



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Communication Server 1000 R7.65, Avaya Aura® Session Manager 7.0 and Avaya Session Border Controller for Enterprise R7.0 to support BT Global Services SIP Trunk Platform (NOAS) - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between BT Global Services SIP Trunk 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. BT 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 BT Global Services SIP Trunk 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 BT Global Services SIP Trunk 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 10000, Session Manager and Avaya SBCE. The enterprise site was configured to connect to the BT Global Services SIP Trunk Platform.

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

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from the PSTN were routed to the DID numbers assigned by BT. Incoming PSTN calls were terminated on Digital, Unistim, SIP and Analog telephones at the enterprise side.
- Outgoing calls from the enterprise site were completed via BT to PSTN telephones. Outgoing calls from the enterprise to the PSTN were made from Digital, Unistim, SIP and Analog telephones.
- Calls using the G.711A and G.729A codecs.
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using T.38.
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Transmission and response of SIP OPTIONS messages sent by BT Global Services SIP Trunk Platform requiring Avaya response and sent by Avaya requiring BT response.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for BT Global Services SIP Trunk 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. 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.
- When testing failover to alternative network SBC, outgoing calls took approximately 32 seconds to set up. A subsequent call did not attempt to set up via the non-operational SBC and was established within an acceptable time though there was no audio. An attempt was made to reduce the initial setup time by reducing SIP timer T1 on the Avaya SBCE but this did not function according to RFC 3261. Fault Report AURORA-7344 was raised to have this investigated by the Avaya SBCE support team.
- The SIP Trunk between the Avaya Galway Lab and the BT Sandbox was unstable and became non-operational several times during testing. This was deemed to be a network issue and not related to the functionality of the BT Global Services SIP Trunk Platform.
- The network responded to an outbound call to an invalid PSTN number with 404 “Service Unavailable-No ports available”. This behaviour did not create an issue and a tone was heard on the calling phone. It is noted however, as the commonly used response is 404 “Not Found”.
- The BT Sandbox did not have a voicemail system in operation at the time of test. Instead DTMF was successfully tested using IVR.
- There are no mobile phones available on the BT sandbox so Mobile X feature was tested with a fixed phone.
- All unwanted MIME was stripped on outbound calls using the Adaptation Module in Session Manager.
- No inbound toll free numbers were tested as none were available from the Service Provider.
- No Emergency Services numbers tested as test calls to these numbers should be pre-arranged with the Operator.

2.3. Support

For technical support on BT Global Services products please contact BT Global Services on 0800 028 5314 or visit their website at www.globalservices.bt.com

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to BT'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.

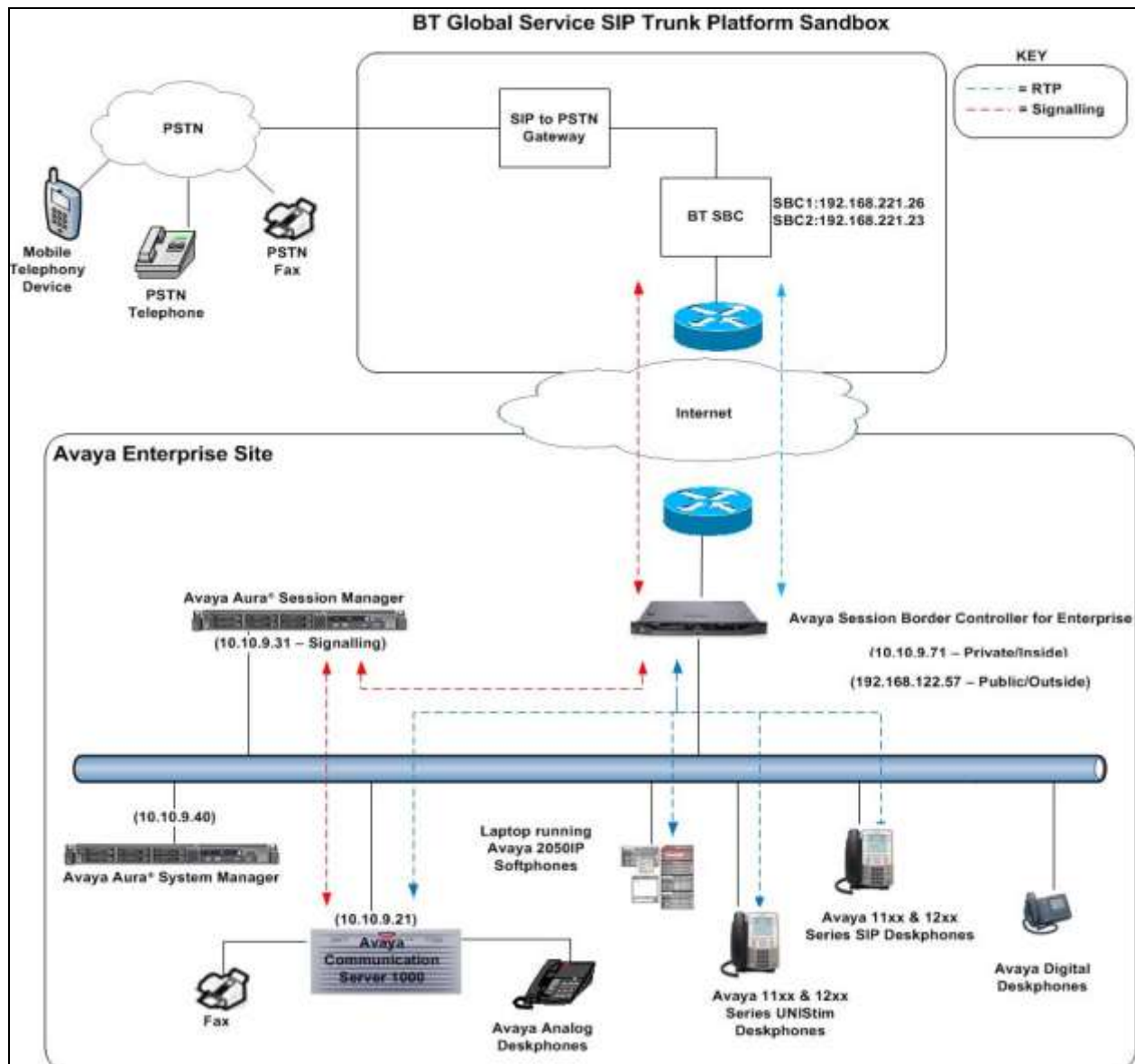


Figure 1: Test Setup BT SIP Trunk to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Session Manager	7.0.0.0.700007
Avaya Aura® System Manager	7.0.0.0.16266
Avaya Communication Server 1000	Avaya Communication Server 1000E R7.6 Version 7.65.P Deplist: CPL_X21_07_65P All CS1000 patches listed in Appendix A
Avaya Communication Server 1000E Media Gateway	CSP Version: MGCC DC01 MSP Version: MGCM AB02 APP Version: MGCA BA18 FPGA Version: MGCF AA22 BOOT Version: MGCB BA18 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 Analogue Telephone	N/A
Avaya M3904 Digital Telephone	N/A
BT Global Services	
Genband S3 Session Border Controller	8.3.7.1
NOAS Call Server	4.38.0.1

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 the BT Global Services SIP trunks. Incoming PSTN calls from the BT Global Services SIP Trunk 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 BT Global Services SIP trunks.

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.

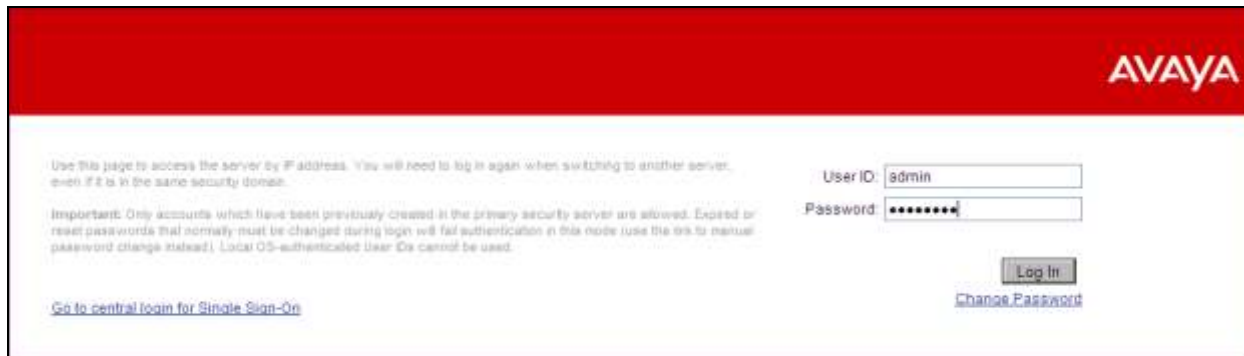
5.1. Logging into the Avaya Communication Server 1000E

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"/>	EM on cs1kv19	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 BT Global Services 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

BT Global Service'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

Voice Codecs

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: 200 * (0-9999)

Call server IP address: 192.168.27.2 *

TLAN address type: ☒ IPv4 only
☐ IPv4 and IPv6

Embedded LAN (ELAN)

Gateway IP address: 192.168.27.1 *

Subnet mask: 255.255.255.0 *

Telephony LAN (TLAN)

Node IPv4 address: 10.10.9.21 *

Subnet mask: 255.255.255.0 *

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:

Proxy Or Redirect Server:	
Proxy Server Route 1:	
Primary TLAN IP address:	<input type="text" value="10.10.9.31"/>
<small>The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"</small>	
Port:	<input type="text" value="5060"/> (1 - 65535)
Transport protocol:	<input type="text" value="TCP"/>
Options:	<input type="checkbox"/> Support registration
	<input type="checkbox"/> Primary CDS proxy

SIP URI Map:	
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 UNISim telephones depending on the particular test case being executed.

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	445511	6000	
2	445511	6001	
3	445511	6002	
4	445511	6003	
5	445511	6005	
6	445511	6007	

5.7. Configure SIP Trunks

CS1000 virtual trunks will be used for all inbound and outbound PSTN calls to the BT Global Services SIP Trunk 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
    OVLR 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.

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

Next, configure virtual trunk members using the 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 data block (DGT) in overlay 86. Load **Overlay 86** at the system terminal and type **new**. The following example shows the values used. **Note: ISPN** is set to **0** as BT Global Services required a prefix of 0 to be inserted before the dialed number for outbound calls. The value for Digit Manipulation Index (**DMI**) is the same as when inputting the **DMI** value during configuration of the Route List Block.

```
Overlay 86
CUST 0
FEAT dgt
DMI 10
DEL 0
ISPN 0
CTYP NPA
```

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

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

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

ISET 0
NALT 5
MFRL 0
OVL 0
```

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	TSC 18	TSC 800	TSC 08
FLEN 0	FLEN 0	FLEN 0	FLEN 0
RRPA NO	RRPA NO	RRPA NO	RRPA NO
RLI 10	RLI 10	RLI 10	RLI 10
CCBA NO	CCBA NO	CCBA NO	CCBA NO

5.8. Calling Line Identification

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

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

5.9. Configure Analog, Digital and IP Telephones

A variety of telephone types were used during the testing, the following is the configuration for the Avaya 1140e 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 OCBD FLXD FTTC DNDY DNO3 MCBN
    FDSF NOVD CDMR PRED RECA MCDD T87D SBMD PKCH CROD CROD
CPND LANG ENG
RCO 0
HUNT
PLEV 02
PUID
DANI NO
SPID NONE
AST
IAPG 1
AACS
ACQ
ASID
SFNB
SFRB
USFB
CALB
FCTB
ITNA NO
DGRP
PRI 01
MLWU_LANG 0
```

---continued on next page---

---continued from previous page----

MLNG ENG

DNDR 0

KEY 00 MCR 6066 0 MARP

CPND

CPND_LANG ROMAN

NAME Digital Set

XPLN 10

DISPLAY_FMT FIRST, LAST

01 MCR 6066 0

CPND

CPND_LANG ROMAN

NAME Digital Set

XPLN 10

DISPLAY_FMT FIRST, LAST

02 DSP

03 MSB

04

05

06

07

08

09

10

11

12

13

14

15

16

17 TRN

18 AO6

19 CFW 16

20 RGA

21 PRK

22 RNP

23

24 PRS

25 CHG

26 CPN

27 CLT

28 RLT

29

30

31

Analog telephones are also configured using overlay 20; the following example shows an analog port configured for Plain Ordinary Telephone Service (POTS) and also configured to allow fax transmission. A unique value is entered for **DN**, this is the extension number. **DTN** is required if the telephone uses DTMF dialing. Values **FAXA** and **MPTD** configure the port for T.38 Fax transmissions.

Overlay 20 - Analog Telephone Configuration

```
DES 500
TN 100 0 00 03
TYPE 500
CDEN 4D
CUST 0
MRT

ERL 00000
WRLS NO
DN 6004
AST NO
IAPG 0
HUNT
TGAR 0
LDN NO
NCOS 0
SGRP 0
RNPG 0
XLST
SCI 0
SCPW
SFLT NO
CAC_MFC 0
CLS UNR DTN FBD XFD WTA THFD FND HTD ONS
    LPR XRD AGRD CWD SWD MWD RMMD SMWD LPD XHD SLKD CCSD LND TVD
    CFTD SFD MRD C6D CNID CLBD AUTU
    ICDD CDMD LLCN EHTD MCTD
    GPUD DPUD CFXD ARHD OVDD AGTD CLTD LDTD ASCD SDND
    MBXD CPFA CPTA UDI RCC HBTD IRGD DDGA NAMA MIND
    NRWD NRCD NROD SPKD CRD PRSD MCRD
    EXR0 SHL SMSD ABDD CFHD DNDY DNO3
    CWND USMD USRD CCBD BNRD 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
```

5.10. 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**

The screenshot shows the 'Node ID: 200 - SIP Line Configuration Details' page. At the top, it says 'Managing: 192.168.27.2 Username: admin' and 'System » IP Network » IP Telephony Nodes » Node Details » SIP Line Configuration'. The page has three tabs: 'General', 'SIP Line Gateway Settings', and 'SIP Line Gateway Service'. The 'SIP Line Gateway Application' checkbox is checked, with the label 'Enable gateway service on this node'. Below this, there are two main sections: 'General' and 'Virtual Trunk Network Health Monitor'. The 'General' section contains fields for 'SIP domain name' (avaya.com), 'SLG endpoint name' (cs1kv19), 'SLG Group ID' (empty), 'SLG Local Sip port' (5070, with a note '(1 - 65535)'), and 'SLG Local Tls port' (5071, with a note '(1 - 65535)'). The 'Virtual Trunk Network Health Monitor' section has a checkbox for 'Monitor IP addresses (listed below)' which is unchecked. Below this checkbox is a note 'Information will be captured for the IP addresses listed below.' There are two input fields: 'Monitor IP:' and 'Monitor addresses:'. The 'Monitor IP:' field has an 'Add' button next to it. The 'Monitor addresses:' field has a 'Remove' button next to it.

5.1. 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 5.8**) value and the telephone number used in **KEY 00**.

```
Load Overlay 20 - SIP Telephone Configuration
DES  SIPD
TN    100 0 03 3  VIRTUAL
TYPE  UEXT
CDEN  8D
CTYP  XDLC
CUST  0
UXTY SIPL
MCCL YES
SIPN 1
SIP3  0
FMCL  0
TLSV  0
SIPU 6002
NDID  200
SUPR  NO
SUBR  DFLT MWI RGA CWI MSB
UXID
NUID
NHTN
CFG_ZONE 00002
CUR_ZONE 00002
ERL   0
ECL   0
VSIT  NO
FDN
TGAR  0
LDN   NO
NCOS  0
SGRP  0
RNPG  0
SCI   0
SSU
XLST
SCPW 1234
SFLT  NO
CAC   MFC 0
CLS   UNR FBD WTA LPR MTD FNA HTA TDD HFD CRPD
      MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
      POD SLKD CCSD SWD LND CNDA
      CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED 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 HBTD 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
```

5.2. 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 of this area, it says 'Managing: 192.168.27.2 Username: admin' and 'Tools » Backup and Restore » Call Server Backup and Restore » Call Server Backup'. Below this is a form with an 'Action' dropdown menu set to 'Backup', and two buttons: 'Submit' (highlighted with a red box) and 'Cancel'.

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 terminal window with the following text: 'Backing up reten.bkp to "/var/opt/nortel/cs/fs/cf2/backup/single"', 'Database backup Complete!', 'TEMU207', and 'Backup process to local Removable Media Device ended successfully.' The last line is highlighted with a red box.

6. Configuring Avaya Aura® Session Manager

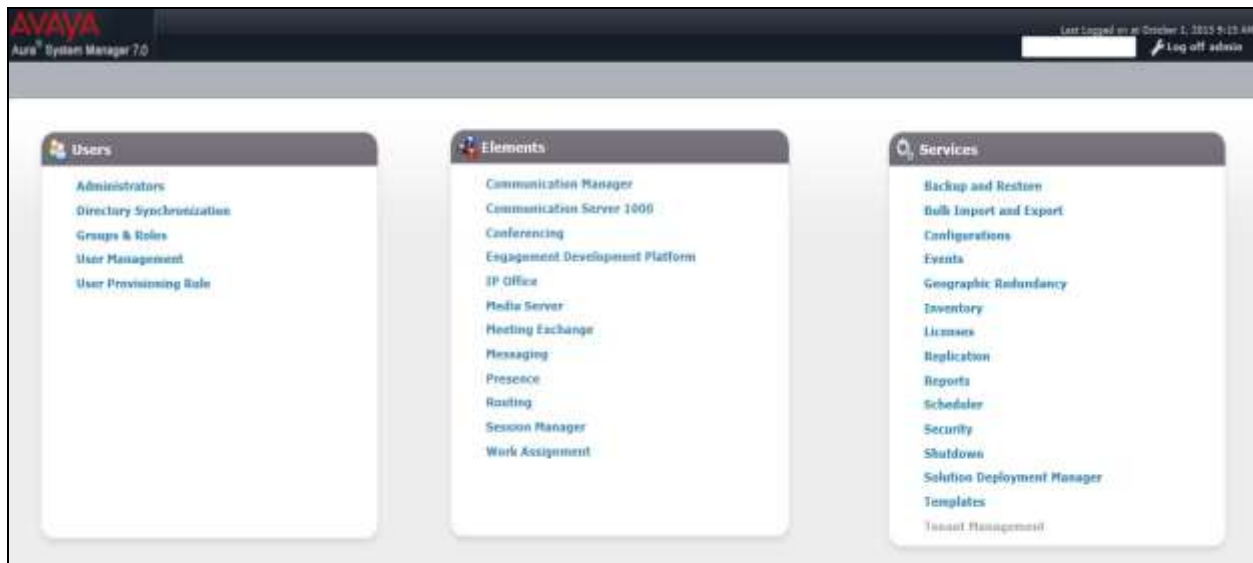
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- 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.

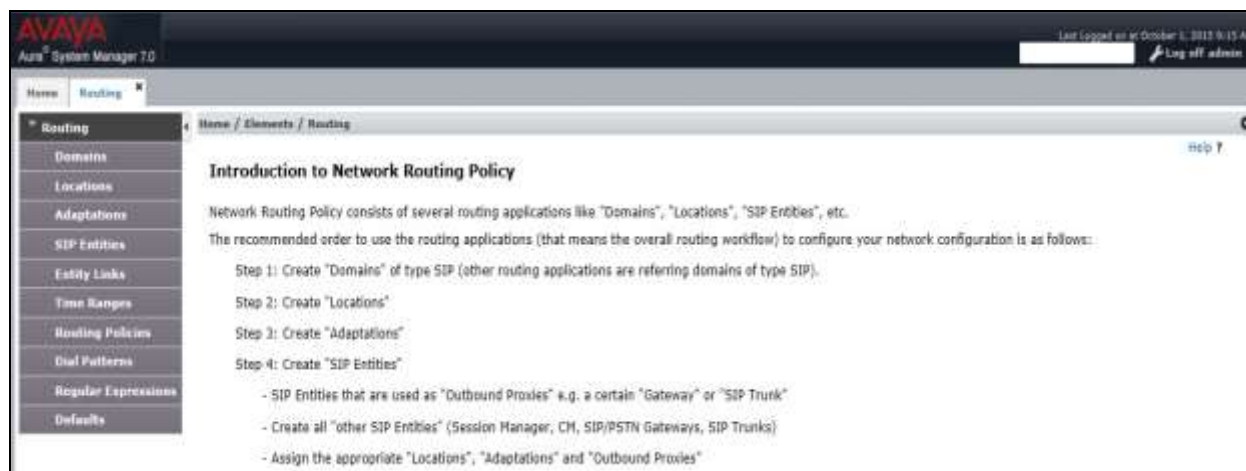
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

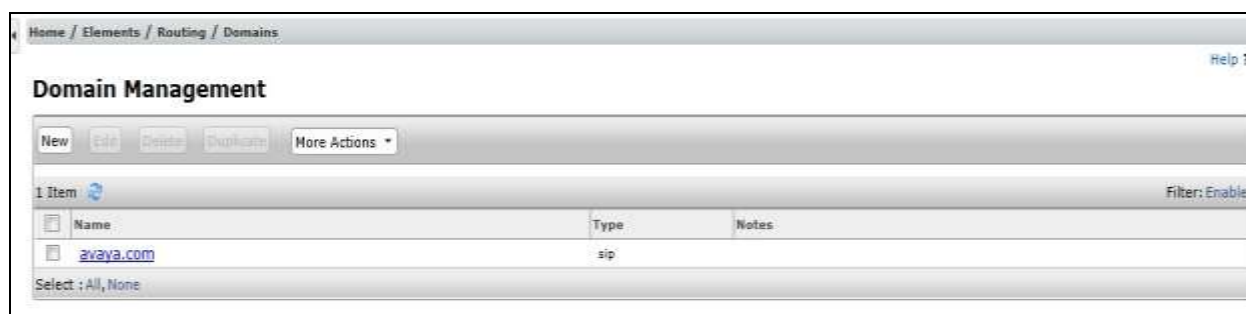


6.2. Administer SIP Domain

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 'Add' and 'Remove' buttons, a 'Filter: Enable' link, and 'Commit' and 'Cancel' buttons at the 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. The example below was applied to the Avaya SBCE SIP Entity and was used in test to convert numbers being passed between the Avaya SBCE and Session Manager.

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

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

Name	Value
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.

Digit Conversion for Incoming Calls to SM

Add Remove

1 Item Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
*+44	3	15		1		both		

Select: All, None

This will ensure any incoming numbers matching +44 will have the + digit removed before being presented to the Communication Server 1000.

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.

Digit Conversion for Outgoing Calls from SM

Add Remove

3 Items Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
*6000	4	4		4	055xxxxxx00	both		
*6001	4	4		4	055xxxxxx01	both		
*6002	4	4		4	055xxxxxx02	both		

Select: All, None

Commit Cancel

This will ensure any destination numbers beginning with 6 will have a specified CLID presented on outbound calls.

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.

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* Name: Session Manager

* FQDN or IP Address: 10.10.9.31

Type: Session Manager

Notes:

Location: SM_7

Outbound Proxy:

Time Zone: Europe/Dublin

Credential name:

SIP Link Monitoring

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.

Listen Ports

TCP Failover port:

TLS Failover port:

Add Remove

3 Items Filter: Enable

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

Select : All, None

6.5.2. Avaya 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 box)
- 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 box)
- 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.

The screenshot shows the 'SIP Link Monitoring' configuration page. It contains the following fields and values:

- Loop Detection Mode:** Off (dropdown menu)
- SIP Link Monitoring:** 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-based configuration interface for 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:

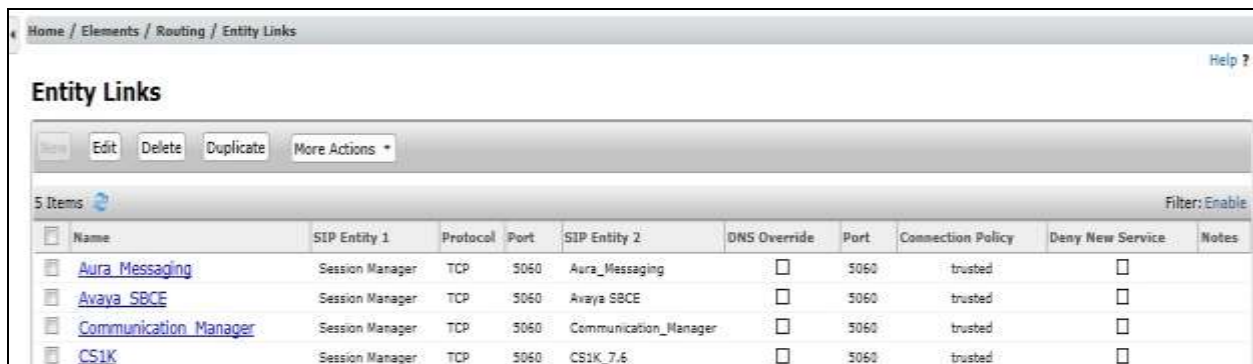
- Name:** Avaya SBCE
- * FQDN or IP Address:** 10.10.9.71
- Type:** SIP Trunk (dropdown menu)
- Notes:** (empty text area)
- Adaptation:** BTG (dropdown menu)
- Location:** SM_7 (dropdown menu)
- Time Zone:** Europe/Dublin (dropdown menu)
- * SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Securable:** ☐
- Call Detail Recording:** egress (dropdown menu)
- Loop Detection Mode:** Off (dropdown menu)

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
Aura_Messaging	Session Manager	TCP	5060	Aura_Messaging	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
Avaya_SBCE	Session Manager	TCP	5060	Avaya_SBCE	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
Communication_Manager	Session Manager	TCP	5060	Communication_Manager	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
CS1K	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. The 'General' section has fields for Name (to_CS1K_7.6), Disabled (checkbox), Retries (0), and Notes. The 'SIP Entity as Destination' section has a 'Select' button and a table with one row: CS1K_7.6, 10.10.9.21, Other. The 'Time of Day' section has 'Add', 'Remove', and 'View Gaps/Overlaps' buttons, a table with one row for 24/7, and a 'Filter: Enable' button.

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

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

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

The screenshot shows the 'Routing Policy Details' configuration page. The breadcrumb trail is 'Home / Elements / Routing / Routing Policies'. The page title is 'Routing Policy Details' with 'Commit' and 'Cancel' buttons. The 'General' tab is active, showing fields for 'Name' (to_Avaya SBCE), 'Disabled' (checkbox), 'Retries' (0), and 'Notes'. Below this is the 'SIP Entity as Destination' section with a 'Select' dropdown and a table listing 'Avaya SBCE' with FQDN '10.10.9.71' and Type 'SIP Trunk'. The 'Time of Day' section includes 'Add', 'Remove', and 'View Gaps/Overlaps' buttons, a '1 Item' indicator, and a table with columns for Ranking, Name, days of the week, Start Time, End Time, and Notes. The table shows a single entry with Ranking 0, Name 24/7, and Time Range 24/7. A 'Filter: Enable' link is also present.

Name	FQDN or IP Address	Type	Notes
Avaya SBCE	10.10.9.71	SIP Trunk	

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7								00:00	23:59	Time Range 24/7

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'. The 'Min' field is '2' and the 'Max' field is '15'. The 'Emergency Call' checkbox is unchecked. The 'Emergency Priority' field is '1'. The 'Emergency Type' field is empty. The 'SIP Domain' dropdown is set to '-ALL-'. The 'Notes' field 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 '4455'. The 'Min' field is '4' and the 'Max' field is '15'. The 'Emergency Call' checkbox is unchecked. The 'Emergency Priority' field is '1'. The 'Emergency Type' field is empty. The 'SIP Domain' dropdown is set to '-ALL-'. The 'Notes' field is empty. Below the 'General' tab is the 'Originating Locations and Routing Policies' section, which contains a table with one item.

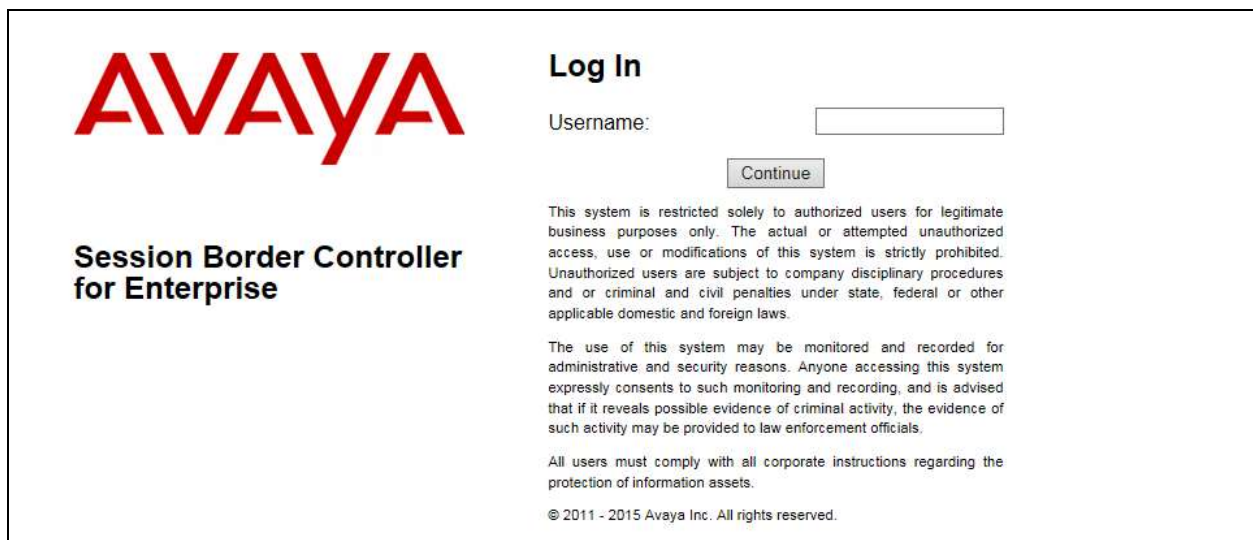
Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
SM_7		to_CS1K_7,6	0	<input type="checkbox"/>	CS1K_7,6	

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 text stating that the system is restricted to authorized users and that unauthorized access is prohibited. Further down, another block of text mentions that system use may be monitored for administrative and security reasons. At the bottom, a copyright notice reads "© 2011 - 2015 Avaya Inc. All rights reserved."

AVAYA

Log In

Username:

Continue

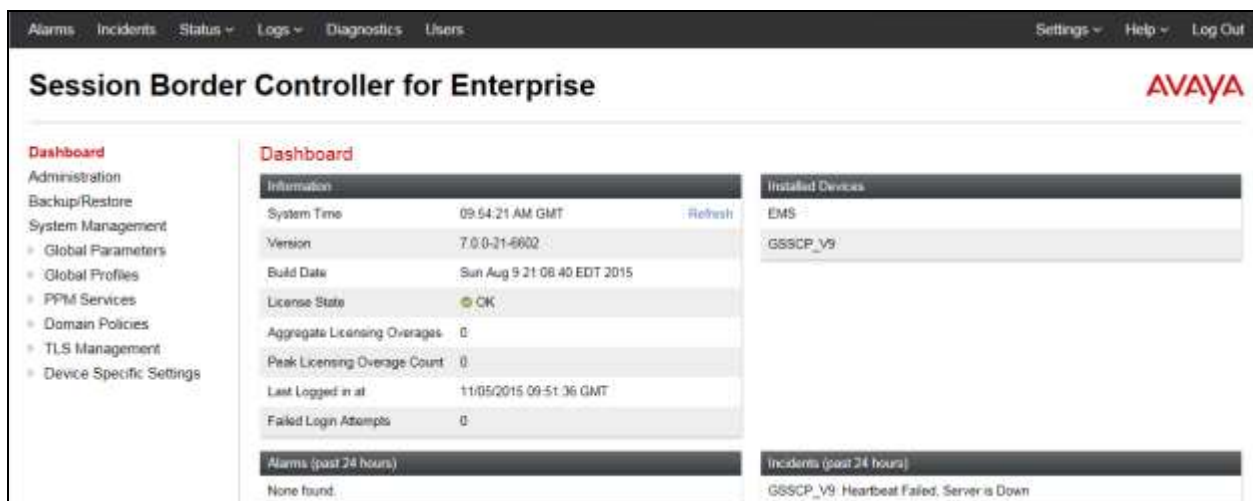
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under 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 for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo on the right. A left-hand menu lists various configuration options. The main content area is divided into three sections: "Information" with system details, "Installed Devices" showing a list of devices, and "Alarms (past 24 hours)" and "Incidents (past 24 hours)" sections.

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise **AVAYA**

Dashboard

Information

System Time	09:54:21 AM GMT	Refresh
Version	7.0.0-31-6602	
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 09:51:36 GMT	
Failed Login Attempts	0	

Alarms (past 24 hours)

None found.

Installed Devices

EMS
GSSCP_V9

Incidents (past 24 hours)

GSSCP_V9: Heartbeat Failed. Server is Down

Dashboard

- Administration
- Backup/Restore
- System Management
 - Global Parameters
 - Global Profiles
 - PPM Services
 - Domain Policies
 - TLS Management
 - Device Specific Settings

7.2. Define Network Management

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** in the main menu on the left hand side and click on **Add**.



Enter details for the external interface in the dialogue box:

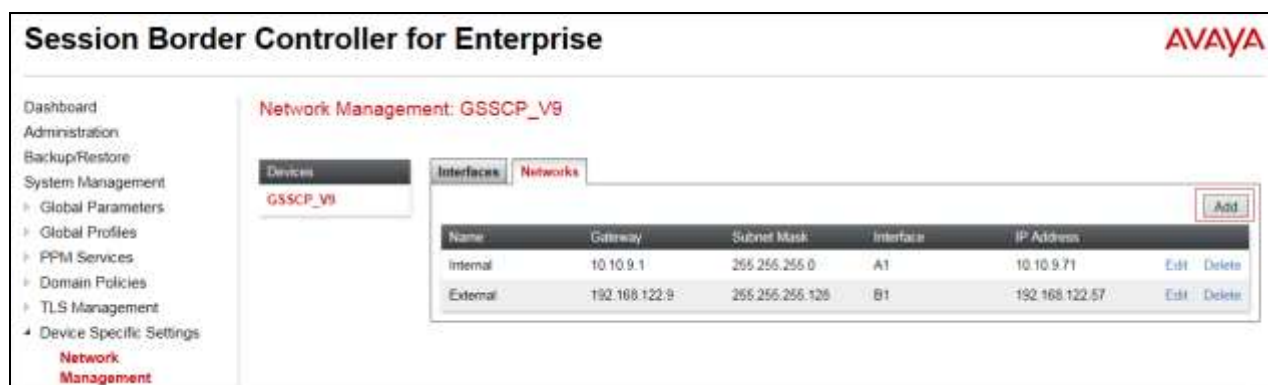
- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the external interface in the **Default Gateway** field.
- Enter the subnet mask in the **Subnet Mask** field.
- Select the external interface to be used from the **Interface** drop down menu. In the test environment, this was **B1**.
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the external IP address in the IP Address field and leave the Public IP and Gateway Override fields blank.
- Click on **Finish** to complete the interface definition.



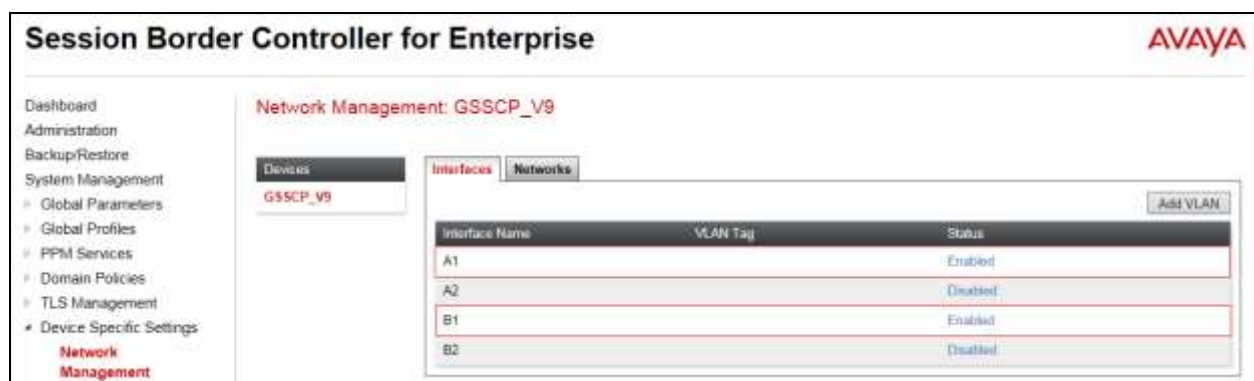
Click on **Add** to define the internal interface. Enter details in the dialogue box (not shown):

- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the internal interface in the **Default Gateway** field.
- Enter the subnet mask in the **Subnet Mask** field.
- Select the internal interface to be used from the **Interface** drop down menu. In the test environment, this was **A1**.
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the internal IP address in the IP Address field and leave the Public IP and Gateway Override fields blank.
- Click on **Finish** to complete the interface definition.

The following screenshot shows the completed Network Management configuration:



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



Note: to ensure that the Avaya SBCE uses the interfaces defined, the Application must be restarted.

- Click on **System Management** in the main menu (not shown).
- Select **Restart Application** indicated by an icon in the status bar (not shown).

7.3. Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces. Testing was carried out with TCP used for transport of signalling between the Session Manager and the Avaya SBCE, and UDP for transport of signalling between the Avaya SBCE and the BT Global Services SIP Trunk. This document shows the configuration for TCP and UDP, if additional security is required, it's recommended to use TLS and port 5061.

7.3.1. Signalling Interfaces

To define the signalling interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Signaling Interface** (not shown) in the main menu on the left hand side. Details of transport protocol and ports for the external and internal SIP signalling are entered here.

- Select **Add** and enter details of the external signalling interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the external signalling interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. Note that when the external network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 7.2**. In the test environment, this was a single IP address **192.168.122.57**.
- Enter the UDP port number in the **UDP Port** field, **5060** is used for the BT Global Services SIP Trunk.

The screenshot shows the 'Session Border Controller for Enterprise' web interface. On the left is a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. Under 'Device Specific Settings', 'Signaling Interface' is highlighted. The main content area shows the 'Add Signaling Interface' dialog box. The dialog has the following fields: Name (set to 'External'), IP Address (set to 'External (BT, VLAN 0)' with a dropdown showing '192.168.122.57'), TCP Port (set to 'Leave blank to disable'), UDP Port (set to '5060'), TLS Port (set to 'Leave blank to disable'), TLS Profile (set to 'None'), Enable Shared Control (checkbox), and Shared Control Port (text field). A 'Finish' button is at the bottom right.

The internal signalling interface is defined in the same way; the dialogue box is not shown:

- Select **Add** and enter details of the internal signalling interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal signalling interface.
- In the **IP Address** drop down menus, select the internal network interface and IP address.
- Select **TCP** port number, **5060** is used for the Session Manager.

The following screenshot shows details of the signalling interfaces:

Signaling Interface: GSSCP_V9

Devices

GSSCP_V9

Signaling Interface

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

Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Internal	10.10.9.71 Internal (A1, VLAN 0)	5060	---	---	None	Edit Delete
External	192.168.122.57 External (B1, VLAN 0)	---	5060	---	None	Edit Delete

Note. In the test environment, the internal IP address was **10.10.9.71**.

7.3.2. Media Interfaces

To define the media interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Media Interface** in the main 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.

- Select **Add** and enter details of the external media interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the external media interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. Note that when the external network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 7.2**. In the test environment, this was a single IP address **192.168.122.57**.
- Define the **RTP Port Range** for the media path with BT Global Services SIP Trunk, during testing this was left at the default values.

Media Interface: GSSCP_V9

Devices

GSSCP_V9

Add Media Interface

Name: External

IP Address: External (B1, VLAN 0)

Port Range: 35000 - 40000

Finish

The internal media interface is defined in the same way; the dialogue box is not shown:

- Select **Add** and enter details of the internal media interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal media interface.
- In the **IP Address** drop down menus, select the internal network interface and IP address.

The following screenshot shows details of the media interfaces:

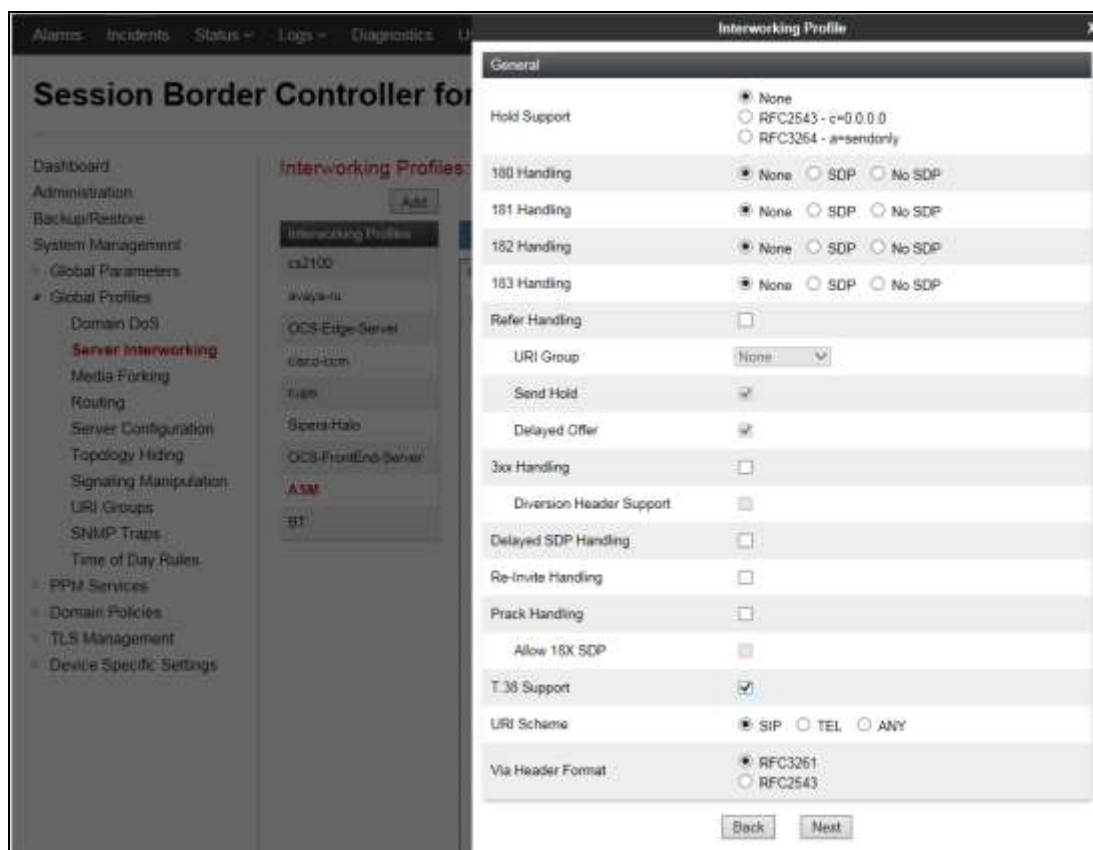


Name	Media IP Network	Port Range	
Internal	10.10.9.71 Internal (A1, VLAN 0)	35000 - 40000	Edit Delete
External	192.168.122.57 External (B1, VLAN 0)	35000 - 40000	Edit Delete

7.4. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, BT Global Services SIP Trunk is connected as the Trunk Server and the Session Manager is connected as the Call Server.

To define server interworking on the Avaya SBCE, navigate to **Global Profiles → Server Interworking** in the main menu on the left hand side. To define Server Interworking for the Session Manager, click on **Add** (not shown). A pop-up menu (not shown) is generated. In the **Name** field enter a descriptive name for the Session Manager and click **Next**.



Configuration of interworking includes Hold support, T.38 fax support and SIP extensions.

- In the General dialogue box shown in the previous screenshot, check the **T.38 Support** box. During testing, the rest of the parameters were left at default values.
- Click on **Next** and **Next** again to go through the next two dialogue boxes. During testing, these were left at default values.

In the final dialogue box, select **None** from the **Extensions** box. And click on **Finish**

To define Server Interworking for BT Global Services SIP Trunk, click on **Add** (not shown). A pop-up menu (not shown) is generated. In the **Name** field enter a descriptive name for the BT Global Services SIP Trunk and click **Next**.

In the dialogue box that appears, settings are as follows:

- Check the **Delayed SDP Handling** box. This inserts an SDP into the empty INVITE sent by the CS1000 when shuffling.
- Check the **T.38** box

Interworking Profile

General

Hold Support ☒ None ☐ RFC2543 - c=0.0.0.0 ☐ RFC3264 - a=sendonly

180 Handling ☒ None ☐ SDP ☐ No SDP

181 Handling ☒ None ☐ SDP ☐ No SDP

182 Handling ☒ None ☐ SDP ☐ No SDP

183 Handling ☒ None ☐ SDP ☐ No SDP

Refer Handling ☐

URI Group

Send Hold ☒

Delayed Offer ☒

3xx Handling ☐

Diversion Header Support ☐

Delayed SDP Handling ☒

Re-Invite Handling ☒

Prack Handling ☐

Allow 18X SDP ☐

T.38 Support ☒

URI Scheme ☒ SIP ☐ TEL ☐ ANY

Via Header Format ☒ RFC3261 ☐ RFC2543

- Click on **Next** and **Next** again to go through the next two dialogue boxes. During testing, these were left at default values.

Interworking Profile

All fields are optional

SIP Timers

Min-SE	<input type="text"/>	seconds, [90 - 86400]
Init Timer	<input type="text"/>	milliseconds, [50 - 1000]
Max Timer	<input type="text"/>	milliseconds, [200 - 8000]
Trans Expire	<input type="text"/>	seconds, [1 - 64]
Invite Expire	<input type="text"/>	seconds, [180 - 300]

Back
Next

Interworking Profile

Privacy

Privacy Enabled	<input type="checkbox"/>
User Name	<input type="text"/>
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	<input type="text"/>

Back
Next

In the final dialogue box, select **None** from the **Extensions** box and click on **Finish**.

Interworking Profile

Record Routes

☐ None
☐ Single Side
☒ Both Sides
☐ Dialog-Initiate Only (Single Side)
☐ Dialog-Initiate Only (Both Sides)

Include End Point IP for Context Lookup
☐

Extensions

None

Diversion Manipulation
☐

Diversion Condition

None

Diversion Header URI

Has Remote SBC
☒

Route Response on Via Port
☐

DTMF

DTMF Support

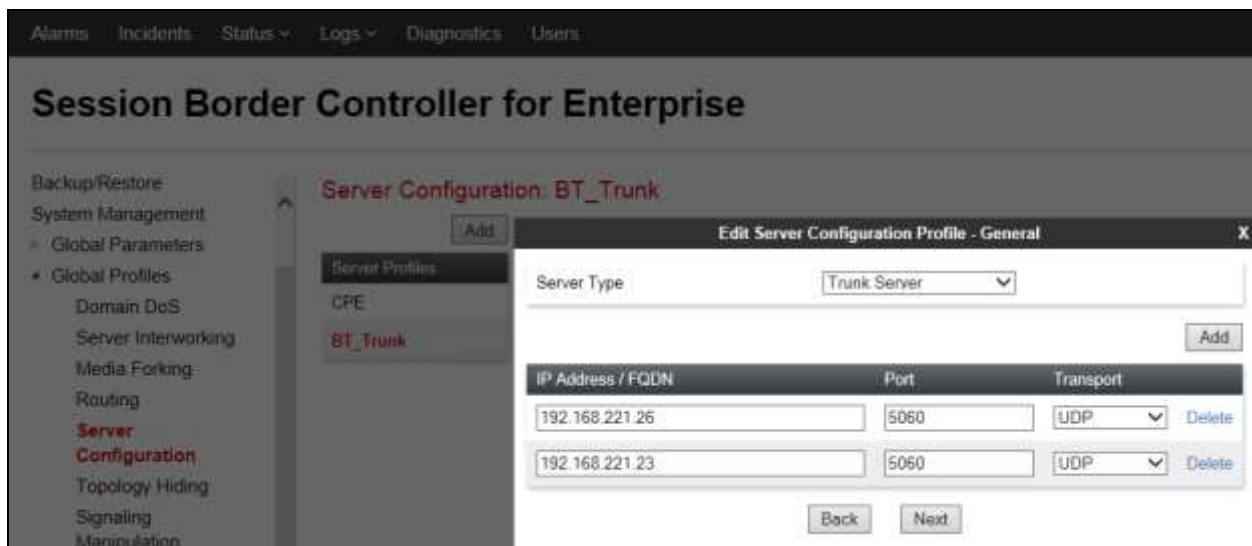
☒ None
☐ SIP NOTIFY
☐ SIP INFO

Back
Finish

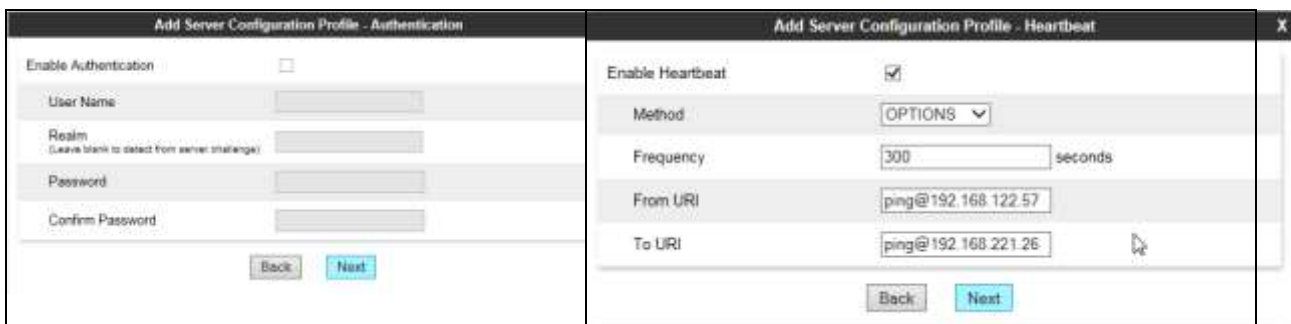
7.5. Define Servers

A server definition is required for each server connected to the Avaya SBCE. In this case, BT Global Services SIP Trunk is connected as the Trunk Server and the Session Manager is connected as the Call Server. To define the BT Global Services SIP Trunk Server, navigate to **Global Profiles → Server Configuration** in the main menu on the left hand side. Click on **Add** and enter an appropriate name in the pop-up menu (not shown). Click on **Next** and enter details in the dialogue box.

- In the **Server Type** drop down menu, select **Trunk Server**.
- Click on **Add** to enter an IP address
- In the **IP Addresses / FQDN** box, type the first BT Global Services network SBC interface address.
- In the **Port** box, enter the port to be used for the SIP Trunk. This was left blank during testing which defaults to 5060 when UDP is used for transport.
- In the **Transport** drop down menu, select **UDP**.
- Click on **Add** and repeat the above for the alternative network SBC. Click on **Next**.



- Click on **Next** and **Next** again to go through the next two dialogue boxes. During testing, these were left at default values.



Note: Although the Heartbeat configuration was left at default values for most of the testing, the screenshot shows values used when verifying the SIP Trunk. For details, refer to **Section 9**.

The final dialogue box is the **Advanced** settings:

- In the **Interworking Profile** drop down menu, select the **Interworking Profile** for the BT Global Services SIP Trunk defined in **Section 7.4**.
- Click **Finish**.

BT Global Services use two network SBCs for resilience. A separate Trunk Server configuration is required for the alternative SBCs. Repeat the above process using the IP address of the alternative SBC, in the test environment this was 192.168.221.23.

Use the process above to define the Call Server configuration for the Session Manager if not already defined.

- Ensure that **Call Server** is selected in the **Server Type** drop down menu in the **General** dialogue box (not shown).
- Ensure that the Interworking Profile defined for the Session Manager in **Section 7.4** is selected in the **Interworking Profile** drop down menu in the Advanced dialogue box (not shown).

The following screenshot shows the completed entry for the Session Manager:

IP Address / FQDN	Port	Transport
10.10.9.31	5060	TCP

7.6. Define Routing

Routing information is required for routing to BT Global SIP Trunk on the external side and the Session Manager on the internal side. The IP addresses and ports defined here will be used as the destination addresses for signalling.

To define routing to BT Global Service SIP Trunk, navigate to **Global Profiles** → **Routing** in the main menu on the left hand side. Click on **Add** and enter an appropriate name in the dialogue box (not shown), click on Next and enter details for the Routing Profile:

- In the **Load Balancing** drop down menu, select the method of load balancing required. During testing this was set to **Priority**. If an even distribution across the network SBCs is required, **Round Robin** could be used.
- Click on **Add** to specify an IP address for the first network SBC.
- Assign a priority in the **Priority / Weight** field
- Select the Server Configuration defined in **Section 7.5** in the **Server Configuration** drop down menu. This automatically populates the **Next Hop Address** field
- Repeat for the alternative network SBC. Click **Finish**.

The screenshot shows the 'Routing Profile' configuration window for the WAN profile. The 'Load Balancing' is set to 'Priority'. The 'Transport' is set to 'None'. The 'Next Hop In-Dialog' checkbox is unchecked. The 'Next Hop Priority' checkbox is checked. The 'Ignore Route Header' checkbox is unchecked. The table below shows two entries for 'BT_Trunk' with 'Next Hop Address' fields containing '192.168.221.26:5060 (UDP)' and '192.168.221.23:5060 (UDP)'. The 'Add', 'Back', and 'Finish' buttons are at the bottom.

Repeat the above process for the Routing Profile for the Session Manager:

The screenshot shows the 'Profile : LAN - Edit Rule' configuration window. The 'Load Balancing' is set to 'Priority'. The 'Transport' is set to 'None'. The 'Next Hop In-Dialog' checkbox is unchecked. The 'Next Hop Priority' checkbox is checked. The 'Ignore Route Header' checkbox is unchecked. The table below shows one entry for 'CPE' with 'Next Hop Address' field containing '10.10.9.31:5060 (TCP)'. The 'Add' and 'Finish' buttons are at the bottom.

7.7. 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 or external interfaces. Topology hiding has the advantage of presenting single Via and Record-Route headers externally where multiple headers may be received from the enterprise, particularly from the Session Manager. In some cases where Topology Hiding can't be applied, in particular the Contact header, IP addresses are translated to the Avaya SBCE external addresses using NAT.

To define Topology Hiding for BT Global Service SIP Trunk, navigate to **Global Profiles** → **Topology Hiding** in the main 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 BT Global Service SIP Trunk and click **Next**.
- Click on **Add Header** and select from the **Header** drop down menu.
- Select **IP** or **IP/Domain** from the **Criteria** drop down menu depending on requirements.
- Leave the **Replace Action** at the default value of **Auto** unless a specific domain name is required. In this case, select **Overwrite** and define a domain name in the **Overwrite Value** field.
- Topology hiding was defined for all headers where the function is available.

Topology Hiding Profiles: BT

Buttons: Add, Rename, Clone, Delete

Click here to add a description

Topology Hiding

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

Edit

To define Topology hiding for the Session Manager, follow the same process. This can be simplified by cloning the profile defined for BT Global Service SIP Trunk. Do this by highlighting the profile defined for the Session Manager and clicking on **Clone**.

Enter an appropriate name for the Session Manager and click on Next. Make any changes where required, in the test environment the settings were left at the same values.

Topology Hiding Profiles: ASM

Add

Topology Hiding Profiles

default

cisco_th_profile

ASM

BT

Click here to add a description

Topology Hiding

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

Edit

Rename

Clone

Delete

7.8. Server Flows

Server Flows combine the previously defined profiles into two End Point Server Flows, one for BT Global Services SIP Trunk and another for the Session Manager. This configuration ties all the previously entered information together so that calls can be routed from the Session Manager to BT Global Services SIP Trunk and vice versa.

To define a Server Flow for the BT Global Services SIP Trunk, 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 BT Global Services SIP Trunk, in the test environment **BT_Trunk** was used.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the BT SIP Trunk is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for BT SIP Trunk is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.3**. This is the interface that media bound for BT SIP Trunk is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the Session Manager defined in **Section 7.6**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the BT SIP Trunk defined in **Section 7.7** and click **Finish**.

Edit Flow: BT_Trunk	
Flow Name	BT_Trunk
Server Configuration	BT_Trunk
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Internal
Signaling Interface	External
Media Interface	External
End Point Policy Group	default-low
Routing Profile	LAN
Topology Hiding Profile	BT
Signaling Manipulation Script	None
Remote Branch Office	Any
Finish	

To define a Server Flow for the 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 the Session Manager, in the test environment **CPE** was used.
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the Session Manager is received on.
- In the **Signaling Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the Session Manager is sent on.
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.3**. This is the interface that media bound for the Session Manager is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of BT SIP Trunk defined in **Section 7.6**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Session Manager defined in **Section 7.7** and click **Finish**.

The screenshot shows a dialog box titled "Edit Flow: CPE" with a close button (X) in the top right corner. The dialog contains the following fields and values:

Field	Value
Flow Name	CPE
Server Configuration	CPE
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	External
Signaling Interface	Internal
Media Interface	Internal
End Point Policy Group	default-low
Routing Profile	WAN
Topology Hiding Profile	ASM
Signaling Manipulation Script	None
Remote Branch Office	Any

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

The information for all Server Flows is shown on a single screen on the Avaya SBCE.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo on the right. A left-hand navigation menu lists various system management and configuration options, with "End Point Flows" highlighted in red. The main content area is titled "End Point Flows: GSSCP_V9" and features two tabs: "Subscriber Flows" and "Server Flows". The "Server Flows" tab is active, showing a table of server configurations. Above the table is a blue bar with the text "Hover over a row to see its description" and an "Add" button. The table is divided into two sections: "Server Configuration: BT_Trunk" and "Server Configuration: CPE". Each section contains a table with columns for Priority, Flow Name, URI Group, Received Interface, Signaling Interface, End Point Policy Group, and Routing Profile. The "BT_Trunk" section has one row with Priority 1, Flow Name BT_Trunk, URI Group *, Received Interface Internal, Signaling Interface External, End Point Policy Group default-low, and Routing Profile LAN. The "CPE" section has one row with Priority 1, Flow Name CPE, URI Group *, Received Interface External, Signaling Interface Internal, End Point Policy Group default-low, and Routing Profile WAN. Each row has "View", "Clone", "Edit", and "Delete" links.

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	BT_Trunk	*	Internal	External	default-low	LAN	View Clone Edit Delete

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	CPE	*	External	Internal	default-low	WAN	View Clone Edit Delete

8. Configure BT SIP Trunk Equipment

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

9. Verification Steps

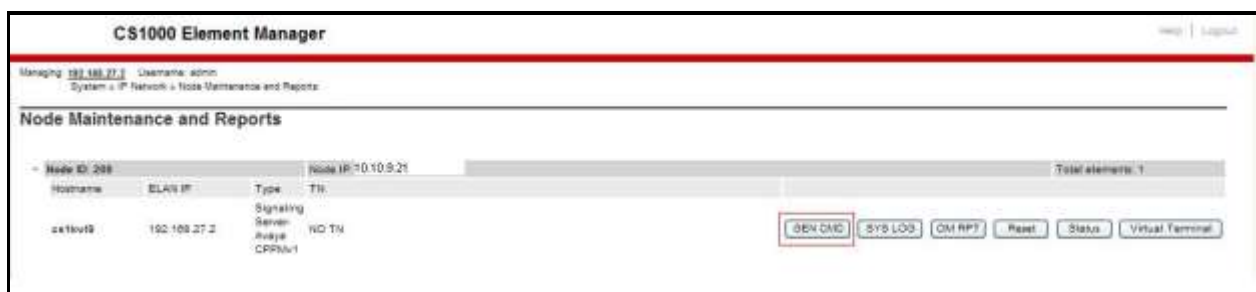
This section provides verification steps that may be performed in the field to verify that the solution is configured properly.

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-Analysis CPPMx1

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

STATUS Status: Active

Primary Proxy IP address: 10.10.9.25
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: 10.10.9.25
Primary Proxy2 port: 5060
Primary Proxy2 Transport: TCP
Active Proxy: Primary: :Registered 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-Analysis CPPMx1

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
IPv4 Endpoints							
6003	6003	100-00-03-03	1	0	0x51e2d0		SIP Line
6002	6002	100-00-03-02	1	0	0x51e158		SIP Line
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-Analysis CPPMx1

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

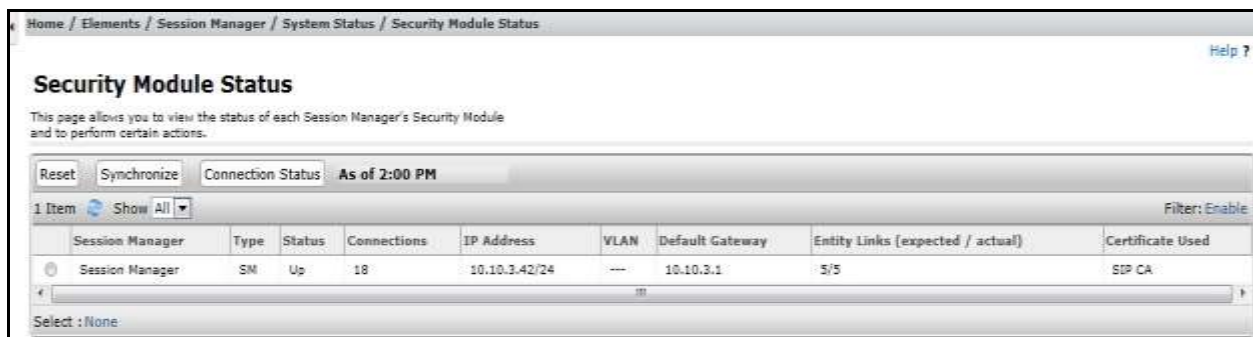
Navigate to **Elements → Session Manager → Dashboard** (not shown) to verify the overall system status for Session Manager. Specifically, verify the status of the following fields as shown below.



The screenshot shows the 'Session Manager Dashboard' with a breadcrumb trail: Home / Elements / Session Manager / Dashboard. The page title is 'Session Manager Dashboard' with a subtitle: 'This page provides the overall status and health summary of each administered Session Manager.' Below the title is a section 'Session Manager Instances' with filters for 'Service State' (dropdown), 'Shutdown System' (dropdown), and 'As of 1:58 PM'. A table lists the instances. The first instance is 'Session Manager' with a 'Type' of 'Core'. The 'Status' column shows 'Up' with a green checkmark. Other columns include 'Tests Pass' (0/0/0), 'Alarms' (Up), 'Security Module' (Accept New Service), 'Service State' (0/5), 'Active Call Count' (0), 'Registrations' (3/3), 'Data Replication' (green checkmark), 'User Data Storage Status' (green checkmark), 'License Mode' (Normal), and 'Version' (7.0.0.0.700007).

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
Session Manager	Core	0/0/0	Up	Accept New Service	0/5	0	3/3				Normal	7.0.0.0.700007

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. The page title is 'Security Module Status' with a subtitle: 'This page allows you to view the status of each Session Manager's Security Module and to perform certain actions.' Below the title are buttons for 'Reset', 'Synchronize', and 'Connection Status', and a timestamp 'As of 2:00 PM'. A table lists the security module status. The first entry is 'Session Manager' with a 'Type' of 'SM'. The 'Status' column shows 'Up'. Other columns include 'Connections' (18), 'IP Address' (10.10.3.42/24), 'VLAN' (---), 'Default Gateway' (10.10.3.1), 'Entity Links (expected / actual)' (5/5), and 'Certificate Used' (SIP CA).

Session Manager	Type	Status	Connections	IP Address	VLAN	Default Gateway	Entity Links (expected / actual)	Certificate Used
Session Manager	SM	Up	18	10.10.3.42/24	---	10.10.3.1	5/5	SIP 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' tab is selected and expanded, showing the following configuration fields:

- SIP Entity Name:** Session Manager
- Description:** (empty field)
- Management Access Point Host Name/IP:** 10.10.3.42
- 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 the following fields and values:

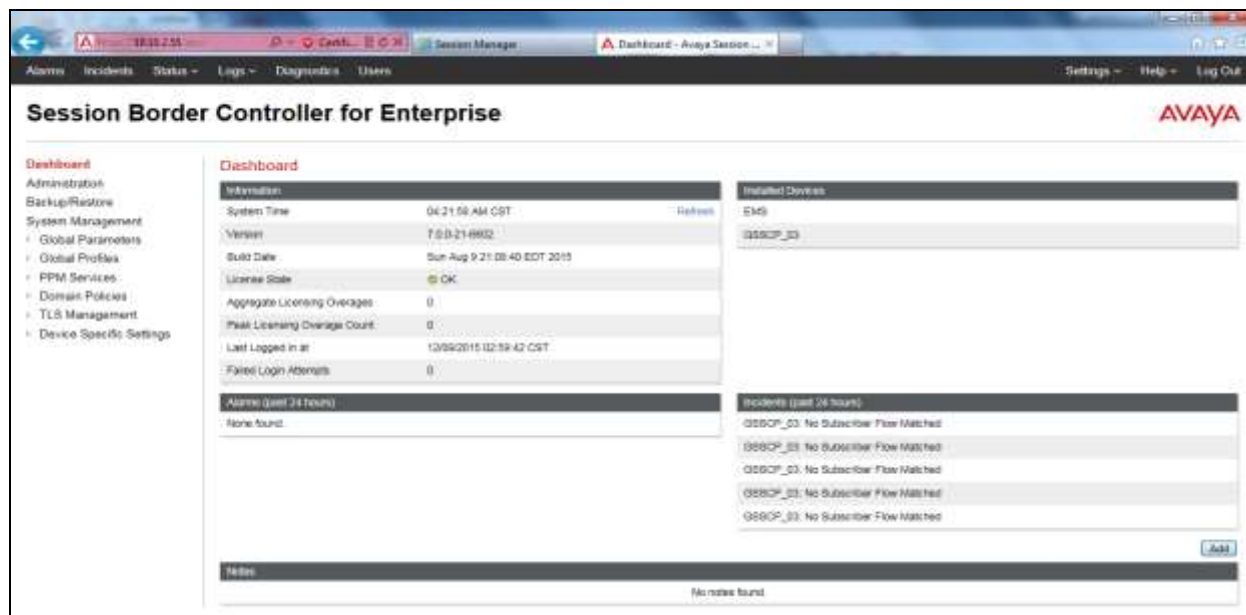
Field	Value
SIP Entity IP Address	10.10.3.42
Network Mask	255.255.255.0
Default Gateway	10.10.3.1
Call Control PHB	46
*SIP Firewall Configuration	SM 6.3.8.0

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


Incident Viewer						
AVAYA						
Device [All] Category [All] Clear Filters Refresh Generate Report						
Displaying results 1 to 15 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	724827988956473	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



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



File Name	File Size (bytes)	Last Modified	
Test_20151209042456.pcap	0	December 9, 2015 4:24:56 AM CST	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 BT Global Services network.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Communication Server R7.65, Avaya Aura® Session Manager R7.0 and Avaya Session Border Controller for Enterprise R7.0 to BT Global Services SIP Trunk. BT Global Services SIP Trunk 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.