIP Domain defined for the sample configuration.



©2012 Avaya Inc. All Rights Reserved.

6.3. Define Location for Avaya Communication Server 1000E

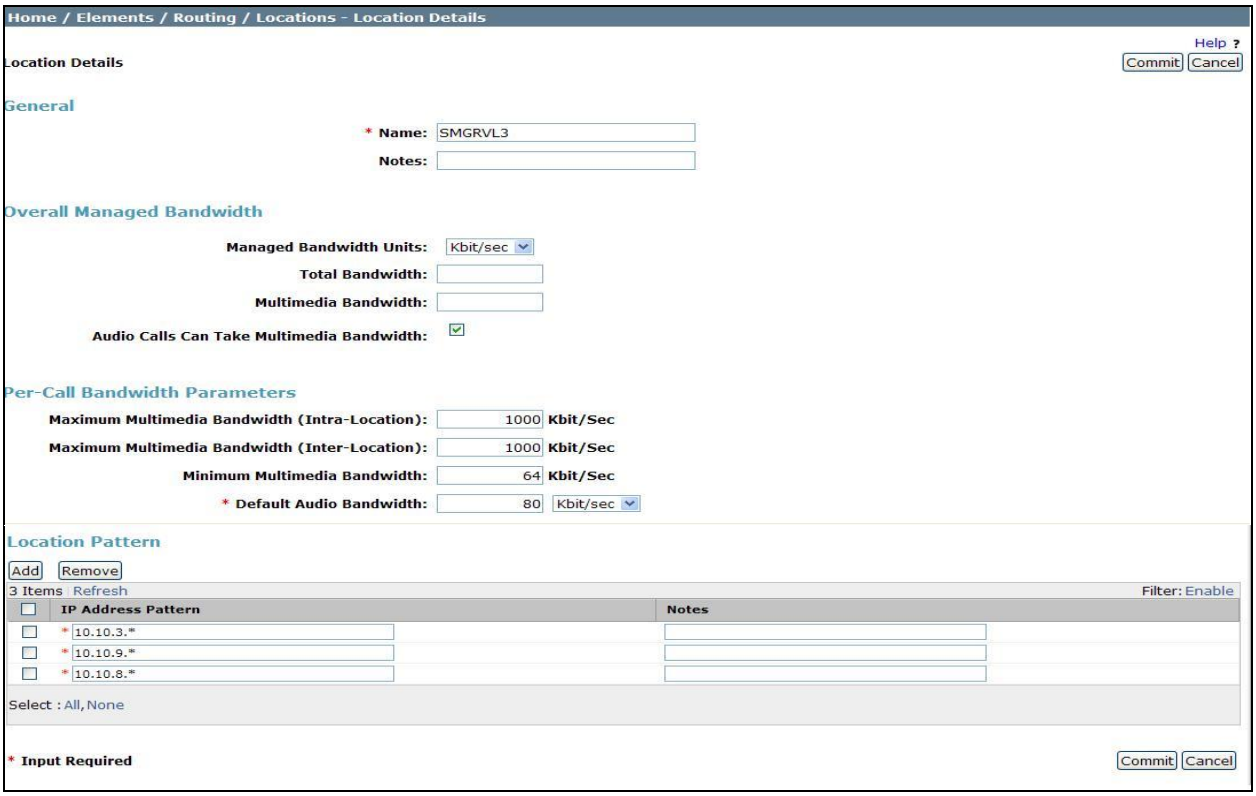
Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing →Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown).In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name for the location
- **Notes:** Add a brief description (optional)

The Location Pattern is used to identify call routing based on IP address. Session Manager matches the IP address against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern then Session Manager uses the location administered for the SIP Entity.
In the **Location Pattern** section, click **Add** and enter the following values.

- **IP Address Pattern** Enter the logical pattern used to identify the location. For the sample configuration, **10.10.3.*** was used
- **Notes** Add a brief description [Optional]

Click **Commit** to save. The screenshot below shows the Location defined for CS1000E in the sample configuration.



©2012 Avaya Inc. All Rights Reserved.

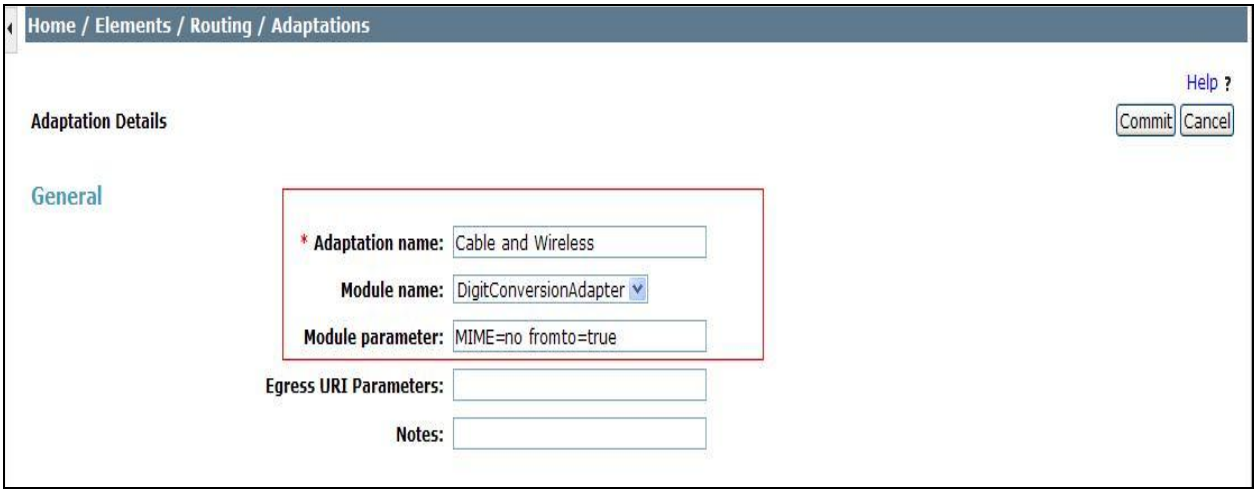
6.4. Configure Adaptation Module

Adaptations can be used to modify the called and calling party numbers to meet the requirements of the service. The called party number present in the SIP INVITE Request URI is modified by the **Digit Conversion** in the Adaptation. Additionally, the called and calling party numbers can also be modified using **Digit Conversion** when **fromto=true** is entered in the **Module Parameters**. The example shown was used in test to convert the called numbers in the Request URI to E.164 format with leading zero according to the standard used by Storm. In addition, the To header is converted to the same format to be consistent with the calling party numbers in the From header.

DigitConversionAdaptor is used and leading zeros are analyzed. Both national and international numbers are converted with national numbers requiring the prefixing of the country code. The two leading zeros of the international number are removed and replaced with a "+".These rules are applied to the destination addresses.

Expand **Elements → Routing** and select **Adaptations** from the left navigational menu. Click **New (**not shown**).** In the **General** section, enter the following values and use default values for remaining fields**.**

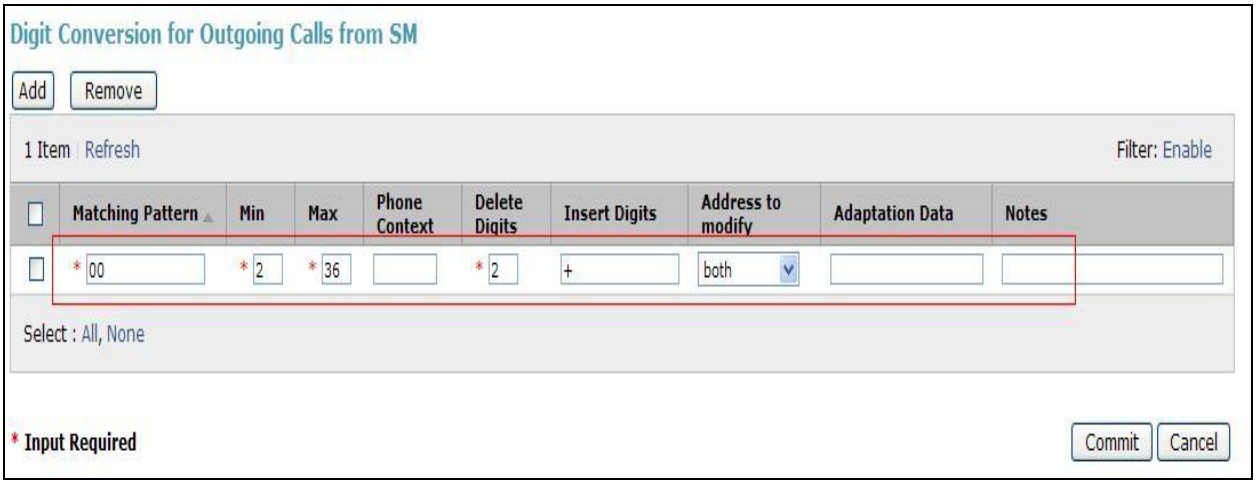
- **Adaptation Name** Enter an identifier for the Adaptation Module. This adaptation is applied to the Avaya SBCE SIP entity in **Section 6.5**
- **Module Name** Select **DigitConversonAdaptor** from drop-down menu
- **Module parameter** **MIME =no** Strips MIME message bodies on egress from Session Manager
  fromto=true →Modifies from and to headers of a message



©2012 Avaya Inc. All Rights Reserved.

In the **Digit Conversion for Incoming Calls to SM** section, click **Add** and enter the following values.

- **Matching Pattern** Enter dialed prefix for calls to SIP endpoints registered to Session Manager
- **Min** Enter minimum number of digits that must be dialed
- **Max** Enter maximum number of digits that may be dialed
- **Delete Digits** Enter number of digits that may be deleted
- **Address to modify** Select **both**



©2012 Avaya Inc. All Rights Reserved.

6.5. Define 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 **SIP Entities** on the left panel menu and then click on the **New** button (not shown). The following will need to be entered for each SIP Entity. Under **General:**

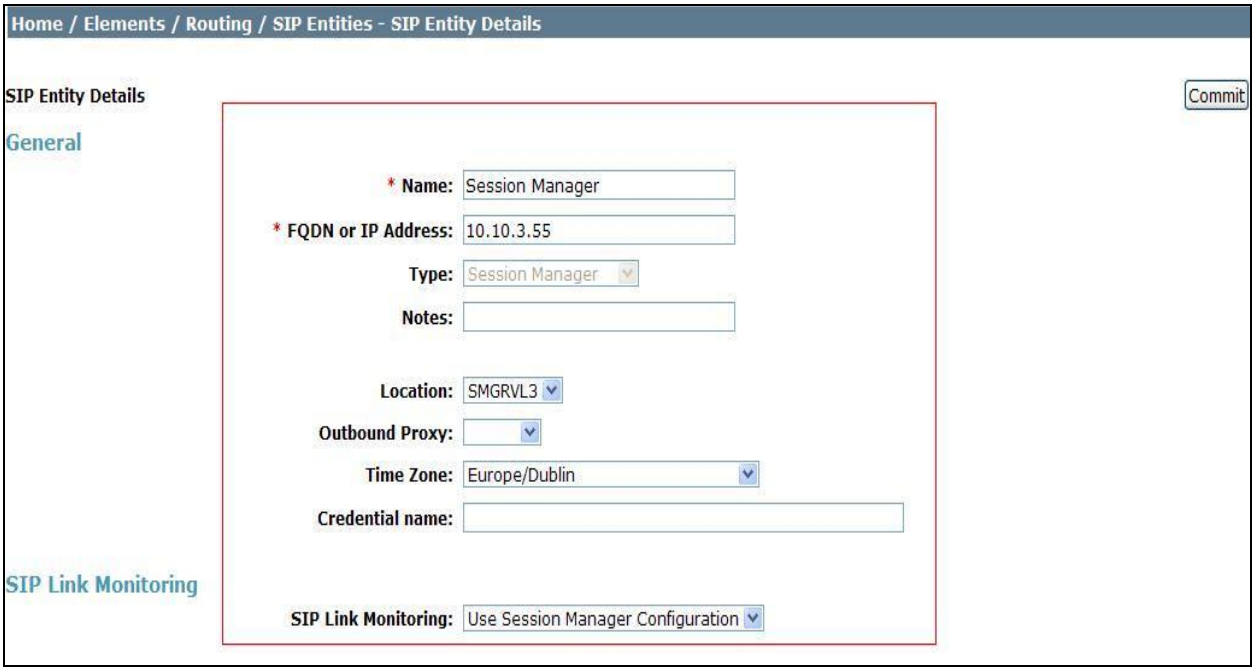
- In the **Name** field enter an informative name
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signaling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **Other** for a CS1000E SIP entity and **Gateway** for the Avaya SBCE SIP entity
- In the **Adaptation** field select the appropriate adaptation defined in **Section 6.4**, in test **Cable & Wireless** was selected for the Avaya SBCE to convert called party numbers to E.164 format with a leading "+"
- In the **Location** field select the appropriate location from the drop down menu
- In the **Time Zone** field enter the time zone for the SIP Entity

In this configuration there are three SIP Entities.

- Session Manager SIP Entity
- CS1000E SIP Entity
- Avaya Session Border Controller SIP Entity

6.5.1. Avaya Aura® Session Manager SIP Entity

The following screens show the SIP entity for Session Manager. The **FQDN or IP Address** field is set to the IP address of the Session Manager SIP signaling interface.

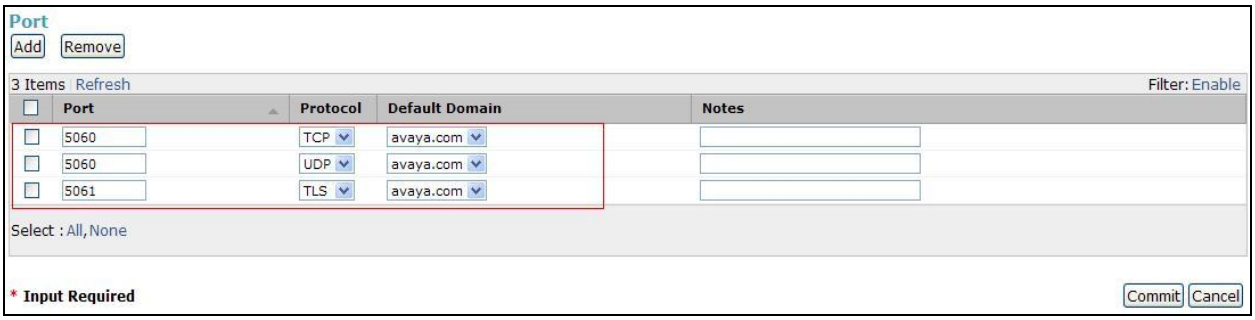


©2012 Avaya Inc. All Rights Reserved.

The Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **Port**, click **Add,** then edit the fields in the resulting new row

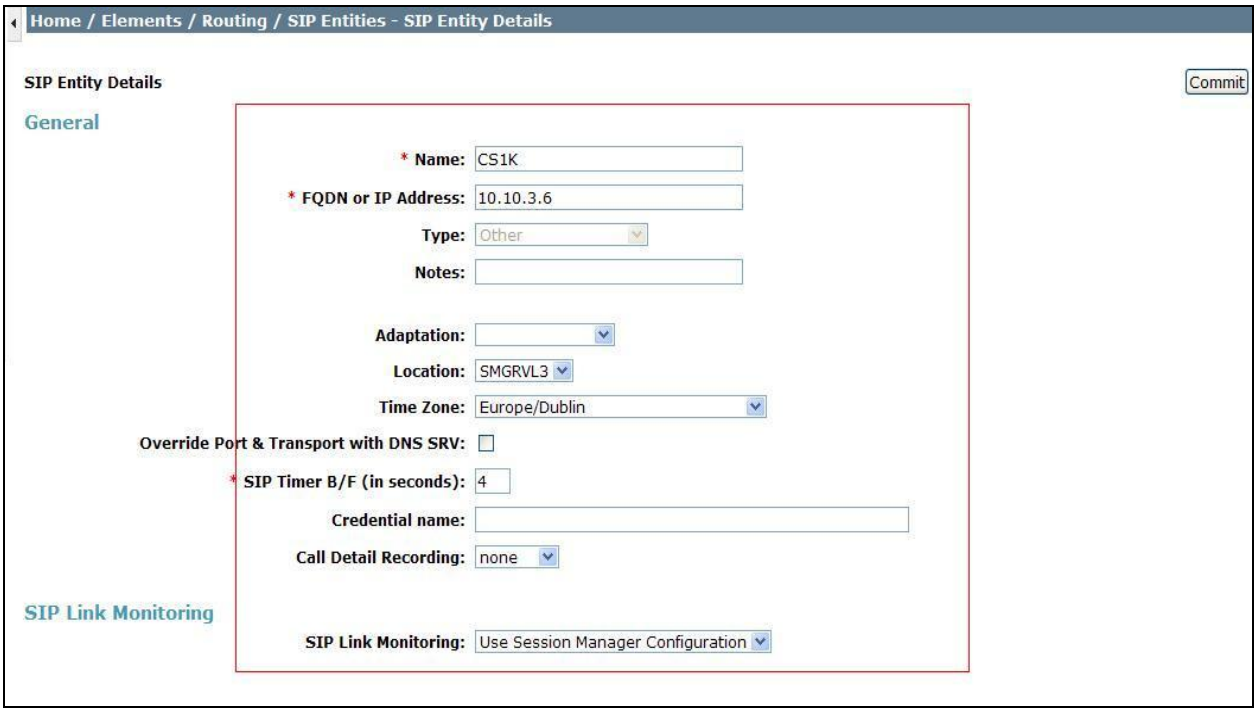
- In the **Port** field enter the port number on which the system listens for SIP requests
- In the **Protocol** field enter the transport protocol to be used for SIP requests
- In the **Default Domain** field, from the drop down menu select **avaya.com** as the default domain

For the compliance test, three **Port** entries were added. Although TLS was added for completeness, only the TCP and UDP ports were used by Session Manger in the reference configuration



6.5.2. Avaya Aura® Communication Server 10000E SIP Entity

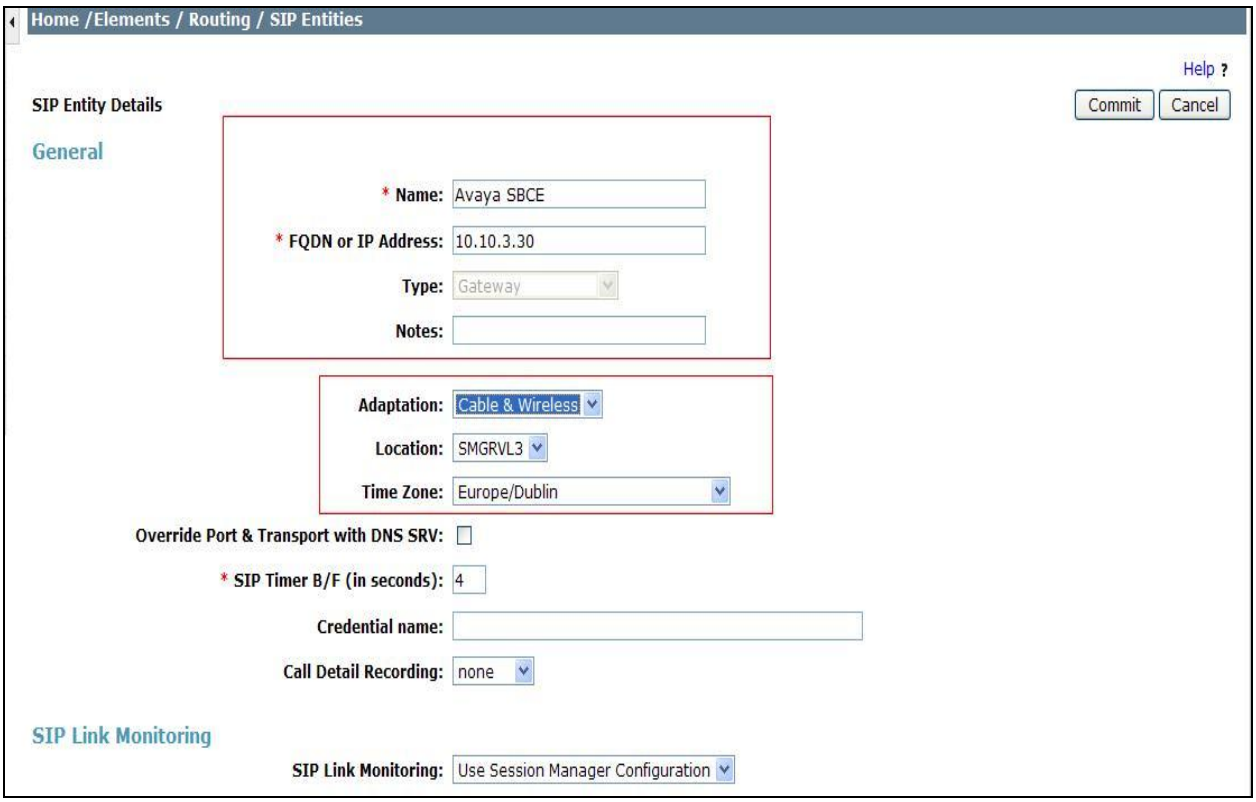
The following screens show the SIP entity for CS1000E. The **FQDN or IP Address** field is set to the TLAN Node IP address defined in **Section 5.4**. The entity **Type** is set to **Other**.



©2012 Avaya Inc. All Rights Reserved.

6.5.3. Avaya Session Border Controller for Enterprise SIP Entities

The following screen shows the SIP entity for the Avaya Session Border Controller for Enterprise used for routing calls. The **FQDN or IP Address** field is set to the IP address of the private interfaces administered in **Section 7** of this document. The Adaptation defined in **Section 6.4** is applied to the Avaya SBCE SIP entity.



©2012 Avaya Inc. All Rights Reserved.

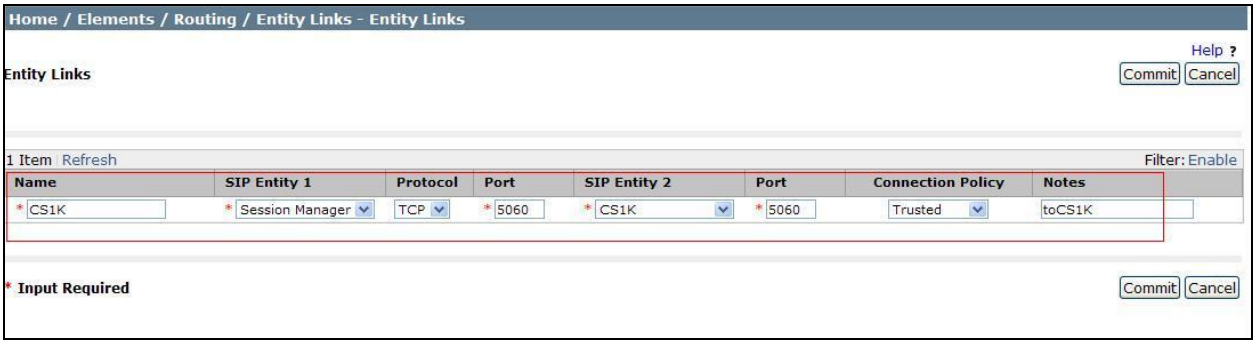
6.6. Define Entity Links

A SIP trunk between Session Manager and a telephony system is described as an Entity Link. Two Entity Links were created; one to CS1000E for use only by service provider traffic and one to Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name
- **SIP Entity 1:** Select the SIP Entity for Session Manager
- **Protocol:** Select the transport protocol used for this link
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. Default listen port is **5060**
- **SIP Entity 2:** Select the name of the other system. Select the CS1000E or Avaya SBCE defined in **Section 6.5**
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. Default listen port is **5060**
- **Trusted:** Check this box. **Note**: If this box is not checked, calls from the associated SIP Entity specified in **Section 6.5** will be denied

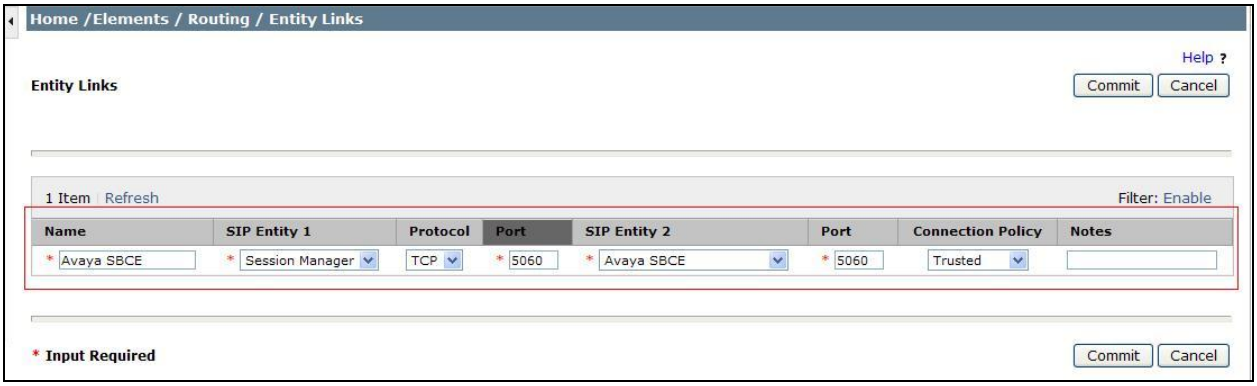
Click **Commit** to save. The following screens illustrate the Entity Links to CS1000E and Avaya SBCE.

Entity Link to CS1000E.



©2012 Avaya Inc. All Rights Reserved.

Entity Link to Avaya SBCE.



6.7. Define Routing Policies

Routing policies describe the conditions under which calls will be routed to CS1000E from either SIP endpoint registered to Session Manager or from other telephony system. It also describes the routing polices for which calls will be routed to the Avaya SBCE and therefore to Storms SIP network. To add a routing policy, Expand **Elements → Routing** and select **Routing Policies.** Click **New** (not shown). In the **General** section, enter the following values.

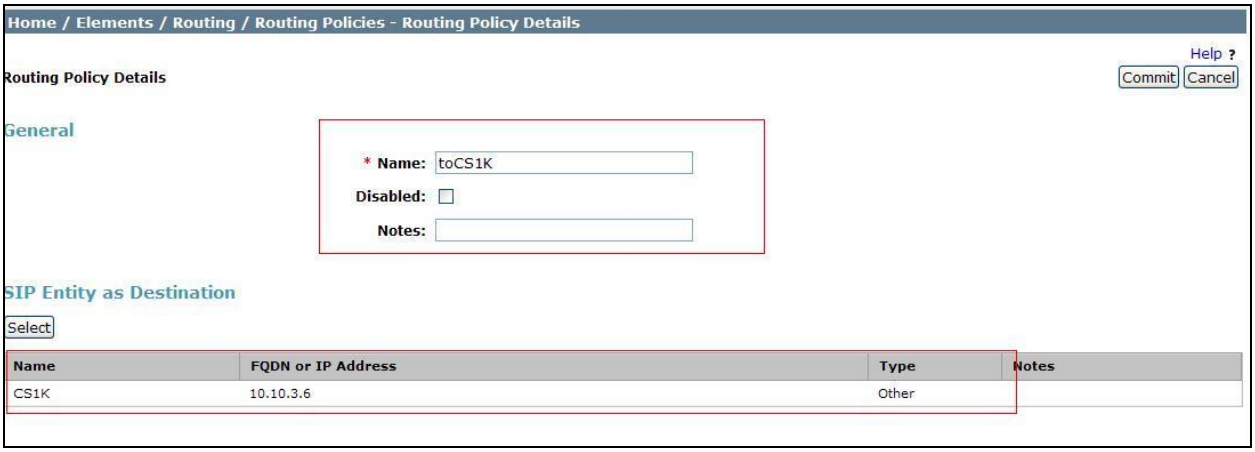
- **Name** Enter an identifier to define the routing policy
- **Disabled** Leave unchecked
- **Notes** Enter a brief description [Optional]

In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown). For routing policy to the CS1000E, select the SIP Entity associated with CS1000E defined in **Section 6.5** and click **Select.** The selected SIP Entity displays on the **Routing Policy Details** page. Use default values for remaining fields. Click **Commit** to save Routing Policy definition.

Note: The routing policy defined in this section is an example and was used in the sample configuration. Other routing policies may be appropriate for different customer networks.

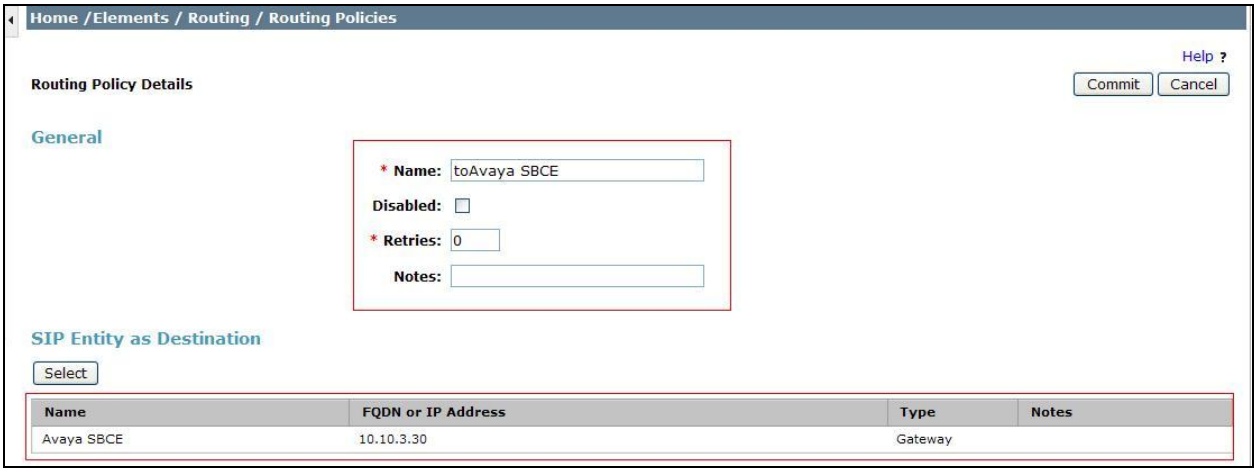
©2012 Avaya Inc. All Rights Reserved.

The following screenshot shows the Routing Policy for CS1000E.



For routing policy to the Avaya SBCE – Storms SIP Trunk, select the SIP Entity associated with Avaya SBCE defined in **Section 6.5** and click **Select**. The selected SIP Entity displays on the **Routing Policy Details** page. Use default values for remaining fields. Click **Commit** to save Routing Policy definition.

The following screenshot shows the Routing Policy for Avaya SBCE – Storms SIP Trunk.



©2012 Avaya Inc. All Rights Reserved.

6.8. Define Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were needed to route calls from CS1000E to Storm and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below. In the **General** section, enter the following values. Use default values for all remaining fields:

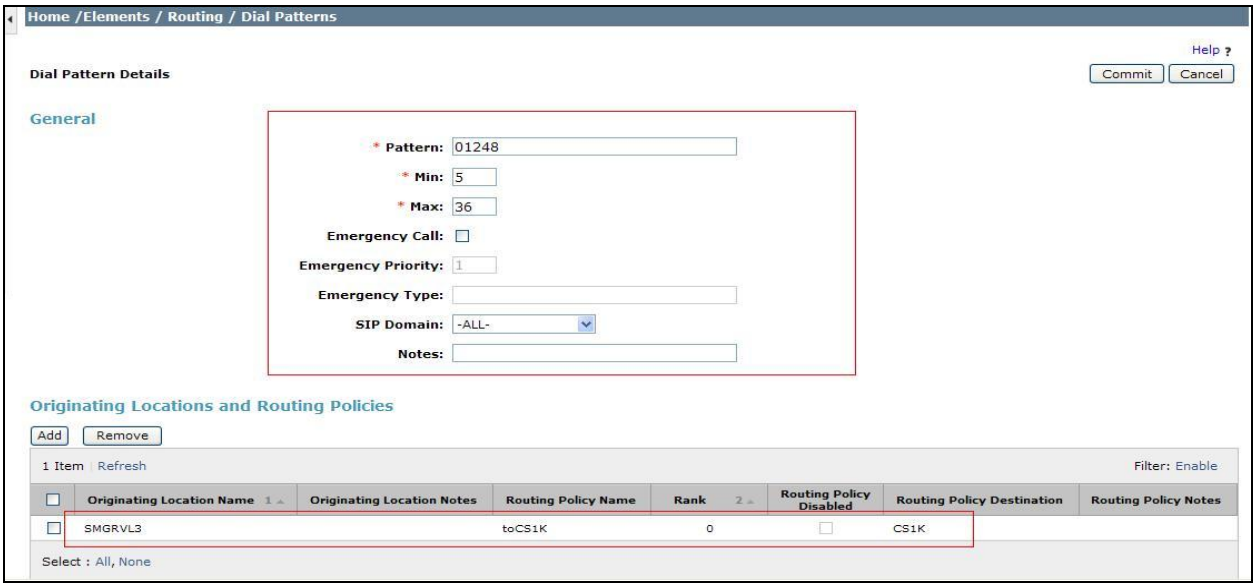
- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call
- **Min:** Enter a minimum length used in the match criteria
- **Max:** Enter a maximum length used in the match criteria
- **SIP Domain:** Enter the destination domain used in the match criteria
- **Notes:** Add a brief description (optional)

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria.

- **Originating Locations** Select **ALL**
- **Routing Policies** Select the required Routing Policy defined in **Section 6.7**

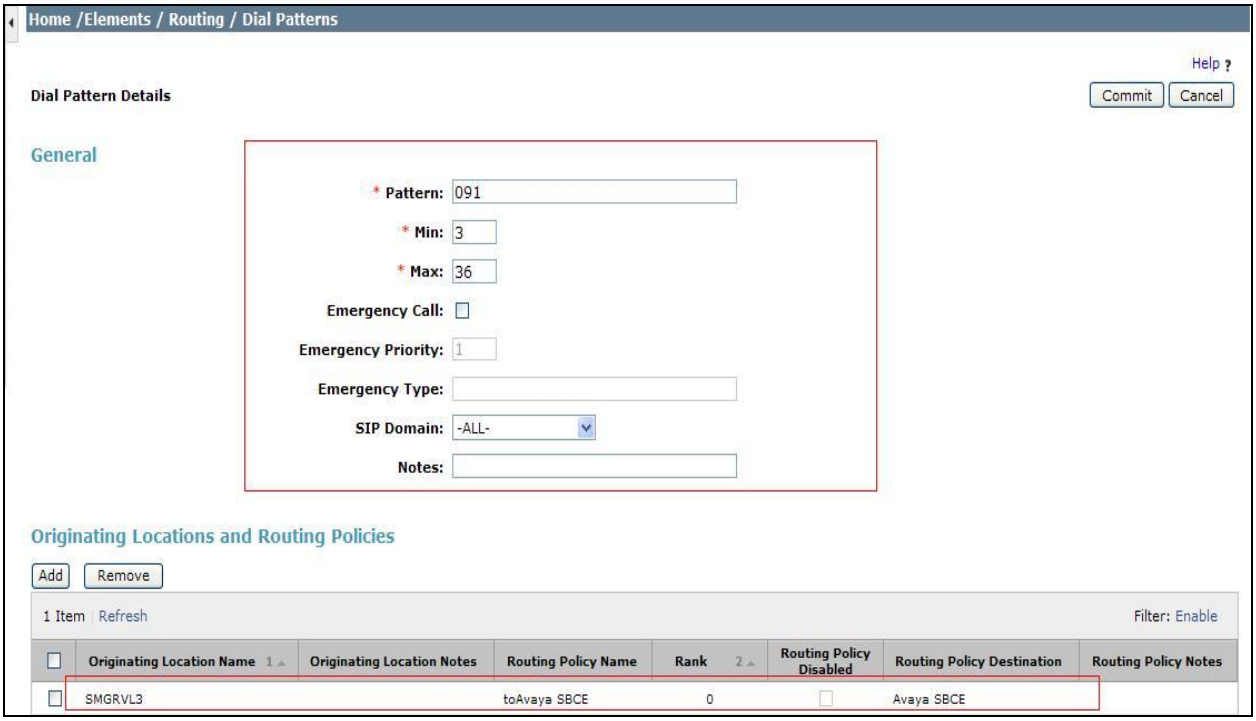
Two examples of the dial patterns used for the compliance test are shown below. This Session Manager is shared between two test environments.

The first example shows that minimum **5** digit dialed numbers that begin with **01248** originating from **SMGRVL3** uses route policy **toCS1K**. This will allow DID numbers assigned to the enterprise from Storm SIP Trunk Service to route to CS1000E.



©2012 Avaya Inc. All Rights Reserved.

The second example shows that a minimum **3** digit dialed numbers that begin with **091** originating from **SMGRVL3** uses route policy **toSipera.** This will allow outbound calls to route from the CS1000E to PSTN test numbers in the Avaya enterprise lab.



©2012 Avaya Inc. All Rights Reserved.

7. Configure Avaya Session Border Controller for Enterprise

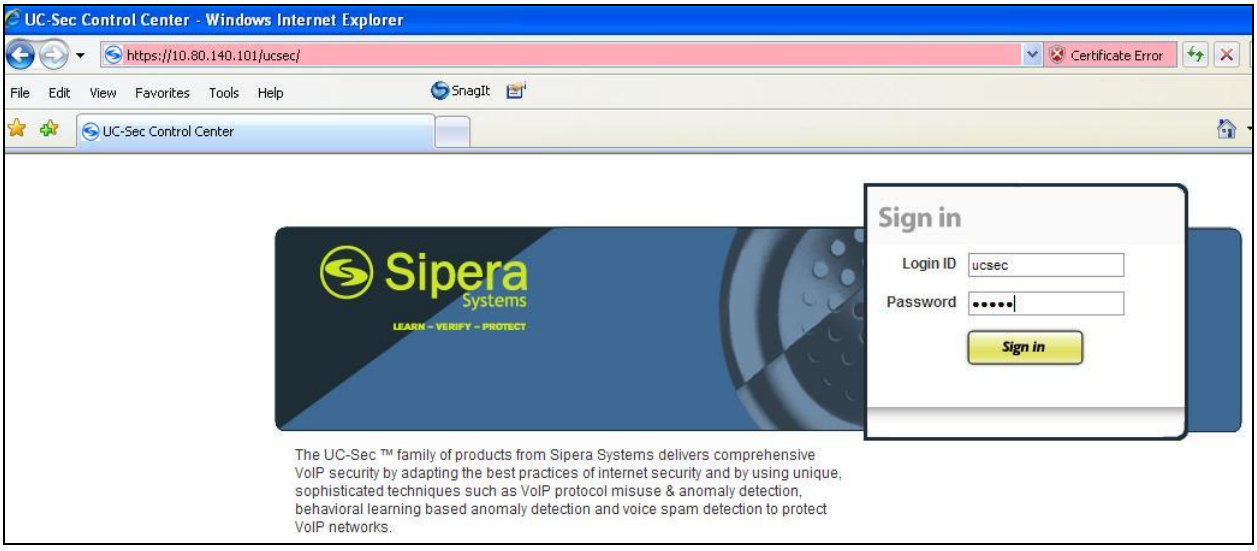
This section describes the configuration of the Session Border Controller. The Avaya SBCE is administered using the UC-Sec Control Center.

7.1. Access Avaya Session Border Controller for Enterprise

Access the Session Border Controller using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation. Select the **UC-Sec Control Center**.

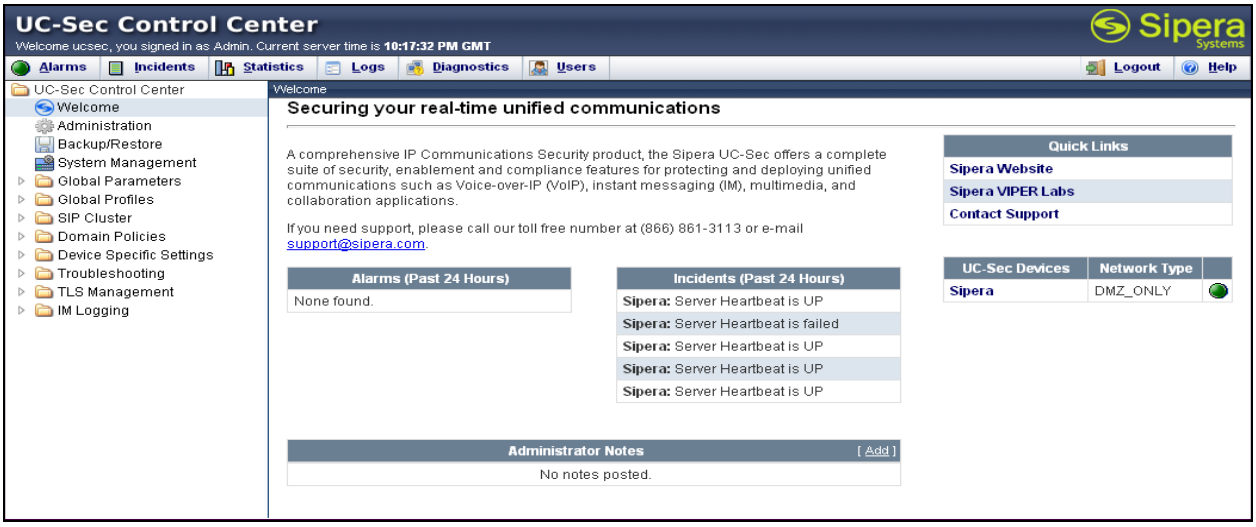


Log in with the appropriate credentials. Click **Sign In**.

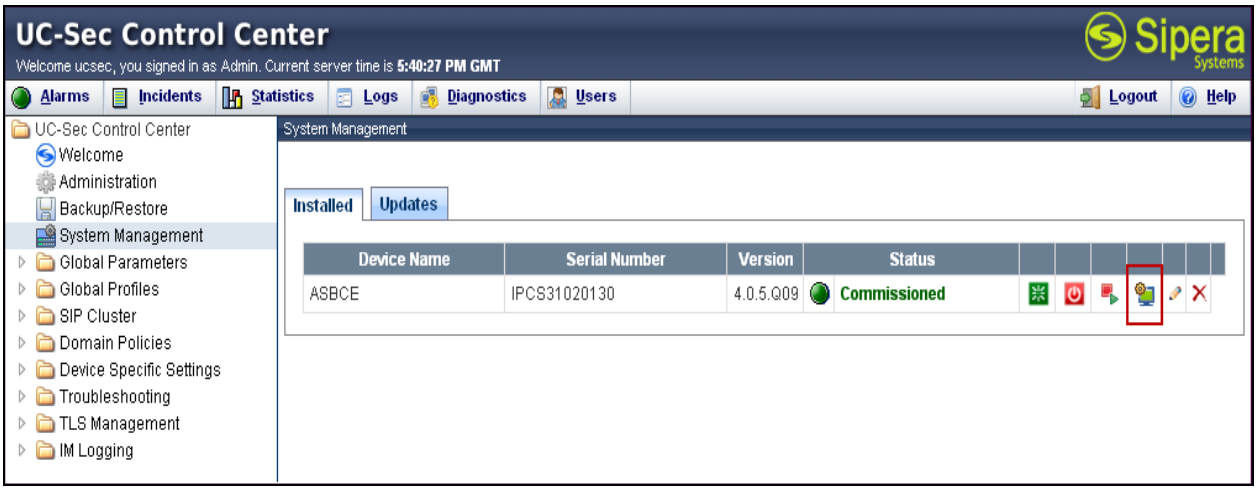


©2012 Avaya Inc. All Rights Reserved.

The main page of the UC-Sec Control Center will appear.

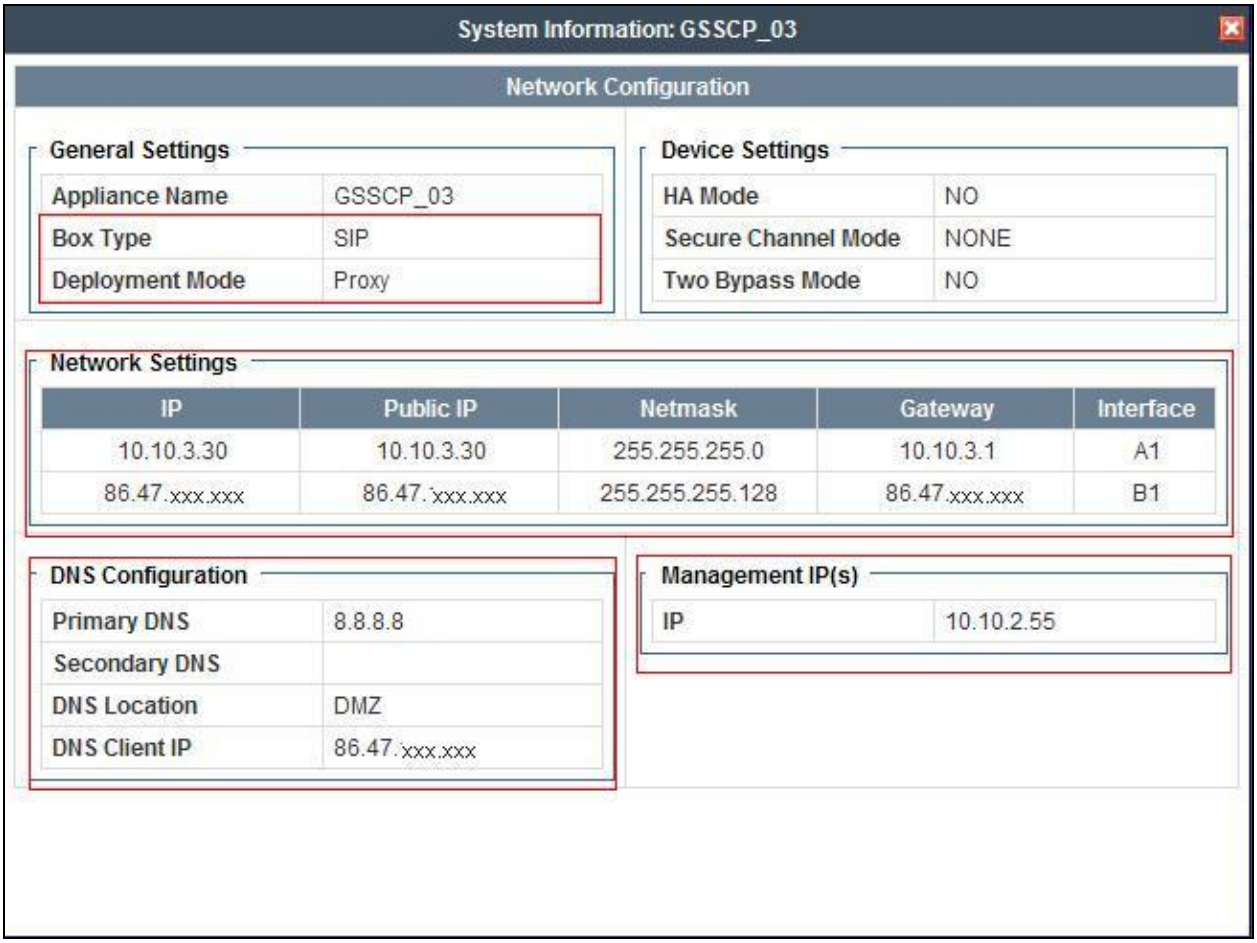


To view system information that was configured during installation, navigate to **UC-Sec Control Center → System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named Sipera is shown. To view the configuration of this device, click the monitor icon (the third icon from the right).



©2012 Avaya Inc. All Rights Reserved.

The **System Information** screen shows the **Network Settings, DNS Configuration** and **Management IP** information provided during installation. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all other fields.



©2012 Avaya Inc. All Rights Reserved.

7.2. Global Profiles

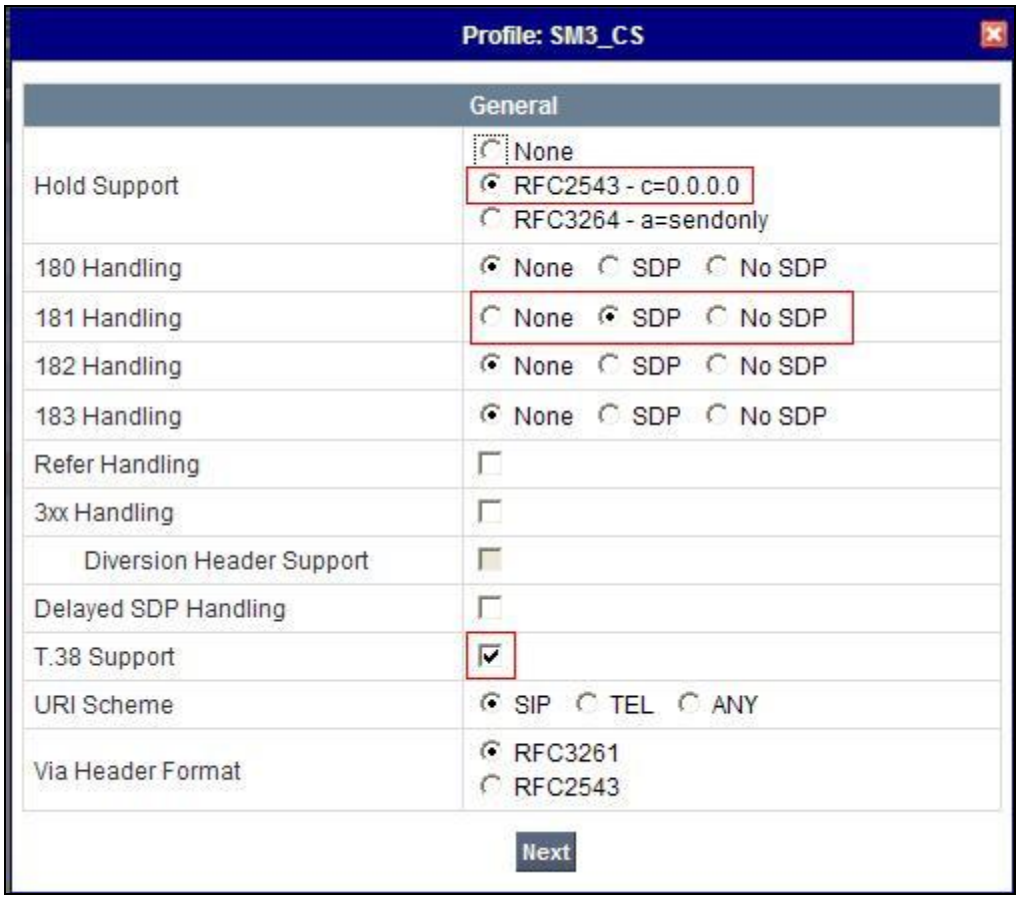
When selected, Global Profiles allows for configuration of parameters across all UC-Sec appliances.

7.2.1. Server Interworking - Avaya Side

Server Internetworking configures and manages various SIP call server specific capabilities such as call hold and T.38. Navigate to **Global Profiles → Server Interworking** and click on **Add Profile** (Not Shown)**.**

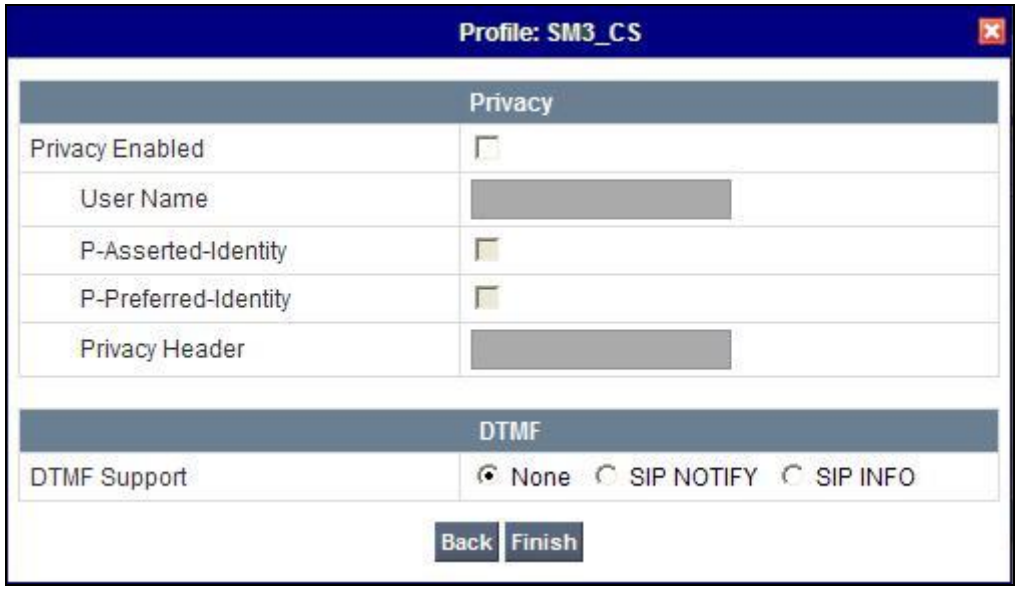
- Enter profile name such as **SM3_CS** and click **Next** (Not Shown)
- **Check Hold Support= RFC2543**
- **Check 181 Handling = SDP**
- **Check T.38 Support**
- All other options on the **General** Tab can be left at default

Click **Next** to continue.

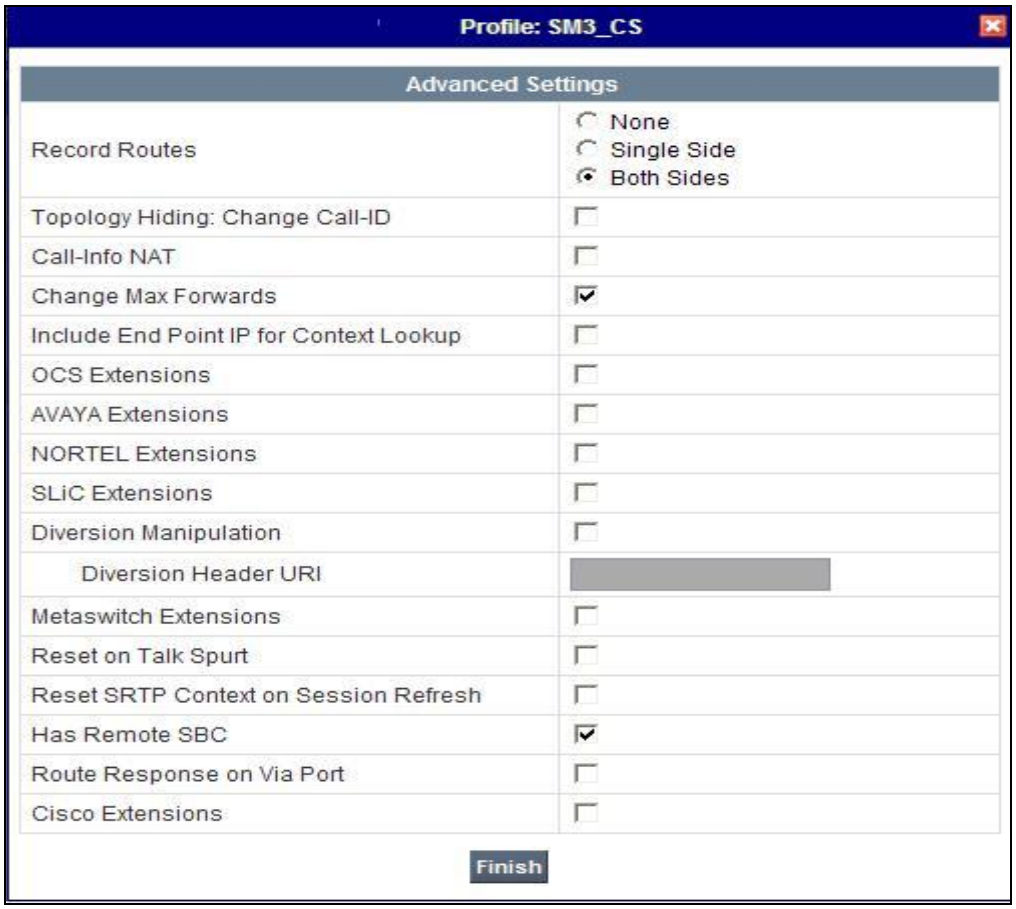


©2012 Avaya Inc. All Rights Reserved.

Default values can be used for the next window that appears. Click **Finish**.



Default values can be used for the **Advanced Settings** window. Click **Finish**.



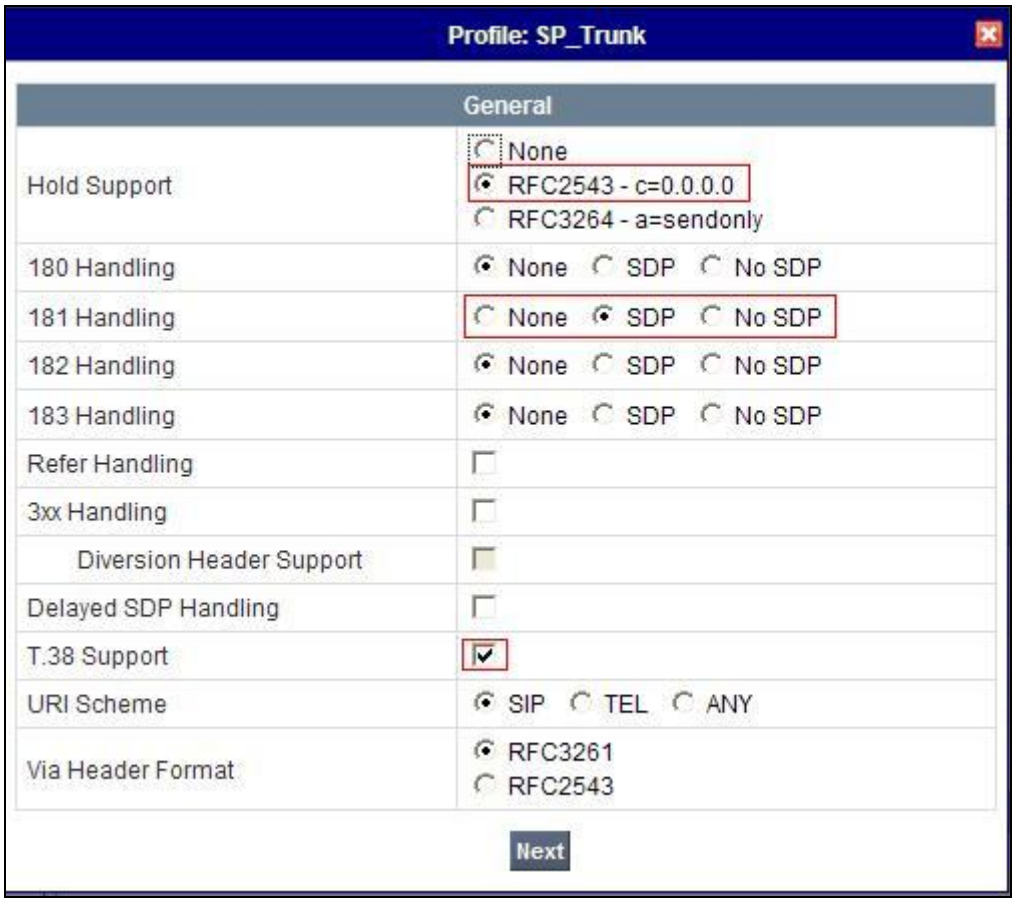
©2012 Avaya Inc. All Rights Reserved.

7.2.2. Server Interworking – Storm Side

Server Internetworking configures and manages various SIP call server specific capabilities such as call hold and T.38. Navigate to **Global Profiles → Server Interworking** and click on **Add Profile** (Not Shown)**.**

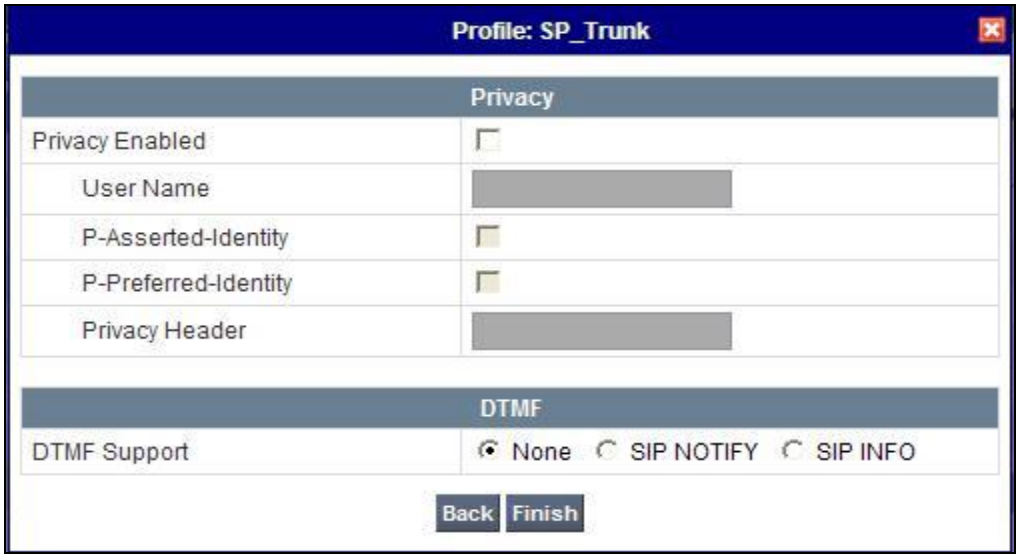
- Enter profile name such as **SP_Trunk** and click **Next** (Not Shown)**.**
- Check **Hold Support= RFC2543**
- **Check 181 Handling = SDP**
- Check **T.38 Support**
- All other options on the **General** Tab can be left at default

Click **Next** to continue.

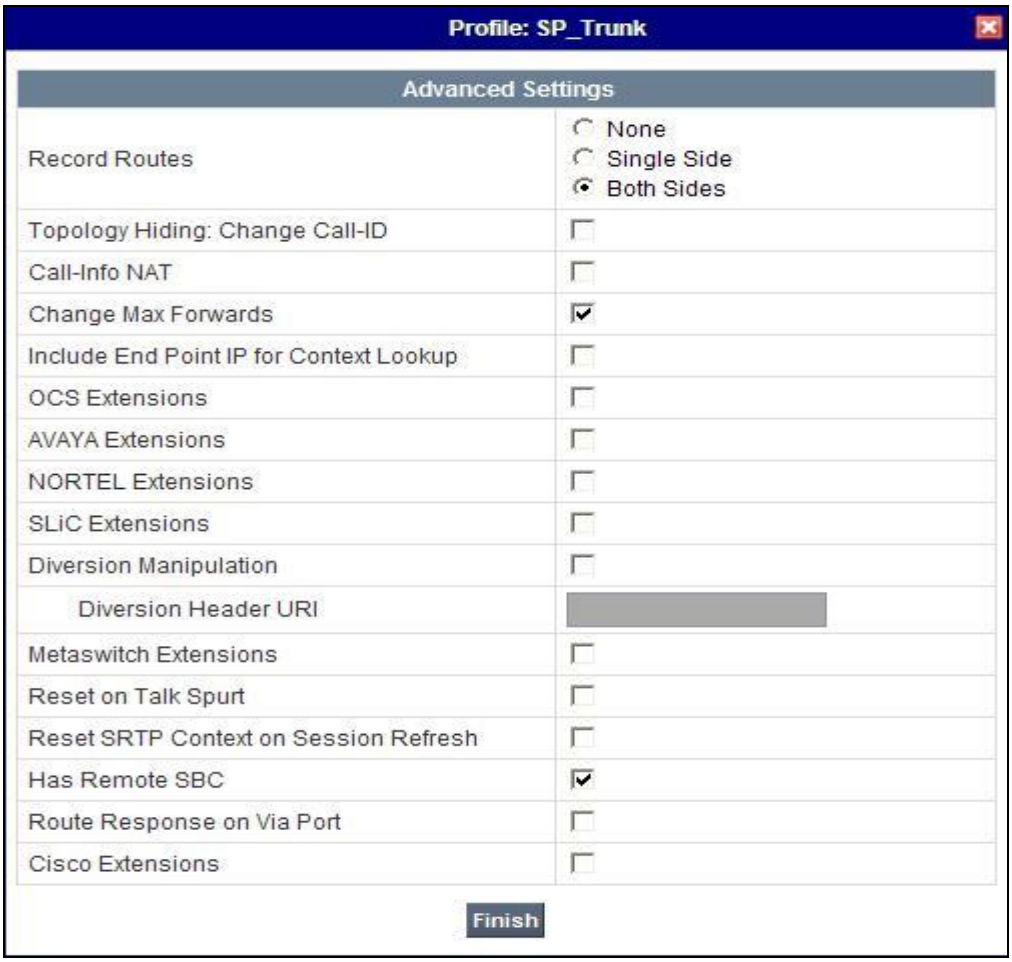


©2012 Avaya Inc. All Rights Reserved.

Default values can be used for the next window that appears. Click **Finish**.



Default values can be used for the **Advanced Settings** window. Click **Finish**.



©2012 Avaya Inc. All Rights Reserved.

7.2.3. Routing

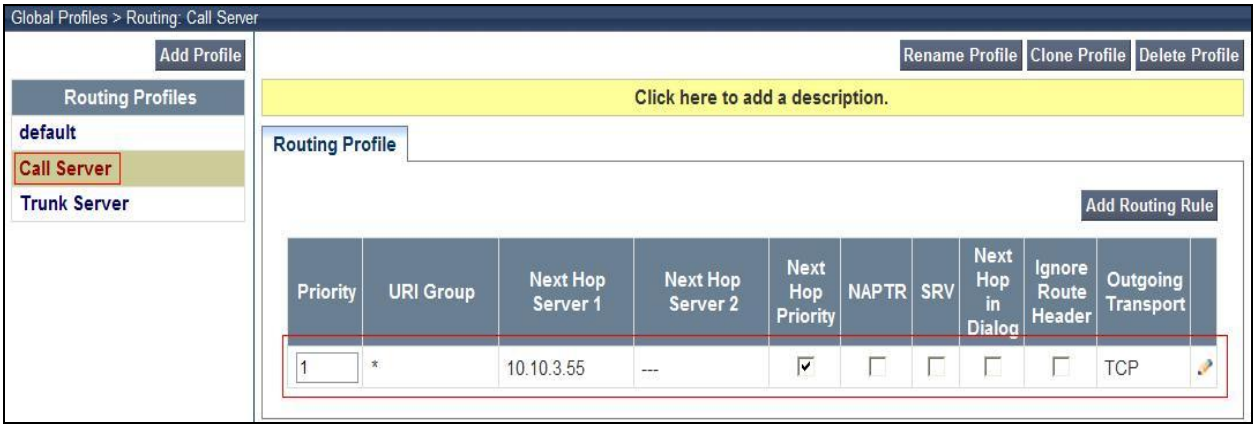
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport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

Create a Routing Profile for Session Manager and a Routing Profile for Storm SIP Trunk. To add a routing profile, navigate to **UC-Sec Control Center → Global Profiles → Routing** and select **Add Profile**. Enter a **Profile Name** and click **Next** to continue.
In the new window that appears, enter the following values. Use default values for all remaining fields:

- **URI Group:** Select "*****" from the drop down box
- **Next Hop Server 1:** Enter the Domain Name or IP address of the Primary Next Hop server
- **Next Hop Server 2:** (Optional) Enter the Domain Name or IP address of the secondary Next Hop server
- **Routing Priority Based on Next Hop Server**: Checked
- **Use Next Hop for In-Dialog Messages**: Select only if there is no secondary Next Hop server
- **Outgoing Transport:** Choose the protocol used for transporting outgoing signaling packets

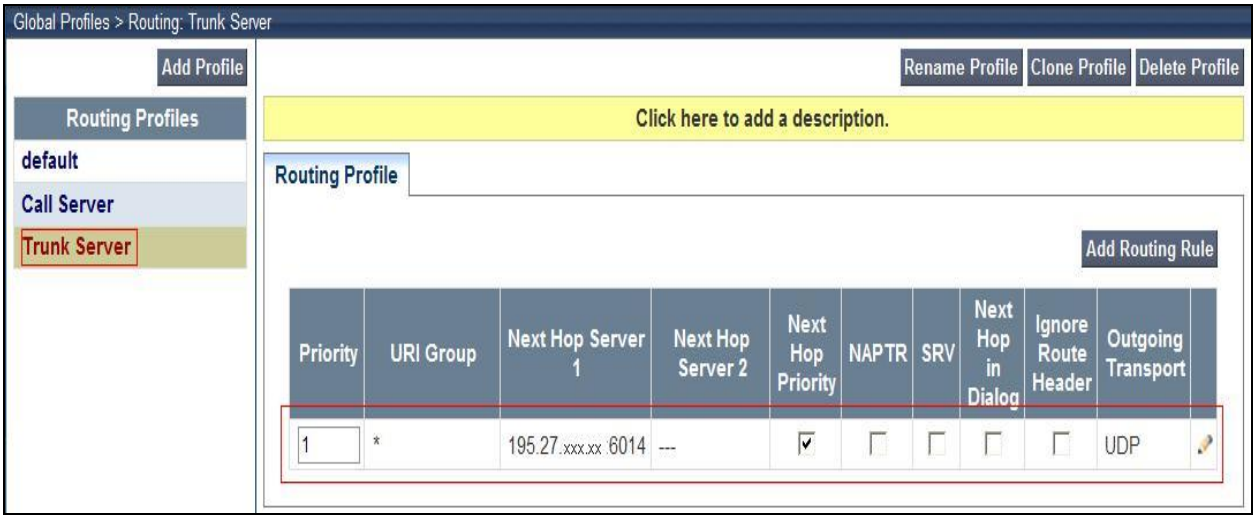
Click **Finish**.

The following screen shows the Routing Profile to Session Manager. The **Next Hop Server 1** IP address must match the IP address of the Session Manager Security Module in **Section 6.5.1**. The Outgoing Transport and port number must match the Session Manager Entity Link created in **Section 6.6**.



©2012 Avaya Inc. All Rights Reserved.

The following screen shows the Routing Profile to Storm. Note that unless default port 5060 is used, this must be included in the next hop IP address. Port **6014** was used by Storm in the test configuration.



©2012 Avaya Inc. All Rights Reserved.

7.2.4. Server - Configuration

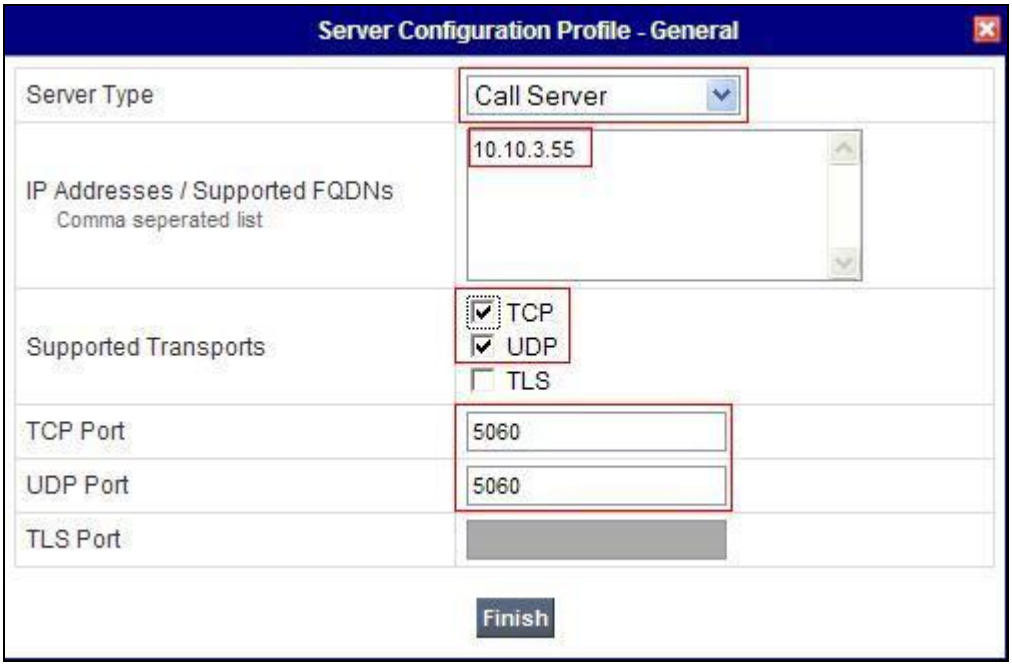
The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs configure and manage various SIP call server specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signaling parameters and some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

7.2.4.1 Server - Configuration – Avaya Side

To add a Server Configuration Profile for Session Manger navigate to **UC-Sec Control Center → Global Profiles → Server Configuration** and click on **Add Profile** (not shown). In the new window that appears, enter the following values. Use default values for all remaining fields:

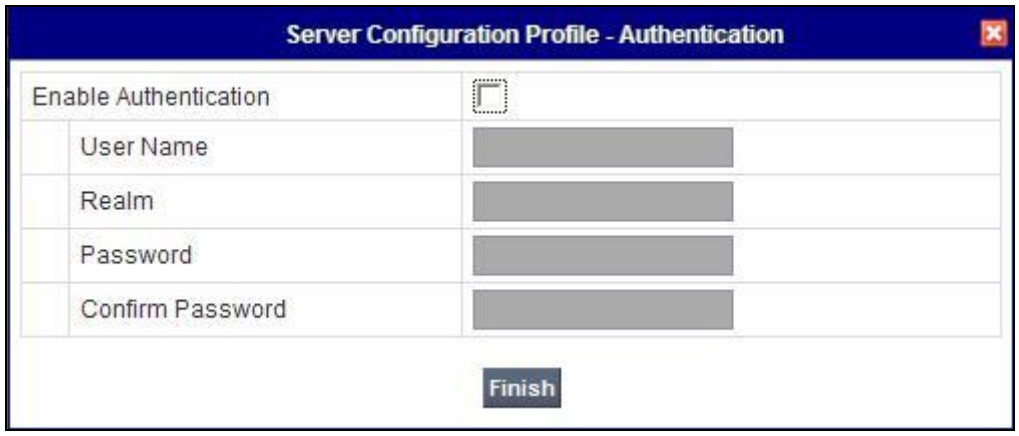
- **Server Type:** Select **Call Server** from the drop-down box
- **IP Addresses / Supported FQDNs:** Enter the IP address of the Session Manager signaling interface.
- **Supported Transports:** Select the transport protocol used to create the Session Manager Entity Link defined in **Section 6.6**
- **TCP Port:** Port number on which to send SIP requests to Session Manager. This should match the port number used in the Session Manager Entity Link defined in **Section 6.6**

Click **Finish** to continue.

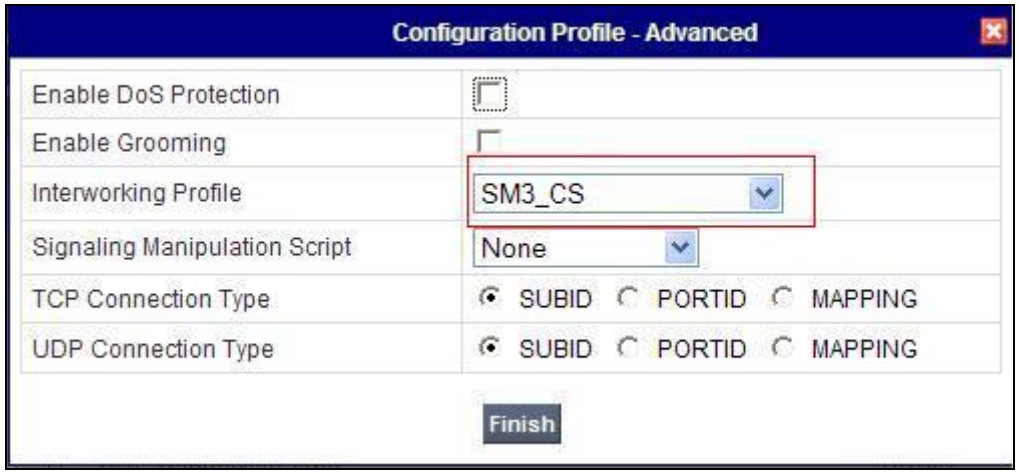


In the new window that appears, verify **Enable Authentication** is unchecked as Session Manager does not require authentication. Click **Finish.**

©2012 Avaya Inc. All Rights Reserved.



In the new window that appears, select the **Interworking Profile** created for the enterprise in **Section 7.2.1**. Use default values for all remaining fields. Click **Finish** to save the configuration.



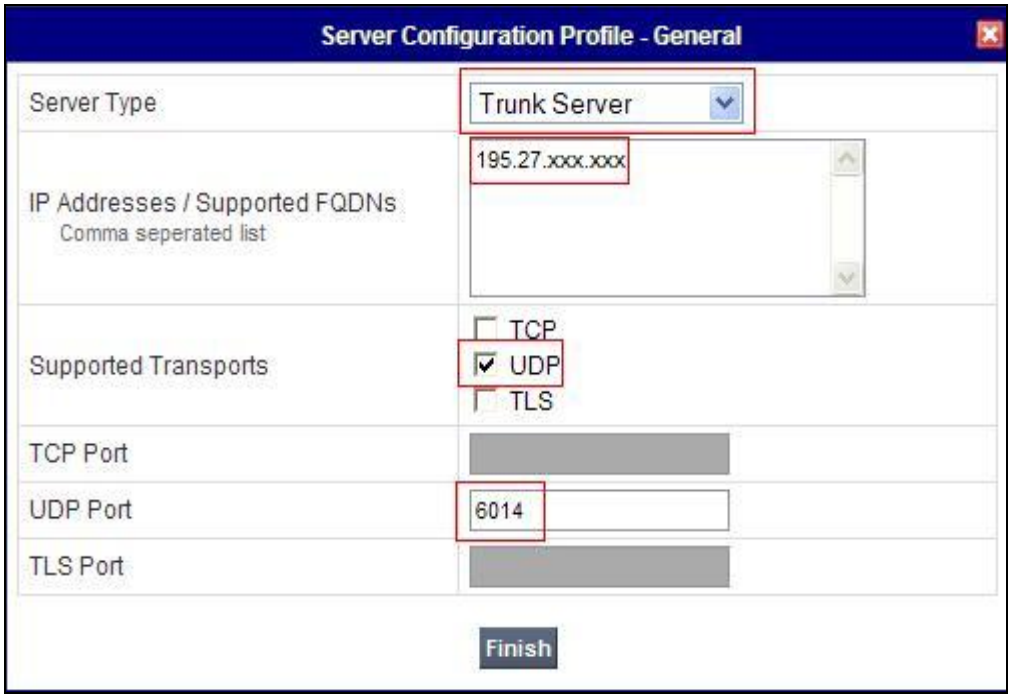
©2012 Avaya Inc. All Rights Reserved.

7.2.4.2 Server - Configuration - Storm

To add a Server Configuration Profile for Storm navigate to **UC-Sec Control Center → Global Profiles → Server Configuration** and click on **Add Profile** (not shown). In the new window that appears, enter the following values. Use default values for all remaining fields:

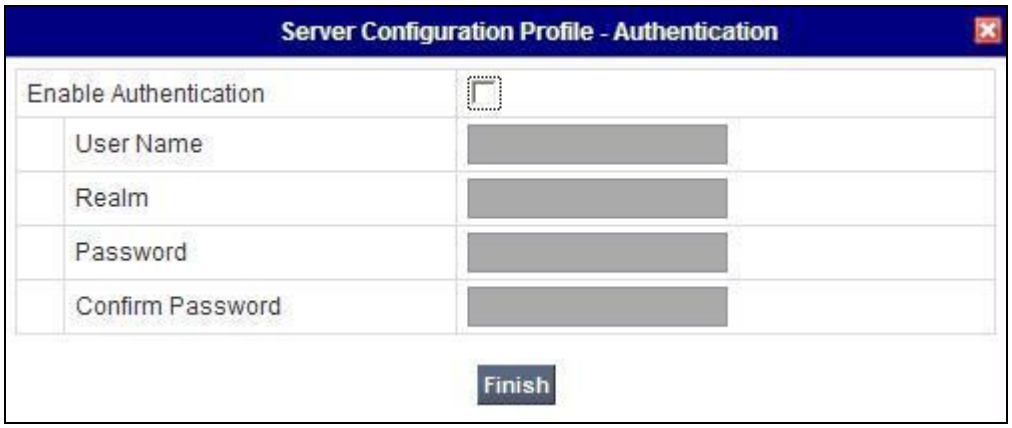
- **Server Type:** Select **Trunk Server** from the drop-down box
- **IP Addresses / Supported FQDNs:** Enter the IP address(es) of the SIP proxy(ies) of the service provider. This will associate the inbound SIP messages from Storm to this Sever Configuration
- **Supported Transports:** Select the transport protocol to be used for SIP traffic between Avaya SBCE and Storm.
- **TCP Port:** Enter the port number that Storm uses to send SIP traffic, **Note**, port **6014** was used by Storm in the test configuration

Click **Finish** to continue.

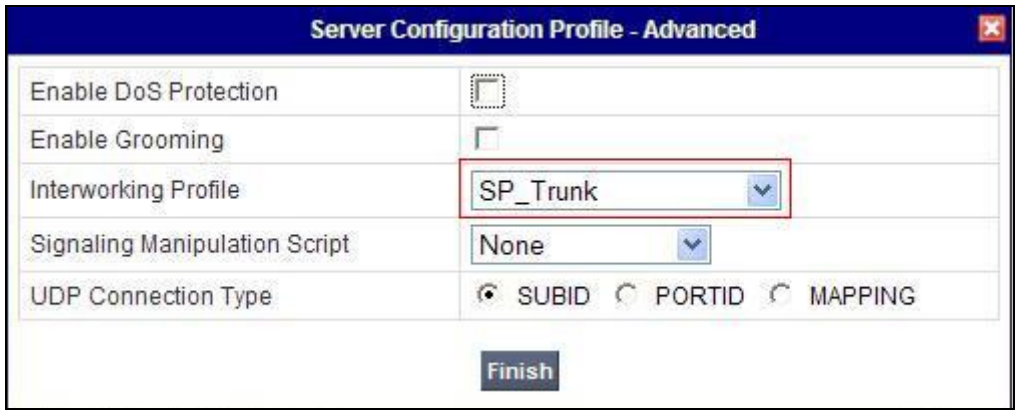


©2012 Avaya Inc. All Rights Reserved.

In the new window that appears, verify **Enable Authentication** is unchecked as Storm do not require authentication. Click **Finish**.



In the new window that appears, select the **Interworking Profile** created for Storm in **Section 7.2.2**. Use default values for all remaining fields. Click **Finish** to save the configuration.



©2012 Avaya Inc. All Rights Reserved.

7.2.5. Topology Hiding – Avaya Side

The **Topology Hiding** screen manages 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. Navigate to **Global Profiles → Topology Hiding** (not shown).

- Click **default** profile and select **Clone Profile** (not shown)
- Enter Profile Name : **SM3_CS**
- Under the **Header** field for **To, From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For **Override Value** type **avaya.com**
- Click **Finish** (not shown)

The screen below is a result of the details configured above.



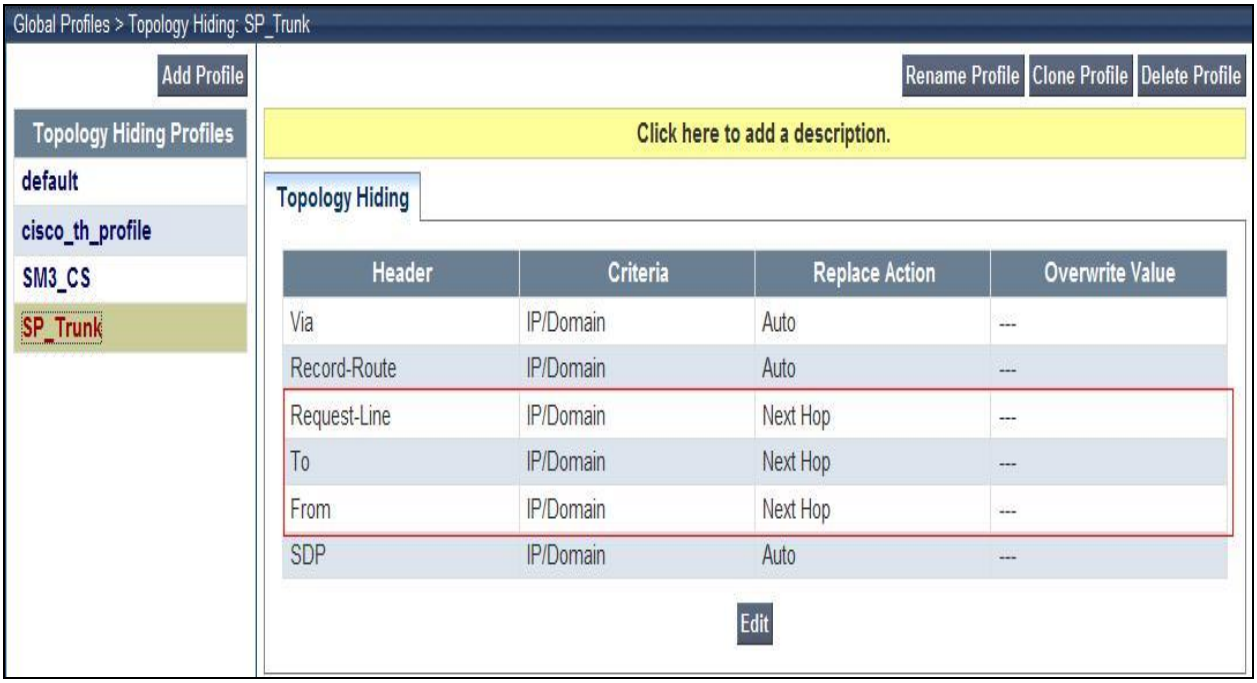
©2012 Avaya Inc. All Rights Reserved.

7.2.6. Topology Hiding – Storm Side

The **Topology Hiding** screen manages 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. Navigate to **Global Profiles → Topology Hiding** (not shown).

- Click **default** profile and select **Clone Profile** (not shown)
- Enter Profile Name : **SP_Trunk**
- For the Header **To, From** and **Request Line** select **IP/Domain** under **Criteria** and **Next Hop** under **Replace Action**
- Click **Finish** (not shown)

The screen below is a result of the details configured above.



©2012 Avaya Inc. All Rights Reserved.

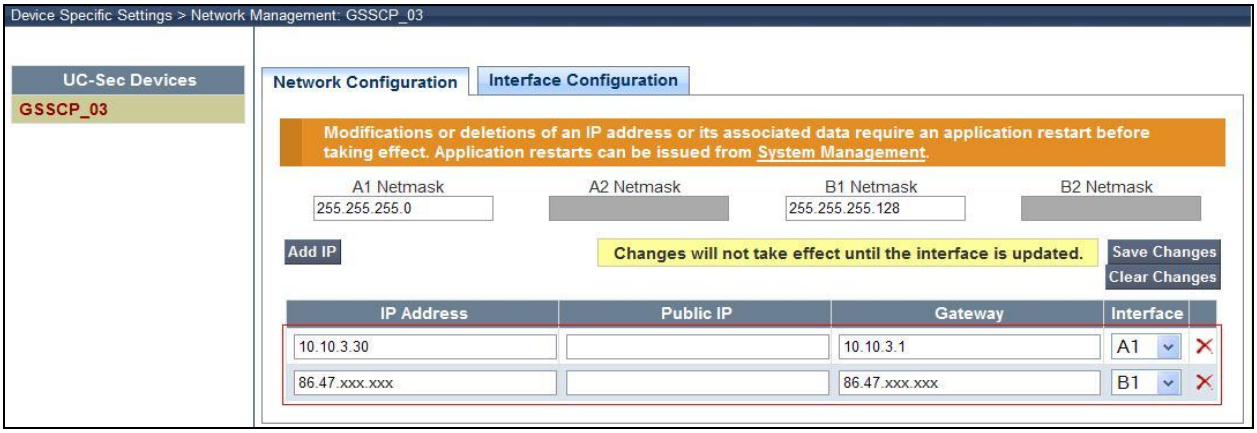
7.3. Device Specific Settings

The Device Specific Settings feature allows aggregation of system information to be viewed, and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network.

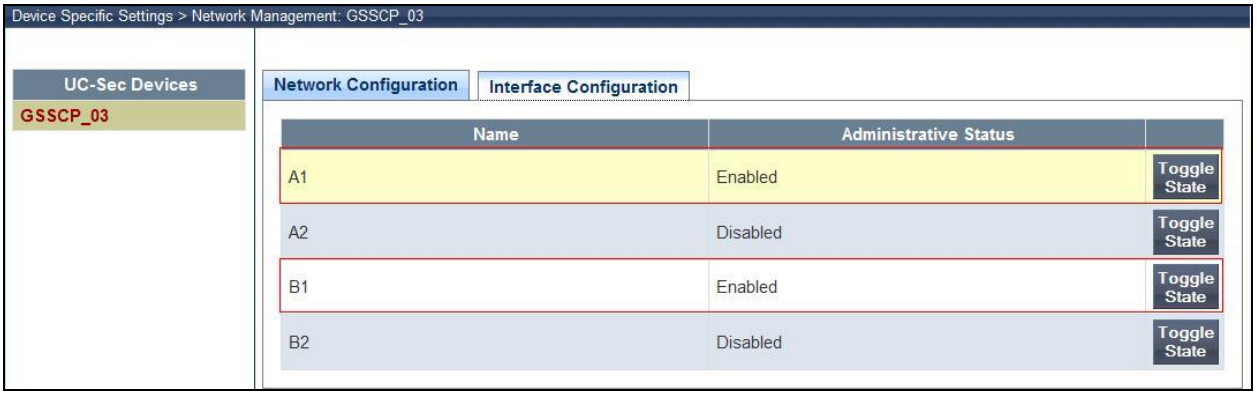
7.3.1. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of the Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc. to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency.

Navigate to **UC-Sec Control Center → Device Specific Settings → Network Management** and verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the private interface is assigned to **A1** and the external interface is assigned to **B1.**



Select the **Interface Configuration** Tab and use the **Toggle State** button to enable the interfaces.



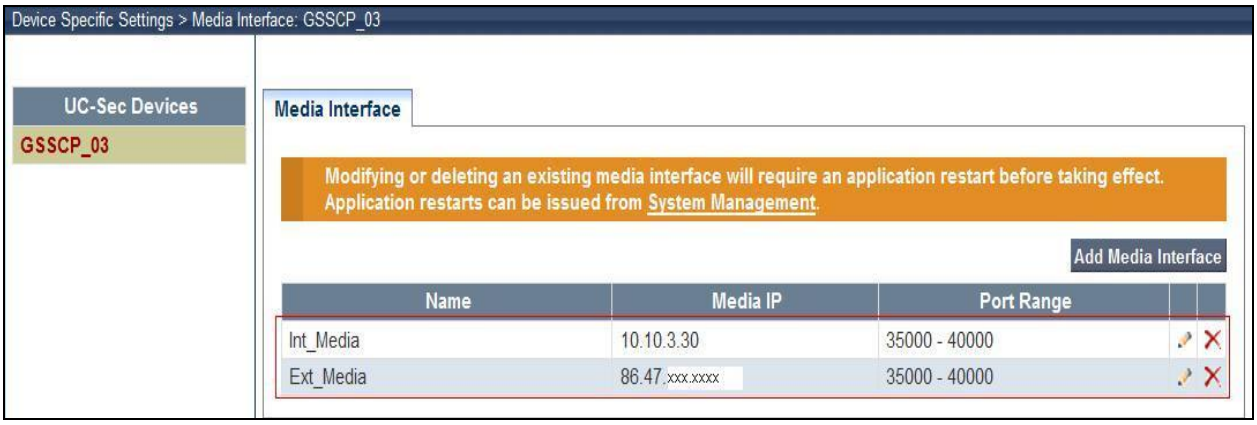
©2012 Avaya Inc. All Rights Reserved.

7.3.2. Media Interface

The Media Interface screen allows the IP address and ports to be set for transporting Media over the SIP trunk. The Avaya SBCE listens for SIP media on the defined ports.
To create a new Media Interface, navigate to **UC-Sec Control Center → Device Specific Settings → Media Interface** and click **Add Media Interface**

- Select **Add Media Interface**
- **Name**: **Int_Media**
- **Media IP**: **10.10.3.30** (Internal address for calls toward CS1000E)
- **Port Range**: **35000-40000**
- Click **Finish**
- Select **Add Media Interface**
- **Name**: **Ext_Media**
- **Media IP**: **86.47.xxx.xxx** (External address for calls toward Storm)
- **Port Range**: **35000-40000**
- Click **Finish**

The following screen shows the Media Interfaces created in the sample configuration for the inside and outside IP interfaces. After the Media Interfaces are created, an application restart is necessary before the changes will take effect.



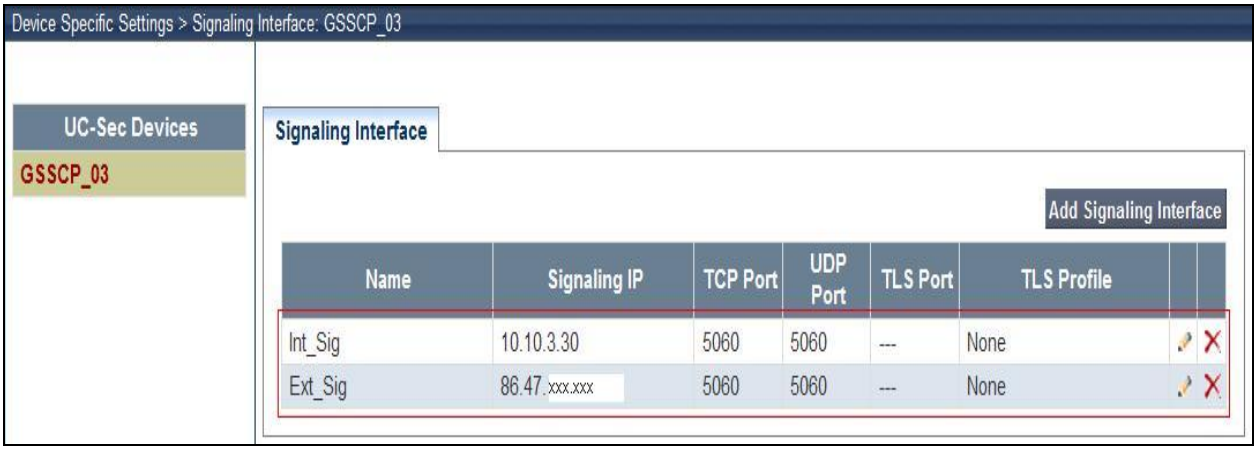
©2012 Avaya Inc. All Rights Reserved.

7.3.3. Signalling Interface

The Signalling Interface screen allows the IP Address and ports to be set for transporting signaling messages over the SIP trunk. The Avaya SBCE listens for SIP requests on the defined ports. Create a Signaling Interface for both the inside and outside IP interfaces. To create a new Signaling Interface, navigate to **UC-Sec Control Center → Device Specific Settings → Signaling Interface** and click **Add Signaling Interface**

- **Name**: **Int_Sig**
- **Signaling IP**: **10.10.3.30** (Internal address for calls toward CS1000E)
- **TCP Port**: **5060**
- **UDP Port**: **5060**
- Click **Finish**
- Select **Add Signaling Interface**
- **Name**: **Ext_Sig**
- **Signaling IP: 86.47.xxx.xxx** (External address for calls toward Storm)
- **TCP Port**: **5060**
- **UDP Port**: **5060**
- Click **Finish**

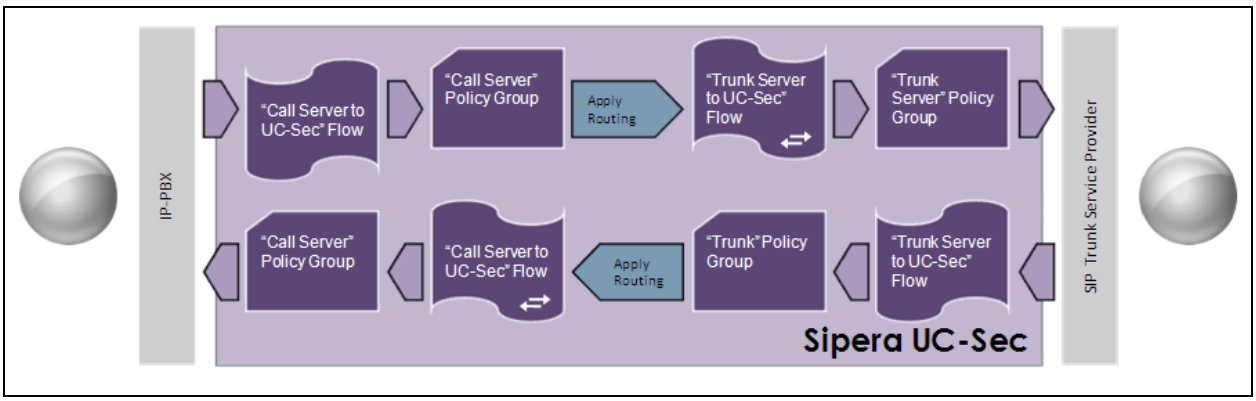
The following screen shows the signaling interfaces created in the sample configuration for the inside and outside IP interfaces.



©2012 Avaya Inc. All Rights Reserved.

7.3.4. End Point Flows

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



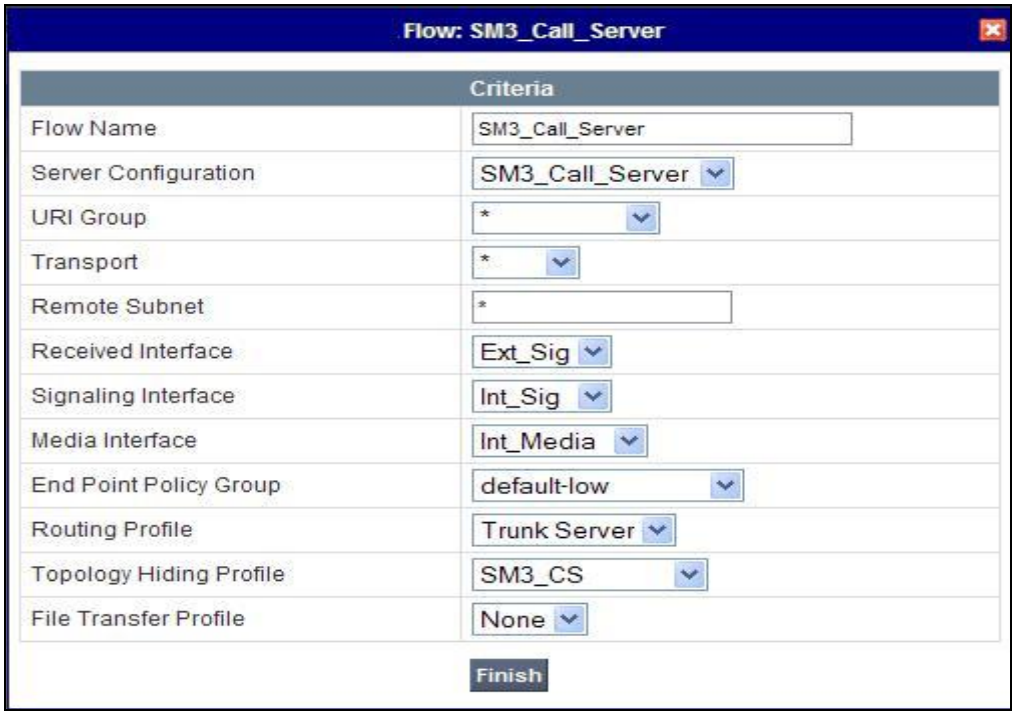
To create a Server Flow, navigate to **UC-Sec Control Center → Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add Flow**.

- **Flow Name:** Enter a descriptive name
- **Server Configuration:** Select a Server Configuration created in **Section 7.1.5** to assign to the Flow
- **Received Interface:** Select the Signaling Interface the Server Configuration is allowed to receive SIP messages from
- **Signaling Interface:** Select the Signaling Interface used to communicate with the Server Configuration
- **Media Interface:** Select the Media Interface used to communicate with the Server Configuration.
- **End Point Policy Group:** Select the policy assigned to the Server Configuration
- **Routing Profile:** Select the profile the Server Configuration will use to route SIP messages to
- **Topology Hiding Profile:** Select the profile to apply toward the Server Configuration

Click **Finish** to save and exit.

©2012 Avaya Inc. All Rights Reserved.

The following screen shows the Sever Flow for Session Manager.



The following screen shows the Sever Flow for Storm.



©2012 Avaya Inc. All Rights Reserved.

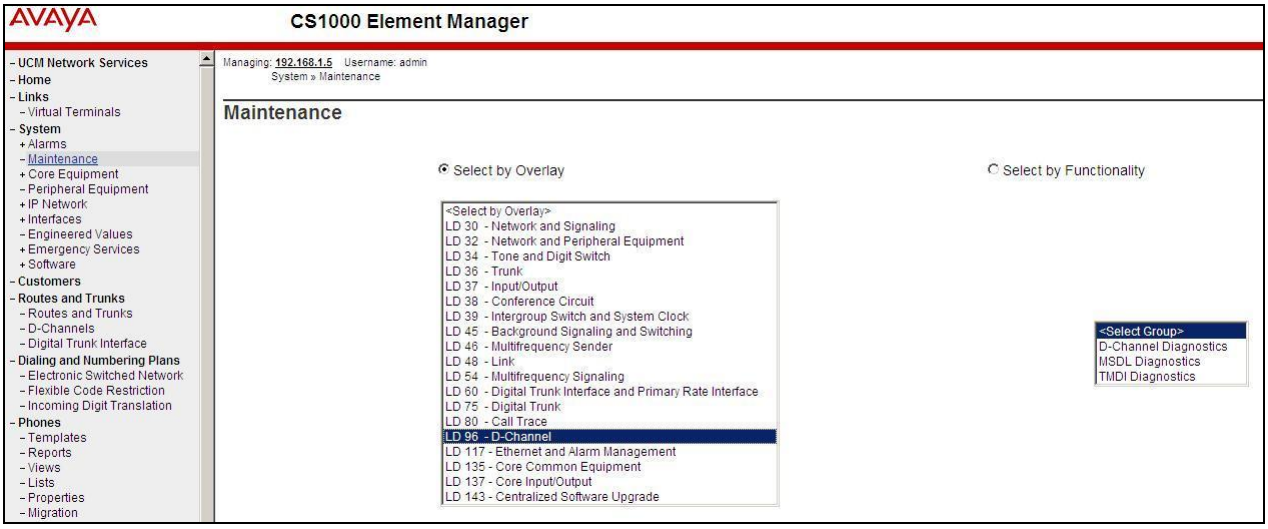
8. Storm SIP Service Provider Configuration

The setup for the use of Storm is by using the SIP trunk with an authenticated service. The configuration of Storms authentication service to support the SIP trunk service is outside of the scope for these Application Notes and will not be covered. To obtain further information on Storms equipment and system configuration please contact an authorized Cable &Wireless representative.

9. Verification

9.1. Verify Avaya Communication Server 1000E Operational Status

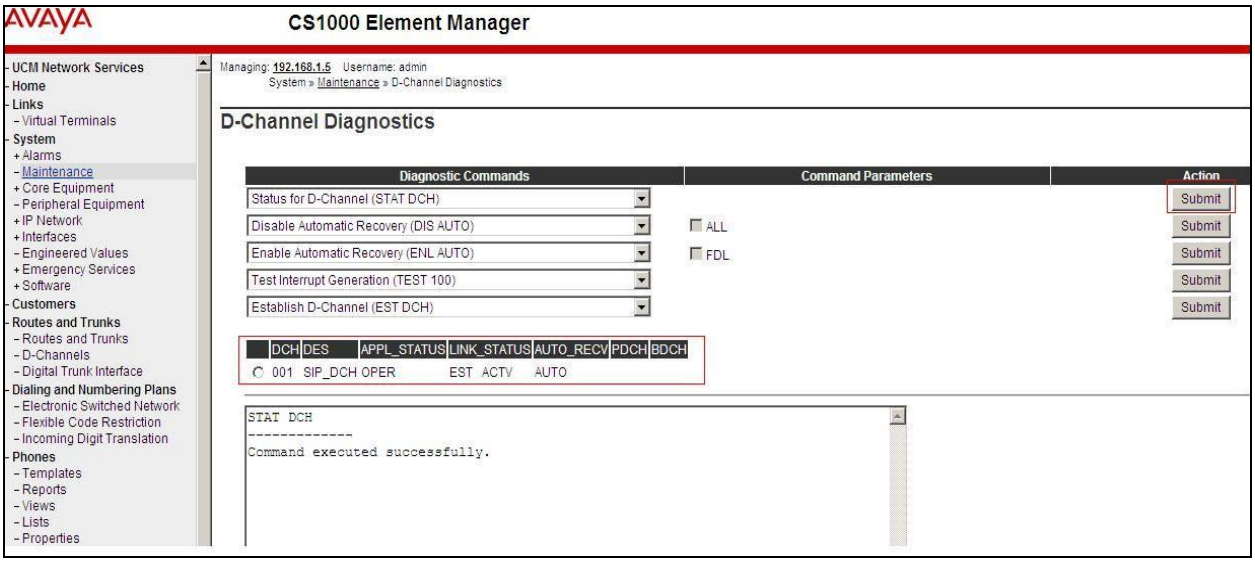
Expand **System** on the left navigation panel and select **Maintenance.** Select **LD 96 - D-Channel** from the **Select by Overlay** table and the **D-Channel Diagnostics** function from the **Select by Functionality** table as shown below.



©2012 Avaya Inc. All Rights Reserved.

Select **Status for D-Channel (STAT DCH)** command and click **Submit** to verify status of virtual D-Channel as shown below. Verify the status of the following fields.

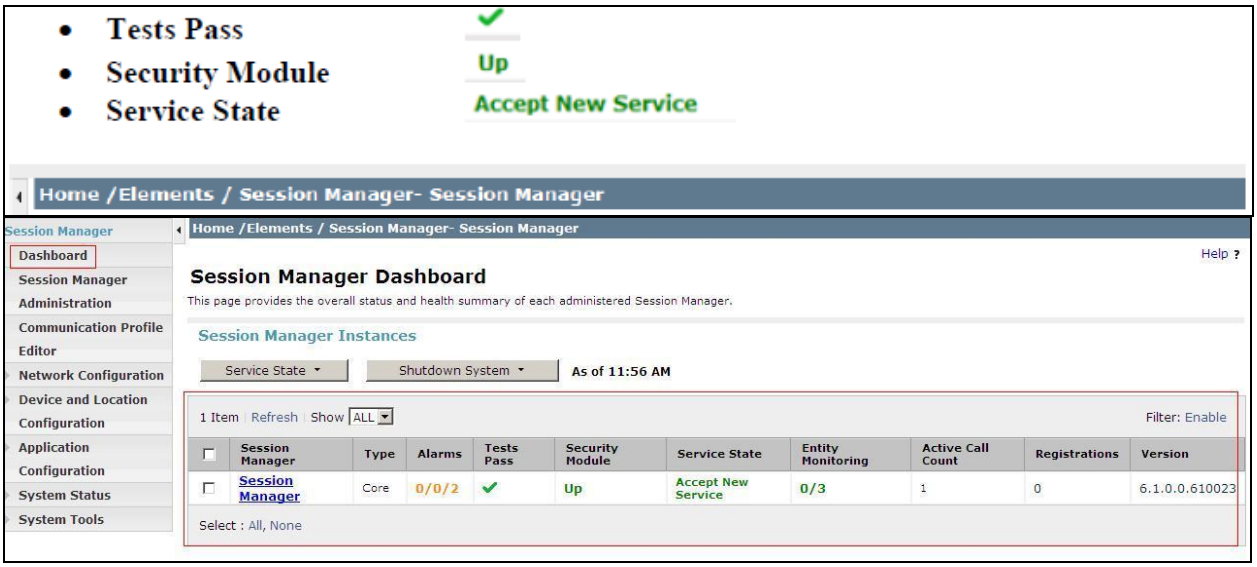
- **APPL_STATUS** Verify status is **OPER**
- **LINK_STATUS** Verify status is **EST ACTV**



9.2. Verify Avaya Aura® Session Manager Operational Status

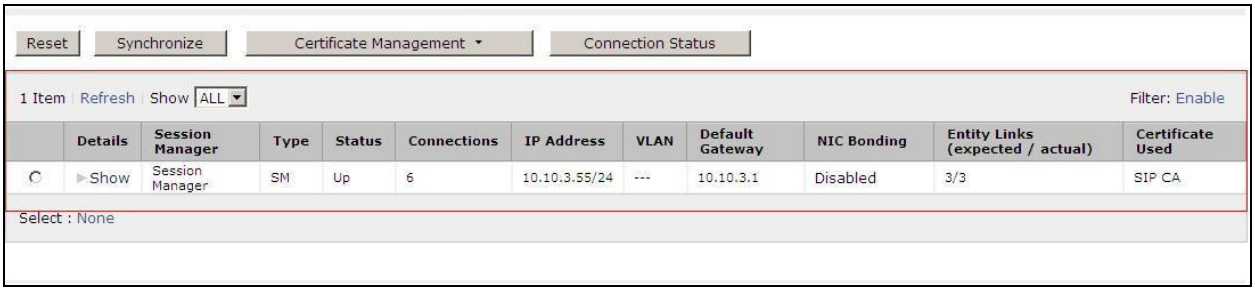
9.2.1. Verify Avaya Aura® Session Manager is Operational

Navigate to **Elements → Session Manager → Dashboard** (not shown) to verify the overall system status for Session Manager. Specifically, verify the status of the following fields as shown below.



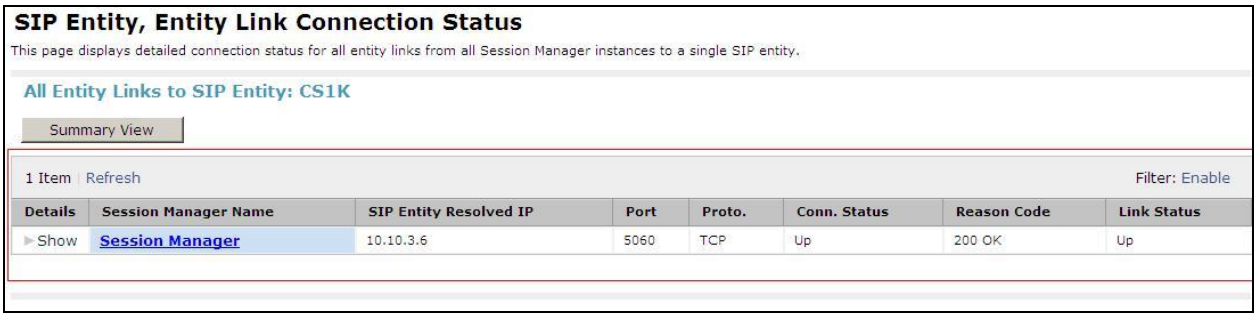
©2012 Avaya Inc. All Rights Reserved.

Navigate to **Elements → Session Manager → System Status → Security Module Status** (not shown) to view more detailed status information on the status of Security Module for the specific Session Manager. Verify the **Status** column displays **Up** as shown below.

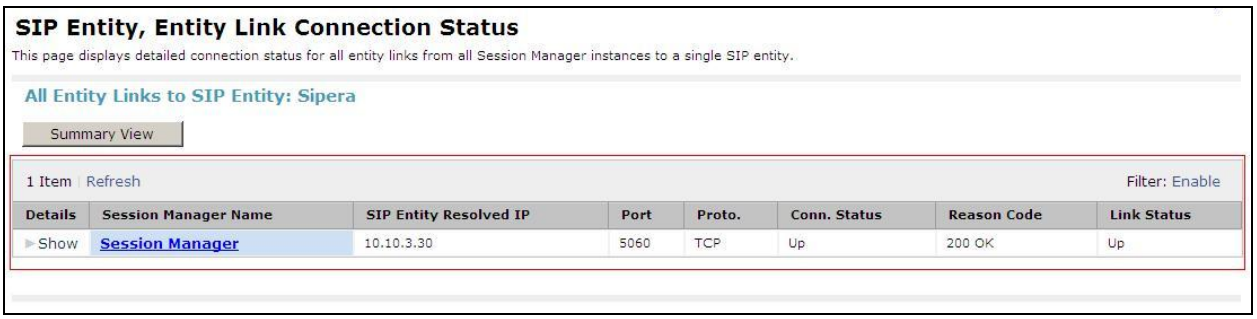


9.2.2. Verify SIP Entity Link Status

Navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring** (not shown) to view more detailed status information for one of the SIP Entity Links. Select the SIP Entity for CS1000E from the **All Monitored SIP Entities** table (not shown) to open the **SIP Entity, Entity Link Connection Status** page. In the **All Entity Links to SIP Entity: CS1K** table, verify the **Conn. Status** for the link is **Up** as shown below.



Verify the status of the SIP link is up between the Session Manager and the Avaya SBCE by going through the same process as outlined above but selecting the SIP Entity for the Avaya SBCE in the **All Monitored SIP Entities:** table.



©2012 Avaya Inc. All Rights Reserved.

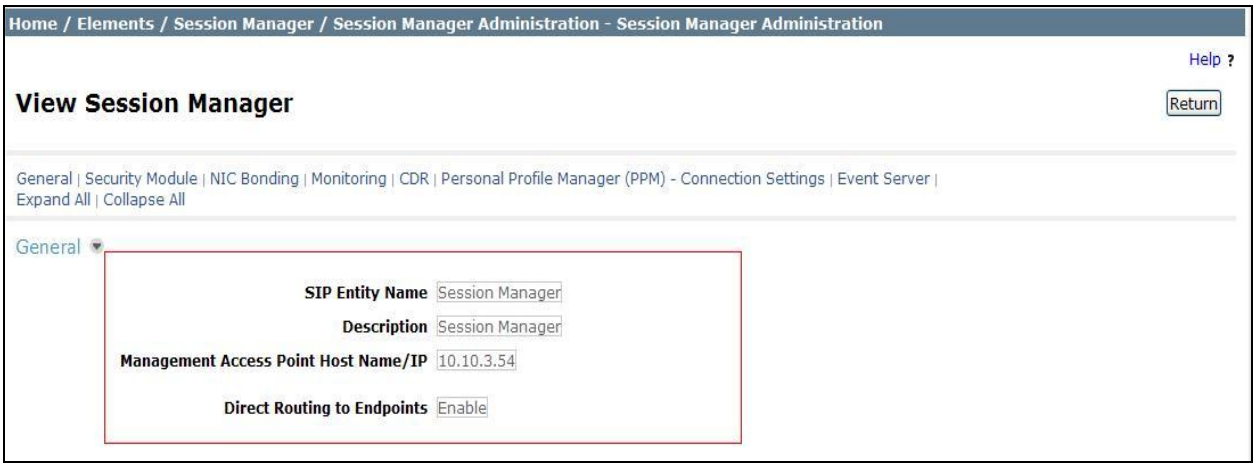
9.2.3. Verify Avaya Aura® Session Manager Instance

The creation of a Session Manager Instance provides the linkage between System Manager and Session Manager. This was most likely done as part of the initial Session Manager installation. To add a Session Manager, navigate to **Elements → Session Manager → Session Manager Administration** in the left-hand navigation pane and click on the **new** button in the right pane (not shown). If the Session Manager instance already exists, click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

In the **General** section, enter the following values:

- **SIP Entity Name:** Select the SIP Entity created for Session Manager
- **Description**: Add a brief description (optional)
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface

The following screen shows the Session Manager values used for the compliance test.

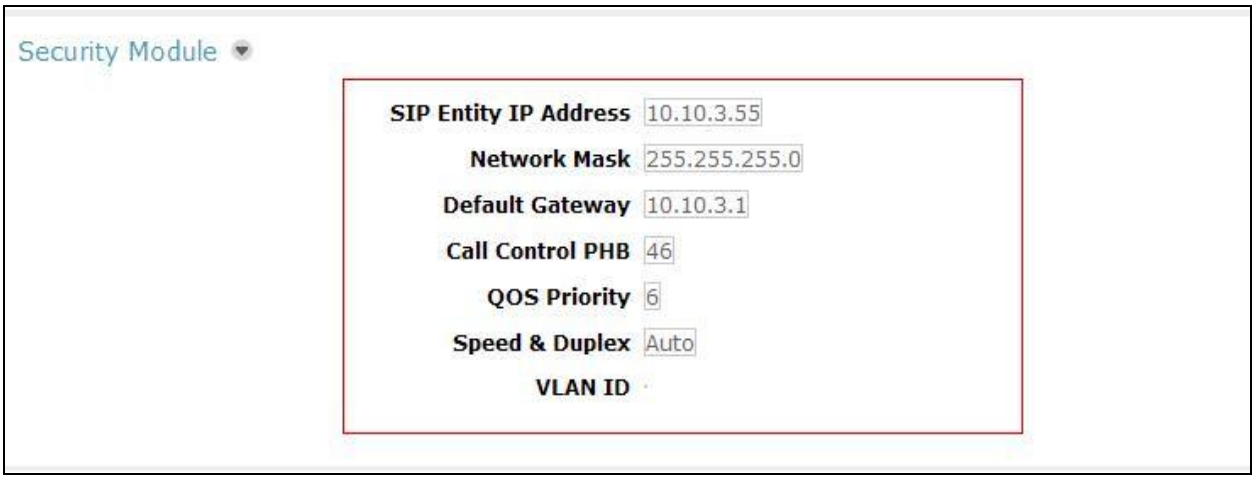


©2012 Avaya Inc. All Rights Reserved.

In the **Security Module** section, enter the following values:

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name. Otherwise, enter IP address of Session Manager signaling interface
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager
- **Default Gateway**: Enter the IP address of the default gateway for Session Manager

Use default values for the remaining fields. Click **Save** (not shown) to add this Session Manager. The following screen shows the remaining Session Manager values used for the compliance test.



©2012 Avaya Inc. All Rights Reserved.

10. Conclusion

These Application Notes describe the configuration necessary to connect the Avaya Communication Server 1000E, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise to Storm SIP Service. Interoperability testing of the sample configuration was completed with successful results for the Storm SIP Trunk with observations which are detailed in **Section 2.2.**

11. Additional References

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

[1] Avaya Aura® Session Manager Overview, Doc ID 03-603323, available at http://support.avaya.com

[2] Installing and Configuring Avaya Aura® Session Manager, available at http://support.avaya.com.

[3] Avaya Aura® Session Manager Case Studies, available at http://support.avaya.com

[4] Maintaining and Troubleshooting Avaya Aura® Session Manager, Doc ID 03-603325, available at http://support.avaya.com

[5] Administering Avaya Aura® Session Manager, Doc ID 03-603324, available at http://support.avaya.com

[6] IP Peer Networking Installation and Commissioning, Release 7.5, Document Number NN43001-313, available at http://support.avaya.com

[7] Network Routing Service Fundamentals, Release 7.5, Document Number NN43001-130, Issue 03.02, available at http://support.avaya.com

[8] Co-resident Call Server and Signaling Server Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-509, available at http://support.avaya.com

[9] Signaling Server and IP Line Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-125, available at http://support.avaya.com

[10] E-SBC (Avaya Session Border Controller for Enterprise) Administration Guide, November 2011

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

©2012 Avaya Inc. All Rights Reserved.

Appendix A – Avaya Communication Server 1000E Software

Avaya Communication Server 1000E call server patches and plug ins

```
TID: 46379

VERSION 4121

System type is - Communication Server 1000E/CPPM Linux
CPPM - Pentium M 1.4 GHz

IPMGs Registered:              1
IPMGs Unregistered:            0
IPMGs Configured/unregistered:  0

RELEASE 7
ISSUE 50 Q  +
IDLE_SET_DISPLAY NORTEL
DepList 1: core Issue: 01(created: 2012-05-16 12:51:18 (est))

MDP>LAST SUCCESSFUL MDP REFRESH :2012-06-06 15:58:07(Local Time)
MDP>USING DEPLIST ZIP FILE DOWNLOADED :2012-06-06 11:11:47(est)
SYSTEM HAS NO USER SELECTED PEPS IN-SERVICE


LOADWARE VERSION: PSWV 100+

INSTALLED LOADWARE PEPS : 3
PAT#  CR #            PATCH REF #     NAME            DATE        FILENAME
00    wi00890367      ISS1:1OF1       MGCCCD02        24/04/2012  MGCCCD02.LW
01    wi00832543      ISS1:1OF1       DSP1AB04        24/04/2012  DSP1AB04.LW
02    wi00946113      ISS1:1OF1       MGCBBA15        24/04/2012  MGCBBA15.LW


ENABLED PLUGINS : 1

PLUGIN    STATUS      PRS/CR NUM    MPLR NUM      DESCRIPTION
------------------------------------------------------------
501       ENABLED     Q02138637     MPLR30070     Enables blind transfer to a SIP endpoint even
if SIP UPDATE is not supported by the far end
```

Avaya Communication Server 1000E call server deplists

```
VERSION 4121
RELEASE 7
ISSUE 50 Q +
DepList 1: core Issue: 01 (created: 2012-07-16 17:52:47 (est)) ALTERED

IN-SERVICE PEPS
PAT# CR #            PATCH REF #     NAME      DATE        FILENAME       SPECINS
000  wi00891626      ISS1:1OF1       p31051 1  11/10/2012  p31051 1.cpl   YES
001  wi00951837      ISS1:1OF1       p31485_1  11/10/2012  p31485_1.cpl   NO
002  wi00946477      ISS1:1OF1       p31426_1  11/10/2012  p31426_1.cpl   NO
003  wi00906163      ISS1:1OF1       p31205 1  11/10/2012  p31205 1.cpl   NO
004  wi00962211      ISS1:1OF1       p31580_1  11/10/2012  p31580_1.cpl   NO
005  wi00877592      ISS1:1OF1       p30880 1  11/10/2012  p30880 1.cpl   NO
006  wi00839134      ISS1:1OF1       p30698_1  11/10/2012  p30698_1.cpl   YES
007  wi00984888      ISS1:1OF1       p31795_1  11/10/2012  p31795_1.cpl   NO
008  wi00868729      ISS1:1OF1       p31163_1  11/10/2012  p31163_1.cpl   NO
009  wi00886321      ISS1:1OF1       p31009 1  11/10/2012  p31009 1.cpl   NO
010  wi00946282      ISS1:1OF1       p31204_1  11/10/2012  p31204_1.cpl   NO
011  wi00841980      ISS1:1OF1       p30618 1  11/10/2012  p30618 1.cpl   NO
012  wi00968448      ISS1:1OF1       p31648 1  11/10/2012  p31648 1.cpl   YES
013  wi00977002      ISS2:1OF1       p30786_2  11/10/2012  p30786_2.cpl   NO
014  wi00843623      ISS1:1OF1       p30731_1  11/10/2012  p30731_1.cpl   YES
015  wi00958776      ISS1:1OF1       p31542 1  11/10/2012  p31542 1.cpl   YES
017  wi00865477      ISS1:1OF1       p30893 1  11/10/2012  p30893 1.cpl   YES
```


©2012 Avaya Inc. All Rights Reserved.

018	wi00879526	ISS1:1OF1	p31007_1	11/10/2012	p31007_1.cpl	NO
019	wi00894243	ISS1:1OF1	p31087_1	11/10/2012	p31087_1.cpl	NO
020	wi00890475	p30952	p31048_1	11/10/2012	p31048_1.cpl	NO
021	WI00927300	ISS1:1OF1	p30999_1	11/10/2012	p30999_1.cpl	NO
022	wi00856991	ISS1:1OF1	p17588_1	11/10/2012	p17588_1.cpl	NO
023	wi00688381	ISS1:1OF1	p30104_1	11/10/2012	p30104_1.cpl	NO
024	wi00881777	ISS1:1OF1	p25747_1	11/10/2012	p25747_1.cpl	NO
025	WI00853473	ISS1:1OF1	p30625_1	11/10/2012	p30625_1.cpl	NO
026	wi00855423	ISS1:1OF1	p31328_1	11/10/2012	p31328_1.cpl	YES
027	wi00943172	ISS1:1OF1	p31402_1	11/10/2012	p31402_1.cpl	NO
028	wi00865477	ISS1:1OF1	p30898_1	11/10/2012	p30898_1.cpl	YES
029	wi00850521	ISS1:1OF1	p30709_1	11/10/2012	p30709_1.cpl	YES
030	wi00898327	ISS1:1OF1	p31136_1	11/10/2012	p31136_1.cpl	NO
031	wi00871739	ISS1:1OF1	p30856_1	11/10/2012	p30856_1.cpl	NO
032	wi00984178	ISS1:1OF1	p31786_1	11/10/2012	p31786_1.cpl	NO
033	wi00839821	ISS1:1OF1	p30619_1	11/10/2012	p30619_1.cpl	NO
034	wi00854130	ISS1:1OF1	p30443_1	11/10/2012	p30443_1.cpl	NO
035	wi00871969	ISS1:1OF1	p30768_1	11/10/2012	p30768_1.cpl	NO
036	wi00973241	ISS1:1OF1	p31715_1	11/10/2012	p31715_1.cpl	NO
037	wi00946876	ISS1:1OF1	p31430_1	11/10/2012	p31430_1.cpl	NO
038	wi01008943	ISS1:1OF1	p31382_1	11/10/2012	p31382_1.cpl	NO
039	wi00969890	ISS1:1OF1	p31664_1	11/10/2012	p31664_1.cpl	YES
040	wi00937672	ISS1:1OF1	p31276_1	11/10/2012	p31276_1.cpl	NO
041	wi00875425	ISS1:1OF1	p30943_1	11/10/2012	p30943_1.cpl	NO
042	wi00862574	iss1:1of1	p30870_1	11/10/2012	p30870_1.cpl	NO
043	wi00859499	ISS1:1OF1	p30694_1	11/10/2012	p30694_1.cpl	NO
044	wi00925208	ISS1:1OF1	p30986_1	11/10/2012	p30986_1.cpl	NO
045	wi00965285	ISS1:1OF1	p31476_1	11/10/2012	p31476_1.cpl	NO
046	wi00900668	ISS1:1OF1	p30456_1	11/10/2012	p30456_1.cpl	NO
047	wi00967509	ISS1:1OF1	p31294_1	11/10/2012	p31294_1.cpl	NO
048	wi00879322	ISS1:1OF1	p30954_1	11/10/2012	p30954_1.cpl	NO
049	wi00976209	ISS1:1OF1	p31717_1	11/10/2012	p31717_1.cpl	YES
050	wi00956788	ISS1:1OF1	p31638_1	11/10/2012	p31638_1.cpl	NO
051	wi00865477	ISS1:1OF1	p30894_1	11/10/2012	p30894_1.cpl	YES
052	wi00991523	ISS1:1OF1	p31603_1	11/10/2012	p31603_1.cpl	NO
053	wi00865477	ISS1:1OF1	p30892_1	11/10/2012	p30892_1.cpl	YES
054	wi01007604	ISS1:1OF1	p31983_1	11/10/2012	p31983_1.cpl	NO
055	wi00931028	ISS1:1OF1	p31354_1	11/10/2012	p31354_1.cpl	YES
056	wi00932948	ISS1:1OF1	p31077_1	11/10/2012	p31077_1.cpl	NO
057	wi01001911	ISS1:1OF1	p31920_1	11/10/2012	p31920_1.cpl	NO
058	wi00838073	ISS1:1OF1	p30588_1	11/10/2012	p30588_1.cpl	NO
059	wi00852365	ISS1:1OF1	p30707_1	11/10/2012	p30707_1.cpl	NO
060	wi00927321	ISS1:1OF1	p31286_1	11/10/2012	p31286_1.cpl	YES
061	wi00937114	ISS1:1OF1	p31310_1	11/10/2012	p31310_1.cpl	NO
062	wi00877367	ISS1:1OF1	p30534_1	11/10/2012	p30534_1.cpl	NO
063	wi00900096	ISS1:1OF1	p31006_1	11/10/2012	p31006_1.cpl	NO
064	wi00905660	ISS1:1OF1	p27968_1	11/10/2012	p27968_1.cpl	NO
065	wi00925141	ISS1:1OF1	p30802_1	11/10/2012	p30802_1.cpl	NO
066	wi00943748	ISS1:1OF1	p31516_1	11/10/2012	p31516_1.cpl	NO
067	wi00827950	ISS2:1OF1	p30471_2	11/10/2012	p30471_2.cpl	NO
068	wi00930649	ISS1:1OF1	p31570_1	11/10/2012	p31570_1.cpl	NO
069	wi00897279	ISS1:1OF1	p31129_1	11/10/2012	p31129_1.cpl	NO
070	wi00961267	ISS1:1OF1	p30288_1	11/10/2012	p30288_1.cpl	NO
071	wi00936714	ISS1:1OF1	p31379_1	11/10/2012	p31379_1.cpl	NO
072	wi00906022	ISS1:1OF1	p31202_1	11/10/2012	p31202_1.cpl	NO
073	wi00852389	ISS1:1OF1	p30641_1	11/10/2012	p30641_1.cpl	NO
074	wi00857566	ISS1:1OF1	p30766_1	11/10/2012	p30766_1.cpl	NO
075	wi00932204	ISS2:1OF1	p31305_2	11/10/2012	p31305_2.cpl	NO
077	wi00891621	ISS1:1OF1	p31037_1	11/10/2012	p31037_1.cpl	NO
078	wi00957235	ISS1:1OF1	p31798_1	11/10/2012	p31798_1.cpl	NO
079	wi00948274	ISS1:1OF1	p31365_1	11/10/2012	p31365_1.cpl	NO
080	wi00923899	ISS1:1OF1	p31270_1	11/10/2012	p31270_1.cpl	NO
081	wi00856410	ISS1:1OF1	p30749_1	11/10/2012	p30749_1.cpl	NO
082	wi00854415	ISS1:1OF1	p30593_1	11/10/2012	p30593_1.cpl	NO
083	wi00896394	ISS1:1OF1	p30807_1	11/10/2012	p30807_1.cpl	NO
084	wi00826075	ISS1:1OF1	p30452_1	11/10/2012	p30452_1.cpl	NO
085	wi00863876	ISS1:1OF1	p30787_1	11/10/2012	p30787_1.cpl	NO
086	wi00880386	ISS1:1OF1	p30977_1	11/10/2012	p30977_1.cpl	NO
087	wi00840590	ISS1:1OF1	p30767_1	11/10/2012	p30767_1.cpl	NO
088	wi00949627	ISS1:1OF1	p31462_1	11/10/2012	p31462_1.cpl	NO

©2012 Avaya Inc. All Rights Reserved.

```
089  wi00842409      ISS1:1OF1       p30621_1  11/10/2012  p30621_1.cpl   NO
090  wi00865477      ISS1:1OF1       p30896_1  11/10/2012  p30896_1.cpl   YES
091  wi00897096      ISS1:1OF1       p30676_1  11/10/2012  p30676_1.cpl   NO
092  wi00899584      ISS1:1OF1       p30809_1  11/10/2012  p30809_1.cpl   NO
093  wi01007960      ISS1:1OF1       p31965_1  11/10/2012  p31965_1.cpl   NO
094  wi00949273      ISS1:1OF1       p31411_1  11/10/2012  p31411_1.cpl   NO
095  wi00839255      ISS1:1OF1       p30591_1  11/10/2012  p30591_1.cpl   NO
096  wi00945997      ISS1:1OF1       p31641_1  11/10/2012  p31641_1.cpl   NO
097  wi00903369      ISS1:1OF1       p31165_1  11/10/2012  p31165_1.cpl   NO
098  wi00875701      ISS1:1OF1       p30942_1  11/10/2012  p30942_1.cpl   NO
099  wi00884699      ISS1:1OF1       p31000_1  11/10/2012  p31000_1.cpl   YES
100  wi00834382      ISS1:1OF1       p30548_1  11/10/2012  p30548_1.cpl   NO
101  wi00960133      ISS2:1OF1       p31557_2  11/10/2012  p31557_2.cpl   NO
102  wi00929140      ISS1:1OF1       p31284_1  11/10/2012  p31284_1.cpl   NO
103  wi00948931      ISS1:1OF1       p31407_1  11/10/2012  p31407_1.cpl   NO
104  wi00887744      ISS2:1OF1       p31026_2  11/10/2012  p31026_2.cpl   NO
105  wi00905600      ISS1:1OF1       p31201_1  11/10/2012  p31201_1.cpl   NO
106  wi00869243      ISS1:1OF1       p30848_1  11/10/2012  p30848_1.cpl   NO
107  WI00854150      ISS1:1OF1       p30468_1  11/10/2012  p30468_1.cpl   NO
108  wi00897176      ISS1:1OF1       p30418_1  11/10/2012  p30418_1.cpl   NO
109  wi00903381      ISS1:1OF1       p30421_1  11/10/2012  p30421_1.cpl   NO
110  wi00950575      ISS1:1OF1       p31724_1  11/10/2012  p31724_1.cpl   NO
111  wi00908598      ISS1:1OF1       p31235_1  11/10/2012  p31235_1.cpl   NO
112  wi00903437      ISS1:1OF1       p31167_1  11/10/2012  p31167_1.cpl   NO
113  wi00900766      ISS1:1OF1       p31159_1  11/10/2012  p31159_1.cpl   NO
114  wi00946558      ISS1:1OF1       p31358_1  11/10/2012  p31358_1.cpl   NO
115  wi00932958      ISS1:1OF1       p31115_1  11/10/2012  p31115_1.cpl   NO
116  wi00895090      ISS1:1OF1       p31105_1  11/10/2012  p31105_1.cpl   NO
117  wi00824257      ISS1:1OF1       p30447_1  11/10/2012  p30447_1.cpl   NO
118  wi00895181      ISS1:1OF1       p31106_1  11/10/2012  p31106_1.cpl   NO
119  WI00928455      ISS1:1OF1       p31297_1  11/10/2012  p31297_1.cpl   NO
120  wi00832106      ISS1:1OF1       p30550_1  11/10/2012  p30550_1.cpl   NO
121  wi00953900      ISS1:1OF1       p31494_1  11/10/2012  p31494_1.cpl   NO
122  wi00942734      ISS1:1OF1       p31409_1  11/10/2012  p31409_1.cpl   NO
123  wi00986337      ISS1:1OF1       p31803_1  11/10/2012  p31803_1.cpl   NO
124  wi00882293      ISS1:1OF1       p31010_1  11/10/2012  p31010_1.cpl   NO
125  WI00843571      ISS1:1OF1       p30627_1  11/10/2012  p30627_1.cpl   NO
126  wi00835294      ISS1:1OF1       p30565_1  11/10/2012  p30565_1.cpl   NO
127  WI00836292      ISS1:1OF1       p30554_1  11/10/2012  p30554_1.cpl   NO
128  wi00969581      ISS1:1OF1       p31661_1  11/10/2012  p31661_1.cpl   YES
129  wi00921295      ISS1:1OF1       p31265_1  11/10/2012  p31265_1.cpl   NO
130  wi00964006      ISS1:1OF1       p31595_1  11/10/2012  p31595_1.cpl   YES
131  WI00836334      ISS1:1OF1       p30481_1  11/10/2012  p30481_1.cpl   NO
132  wi00858335      ISS1:1OF1       p30819_1  11/10/2012  p30819_1.cpl   NO
133  wi00859123      ISS1:1OF1       p30648_1  11/10/2012  p30648_1.cpl   NO
134  wi00959820      ISS1:1OF1       p31562_1  11/10/2012  p31562_1.cpl   NO
135  wi00905297      ISS1:1OF1       p31195_1  11/10/2012  p31195_1.cpl   NO
136  wi00907697      ISS1:1OF1       p31227_1  11/10/2012  p31227_1.cpl   NO
137  wi00951427      ISS1:1OF1       p31478_1  11/10/2012  p31478_1.cpl   NO
138  wi00883604      ISS1:1OF1       p30973_1  11/10/2012  p30973_1.cpl   NO
139  wi00962955      ISS1:1OF1       p31585_1  11/10/2012  p31585_1.cpl   NO
140  wi00860279      ISS1:1OF1       p30789_1  11/10/2012  p30789_1.cpl   NO
141  wi00909476      ISS1:1OF1       p31340_1  11/10/2012  p31340_1.cpl   NO
142  wi00925218      ISS1:1OF1       p30675_1  11/10/2012  p30675_1.cpl   NO
143  wi00836182      ISS1:1OF1       p30450_1  11/10/2012  p30450_1.cpl   NO
144  wi00841273      ISS1:1OF1       p30713_1  11/10/2012  p30713_1.cpl   NO
145  WI00889786      ISS1:1OF1       p30750_1  11/10/2012  p30750_1.cpl   NO
146  wi00894443      ISS1:1OF1       p31093_1  11/10/2012  p31093_1.cpl   NO
147  wi00896420      ISS1:1OF1       p30867_1  11/10/2012  p30867_1.cpl   NO
148  wi00971029      ISS1:1OF1       p31794_1  11/10/2012  p31794_1.cpl   NO
149  wi00955753      ISS1:1OF1       p31733_1  11/10/2012  p31733_1.cpl   NO
150  wi00968531      ISS1:1OF1       p31645_1  11/10/2012  p31645_1.cpl   NO
151  wi00930864      ISS1:1OF1       p31325_1  11/10/2012  p31325_1.cpl   NO
152  wi00957252      ISS1:1OF1       p31530_1  11/10/2012  p31530_1.cpl   NO
153  wi00880836      ISS1:1OF1       p30976_1  11/10/2012  p30976_1.cpl   NO
154  wi00959457      ISS1:1OF1       p31551_1  11/10/2012  p31551_1.cpl   NO
155  wi00896680      ISS1:1OF1       p30357_1  11/10/2012  p30357_1.cpl   NO
156  wi00856702      ISS1:1OF1       p30573_1  11/10/2012  p30573_1.cpl   NO
157  wi00897082      ISS1:1OF1       p31124_1  11/10/2012  p31124_1.cpl   NO
158  wi00853178      ISS1:1OF1       p30719_1  11/10/2012  p30719_1.cpl   NO
```


©2012 Avaya Inc. All Rights Reserved.

159	wi00938555	ISS1:1OF1	p30881_1	11/10/2012	p30881_1.cpl	YES
160	WI00839794	ISS1:1OF1	p28647_1	11/10/2012	p28647_1.cpl	NO
161	wi00965838	ISS1:1OF1	p31623_1	11/10/2012	p31623_1.cpl	NO
162	wi00977393	ISS1:1OF1	p31744_1	11/10/2012	p31744_1.cpl	YES
163	wi00959284	ISS1:1OF1	p31531_1	11/10/2012	p31531_1.cpl	NO
164	wi00968353	ISS1:1OF1	p31412_1	11/10/2012	p31412_1.cpl	NO
165	wi00998121	ISS1:1OF1	p31897_1	11/10/2012	p31897_1.cpl	NO
166	wi00968157	ISS1:1OF1	p31637_1	11/10/2012	p31637_1.cpl	NO
167	wi00967510	ISS1:1OF1	p31147_1	11/10/2012	p31147_1.cpl	NO
168	wi00949410	ISS1:1OF1	p31248_1	11/10/2012	p31248_1.cpl	NO
169	wi00969039	ISS1:1OF1	p31643_1	11/10/2012	p31643_1.cpl	NO
170	wi00959463	ISS1:1OF1	p31528_1	11/10/2012	p31528_1.cpl	NO
171	wi00983505	ISS1:1OF1	p31758_1	11/10/2012	p31758_1.cpl	NO
172	wi00924886	ISS1:1OF1	p31062_1	11/10/2012	p31062_1.cpl	YES
173	wi00969208	ISS1:1OF1	p31656_1	11/10/2012	p31656_1.cpl	NO
174	wi00974272	ISS1:1OF1	p31690_1	11/10/2012	p31690_1.cpl	YES
175	wi00988285	ISS1:1OF1	p31824_1	11/10/2012	p31824_1.cpl	NO
176	wi00975659	ISS1:1OF1	p31707_1	11/10/2012	p31707_1.cpl	NO
177	wi00960809	ISS1:1OF1	p31564_1	11/10/2012	p31564_1.cpl	NO
178	wi00936935	ISS1:1OF1	p31362_1	11/10/2012	p31362_1.cpl	NO
179	wi01012229	ISS1:1OF1	p31993_1	11/10/2012	p31993_1.cpl	NO
180	wi00989828	ISS1:1OF1	p31836_1	11/10/2012	p31836_1.cpl	NO
182	wi00985760	ISS1:1OF1	p31913_1	11/10/2012	p31913_1.cpl	NO
183	wi01003896	ISS1:1OF1	p31631_1	11/10/2012	p31631_1.cpl	NO
184	wi00978064	ISS1:1OF1	p31760_1	11/10/2012	p31760_1.cpl	NO
185	wi00996889	ISS1:1OF1	p31933_1	11/10/2012	p31933_1.cpl	NO
186	wi00991907	iss1:1of1	p31907_1	11/10/2012	p31907_1.cpl	NO
187	wi01005653	ISS1:1OF1	p31952_1	11/10/2012	p31952_1.cpl	NO
188	wi01005513	ISS1:1OF1	p31951_1	11/10/2012	p31951_1.cpl	NO
189	wi00967512	ISS1:1OF1	p31384_1	11/10/2012	p31384_1.cpl	NO
190	wi01003814	ISS1:1OF1	p31940_1	11/10/2012	p31940_1.cpl	NO
191	wi00984652	ISS1:1OF1	p31792_1	11/10/2012	p31792_1.cpl	NO
192	wi00967514	ISS1:1OF1	p31351_1	11/10/2012	p31351_1.cpl	NO
193	wi00978818	ISS1:1OF1	p31919_1	11/10/2012	p31919_1.cpl	NO
194	WI00980321	ISS1:1OF1	p31912_1	11/10/2012	p31912_1.cpl	YES
195	wi00999802	ISS1:1OF1	p31577_1	11/10/2012	p31577_1.cpl	NO
196	wi01008316	ISS1:1OF1	p32026_1	11/10/2012	p32026_1.cpl	YES
197	wi01003384	ISS1:1OF1	p31479_1	11/10/2012	p31479_1.cpl	NO
198	wi01003999	ISS1:1OF1	p31946_1	11/10/2012	p31946_1.cpl	YES
199	wi01011078	ISS1:1OF1	p31996_1	11/10/2012	p31996_1.cpl	NO
200	wi01016398	ISS1:1OF1	p32019_1	11/10/2012	p32019_1.cpl	NO
201	wi00973270	ISS1:1OF1	p31751_1	11/10/2012	p31751_1.cpl	NO
202	wi00981711	ISS1:1OF1	p31766_1	11/10/2012	p31766_1.cpl	NO
203	wi00977978	ISS1:1OF1	p31831_1	11/10/2012	p31831_1.cpl	NO
204	wi00992974	ISS1:1OF1	p31889_1	11/10/2012	p31889_1.cpl	NO
205	wi00980476	ISS1:1OF1	p31387_1	11/10/2012	p31387_1.cpl	NO
206	wi01008106	ISS1:1OF1	p31861_1	11/10/2012	p31861_1.cpl	NO
207	wi00906350	ISS1:1OF1	p31219_1	11/10/2012	p31219_1.cpl	NO
208	wi01006063	ISS1:1OF1	p31957_1	11/10/2012	p31957_1.cpl	NO
209	wi00971980	ISS1:1OF1	p31863_1	11/10/2012	p31863_1.cpl	NO
210	wi01020959	ISS1:1OF1	p32062_1	11/10/2012	p32062_1.cpl	NO
211	wi01011537	ISS1:1OF1	p32024_1	11/10/2012	p32024_1.cpl	NO
212	wi01008505	ISS1:1OF1	p31968_1	11/10/2012	p31968_1.cpl	NO
213	wi01014835	ISS1:1OF1	p32015_1	11/10/2012	p32015_1.cpl	NO
214	wi00983007	ISS1:1OF1	p31778_1	11/10/2012	p31778_1.cpl	YES
215	wi00987424	ISS1:1OF1	p31815_1	11/10/2012	p31815_1.cpl	NO
216	wi00997559	ISS1:1OF1	p31898_1	11/10/2012	p31898_1.cpl	NO
217	wi01012638	ISS1:1OF1	p32008_1	11/10/2012	p32008_1.cpl	NO
218	wi00985153	ISS1:1OF1	p31859_1	11/10/2012	p31859_1.cpl	NO
219	wi00979591	ISS1:1OF1	p31746_1	11/10/2012	p31746_1.cpl	NO
220	wi00978892	ISS1:1OF1	p31894_1	11/10/2012	p31894_1.cpl	NO
221	wi00996639	ISS1:1OF1	p31886_1	11/10/2012	p31886_1.cpl	NO
222	wi00994044	ISS1:1OF1	p31871_1	11/10/2012	p31871_1.cpl	NO
223	wi00991892	ISS1:1OF1	p31853_1	11/10/2012	p31853_1.cpl	NO
224	wi00974856	ISS1:1OF1	p31823_1	11/10/2012	p31823_1.cpl	NO
225	wi00993377	ISS1:1OF1	p31860_1	11/10/2012	p31860_1.cpl	NO
226	wi00982566	ISS1:1OF1	p31774_1	11/10/2012	p31774_1.cpl	NO
227	wi00993743	ISS1:1OF1	p31865_1	11/10/2012	p31865_1.cpl	NO
228	wi00944019	ISS1:1OF1	p31874_1	11/10/2012	p31874_1.cpl	NO
229	wi00998328	ISS1:1OF1	p31899_1	11/10/2012	p31899_1.cpl	NO

©2012 Avaya Inc. All Rights Reserved.

```
230  wi01008188      ISS1:1OF1       p32020 1  11/10/2012  p32020 1.cpl   NO
231  wi00987089      ISS1:1OF1       p31809 1  11/10/2012  p31809 1.cpl   NO
232  wi00979414      ISS1:1OF1       p31748_1  11/10/2012  p31748_1.cpl   YES
233  wi01006811      ISS1:1OF1       p31967_1  11/10/2012  p31967_1.cpl   YES
234  wi01012289      p31274          p31999_1  11/10/2012  p31999_1.cpl   NO
235  wi00971209      ISS1:1OF1       p31750 1  11/10/2012  p31750 1.cpl   NO
236  wi00997316      ISS1:1OF1       p31870_1  11/10/2012  p31870_1.cpl   NO
237  wi00990993      ISS1:1OF1       p31825 1  11/10/2012  p31825 1.cpl   NO
238  wi00977436      ISS1:1OF1       p31834_1  11/10/2012  p31834_1.cpl   NO
239  wi01001938      ISS1:1OF1       p31921_1  11/10/2012  p31921_1.cpl   YES
240  wi01012423      ISS1:1OF1       p26155_1  11/10/2012  p26155_1.cpl   NO
241  wi01010472      ISS1:1OF1       p31975_1  11/10/2012  p31975_1.cpl   NO
242  wi01000796      ISS1:1OF1       p31800_1  11/10/2012  p31800_1.cpl   NO
243  wi00981928      ISS1:1OF1       p31869 1  11/10/2012  p31869 1.cpl   NO
244  wi00992921      ISS1:1OF1       p31878_1  11/10/2012  p31878_1.cpl   NO
245  wi01001588      ISS1:1OF1       p31976_1  11/10/2012  p31976_1.cpl   NO
246  wi00976951      ISS1:1OF1       p30112_1  11/10/2012  p30112_1.cpl   NO
MDP>LAST SUCCESSFUL MDP REFRESH :2012-10-02 13:46:39(Local Time)
MDP>USING DEPLIST ZIP FILE DOWNLOADED :2012-08-20 11:29:05(est)
```

Avaya Communication Server 1000E signaling server service updates

```
Product Release: 7.50.17.00
In system patches: 1
PATCH#  NAME       IN_SERVICE   DATE      SPECINS  TYPE   RPM
2       p27159_1   Yes          13/04/12  NO       FRU    cs1000-pi-control-1.00.00.00-00.noarch

In System service updates: 31
PATCH#  IN_SERVICE   DATE       SPECINS   REMOVABLE   NAME
0       Yes          09/10/12   NO        YES         cs1000-vtrk-7.50.17.16-105.i386.000
1       Yes          02/10/12   NO        YES         cs1000-patchWeb-7.50.17.16-9.i386.000
3       Yes          20/01/12   NO        YES         cs1000-dbcom-7.50.17-02.i386.000
5       Yes          20/01/12   NO        YES         cs1000-shared-pbx-7.50.17.16-1.i386.000
6       Yes          20/01/12   NO        YES         cs1000-kcv-7.50.17.16-1.i386.000
7       Yes          20/01/12   NO        YES         cs1000-nrsmWebService-7.50.17.16-1.i386.000
8       Yes          02/10/12   NO        YES         cs1000-linuxbase-7.50.17.16-11.i386.000
9       Yes          02/10/12   YES       YES         cs1000-baseWeb-7.50.17.16-2.i386.000
10      Yes          20/01/12   NO        YES         cs1000-ipsec-7.50.17.16-1.i386.000
11      Yes          02/10/12   NO        yes         avaya-cs1000-cnd-4.0.20-00.i386.000
12      Yes          02/10/12   NO        YES         cs1000-pd-7.50.17.16-1.i386.000
13      Yes          02/10/12   NO        YES         cs1000-ncs-7.50.17.16-1.i386.000
14      Yes          20/01/12   NO        YES         ipsec-tools-0.6.5-14.el5.3 avaya 1.i386.000
15      Yes          20/01/12   NO        YES         spiritAgent-6.1-1.0.0.108.208.i386.000
17      Yes          02/10/12   NO        YES         cs1000-EmCentralLogic-7.50.17.16-2.i386.000
18      Yes          02/10/12   NO        YES         cs1000-tps-7.50.17.16-21.i386.000
19      Yes          02/10/12   NO        YES         cs1000-ftrpkg-7.50.17.16-10.i386.000
20      Yes          02/10/12   NO        YES         cs1000-cs1000WebService_6-0-7.50.17.16-
1.i386.000
21      Yes          02/10/12   NO        YES         cs1000-mscMusc-7.50.17.16-11.i386.000
22      Yes          02/10/12   NO        YES         cs1000-mscAnnc-7.50.17.16-10.i386.000
24      Yes          27/03/12   NO        YES         cs1000-mscTone-7.50.17.16-1.i386.000
27      Yes          02/10/12   NO        YES         cs1000-csoneksvrmgr-7.50.17.16-1.i386.000
30      Yes          27/03/12   NO        YES         cs1000-sps-7.50.17.16-4.i386.000
35      Yes          02/10/12   YES       YES         cs1000-nrsm-7.50.17.16-4.i386.000
36      Yes          02/10/12   NO        YES         cs1000-csmWeb-7.50.17.16-6.i386.000
37      Yes          02/10/12   NO        YES         cs1000-mscConf-7.50.17.16-1.i386.000
38      Yes          02/10/12   NO        YES         cs1000-emWeb_6-0-7.50.17.16-34.i386.000
39      Yes          02/10/12   NO        YES         cs1000-dmWeb-7.50.17.16-5.i386.000
40      Yes          02/10/12   NO        YES         cs1000-Jboss-Quantum-7.50.17.16-30.i386.000
41      Yes          02/10/12   NO        YES         cs1000-bcc-7.50.17.16-75.i386.000
42      Yes          02/10/12   NO        YES         cs1000-emWebLocal_6-0-7.50.17.16-3.i386.000
```

Avaya Communication Server 1000E system software

```
Product Release: 7.50.17.00
Base Applications
   base                        7.50.17     [patched]
```


©2012 Avaya Inc. All Rights Reserved.

```
   NTAFS                        7.50.17
   sm                           7.50.17
   cs1000-Auth                  7.50.17
   Jboss-Quantum                7.50.17     [patched]
   cnd                          n/a         [patched]
   lhmonitor                    7.50.17
   baseAppUtils                 7.50.17     [patched]
   dfoTools                     7.50.17
   nnnm                         7.50.17
   cppmUtil                     7.50.17
   oam-logging                  7.50.17     [patched]
   dmWeb                        n/a         [patched]
   baseWeb                      n/a         [patched]
   ipsec                        n/a         [patched]
   Snmp-Daemon-TrapLib          7.50.17     [patched]
   ISECSH                       7.50.17
   patchWeb                     n/a         [patched]
   EmCentralLogic               n/a         [patched]



Application configuration: CS+SS+NRS+EM
Packages:
CS+SS+NRS+EM
Configuration version:     7.50.17-00
   cs                           7.50.17
   dbcom                        7.50.17     [patched]
   cslogin                      7.50.17
   sigServerShare               7.50.17     [patched]
   csv                          7.50.17
   tps                          7.50.17.16  [patched]
   vtrk                         7.50.17.16  [patched]
   pd                           7.50.17.16  [patched]
   sps                          7.50.17.16  [patched]
   ncs                          7.50.17.16  [patched]
   gk                           7.50.17
   nrsm                         7.50.17     [patched]
   nrsmWebService               7.50.17     [patched]
   managedElementWebService     7.50.17
   EmConfig                     7.50.17
   emWeb 6-0                    7.50.17     [patched]
   emWebLocal_6-0               7.50.17     [patched]
   csmWeb                       7.50.17     [patched]
   bcc                          7.50.17     [patched]
   ftrpkg                       7.50.17     [patched]
   cs1000WebService_6-0         7.50.17     [patched]
   mscAnnc                      7.50.17.16  [patched]
   mscAttn                      7.50.17
   mscConf                      7.50.17.16  [patched]
   mscMusc                      7.50.17.16  [patched]
   mscTone                      7.50.17.16  [patched
```


©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.

©2012 Avaya Inc. All Rights Reserved.