



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Configuring Avaya Aura ® Communication Server 1000 R7.65, Avaya Aura ® Session Manager 7.0 and Avaya Session Border Controller for Enterprise R7.0 to support KCOM SIP Connect - Issue 1.0**

## **Abstract**

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between KCOM SIP Connect and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise, Avaya Aura® Session Manager and Avaya Communication Server 1000. KCOM is a member of the DevConnect Service Provider program.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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

# 1. Introduction

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between KCOM SIP Connect and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of the following: Avaya Communication Server 1000 R7.65 (CS1000); Avaya Aura® Session Manager R7.0 (Session Manager) and Avaya Session Border Controller for Enterprise R7.0 (Avaya SBCE). Note that the shortened names shown in brackets will be used throughout the remainder of the document. Customers using this Avaya SIP-enabled enterprise solution with KCOM SIP Connect are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise customer.

## 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 1000, Session Manager and Avaya SBCE. The enterprise site was configured to connect to KCOM SIP Connect.

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 PSTN phones using the SIP trunk provided by KCOM, calls made to SIP, UNISim, Digital and Analog telephones at the enterprise.
- All inbound PSTN calls were routed to the enterprise across the SIP trunk to KCOM.
- Outgoing calls from the enterprise site completed via KCOM's SIP trunk to PSTN destinations, calls made from SIP, UNISim, Digital and Analog telephones.
- All outbound PSTN calls were routed from the enterprise across the SIP trunk to KCOM.
- Inbound and outbound PSTN calls to/from Avaya One-X® Communicator softphone.
- Calls using the G.711A and G.729 codec's.
- Fax calls to/from a group 3 fax machine to a PSTN-connected fax machine using T.38.
- Caller ID Presentation and Caller ID Restriction.
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer and conference.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Off-net call forwarding and mobile twinning.
- Transmission and response of SIP OPTIONS messages sent by KCOM's SIP trunk requiring Avaya response and sent by Avaya requiring KCOM' response.

## 2.2. Test Results

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

- The CS1000 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 for blind transfer. With the installation of plugin 501 on the CS1000, 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 features such as on-net and off-net calling were not tested as the From Header CLID containing the Mobile-X mobility number on inbound calls to KCOM SIP Connect was automatically changed by KCOM to a CLID number recognizable to the KCOM network.
- All unwanted MIME was stripped on outbound calls using the Adaptation Module in Session Manager.
- No inbound toll free numbers were tested, however routing of inbound DDI numbers and the relevant number translation was successfully tested.
- Access to Emergency Services was not tested as no test call had been booked with the Emergency Services Operator.

## 2.3. Support

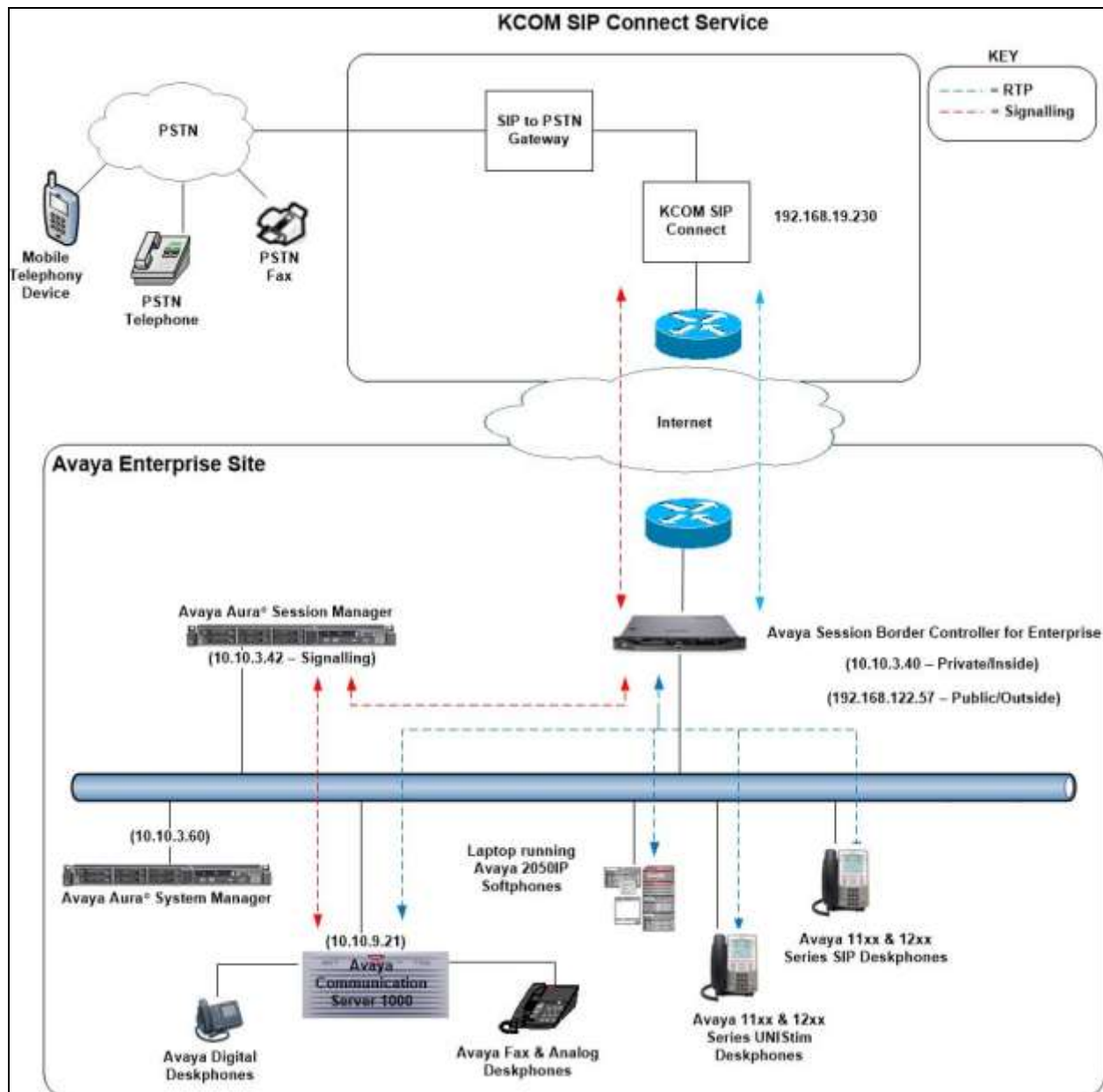
For technical support on the Avaya products described in these Application Notes visit <http://support.avaya.com>.

For technical support on KCOM products described in these Application Notes, please contact KCOM Customer Support at:

- Telephone 0800 138 4858 – Option 2.
- <https://www.kcom.com>

### 3. Reference Configuration

**Figure 1** illustrates the test configuration. The test configuration shows an Enterprise site connected to KCOM's SIP Trunk Service. Located at the Enterprise site is an Avaya SBCE, Session Manager and CS1000. Endpoints are Avaya 1140 series IP telephones (with UNISTim and SIP firmware), Avaya 1200 series IP telephones (with UNISTim and SIP firmware), Avaya IP 2050PC Softphone, 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 KCOM SIP Connect to Avaya Enterprise**

## 4. Equipment and Software Validated

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

| Equipment/Software                             | Release/Version                                                                                                                                             |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Avaya</b>                                   |                                                                                                                                                             |
| Avaya Aura® Session Manager                    | 7.0.0.2.700201                                                                                                                                              |
| Avaya Aura® System Manager                     | 7.0.0.2.<br>Build No. – 7.0.0.016266-7.0.9.7002010<br>Software Update Revision No:<br>7.0.0.2.4416                                                          |
| Avaya Aura® Communication Server 1000          | Avaya Communication Server 1000 R7.6<br>Version 7.65.P<br>Deplst: CPL_X21_07_65P<br>All CS1000 patches listed in <b>Appendix A</b>                          |
| Avaya Communication Server 1000 Media Gateway  | CSP Version: MGCC DC01<br>MSP Version: MGCM AB02<br>APP Version: MGCA BA18<br>FPGA Version: MGCF AA22<br>BOOT Version: MGCB BA18<br>DSP1 Version: DSP2 AB07 |
| Avaya Session Border Controller for Enterprise | 7.0.0-21-6602                                                                                                                                               |
| Avaya 1140e and 1230 UNISTim Telephones        | FW: 0625C8A                                                                                                                                                 |
| Avaya 1140e and 1230 SIP Telephones            | FW: 04.10.18.00.bin                                                                                                                                         |
| Avaya 2050PC                                   | Release 4.3.0081                                                                                                                                            |
| Avaya Analog Telephone                         | N/A                                                                                                                                                         |
| Avaya M3904 Digital Telephone                  | N/A                                                                                                                                                         |
| <b>KCOM</b>                                    |                                                                                                                                                             |
| Metaswitch Call Feature Server                 | V9.0.10 SU20                                                                                                                                                |
| Metaswitch Universal Media Gateway             | V9.0.10 SU27                                                                                                                                                |
| Metaswitch Perimeta SBC                        | V3.7.40 SU16                                                                                                                                                |

## 5. Configure Avaya Communication Server 1000

This section describes the steps required to configure CS1000 for SIP Trunking and also the basic configuration for telephones (analog, SIP and IP phones). SIP trunks are established between CS1000 and Session Manager. SIP trunks are also established between Session Manager and the Avaya SBCE private interface. The Avaya SBCE public interface connects to KCOM SIP Connect. Incoming PSTN calls from the KCOM SIP Connect service traverse the Avaya SBCE and are directed to the Session Manager, which directs the calls to CS1000 (see **Figure 1**).

When a SIP message arrives at CS1000, 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 CS1000 and may be first subject to outbound features such as route selection, digit manipulation and class of service restrictions. When CS1000 selects a SIP trunk for outgoing PSTN calls, SIP signaling 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 the KCOM SIP Connect service.

Specific CS1000 configuration was performed using Element Manager and the system terminal interface. The general installation of the CS1000, 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.

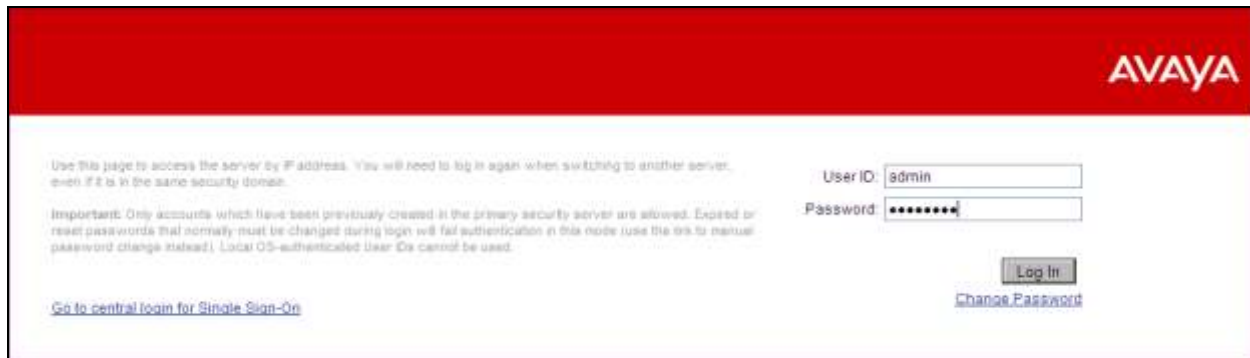
### 5.1. Logging into the Avaya Communication Server 1000

Configuration on the CS1000 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 CS1000. Avaya Unified Communications Management can also be implemented on System Manager.

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



AVAYA

Use this page to access the server by IP address. You will need to log in again when switching to another server, even if it is in the same security domain.

Important: Only accounts which have been previously created in the primary security server are allowed. Expired or reset passwords that normally must be changed during login will fail authentication in this mode (use the link to manual password change instead). Local OS-authenticated user IDs cannot be used.

User ID:

Password:

[Change Password](#)

[Go to central login for Single Sign-On](#)

The Avaya Unified Communications Management **Elements** page will be used for configuration. Click on the Element Name corresponding to CS1000 in the Element Type column. In the abridged screen below, the user would click on the Element Name **EM on cs1kv19**.

Host Name: 10.10.9.57 User Name: admin

### Elements

New elements are registered into the security framework, or may be added as simple hyperlinks. Click an element name to launch its management service. You can optionally filter the list by entering a search term.

| <input type="checkbox"/> | Element Name               | Element Type             | Release | Address      | Description      |
|--------------------------|----------------------------|--------------------------|---------|--------------|------------------|
| <input type="checkbox"/> | smgrv9.avaya.com (primary) | Base OS                  | 7.6     | 10.10.9.57   | Base OS element. |
| <input type="checkbox"/> | <b>EM on cs1kv19</b>       | CS1000                   | 7.6     | 192.168.27.2 | New element.     |
| <input type="checkbox"/> | cs1kv19.avaya.com (member) | Linux Base               | 7.6     | 88.47.122.35 | Base OS element. |
| <input type="checkbox"/> | 192.168.27.3               | Media Gateway Controller | 7.6     | 192.168.27.3 | New element.     |
| <input type="checkbox"/> | NRSM on cs1kv19            | Network Routing Service  | 7.6     | 192.168.27.2 | New element.     |

## 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 CS1000 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 KCOM 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 CS1000.

```

System type is - Communication Server 1000/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

KCOM's SIP Trunk supports G.711A and G.729 voice codecs. Using the CS1000 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 CS1000 **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.

Managing: 192.168.27.2 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details » VGW and Codecs

#### Node ID: 200 - Voice Gateway (VGW) and Codecs

[General](#) | [Voice Codecs](#) | [Fax](#)

##### Voice Codecs

Codec G711: ☒ Enabled (required)

Voice payload size: 20 (milliseconds per frame)

Voice playout (jitter buffer) delay: 40 80 (milliseconds)

Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

☐ Voice Activity Detection (VAD)

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

Managing: 192.168.27.2 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details » VGW and Codecs

### Node ID: 200 - Voice Gateway (VGW) and Codecs

[General](#) | [Voice Codecs](#) | [Fax](#)

Codec G729: ☒ Enabled

Voice payload size: 20 (milliseconds per frame)

Voice playout (jitter buffer) delay: 40 80 (milliseconds)

Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

☐ Voice Activity Detection (VAD)

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

**Fax**

Codec name: T.38 FAX

Maximum rate: 14400 (bps)

Fax TCF method: 2

Fax playout nominal delay: 100 (0 - 300 milliseconds)

FAX no activity timeout: 20 (10 - 32000 milliseconds)

Packet size: 30 (bps)

## 5.4. Virtual Trunk Gateway Configuration

Use CS1000 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 CS1000, it is the Node IPv4 address that is used (see **Section 6.5** – Define SIP Entities for more details).

Managing: 192.168.27.2 Username: admin

System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 200 - SIP Line, LTPS, PD, Gateway ( SIPGw ))

Node ID:  \* (0-9999)

Call server IP address:  \*

Embedded LAN (ELAN)  
Gateway IP address:  \*  
Subnet mask:  \*

TLAN address type: ☒ IPv4 only  
☐ IPv4 and IPv6

Telephony LAN (TLAN)  
Node IPv4 address:  \*  
Subnet mask:  \*  
Node IPv6 address:

IP Telephony Node Properties

- [Voice Gateway \(VGW\) and Codecs](#)
- [Quality of Service \(QoS\)](#)
- [LAN](#)
- [SNTP](#)
- [Numbering Zones](#)
- [MCDN Alternative Routing Treatment \(MALT\) Causes](#)

Applications (click to edit configuration)

- [SIP Line](#)
- [Terminal Proxy Server \(TPS\)](#)
- [Gateway \(SIPGw\)](#)
- [Personal Directories \(PD\)](#)
- [Presence Publisher](#)
- [IP Media Services](#)

\* Required Value.

Save

Cancel

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.

Managing: 192.168.27.2 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

### Node ID: 200 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

Vtrk gateway application: ☒ Enable gateway service on this node

**General**

Vtrk gateway application: SIP Gateway (SIPGw) ▼

SIP domain name: avaya.com \*

Local SIP port: 5060 \* (1 - 65535)

Gateway endpoint name: cs1kv9 \*

Gateway password: \*

Application node ID: 200 \* (0-9999)

Enable failsafe NRS: ☐

Note: FailSafe NRS cannot be enabled, if all servers in the node have NRS application deployed.

**Virtual Trunk Network Health Monitor**

☐ Monitor IP addresses (listed below)

Information will be captured for the IP addresses listed below.

Monitor IP:

Monitor addresses:

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                             |                           |                      |                                         |                                       |                                                     |                                           |                                                            |                                                             |                                                     |                                                            |  |                                        |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|---------------------------|----------------------|-----------------------------------------|---------------------------------------|-----------------------------------------------------|-------------------------------------------|------------------------------------------------------------|-------------------------------------------------------------|-----------------------------------------------------|------------------------------------------------------------|--|----------------------------------------|--|
| <b>Proxy Or Redirect Server:</b><br><b>Proxy Server Route 1:</b><br>Primary TLAN IP address: <input type="text" value="10.10.3.42"/><br><small>The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"</small><br>Port: <input type="text" value="5060"/> (1 - 65535)<br>Transport protocol: <input type="text" value="TCP"/><br>Options: <input checked="" type="checkbox"/> Support registration<br><input checked="" type="checkbox"/> Primary CDS proxy<br>Secondary TLAN IP address: <input type="text" value="0.0.0.0"/><br><small>The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"</small><br>Port: <input type="text" value="5060"/> (1 - 65535) |                                                             |                           |                      |                                         |                                       |                                                     |                                           |                                                            |                                                             |                                                     |                                                            |  |                                        |  |
| <b>SIP URI Map:</b><br><table border="0"> <tr> <td>Public E.164 domain names</td> <td>Private domain names</td> </tr> <tr> <td>National: <input type="text" value=""/></td> <td>UDP: <input type="text" value="udp"/></td> </tr> <tr> <td>Subscriber: <input type="text" value="subscriber"/></td> <td>CDP: <input type="text" value="cdp.udp"/></td> </tr> <tr> <td>Special number: <input type="text" value="PublicSpecial"/></td> <td>Special number: <input type="text" value="PrivateSpecial"/></td> </tr> <tr> <td>Unknown: <input type="text" value="PublicUnknown"/></td> <td>Vacant number: <input type="text" value="PrivateUnknown"/></td> </tr> <tr> <td></td> <td>Unknown: <input type="text" value=""/></td> </tr> </table> |                                                             | Public E.164 domain names | Private domain names | National: <input type="text" value=""/> | UDP: <input type="text" value="udp"/> | Subscriber: <input type="text" value="subscriber"/> | CDP: <input type="text" value="cdp.udp"/> | Special number: <input type="text" value="PublicSpecial"/> | Special number: <input type="text" value="PrivateSpecial"/> | Unknown: <input type="text" value="PublicUnknown"/> | Vacant number: <input type="text" value="PrivateUnknown"/> |  | Unknown: <input type="text" value=""/> |  |
| Public E.164 domain names                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Private domain names                                        |                           |                      |                                         |                                       |                                                     |                                           |                                                            |                                                             |                                                     |                                                            |  |                                        |  |
| National: <input type="text" value=""/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | UDP: <input type="text" value="udp"/>                       |                           |                      |                                         |                                       |                                                     |                                           |                                                            |                                                             |                                                     |                                                            |  |                                        |  |
| Subscriber: <input type="text" value="subscriber"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | CDP: <input type="text" value="cdp.udp"/>                   |                           |                      |                                         |                                       |                                                     |                                           |                                                            |                                                             |                                                     |                                                            |  |                                        |  |
| Special number: <input type="text" value="PublicSpecial"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Special number: <input type="text" value="PrivateSpecial"/> |                           |                      |                                         |                                       |                                                     |                                           |                                                            |                                                             |                                                     |                                                            |  |                                        |  |
| Unknown: <input type="text" value="PublicUnknown"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Vacant number: <input type="text" value="PrivateUnknown"/>  |                           |                      |                                         |                                       |                                                     |                                           |                                                            |                                                             |                                                     |                                                            |  |                                        |  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Unknown: <input type="text" value=""/>                      |                           |                      |                                         |                                       |                                                     |                                           |                                                            |                                                             |                                                     |                                                            |  |                                        |  |

## 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.

Managing: 192.168.27.2 Username: admin  
System » IP Network » Zones » Bandwidth Zones

### Bandwidth Zones

Add... Edit... Import... Export Maintenance... Delete

|   | Zone ▲ | Intrazone Bandwidth | Intrazone Strategy | Interzone Bandwidth | Interzone Strategy | Resource Type | Zone Intent | Description |
|---|--------|---------------------|--------------------|---------------------|--------------------|---------------|-------------|-------------|
| 1 | 1      | 1000000             | BQ                 | 1000000             | BQ                 | SHARED        | VTRK        |             |
| 2 | 2      | 1000000             | BQ                 | 1000000             | BQ                 | SHARED        | MO          |             |

## 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 UNISlim telephones depending on the particular test case being executed.

Managing: 192.168.27.2 Username: admin  
Dialing and Numbering Plans » Incoming Digit Translation » Customer 00 » Digit Conversion Tree 0 Configuration

### Digit Conversion Tree 0 Configuration

Regular IDC tree  
Send calling party DID disabled

Add... Delete IDC Delete IDC tree

|   | Incoming Digits ▼ | Converted Digits | CPND Name |
|---|-------------------|------------------|-----------|
| 1 | 11 69             | 6500             |           |
| 2 | 11 68             | 6003             |           |
| 3 | 11 67             | 6005             |           |
| 4 | 11 66             | 6001             |           |
| 5 | 11 65             | 6000             |           |

## 5.7. Configure SIP Trunks

CS1000 virtual trunks will be used for all inbound and outbound PSTN calls to the KCOM SIP Connect service. Six separate steps are required to configure CS1000 virtual trunks:

- Configure a D-Channel Handler (**DCH**); configure using the CS1000 system terminal and overlay 17.
- Configure a SIP trunk Route Data Block (**RDB**); configure using the CS1000 system terminal and overlay 16.
- Configure SIP trunk members; configure using the CS1000 system terminal and overlay 14.
- Configure a Digit Manipulation Data Block (**DGT**), configure using the CS1000 system terminal and overlay 86.
- Configure a Route List Block (**RLB**); configure using the CS1000 system terminal and overlay 86.
- Configure Co-ordinated Dialling Plan(s) (**CDP**); configure using the CS1000 system terminal and overlay 87.

The following is an example DCH configuration for SIP trunks. Load **Overlay 17** at the CS1000 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
OVLN NO
OVLS NO
```

Next, configure the SIP trunk Route Data Block (RDB) using the CS1000 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.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Overlay 16</b><br>TYPE: <b>RDB</b><br>CUST 00<br>ROUT 1<br>TYPE RDB<br>CUST 00<br><b>ROUT 1</b><br>DES VIR_TRK<br><b>TKTP TIE</b><br>NPID_TBL_NUM 0<br>ESN NO<br>RPA NO<br>CNVT NO<br>SAT NO<br>RCLS EXT<br><b>VTRK YES</b><br><b>ZONE 00001</b><br><b>PCID SIP</b><br>CRID NO<br><b>NODE 200</b><br>DTRK NO<br><b>ISDN YES</b><br><b>MODE ISLD</b><br><b>DCH 1</b><br><b>IFC SL1</b><br>PNI 00000<br>NCNA YES<br>NCRD YES<br>TRO NO<br>FALT NO<br>CTYP UKWN<br>INAC NO<br>ISAR NO<br>DAPC NO<br>MBXR NO<br>MBXOT NPA<br>MBXT 0<br>PTYP ATT<br>CNDP UKWN<br>AUTO NO<br>DNIS NO<br>DCDR NO<br><b>ICOG IAO</b><br>SRCH LIN<br>TRMB YES<br>STEP | <b>ACOD 1111</b><br>TCPP NO<br>PII NO<br>AUXP NO<br>TARG<br>CLEN 1<br>BILN NO<br>OABS<br>INST<br><b>IDC YES</b><br>DCNO 0<br>NDNO 0 *<br>DEXT NO<br>DNAM NO<br>SIGO STD<br>STYP SDAT<br>MFC NO<br>ICIS YES<br>OGIS YES<br>TIMR ICF 1920<br>OGF 1920<br>EOD 13952<br>LCT 256<br>DSI 34944<br>NRD 10112<br>DDL 70<br>ODT 4096<br>RGV 640<br>GTO 896<br>GTI 896<br>SFB 3<br>PRPS 800<br>NBS 2048<br>NBL 4096<br>IENB 5<br>TFD 0<br>VSS 0<br>VGD 6<br>EESD 1024<br>SST 5 0<br>DTD NO<br>SCDT NO<br>2 DT NO<br>NEDC ORG<br>FEDC ORG | CPDC NO<br>DLTN NO<br>HOLD 02 02 40<br>SEIZ 02 02<br>SVFL 02 02<br>DRNG NO<br>CDR NO<br>NATL YES<br>SSL<br>CFWR NO<br>IDOP NO<br>VRAT NO<br>MUS YES<br>MRT 21<br>PANS YES<br>RACD NO<br>MANO NO<br>FRL 0 0<br>FRL 1 0<br>FRL 2 0<br>FRL 3 0<br>FRL 4 0<br>FRL 5 0<br>FRL 6 0<br>FRL 7 0<br>OHQ NO<br>OHQT 00<br>CBQ NO<br>AUTH NO<br>TTBL 0<br>ATAN NO<br>OHTD NO<br>PLEV 2<br>OPR NO<br>ALRM NO<br>ART 0<br>PECL NO<br>DCTI 0<br>TIDY 1600 100<br>ATRR NO<br>TRRL NO<br>SGRP 0<br>ARDN NO<br>CTBL 0<br>AACR NO |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Next, configure virtual trunk members using the CS1000 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 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 KCOM 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 and **DMI** value is set to 10 as previously configured in the Digit Manipulation Block (DGT) in **Overlay 86**.

|                                                                                                                                                                                                                    |  |                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--------------------------------------------------------------------------------------------------------------------------------|
| <pre> <b>Overlay 86</b> CUST 0 FEAT rlb <b>RLI 10</b> ELC NO ENTR 0 LTER NO <b>ROUT 1</b> 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           </pre> |  | <pre> 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           </pre> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--------------------------------------------------------------------------------------------------------------------------------|

Next, configure Co-ordinated Dialling Plan(s) (CDP) which users will dial to reach PSTN numbers. Use the CS1000 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<br>FLEN 0<br>RRPA NO<br><b>RLI 10</b><br>CCBA NO | TSC 18<br>FLEN 0<br>RRPA NO<br><b>RLI 10</b><br>CCBA NO | TSC 800<br>FLEN 0<br>RRPA NO<br><b>RLI 10</b><br>CCBA NO | TSC 08<br>FLEN 0<br>RRPA NO<br><b>RLI 10</b><br>CCBA NO |
|------------------------------------------------------------|---------------------------------------------------------|----------------------------------------------------------|---------------------------------------------------------|

## 5.8. Configure Analog, Digital and IP Telephones

A variety of telephone types were used during the testing, the following is the configuration for the Avaya 1140e UNISim 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 RCBF
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 CCBF RTDD RBDD RBHD PGND OCBF 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 RCBF
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 CCBF RTDD RBDD RBHD PGND OCBF 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 CCBF BNRD OCBF 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
```

## 5.9. Configure the SIP Line Gateway Service

SIP terminal operation requires the CS1000 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 CS1000 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**.

Managing: 192.168.27.2 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details » SIP Line Configuration

### Node ID: 200 - SIP Line Configuration Details

General | SIP Line Gateway Settings | SIP Line Gateway Service

SIP Line Gateway Application: ☒ Enable gateway service on this node

**General**

SIP domain name:  \*

SLG endpoint name:

SLG Group ID:

SLG Local Sip port:  (1 - 65535)

SLG Local Tls port:  (1 - 65535)

**Virtual Trunk Network Health Monitor**

☐ Monitor IP addresses (listed below)  
Information will be captured for the IP addresses listed below.

Monitor IP:

Monitor addresses:

## 5.10. Configure SIP Line Telephones

When SIP Line service configuration is completed, use the CS1000 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 5.9**) 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 RCBF
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---
```

```

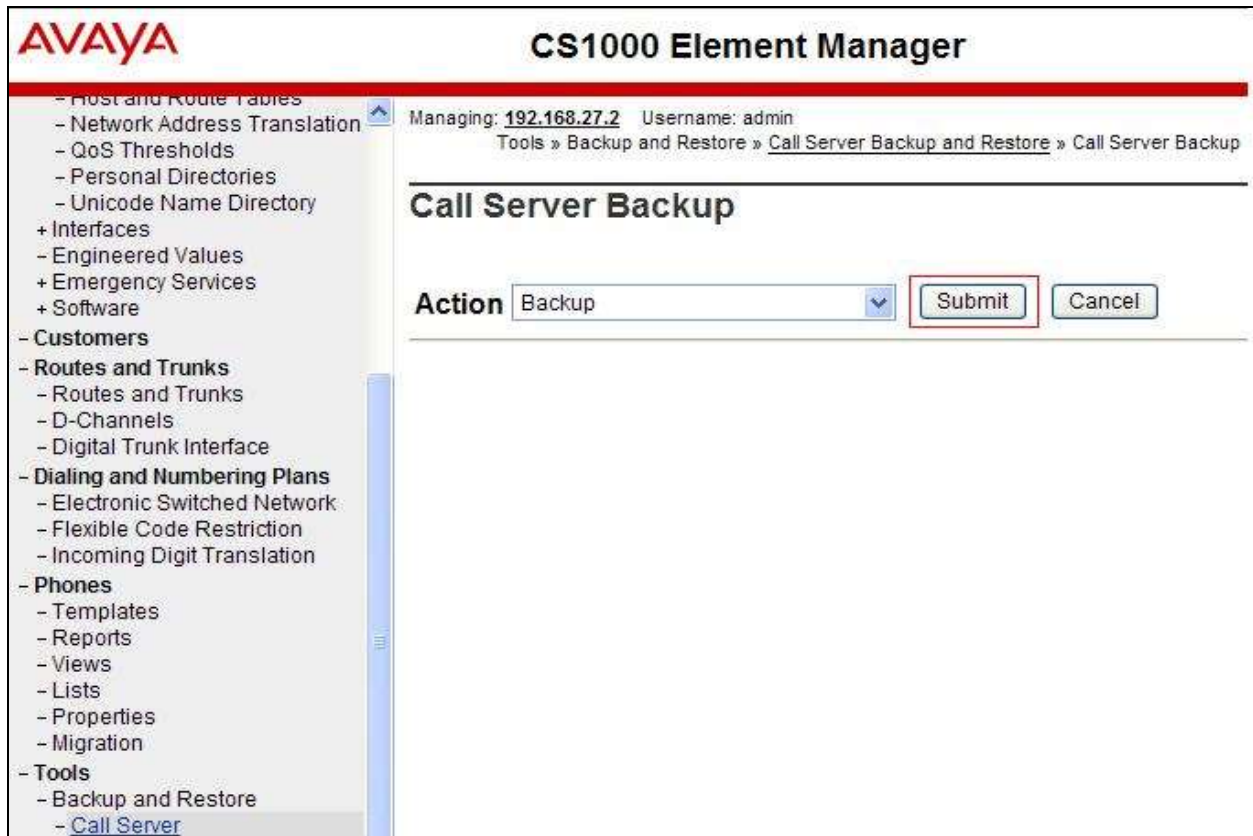
UDI RCC HBTB AHA IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
DRDD EXR0
USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBF FLXD FTTC DNDY DNO3 MCBN
FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD ELMD MSNV FRA PKCH MWTD DVLD
CROD CROD
CPND_LANG ENG
RCO 0
HUNT
LHK 0
PLEV 02
PUID
DANI NO
AST
IAPG 0 *

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

```

## 5.11. 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 screenshot shows the AVAYA CS1000 Element Manager web interface. On the left is a navigation tree with categories like Host and Route Tables, Network Address Translation, QoS Thresholds, Personal Directories, Unicode Name Directory, Interfaces, Engineered Values, Emergency Services, Software, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, and Tools. The 'Tools' category is expanded, showing 'Backup and Restore' and 'Call Server'. The main content area is titled 'Call Server Backup'. At the top, it shows 'Managing: 192.168.27.2' and 'Username: admin'. Below this is a breadcrumb trail: 'Tools » Backup and Restore » Call Server Backup and Restore » Call Server Backup'. The 'Action' dropdown menu is set to 'Backup', and the 'Submit' button is highlighted with a red box.

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.



The screenshot shows a message box with the following text: 'Backing up reten.bkp to "/>

## 6. Configuring Avaya Aura® Session Manager

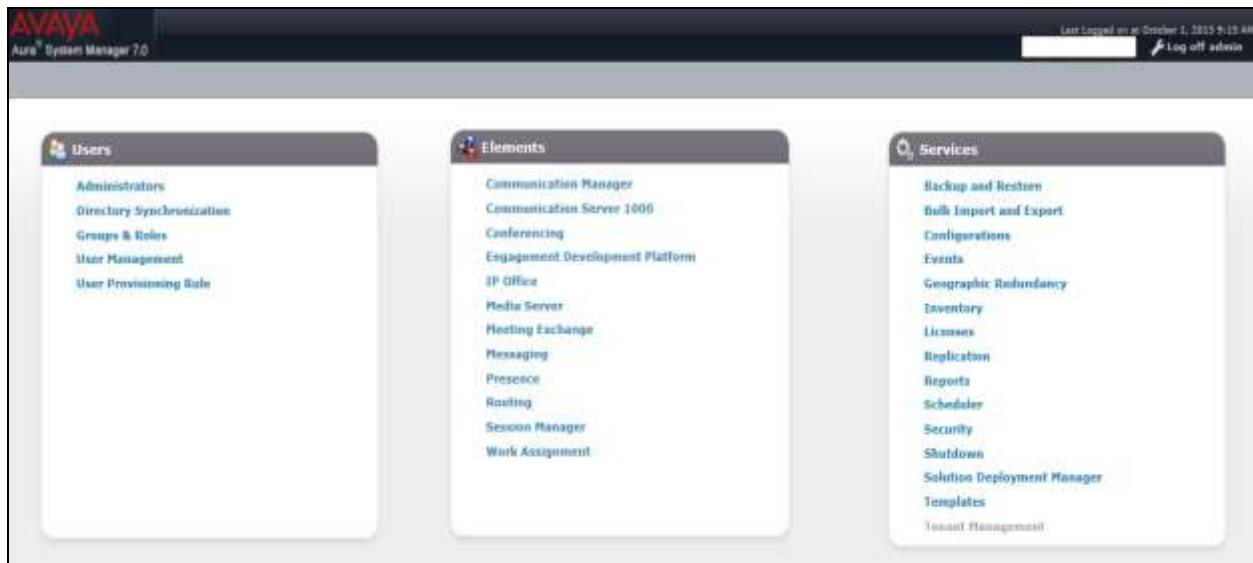
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- 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.

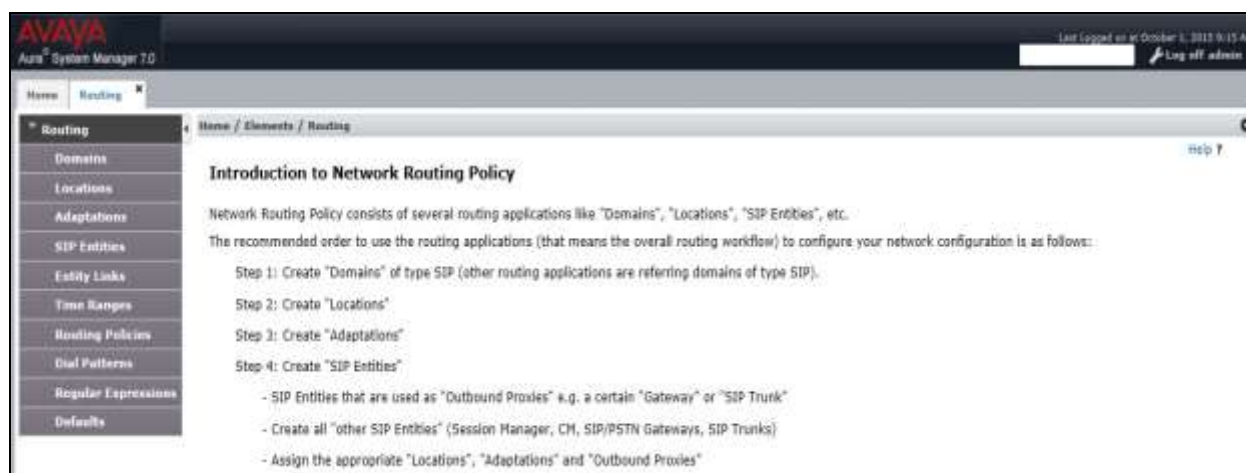
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

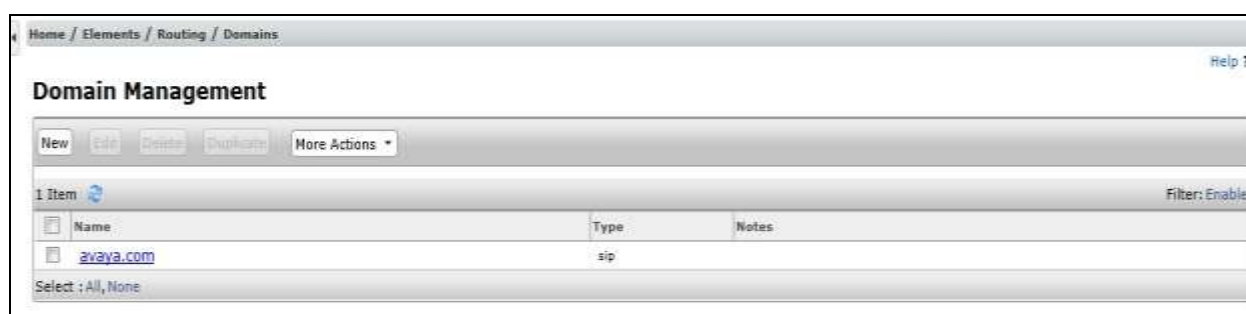


## 6.2. Administer SIP Domain

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 **SM\_7** defined for the compliance testing.

The screenshot displays the 'Location Details' configuration page for 'SM\_7'. The 'General' section includes fields for 'Name' (SM\_7) and 'Notes'. Below this is the 'Dial Plan Transparency in Survivable Mode' section with an 'Enabled' checkbox and fields for 'Listed Directory Number' and 'Associated CM SIP Entity'. The 'Overall Managed Bandwidth' section features a 'Managed Bandwidth Units' dropdown set to 'Kbit/sec', and fields for 'Total Bandwidth' and 'Multimedia Bandwidth'. A checkbox for 'Audio Calls Can Take Multimedia Bandwidth' is also present. The 'Location Pattern' section at the bottom shows a table with 3 items, each with an 'IP Address Pattern' and a 'Notes' field. The patterns listed are '\*10.10.3.\*', '\*10.10.5.\*', and '\*10.10.8.\*'. The interface includes 'Commit' and 'Cancel' buttons at the top and bottom.

| IP Address Pattern | Notes |
|--------------------|-------|
| *10.10.3.*         |       |
| *10.10.5.*         |       |
| *10.10.8.*         |       |

## 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. In order to improve interoperability with third party elements, Session Manager 7.0 incorporates the ability to use Adaptation modules to remove specific SIP headers that are either Avaya proprietary or deemed excessive/unnecessary for non-Avaya elements

For the compliance test, an Adaptation named “**KCOM**” was created to block the following headers from outbound messages, before they were forwarded to the Avaya SBCE: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector, and P-Location. These headers contain private information from the enterprise, which should not be propagated outside of the enterprise boundaries. They also add unnecessary size to outbound messages, while they have no significance to the service provider.

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**:

- **Adaption Name:** Enter an appropriate name such as **KCOM**.
- **Module Name:** Select **DigitConversionAdapter**.
- **Modular Parameter Type:** Select **Name-Value Parameter**.

Click **Add** to add the name and value parameters.

- **Name:** Enter **eRHdrs**. This parameter will remove the specific headers from messages in the egress direction.
- **Value:** Enter **AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector, P-Location**.
- **Name:** Enter **fromto**. Modifies From and To header of a message.
- **Value:** Enter **true**.
- **Name:** Enter **MIME**. Remove MIME message bodies from Session Manager.
- **Value:** Enter **no**.

| Name   | Value                                                                                           |
|--------|-------------------------------------------------------------------------------------------------|
| eRHdrs | Alert-Info, P-Charging-Vector, AV-Global-Session-ID, P-Location, P-AV-Message-ID, Endpoint-View |
| fromto | true                                                                                            |
| MIME   | no                                                                                              |

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.

| Matching Pattern | Min | Max | Phone Context | Delete Digits | Insert Digits | Address to modify | Adaptation Data | Notes |
|------------------|-----|-----|---------------|---------------|---------------|-------------------|-----------------|-------|
| *+44             | 3   | 15  |               | 3             |               | both              |                 |       |

This will ensure any incoming numbers matching +44 will have the +44 digits removed before being presented to the CS1000.

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

- 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.

| Matching Pattern | Min | Max | Phone Context | Delete Digits | Insert Digits | Address to modify | Adaptation Data | Notes |
|------------------|-----|-----|---------------|---------------|---------------|-------------------|-----------------|-------|
| *00353           | 5   | 15  |               | 2             | +             | both              |                 |       |

This will ensure any outbound numbers beginning with 00353 will be converted into E.164 international format.

## 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 1000 SIP Entity and **SIP Trunk** for the Avaya SBCE SIP Entity.
- 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 1000 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 the Session Manager SIP signalling interface and **Type** is **Session Manager**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time.

The screenshot shows the 'SIP Entity Details' configuration page. The breadcrumb trail is 'Home / Elements / Routing / SIP Entities'. The page title is 'SIP Entity Details' with 'Commit' and 'Cancel' buttons. The 'General' tab is active. Fields include: 'Name' (Session Manager), 'FQDN or IP Address' (10.10.3.42), 'Type' (Session Manager), 'Notes' (empty), 'Location' (SM\_7), 'Outbound Proxy' (empty), 'Time Zone' (Europe/Dublin), 'Credential name' (empty), and 'SIP Link Monitoring' (Use Session Manager Configuration).

| Field               | Value                             |
|---------------------|-----------------------------------|
| Name                | Session Manager                   |
| FQDN or IP Address  | 10.10.3.42                        |
| Type                | Session Manager                   |
| Notes               |                                   |
| Location            | SM_7                              |
| Outbound Proxy      |                                   |
| Time Zone           | Europe/Dublin                     |
| Credential name     |                                   |
| SIP Link Monitoring | Use Session Manager Configuration |

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 the domain added in **Section 6.2** as the default domain.

The screenshot shows the 'Listen Ports' configuration section. It includes 'TCP Failover port' and 'TLS Failover port' fields. Below is a table with 3 items, showing columns for 'Listen Ports', 'Protocol', 'Default Domain', and 'Notes'. The table contains three rows: 5060 (TCP, avaya.com), 5060 (UDP, avaya.com), and 5061 (TLS, avaya.com). There are 'Add' and 'Remove' buttons above the table, and a 'Filter: Enable' button on the right.

| Listen Ports | Protocol | Default Domain | Notes |
|--------------|----------|----------------|-------|
| 5060         | TCP      | avaya.com      |       |
| 5060         | UDP      | avaya.com      |       |
| 5061         | TLS      | avaya.com      |       |

## 6.5.2. Avaya Aura® Communication Server 1000 SIP Entity

The following screen shows the SIP entity for CS1000. The **FQDN or IP Address** field is set to the IP address of the interface on CS1000 that will be providing SIP signalling and **Type** is **Other**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time.

The screenshot shows the 'SIP Entity Details' configuration page. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / SIP Entities'. Below this, the title 'SIP Entity Details' is followed by 'Commit' and 'Cancel' buttons. The 'General' tab is selected. The form contains the following fields and values:

- Name:** CS1K\_7.6
- \* FQDN or IP Address:** 10.10.9.21
- Type:** Other (dropdown menu)
- Notes:** (empty text area)
- Adaptation:** (empty dropdown menu)
- Location:** SM\_7 (dropdown menu)
- Time Zone:** Europe/Dublin (dropdown menu)
- \* SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text area)
- Securable:** ☐
- Call Detail Recording:** none (dropdown menu)
- CommProfile Type Preference:** (empty dropdown menu)

Below the 'General' section, the 'Loop Detection' section is visible, showing:

- Loop Detection Mode:** Off (dropdown menu)

Other parameters can be set for the SIP Entity as shown in the following screenshot, but for test, these were left at default values.

This screenshot shows two additional configuration sections:

- Loop Detection:** Shows 'Loop Detection Mode' set to 'Off' (dropdown menu).
- SIP Link Monitoring:** Shows 'SIP Link Monitoring' set to 'Use Session Manager Configuration' (dropdown menu).

### 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.

The screenshot shows a web interface for configuring SIP entities. The breadcrumb navigation at the top reads "Home / Elements / Routing / SIP Entities". The main heading is "SIP Entity Details", with "General" selected as the tab. In the top right corner are "Commit" and "Cancel" buttons. The form contains the following fields and values:

- Name:** Avaya SBCE
- \* FQDN or IP Address:** 10.10.3.40
- Type:** SIP Trunk (dropdown menu)
- Notes:** (empty text area)
- Adaptation:** KCOM (dropdown menu)
- Location:** SM\_7 (dropdown menu)
- Time Zone:** Europe/Dublin (dropdown menu)
- \* SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text area)
- Securable:** ☐
- Call Detail Recording:** egress (dropdown menu)
- Loop Detection Mode:** Off (dropdown menu)

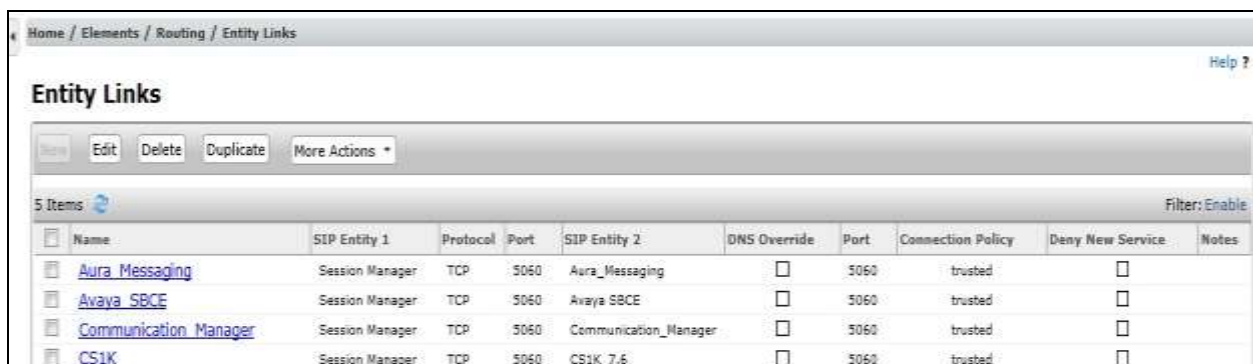
The "Loop Detection" section is partially visible at the bottom of the form.

## 6.6. Administer Entity Links

A SIP trunk between a 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 6.4**.
- 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 screenshot shows the Entity Links used in this configuration.



| Name                                  | SIP Entity 1    | Protocol | Port | SIP Entity 2          | DNS Override             | Port | Connection Policy | Deny New Service         | Notes |
|---------------------------------------|-----------------|----------|------|-----------------------|--------------------------|------|-------------------|--------------------------|-------|
| <a href="#">Aura_Messaging</a>        | Session Manager | TCP      | 5060 | Aura_Messaging        | <input type="checkbox"/> | 5060 | trusted           | <input type="checkbox"/> |       |
| <a href="#">Avaya_SBCE</a>            | Session Manager | TCP      | 5060 | Avaya_SBCE            | <input type="checkbox"/> | 5060 | trusted           | <input type="checkbox"/> |       |
| <a href="#">Communication_Manager</a> | Session Manager | TCP      | 5060 | Communication_Manager | <input type="checkbox"/> | 5060 | trusted           | <input type="checkbox"/> |       |
| <a href="#">CS1K</a>                  | Session Manager | TCP      | 5060 | CS1K_7.6              | <input type="checkbox"/> | 5060 | trusted           | <input type="checkbox"/> |       |

## 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 CS1000.

The screenshot shows the 'Routing Policy Details' form in a web application. The breadcrumb trail at the top is 'Home / Elements / Routing / Routing Policies'. The form has a 'Help' link and 'Commit' and 'Cancel' buttons. It is divided into three sections: 'General', 'SIP Entity as Destination', and 'Time of Day'.

**General**

- Name:
- Disabled: ☐
- Retries:
- Notes:

**SIP Entity as Destination**

Select

| Name     | FQDN or IP Address | Type  | Notes |
|----------|--------------------|-------|-------|
| CS1K_7.6 | 10.10.9.21         | Other |       |

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item

| Ranking | Name | Mon                                 | Tue                                 | Wed                                 | Thu                                 | Fri                                 | Sat                                 | Sun                                 | Start Time | End Time | Notes           |
|---------|------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|------------|----------|-----------------|
| 0       | 24/7 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 00:00      | 23:59    | Time Range 24/7 |

Select: All, None

The following screen shows the Routing Policy for the Avaya SBCE.

Home / Elements / Routing / Routing Policies

Routing Policy Details Commit Cancel Help ?

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

| Name       | FQDN or IP Address | Type      | Notes |
|------------|--------------------|-----------|-------|
| Avaya SBCE | 10.10.3.40         | SIP Trunk |       |

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

| Ranking                    | Name | Mon                                 | Tue                                 | Wed                                 | Thu                                 | Fri                                 | Sat                                 | Sun                                 | Start Time | End Time | Notes           |
|----------------------------|------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|------------|----------|-----------------|
| <input type="checkbox"/> 0 | 24/7 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 00:00      | 23:59    | Time Range 24/7 |

Select : All, None

## 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 dialled number or prefix to be matched.
- In the **Min** field enter the minimum length of the dialled number.
- In the **Max** field enter the maximum length of the dialled number.
- In the **SIP Domain** field select **ALL** or alternatively one of those configured in **Section 6.2**.

Under **Originating Locations and Routing Policies**:

- Click **Add**, in the resulting screen (not shown).
- Under **Originating Location**, select the location defined in **Section 6.3** or **ALL**.
- Under **Routing Policies** select one of the routing policies defined in **Section 6.6**.
- Click **Select** button to save.

The following screen shows an example dial pattern configured for the Avaya SBCE.

The screenshot shows the 'Dial Pattern Details' configuration page. The 'General' tab is active. The 'Pattern' field is set to '00', 'Min' is '2', and 'Max' is '15'. 'Emergency Call' is unchecked, 'Emergency Priority' is '1', 'Emergency Type' is empty, 'SIP Domain' is '-ALL-', and 'Notes' is empty. Below the 'General' tab is the 'Originating Locations and Routing Policies' section, which contains a table with one item.

| Originating Location Name | Originating Location Notes | Routing Policy Name | Rank | Routing Policy Disabled  | Routing Policy Destination | Routing Policy Notes |
|---------------------------|----------------------------|---------------------|------|--------------------------|----------------------------|----------------------|
| SM_7                      |                            | to_Avaya SBCE       | 0    | <input type="checkbox"/> | Avaya SBCE                 |                      |

The following screen shows the test dial pattern configured for CS1000.

The screenshot shows the 'Dial Pattern Details' configuration page. The 'General' tab is active. The 'Pattern' field is set to '+4411', 'Min' is '5', and 'Max' is '15'. 'Emergency Call' is unchecked, 'Emergency Priority' is '1', 'Emergency Type' is empty, 'SIP Domain' is '-ALL-', and 'Notes' is empty. Below the 'General' tab is the 'Originating Locations and Routing Policies' section, which contains a table with one item.

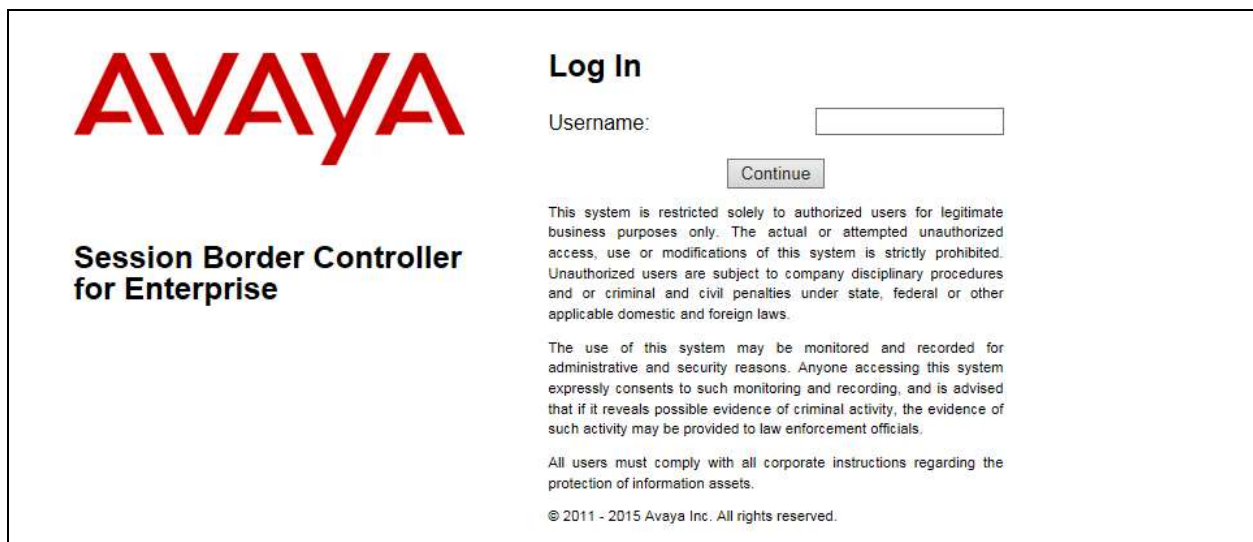
| Originating Location Name | Originating Location Notes | Routing Policy Name | Rank | Routing Policy Disabled  | Routing Policy Destination | Routing Policy Notes |
|---------------------------|----------------------------|---------------------|------|--------------------------|----------------------------|----------------------|
| SM_7                      |                            | to_CS1K_7-6         | 0    | <input type="checkbox"/> | CS1K_7-6                   |                      |

## 7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya Session Border Controller for Enterprise (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 Session Border Controller using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured at installation. A log in screen is presented.



The login screen features the Avaya logo in red on the left. To the right, under the heading "Log In", is a "Username:" label followed by a text input field and a "Continue" button. Below the input field, there is a block of legal disclaimer text. At the bottom, it states "© 2011 - 2015 Avaya Inc. All rights reserved."

**AVAYA**

**Session Border Controller for Enterprise**

**Log In**

Username:

Continue

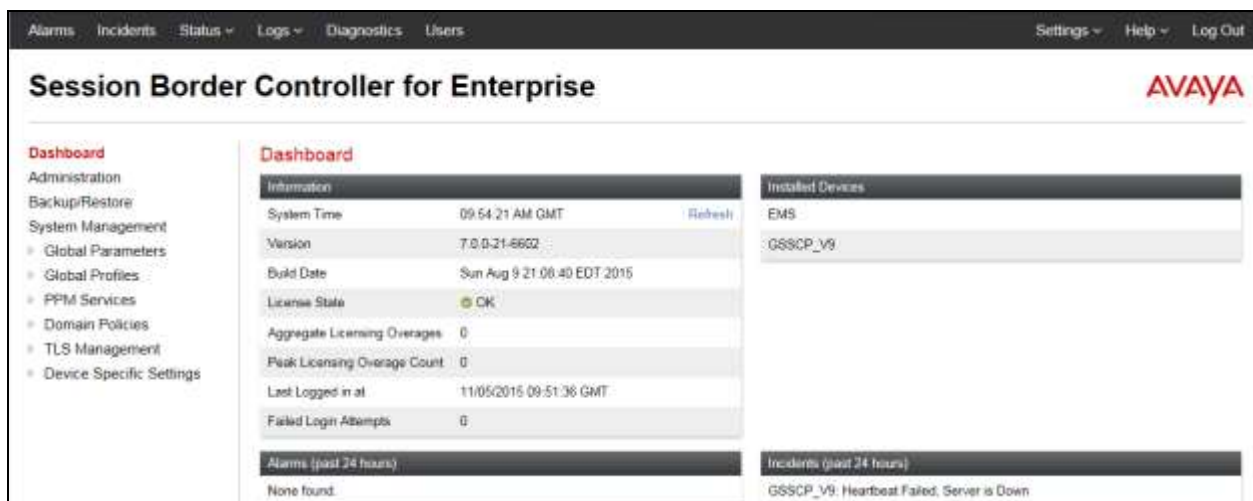
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2015 Avaya Inc. All rights reserved.

Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.



The dashboard has a top navigation bar with links: Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Session Border Controller for Enterprise" and the Avaya logo. A left-hand menu lists various configuration options. The main content area is divided into three sections: "Information" (system details), "Installed Devices" (list of devices), and "Alarms (just 24 hours)" (list of recent alarms).

**Session Border Controller for Enterprise**

**Dashboard**

**Information**

| System Time                  | 09:54:21 AM GMT             | Refresh |
|------------------------------|-----------------------------|---------|
| Version                      | 7.0.0-21-8602               |         |
| Build Date                   | Sun Aug 9 21:06:40 EDT 2015 |         |
| License State                | OK                          |         |
| Aggregate Licensing Overages | 0                           |         |
| Peak Licensing Overage Count | 0                           |         |
| Last Logged in at            | 11/05/2015 09:51:38 GMT     |         |
| Failed Login Attempts        | 0                           |         |

**Installed Devices**

| EMS      |
|----------|
| GSSCP_V9 |

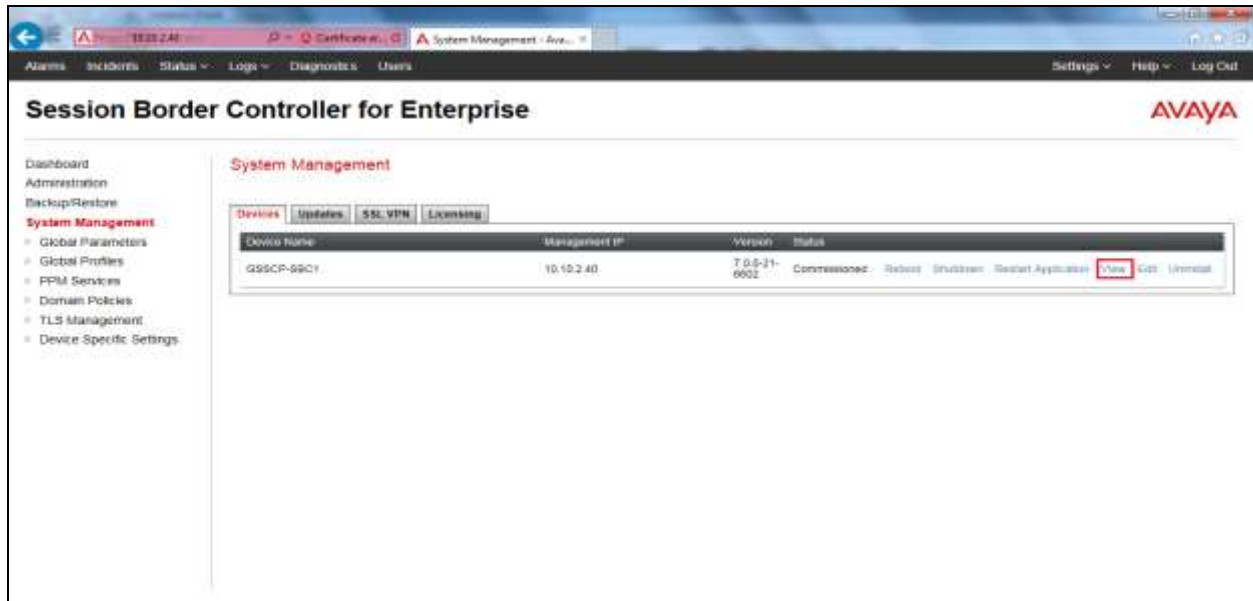
**Alarms (just 24 hours)**

| None found. |
|-------------|
|-------------|

**Incidents (just 24 hours)**

| GSSCP_V9: Heartbeat Failed. Server is Down |
|--------------------------------------------|
|--------------------------------------------|

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-SBC1** is shown. To view the configuration of this device, click **View** (the third option from the right).



The **System Information** screen shows the **General Configuration**, **Device Configuration**, **License Allocation**, **Network Configuration**, **DNS Configuration** and **Management IP** information.

System Information: GSSCP-SBC1

General Configuration

Appliance Name

GSSCP-SBC1

Box Type

SIP

Deployment Mode

Proxy

Device Configuration

HA Mode

No

Two Bypass Mode

No

License Allocation

Standard Sessions

Requested: 0

0

Advanced Sessions

Requested: 0

0

Scopia Video Sessions

Requested: 0

0

CES Sessions

Requested: 0

0

Encryption

☒

Network Configuration

| IP             | Public IP      | Netmask         | Gateway       | Interface |
|----------------|----------------|-----------------|---------------|-----------|
| 10.10.3.40     | 10.10.3.40     | 255.255.255.0   | 10.10.3.1     | A1        |
| 192.168.122.27 | 192.168.122.27 | 255.255.255.128 | 192.168.122.7 | B1        |

DNS Configuration

Primary DNS

8.8.8.8

Secondary DNS

10.10.7.100

DNS Location

DMZ

Management IP(s)

IP

10.10.2.40

## 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**.

- Enter profile name such as Avaya 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.

| General                  |                                                                                                                                  |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Hold Support             | <input checked="" type="radio"/> None<br><input type="radio"/> RFC2543 - c=0.0.0.0<br><input type="radio"/> RFC3264 - s=sendonly |
| 180 Handling             | <input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP                                     |
| 181 Handling             | <input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP                                     |
| 182 Handling             | <input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP                                     |
| 183 Handling             | <input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP                                     |
| Refer Handling           | <input type="checkbox"/>                                                                                                         |
| URI Group                | None ▾                                                                                                                           |
| Send Hold                | <input type="checkbox"/>                                                                                                         |
| Delayed Offer            | <input type="checkbox"/>                                                                                                         |
| 3xx Handling             | <input type="checkbox"/>                                                                                                         |
| Diversion Header Support | <input type="checkbox"/>                                                                                                         |
| Delayed SDP Handling     | <input type="checkbox"/>                                                                                                         |
| Re-Invite Handling       | <input type="checkbox"/>                                                                                                         |
| Prack Handling           | <input type="checkbox"/>                                                                                                         |
| Allow 18X SDP            | <input type="checkbox"/>                                                                                                         |
| T.38 Support             | <input checked="" type="checkbox"/>                                                                                              |
| URI Scheme               | <input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY                                         |
| Via Header Format        | <input checked="" type="radio"/> RFC3261<br><input type="radio"/> RFC2543                                                        |

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

|                                         |                                                                                                                                                                                                                                       |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Record Routes                           | <input type="radio"/> None<br><input type="radio"/> Single Side<br><input checked="" type="radio"/> Both Sides<br><input type="radio"/> Dialog-Initiate Only (Single Side)<br><input type="radio"/> Dialog-Initiate Only (Both Sides) |
| Include End Point IP for Context Lookup | <input type="checkbox"/>                                                                                                                                                                                                              |
| Extensions                              | Avaya ▼                                                                                                                                                                                                                               |
| Diversion Manipulation                  | <input type="checkbox"/>                                                                                                                                                                                                              |
| Diversion Condition                     | None ▼                                                                                                                                                                                                                                |
| Diversion Header URI                    | <input type="text"/>                                                                                                                                                                                                                  |
| Has Remote SBC                          | <input checked="" type="checkbox"/>                                                                                                                                                                                                   |
| Route Response on Via Port              | <input type="checkbox"/>                                                                                                                                                                                                              |
| <b>DTMF</b>                             |                                                                                                                                                                                                                                       |
| DTMF Support                            | <input checked="" type="radio"/> None<br><input type="radio"/> SIP NOTIFY<br><input type="radio"/> SIP INFO                                                                                                                           |
| <input type="button" value="Finish"/>   |                                                                                                                                                                                                                                       |

### 7.2.2. Server Interworking – KCOM

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**.

- Enter profile name such as KCOM and click **Next** (Not Shown).
- Check **Hold Support** = **None**.
- Check **180 Handling** = **No SDP**.
- Check **183 Handling** = **No SDP**.
- Check **T.38 Support**.
- All other options on the **General** Tab can be left at default.

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

The screenshot shows the 'General' configuration tab for a server interworking profile. The settings are as follows:

| Setting                  | Value                                                                                                                            |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Hold Support             | <input checked="" type="radio"/> None<br><input type="radio"/> RFC2543 - c=0.0.0.0<br><input type="radio"/> RFC3264 - a=sendonly |
| 180 Handling             | <input type="radio"/> None <input type="radio"/> SDP <input checked="" type="radio"/> No SDP                                     |
| 181 Handling             | <input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP                                     |
| 182 Handling             | <input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP                                     |
| 183 Handling             | <input type="radio"/> None <input type="radio"/> SDP <input checked="" type="radio"/> No SDP                                     |
| Refer Handling           | <input type="checkbox"/>                                                                                                         |
| URI Group                | None (dropdown)                                                                                                                  |
| Send Hold                | <input type="checkbox"/>                                                                                                         |
| Delayed Offer            | <input type="checkbox"/>                                                                                                         |
| 3xx Handling             | <input type="checkbox"/>                                                                                                         |
| Diversion Header Support | <input type="checkbox"/>                                                                                                         |
| Delayed SDP Handling     | <input type="checkbox"/>                                                                                                         |
| Re-Invite Handling       | <input type="checkbox"/>                                                                                                         |
| Prack Handling           | <input type="checkbox"/>                                                                                                         |
| Allow 18X SDP            | <input type="checkbox"/>                                                                                                         |
| T.38 Support             | <input checked="" type="checkbox"/>                                                                                              |
| URI Scheme               | <input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY                                         |
| Via Header Format        | <input checked="" type="radio"/> RFC3261<br><input type="radio"/> RFC2543                                                        |

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

|                                         |                                                                                                                                                                                                                                       |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Record Routes                           | <input type="radio"/> None<br><input type="radio"/> Single Side<br><input checked="" type="radio"/> Both Sides<br><input type="radio"/> Dialog-Initiate Only (Single Side)<br><input type="radio"/> Dialog-Initiate Only (Both Sides) |
| Include End Point IP for Context Lookup | <input type="checkbox"/>                                                                                                                                                                                                              |
| Extensions                              | Avaya ▼                                                                                                                                                                                                                               |
| Diversion Manipulation                  | <input type="checkbox"/>                                                                                                                                                                                                              |
| Diversion Condition                     | None ▼                                                                                                                                                                                                                                |
| Diversion Header URI                    | <input type="text"/>                                                                                                                                                                                                                  |
| Has Remote SBC                          | <input checked="" type="checkbox"/>                                                                                                                                                                                                   |
| Route Response on Via Port              | <input type="checkbox"/>                                                                                                                                                                                                              |
| <b>DTMF</b>                             |                                                                                                                                                                                                                                       |
| DTMF Support                            | <input checked="" type="radio"/> None<br><input type="radio"/> SIP NOTIFY<br><input type="radio"/> SIP INFO                                                                                                                           |
| <input type="button" value="Finish"/>   |                                                                                                                                                                                                                                       |

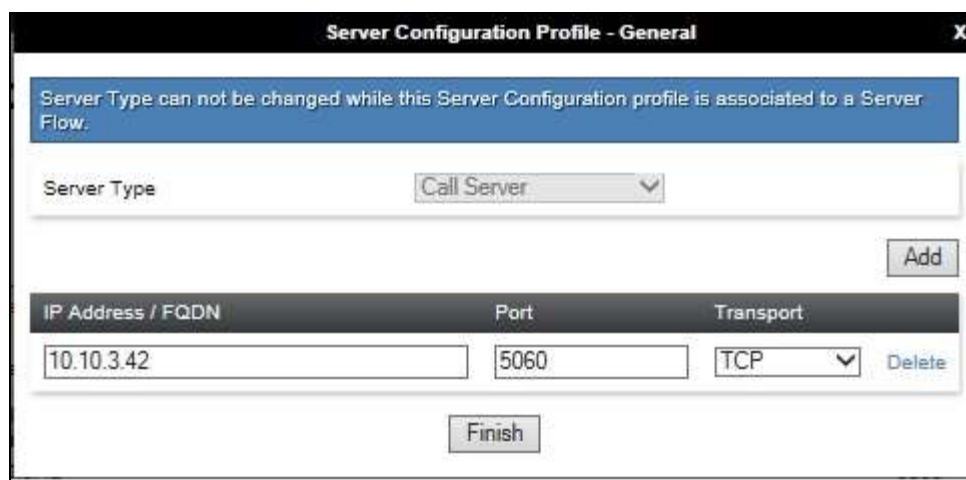
### 7.2.3. Server Configuration– Avaya

Servers are defined for each server connected to the Avaya SBCE. In this case, KCOM 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 the configuration and management of various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signalling parameters and some advanced options.

From the left-hand menu select **Global Profiles → Server Configuration** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Call Server**.
- Enter **IP Address / FQDN** to **10.10.3.42** (Session Manager IP Address).
- For **Port**, enter **5060**.
- For **Transport**, select **TCP**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.



Server Configuration Profile - General

Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.

Server Type: Call Server

Add

| IP Address / FQDN | Port | Transport |        |
|-------------------|------|-----------|--------|
| 10.10.3.42        | 5060 | TCP       | Delete |

Finish

On the **Advanced** tab:

- Select **Avaya** for **Interworking Profile**.
- Click **Finish**.

The screenshot shows the 'Server Configuration Profile - Advanced' dialog box. It contains several configuration options: 'Enable DoS Protection' (checkbox), 'Enable Grooming' (checkbox), 'Interworking Profile' (dropdown menu set to 'Avaya'), 'Signaling Manipulation Script' (dropdown menu set to 'None'), 'Connection Type' (dropdown menu set to 'SUBID'), and 'Securable' (checkbox). A 'Finish' button is located at the bottom right of the dialog.

#### 7.2.4. Server Configuration – KCOM

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

- Select **Server Type** to be **Trunk Server**.
- Enter **IP Address / FQDN** to **192.168.19.230** (KCOM SBC IP Address).
- For **Port**, enter **5060**.
- For **Transport**, select **UDP**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.

The screenshot shows the 'Edit Server Configuration Profile - General' dialog box. At the top, a blue message box states: 'Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.' Below this, the 'Server Type' dropdown menu is set to 'Trunk Server'. There is an 'Add' button to the right. Below the dropdown, there is a table with three columns: 'IP Address / FQDN', 'Port', and 'Transport'. The first row contains the values '192.168.19.230', '5060', and 'UDP' (selected from a dropdown). A 'Delete' button is next to the row. At the bottom, there is a 'Finish' button.

On the Advanced tab:

- Select **KCOM** for Interworking Profile.
- Click **Finish**.

**Server Configuration Profile - Advanced** X

|                               |                          |
|-------------------------------|--------------------------|
| Enable DoS Protection         | <input type="checkbox"/> |
| Enable Grooming               | <input type="checkbox"/> |
| Interworking Profile          | KCOM ▼                   |
| Signaling Manipulation Script | None ▼                   |
| Connection Type               | SUBID ▼                  |
| Securable                     | <input type="checkbox"/> |

Finish

## 7.2.5. 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 KCOM addresses 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.

### 7.2.5.1 Routing – Avaya

Create a Routing Profile for Session Manager.

- Navigate to **Global Profiles → Routing** and select **Add Profile**.
- Enter a **Profile Name** and click **Next**.



The screenshot shows a window titled "Routing Profile" with a close button (X) in the top right corner. Inside the window, there is a text input field labeled "Profile Name" containing the text "Avaya". Below the input field is a button labeled "Next".

The Routing Profile window will open. Use the default values displayed and click **Add**.



The screenshot shows a window titled "Routing Profile" with a close button (X) in the top right corner. The window contains several settings:

| URI Group                | Time of Day                         |
|--------------------------|-------------------------------------|
| *                        | default                             |
| Load Balancing           | NAPTR                               |
| Priority                 | <input type="checkbox"/>            |
| Transport                | Next Hop Priority                   |
| None                     | <input checked="" type="checkbox"/> |
| Next Hop In-Dialog       | Ignore Route Header                 |
| <input type="checkbox"/> | <input type="checkbox"/>            |

Below the settings table is a button labeled "Add". At the bottom of the window, there is a blue banner with the text "Click the Add button to add a Next-Hop Address." and two buttons labeled "Back" and "Finish".

On the **Next Hop Address** window, set the following:

- **Priority/Weight = 1.**
- **Server Configuration = Avaya** (Section 7.2.3) from drop down menu.
- **Next Hop Address = Select 10.10.3.42:5060 TCP** from drop down menu.
- Click **Finish**.

| Priority / Weight | Server Configuration | Next Hop Address      | Transport |
|-------------------|----------------------|-----------------------|-----------|
| 1                 | Avaya                | 10.10.3.42:5060 (TCP) | None      |

## 7.2.5.2 Routing – KCOM

Create a Routing Profile for KCOM.

- Navigate to **Global Profiles → Routing** and select **Add Profile**.
- Enter a **Profile Name** and click **Next**.

Profile Name: KCOM

Next

The Routing Profile window will open. Use the default values displayed and click **Add**.



The Routing Profile window is a configuration dialog with a title bar 'Routing Profile' and a close button 'X'. It contains several settings:

- URI Group: A dropdown menu with an asterisk '\*' as the selected value.
- Time of Day: A dropdown menu with 'default' as the selected value.
- Load Balancing: A dropdown menu with 'Priority' as the selected value.
- NAPTR: A checkbox that is currently unchecked.
- Transport: A dropdown menu with 'None' as the selected value.
- Next Hop Priority: A checkbox that is currently checked.
- Next Hop In-Dialog: A checkbox that is currently unchecked.
- Ignore Route Header: A checkbox that is currently unchecked.

At the bottom right is an 'Add' button. Below the settings is a blue banner with the text 'Click the Add button to add a Next-Hop Address.' At the very bottom are 'Back' and 'Finish' buttons.

On the **Next Hop Address** window, set the following:

- **Priority/Weight = 1.**
- **Server Configuration = KCOM (Section 7.2.4)** from drop down menu.
- **Next Hop Address = Select 192.168.19.230:5060 UDP** from drop down menu.
- Click **Finish**.



The Profile : KCOM window is a configuration dialog with a title bar 'Profile : KCOM' and a close button 'X'. It contains the same settings as the Routing Profile window, plus an 'Add' button at the bottom right. Below the settings is a table with the following data:

| Priority / Weight | Server Configuration | Next Hop Address          | Transport |        |
|-------------------|----------------------|---------------------------|-----------|--------|
| 1                 | KCOM                 | 192.168.19.230:5060 (UDP) | None      | Delete |

At the bottom center is a 'Finish' button.

### 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. 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 menu on the left hand side. Click on **Add** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- Enter a descriptive Profile Name such as **Avaya**.
- If the required Header is not shown, click on **Add Header**.
- 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).

The screenshot shows the 'Topology Hiding Profiles: Avaya' configuration window. On the left, a sidebar lists 'Topology Hiding Profiles' with options: 'default', 'cisco\_th\_profile', 'Avaya' (selected), and 'KCOM'. The main area has a title bar with 'Rename', 'Clone', and 'Delete' buttons. Below the title bar is a blue bar with the text 'Click here to add a description.' The main content area is titled 'Topology Hiding' and contains a table with the following data:

| Header       | Criteria  | Replace Action | Overwrite Value |
|--------------|-----------|----------------|-----------------|
| SDP          | IP/Domain | Auto           | ---             |
| Record-Route | IP/Domain | Auto           | ---             |
| Refer-To     | IP/Domain | Auto           | ---             |
| Request-Line | IP/Domain | Overwrite      | avaya.com       |
| Via          | IP/Domain | Auto           | ---             |
| From         | IP/Domain | Overwrite      | avaya.com       |
| Referred-By  | IP/Domain | Auto           | ---             |
| To           | IP/Domain | Overwrite      | avaya.com       |

An 'Edit' button is located at the bottom right of the table.

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

- In the **Profile Name** field enter a descriptive name for KCOM and click **Next**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Auto** under **Replace Action**.
- Click **Finish** (not shown).

Topology Hiding Profiles: KCOM

Buttons: Add, Rename, Clone, Delete

Click here to add a description.

| Header       | Criteria  | Replace Action | Overwrite Value |
|--------------|-----------|----------------|-----------------|
| SDF          | IP/Domain | Auto           | ---             |
| Record-Route | IP/Domain | Auto           | ---             |
| Refer-To     | IP/Domain | Auto           | ---             |
| Request-Line | IP/Domain | Auto           | ---             |
| Via          | IP/Domain | Auto           | ---             |
| From         | IP/Domain | Auto           | ---             |
| Referred-By  | IP/Domain | Auto           | ---             |
| To           | IP/Domain | Auto           | ---             |

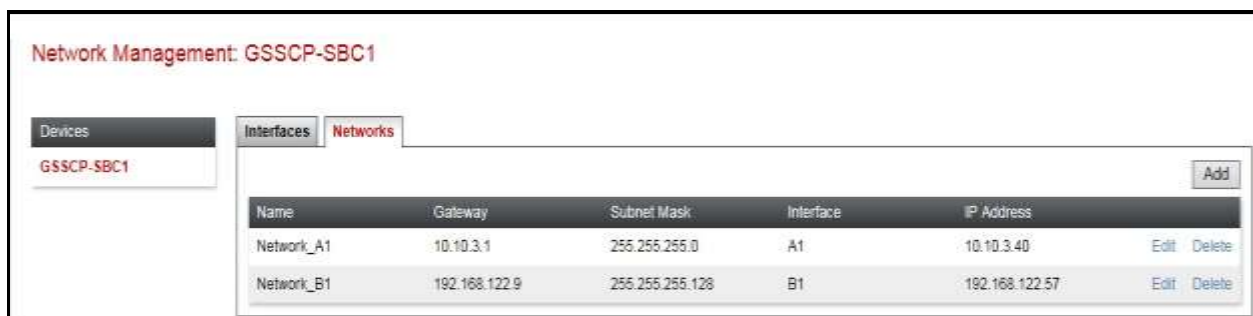
Edit

### 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.

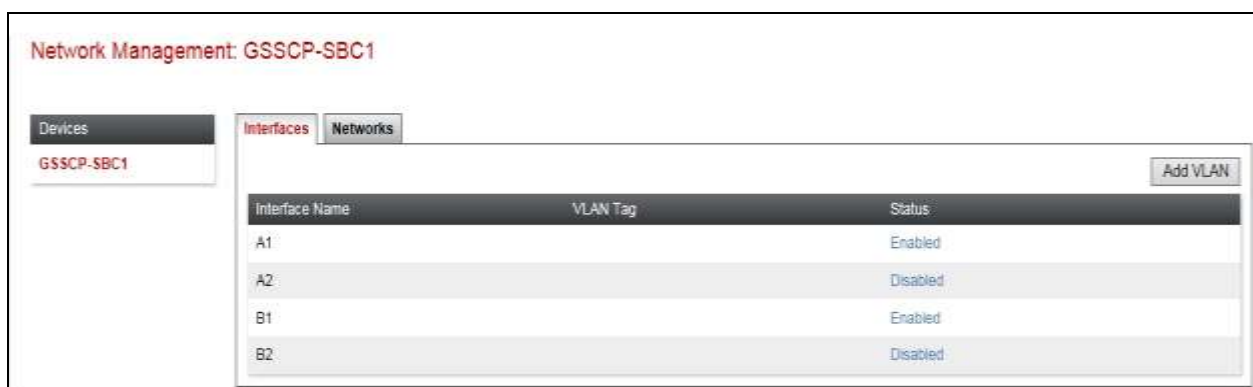
To define the network information, navigate to **Device Specific Settings → Network Management** from the menu on the left-hand side and click on **Add**. Enter details in the blank box that appears at the end of the list.

- Define the internal IP address with screening mask and assign to interface **A1**.
- Select **Save** to save the information.
- Click on **Add**.
- Define the external IP address with screening mask and assign to interface **B1**.
- Select **Save** 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).



| Name       | Gateway       | Subnet Mask     | Interface | IP Address     |             |
|------------|---------------|-----------------|-----------|----------------|-------------|
| Network_A1 | 10.10.3.1     | 255.255.255.0   | A1        | 10.10.3.40     | Edit Delete |
| Network_B1 | 192.168.122.9 | 255.255.255.128 | B1        | 192.168.122.57 | Edit Delete |

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



| Interface Name | VLAN Tag | Status   |
|----------------|----------|----------|
| A1             |          | Enabled  |
| A2             |          | Disabled |
| B1             |          | Enabled  |
| B2             |          | Disabled |

## 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

To define the signalling interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Signaling Interface** from the menu on the left hand side. Details of transport protocol and ports for the internal and external SIP signalling are entered here.

To enter details of transport protocol and ports for the SIP signalling on the internal interface:

- Select **Add** and enter details of the internal signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the interface.
- For **Signaling IP**, select the **internal** signalling interface IP addresses defined in **Section 7.3**.
- Select **TCP** port number, **5060** is used for Session Manager.

To enter details of transport protocol and ports for the SIP signalling on the external interface:

- Select **Add** and enter details of the external signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the external signalling interface.
- For **Signaling IP**, select the **external** signalling interface IP address defined in **Section 7.3**.
- Select **UDP** port number, **5060** is used for KCOM SIP Connect.

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

| Name    | Signaling IP Network                      | TCP Port | UDP Port | TLS Port | TLS Profile |             |
|---------|-------------------------------------------|----------|----------|----------|-------------|-------------|
| Int_Sig | 10.10.3.40<br>Network_A1 (A1, VLAN 0)     | 5060     | 5060     | ---      | None        | Edit Delete |
| Ext_Sig | 192.168.122.57<br>Network_B1 (B1, VLAN 0) | 5060     | 5060     | ---      | None        | Edit Delete |

## 7.4.2. Media Interfaces

To define the media interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Media Interface** from the menu on the left hand side. Details of the RTP and SRTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signalling.

To define the media interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Media Interface** from the menu on the left hand side. Details of the RTP and SRTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signalling.

To enter details of the media IP and RTP port range on the internal interface to be used in the server flow:

- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal media interface.
- For **Media IP**, select the **internal** media interface IP address defined in **Section 7.3**.
- Select **RTP port** ranges for the media path with the enterprise end-points.

To enter details of the media IP and RTP port range on the external interface to be used in the server flow.

- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the external media interface.
- For **Media IP**, select the **external** media interface IP address defined in **Section 7.3**.
- Select **RTP port** ranges for the external media path.

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

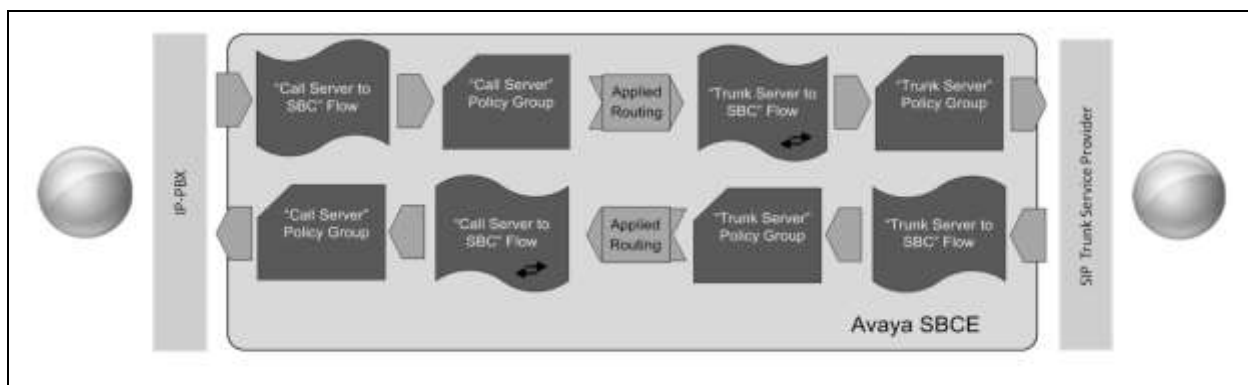
Media Interface: GSSCP-SBC1

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

| Name      | Media IP Network                          | Port Range    | Edit | Delete |
|-----------|-------------------------------------------|---------------|------|--------|
| Int_Media | 10.10.3.40<br>Network_A1 (A1, VLAN 0)     | 35000 - 40000 | Edit | Delete |
| Ext_Media | 192.168.122.57<br>Network_B1 (B1, VLAN 0) | 35000 - 40000 | Edit | Delete |

## 7.5. Server Flows

Server Flows combine the previously defined profiles into outgoing flows from Session Manager to KCOM's SIP Trunk and incoming flows from KCOM's SIP Trunk to Session Manager. This configuration ties all the previously entered information together so that signalling can be routed from Session Manager to the PSTN via the KCOM network and vice versa. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.



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

Subscriber Flows

Server Flows

Add

Hover over a row to see its description.

Server Configuration: Avaya

| Priority | Flow Name   | URI Group | Received Interface | Signaling Interface | End Point Policy Group | Routing Profile |                                                                                        |
|----------|-------------|-----------|--------------------|---------------------|------------------------|-----------------|----------------------------------------------------------------------------------------|
| 1        | Call_Server | *         | Ext_Sig            | Int_Sig             | default-low            | KCOM            | <a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a> |

Server Configuration: KCOM

| Priority | Flow Name    | URI Group | Received Interface | Signaling Interface | End Point Policy Group | Routing Profile |                                                                                        |
|----------|--------------|-----------|--------------------|---------------------|------------------------|-----------------|----------------------------------------------------------------------------------------|
| 1        | Trunk_Server | *         | Int_Sig            | Ext_Sig             | default-low            | Avaya           | <a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a> |

To define a Server Flow for the KCOM SIP Connect, navigate to **Device Specific Settings → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for KCOM SIP Connect, in the test environment **Trunk\_Server** was used.
- In the **Server Configuration** drop-down menu, select the KCOM server configuration defined in **Section 7.2.4**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.4.1**. This is the interface that signalling bound for KCOM SIP Connect is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4.1**. This is the interface that signalling bound for KCOM SIP Connect is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.4.2**. This is the interface that media bound for KCOM SIP Connect is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager Office defined in **Section 7.2.5**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of KCOM SIP Connect defined in **Section 7.2.6** and click **Finish**.

The screenshot shows a configuration window titled "Flow: Trunk\_Server". It contains the following fields and values:

| Field                         | Value        |
|-------------------------------|--------------|
| Flow Name                     | Trunk_Server |
| Server Configuration          | KCOM         |
| URI Group                     | *            |
| Transport                     | *            |
| Remote Subnet                 | *            |
| Received Interface            | Int_Sig      |
| Signaling Interface           | Ext_Sig      |
| Media Interface               | Ext_Media    |
| End Point Policy Group        | default-low  |
| Routing Profile               | Avaya        |
| Topology Hiding Profile       | KCOM         |
| Signaling Manipulation Script | None         |
| Remote Branch Office          | Any          |

At the bottom of the window is a "Finish" button.

To define a Server Flow for Session Manager, navigate to **Device Specific Settings → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for Session Manager, in the test environment **Call\_Server** was used.
- In the **Server Configuration** drop-down menu, select the Session Manager server configuration defined in **Section 7.2.3**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.4.1**. This is the interface that signalling bound for Session Manager is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4.1**. This is the interface that signalling bound for Session Manager is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.4.2**. This is the interface that media bound for Session Manager is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the KCOM SIP Connect defined in **Section 7.2.5**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.2.6** and click **Finish**.

| Flow: Call_Server             |             |
|-------------------------------|-------------|
| Flow Name                     | Call_Server |
| Server Configuration          | Avaya       |
| URI Group                     | *           |
| Transport                     | *           |
| Remote Subnet                 | *           |
| Received Interface            | Ext_Sig     |
| Signaling Interface           | Int_Sig     |
| Media Interface               | Int_Media   |
| End Point Policy Group        | default-low |
| Routing Profile               | KCOM        |
| Topology Hiding Profile       | Avaya       |
| Signaling Manipulation Script | None        |
| Remote Branch Office          | Any         |
| <b>Finish</b>                 |             |

## 8. KCOM SIP Connect Configuration

The configuration of the KCOM equipment used to support KCOM's SIP trunk is outside of the scope of these Application Notes and will not be covered. To obtain further information on KCOM equipment and system configuration please contact an authorized KCOM 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 1000 Verification

This section illustrates sample verifications that may be performed using the Avaya CS1000 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”**.

Managing: 192.168.27.2 Username: admin  
System > IP Network > Tools Maintenance and Reports > General Commands

### General Commands

Element IP: 192.168.27.2 Element Type: Signaling Server-Analyz CPMx1

Group: **Sip** Command: **SIPShow** IP address: 192.168.27.2 Number of pings: 3

**STATUS** Status: Active

Primary Proxy IP address: 10.10.9.55  
 Primary Proxy port: 5060  
 Primary Proxy Transport: TCP  
 Secondary Proxy IP address: 0.0.0.0  
 Secondary Proxy port: 5060  
 Secondary Proxy Transport: TCP  
 Primary Proxy2 IP address: 10.10.9.55  
 Primary Proxy2 port: 5060  
 Primary Proxy2 Transport: TCP  
 Active Proxy: Primary: :Register Not Supported  
 Time To Next Registration: 0 Seconds  
 Channels Busy / Idle / Total: 0 / 34 / 34  
 Stack version: 5.6.0.19  
 TLS Security Policy: Security Disabled

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

Managing: 192.168.27.2 Username: admin  
System > IP Network > Tools Maintenance and Reports > General Commands

### General Commands

Element IP: 192.168.27.2 Element Type: Signaling Server-Analyz CPMx1

Group: **SipLine** Command: **sigSetShowAll** IP address: 192.168.27.2 Number of pings: 3

| UserID                                                        | AuthId | TN           | Clients | Calls | SetHandle | Ext ID | SIP Line Type |
|---------------------------------------------------------------|--------|--------------|---------|-------|-----------|--------|---------------|
| <b>IPv4 Endpoints</b>                                         |        |              |         |       |           |        |               |
| 6003                                                          | 6003   | 100-00-03-03 | 1       | 0     | 0x51e22d0 |        | SIP Lines     |
| 6002                                                          | 6002   | 100-00-03-02 | 1       | 0     | 0x51e4158 |        | SIP Lines     |
| Total User Registered = 2 V4 Registered = 2 V6 Registered = 0 |        |              |         |       |           |        |               |

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

Managing: 192.168.27.2 Username: admin  
System > IP Network > Tools Maintenance and Reports > General Commands

### General Commands

Element IP: 192.168.27.2 Element Type: Signaling Server-Analyz CPMx1

Group: **Iset** Command: **isetShow** IP address: 192.168.27.2 Range: 0 500 Number of pings: 3

**Set Information**

| IP Address     | NAT | Model Name         | Type | RegType | State  | Op |
|----------------|-----|--------------------|------|---------|--------|----|
| 10.10.9.200    |     | 1230 IP Deskphone  | 1230 | Regular | online | 13 |
| 10.10.9.201    |     | 1140E IP Deskphone | 1140 | Regular | online | 13 |
| Total sets = 2 |     |                    |      |         |        |    |

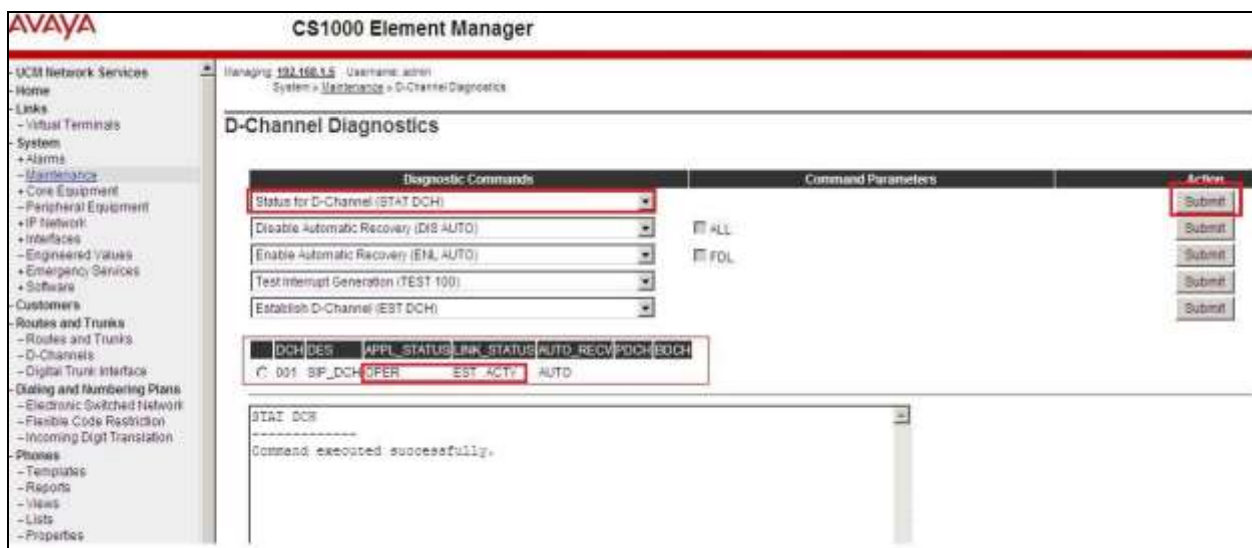
## 9.2. Verify Avaya Communication Server 1000 Operational Status

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

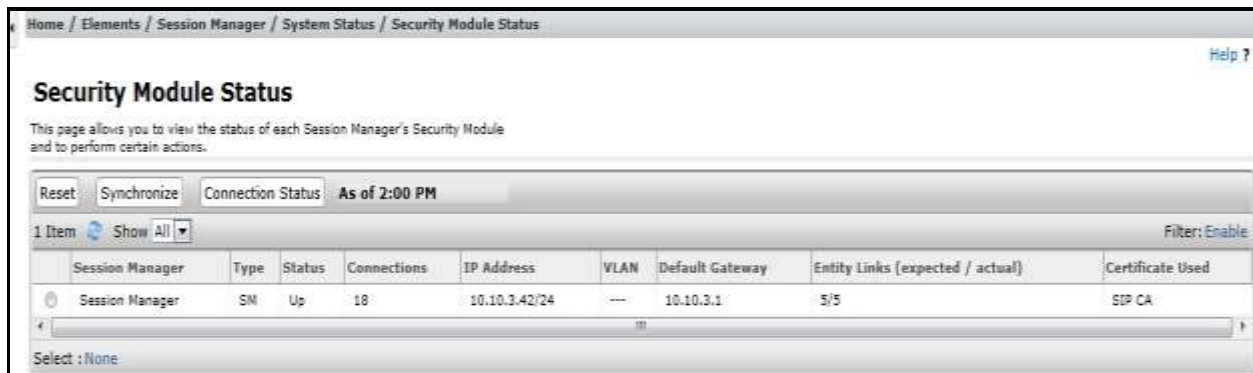
Navigate to **Elements → Session Manager → Dashboard** (not shown) to verify the overall system status for Session Manager. Specifically, verify the status of the following fields as shown below.



The screenshot shows the 'Session Manager Dashboard' with a breadcrumb trail: Home / Elements / Session Manager / Dashboard. Below the title, a description states: 'This page provides the overall status and health summary of each administered Session Manager.' The main section is titled 'Session Manager Instances' and includes filters for 'Service State' (set to 'Shutdown System') and 'As of 2:25 PM'. A table lists the instances, with one item shown: 'Session Manager' (Core). The table columns include: Session Manager, Type, Tests Pass, Alarms, Security Module, Service State, Entity Monitoring, Active Call Count, Registrations, Data Replication, User Data Storage Status, License Mode, and Version. The 'Status' column for the 'Session Manager' instance shows 'Up'.

| Session Manager                 | Type | Tests Pass | Alarms | Security Module | Service State      | Entity Monitoring | Active Call Count | Registrations | Data Replication | User Data Storage Status | License Mode | Version        |
|---------------------------------|------|------------|--------|-----------------|--------------------|-------------------|-------------------|---------------|------------------|--------------------------|--------------|----------------|
| <a href="#">Session Manager</a> | Core | ✓          | 0/0/0  | Up              | Accept New Service | 0/4               | 0                 | 3/3           | ✓                | ✓                        | Normal       | 7.0.0.2.700201 |

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.



The screenshot shows the 'Security Module Status' page with a breadcrumb trail: Home / Elements / Session Manager / System Status / Security Module Status. Below the title, a description states: 'This page allows you to view the status of each Session Manager's Security Module and to perform certain actions.' The main section includes buttons for 'Reset', 'Synchronize', and 'Connection Status', and a filter for 'As of 2:00 PM'. A table lists the security module status for the 'Session Manager' (SM). The table columns include: Session Manager, Type, Status, Connections, IP Address, VLAN, Default Gateway, Entity Links (expected / actual), and Certificate Used. The 'Status' column for the 'Session Manager' instance shows 'Up'.

| Session Manager                 | Type | Status | Connections | IP Address    | VLAN | Default Gateway | Entity Links (expected / actual) | Certificate Used |
|---------------------------------|------|--------|-------------|---------------|------|-----------------|----------------------------------|------------------|
| <a href="#">Session Manager</a> | SM   | Up     | 18          | 10.10.3.42/24 | ---  | 10.10.3.1       | 5/5                              | SDP CA           |

### 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 CS1000 from the **All Monitored SIP Entities** table (not shown) to open the **SIP Entity, Entity Link Connection Status** page.

SIP Entities Status for All Monitoring Session Manager Instances

Run Monitor

1 Items Refresh Filter: Enable

| Session Manager                          | Type | Monitored Entities |              |    |               |      | Total |
|------------------------------------------|------|--------------------|--------------|----|---------------|------|-------|
|                                          |      | Down               | Partially Up | Up | Not Monitored | Deny |       |
| <input type="checkbox"/> Session Manager | Core | 0                  | 0            | 5  | 0             | 0    | 5     |
|                                          |      |                    |              |    |               |      |       |
|                                          |      |                    |              |    |               |      |       |
|                                          |      |                    |              |    |               |      |       |
|                                          |      |                    |              |    |               |      |       |

Select: All, None

Verify the status of the SIP link is up between Session Manager and CS1000 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.

All Entity Links to SIP Entity: CS1K\_7.6

Summary View

Status Details for the selected Session Manager:

1 Items Refresh Filter: Enable

| Session Manager Name                             | SIP Entity Resolved IP | Port | Proto. | Deny  | Conn. Status | Reason Code | Link Status |
|--------------------------------------------------|------------------------|------|--------|-------|--------------|-------------|-------------|
| <input checked="" type="radio"/> Session Manager | 10.10.9.21             | 5060 | TCP    | FALSE | 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.

The screenshot displays the 'View Session Manager' configuration page. The breadcrumb trail at the top reads: Home / Elements / Session Manager / Session Manager Administration. A 'Return' button is located in the top right corner. Below the title, there is a navigation bar with links: General | Security Module | Monitoring | CDR | Personal Profile Manager (PPM) | Connection Settings | Event Server |. Below this, there are links for 'Expand All' and 'Collapse All'. The 'General' section is expanded, showing the following fields:

- SIP Entity Name: Session Manager
- Description: (empty field)
- Management Access Point Host Name/IP: 10.10.3.41
- Direct Routing to Endpoints: Enable
- Maintenance Mode: ☐

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.



The screenshot displays the 'Security Module' configuration interface. It contains several input fields with the following values: 'SIP Entity IP Address' is 10.10.3.42, 'Network Mask' is 255.255.255.0, 'Default Gateway' is 10.10.3.1, 'Call Control PHB' is 46, and 'SIP Firewall Configuration' is SM 6.3.8.0. The 'SIP Firewall Configuration' field has a dropdown arrow on its right side.

| Field                      | Value         |
|----------------------------|---------------|
| SIP Entity IP Address      | 10.10.3.42    |
| Network Mask               | 255.255.255.0 |
| Default Gateway            | 10.10.3.1     |
| Call Control PHB           | 46            |
| SIP Firewall Configuration | SM 6.3.8.0    |

## 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 screenshot shows the Avaya Session Border Controller for Enterprise dashboard. The top navigation bar includes links for Alarms, Incidents (selected), Status, Logs, Diagnostics, and Users. The dashboard is divided into several sections:

- Information:** System Time (08:53:59 AM CDT), Version (7.0.0-21-8802), Build Date (Sun Aug 9 21:00:40 EDT 2015), License State (OK), Aggregate Licensing Overages (0), Peak Licensing Overage Count (0), Last Logged in at (04/05/2016 05:57:24 CDT), and Failed Login Attempts (3).
- Installed Devices:** Lists EMS and GSSCP-SBC1.
- Alarms (past 24 hours):** None found.
- Incidents (past 24 hours):** GSSCP-SBC1: General Method not allowed Out-Of-Dialog.
- Notes:** No notes found.

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

The screenshot shows the Incident Viewer interface. It includes filters for Device (All) and Category (All), a Clear Filters button, and buttons for Refresh and Generate Report. The table displays 15 results out of 2000.

| Type            | ID              | Date    | Time    | Category | Device   | Cause                      |
|-----------------|-----------------|---------|---------|----------|----------|----------------------------|
| Message Dropped | 724828081147236 | 12/9/15 | 4:16 AM | Policy   | GSSCP_03 | No Subscriber Flow Matched |
| Message Dropped | 724828069540139 | 12/9/15 | 4:15 AM | Policy   | GSSCP_03 | No Subscriber Flow Matched |
| Message Dropped | 724828051067038 | 12/9/15 | 4:15 AM | Policy   | GSSCP_03 | No Subscriber Flow Matched |
| Message Dropped | 724828039459870 | 12/9/15 | 4:14 AM | Policy   | GSSCP_03 | No Subscriber Flow Matched |
| Message Dropped | 724828021049515 | 12/9/15 | 4:14 AM | Policy   | GSSCP_03 | No Subscriber Flow Matched |
| Message Dropped | 724828009441902 | 12/9/15 | 4:13 AM | Policy   | GSSCP_03 | No Subscriber Flow Matched |
| Message Dropped | 724827990985367 | 12/9/15 | 4:13 AM | Policy   | GSSCP_03 | No Subscriber Flow Matched |
| Message Dropped | 724827988056473 | 12/9/15 | 4:12 AM | Policy   | GSSCP_03 | No Subscriber Flow Matched |
| Message Dropped | 724827987936465 | 12/9/15 | 4:12 AM | Policy   | GSSCP_03 | No Subscriber Flow Matched |
| Message Dropped | 724827987416506 | 12/9/15 | 4:12 AM | Policy   | GSSCP_03 | No Subscriber Flow Matched |
| Message Dropped | 724827987147196 | 12/9/15 | 4:12 AM | Policy   | GSSCP_03 | No Subscriber Flow Matched |
| Message Dropped | 724827979397279 | 12/9/15 | 4:12 AM | Policy   | GSSCP_03 | No Subscriber Flow Matched |

### 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

The screenshot shows the 'Trace: GSSCP-SBC1' interface. On the left, a sidebar lists 'Devices' with 'GSSCP-SBC1' selected. The main area has two tabs: 'Packet Capture' (active) and 'Captures'. The 'Packet Capture Configuration' form includes the following fields:

- Status: Ready
- Interface: B1 (dropdown)
- Local Address (IP/Port): All (dropdown) and an empty text box
- Remote Address (\*-Port, IP, IP/Port): \* (text box)
- Protocol: All (dropdown)
- Maximum Number of Packets to Capture: 10000 (text box)
- Capture Filename: Test.pcap (text box, with a note: 'Using the name of an existing capture will overwrite it')

At the bottom right of the form are 'Start Capture' and 'Clear' buttons.

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

The screenshot shows the 'Trace: GSSCP-SBC1' interface with the 'Captures' tab selected. A table lists the captured files. A 'Refresh' button is in the top right corner of the table area.

| File Name                | File Size (bytes) | Last Modified                 |        |
|--------------------------|-------------------|-------------------------------|--------|
| Test_20160413085450.pcap | 0                 | April 13, 2016 8:54:50 AM CDT | Delete |

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 KCOM SIP Connect network.

## 10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Server R7.65, Avaya Aura® Session Manager R7.0 and Avaya Session Border Controller for Enterprise R7.0 to KCOM SIP Connect. KCOM SIP Connect 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. Additional References

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

- [1] *Migrating and Installing Avaya Appliance Virtualization Platform*, Release 7.0, Nov 2015.
- [2] *Upgrading and Migrating Avaya Aura® applications to 7.0*, Release 7.0, Nov 2015.
- [3] *Deploying Avaya Aura® applications*, Release 7.0, Oct 2015
- [4] *Deploying Avaya Aura® System Manager* Release 7.0 Nov 2015
- [5] *Upgrading Avaya Aura® System Manager to Release 7.0*, Nov 2015.
- [6] *Administering Avaya Aura® System Manager for Release 7.0* Release 7.0, Nov 2015
- [7] *Deploying Avaya Aura® Session Manager on VMware* , Release 7.0 August 2015
- [8] *Upgrading Avaya Aura® Session Manager* Release 7.0, August 2015
- [9] *Administering Avaya Aura® Session Manager* Release 7.0, August 2015
- [10] *Avaya Communication Server 1000 Installation and Commissioning*, Document Number NN43041-310
- [11] *Linux Platform Base and Applications Installation and Commissioning Avaya Communication Server 1000*, Document Number NN43001-315
- [12] *Software Input Output Reference – Maintenance Avaya Communication Server 1000*, Document Number NN43001-711
- [13] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015
- [14] *Upgrading Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015
- [15] *Administering Avaya Session Border Controller for Enterprise*, Release 7.0, Nov 2015
- [16] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

## Appendix A – Communication Server 1000 Software

### Communication Server 1000 call server patches and plug ins

TID: 46379

VERSION 4121

System type is - Communication Server 1000/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: 2015-09-28 04:19:50 (est))

MDP>LAST SUCCESSFUL MDP REFRESH :2015-11-12 14:50:17(Local Time)

MDP>USING DEPLIST ZIP FILE DOWNLOADED :2013-09-28 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 1000 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 | 16/11/2015 | p32331_1.cpl | NO      |
| 001  | wi01064599 | iss1:1of1   | p32580_1 | 16/11/2015 | p32580_1.cpl | NO      |
| 002  | wi01056067 | ISS1:1OF1   | p32457_1 | 16/11/2015 | p32457_1.cpl | NO      |
| 003  | wi01063263 | ISS1:1OF1   | p32573_1 | 16/11/2015 | p32573_1.cpl | NO      |
| 004  | wi01065842 | ISS1:1OF1   | p32478_1 | 16/11/2015 | p32478_1.cpl | NO      |
| 005  | wi01062607 | ISS1:1OF1   | p32503_1 | 16/11/2015 | p32503_1.cpl | NO      |
| 006  | wi01070756 | ISS1:1OF1   | p32444_1 | 16/11/2015 | p32444_1.cpl | NO      |
| 007  | wi01039280 | ISS1:1OF1   | p32423_1 | 16/11/2015 | p32423_1.cpl | NO      |
| 008  | wi01087543 | ISS1:1OF1   | p32662_1 | 16/11/2015 | p32662_1.cpl | NO      |
| 009  | wi00933195 | ISS1:1OF1   | p32491_1 | 16/11/2015 | p32491_1.cpl | NO      |
| 010  | wi01071379 | ISS1:1OF1   | p32522_1 | 16/11/2015 | p32522_1.cpl | NO      |
| 011  | wi01068669 | ISS1:1OF1   | p32333_1 | 16/11/2015 | p32333_1.cpl | NO      |
| 012  | wi01066991 | ISS1:1OF1   | p32449_1 | 16/11/2015 | p32449_1.cpl | NO      |
| 013  | wi01070474 | iss1:1of1   | p32407_1 | 16/11/2015 | p32407_1.cpl | NO      |
| 014  | WI0110261  | ISS1:1OF1   | p32758_1 | 16/11/2015 | p32758_1.cpl | NO      |
| 015  | wi01094305 | ISS1:1OF1   | p32640_1 | 16/11/2015 | p32640_1.cpl | NO      |
| 016  | wi01047890 | ISS1:1OF1   | p32697_1 | 16/11/2015 | p32697_1.cpl | NO      |
| 017  | wi01055300 | ISS1:1OF1   | p32543_1 | 16/11/2015 | p32543_1.cpl | NO      |

|     |            |           |          |            |              |     |
|-----|------------|-----------|----------|------------|--------------|-----|
| 018 | wi01082456 | ISS1:10F1 | p32596_1 | 16/11/2015 | p32596_1.cpl | NO  |
| 019 | wi01058621 | ISS1:10F1 | p32339_1 | 16/11/2015 | p32339_1.cpl | NO  |
| 020 | wi01061484 | ISS1:10F1 | p32576_1 | 16/11/2015 | p32576_1.cpl | NO  |
| 021 | wi01078723 | ISS1:10F1 | p32532_1 | 16/11/2015 | p32532_1.cpl | NO  |
| 022 | wi01048457 | ISS1:10F1 | p32581_1 | 16/11/2015 | p32581_1.cpl | NO  |
| 023 | wi01075355 | ISS1:10F1 | p32594_1 | 16/11/2015 | p32594_1.cpl | NO  |
| 024 | wi01053597 | ISS1:10F1 | p32304_1 | 16/11/2015 | p32304_1.cpl | NO  |
| 025 | wi01045058 | ISS1:10F1 | p32214_1 | 16/11/2015 | p32214_1.cpl | NO  |
| 026 | wi01075359 | ISS1:10F1 | p32671_1 | 16/11/2015 | p32671_1.cpl | NO  |
| 027 | wi01025156 | ISS1:10F1 | p32136_1 | 16/11/2015 | p32136_1.cpl | NO  |
| 028 | wi01061481 | ISS1:10F1 | p32382_1 | 16/11/2015 | p32382_1.cpl | NO  |
| 029 | wi01035976 | ISS1:10F1 | p32173_1 | 16/11/2015 | p32173_1.cpl | NO  |
| 030 | wi01088775 | ISS1:10F1 | p32659_1 | 16/11/2015 | p32659_1.cpl | NO  |
| 031 | wi01070465 | iss1:10f1 | p32562_1 | 16/11/2015 | p32562_1.cpl | NO  |
| 032 | wi01088585 | ISS1:10F1 | p32656_1 | 16/11/2015 | p32656_1.cpl | NO  |
| 033 | wi01063864 | ISS1:10F1 | p32410_1 | 16/11/2015 | p32410_1.cpl | YES |
| 034 | wi01034961 | ISS1:10F1 | p32144_1 | 16/11/2015 | p32144_1.cpl | NO  |
| 035 | wi01055480 | ISS1:10F1 | p32712_1 | 16/11/2015 | p32712_1.cpl | NO  |
| 036 | wi01034307 | ISS1:10F1 | p32615_1 | 16/11/2015 | p32615_1.cpl | NO  |
| 037 | wi01065118 | ISS1:10F1 | p32397_1 | 16/11/2015 | p32397_1.cpl | NO  |
| 038 | wi01075360 | iss1:10f1 | p32602_1 | 16/11/2015 | p32602_1.cpl | NO  |
| 039 | wi00884716 | ISS1:10F1 | p32517_1 | 16/11/2015 | p32517_1.cpl | NO  |
| 040 | wi01068851 | ISS1:10F1 | p32439_1 | 16/11/2015 | p32439_1.cpl | NO  |
| 041 | wi01053314 | ISS1:10F1 | p32555_1 | 16/11/2015 | p32555_1.cpl | NO  |
| 042 | wi01059388 | iss1:10f1 | p32628_1 | 16/11/2015 | p32628_1.cpl | NO  |
| 043 | wi01087528 | ISS1:10F1 | p32700_1 | 16/11/2015 | p32700_1.cpl | NO  |
| 044 | wi01072027 | ISS1:10F1 | p32689_1 | 16/11/2015 | p32689_1.cpl | NO  |
| 045 | wi01052428 | ISS1:10F1 | p32606_1 | 16/11/2015 | p32606_1.cpl | NO  |
| 046 | wi01053920 | ISS1:10F1 | p32303_1 | 16/11/2015 | p32303_1.cpl | NO  |
| 047 | wi01070468 | iss1:10f1 | p32418_1 | 16/11/2015 | p32418_1.cpl | NO  |
| 048 | wi01067822 | ISS1:10F1 | p32466_1 | 16/11/2015 | p32466_1.cpl | YES |
| 049 | wi01060826 | ISS1:10F1 | p32379_1 | 16/11/2015 | p32379_1.cpl | NO  |
| 050 | wi01075352 | ISS1:10F1 | p32603_1 | 16/11/2015 | p32603_1.cpl | NO  |
| 051 | wi01043367 | ISS1:10F1 | p32232_1 | 16/11/2015 | p32232_1.cpl | NO  |
| 052 | wi01083584 | ISS1:10F1 | p32619_1 | 16/11/2015 | p32619_1.cpl | NO  |
| 053 | wi01060241 | ISS1:10F1 | p32381_1 | 16/11/2015 | p32381_1.cpl | NO  |
| 054 | wi01053195 | ISS1:10F1 | p32297_1 | 16/11/2015 | p32297_1.cpl | NO  |
| 055 | wi00897254 | ISS1:10F1 | p31127_1 | 16/11/2015 | p31127_1.cpl | NO  |
| 056 | wi01061483 | ISS1:10F1 | p32359_1 | 16/11/2015 | p32359_1.cpl | NO  |
| 057 | wi01085855 | ISS1:10F1 | p32658_1 | 16/11/2015 | p32658_1.cpl | NO  |
| 058 | wi01075353 | ISS1:10F1 | p32613_1 | 16/11/2015 | p32613_1.cpl | NO  |
| 059 | wi01070471 | ISS1:10F1 | p32415_1 | 16/11/2015 | p32415_1.cpl | NO  |
| 060 | wi01074003 | ISS1:10F1 | p32421_1 | 16/11/2015 | p32421_1.cpl | NO  |
| 061 | wi01060382 | iss1:10f1 | p32623_1 | 16/11/2015 | p32623_1.cpl | YES |
| 062 | wi01068042 | ISS1:10F1 | p32669_1 | 16/11/2015 | p32669_1.cpl | NO  |
| 063 | wi01072023 | ISS1:10F1 | p32130_1 | 16/11/2015 | p32130_1.cpl | YES |
| 064 | wi01065922 | ISS1:10F1 | p32516_1 | 16/11/2015 | p32516_1.cpl | NO  |
| 065 | wi01057403 | ISS1:10F1 | p32591_1 | 16/11/2015 | p32591_1.cpl | NO  |
| 066 | wi01069441 | ISS1:10F1 | p32097_1 | 16/11/2015 | p32097_1.cpl | NO  |
| 067 | wi01070473 | ISS1:10F1 | p32413_1 | 16/11/2015 | p32413_1.cpl | NO  |
| 068 | wi01056633 | ISS1:10F1 | p32322_1 | 16/11/2015 | p32322_1.cpl | NO  |
| 069 | wi01052968 | ISS1:10F1 | p32540_1 | 16/11/2015 | p32540_1.cpl | NO  |
| 070 | wi01072032 | ISS1:10F1 | p32448_1 | 16/11/2015 | p32448_1.cpl | NO  |
| 071 | wi01073100 | ISS1:10F1 | p32599_1 | 16/11/2015 | p32599_1.cpl | NO  |
| 072 | wi01035980 | ISS1:10F1 | p32558_1 | 16/11/2015 | p32558_1.cpl | NO  |
| 073 | wi01041453 | ISS1:10F1 | p32587_1 | 16/11/2015 | p32587_1.cpl | NO  |
| 074 | wi01032756 | ISS1:10F1 | p32673_1 | 16/11/2015 | p32673_1.cpl | NO  |
| 075 | wi01092300 | ISS1:10F1 | p32692_1 | 16/11/2015 | p32692_1.cpl | NO  |
| 076 | wi00996734 | ISS1:10F1 | p32550_1 | 16/11/2015 | p32550_1.cpl | NO  |
| 077 | wi01022599 | ISS1:10F1 | p32080_1 | 16/11/2015 | p32080_1.cpl | NO  |
| 078 | wi01060341 | ISS1:10F1 | p32578_1 | 16/11/2015 | p32578_1.cpl | NO  |
| 079 | wi01091447 | ISS1:10F1 | p32675_1 | 16/11/2015 | p32675_1.cpl | NO  |
| 080 | wi01070580 | ISS1:10F1 | p32380_1 | 16/11/2015 | p32380_1.cpl | NO  |
| 081 | wi01089519 | ISS1:10F1 | p32665_1 | 16/11/2015 | p32665_1.cpl | NO  |
| 082 | WI01077073 | ISS1:10F1 | p32534_1 | 16/11/2015 | p32534_1.cpl | NO  |
| 083 | wi01080753 | ISS1:10F1 | p32518_1 | 16/11/2015 | p32518_1.cpl | NO  |
| 084 | wi01065125 | ISS1:10F1 | p32416_1 | 16/11/2015 | p32416_1.cpl | NO  |

### Communication Server 1000 signaling server service updates

In System service updates: 41

| 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        | 14/10/15 | YES     | YES       | cs1000-dmWeb-7.65.16.23-4.i386.000          |
| 3                      | Yes        | 15/10/15 | NO      | YES       | cs1000-sps-7.65.16.23-1.i386.000            |
| 4                      | Yes        | 14/07/14 | YES     | YES       | cs1000-patchWeb-7.65.16.22-4.i386.000       |
| 5                      | Yes        | 14/10/15 | YES     | YES       | cs1000-linuxbase-7.65.16.23-19.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         |
| 16                     | Yes        | 14/10/15 | NO      | YES       | cs1000-Jboss-Quantum-7.65.16.23-5.i386.000  |
| 17                     | Yes        | 15/10/15 | YES     | YES       | cs1000-cs-7.65.P.100-03.i386.000            |
| 18                     | Yes        | 15/10/15 | NO      | YES       | bash-3.2-33.el5_11.4.i386.000               |
| 19                     | Yes        | 15/10/15 | YES     | YES       | cs1000-shared-pbx-7.65.16.23-1.i386.000     |
| 20                     | Yes        | 15/10/15 | YES     | YES       | cs1000-emWeb_6-0-7.65.16.23-3.i386.000      |
| 21                     | Yes        | 15/10/15 | NO      | YES       | libxml2-2.6.26-2.1.25.el5_11.i386.000       |
| 22                     | Yes        | 15/10/15 | NO      | YES       | libxml2-python-2.6.26-                      |
| 2.1.25.el5_11.i386.000 |            |          |         |           |                                             |
| 23                     | Yes        | 02/04/14 | NO      | YES       | cs1000-shared-omm-7.65.16.21-2.i386.000     |
| 24                     | Yes        | 15/10/15 | NO      | YES       | freetype-2.2.1-32.el5_9.1.i386.000          |
| 26                     | Yes        | 15/10/15 | NO      | YES       | cs1000-cs1000WebService_6-0-7.65.16.23-     |
| 1.i386.000             |            |          |         |           |                                             |
| 27                     | Yes        | 14/07/14 | YES     | YES       | cs1000-oam-logging-7.65.16.22-4.i386.000    |
| 28                     | Yes        | 15/10/15 | YES     | YES       | cs1000-ftrpkg-7.65.16.23-1.i386.000         |
| 29                     | Yes        | 15/10/15 | NO      | YES       | cs1000-cppmUtil-7.65.16.23-4.i686.000       |
| 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            |
| 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 |
| 39                     | Yes        | 15/10/15 | NO      | YES       | tzdata-2015a-1.el5.i386.000                 |
| 40                     | Yes        | 02/04/14 | YES     | YES       | cs1000-ipsec-7.65.16.22-1.i386.000          |
| 41                     | Yes        | 15/10/15 | YES     | YES       | cs1000-tps-7.65.16.23-15.i386.000           |
| 43                     | Yes        | 15/10/15 | YES     | YES       | kernel-2.6.18-406.el5.i686.000              |
| 44                     | Yes        | 15/10/15 | YES     | YES       | cs1000-vtrk-7.65.16.23-76.i386.000          |
| 45                     | Yes        | 15/10/15 | YES     | YES       | cs1000-bcc-7.65.16.23-10.i386.000           |
| 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             |
| 53                     | Yes        | 14/07/14 | YES     | YES       | cs1000-shared-xmsg-7.65.16.22-1.i386.000    |

## Communication Server 1000 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 |           |
| c ppmUtil           | 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] |

---

**©2016 Avaya Inc. All Rights Reserved.**

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

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