Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Communication Server 1000E R7.6 with Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise R6.2 to support Eircom SIP Trunk Service - Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between an Avaya SIP enabled enterprise solution and Eircom SIP Trunk service. The Avaya solution consists of Avaya Aura® Session Manager and Avaya Communication Server 1000E connected to an Avaya Session Border Controller for Enterprise. Eircom is a member of the Global 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.

1. Introduction

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

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 Communication Server 1000E, Session Manager, and the Avaya SBCE. The enterprise site was configured to use the SIP Trunk service provided by Eircom, with all PSTN traffic transiting via the Eircom SIP Trunk service.

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 calls to the enterprise site from the PSTN were routed to the DDI numbers assigned by Eircom. Incoming PSTN calls were terminated on Digital, UNIStim, SIP and Analog telephones at the enterprise side.
- Outgoing calls from the enterprise site were completed via Eircom to PSTN telephones. Outgoing calls from the enterprise to the PSTN were made from Digital, UNIStim, SIP and Analog telephones.
- Calls were made using G.729 and G.711A codecs.
- Fax calls to/from a group 3 fax machine to a PSTN-connected fax machine using T.38
- DTMF transmission using RFC 2833 with successful IVR menu progression.
- Various call types including: local, long distance, international, toll free (outbound) and directory assistance.
- 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.

2.2. Test Results

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

- The CS1000E default configuration will not allow a blind transfer to be executed (incoming SIP Service Provider trunk to outgoing SIP Service Provider trunk) if the SIP Service Provider in question does 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-7.65.16.22.-4.i386.000.ntl"** or higher be used on all SSG signalling 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 UPDATE method, but rather extends support to those parties that do not. Note that plugin 501 is independent of and does not require the Global Plugin Package 409.
- Mobile X was not tested and is not supported by Eircom.
- 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

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

For technical support on Eircom products please contact Eircom Customer Care at:

- Telephone: 1800 255 255
- Telephone: +353 1 4688530
- Email: servicedesk@eircom.ie

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to Eircom's SIP Trunk service. Located at the Enterprise site is an Avaya SBCE, Session Manager and CS1000E. Endpoints are Avaya 1140 series IP telephones, Avaya 1230 series IP telephones (with Unistim and SIP firmware), Avaya IP Softphones (Avaya 3456 IP Softphone, 2050 IP Softphone 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.

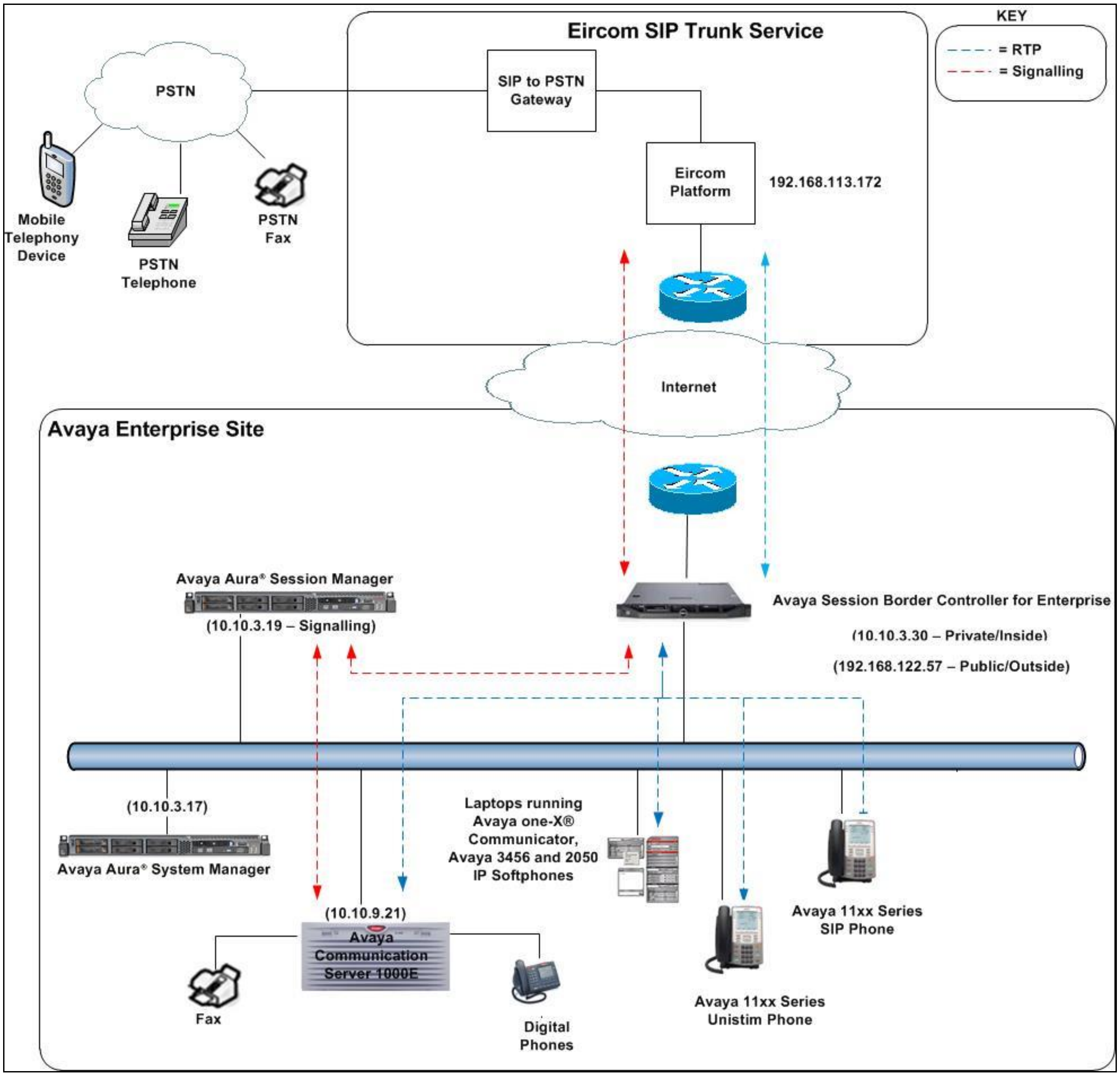


Figure 1: Test Setup Eircom SIP Trunk Service to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment	Software
Dell PowerEdge R620 running Session Manager on VM Version 8	R6.3.9 - 6.3.9.0.639011
Dell PowerEdge R620 running System Manager on VM Version 8	R6.3.9 - Build No. - 6.3.0.8.5682-6.3.8.4417 Software Update Revision No: 6.3.9.1.2538
Avaya Session Border Controller for Enterprise	Version 6.2.1.Q07
Avaya Communication Server 1000E running on CP+PM server as co-resident configuration	Avaya Communication Server 1000E R7.6 Version 7.65.P Deplist: CPL_X21_07_65P All CS1000E patches listed in **Appendix A**
Avaya Communication Server 1000E Media Gateway	CSP Version: MGCC DC01 MSP Version: MGCM AB02 APP Version: MGCA BA18 FPGA Version: MGCF AA22 BOOT Version: MGCB BA18 DBL1 Version: DSP2 AB07
Avaya 1140e and 1230 UNIStim Telephones	FW: 0625C8A
Avaya 1140e and 1230 SIP Telephones	FW: 04.04.10.00.bin
Avaya IP Softphone 3456	Version 2.6 build 53715
Avaya 2050 IP Softphone	Release 4.3.0081
Avaya Analogue Telephone	N/A
Avaya M3904 Digital Telephone	N/A
Eircom Equipment	**Software**
Eircom SIP Trunk	Broadsoft Broadworks rel 19SP1 Ericsson IMS rel 13A AcmePacket SD running on 4500 platform, software release 6.4

5. Configure Avaya Communication Server 1000E

This section describes the steps required to configure Communication Server 1000E for SIP Trunking and also the basic configuration for telephones (analog, SIP and IP phones). SIP trunks are established between CS1000E and Session Manager. SIP trunks are also established between Session Manager and the Avaya SBCE private interface. The Avaya SBCE public interface connects to the Eircom's SIP trunks. Incoming PSTN calls from the Eircom SIP Trunk service traverse the Avaya SBCE and are directed to Session Manager, which directs the calls to CS1000E (see **Figure 1**).

When 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. When CS1000E selects a SIP trunk for outgoing PSTN calls, SIP signalling is directed to Session Manager. Session Manager directs the outbound SIP messages to the Avaya SBCE private interface. The Avaya SBCE public interface manages outgoing SIP sessions onwards to Eircom's SIP trunks.

Specific CS1000E configuration was performed using Element Manager and the system terminal interface. The general installation of the CS1000E, System Manager, Session Manager and Avaya SBCE is presumed to have been previously completed and is not discussed here. Configuration details will be provided as required to draw attention to changes in default system configurations.

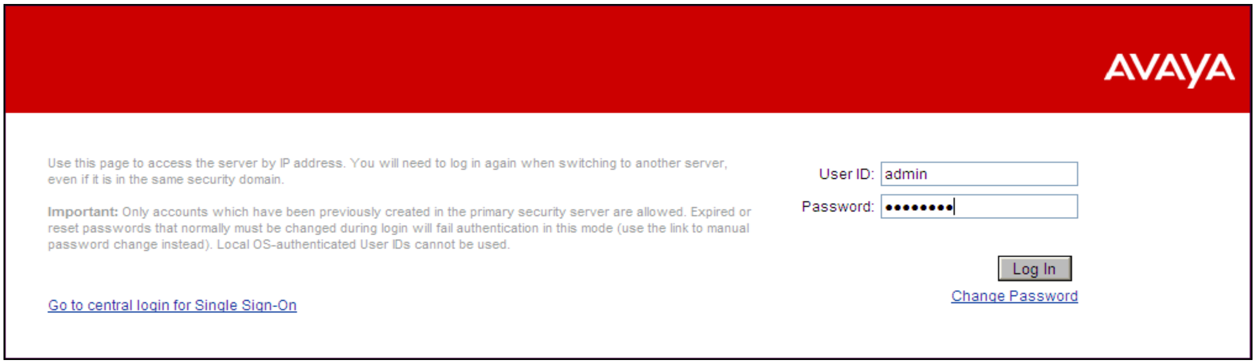
5.1. Logging into the Avaya Communication Server 1000E

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

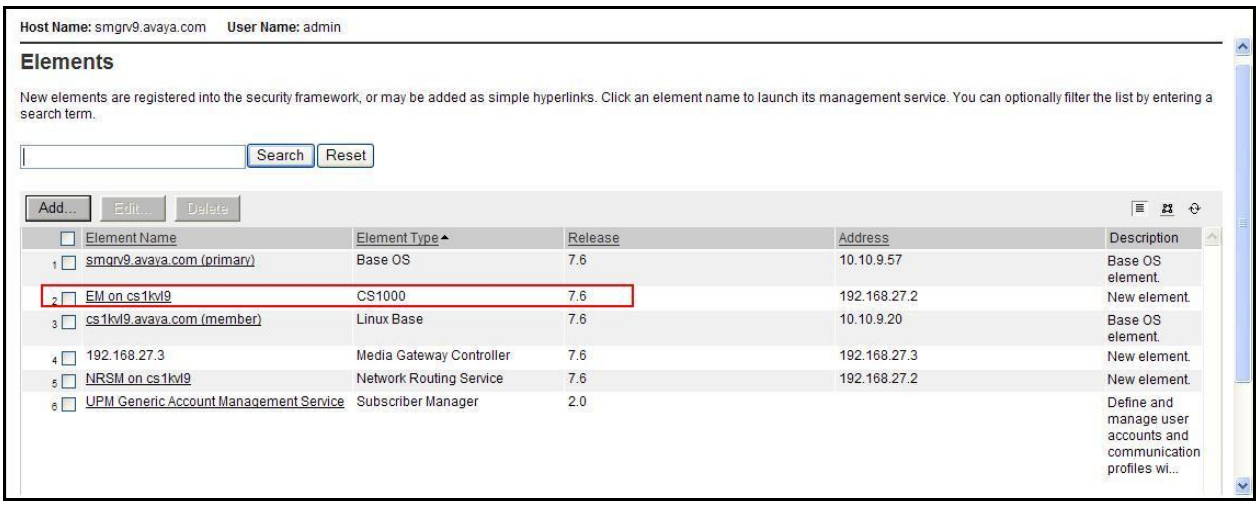
Log in using SSH to the ELAN IP address of the Call Server with a username containing the correct privileges. Once logged in type **csconsole,** this will take the user into the VxWorks shell of the call server. Next type **login**; the user will then be asked to login with correct credentials. Once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

Log in using the web based Avaya Unified Communications Management GUI. Avaya Unified Communications Management GUI may be launched directly via http://<ipaddress> where the relevant <ipaddress> is the TLAN IP address of the CS1000E. Avaya Unified Communications Management can also be implemented on System Manager.

The following screen shows the login screen. Login with the appropriate credentials.



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 cs1kvl9**.



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 the Eircom 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.

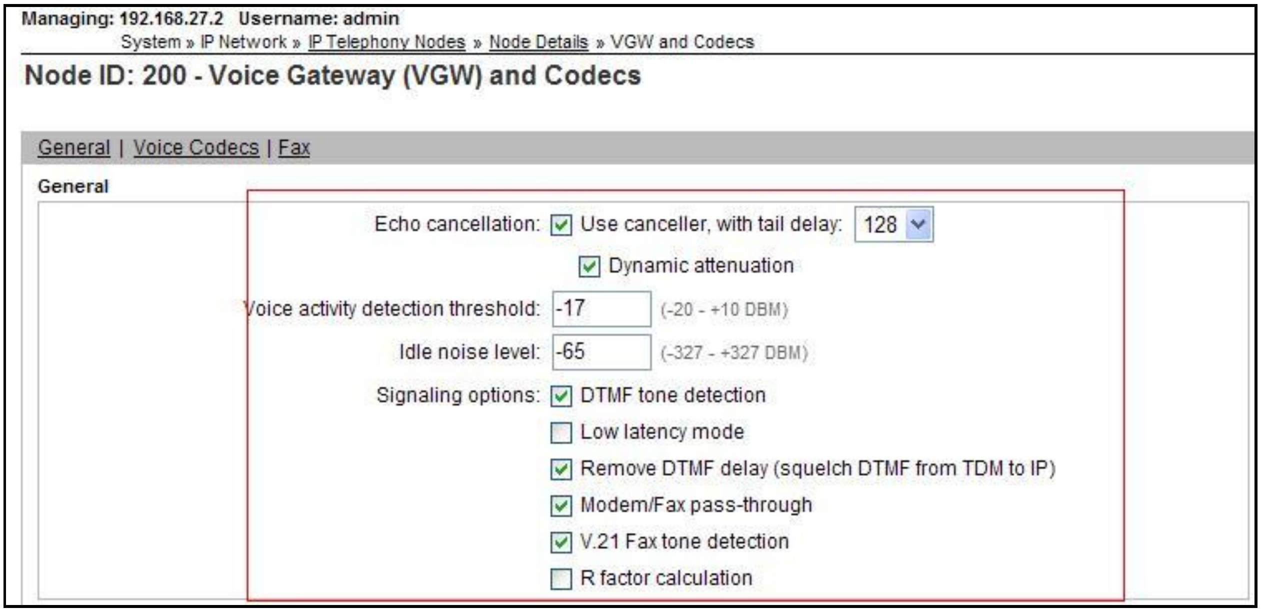
```
System type is - Communication Server 1000E/CP PM
CP PM - Pentium M 1.4 GHz

IPMGs Registered:              4
IPMGs Unregistered:            0
IPMGs Configured/unregistered:  2

TRADITIONAL TELEPHONES   120    LEFT   110    USED    10
DECT USERS                16    LEFT    16    USED     0
IP USERS               10000    LEFT  9954    USED    46
BASIC IP USERS            16    LEFT    13    USED     3
TEMPORARY IP USERS         8    LEFT     8    USED     0
DECT VISITOR USER         16    LEFT    16    USED     0
ACD AGENTS               192    LEFT   185    USED     7
MOBILE EXTENSIONS          8    LEFT     7    USED     1
TELEPHONY SERVICES        16    LEFT    13    USED     3
CONVERGED MOBILE USERS     8    LEFT     8    USED     0
AVAYA SIP LINES           16    LEFT    12    USED     4
THIRD PARTY SIP LINES     16    LEFT    16    USED     0
PCA                       20    LEFT    18    USED     2
ITG ISDN TRUNKS            0    LEFT     0    USED     0
H.323 ACCESS PORTS       524    LEFT   524    USED     0
AST                     6652    LEFT  6640    USED    12
SIP CONVERGED DESKTOPS    16    LEFT    16    USED     0
SIP CTI TR87              16    LEFT     8    USED     8
SIP ACCESS PORTS         524    LEFT   518    USED     6
RAN CON                   90    LEFT    90    USED     0
MUS CON                  120    LEFT   120    USED     0
```

Load Overlay 21 and confirm the customer is setup to use **ISDN** trunks by typing the **PRT** and **NET_DATA** commands as shown below.

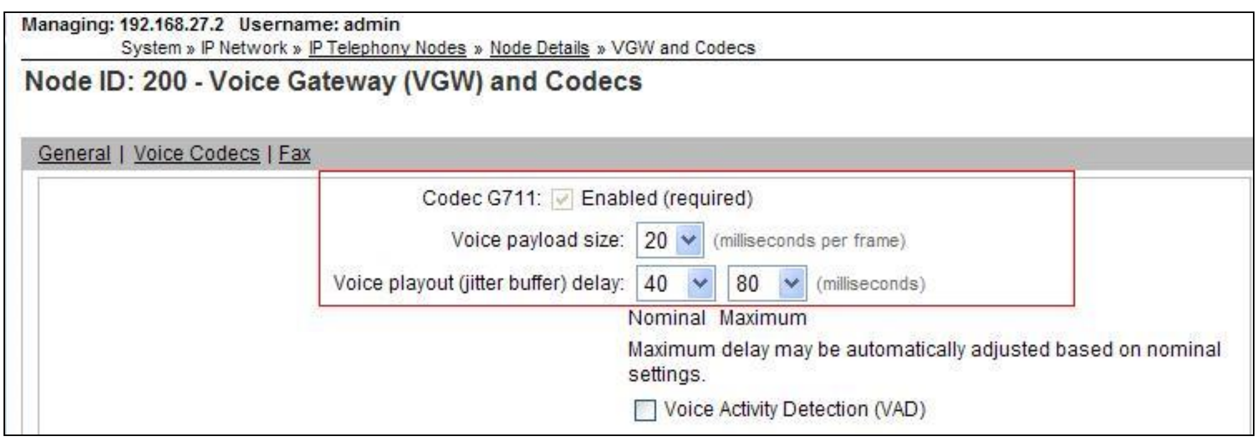
```
REQ: prt
TYPE: net
TYPE NET_DATA
CUST 0

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

5.3. Configure Codecs for Voice and FAX operation

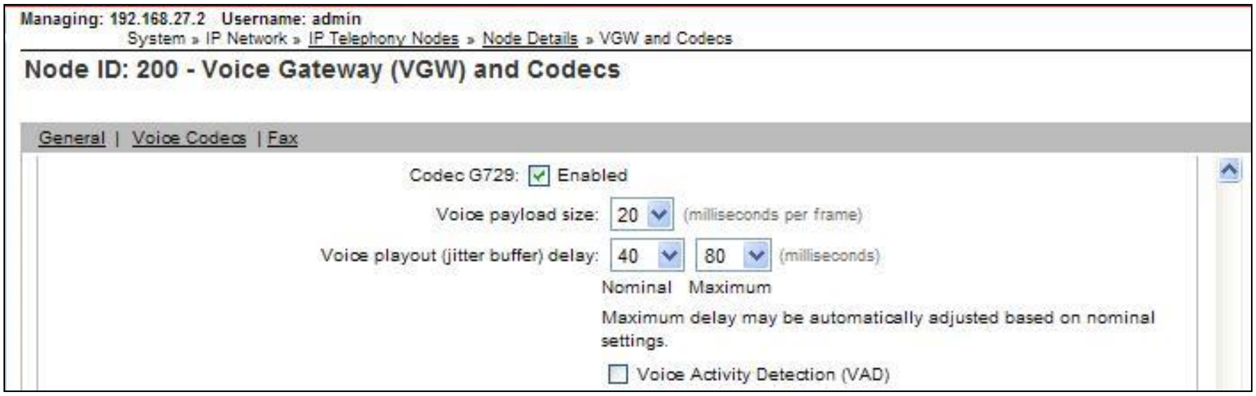
Eircom's SIP Trunk service supports G.711A and G.729 voice codecs. Using the CS1000E Element Manager sidebar, select **Nodes, Servers, Media Cards**. Navigate to the **IP Network → IP Telephony Nodes → Node Details → VGW and Codecs** property page and configure the CS1000E **General** codec settings as in the following screenshots. The values highlighted are required for correct operation. The following screenshot shows the necessary **General** settings.



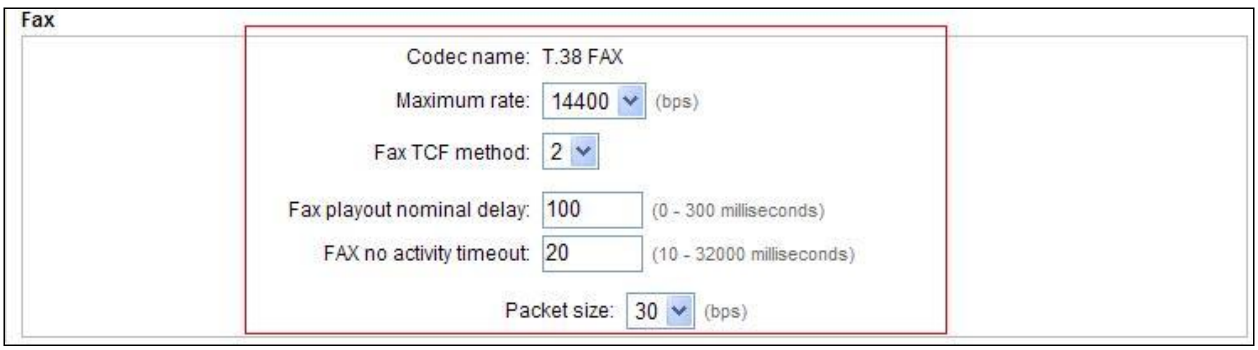
Move down to the Voice Codecs section and configure the G.711 codec settings. The following screenshot shows the G.711 codec settings.



Next, scroll down to the G.729 codec section and configure the settings.

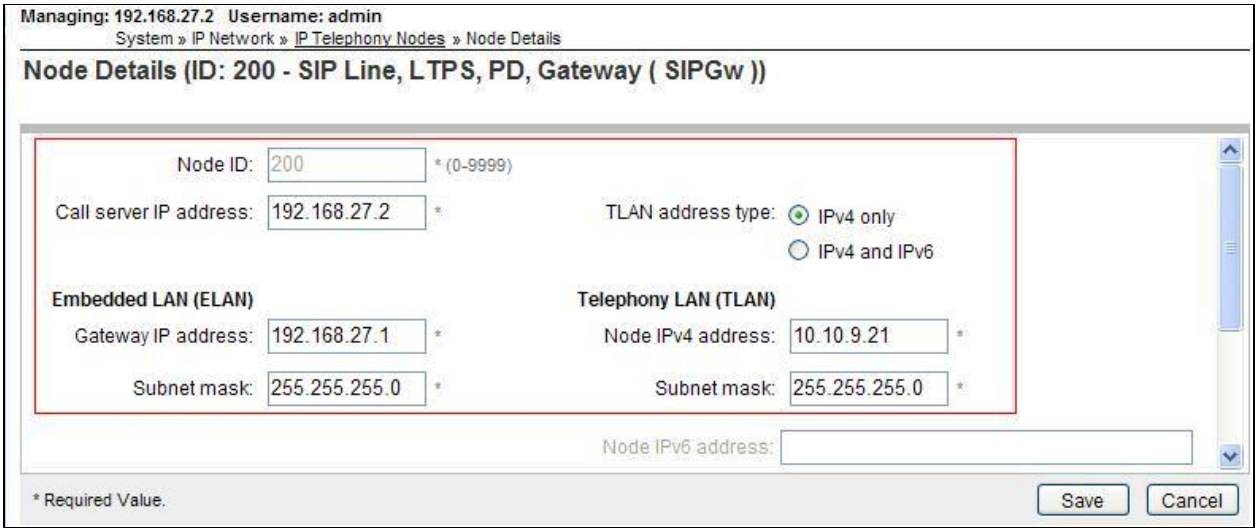


Finally, configure the Fax settings as in the highlighted section of the next screenshot. Click on the **Save** button when finished.



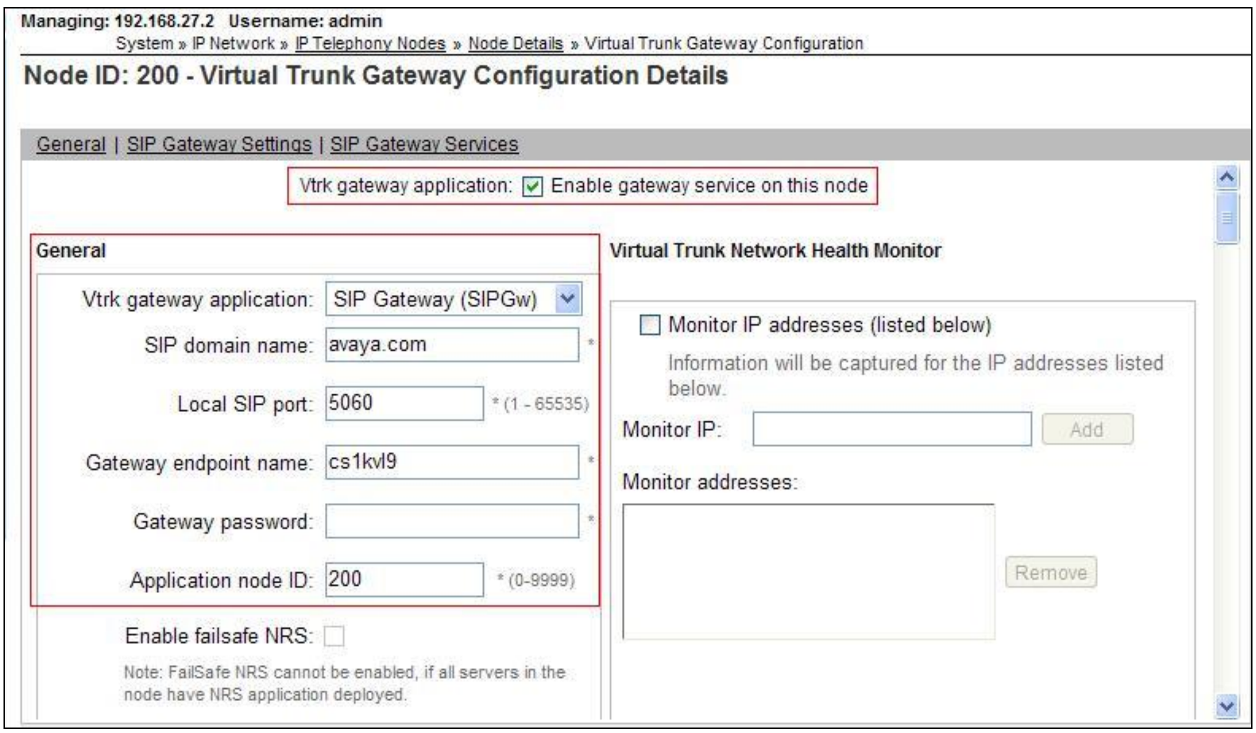
5.4. Virtual Trunk Gateway Configuration

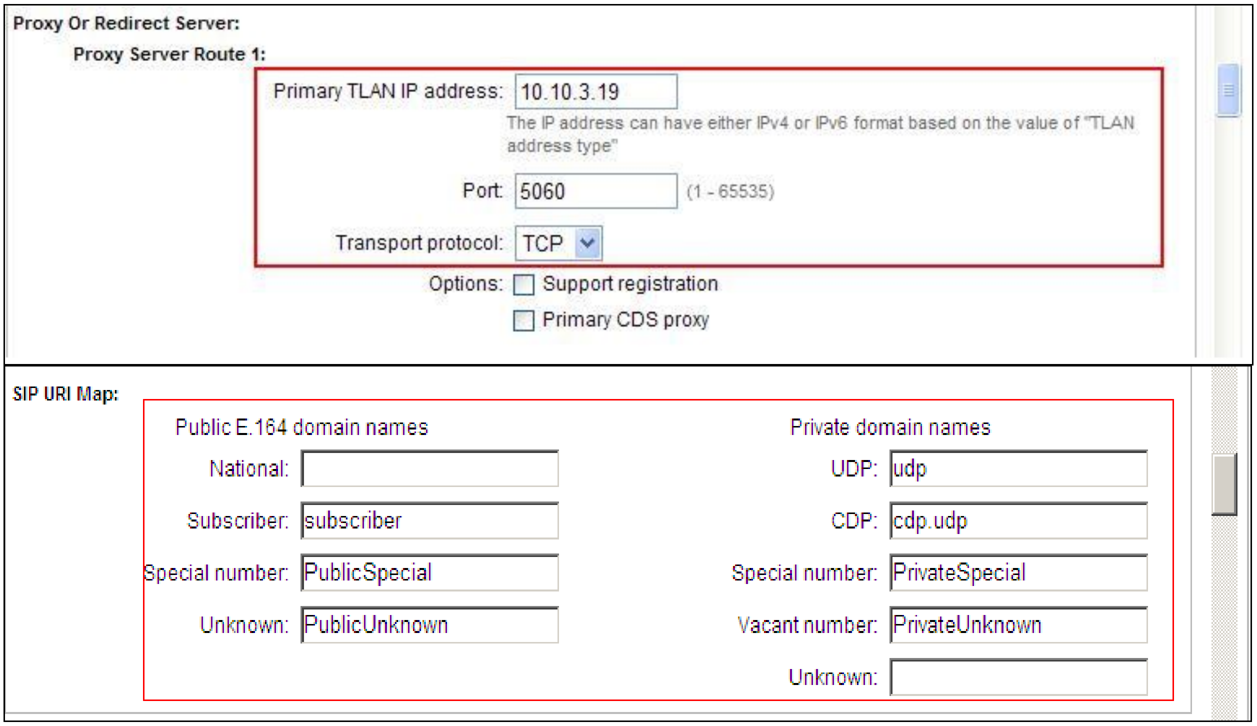
Use CS1000E Element Manager to configure the system node properties. Navigate to the **System → IP Networks → IP Telephony Nodes → Node Details** and verify the highlighted section is completed with the correct IP addresses and subnet masks of the Node. The call server and signaling server have previously been configured with IP addresses. The Node IPv4 address is the IP address that the IP phones use to register. This is also where the SIP trunk connection is made to Session Manager. When an entity link is added in Session Manager for the CS1000E, it is the Node IPv4 address that is used (see **Section 6.5** – Administer SIP Entities for more details).



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 and H.323Gw**.
- **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 Session Manager; in this case **avaya.com**.
- **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 **200**.
- **Proxy or Redirect Server:** Primary TLAN IP address is the Security Module IP address of Session Manager. The **Transport protocol** used for SIP, in this case is **TCP**.
- **SIP URI Map: Public E.164 - National** and **Private - Unknown** are left blank. All other fields in the SIP URI Map are left with default values.

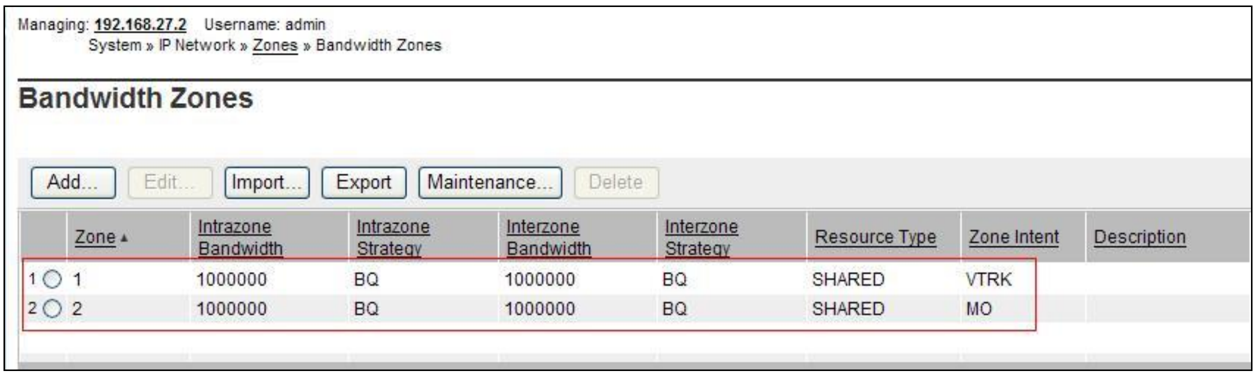



Proxy Or Redirect Server:
Proxy Server Route 1:
Primary TLAN IP address: 10.10.3.19
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"
Port: 5060 (1 - 65535)
Transport protocol: TCP
Options: Support registration
Primary CDS proxy
SIP URI Map:
Public E.164 domain names
National:
Subscriber: subscriber
Special number: PublicSpecial
Unknown: PublicUnknown
Private domain names
UDP: udp
CDP: cdp.udp
Special number: PrivateSpecial
Vacant number: PrivateUnknown
Unknown:

5.5. Configure Bandwidth Zones

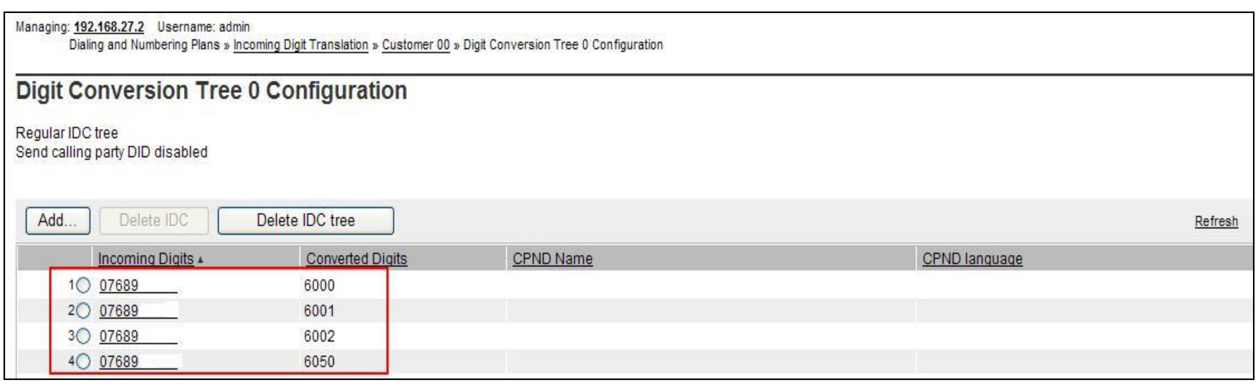
Bandwidth Zones are used for alternate call routing between IP stations and for bandwidth management. SIP trunks require a unique zone, not shared with other resources and best practice dictates that IP telephones and Media Gateways are all placed in separate zones. In the sample configuration SIP trunks use zone 01 and IP and SIP Telephones use zone 02; 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 **Main Office**.

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 Incoming Digit Conversion (IDC) table was configured to translate incoming PSTN numbers to four 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.



5.7. Configure SIP Trunks

Communication Server 1000E virtual trunks will be used for all inbound and outbound PSTN calls to the Eircom SIP Trunk service. Six separate steps are required to configure Communication Server 1000E 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
```

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 **VTRK**. The remaining highlighted values are important for correct SIP trunk operation.

```
Overlay 16
TYPE: RDB
CUST 00
ROUT 1
TYPE RDB
CUST 00
ROUT 1
DES  VIR_TRK
TKTP TIE
NPID_TBL_NUM   0
ESN  NO
RPA  NO
CNVT NO
SAT  NO
RCLS EXT
VTRK YES
ZONE 00001
PCID SIP
CRID NO
NODE 200
DTRK NO
ISDN YES
    MODE ISLD
    DCH  1
    IFC  SL1
    PNI  00000
    NCNA YES
    NCRD YES
    TRO  NO
    FALT NO
    CTYP UKWN
    INAC NO
    ISAR NO
    DAPC NO
MBXR NO
MBXOT NPA
MBXT 0
PTYP ATT
CNDP UKWN
AUTO NO
DNIS NO
DCDR NO
ICOG IAO
SRCH LIN
TRMB YES
STEP
```

```
ACOD 1111
TCPP NO
PII NO
AUXP NO
TARG
CLEN 1
BILN NO
OABS
INST
IDC  YES
DCNO 0
NDNO 0 *
DEXT NO
DNAM NO
SIGO STD
STYP SDAT
MFC  NO
ICIS YES
OGIS YES
TIMR ICF  1920
     OGF  1920
     EOD  13952
     LCT  256
     DSI  34944
     NRD  10112
     DDL  70
     ODT  4096
     RGV  640
     GTO  896
     GTI  896
     SFB  3
     PRPS  800
     NBS  2048
     NBL  4096
     IENB  5
     TFD  0
     VSS  0
     VGD  6
     EESD  1024
SST  5 0
DTD  NO
SCDT NO
2 DT NO
NEDC ORG
FEDC ORG
```

```
CPDC NO
DLTN NO
HOLD 02 02 40
SEIZ 02 02
SVFL 02 02
DRNG NO
CDR  NO
NATL YES
SSL
CFWR NO
IDOP NO
VRAT NO
MUS  YES
MRT  21
PANS YES
RACD NO
MANO NO
FRL  0 0
FRL  1 0
FRL  2 0
FRL  3 0
FRL  4 0
FRL  5 0
FRL  6 0
FRL  7 0
OHQ  NO
OHQT 00
CBQ  NO
AUTH NO
TTBL 0
ATAN NO
OHTD NO
PLEV 2
OPR  NO
ALRM NO
ART  0
PECL NO
DCTI 0
TIDY 1600 100
ATRR NO
TRRL NO
SGRP 0
ARDN NO
CTBL 0
AACR NO
```

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
```

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. **Note: ISPN** is set to **0** as Eircom required a prefix of 0 to be inserted before the dialed number for outbound calls. The value for Digit Manipulation Index (**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 0
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

5.8. Calling Line Identification

This section documents basic configuration relevant to the Eircom configuration. **Load Overlay 15** at system terminal and enter the required values in bold. As shown below, **CLID** is set to **YES** and **ENTRY** is set to **0**. **HNTN** and **HLCL** match the required digits assigned by Eircom and **DIDN** is set to **NO**.

```
Load Overlay 15
TYPE NET_DATA
CUST 0
OPT
AC2
FNP
CLID YES
  SIZE
  INTL
  ENTRY 0
HNTN 07689
  ESA_HLCL
  ESA_INHN NO
  ESA_APDN NO
  HLCL 11010
  DIDN NO
  DIDN_LEN 0
  HLOC
  LSC
  CLASS_FMT DN
```

5.9. 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**. The value for **CFG_ZONE** is the value used in **Section 5.5** for IP and SIP Telephones.

```
Load Overlay 20 IP Telephone configuration
DES  1140
TN   100 0 03 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----
```

```
---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 6000 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME IP1140
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     01 MCR 6000 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
```

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   000 0 09 08  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----
```

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

MLNG ENG
DNDR 0
KEY  00 MCR 6066 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME Digital Set
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     01 MCR 6066 0
        CPND
          CPND_LANG ROMAN
            NAME Digital Set
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     02 DSP
     03 MSB
     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
```

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 fax transmission. A unique value is entered for **DN**, this is the extension number. **DTN** is required if the telephone uses DTMF dialing. Values **FAXA** and **MPTD** configure the port for T.38 Fax transmissions.

```
Overlay 20 – Analog Telephone Configuration
DES  500
TN   100 0 00 03
TYPE 500
CDEN 4D
CUST 0
MRT

ERL 00000
WRLS NO
DN   6004
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 FAXA CNUD CNAD PGND FTTC
     FDSD NOVD CDMR PRED MCDD T87D SBMD PKCH MPTD
PLEV 02
PUID
AACS NO
MLWU_LANG 0
FTR  DCFW 4
```

5.10.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 Communication Server 1000E system terminal and overlay 15 to activate SIP Line services (SLS_DATA), 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**

5.11. Configure SIP Line Telephones

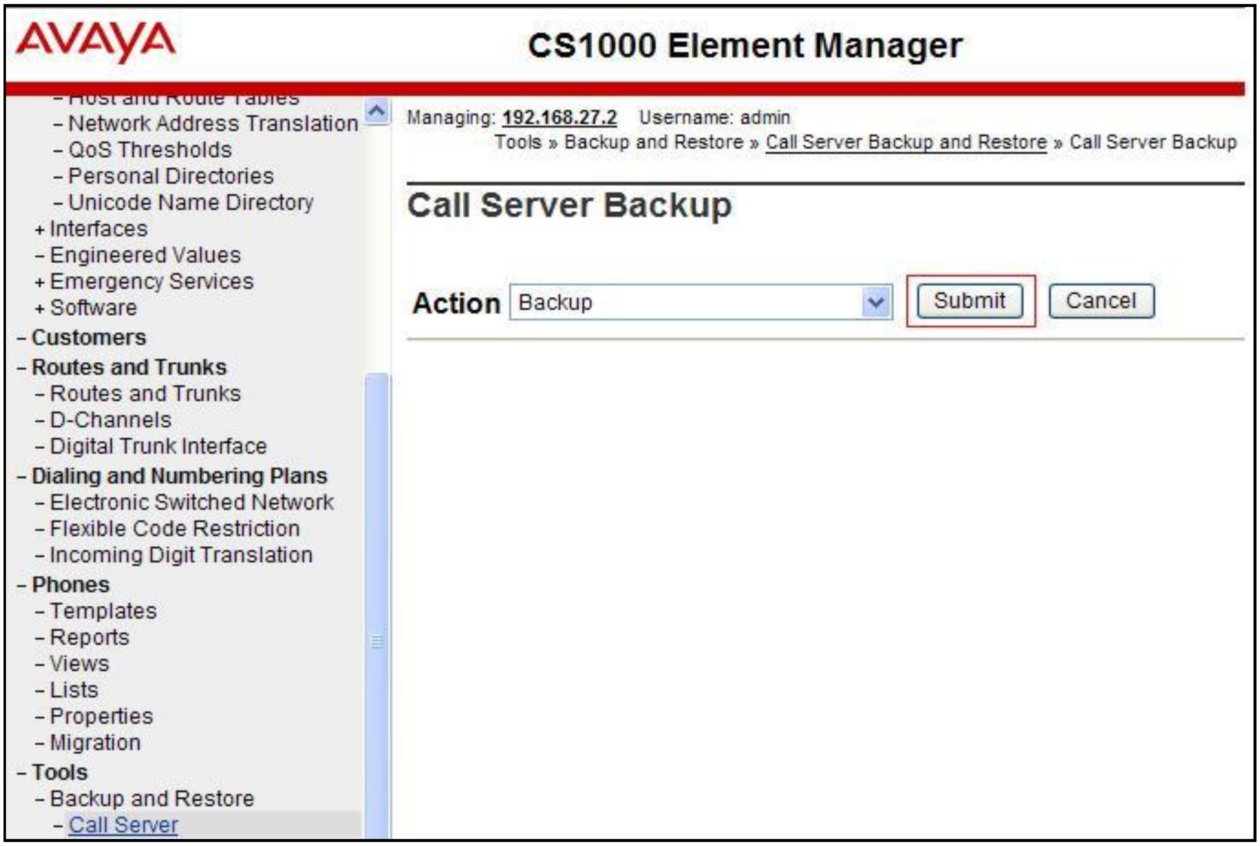
When SIP Line service configuration is completed, use the CS1000E system terminal and **Overlay 20** to add a Universal Extension (UEXT). See the following example of a SIP Line extension. The value for **UXTY** must be **SIPL**. This example is for an Avaya SIP telephone, so the value for **SIPN** is 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 used in **Section 5.5** for IP and SIP Telephones. 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**.

```
Load Overlay 20 – SIP Telephone Configuration
DES  SIPD
TN   100 0 03 3  VIRTUAL
TYPE UEXT
CDEN 8D
CTYP XDLC
CUST 0
UXTY SIPL
MCCL YES
SIPN 1
SIP3 0
FMCL 0
TLSV 0
SIPU 6002
NDID 200
SUPR NO
SUBR DFLT MWI RGA CWI MSB
UXID
NUID
NHTN
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---
```

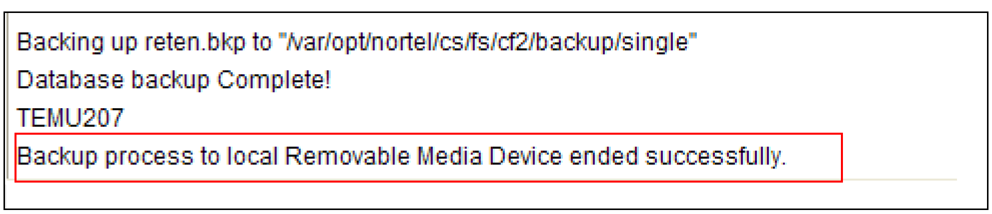
```
---continued from previous page---

     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 MCR 6002 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME Sigma 1140
            XPLN 11
            DISPLAY_FMT FIRST,LAST*
     01 HOT U 116002 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
```

5.12. Save Configuration

Expand **Tools → Backup and Restore** on the left navigation panel and select **Call Server**. Select **Backup** (not shown) and click **Submit** to save configuration changes as shown below.



The 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 Communication Server 1000E is complete.

6. Configuring Avaya Aura® Session Manager

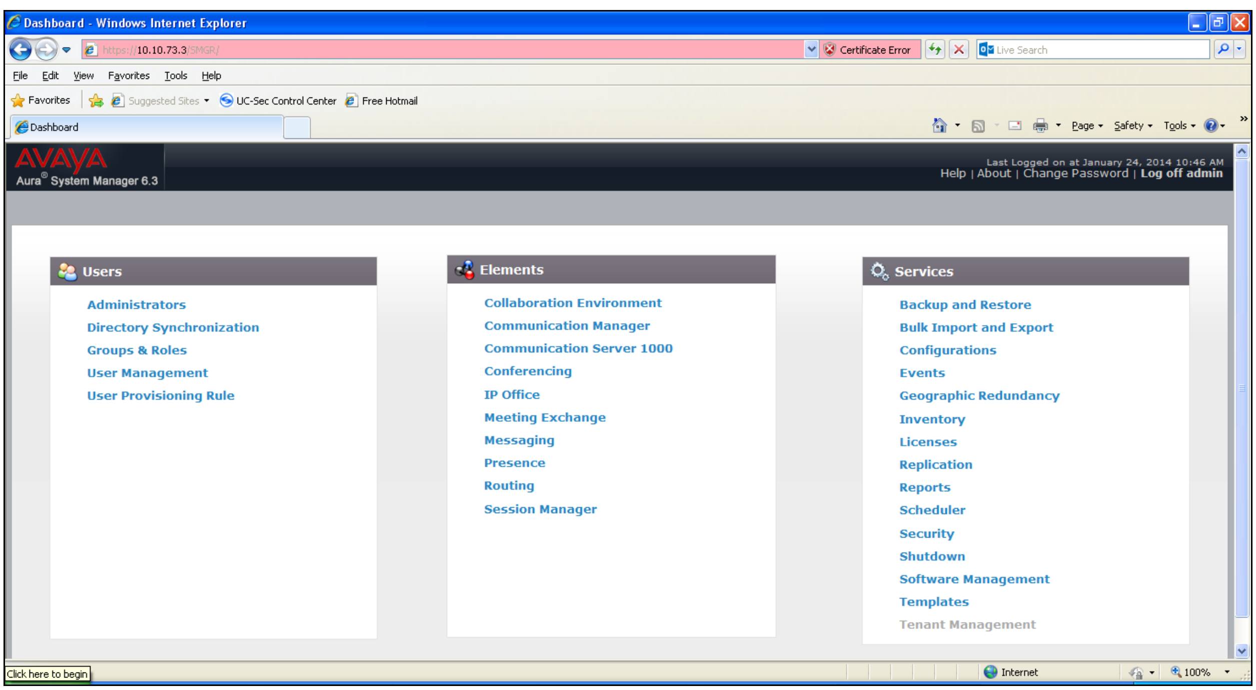
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Log in to Avaya Aura® System Manager
- Administer SIP Domain
- Administer SIP Location
- Administer Adaptations
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns

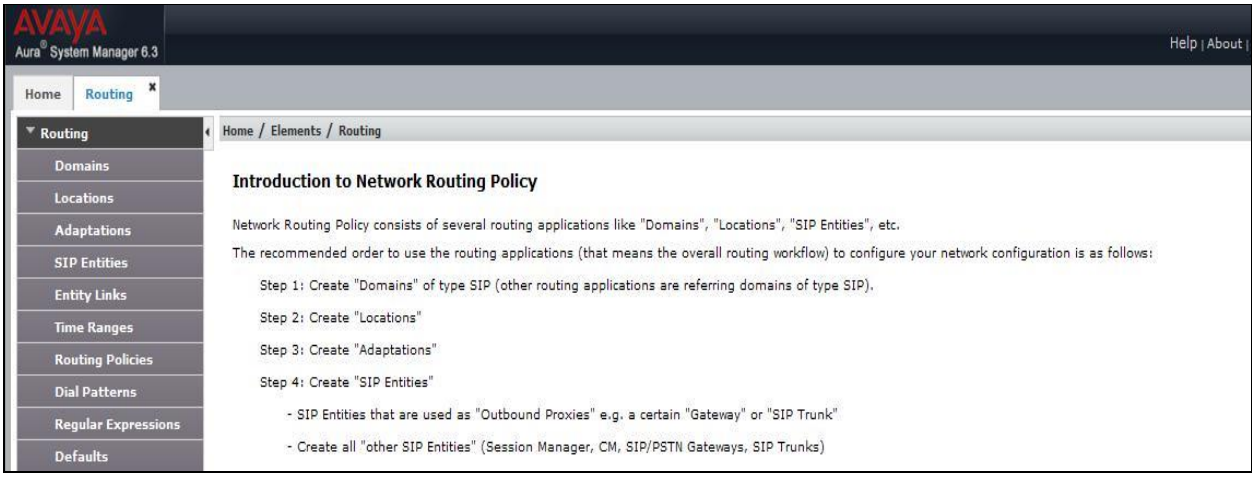
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

6.1. Log in to Avaya Aura® System Manager

Access the System Manager using a Web Browser by entering **http://<FQDN >/SMGR**, where **<FQDN>** is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown) and the **Home** tab will be presented with menu options shown below.



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.

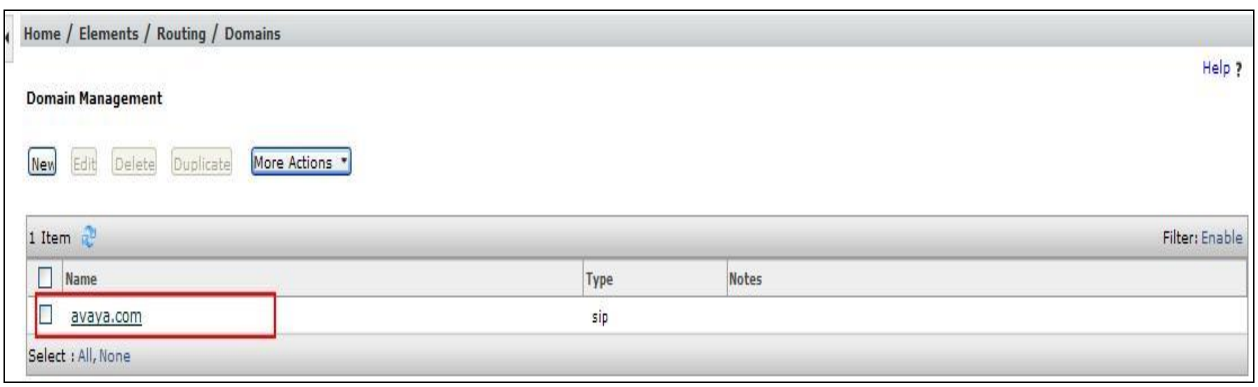


6.2. Administer SIP Domain

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 a Domain Name. 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.



6.3. Administer Locations

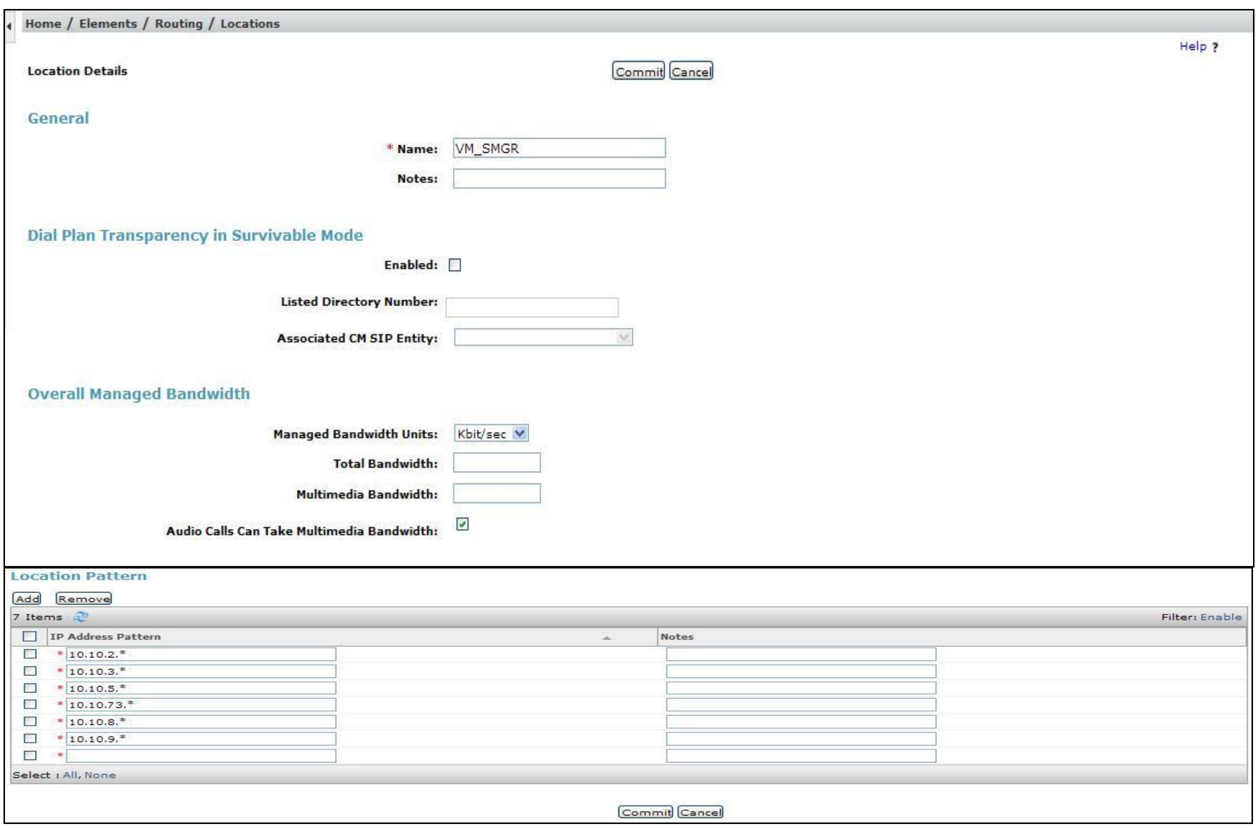
Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing →Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). 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.
- **Notes** Add a brief description [Optional].

Click **Commit** to save. The screenshot below shows the Location **VM_SMGR** defined for the compliance testing.

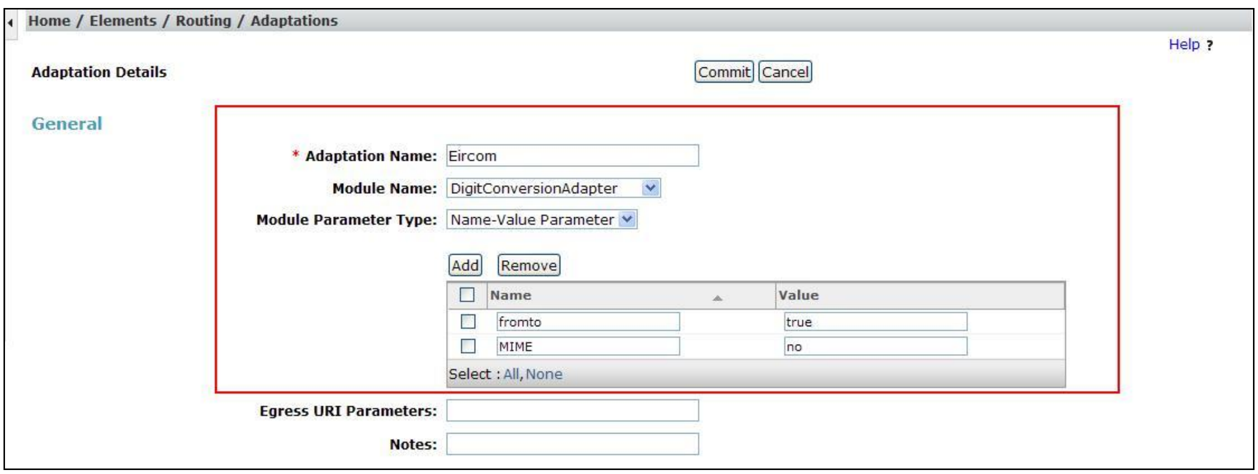


6.4. Administer Adaptations

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. The example below was applied to the Avaya SBCE SIP Entity and was used in test to convert numbers being passed between the Avaya SBCE and Session Manager.

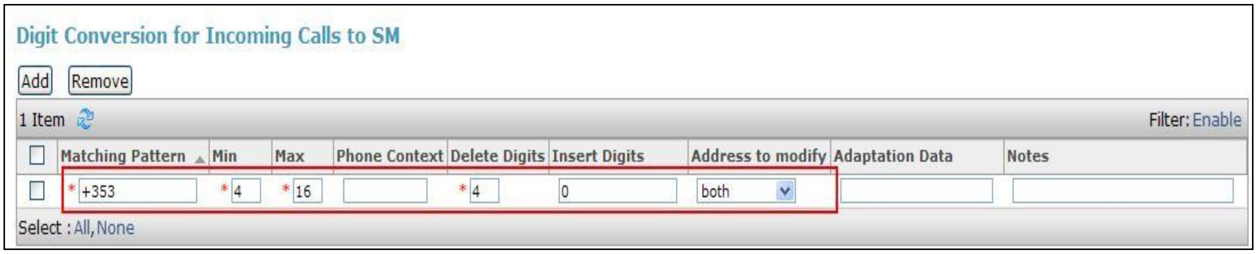
To add an adaptation, under the **Routing** tab select **Adaptations** on the left hand menu and then click on the **New** button (not shown). Under **Adaptation Details →General**:

- In the **Adaptation Name** field enter an informative name.
- In the **Module Name** field click on the down arrow and then select the <**click to add module**> entry from the drop down list and type **DigitConversionAdapter** in the resulting **New Module Name** field.
- **Module parameter** **MIME =no** Strips MIME message bodies on egress from Session Manager
fromto=true Modifies from and to headers of a message



Scroll down the page and under **Digit Conversion for Incoming Calls to SM**, click the **Add** button and specify the digit manipulation to be performed as follows:

- Enter the leading digits that will be matched in the Matching Pattern field.
- In the **Min** and **Max** fields set the minimum and maximum digits allowed in the digit string to be matched.
- In the **Delete Digits** field enter the number of leading digits to be removed.
- In the **Insert Digits** field specify the digits to be prefixed to the digit string.
- In the **Address to modify** field specify the digits to manipulate by the adaptation. In this configuration the dialed number is the target so **both** have been selected.



Digit Conversion for Incoming Calls to SM

Add Remove

1 Item Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
	* +353	* 4	* 16		* 4	0	both		

Select : All, None

This will ensure any incoming numbers will have the + 353 digits removed and 0 digit inserted before being presented to the Communication Server 1000E.

6.5. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system, supported by a SIP connection to 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:**

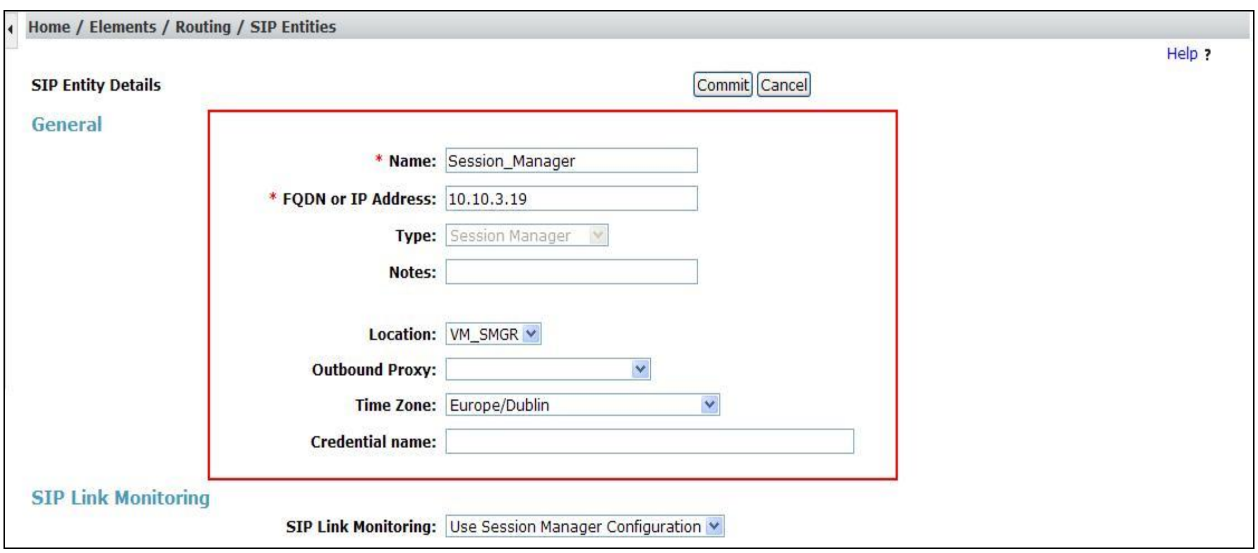
- In the **Name** field enter an informative name.
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signalling interface on the connecting system.
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **Other** for a Communication Server 1000E SIP entity and **SIP Trunk** for the Avaya SBCE SIP entity.
- In the **Adaptation** field (not available for Session Manager SIP Entity), select the appropriate Adaptation from the drop down menu.
- 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
- Communication Server 1000E SIP Entity
- Avaya SBCE SIP Entity

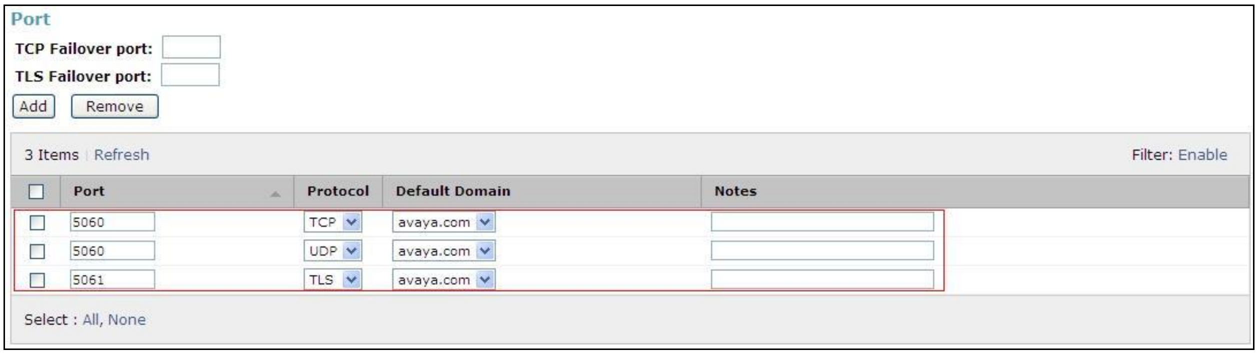
6.5.1. Avaya Aura® Session Manager SIP Entity

The following screens show the SIP entity for Session Manager. The **FQDN or IP Address** field is set to the IP address of Session Manager SIP signaling interface. Set the location to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.



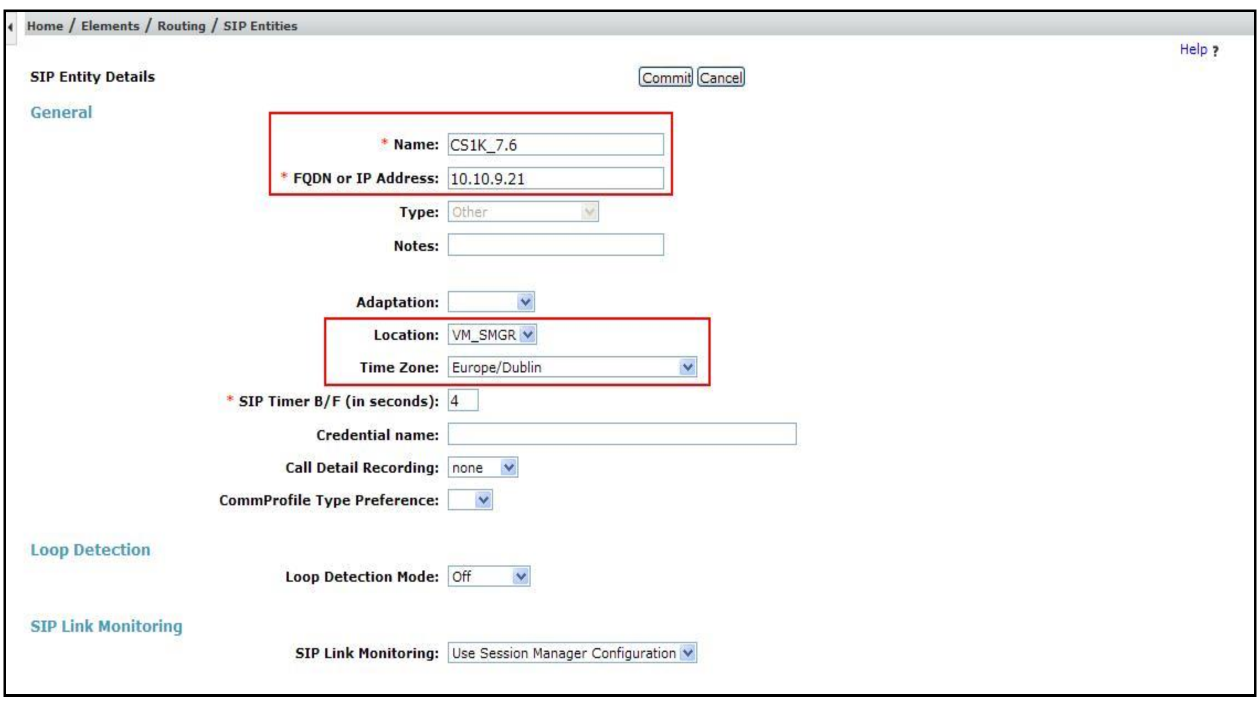
Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **Port**, click **Add,** then edit the fields in the resulting new row.

- 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.



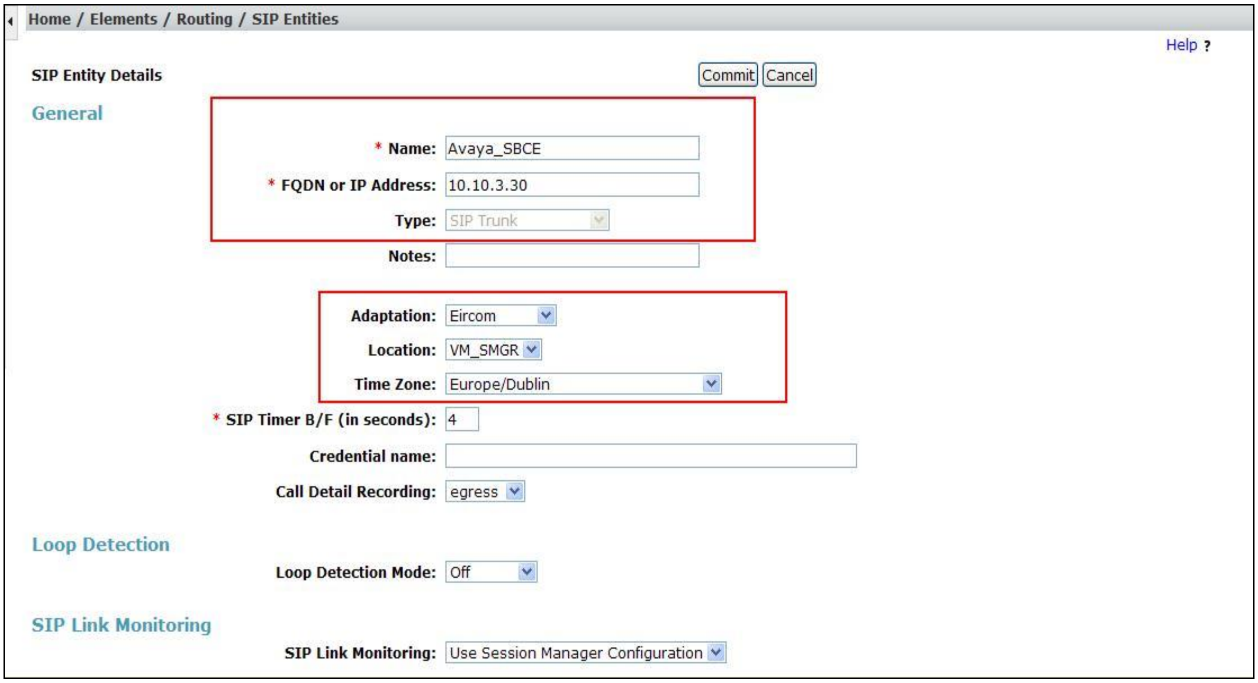
6.5.2. Avaya Communication Server 1000E SIP Entity

The following screen shows the SIP entity for Communication Server 1000E. The **FQDN or IP Address** field is set to the Node IP address of the interface on CS1000E that will be providing SIP signalling as shown in **Section 5.4**. Set the location to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.



6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the SIP entity for the Avaya SBCE 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. Set the location to that defined in **Section 6.3**, set **Adaptation** to one created in **Section 6.4** and the **Time Zone** to the appropriate time zone.

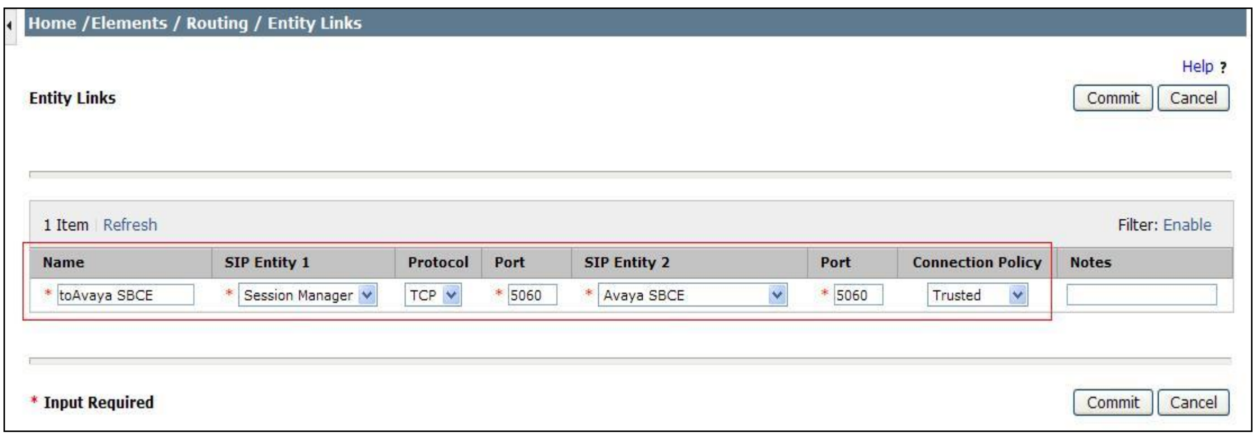


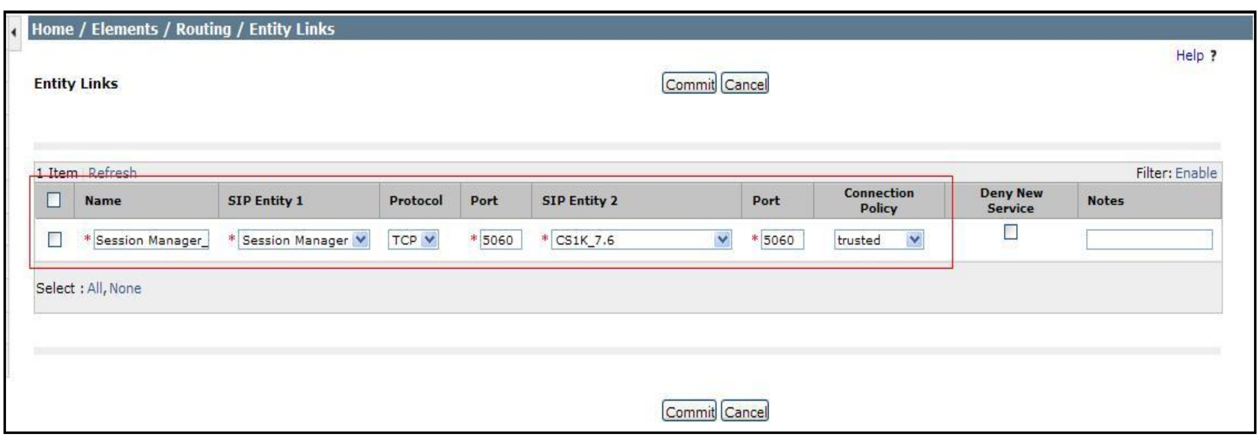
6.6. Administer Entity Links

A SIP trunk between Session Manager and another system is described by an Entity Link. To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button (not shown). Fill in the following fields in the new row that is displayed.

- In the **Name** field enter an informative name.
- In the **SIP Entity 1** field select **Session Manager**.
- In the **Protocol** field enter the transport protocol to be used to send SIP requests.
- In the **Port** field enter the port number to which the other system sends its SIP requests.
- In the **SIP Entity 2** field enter the other SIP Entity for this link, created in **Section 6.5**.
- In the **Port** field enter the port number to which the other system expects to receive SIP requests.
- Select **Trusted** from the drop down menu to make the other system trusted.

Click **Commit** to save changes. The following screen shows the Entity Links used in this configuration.





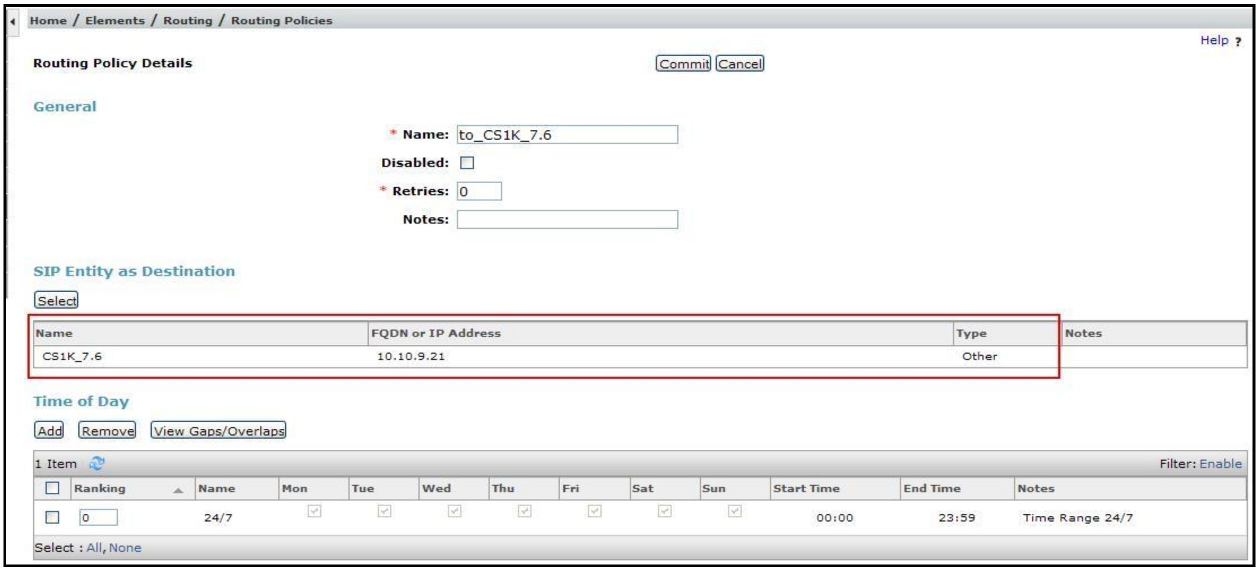
6.7. Administer Routing Policies

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

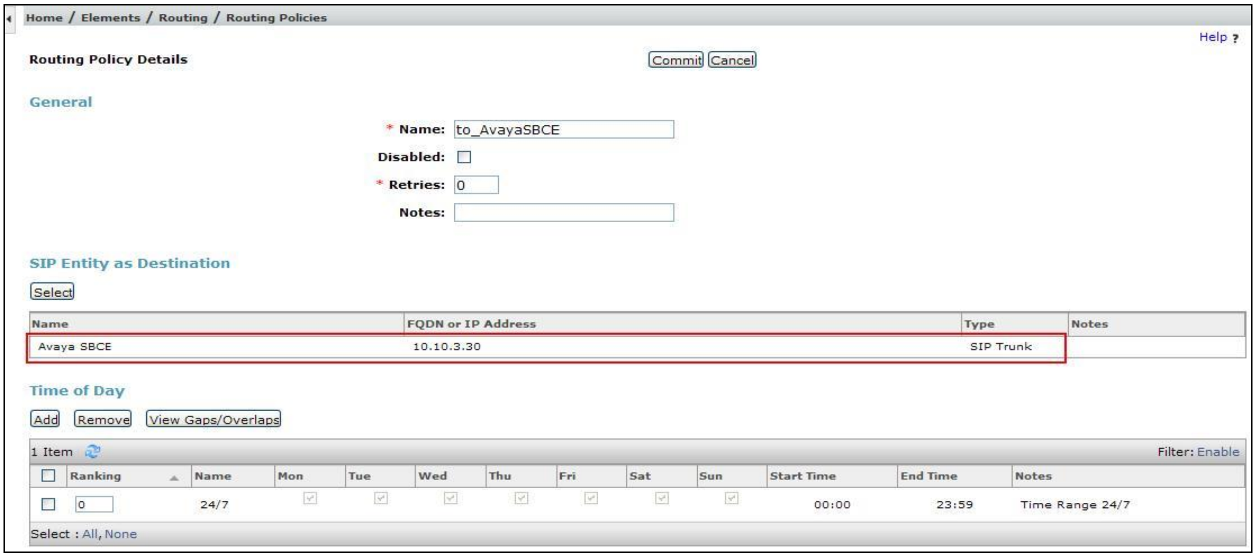
Under **General**:

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

The following screen shows the routing policy for Communication Server 1000E:



The following screen shows the routing policy for the Avaya SBCE:



6.8. Administer Dial Patterns

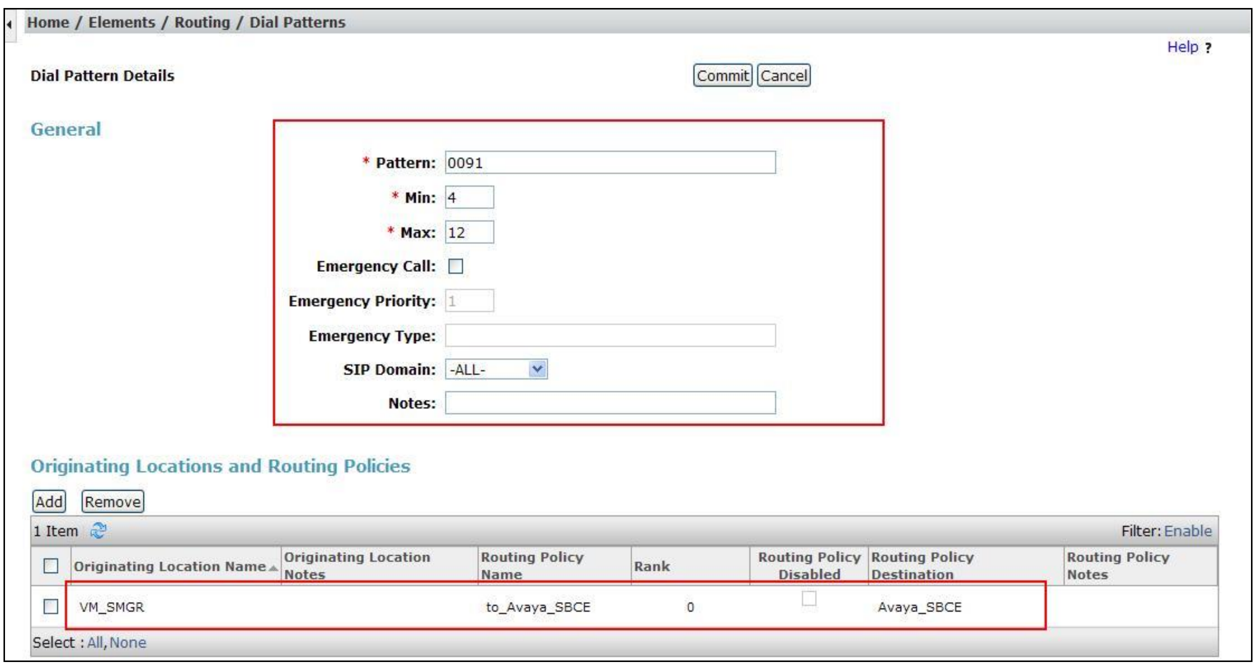
A dial pattern must be defined to direct calls to the appropriate telephony system. To configure a dial pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

Under **General**:

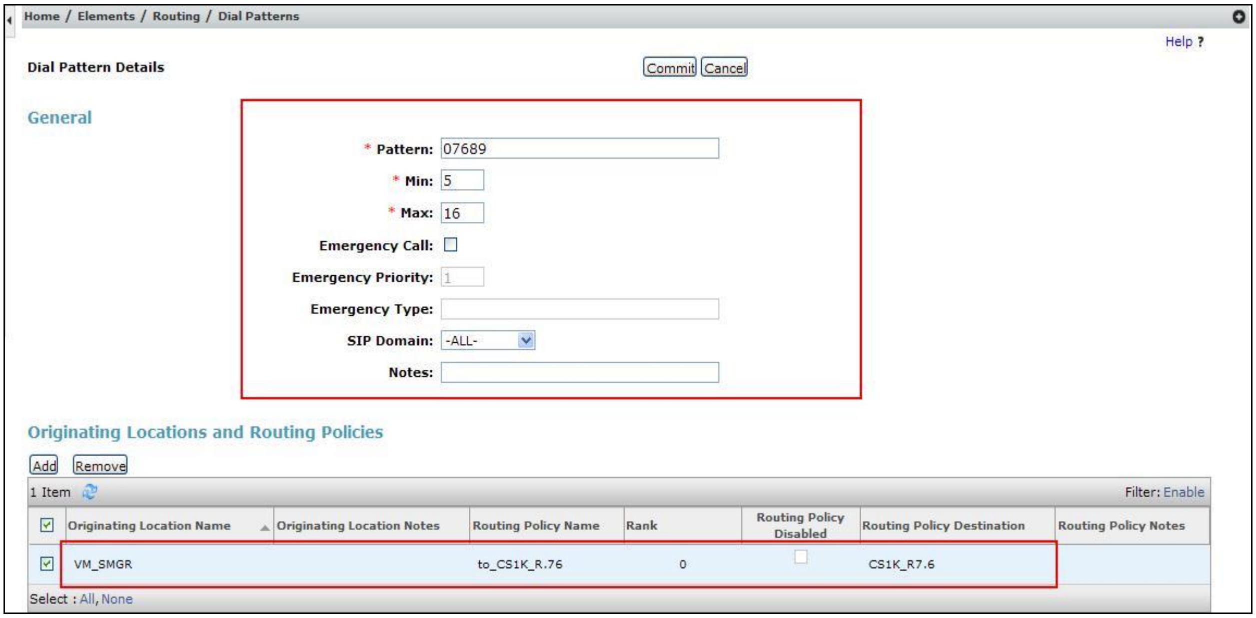
- In the **Pattern** field enter a dialed number or prefix to be matched.
- In the **Min** field enter the minimum length of the dialed number.
- In the **Max** field enter the maximum length of the dialed number.
- In the **SIP Domain** field select **–ALL-**.

Under **Originating Locations and Routing Policies**. Click **Add**, in the resulting screen (not shown) under **Originating Location** select **Locations** created in **Section 6.3** and under **Routing Policies** select one of the routing policies defined in **Section 6.7**. Click **Select** button to save (not shown).

The following screen shows an example dial pattern configured for the Avaya SBCE which will route the calls out to the PSTN via the Eircom SIP Trunk service.



The following screen shows an example dial pattern configured for the CS1000E. This dial pattern will route the calls to the CS1000E endpoints.

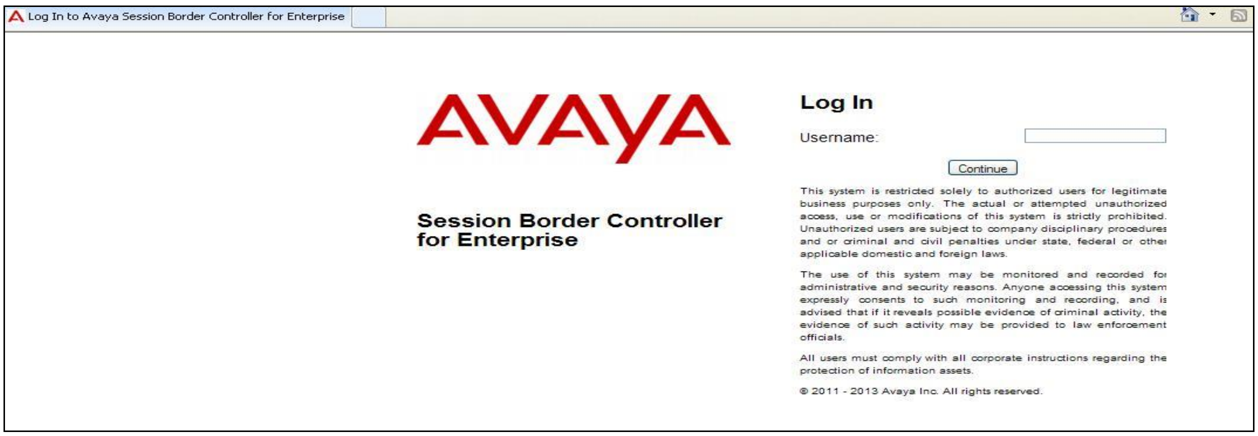


7. Configure Avaya Session Border Controller for Enterprise

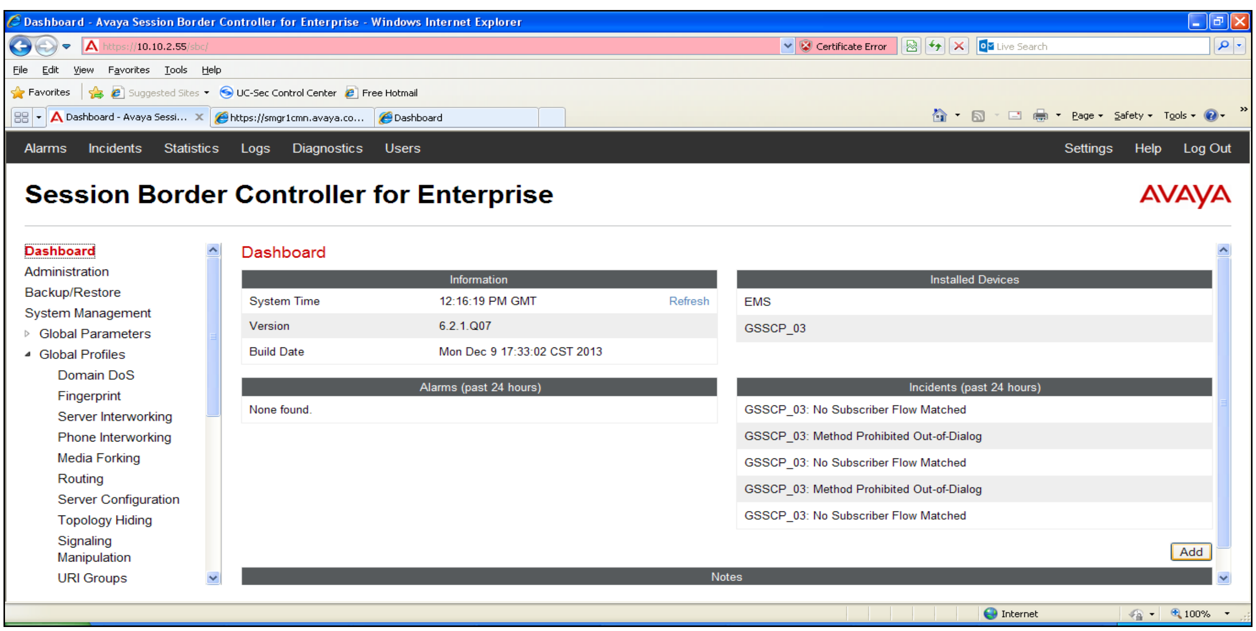
This section describes the configuration of the Avaya SBCE. The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP implementation where necessary.

7.1. Access Avaya Session Border Controller for Enterprise

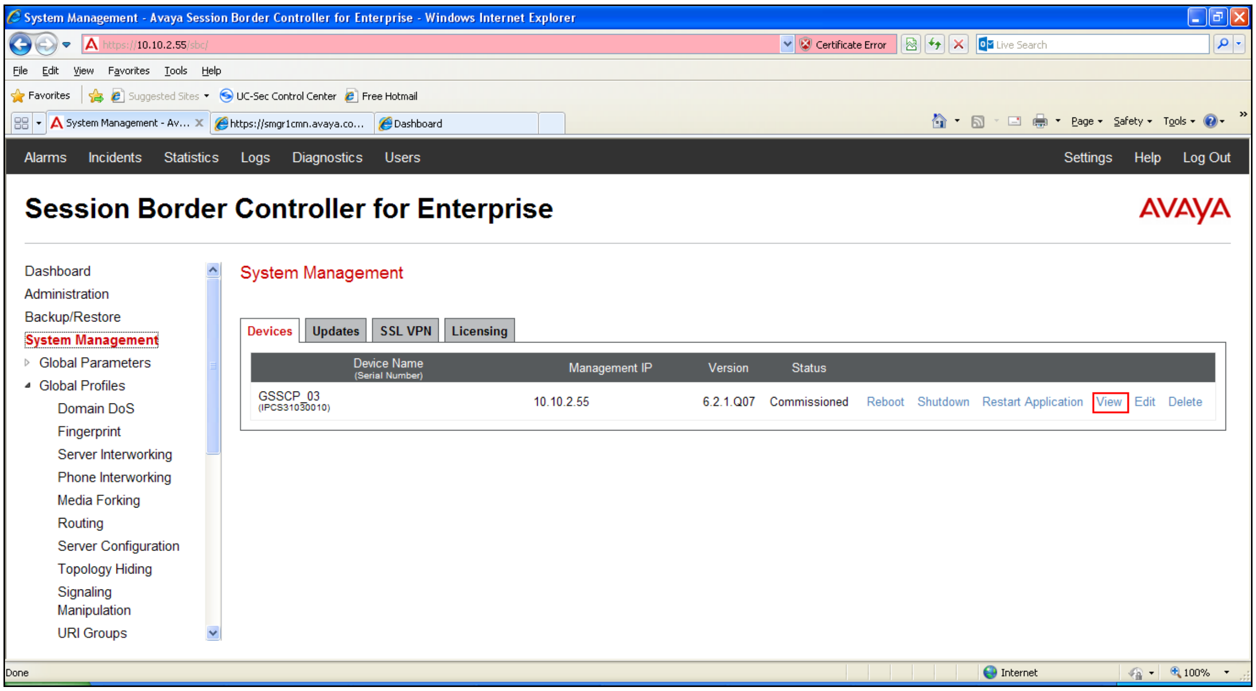
Access the Avaya SBCE using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.



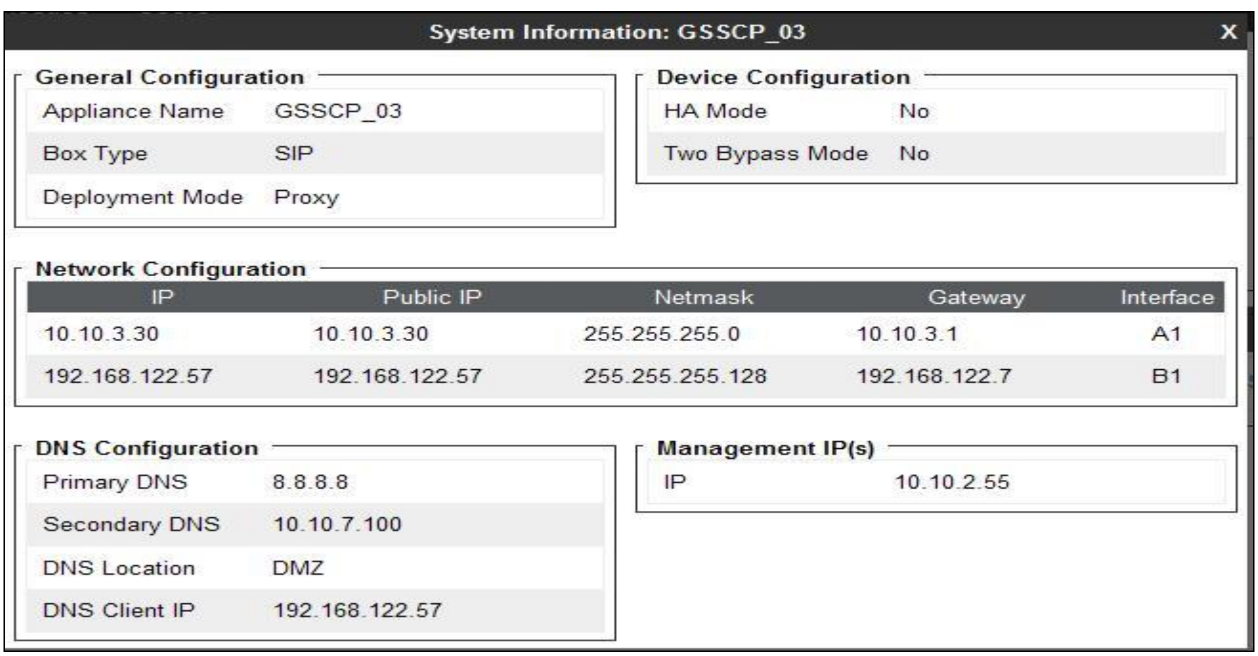
The main page of the Avaya SBCE will appear.



To view system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **GSSCP_03** is shown. To view the configuration of this device, click **View** (the third option from the right).



The System Information screen shows the **Appliance Name**, **Device Settings** and **DNS Configuration** information.



7.2. Global Profiles

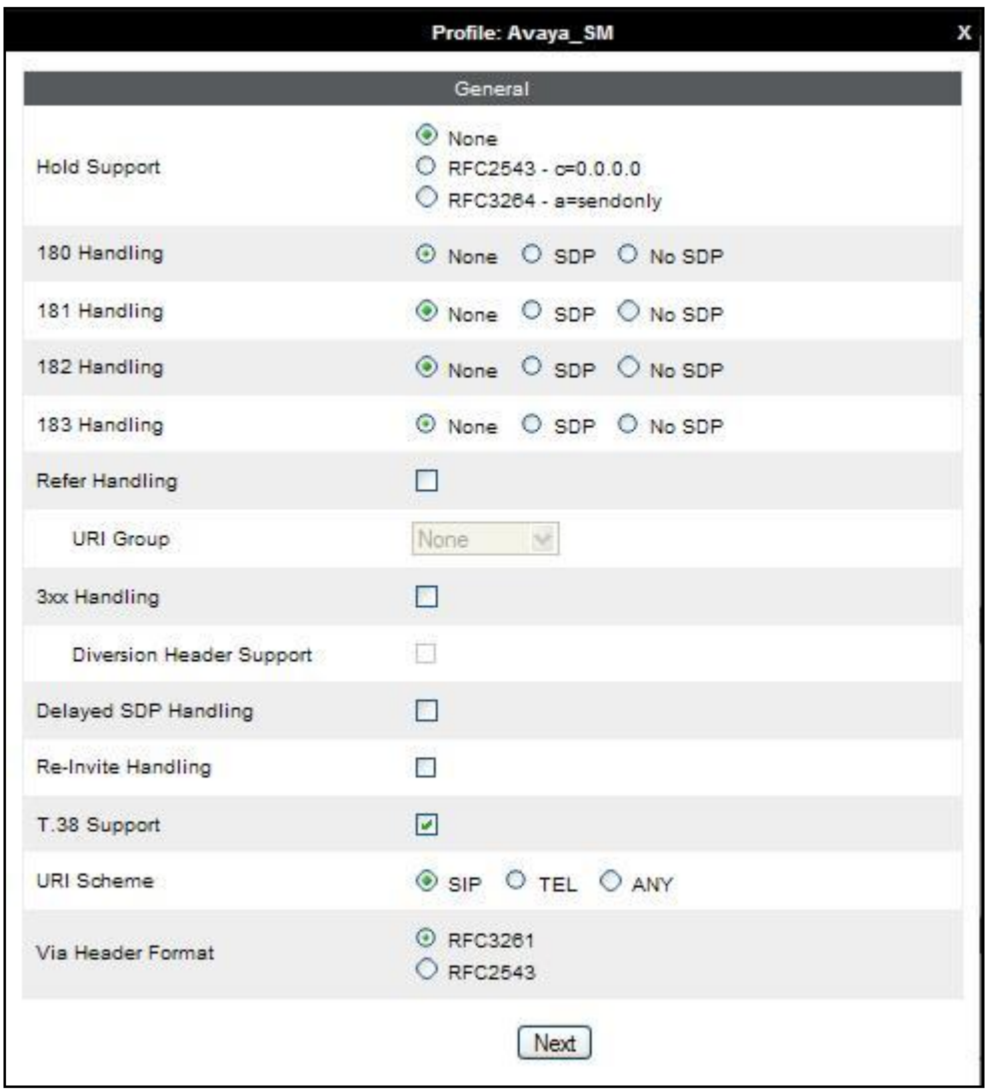
When selected, Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

7.2.1. Server Interworking - Avaya

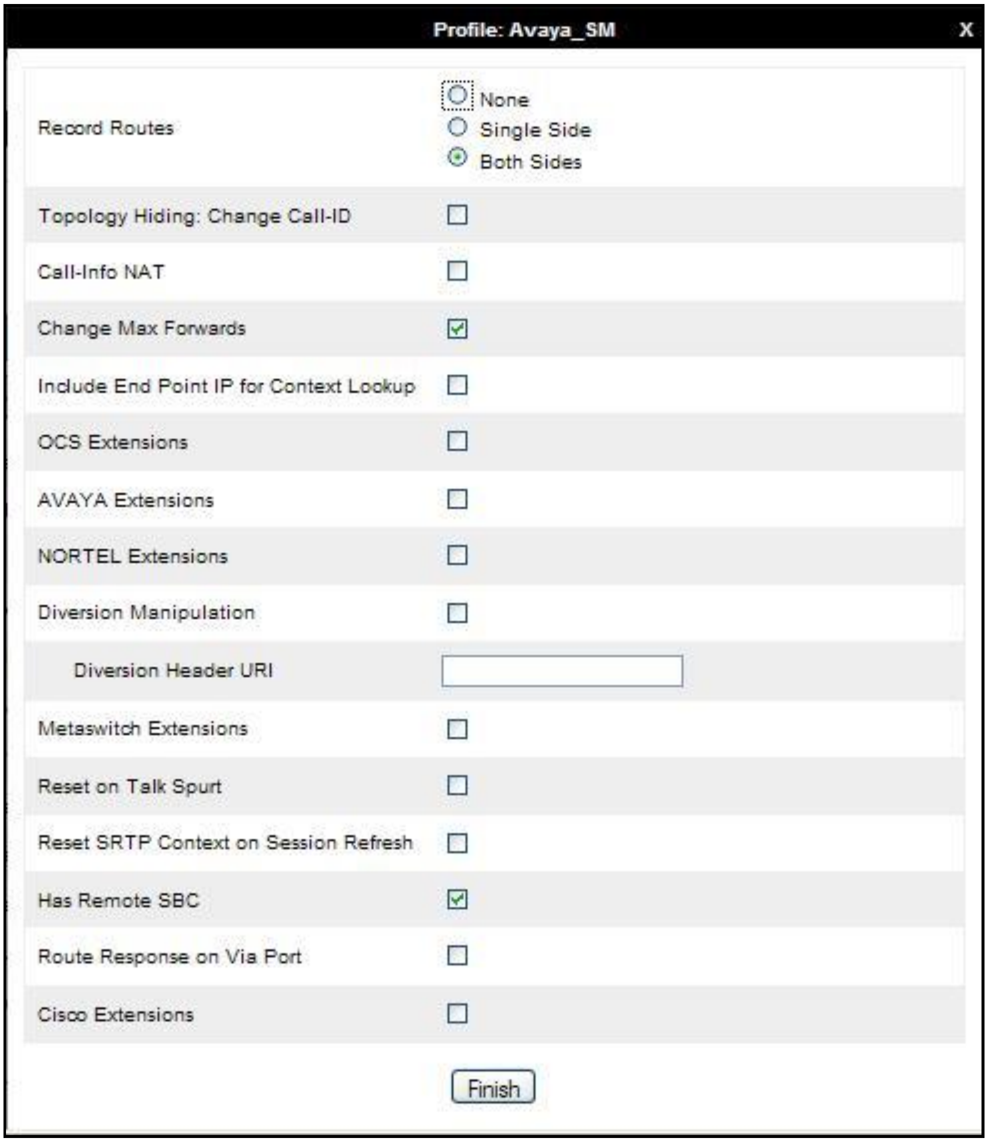
Server Interworking allows the configuration and management of various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Global Profiles → Server Interworking** and click on **Add Profile.**

- Enter profile name such as **Avaya_SM** and click **Next** (Not Shown)
- Check **Hold Support=None**
- Check **T.38 Support**
- All other options on the **General** Tab can be left at default

Click on **Next** on the following screens.



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

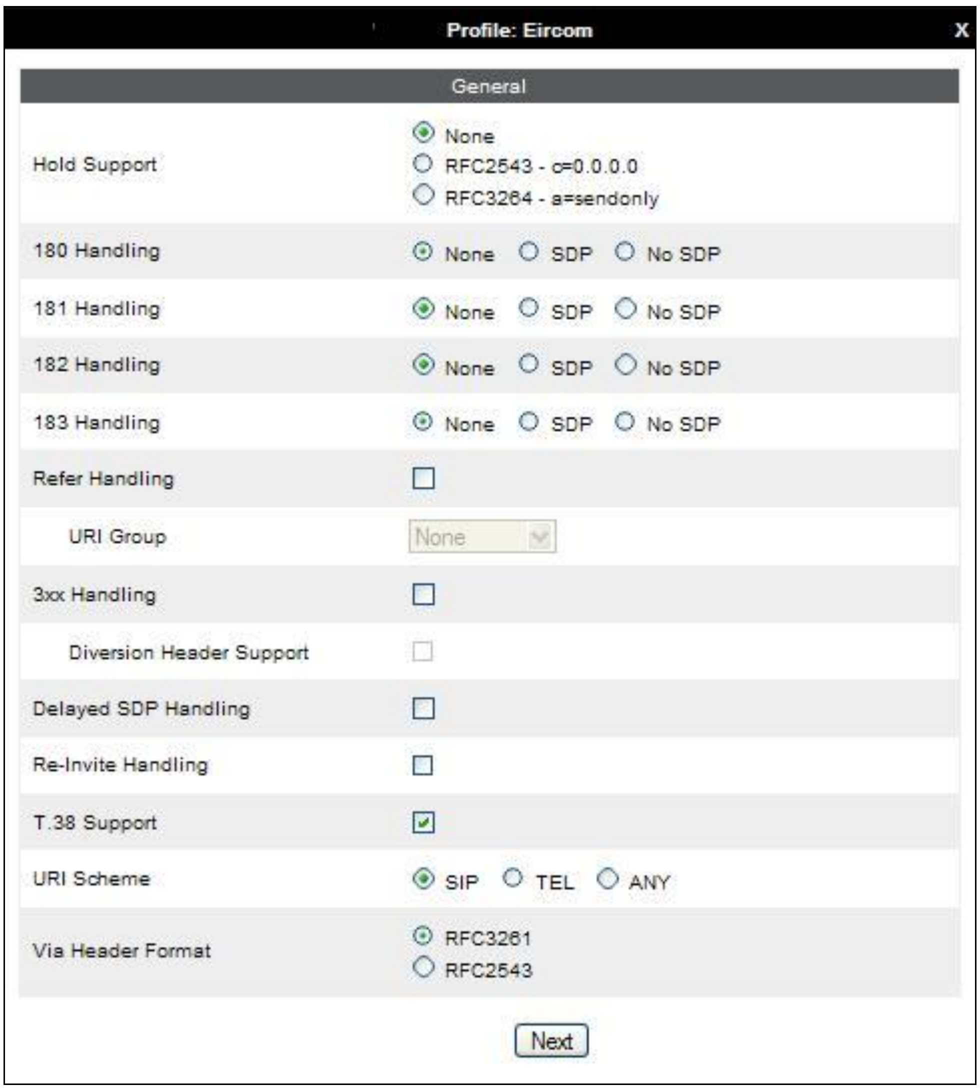


7.2.2. Server Interworking – Eircom

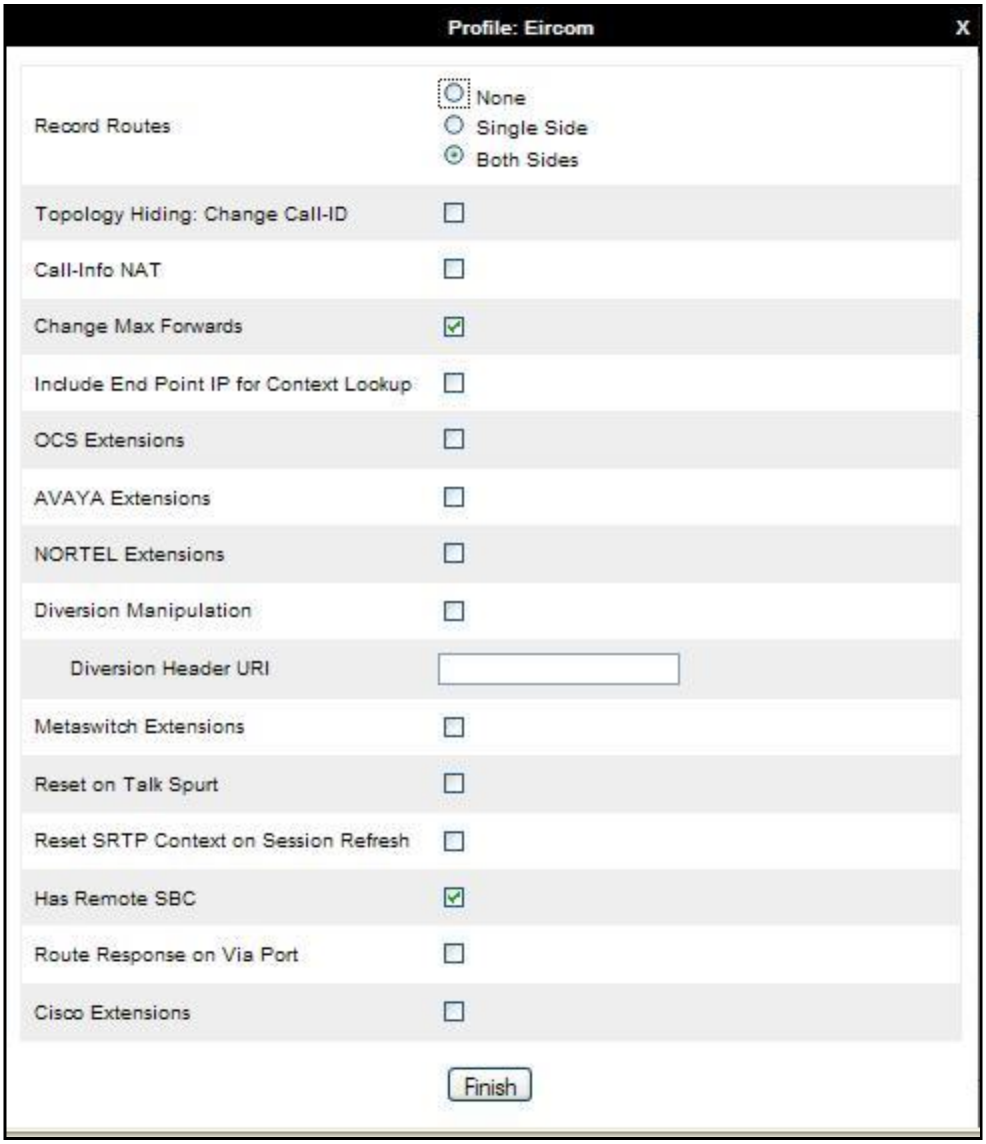
Server Interworking allows the configuration and management of various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Global Profiles → Server Interworking** and click on **Add Profile**.

- Enter profile name such as **Eircom** and click **Next** (Not Shown)
- Check **Hold Support = None**
- Check **T.38 Support**
- All other options on the **General** Tab can be left at default

Click on **Next** on the following screens.



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



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.

Routing information is required for routing to Session Manager on the internal side and the Eircom address on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop IP Address**, default 5060 is used.

Create a Routing Profile for both Session Manager and Eircom SIP trunk. To add a routing profile, navigate to **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, e.g. Session Manager
- **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 Hopserver
- **Outgoing Transport:** Choose the protocol used for transporting outgoing signaling packets

Click **Finish**.

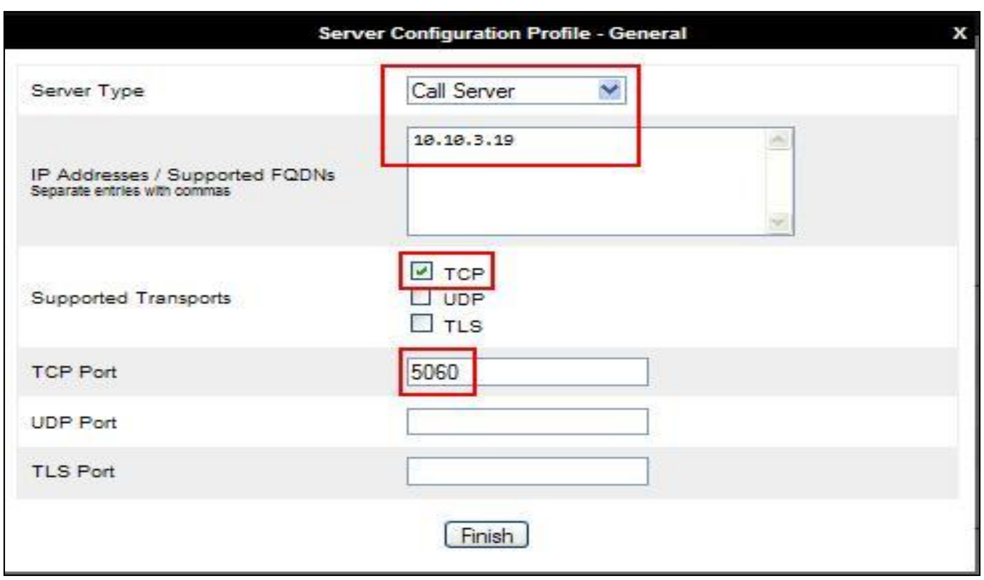
The following screen shows the Routing Profile to Session Manager.

The following screen shows the Routing Profile to Eircom.

7.2.4. Server Configuration– Avaya Aura® Session Manager

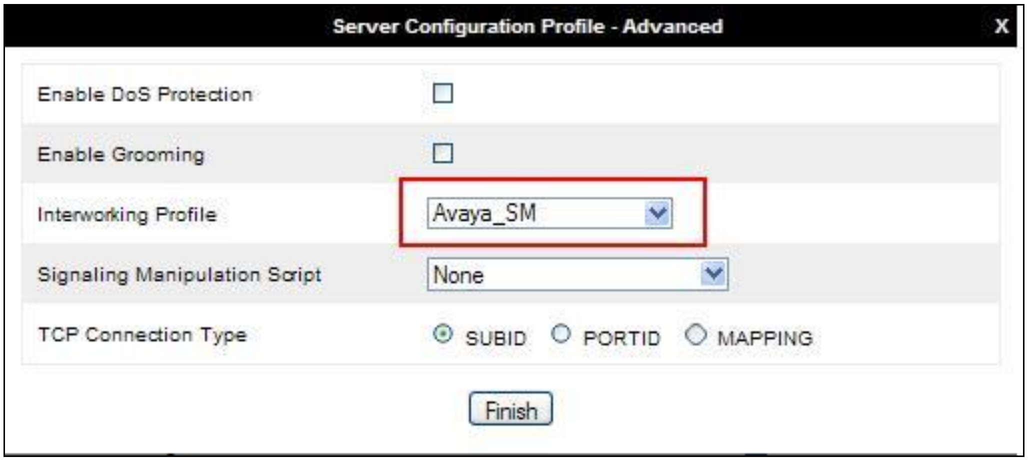
Servers are defined for each server connected to the Avaya SBCE. In this case, Eircom is connected as the Trunk Server and Session Manager is connected as the Call Server.
The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow you to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signaling parameters and some advanced options. From the left-hand menu, select **Global Profiles → Server Configuration** and click on **Add Profile** and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Call Server**
- Enter **IP Addresses / Supported FQDNs** to **10.10.3.19** (Session Manager IP address)
- For **Supported Transports,** check **TCP**
- **TCP Port:5060**
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs



On the **Advanced** tab:

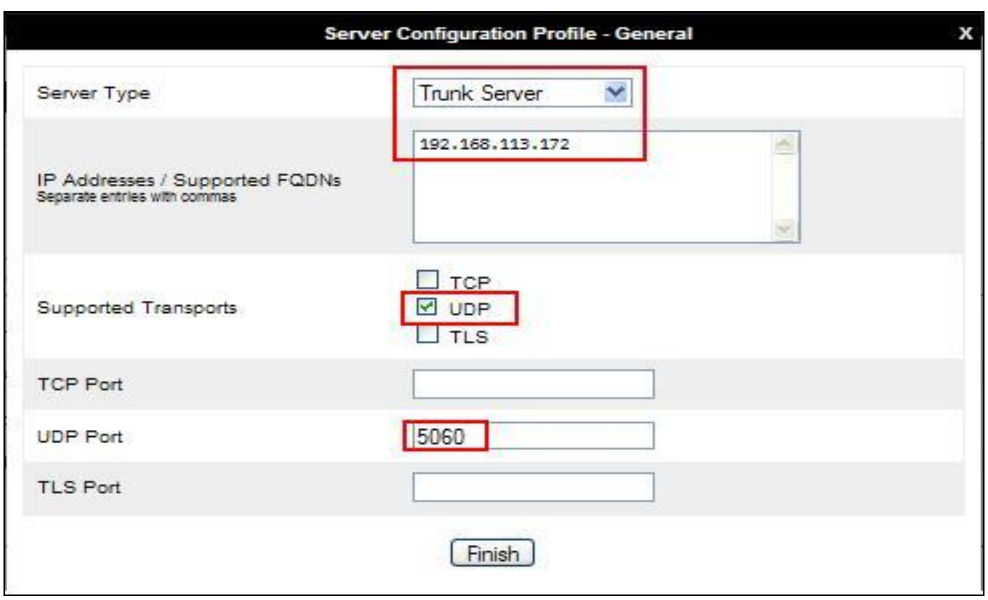
- Select **Avaya_SM** for **Interworking Profile**
- Click **Finish**



7.2.5. Server Configuration – Eircom

To define the Eircom Trunk Server, navigate to select **Global Profiles → Server Configuration** and click on **Add Profile** and enter a descriptive name. On the **Add Server Configuration Profile** tab, click on **Edit** and set the following:

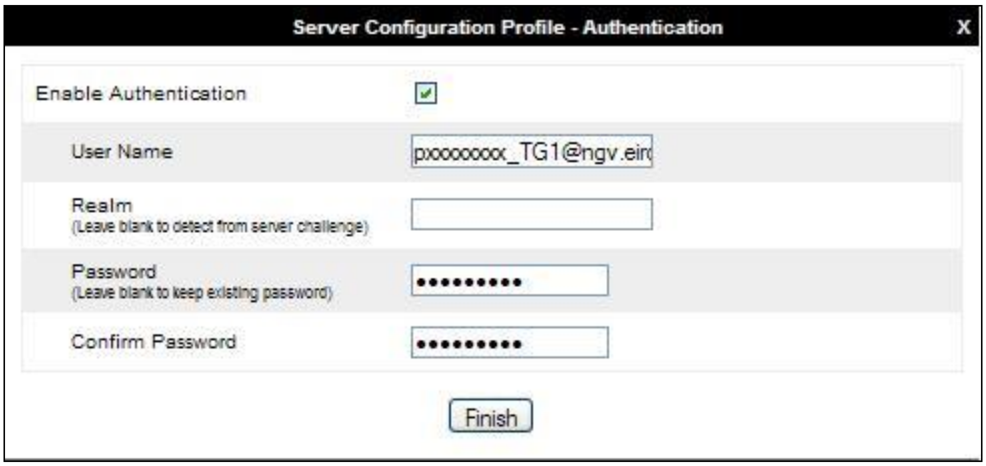
- Select **Server Type** as **Trunk Server**
- Set **IP Address** to **192.168.113.172** (Eircom SIP Trunk)
- **Supported Transports**: Check **UDP**
- **UDP Port: 5060**
- Hit **Next** (not shown)



In the new window that appears, enter the following values as Eircom require authentication to connect to their network:

- **Enabled Authentication:** Checked
- **User Name:** Enter username provided by the Service Provider
- **Realm:** Enter realm details provided by the Service Provider
- **Password** Enter password provided by the Service Provider
- **Confirm Password** Re-enter password provided by the Service Provider

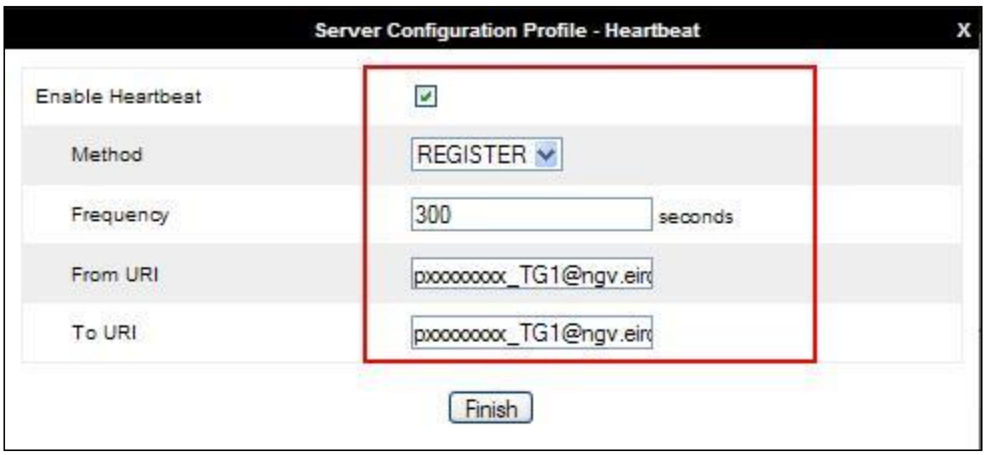
Click **Next** to continue.



In the new window that appears, enter the following values.

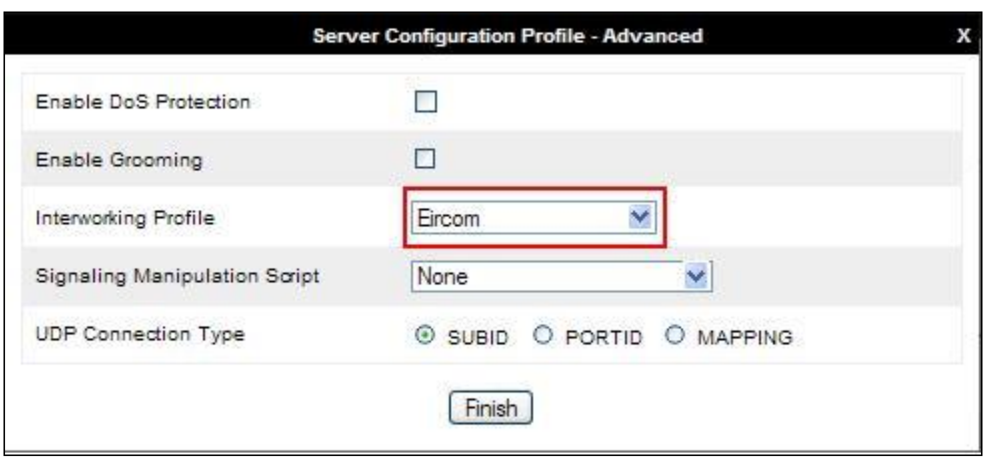
- **Enabled Heartbeat:** Checked
- **Method:** Select **REGISTER** from the drop-down box
- **Frequency:** Choose the desired frequency in seconds the Avaya SBCE will send SIP REGISTERS
- **From URI:** Enter an URI to be sent in the FROM header for SIP REGISTERS
- **TO URI:** Enter an URI to be sent in the TO header for SIP REGISTERS

Click **Next** (not shown) to continue.



On the **Advanced** tab:

- Select **Eircom** for **Interworking Profile**
- Click **Finish**



7.2.6. Topology Hiding

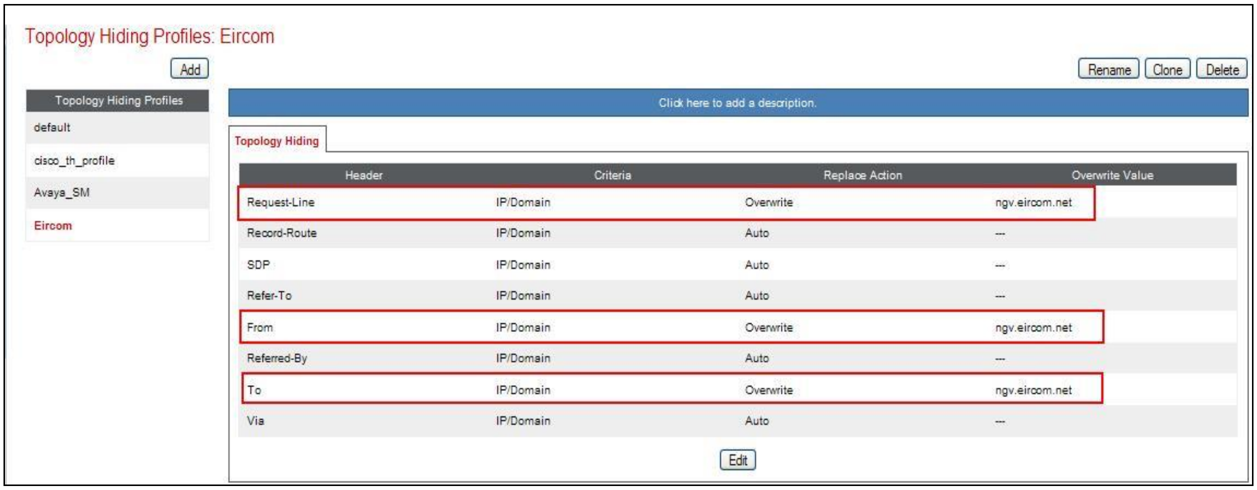
Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten with a domain name or IP addresses. The default **Replace Action** is **Auto**, this replaces local information with IP addresses, generally the next hop. Topology hiding has the advantage of presenting single Via and Record-Route headers externally where multiple headers may be received from the enterprise, particularly from Session Manager. In some cases where Topology Hiding can’t be applied, in particular the Contact header, IP addresses are translated to the Avaya SBCE external addresses using NAT.

To define Topology Hiding for Session Manager, navigate to **Global Profiles → Topology Hiding** from the menu on the left-hand side. Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- In the **Profile Name** field enter a descriptive name such as **Avaya_SM** and click **Next**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For Overwrite value, insert **avaya.com**.
- Click **Finish** (not shown).

To define Topology Hiding for the Eircom, navigate to **Global Profiles → Topology Hiding** from the menu on the left hand side. Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- Enter a descriptive Profile Name such as **Eircom**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For Overwrite value, insert **ngv.eircom.net**.
- Click **Finish** (not shown).

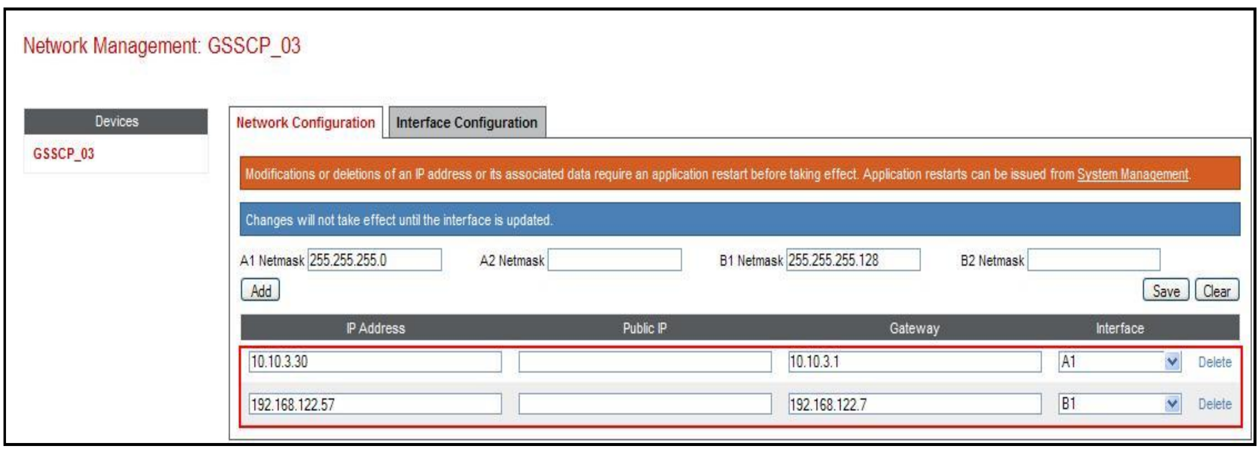


7.3. Define Network Information

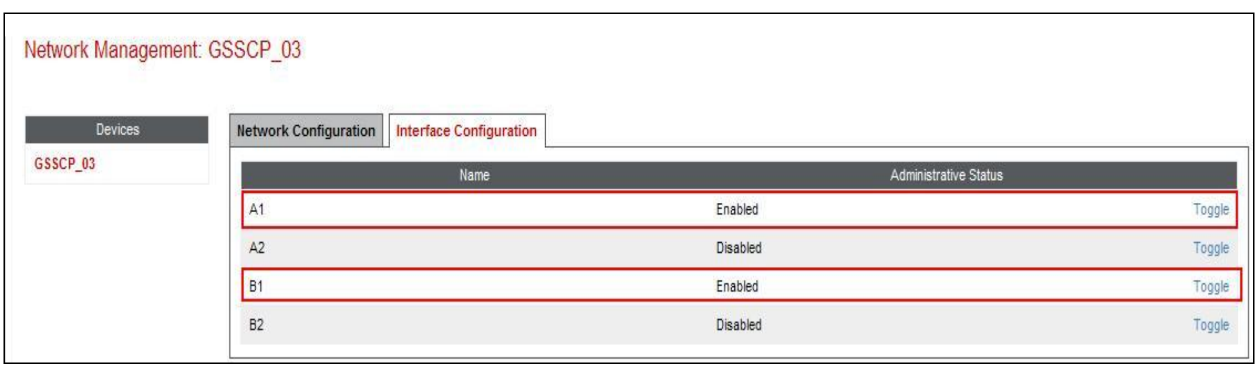
Network information is required on the Avaya SBCE to allocate IP addresses and masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external. Each side of the Avaya SBCE can have only one interface assigned.

To define the network information, navigate to **Device Specific Settings → Network Management** from the menu on the left-hand side and click on **Add IP**. Enter details in the blank box that appears at the end of the list.

- Define the internal IP address with screening mask and assign to interface **A1**.
- Select **Save Changes** to save the information.
- Click on **Add IP**.
- Define the external IP address with screening mask and assign to interface **B1**.
- Select **Save Changes** to save the information.
- Click on **System Management** in the main menu.
- Select **Restart Application** indicated by an icon in the status bar (not shown).



Select the **Interface Configuration** tab and click on **Toggle State** to enable the interfaces.



7.4. Define Interfaces

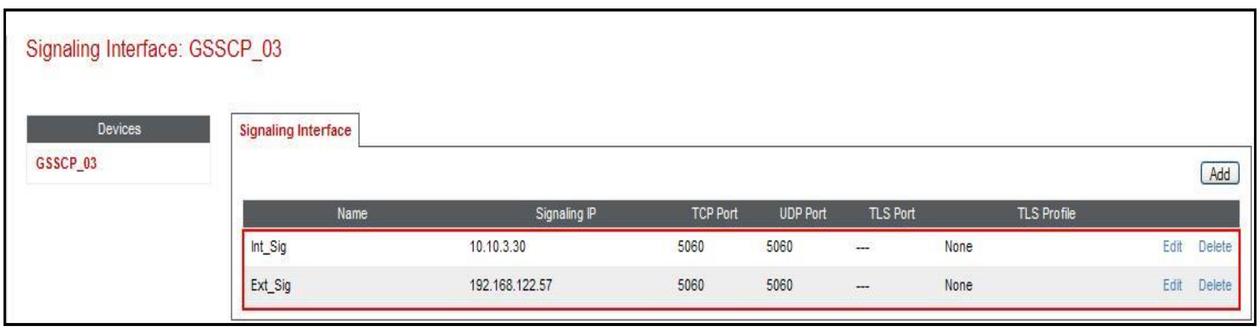
When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces.

7.4.1. Signalling Interfaces

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 **Device Specific Settings → Signaling Interface** and click **Add**.

- **Name**: **Int_Sig**
- **Signaling IP**: **10.10.3.30** (Internal address for calls toward Session Manager)
- **TCP Port**: **5060**
- **UDP Port**: **5060**
- Click **Finish**
- Select **Add**
- **Name**: **Ext_Sig**
- **Signaling IP: 192.168.122.57** (External address for calls toward Eircom)
- **UDP Port**: **5060**
- Click **Finish**

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

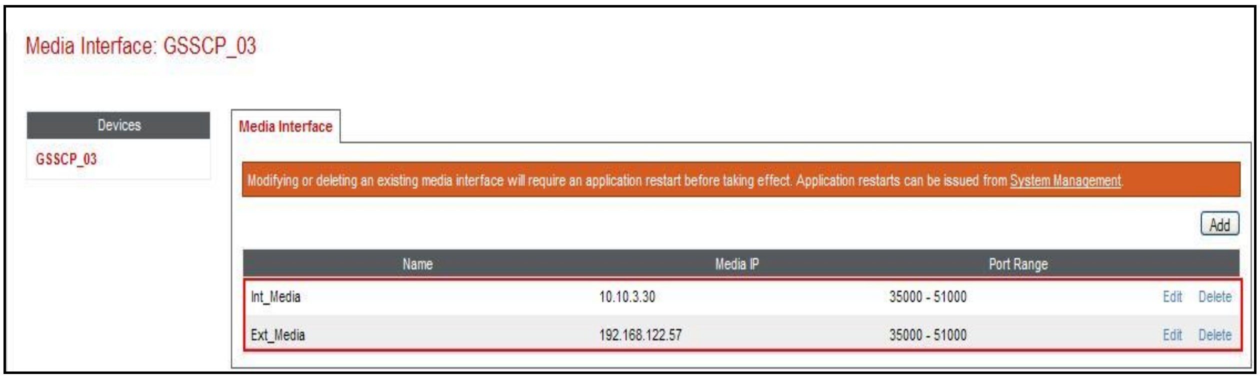


7.4.2. Media Interfaces

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 **Device Specific Settings → Media Interface**.

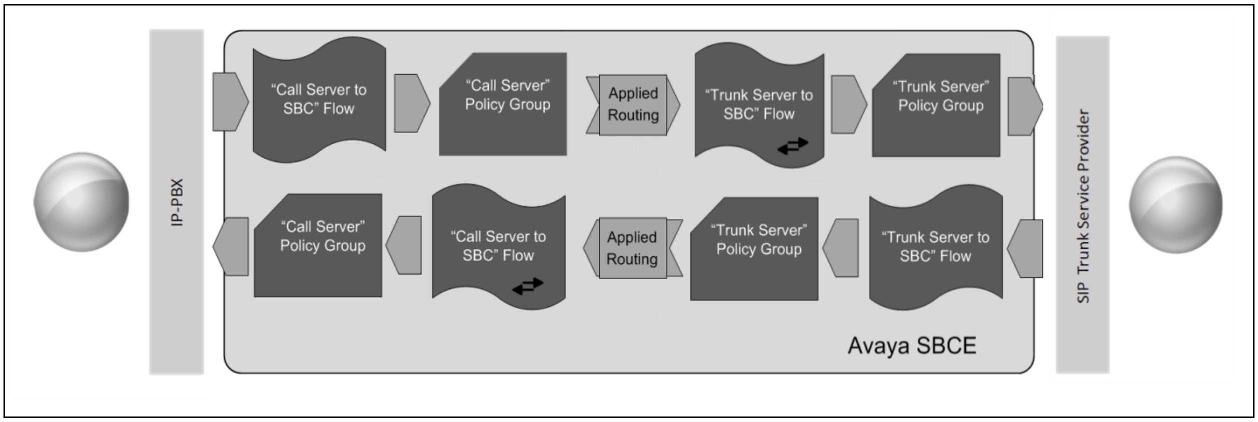
- Select **Add**
- **Name**: **Int_Media**
- **Media IP**: **10.10.3.30** (Internal address for calls toward Session Manager)
- **Port Range**: **35000-51000**
- Click **Finish**
- Select **Add**
- **Name**: **Ext_Media**
- **Media IP**: **192.168.122.57** (External address for calls toward Eircom)
- **Port Range**: **35000-51000**
- Click **Finish**

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



7.5. Server Flows

When a packet is received by the Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy 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.

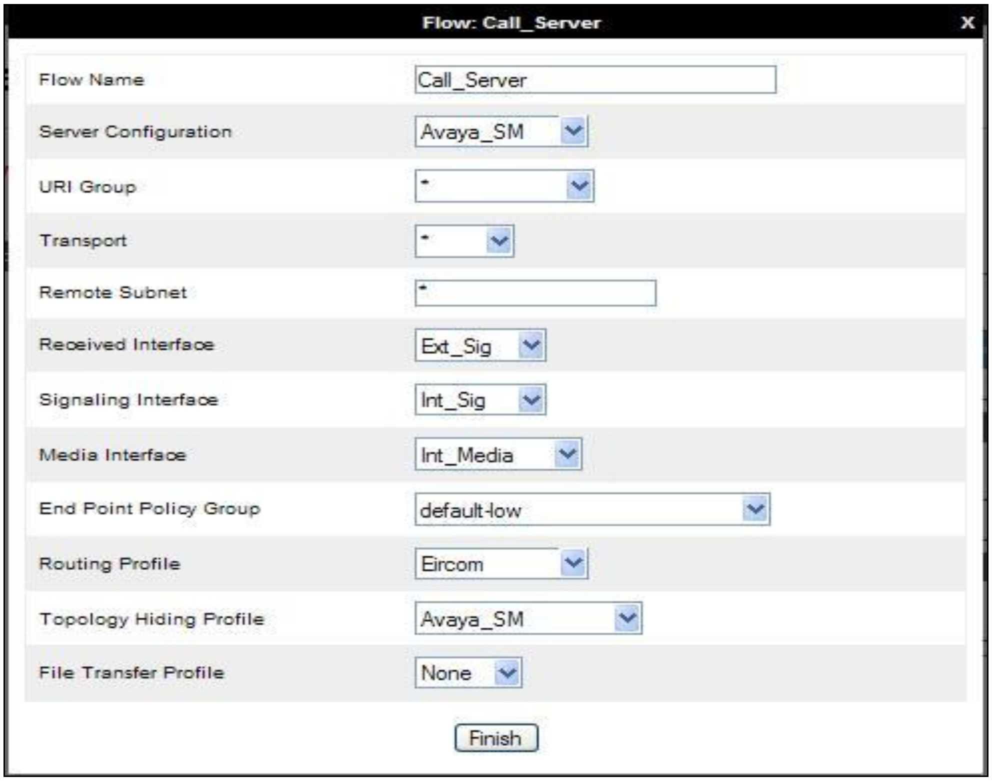


To create a Server Flow, navigate to **Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add Flow**.

- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select a Server Configuration created in **Section 7.2.4** and **7.2.5** and 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.
- **Topology Hiding Profile:** Select the profile to apply toward the Server Configuration.

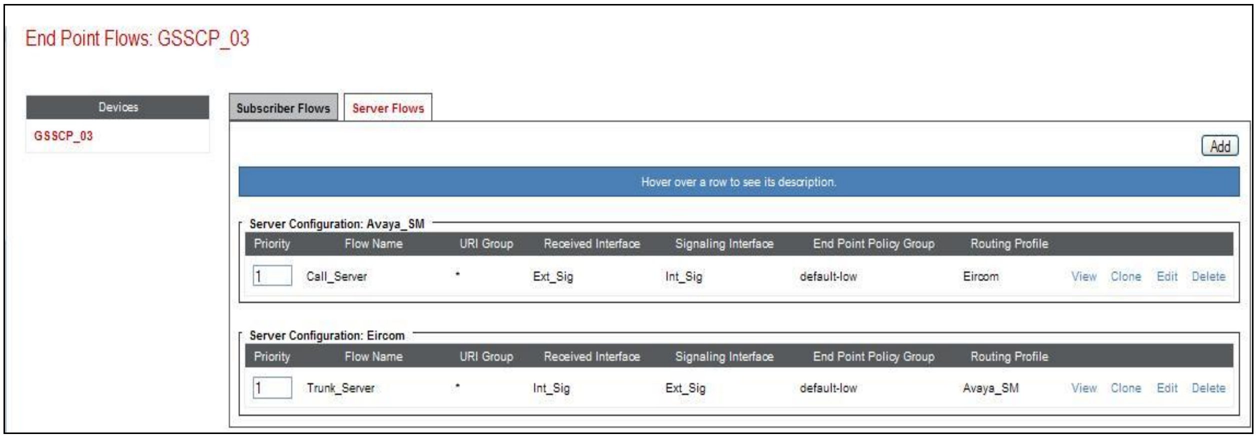
Click **Finish** to save and exit.

The following screen shows the Server Flow for Session Manager.



The following screen shows the Server Flow for Eircom.

This configuration ties all the previously entered information together so that calls can be routed from Session Manager to Eircom SIP Trunk service and vice versa. The following screenshot shows all configured flows.



8. Eircom Configuration

The configuration of the Eircom equipment used to support the Eircom SIP Trunk service is outside of the scope of these Application Notes and will not be covered. To obtain further information on Eircom equipment and system configuration, please contact an authorized Eircom representative.

9. Verification Steps

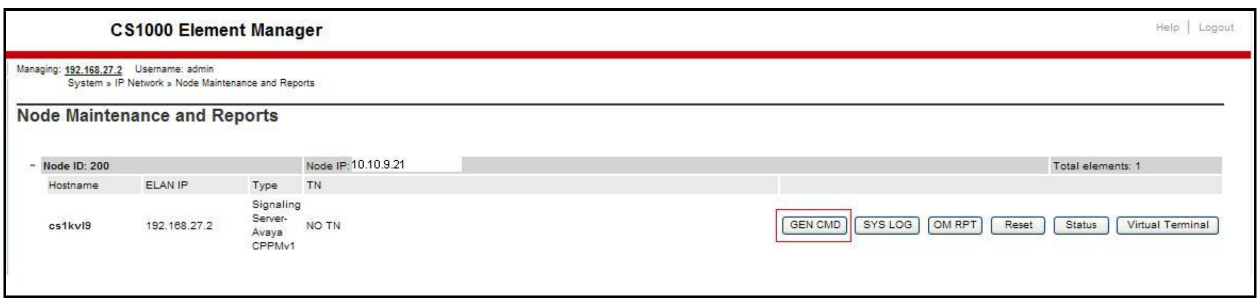
This section provides verification steps that may be performed in the field to verify that the solution is configured properly.

9.1. Avaya Communication Server 1000E Verification

This section illustrates sample verifications that may be performed using the Avaya CS1000E Element Manager GUI.

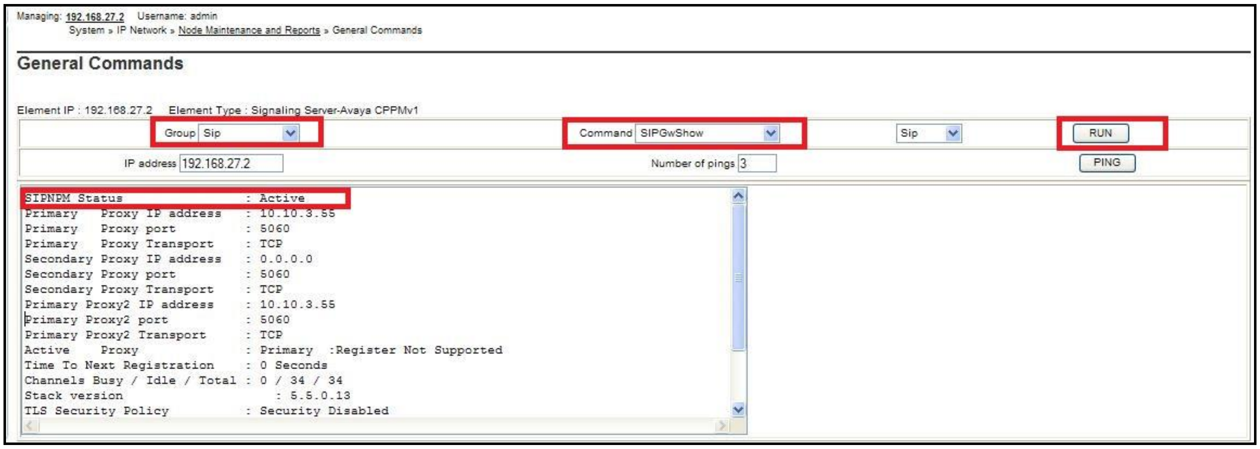
9.1.1. IP Network Maintenance and Reports Commands

From Element Manager, navigate to **System → IP Network → Maintenance and Reports** as shown below. In the resultant screen on the right, click the **Gen CMD** button.

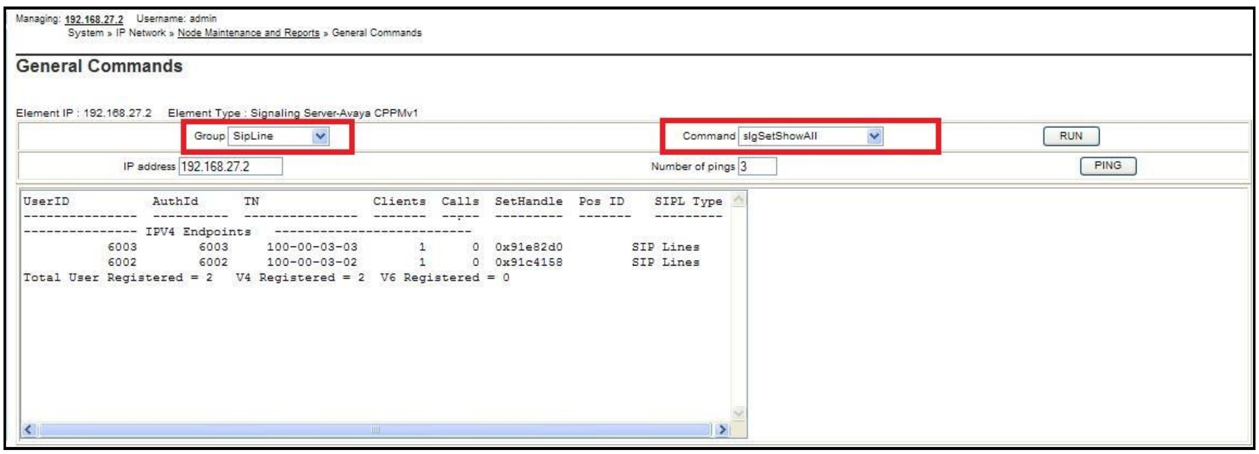


The **General Commands** page is displayed. A variety of commands are available by selecting an appropriate Group and Command from the drop-down menus, and selecting **Run**.

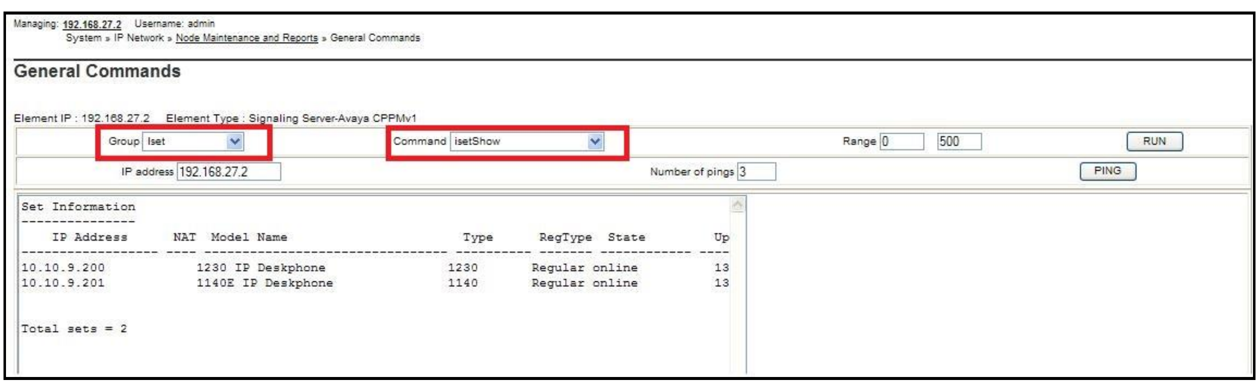
To check the status of the SIP Gateway to Session Manager in the sample configuration, select **Sip** from the Group menu and **SIPGwShow** from the **Command** menu. Click **Run**. The example output below shows that Session Manager has **SIPNPM Status** "**Active**".



The following screen shows a means to view registered SIP telephones. The screen shows the output of the **Command sigSetShowAll** in **Group SipLine**.



The following screen shows a means to view IP UNIStim telephones. The screen shows the output of the **Command isetShow** in **Group Iset**.

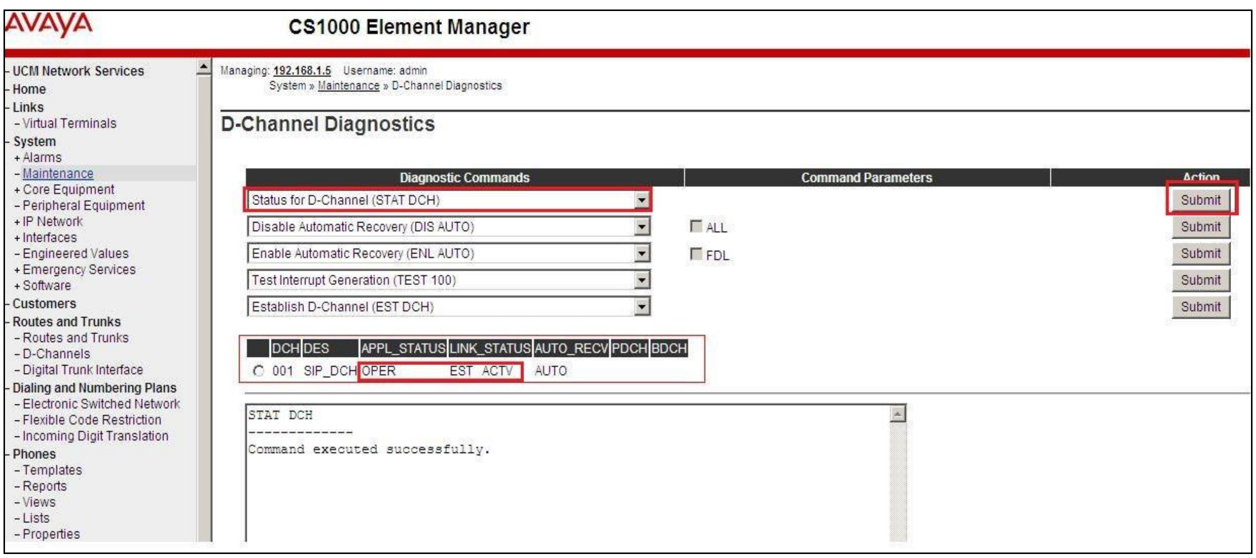


9.2. Verify Avaya Communication Server 1000E Operational Status

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.

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.

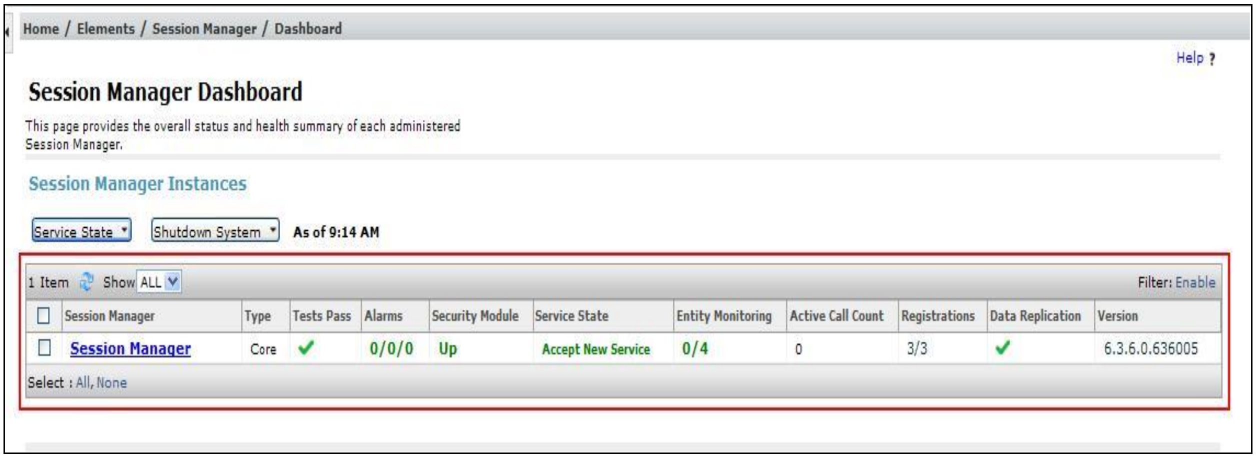
- **APPL_STATUS** Verify status is **OPER**
- **LINK_STATUS** Verify status is **EST ACTV**



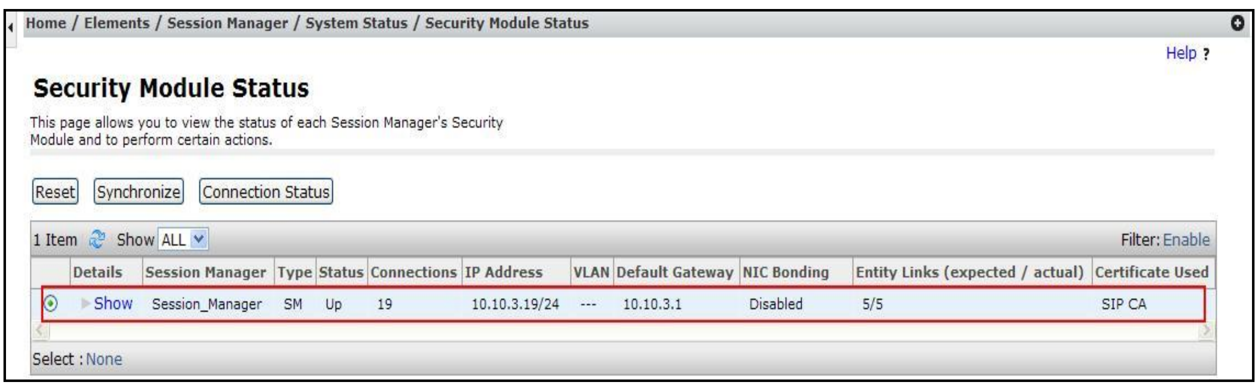
9.3. Verify Avaya Aura® Session Manager Operational Status

9.3.1. 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.

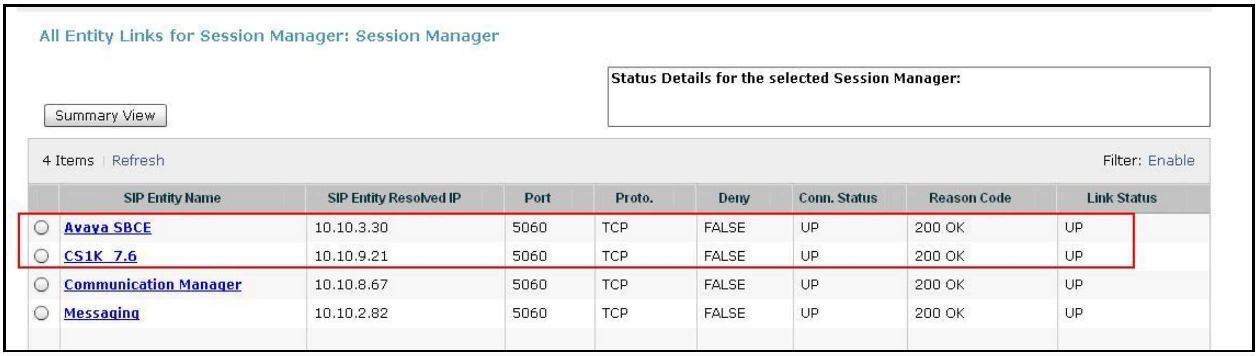


Navigate to **Elements → Session Manager → System Status → Security Module Status** (not shown) to view more detailed status information on the status of Security Module for the specific Session Manager. Verify the **Status** column displays **Up** as shown below.



9.3.2. 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: Session Manager** table, verify the **Conn. Status** for the link is **Up** as shown below.



All Entity Links for Session Manager: Session Manager

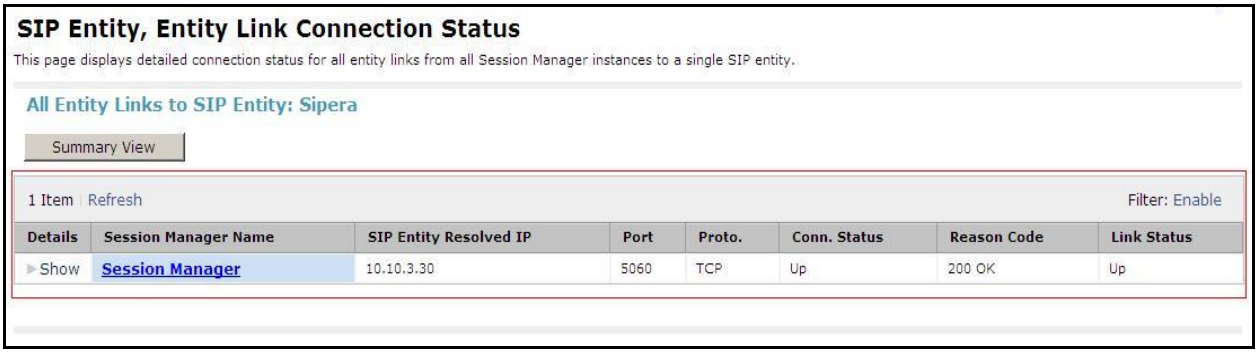
Status Details for the selected Session Manager:

Summary View

4 Items | Refresh   Filter: Enable

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	Avaya SBCE	10.10.3.30	5060	TCP	FALSE	UP	200 OK	UP
○	CS1K_7.6	10.10.9.21	5060	TCP	FALSE	UP	200 OK	UP
○	Communication Manager	10.10.8.67	5060	TCP	FALSE	UP	200 OK	UP
○	Messaging	10.10.2.82	5060	TCP	FALSE	UP	200 OK	UP

Verify the status of the SIP link is up between 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.



SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: Sipera

Summary View

1 Item | Refresh   Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶Show	Session Manager	10.10.3.30	5060	TCP	Up	200 OK	Up

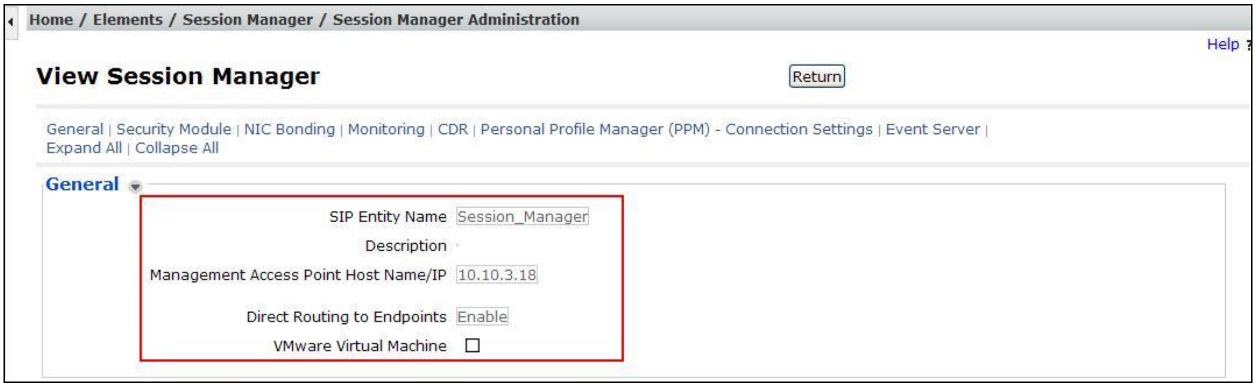
9.3.3. Verify Avaya Aura® Session Manager Instance

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 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 Session Manager management interface

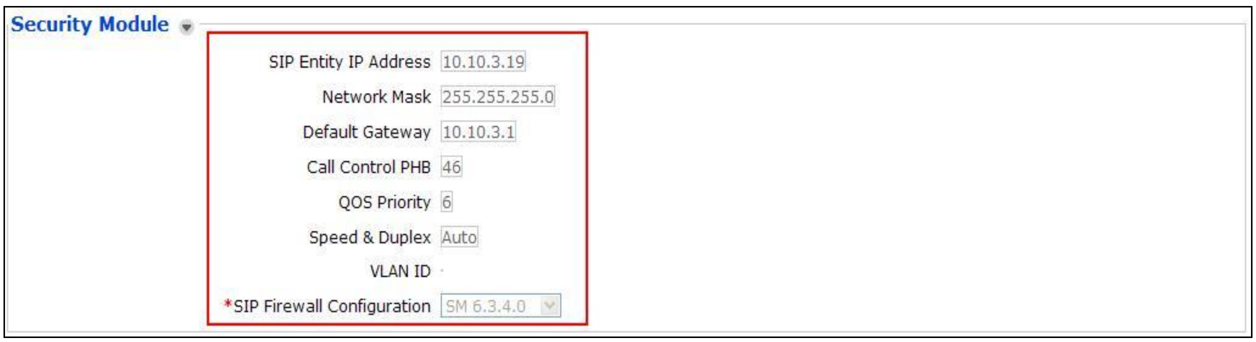
The following screen shows Session Manager values used for the compliance test.



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

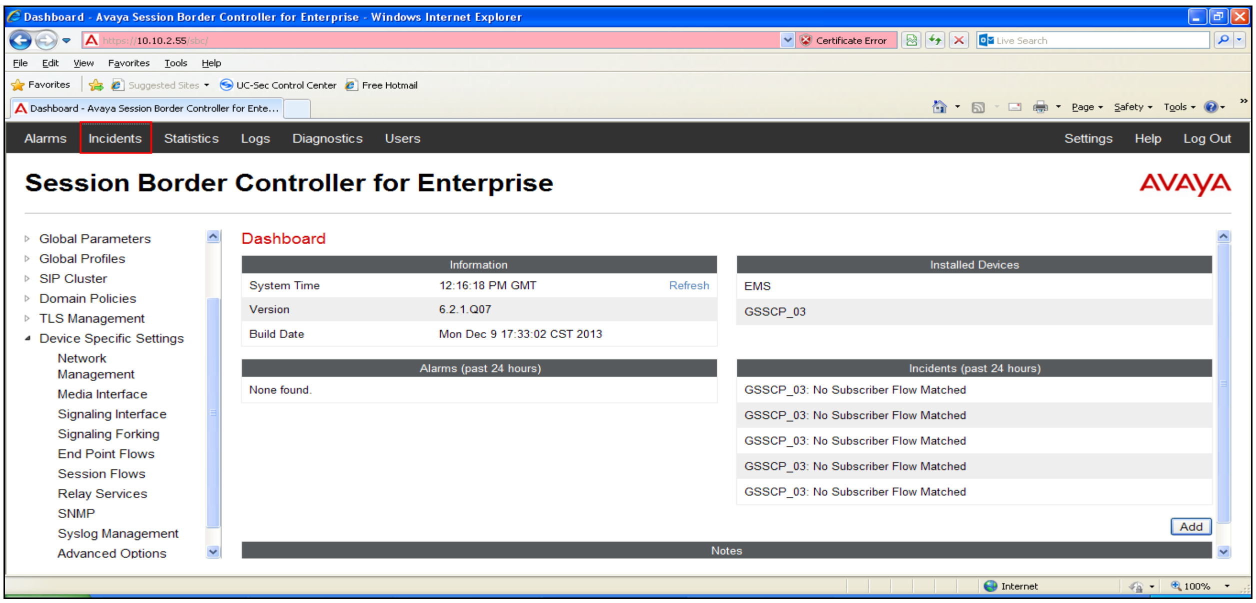


9.4. Avaya Session Boarder Controller for Enterprise Verification

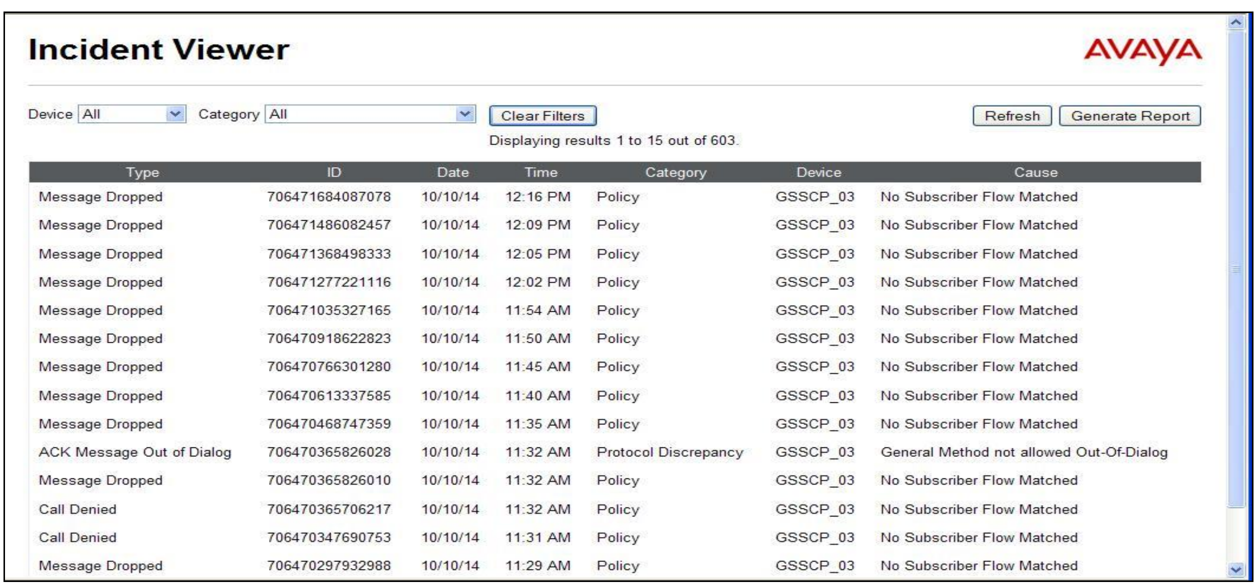
This section contains verification steps that may be performed using the Avaya Session Border Controller for Enterprise.

9.4.1. Incidents

The Incidents Log Viewer display alerts captured by the Avaya SBCE. Select the **Incidents** link along the top of the screen.



The following screen shows example SIP messages that do not match a Server Flow for an incoming message.

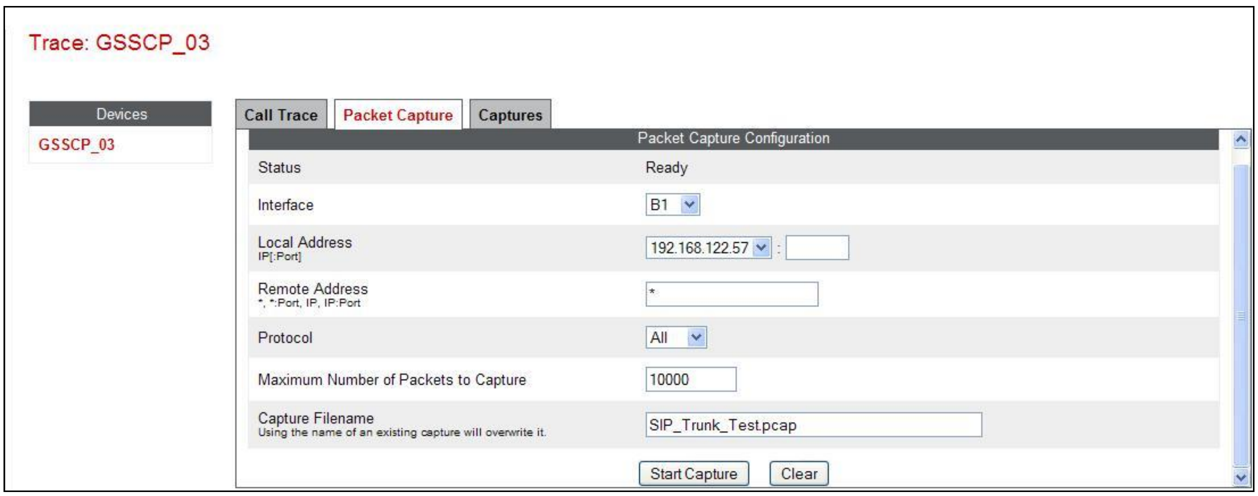


9.4.2. Trace Settings

The Trace Settings tool is for configuring and displaying call traces and packet captures for the Avaya SBCE.

To define the trace, navigate to **Device Specific Settings → Advanced Options → Troubleshooting → Trace** in the main menu on the left hand side and select the **Packet Capture** tab.

- Select the SIP Trunk interface from the **Interface** drop down menu
- Select the signalling interface IP address from the **Local Address** drop down menu
- Enter the IP address of the network SBC in the **Remote Address** field or enter a ***** to capture all traffic
- Specify the **Maximum Number of Packets to Capture**, 10000 is shown as an example
- Specify the filename of the resultant pcap file in the **Capture Filename** field



To view the trace, select the **Captures** tab and click on the relevant filename in the list of traces.

The trace is viewed as a standard pcap file in Wireshark. If the SIP trunk is working correctly, a SIP response in the form of a 200 OK will be seen from the Eircom network.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Communication Server 1000E R7.6, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise to Eircom SIP Trunk service. Eircom's SIP Trunk service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.

11. References

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

[1] *Implementing Avaya Aura® Session Manager*, Release 6.3

[2] *Installing Service Packs for Avaya Aura® Session Manager*, Release 6.3

[3] *Upgrading Avaya Aura® Session Manager*, Release 6.3

[4] *Maintaining and Troubleshooting Avaya Aura® Session Manager Release 6.3*

[5] *Installing and Configuring Avaya Aura® System Platform Release 6.3*

[6] *Implementing Avaya Aura® System Manager Release 6.3*

[7] *Upgrading Avaya Aura® System Manager to 6.3*

[8] *Avaya Communication Server 1000E Installation and Commissioning*, Document Number NN43041-310.

[9] *Feature Listing Reference Avaya Communication Server 1000*, Document Number NN43001-111, 05.01.

[10] *Linux Platform Base and Applications Installation and Commissioning Avaya Communication Server 1000*, Document Number NN43001-315

[11] *Unified Communications Management Common Servers Fundamentals Avaya Communication Server 1000*, Document Number NN43001-116

[12] *Software Input Output Reference – Maintenance Avaya Communication Server 1000*, Document Number NN43001-711

[13] *Signaling Server IP Line Applications Fundamentals Avaya Communication Server 1000*, Document Number NN43001-125

[14] *SIP Software for Avaya 1100 Series IP Deskphones-Administration*, Document Number NN43170-600

[15] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2

[16] *Upgrading Avaya Session Border Controller for Enterprise* Release 6.2

[17] *Administering Avaya Session Border Controller for Enterprise* Release 6.2

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

Appendix A – Communication Server 1000 Software

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 65 P  +
IDLE_SET_DISPLAY NORTEL
DepList 1: core Issue: 01(created: 2013-05-28 04:19:50 (est))

MDP>LAST SUCCESSFUL MDP REFRESH :2013-09-12 14:50:17(Local Time)
MDP>USING DEPLIST ZIP FILE DOWNLOADED :2013-05-28 04:30:29(est)
SYSTEM HAS NO USER SELECTED PEPS IN-SERVICE


LOADWARE VERSION: PSWV 100+

INSTALLED LOADWARE PEPS : 1
PAT#  CR #            PATCH REF #     NAME            DATE        FILENAME
00    wi01057886      ISS1:1OF1       DSP2AB07        13/09/2013  DSP2AB07.LW


ENABLED PLUGINS : 2

PLUGIN    STATUS      PRS/CR_NUM    MPLR_NUM      DESCRIPTION
-------------------------------------------------------------
201       ENABLED     Q00424053     MPLR08139     PI:Cant XFER OUTG TRK TO OUTG TRK
501       ENABLED     Q02138637     MPLR30070     Enables blind transfer to a SIP endpoint even
if SIP UPDATE is not supported by the far en
```

Communication Server 1000E call server deplists

```
VERSION 4121
RELEASE 7
ISSUE 65 P +
DepList 1: core Issue: 01 (created: 2013-05-28 04:19:50 (est))

IN-SERVICE PEPS
PAT# CR #            PATCH REF #     NAME      DATE        FILENAME       SPECINS
000  wi01058359      ISS1:1OF1       p32331_1  24/04/2014  p32331_1.cpl   NO
001  wi01064599      iss1:1of1       p32580_1  24/04/2014  p32580_1.cpl   NO
002  wi01056067      ISS1:1OF1       p32457_1  24/04/2014  p32457_1.cpl   NO
003  wi01063263      ISS1:1OF1       p32573_1  24/04/2014  p32573_1.cpl   NO
004  wi01065842      ISS1:1OF1       p32478_1  24/04/2014  p32478_1.cpl   NO
005  wi01062607      ISS1:1OF1       p32503_1  24/04/2014  p32503_1.cpl   NO
006  wi01070756      ISS1:1OF1       p32444_1  24/04/2014  p32444_1.cpl   NO
007  wi01039280      ISS1:1OF1       p32423_1  24/04/2014  p32423_1.cpl   NO
008  wi01087543      ISS1:1OF1       p32662_1  24/04/2014  p32662_1.cpl   NO
009  wi00933195      ISS1:1OF1       p32491_1  24/04/2014  p32491_1.cpl   NO
010  wi01071379      ISS1:1OF1       p32522_1  24/04/2014  p32522_1.cpl   NO
011  wi01068669      ISS1:1OF1       p32333_1  24/04/2014  p32333_1.cpl   NO
012  wi01066991      ISS1:1OF1       p32449_1  24/04/2014  p32449_1.cpl   NO
013  wi01070474      iss1:1of1       p32407_1  24/04/2014  p32407_1.cpl   NO
014  WI0110261       ISS1:1OF1       p32758_1  24/04/2014  p32758_1.cpl   NO
015  wi01094305      ISS1:1OF1       p32640_1  24/04/2014  p32640_1.cpl   NO
016  wi01047890      ISS1:1OF1       p32697_1  24/04/2014  p32697_1.cpl   NO
017  wi01055300      ISS1:1OF1       p32543_1  24/04/2014  p32543_1.cpl   NO
```

018	wi01082456	ISS1:1OF1	p32596_1	24/04/2014	p32596_1.cpl	NO
019	wi01058621	ISS1:1OF1	p32339_1	24/04/2014	p32339_1.cpl	NO
020	wi01061484	ISS1:1OF1	p32576_1	24/04/2014	p32576_1.cpl	NO
021	wi01078723	ISS1:1OF1	p32532_1	24/04/2014	p32532_1.cpl	NO
022	wi01048457	ISS1:1OF1	p32581_1	24/04/2014	p32581_1.cpl	NO
023	wi01075355	ISS1:1OF1	p32594_1	24/04/2014	p32594_1.cpl	NO
024	wi01053597	ISS1:1OF1	p32304_1	24/04/2014	p32304_1.cpl	NO
025	wi01045058	ISS1:1OF1	p32214_1	24/04/2014	p32214_1.cpl	NO
026	wi01075359	ISS1:1OF1	p32671_1	24/04/2014	p32671_1.cpl	NO
027	wi01025156	ISS1:1OF1	p32136_1	24/04/2014	p32136_1.cpl	NO
028	wi01061481	ISS1:1OF1	p32382_1	24/04/2014	p32382_1.cpl	NO
029	wi01035976	ISS1:1OF1	p32173_1	24/04/2014	p32173_1.cpl	NO
030	wi01088775	ISS1:1OF1	p32659_1	24/04/2014	p32659_1.cpl	NO
031	wi01070465	iss1:1of1	p32562_1	24/04/2014	p32562_1.cpl	NO
032	wi01088585	ISS1:1OF1	p32656_1	24/04/2014	p32656_1.cpl	NO
033	wi01063864	ISS1:1OF1	p32410_1	24/04/2014	p32410_1.cpl	YES
034	wi01034961	ISS1:1OF1	p32144_1	24/04/2014	p32144_1.cpl	NO
035	wi01055480	ISS1:1OF1	p32712_1	24/04/2014	p32712_1.cpl	NO
036	wi01034307	ISS1:1OF1	p32615_1	24/04/2014	p32615_1.cpl	NO
037	wi01065118	ISS1:1OF1	p32397_1	24/04/2014	p32397_1.cpl	NO
038	wi01075360	iss1:1of1	p32602_1	24/04/2014	p32602_1.cpl	NO
039	wi00884716	ISS1:1OF1	p32517_1	24/04/2014	p32517_1.cpl	NO
040	wi01068851	ISS1:1OF1	p32439_1	24/04/2014	p32439_1.cpl	NO
041	wi01053314	ISS1:1OF1	p32555_1	24/04/2014	p32555_1.cpl	NO
042	wi01059388	iss1:1of1	p32628_1	24/04/2014	p32628_1.cpl	NO
043	wi01087528	ISS1:1OF1	p32700_1	24/04/2014	p32700_1.cpl	NO
044	wi01072027	ISS1:1OF1	p32689_1	24/04/2014	p32689_1.cpl	NO
045	wi01052428	ISS1:1OF1	p32606_1	24/04/2014	p32606_1.cpl	NO
046	wi01053920	ISS1:1OF1	p32303_1	24/04/2014	p32303_1.cpl	NO
047	wi01070468	iss1:1of1	p32418_1	24/04/2014	p32418_1.cpl	NO
048	wi01067822	ISS1:1OF1	p32466_1	24/04/2014	p32466_1.cpl	YES
049	wi01060826	ISS1:1OF1	p32379_1	24/04/2014	p32379_1.cpl	NO
050	wi01075352	ISS1:1OF1	p32603_1	24/04/2014	p32603_1.cpl	NO
051	wi01043367	ISS1:1OF1	p32232_1	24/04/2014	p32232_1.cpl	NO
052	wi01083584	ISS1:1OF1	p32619_1	24/04/2014	p32619_1.cpl	NO
053	wi01060241	ISS1:1OF1	p32381_1	24/04/2014	p32381_1.cpl	NO
054	wi01053195	ISS1:1OF1	p32297_1	24/04/2014	p32297_1.cpl	NO
055	wi00897254	ISS1:1OF1	p31127_1	24/04/2014	p31127_1.cpl	NO
056	wi01061483	ISS1:1OF1	p32359_1	24/04/2014	p32359_1.cpl	NO
057	wi01085855	ISS1:1OF1	p32658_1	24/04/2014	p32658_1.cpl	NO
058	wi01075353	ISS1:1OF1	p32613_1	24/04/2014	p32613_1.cpl	NO
059	wi01070471	ISS1:1OF1	p32415_1	24/04/2014	p32415_1.cpl	NO
060	wi01074003	ISS1:1OF1	p32421_1	24/04/2014	p32421_1.cpl	NO
061	wi01060382	iss1:1of1	p32623_1	24/04/2014	p32623_1.cpl	YES
062	wi01068042	ISS1:1OF1	p32669_1	24/04/2014	p32669_1.cpl	NO
063	wi01072023	ISS1:1OF1	p32130_1	24/04/2014	p32130_1.cpl	YES
064	wi01065922	ISS1:1OF1	p32516_1	24/04/2014	p32516_1.cpl	NO
065	wi01057403	ISS1:1OF1	p32591_1	24/04/2014	p32591_1.cpl	NO
066	wi01069441	ISS1:1OF1	p32097_1	24/04/2014	p32097_1.cpl	NO
067	wi01070473	ISS1:1OF1	p32413_1	24/04/2014	p32413_1.cpl	NO
068	wi01056633	ISS1:1OF1	p32322_1	24/04/2014	p32322_1.cpl	NO
069	wi01052968	ISS1:1OF1	p32540_1	24/04/2014	p32540_1.cpl	NO
070	wi01072032	ISS1:1OF1	p32448_1	24/04/2014	p32448_1.cpl	NO
071	wi01073100	ISS1:1OF1	p32599_1	24/04/2014	p32599_1.cpl	NO
072	wi01035980	ISS1:1OF1	p32558_1	24/04/2014	p32558_1.cpl	NO
073	wi01041453	ISS1:1OF1	p32587_1	24/04/2014	p32587_1.cpl	NO
074	wi01032756	ISS1:1OF1	p32673_1	24/04/2014	p32673_1.cpl	NO
075	wi01092300	ISS1:1OF1	p32692_1	24/04/2014	p32692_1.cpl	NO
076	wi00996734	ISS1:1OF1	p32550_1	24/04/2014	p32550_1.cpl	NO
077	wi01022599	ISS1:1OF1	p32080_1	24/04/2014	p32080_1.cpl	NO
078	wi01060341	ISS1:1OF1	p32578_1	24/04/2014	p32578_1.cpl	NO
079	wi01091447	ISS1:1OF1	p32675_1	24/04/2014	p32675_1.cpl	NO
080	wi01070580	ISS1:1OF1	p32380_1	24/04/2014	p32380_1.cpl	NO
081	wi01089519	ISS1:1OF1	p32665_1	24/04/2014	p32665_1.cpl	NO
082	WI01077073	ISS1:1OF1	p32534_1	24/04/2014	p32534_1.cpl	NO
083	wi01080753	ISS1:1OF1	p32518_1	24/04/2014	p32518_1.cpl	NO
084	wi01065125	ISS1:1OF1	p32416_1	24/04/2014	p32416_1.cpl	NO

Communication Server 1000E signaling server service updates

```
In System service updates: 36
PATCH#  IN_SERVICE   DATE       SPECINS   REMOVABLE   NAME
0       Yes          14/07/14   YES       YES         cs1000-csmWeb-7.65.16.22-2.i386.000
1       Yes          14/07/14   YES       YES         cs1000-linuxbase-7.65.16.23-1.i386.000
2       Yes          02/04/14   YES       yes         tzdata-2013c-2.el5.i386.001
3       Yes          14/07/14   NO        YES         cs1000-Jboss-Quantum-7.65.16.22-8.i386.000
4       Yes          14/07/14   YES       YES         cs1000-patchWeb-7.65.16.22-4.i386.000
5       Yes          14/07/14   YES       YES         cs1000-dmWeb-7.65.16.22-6.i386.000
6       Yes          27/09/13   NO        yes         cs1000-cs1000WebService_6-0-7.65.16.21-
00.i386.000
7       Yes          14/07/14   YES       YES         cs1000-csoneksvrmgr-7.65.16.22-5.i386.000
8       Yes          27/09/13   NO        YES         cs1000-pd-7.65.16.21-00.i386.000
9       Yes          27/09/13   NO        YES         cs1000-shared-carrdtct-7.65.16.21-
01.i386.000
10      Yes          27/09/13   NO        YES         cs1000-shared-tpselect-7.65.16.21-
01.i386.000
11      Yes          14/07/14   YES       YES         cs1000-baseWeb-7.65.16.22-4.i386.000
12      Yes          27/09/13   NO        yes         cs1000-dbcom-7.65.16.21-00.i386.000
13      Yes          14/07/14   YES       YES         cs1000-bcc-7.65.16.22-14.i386.000
15      Yes          02/04/14   YES       YES         cs1000-cs-7.65.P.100-02.i386.000
23      Yes          02/04/14   NO        YES         cs1000-shared-omm-7.65.16.21-2.i386.000
25      Yes          14/07/14   YES       YES         cs1000-ftrpkg-7.65.16.22-2.i386.000
27      Yes          14/07/14   YES       YES         cs1000-oam-logging-7.65.16.22-4.i386.000
30      Yes          02/10/13   NO        YES         cs1000-snmp-7.65.16.21-00.i686.000
31      Yes          14/07/14   YES       YES         cs1000-csv-7.65.16.22-2.i386.000
32      Yes          14/07/14   YES       YES         cs1000-tps-7.65.16.22-8.i386.000
33      Yes          14/07/14   YES       YES         cs1000-nrsm-7.65.16.22-3.i386.000
34      Yes          14/07/14   YES       YES         cs1000-mscTone-7.65.16.22-2.i386.000
35      Yes          14/07/14   YES       YES         cs1000-mscMusc-7.65.16.22-4.i386.000
36      Yes          14/07/14   YES       YES         cs1000-mscConf-7.65.16.22-2.i386.000
38      Yes          02/04/14   YES       YES         cs1000-emWebLocal_6-0-7.65.16.22-1.i386.000
40      Yes          02/04/14   YES       YES         cs1000-ipsec-7.65.16.22-1.i386.000
42      Yes          02/04/14   NO        YES         cs1000-cppmUtil-7.65.16.22-1.i686.000
47      Yes          14/07/14   YES       YES         cs1000-mscAnnc-7.65.16.22-2.i386.000
48      Yes          14/07/14   YES       YES         cs1000-mscAttn-7.65.16.22-2.i386.000
49      Yes          14/07/14   NO        YES         cs1000-gk-7.65.16.22-1.i386.000
50      Yes          14/07/14   YES       YES         cs1000-emWeb_6-0-7.65.16.22-9.i386.000
51      Yes          14/07/14   NO        YES         cs1000-sps-7.65.16.22-3.i386.000
52      Yes          14/07/14   YES       YES         cs1000-shared-pbx-7.65.16.22-3.i386.000
53      Yes          14/07/14   YES       YES         cs1000-shared-xmsg-7.65.16.22-1.i386.000
54      Yes          14/07/14   YES       YES         cs1000-vtrk-7.65.16.22-50.i386.000
```

Communication Server 1000E system software

```
Product Release: 7.65.16.00
Base Applications
   base                        7.65.16     [patched]
   NTAFS                       7.65.16
   sm                          7.65.16
   cs1000-Auth                 7.65.16
   Jboss-Quantum               n/a         [patched]
   cnd                         7.65.16
   lhmonitor                   7.65.16
   baseAppUtils                7.65.16
   dfoTools                    7.65.16
   cppmUtil                    n/a         [patched]
   oam-logging                 n/a         [patched]
   dmWeb                       n/a         [patched]
   baseWeb                     n/a         [patched]
   ipsec                       n/a         [patched]
   Snmp-Daemon-TrapLib         n/a         [patched]
   ISECSH                      7.65.16
   patchWeb                    n/a         [patched]
   EmCentralLogic              7.65.16
Application configuration: CS+SS+NRS+EM
Packages:
CS+SS+NRS+EM
Configuration version:     7.65.16-00
   cs                          7.65.16     [patched]
```

```
    dbcom                        7.65.16.21  [patched]
    cslogin                      7.65.16
    sigServerShare               7.65.16     [patched]
    csv                          7.65.16     [patched]
    tps                          7.65.16     [patched]
    vtrk                         7.65.16     [patched]
    pd                           7.65.16.21  [patched]
    sps                          7.65.16     [patched]
    ncs                          7.65.16
    gk                           7.65.16     [patched]
    nrsm                         7.65.16     [patched]
    nrsmWebService               7.65.16
    managedElementWebService     7.65.16
    EmConfig                     7.65.16
    emWeb_6-0                    7.65.16     [patched]
    emWebLocal_6-0               7.65.16     [patched]
    csmWeb                       7.65.16     [patched]
    bcc                          7.65.16     [patched]
    ftrpkg                       7.65.16     [patched]
    cs1000WebService_6-0         7.65.16     [patched]
    mscAnnc                      7.65.16     [patched]
    mscAttn                      7.65.16     [patched]
    mscConf                      7.65.16     [patched]
    mscMusc                      7.65.16     [patched]
    mscTone                      7.65.16     [patched]
```

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.