



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Communication Server 1000 R7.65, Avaya Aura® Session Manager R7.1 and Avaya Session Border Controller for Enterprise R7.2 to support Sunrise Business Voice Direct SIP Trunk - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Sunrise Business Voice Direct 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.

The Sunrise Business Voice Direct SIP Trunk provides PSTN access via a SIP trunk connected to the Sunrise Voice Over Internet Protocol (VoIP) network as an alternative to legacy Analogue or Digital trunks. Sunrise is a member of the Avaya 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 Sunrise Business Voice Direct 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 R7.1 (Session Manager) and Avaya Session Border Controller for Enterprise R7.2 (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 Sunrise Business Voice Direct 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 CS1000, Session Manager and Avaya SBCE. The enterprise site was configured to connect to Sunrise Business Voice Direct SIP Trunk.

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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between Avaya systems and the Sunrise SIP trunk does not include the use of any specific encryption features.

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from PSTN phones using the SIP trunk provided by Sunrise, calls made to SIP, UNISim, Digital and Analog telephones at the enterprise.
- All inbound PSTN calls were routed to the enterprise across the SIP trunk to Sunrise.
- Outgoing calls from the enterprise site completed via Sunrise's SIP trunk to PSTN destinations, calls made from SIP, UNISim, Digital and Analog telephones.
- All outbound PSTN calls were routed from the enterprise across the SIP trunk to Sunrise.
- Inbound and outbound PSTN calls to/from Avaya 2050PC IP softphone.
- Calls using the G.711A and G722 codecs.
- Fax calls to/from a group 3 fax machine to a PSTN-connected fax machine using G.711 pass-through transmission.
- Caller ID Presentation and Caller ID Restriction.
- DTMF transmission using RFC 2833 with successful Voice Mail/ACD navigation for inbound and outbound calls.
- User features such as hold and resume, transfer and conference.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Off-net call forwarding and mobile twinning.
- Transmission and response of SIP OPTIONS messages sent by Sunrise's SIP trunk requiring Avaya response and sent by Avaya requiring Sunrise's response.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for Sunrise Business Voice Direct SIP Trunk with the following observations:

- G.729 codec is not supported by Sunrise and therefore was not tested.
- T.38 fax transmission was not tested.
- All unwanted MIME was stripped on outbound calls using the Adaptation Module in Session Manager in **Section 6.4**.
- No inbound toll-free numbers were tested, however routing of inbound DDI numbers and the relevant number translation was successfully tested.
- Access to Emergency Services was not tested as no test call had been booked with the Emergency Services Operator.

2.3. Support

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

For technical support on the Sunrise Business Voice Direct SIP Trunk described in these Application Notes please contact Sunrise technical support 0800 55 00 20.

3. Reference Configuration

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

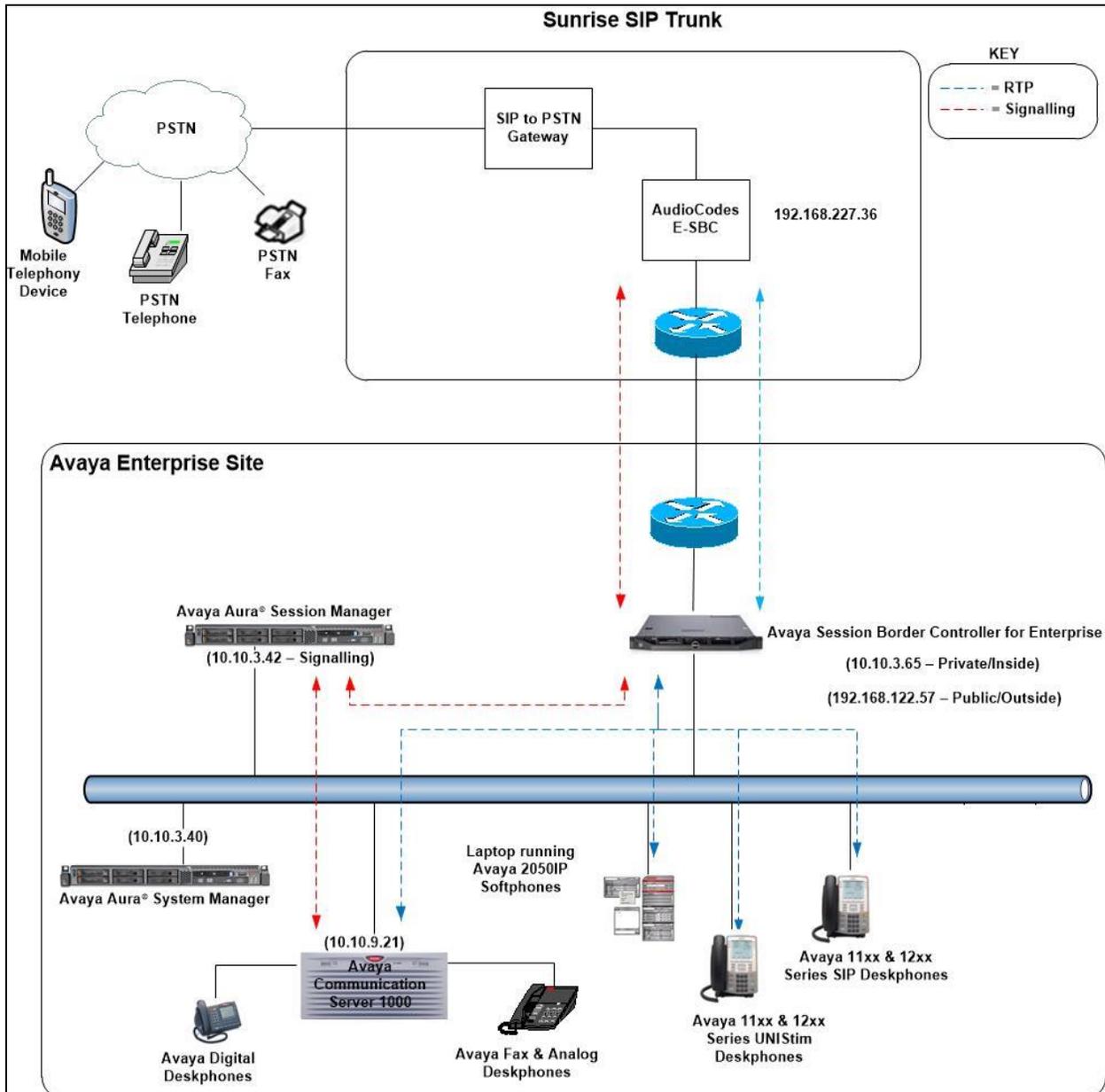


Figure 1: Test Setup Sunrise SIP Trunk to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® System Manager	7.1.2.0. Build No. – 7.1.0.0.1125193 Software Update Revision No: 7.1.2.0.057353 FP2
Avaya Aura® Session Manager	7.1.2.0.712004
Avaya Communication Server 1000	Avaya Communication Server 1000 R7.6 Version 7.65.P – Service Pack 9 Deplist: CPL_X21_07_65P All CS1000 patches listed in Appendix A
Avaya Communication Server 1000 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	7.2.1-05-14222
Avaya 1140e and 1230 UNISlim Telephones	FW: 0625C8A
Avaya 1140e and 1230 SIP Telephones	FW: 04.10.18.00.bin
Avaya 2050PC	Release 4.3.0081
Avaya Analog Telephone	N/A
Avaya M3904 Digital Telephone	N/A
Sunrise	
IMS Switch	20180601
AudioCodes E-SBC	7.20A.158.056

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 Sunrise Business Voice Direct SIP Trunk. Incoming PSTN calls from the Sunrise Business Voice Direct 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 Sunrise Business Voice Direct SIP Trunk service.

Specific CS1000 configuration was performed using Element Manager and the system terminal interface. The general installation of the CS1000, System Manager, Session Manager and Avaya SBCE is presumed to have been previously completed and is not discussed here. Configuration details will be provided as required to draw attention to changes in default system configurations.

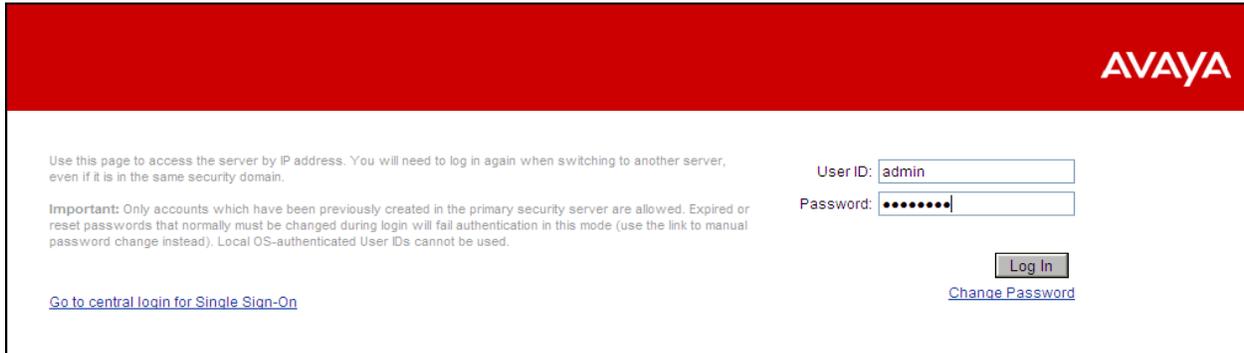
5.1. Logging into the Avaya Communication Server 1000

Configuration on the CS1000 will be performed by using both SSH Putty session and Avaya Unified Communications Management GUI.

Log in using SSH to the ELAN IP address of the Call Server with a username containing the correct privileges. Once logged in type **cconsole**, 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.

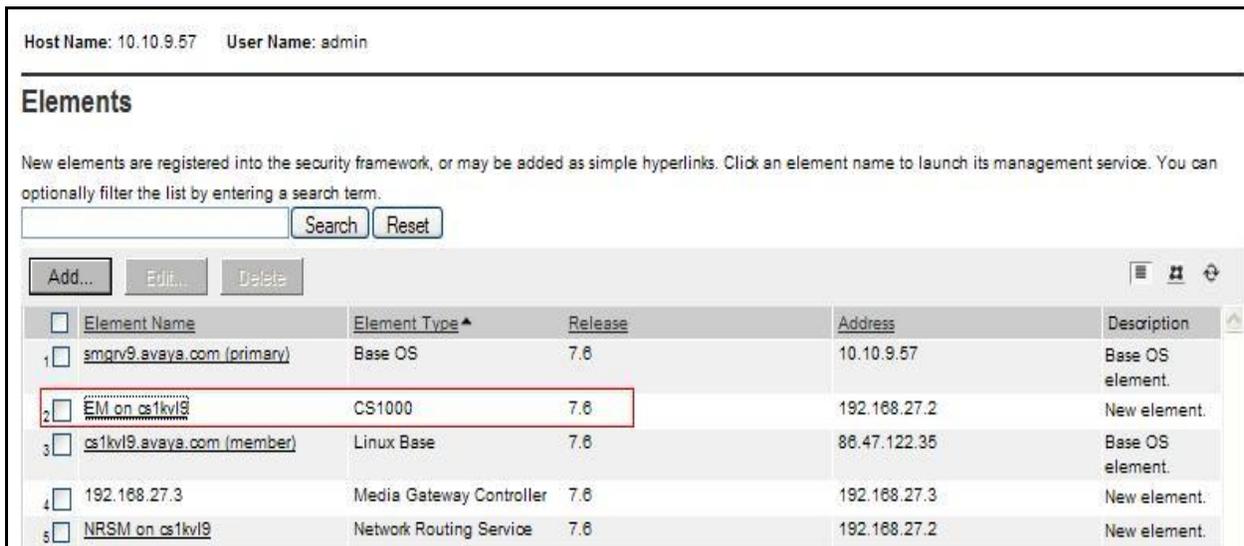
Log in using the web based Avaya Unified Communications Management GUI. Avaya Unified Communications Management GUI may be launched directly via <http://<ipaddress>> where the relevant <ipaddress> is the TLAN IP address of the CS1000. Avaya Unified Communications Management can also be implemented on System Manager.

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



The screenshot shows the Avaya login interface. At the top right is the Avaya logo. Below it, there is a message: "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." Below this is an "Important" note: "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." There is a link: "Go to central login for Single Sign-On". On the right side, there are input fields for "User ID:" (containing "admin") and "Password:" (containing "*****"). Below these fields are "Log In" and "Change Password" buttons.

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**.



The screenshot shows the "Elements" page in the Avaya Unified Communications Management interface. At the top, it displays "Host Name: 10.10.9.57" and "User Name: admin". Below the title "Elements", there is a message: "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." There is a search input field with "Search" and "Reset" buttons. Below the search field are "Add...", "Edit...", and "Delete" buttons. The main content is a table with the following data:

<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 Sunrise 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.

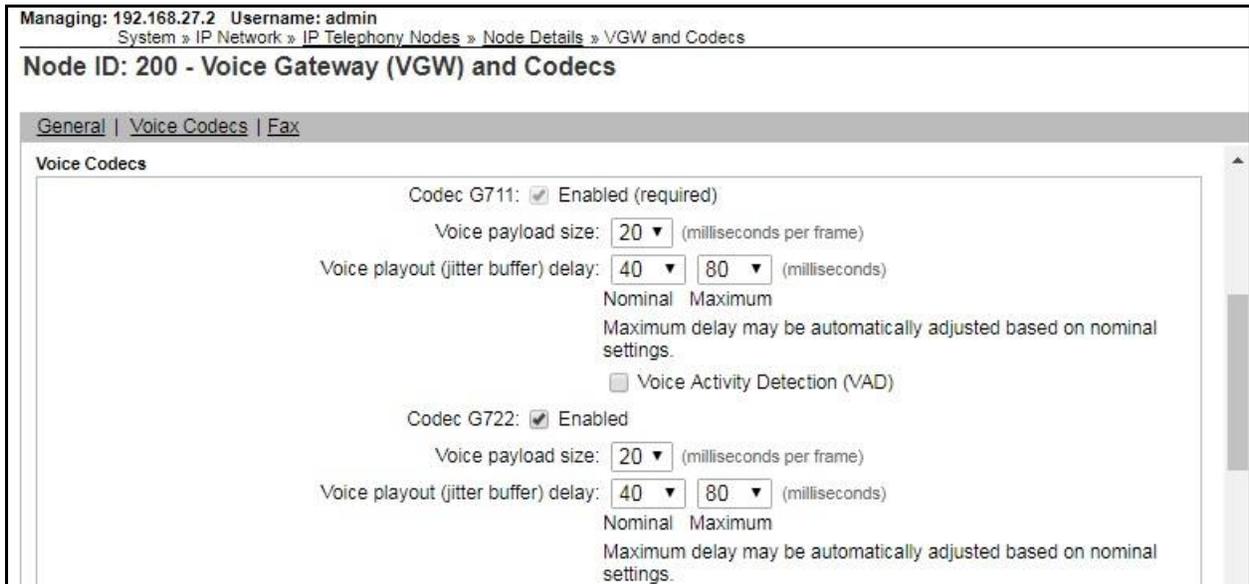
```
REQ: prt
TYPE: net
TYPE NET_DATA
CUST 0

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

Sunrise's SIP Trunk supports G.711A and G.722 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 both G.711 and G.722 codec settings. The following screenshot shows the G.711 and G.722 codec settings.



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: <input type="text" value="200"/> * (0-9999)	TLAN address type: <input checked="" type="radio"/> IPv4 only <input type="radio"/> IPv4 and IPv6
Call server IP address: <input type="text" value="192.168.27.2"/> *	
Embedded LAN (ELAN)	Telephony LAN (TLAN)
Gateway IP address: <input type="text" value="192.168.27.1"/> *	Node IPv4 address: <input type="text" value="10.10.9.21"/> *
Subnet mask: <input type="text" value="255.255.255.0"/> *	Subnet mask: <input type="text" value="255.255.255.0"/> *
	Node IPv6 address: <input type="text"/>

IP Telephony Node Properties	Applications (click to edit configuration)
<ul style="list-style-type: none">• Voice Gateway (VGW) and Codecs• Quality of Service (QoS)• LAN• SNTP• Numbering Zones• MCDN Alternative Routing Treatment (MALT) Causes	<ul style="list-style-type: none">• SIP Line• Terminal Proxy Server (TPS)• Gateway (SIPGw)• Personal Directories (PD)• Presence Publisher• IP Media Services

* Required Value.

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:
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: (1 - 65535)

Transport protocol: ▼

Options: Support registration
 Primary CDS proxy

Secondary TLAN IP address:
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: (1 - 65535)

SIP URI Map:

Public E.164 domain names		Private domain names	
National:	<input type="text"/>	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"/>

5.5. Configure Bandwidth Zones

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

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

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

Bandwidth Zones

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

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

5.6. Configure Incoming Digit Conversion Table

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

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

0 Configuration

Regular IDC tree
Send calling party DID disabled

Add... Delete IDC Delete IDC tree Refresh

Incoming Digits *	Converted Digits	CPND Name	CPND language
1 416 60	6000		
2 416 61	6001		
3 416 62	6002		
4 416 63	6005		
5 416 64	6004		
6 416 65	6003		

5.7. Configure SIP Trunks

CS1000 virtual trunks will be used for all inbound and outbound PSTN calls to the Sunrise Business Voice Direct 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.

<pre> 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 </pre>	<pre> 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 </pre>	<pre> 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 ATTR NO TRRL NO SGRP 0 ARDN NO CTBL 0 AACR NO </pre>
---	---	--

Next, configure virtual trunk members using the CS1000 system terminal and **Overlay 14**. Configure sufficient trunk members to carry both incoming and outgoing PSTN calls. The following example shows a single SIP trunk member configuration. Load **Overlay 14** at the system terminal and type **new X**, where X is the required number of trunks. Continue entering data until the overlay exits. The **RTMB** value is a combination of the **ROUT** value entered in the previous step and the first trunk member (usually 1). The remaining highlighted values are important for correct SIP trunk operation.

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

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

```

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

```

Configure a Route List Block (RLB) in overlay 86. Load **Overlay 86** at the system terminal and type **new**. The following example shows the values used. The value for **ROUT** is the same as previously entered in overlay 16. The **RLI** value is unique to each RLB and **DMI** value is set to 10 as previously configured in the Digit Manipulation Block (DGT) in **Overlay 86**.

```

Overlay 86
CUST 0
FEAT rlb
RLI 10
ELC NO
ENTR 0
LTER NO
ROUT 1
TOD 0 ON 1 ON 2 ON 3 ON
    4 ON 5 ON 6 ON 7 ON
VNS NO
SCNV NO
CNV NO
EXP NO
FRL 0
DMI 10
CTBL 0
ISDM 0
FCI 0
FSNI 0
BNE NO
DORG NO
SBOC NRR
PROU 1
IDBB DBD
IOHQ NO
OHQ NO
CBQ NO
ISET 0
NALT 5
MFRL 0
OVLL 0

```

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

5.8. 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 RCB
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 CCB
D RTDD RBDD RBHD PGND OCB
D 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 HBTB AHA IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
DRDD EXR0
USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
FDSD NOVD CDMR PRED RECA MCDD T87D SBMD PKCH CROD CROD
CPND LANG ENG
RCO 0
HUNT
PLEV 02
PUID
DANI NO
SPID NONE
AST
IAPG 1
AACS
ACQ
ASID
SFNB
SFRB
USFB
CALB
FCTB
ITNA NO
DGRP
PRI 01
MLWU_LANG 0
```

---continued on next page---

---continued from previous page---

MLNG ENG

DNDR 0

KEY 00 MCR 6066 0 MARP

CPND

CPND_LANG ROMAN

NAME Digital Set

XPLN 10

DISPLAY_FMT FIRST, LAST

01 MCR 6066 0

CPND

CPND_LANG ROMAN

NAME Digital Set

XPLN 10

DISPLAY_FMT FIRST, LAST

02 DSP

03 MSB

04

05

06

07

08

09

10

11

12

13

14

15

16

17 TRN

18 AO6

19 CFW 16

20 RGA

21 PRK

22 RNP

23

24 PRS

25 CHG

26 CPN

27 CLT

28 RLT

29

30

31

Analog telephones are also configured using overlay 20; the following example shows an analog port configured for 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 **FAXD** and **MPTA** configure the port for G.711 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 CCB D BNRD OCB D RTDD RBDD RBHD FAXA CNUD CNAD PGND FTTC
FDSD NOVD CDMR PRED MCDD T87D SBMD PKCH MPTD
PLEV 02
PUID
AACS NO
MLWU_LANG 0
FTR DCFW 4
```

5.9. Configure the SIP Line Gateway Service

SIP terminal operation requires the CS1000 node to be configured as a SIP Line Gateway (SLG) before SIP telephones can be configured. Prior to configuring the SIP Line node properties, the SIP Line service must be enabled in the customer data block. Use the CS1000 system terminal and overlay 15 to activate SIP Line services (SLS_DATA), as in the following example where **SIPL_ON** is set to **YES**.

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

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

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

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

Node ID: 200 - SIP Line Configuration Details

General | SIP Line Gateway Settings | SIP Line Gateway Service

SIP Line Gateway Application: Enable gateway service on this node

General	Virtual Trunk Network Health Monitor
SIP domain name: <input type="text" value="avaya.com"/> *	<input type="checkbox"/> Monitor IP addresses (listed below)
SLG endpoint name: <input type="text" value="cs1kv19"/>	Information will be captured for the IP addresses listed below.
SLG Group ID: <input type="text"/>	Monitor IP: <input type="text"/> <input type="button" value="Add"/>
SLG Local Sip port: <input type="text" value="5070"/> (1 - 65535)	Monitor addresses: <input type="text"/> <input type="button" value="Remove"/>
SLG Local Tls port: <input type="text" value="5071"/> (1 - 65535)	

5.10. Configure SIP Line Telephones

When SIP Line service configuration is completed, use the CS1000 system terminal and **Overlay 20** to add a Universal Extension (UEXT). See the following example of a SIP Line extension. The value for **UXTY** must be **SIPL**. This example is for an Avaya SIP telephone, so the value for **SIPN** is 1. The **SIPU** value is the username, **SCPW** is the logon password and these values are required to register the SIP telephone to the SLG. The value for **CFG_ZONE** is the value used in **Section 5.5** for IP and SIP Telephones. A unique telephone number is entered for value **KEY 00**. The value for **KEY 01** is comprised of the **UAPR** (set in **Section 5.9**) value and the telephone number used in **KEY 00**.

Load Overlay 20 – SIP Telephone Configuration

```
DES SIPD
TN 100 0 03 3 VIRTUAL
TYPE UEXT
CDEN 8D
CTYP XDLC
CUST 0
UXTY SIPL
MCCL YES
SIPN 1
SIP3 0
FMCL 0
TLSV 0
SIPU 6002
NDID 200
SUPR NO
SUBR DFLT MWI RGA CWI MSB
UXID
NUID
NHTN
CFG_ZONE 00002
CUR_ZONE 00002
ERL 0
ECL 0
VSIT NO
FDN
TGAR 0
LDN NO
NCOS 0
SGRP 0
RNPG 0
SCI 0
SSU
XLST
SCPW 1234
SFLT NO
CAC_MFC 0
CLS UNR FBD WTA LPR MTD FNA HTA TDD HFD CRPD
MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LND CNDA
CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
ICDD CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDA CFXA ARHD FITD CLTD ASCD
CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD

---continued on next page---
---continued from previous page---
```

```

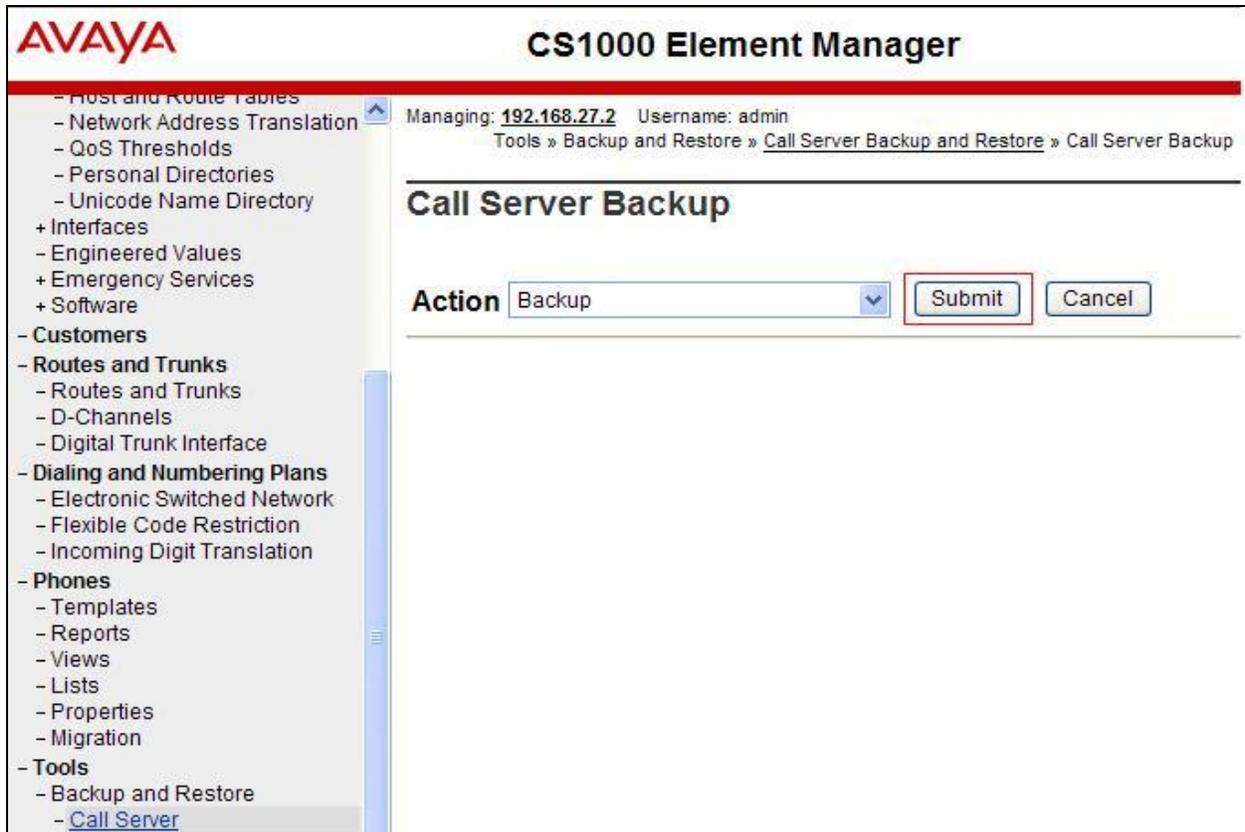
UDI RCC HBTD AHA IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
DRDD EXR0
USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD ELMD MSNV FRA PKCH MWTD DVLD
CROD CROD
CPND_LANG ENG
RCO 0
HUNT
LHK 0
PLEV 02
PUID
DANI NO
AST
IAPG 0 *

AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY 00 MCR 6002 0      MARP
      CPND
      CPND_LANG ROMAN
      NAME Sigma 1140
      XPLN 11
      DISPLAY_FMT FIRST, LAST*
01 HOT U 116002 MARP 0
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16
17 TRN
18 AO6
19 CFW 16
20 RGA
21 PRK
22 RNP
23 *
24 PRS
25 CHG
26 CPN
27
28
29
30
31

```

5.11. Save Configuration

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



The 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.



6. Configuring Avaya Aura® Session Manager

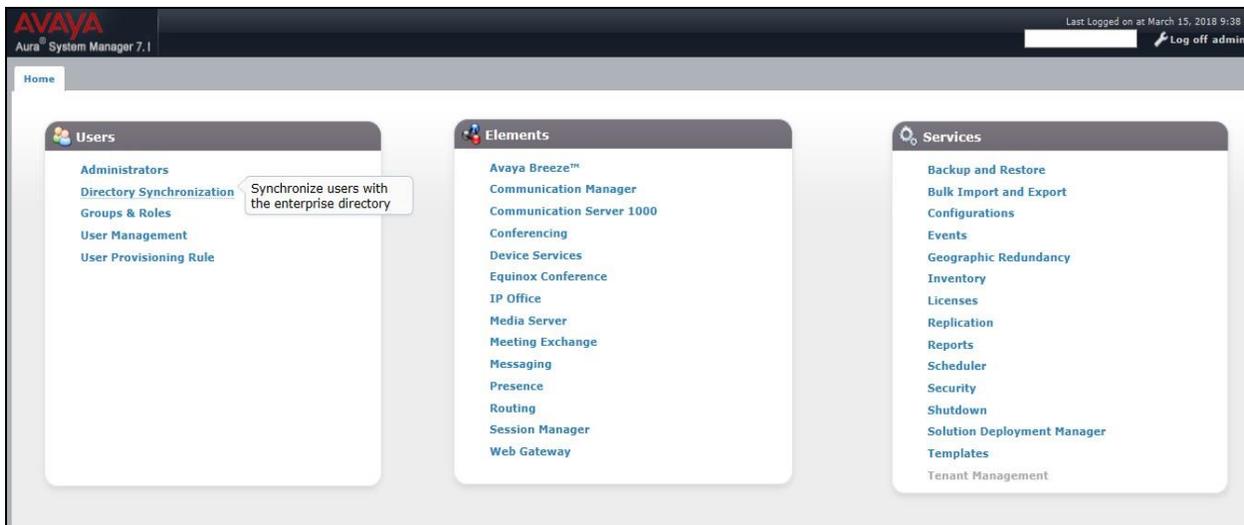
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- 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.

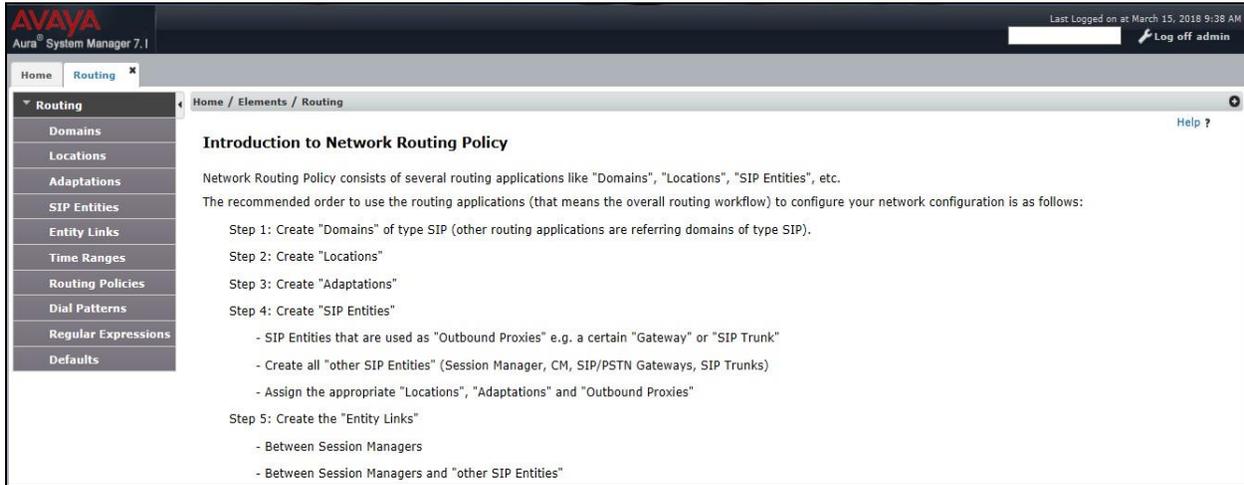
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

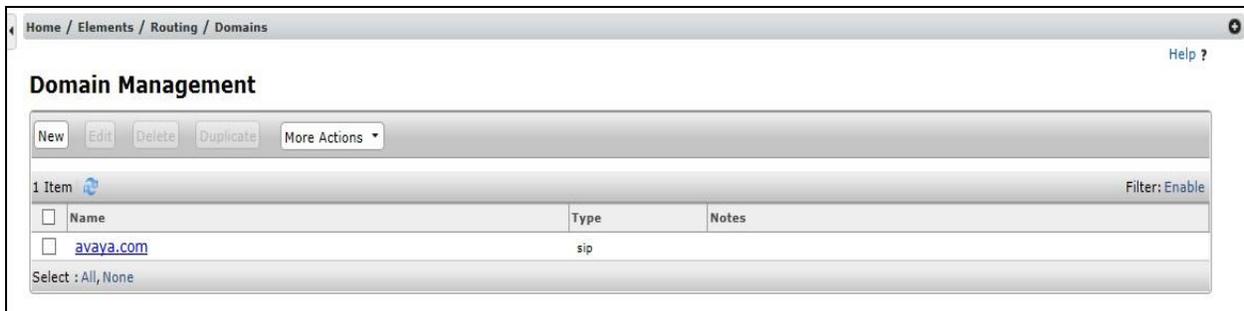


6.2. Administer SIP Domain

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 shows a web-based configuration interface for 'Locations'. The top navigation bar indicates the path: Home / Elements / Routing / Locations. The main section is titled 'Location Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' section, the 'Name' field is populated with 'SMGR_7'. Below this, there are sections for 'Dial Plan Transparency in Survivable Mode' (with an 'Enabled' checkbox) and 'Overall Managed Bandwidth' (with fields for 'Managed Bandwidth Units', 'Total Bandwidth', and 'Multimedia Bandwidth'). At the bottom of this section, there is a checkbox for 'Audio Calls Can Take Multimedia Bandwidth'. The 'Location Pattern' section is expanded, showing a table with 3 items. The table has columns for 'IP Address Pattern' and 'Notes'. The patterns listed are '*10.10.3.*', '*10.10.4.*', and '*10.10.9.*'. The interface also includes 'Add' and 'Remove' buttons, a 'Filter: Enable' option, and 'Commit' and 'Cancel' buttons at the bottom.

6.4. Administer Adaptations

Adaptations can be used to modify the called and calling party numbers to meet the requirements of the service. The called party number present in the SIP INVITE Request URI is modified by the **Digit Conversion** in the Adaptation. In order to improve interoperability with third party elements, Session Manager 7.1 incorporates the ability to use Adaptation modules to remove specific SIP headers that are either Avaya proprietary or deemed excessive/unnecessary for non-Avaya elements

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

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

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

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

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

Home / Elements / Routing / Adaptations

Adaptation Details Commit Cancel Help ?

General

* **Adaptation Name:**

* **Module Name:**

Module Parameter Type:

Add		Remove
<input type="checkbox"/>	Name	Value
<input type="checkbox"/>	eRHdrs	AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-
<input type="checkbox"/>	fromto	true
<input type="checkbox"/>	MIME	no

Select : All, None

Egress URI Parameters:

Notes:

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

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

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

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

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

This will ensure any outbound numbers will have the dialing code 00 removed and international dialing symbol + inserted before being presented to the Avaya SBCE.

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, **SIP Trunk** for a CS1000 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 Help ?

SIP Entity Details

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Location:

Outbound Proxy:

Time Zone:

Minimum TLS Version:

Credential name:

Monitoring

SIP Link Monitoring:

CRLF Keep Alive Monitoring:

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:

3 Items Filter: Enable

Listen Ports	Protocol	Default Domain	Notes
<input type="checkbox"/> 5060	TCP	avaya.com	<input type="text"/>
<input type="checkbox"/> 5060	UDP	avaya.com	<input type="text"/>
<input type="checkbox"/> 5061	TLS	avaya.com	<input type="text"/>

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.

Home / Elements / Routing / SIP Entities Help ?

SIP Entity Details Commit Cancel

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

* SIP Timer B/F (in seconds):

Minimum TLS Version:

Credential name:

Securable:

Call Detail Recording:

Loop Detection

Loop Detection Mode:

Loop Count Threshold:

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 displays the configuration page for a SIP Entity in the Avaya SBCE. The breadcrumb navigation at the top reads "Home / Elements / Routing / SIP Entities". The page title is "SIP Entity Details", with "Commit" and "Cancel" buttons in the top right corner. The "General" section is active and contains the following fields:

- Name:** Avaya_SBCE
- FQDN or IP Address:** 10.10.3.65
- Type:** SIP Trunk
- Notes:** (empty text area)
- Adaptation:** Sunrise
- Location:** SMGR_7
- Time Zone:** Europe/Dublin
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty text area)
- Securable:**
- Call Detail Recording:** egress

The "Loop Detection" section is also visible and contains:

- Loop Detection Mode:** On
- Loop Count Threshold:** 5

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.



The screenshot displays the 'Entity Links' configuration page. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Entity Links'. Below the title, there are buttons for 'New', 'Edit', 'Delete', 'Duplicate', and a 'More Actions' dropdown. A 'Filter: Enable' link is visible on the right. The main content is a table with 4 items, showing the following data:

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	Avaya SBCE	Session Manager	TCP	5060	Avaya_SBCE	5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Communication Manager	Session Manager	TCP	5060	Communication_Manager	5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	CS1K_R76	Session Manager	TCP	5060	CS1K_R76	5060	<input type="checkbox"/>	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' 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' section contains fields for 'Name' (to_CS1K_R76), 'Disabled' (checkbox), 'Retries' (0), and 'Notes'. The 'SIP Entity as Destination' section has a 'Select' button and a table with one entry: CS1K_R76, FQDN or IP Address: 10.10.9.21, Type: SIP Trunk. The 'Time of Day' section has 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. It shows '1 Item' with a table of days and times. The table has columns for Ranking, Name, Mon, Tue, Wed, Thu, Fri, Sat, Sun, Start Time, End Time, and Notes. The entry is: Ranking: 0, Name: 24/7, Mon: checked, Tue: checked, Wed: checked, Thu: checked, Fri: checked, Sat: checked, Sun: checked, Start Time: 00:00, End Time: 23:59, Notes: Time Range 24/7. A 'Filter: Enable' button is also present.

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	<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 path is 'Home / Elements / Routing / Routing Policies'. The page title is 'Routing Policy Details' with 'Commit' and 'Cancel' buttons. The 'General' section includes fields for Name (to_Avaya_SBCE), Disabled (checkbox), Retries (0), and Notes. The 'SIP Entity as Destination' section shows a table with one entry: Avaya_SBCE, FQDN or IP Address 10.10.3.35, Type SIP Trunk. The 'Time of Day' section includes an 'Add' button, 'Remove', and 'View Gaps/Overlaps'. It shows one item with a ranking of 0, name 24/7, and a time range from 00:00 to 23:59, active on all days of the week.

Name	FQDN or IP Address	Type	Notes
Avaya_SBCE	10.10.3.35	SIP Trunk	

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	<input checked="" type="checkbox"/>	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 6.7**.
- Click **Select** button to save.

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

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details Commit Cancel

General

* Pattern:
 * Min:
 * Max:
 Emergency Call:
 Emergency Priority:
 Emergency Type:
 SIP Domain:
 Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	SMGR_7		to_Avaya_SBCE	0	<input type="checkbox"/>	Avaya_SBCE	

Select : All, None

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

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details Commit Cancel

General

* Pattern:
 * Min:
 * Max:
 Emergency Call:
 Emergency Priority:
 Emergency Type:
 SIP Domain:
 Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	SMGR_7		to_CS1K_R76	0	<input type="checkbox"/>	CS1K_R76	

Select : All, None

7. Configure Avaya Session Border Controller for Enterprise

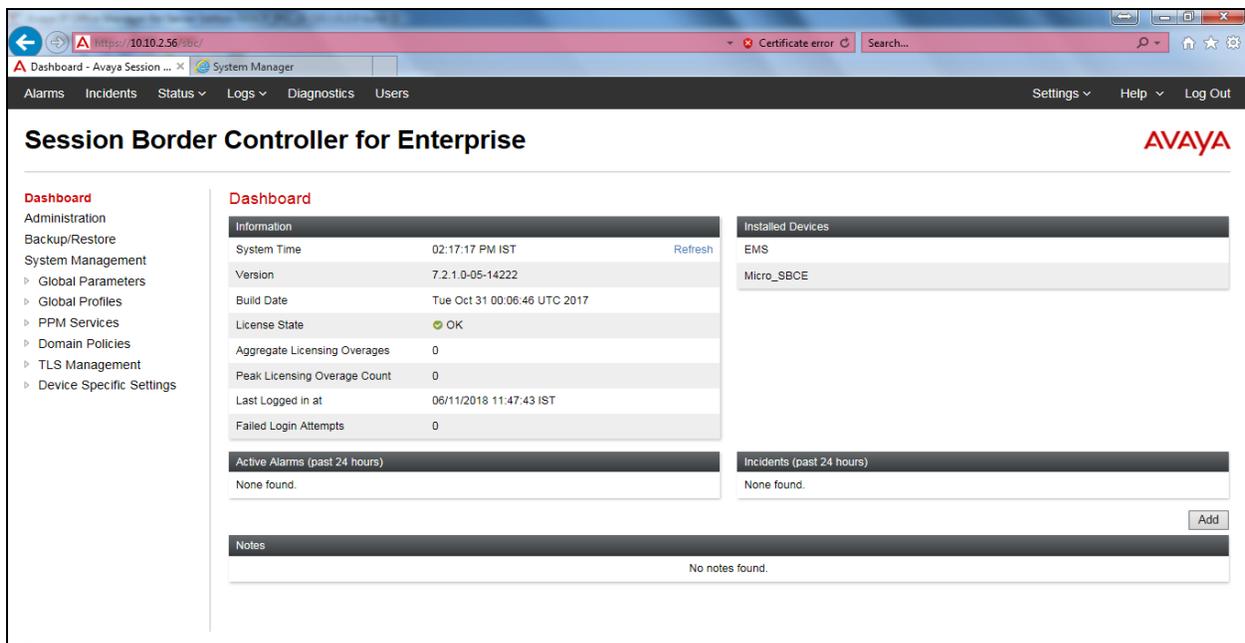
This section describes the configuration of the Avaya Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's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

7.1. Access Avaya Session Border Controller for Enterprise

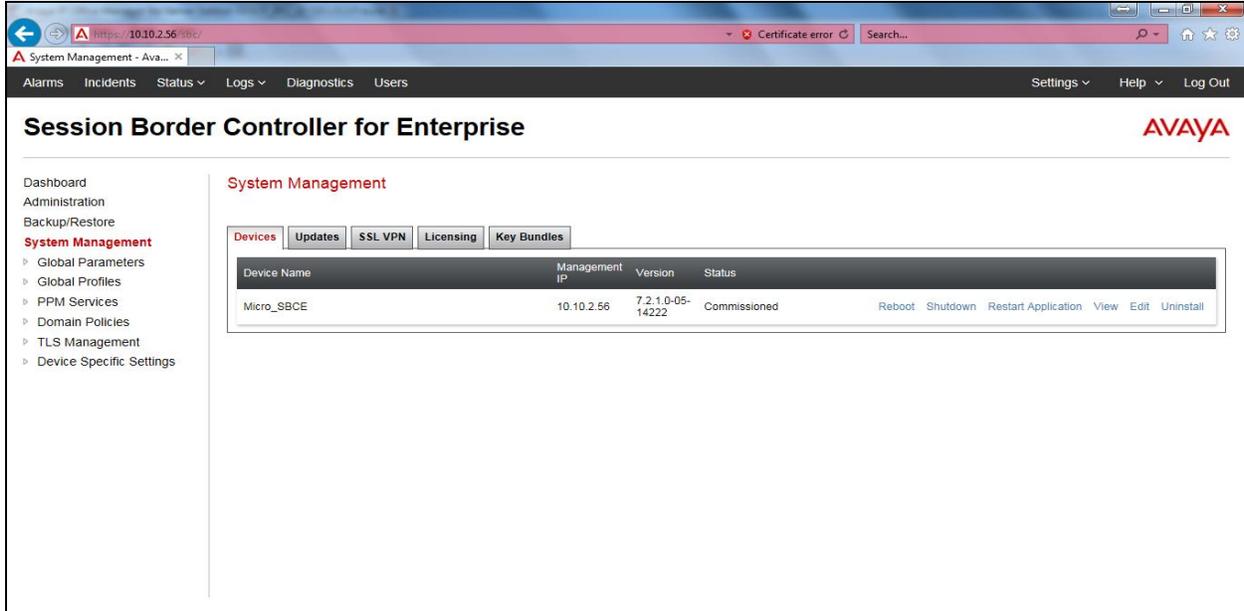
Access the Session Border Controller using a web browser by entering the URL **https://<ip-address>**, where <ip-address> is the private IP address configured at installation. A log in screen is presented.



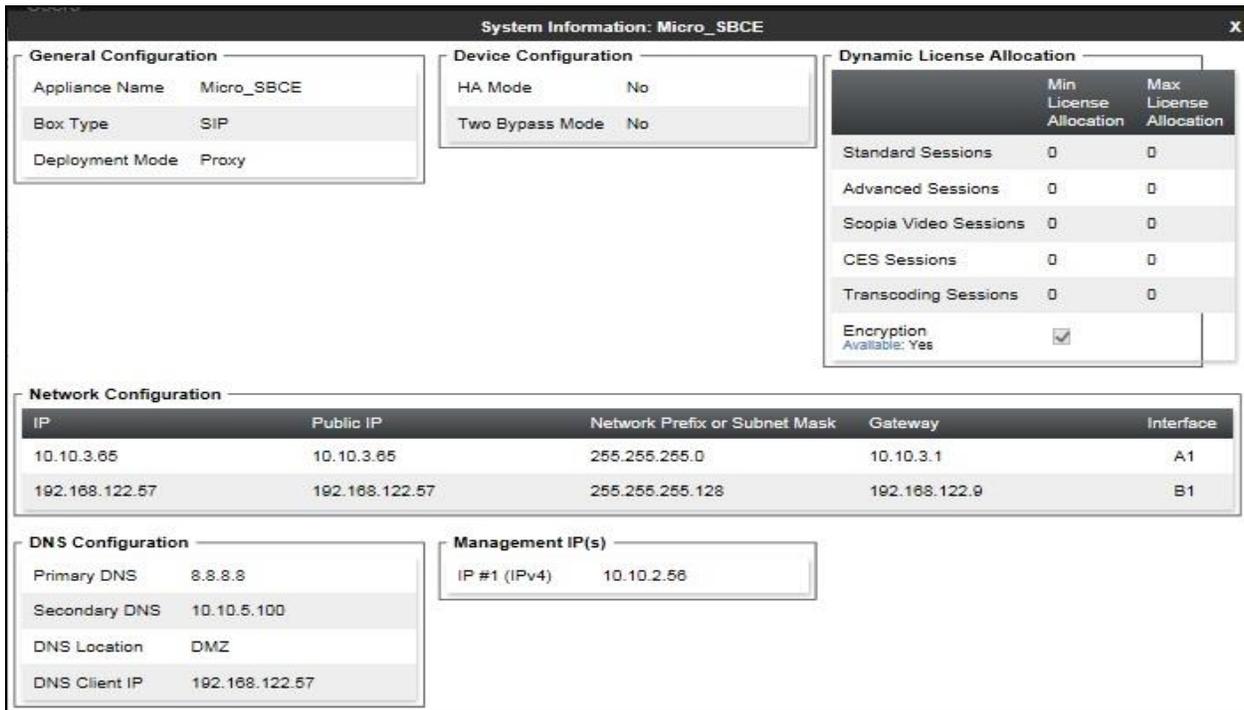
Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.



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



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



7.2. Global Profiles

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

7.2.1. Server Interworking Avaya

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

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

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

On the **Advanced** Tab:

- Check **Record Routes = Both Sides**.
- Ensure **Extensions = Avaya**.
- Check **Has Remote SBC**.
- All other options on the **Advanced** Tab can be left at default.

Click **Finish**.

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

Diversion Manipulation

Diversion Condition

Diversion Header URI

Has Remote SBC

Route Response on Via Port

Relay INVITE Replace for SIPREC

MOBX Re-INVITE Handling

DTMF

DTMF Support

None
 SIP Notify
 RFC 2833 Relay & SIP Notify
 SIP Info
 RFC 2833 Relay & SIP Info
 Inband

7.2.2. Server Interworking – Sunrise

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

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

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

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

On the **Advanced** Tab:

- Check **Record Routes = Both Sides**.
- Ensure **Extensions = None**.
- Check **Has Remote SBC**.
- All other options on the **Advanced** Tab can be left at default.

Click **Finish**.

The screenshot displays a configuration interface with the following settings:

- Record Routes:** Radio buttons for None, Single Side, **Both Sides** (selected), Dialog-Initiate Only (Single Side), and Dialog-Initiate Only (Both Sides).
- Include End Point IP for Context Lookup:** Checked checkbox.
- Extensions:** Dropdown menu set to None.
- Diversion Manipulation:** Unchecked checkbox.
- Diversion Condition:** Dropdown menu set to None.
- Diversion Header URI:** Empty text input field.
- Has Remote SBC:** Checked checkbox.
- Route Response on Via Port:** Unchecked checkbox.
- Relay INVITE Replace for SIPREC:** Unchecked checkbox.
- DTMF Section:** Header bar.
- DTMF Support:** Radio buttons for **None** (selected), SIP Notify, SIP Info, and Inband.
- Finish:** Button at the bottom.

7.2.3. Server Configuration– Avaya

Servers are defined for each server connected to the Avaya SBCE. In this case, Sunrise is connected as the Trunk Server and Session Manager is connected as the Call Server.

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow the configuration and management of various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signalling parameters and some advanced options.

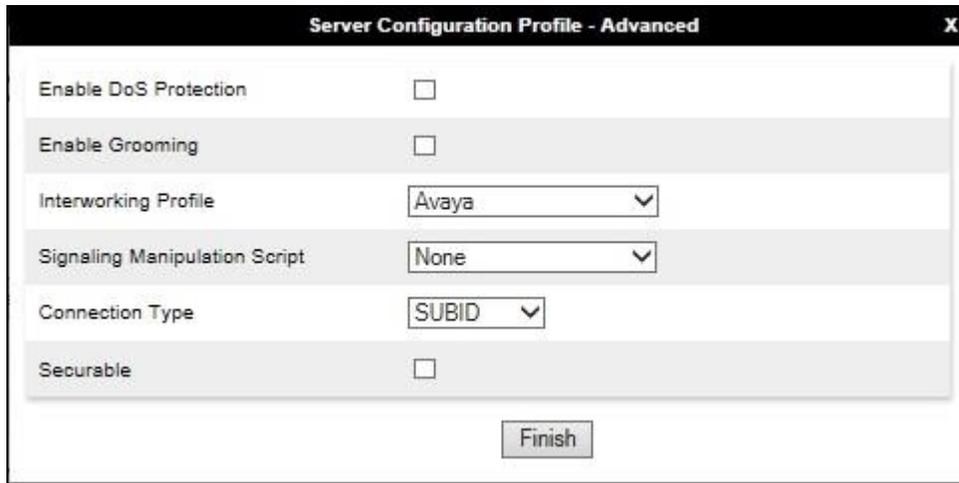
From the left-hand menu select **Global Profiles** → **Server Configuration** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

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

IP Address / FQDN	Port	Transport
10.10.3.42	5060	TCP

On the **Advanced** tab:

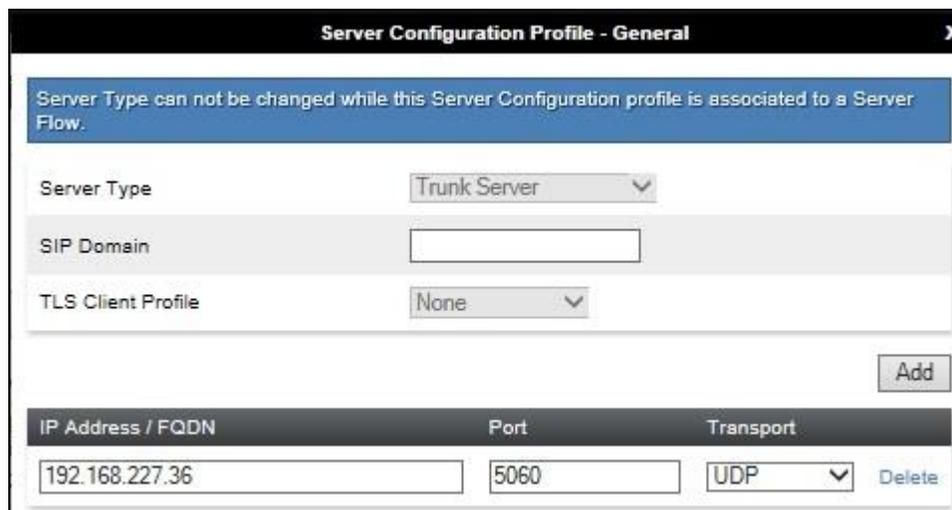
- Select **Avaya** for **Interworking Profile**.
- Click **Finish**.



7.2.4. Server Configuration – Sunrise

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

- Select **Server Type** to be **Trunk Server**.
- Enter **IP Address / FQDN** to **192.168.227.36** (Sunrise SBC IP Address).
- For **Port**, enter **5060**.
- For **Transport**, select **UDP**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.



On the Advanced tab:

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

Server Configuration Profile - Advanced X

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Sunrise ▾
Signaling Manipulation Script	None ▾
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	<input type="text"/>
TLS Failover Port	<input type="text"/>
Tolerant	<input type="checkbox"/>
URI Group	None ▾

Finish

7.2.5. Routing

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

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

7.2.5.1 Routing – Avaya

Create a Routing Profile for Session Manager.

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



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

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



The screenshot shows the "Routing Profile" window with various configuration options. The "URI Group" is set to "*", "Time of Day" is "default", "Load Balancing" is "Priority", "Transport" is "None", "Next Hop In-Dialog" is unchecked, "NAPTR" is unchecked, and "Next Hop Priority" is checked. "Ignore Route Header" is unchecked. There is an "Add" button at the bottom right. Below the "Add" button is a blue message box that says "Click the Add button to add a Next-Hop Address." At the bottom of the window are "Back" and "Finish" buttons.

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

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

Profile : Avaya

URI Group: *
Time of Day: default

Load Balancing: Priority
NAPTR:

Transport: None
Next Hop Priority:

Next Hop In-Dialog:
Ignore Route Header:

ENUM:
ENUM Suffix:

Add

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

7.2.5.2 Routing – Sunrise

Create a Routing Profile for Sunrise.

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

Routing Profile

Profile Name: Sunrise

Next

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

The screenshot shows the 'Routing Profile' configuration window. It contains several settings: 'URI Group' is set to '*', 'Time of Day' is 'default', 'Load Balancing' is 'Priority', 'NAPTR' is unchecked, 'Transport' is 'None', 'Next Hop Priority' is checked, 'Next Hop In-Dialog' is unchecked, and 'Ignore Route Header' is unchecked. There is an 'Add' button at the bottom right. Below the settings is a blue banner with the text 'Click the Add button to add a Next-Hop Address.' At the very bottom are 'Back' and 'Finish' buttons.

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

- **Priority/Weight = 1.**
- **Server Configuration = Sunrise (Section 7.2.4)** from drop down menu.
- **Next Hop Address = Select 192.168.227.36:5060 (UDP)** from drop down menu.
- Click **Finish**.

The screenshot shows the 'Profile: Sunrise' configuration window. It has the same settings as the previous window. Below the settings is an 'Add' button. At the bottom, there is a table with the following data:

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	Sunrise	192.168.227.36:5060 (UDP)	None	Delete

There is a 'Finish' button at the bottom center of the window.

7.2.6. Topology Hiding

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

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

- Enter a descriptive Profile Name such as **Avaya**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For Overwrite value, insert **avaya.com**.
- Click **Finish** (not shown).

Topology Hiding Profiles: Avaya

Buttons: Add, Rename, Clone, Delete

Topology Hiding Profiles: default, cisco_th_profile, **Avaya**, Sunrise

Click here to add a description.

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

Buttons: Edit

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

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

Topology Hiding Profiles: Sunrise

Add Rename Clone Delete

Topology Hiding Profiles Click here to add a description.

- default
- cisco_th_profile
- Avaya
- Sunrise**

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

Edit

7.3. Define Network Information

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

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

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

Network Management: Micro_SBCE

Devices: Micro_SBCE

Interfaces: Networks

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
A1_Internal	10.10.3.1	255.255.255.0	A1	10.10.3.65	Edit Delete
B1_External	192.168.122.9	255.255.255.128	B1	192.168.122.57	Edit Delete

Add

Select the **Interface Configuration** tab and click on the **Status** of the physical interface to toggle the state. Change the state to **Enabled** where required.

Network Management: Micro_SBCE

Devices: Micro_SBCE

Interfaces: Networks

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled

Add VLAN

7.4. Define Interfaces

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

7.4.1. Signalling Interfaces

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

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

- Select **Add** and enter details of the internal signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the interface.
- In the **IP Address** drop down menus, select the internal network interface and IP address. When the internal network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 7.3**.
- Insert **TCP** port number, **5060** is used for Session Manager.

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

- Select **Add** and enter details of the external signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the external signalling interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. When the external network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 7.3**.
- Insert **UDP** port number, **5060** is used for Sunrise SIP Trunk.

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

Signaling Interface: Micro_SBCE

Devices

Micro_SBCE

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	
Ext_Sig	192.168.122.57 B1_External (B1, VLAN 0)	---	5060	---	None	Edit Delete
Int_Sig	10.10.3.65 A1_Internal (A1, VLAN 0)	5060	---	---	None	Edit Delete

7.4.2. Media Interfaces

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

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

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

- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal media interface.
- In the **IP Address** drop down menus, select the internal network interface and IP address. When the internal network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 7.3**.
- Select **RTP port** ranges for the media path with the enterprise end-points.

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

- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the external media interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. When the external network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 7.3**.
- Select **RTP port** ranges for the external media path. The port ranges used in the screenshot below were specified by Sunrise.

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

Media Interface: Micro_SBCE

Devices

- Micro_SBCE

Media Interface

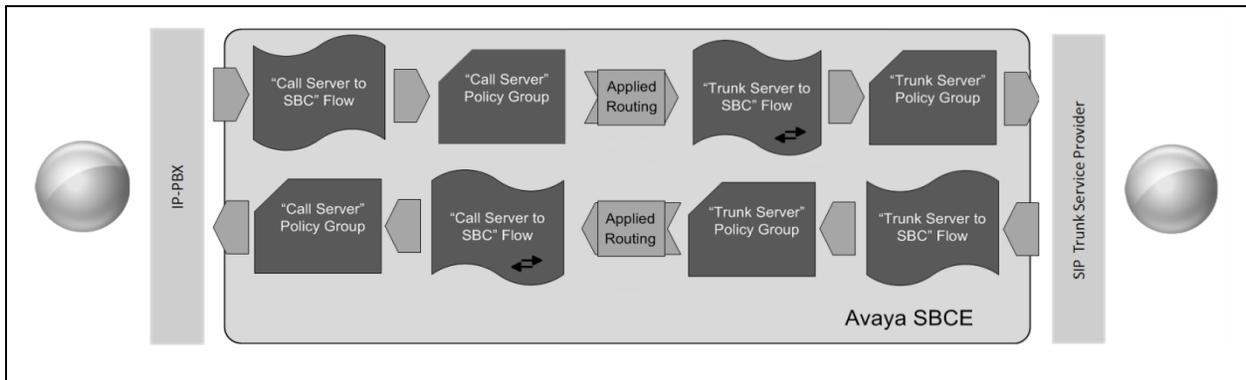
Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Add

Name	Media IP Network	Port Range	Edit	Delete
Int_Media	10.10.3.65 A1_Internal (A1, VLAN 0)	35000 - 40000	Edit	Delete
Ext_Media	192.168.122.57 B1_External (B1, VLAN 0)	6000 - 8999	Edit	Delete

7.5. Server Flows

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



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

Subscriber Flows	Server Flows						
Add							
Hover over a row to see its description.							
Server Configuration: Avaya							
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Call_Server	*	Ext_Sig	Int_Sig	default-low	Sunrise	View Clone Edit Delete
Server Configuration: Sunrise							
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Trunk_Server	*	Int_Sig	Ext_Sig	default-low	Avaya	View Clone Edit Delete

To define a Server Flow for the Sunrise Business Voice Direct 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 Sunrise Business Voice Direct SIP Trunk, in the test environment **Trunk_Server** was used.
- In the **Server Configuration** drop-down menu, select the Sunrise server configuration defined in **Section 7.2.4**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.4.1**. This is the interface that signalling bound for Sunrise Business Voice Direct SIP Trunk is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4.1**. This is the interface that signalling bound for Sunrise Business Voice Direct SIP Trunk is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.4.2**. This is the interface that media bound for Sunrise Business Voice Direct SIP Trunk is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager Office defined in **Section 7.2.5**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Sunrise Business Voice Direct SIP Trunk defined in **Section 7.2.6** and click **Finish**.

The screenshot shows a configuration window titled "Flow: Trunk_Server" with a close button (X) in the top right corner. The window is divided into two main sections: "Criteria" and "Profile".

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

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

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

The screenshot shows a configuration window titled "Flow: Call_Server" with a close button (X) in the top right corner. The window is divided into two main sections: "Criteria" and "Profile".

Criteria		Profile	
Flow Name	Call_Server	Signaling Interface	Int_Sig
Server Configuration	Avaya	Media Interface	Int_Media
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	default-low
Remote Subnet	*	Routing Profile	Sunrise
Received Interface	Ext_Sig	Topology Hiding Profile	Avaya
		Signaling Manipulation Script	None
		Remote Branch Office	Any

8. Sunrise SIP Trunk Configuration

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

9. Verification Steps

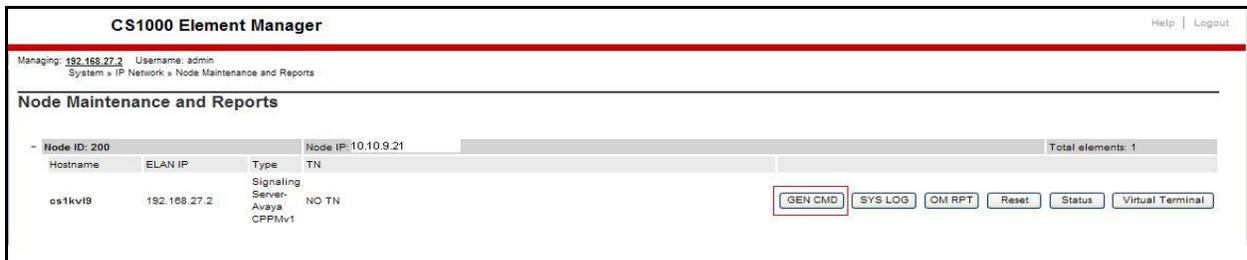
This section provides verification steps that may be performed in the field to verify that the solution is configured properly.

9.1. Avaya Communication Server 1000 Verification

This section illustrates sample verifications that may be performed using the Avaya CS1000 Element Manager GUI.

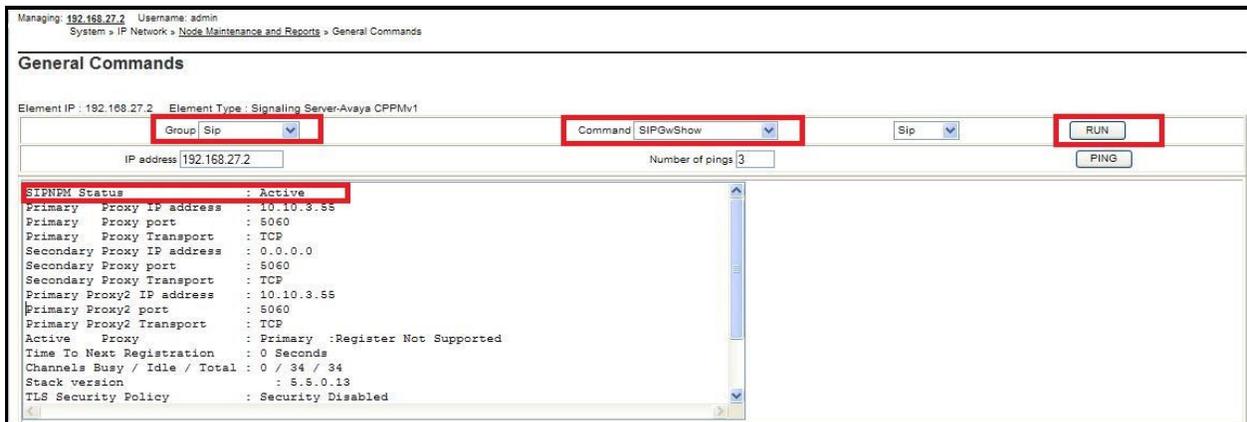
9.1.1. IP Network Maintenance and Reports Commands

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".



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 > Node Maintenance and Reports > General Commands

General Commands

Element IP : 192.168.27.2 Element Type : Signaling Server-Avaya CPPMv1

Group: SipLine Command: sigSetShowAll RUN

IP address: 192.168.27.2 Number of pings: 3 PING

UserID	AuthId	TN	Clients	Calls	SetHandle	Pos ID	SIPL Type
----- IPv4 Endpoints -----							
6003	6003	100-00-03-03	1	0	0x91e22d0		SIP Lines
6002	6002	100-00-03-02	1	0	0x91c4158		SIP Lines
Total User Registered = 2 V4 Registered = 2 V6 Registered = 0							

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

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

General Commands

Element IP : 192.168.27.2 Element Type : Signaling Server-Avaya CPPMv1

Group: Iset Command: isetShow RUN

IP address: 192.168.27.2 Range: 0 500 Number of pings: 3 PING

IP Address	NAT	Model Name	Type	RegType	State	Up
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.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left navigation pane is expanded to 'System' > 'Maintenance'. The main area displays the 'Maintenance' page with two selection options: 'Select by Overlay' (selected) and 'Select by Functionality'. The 'Select by Overlay' table lists various LDs, with 'LD 96 - D-Channel' highlighted. The 'Select by Functionality' table shows 'D-Channel Diagnostics' selected.

Select by Overlay	
<Select by Overlay>	
LD 30 - Network and Signaling	
LD 32 - Network and Peripheral Equipment	
LD 34 - Tone and Digit Switch	
LD 36 - Trunk	
LD 37 - Input/Output	
LD 38 - Conference Circuit	
LD 39 - Intergroup Switch and System Clock	
LD 45 - Background Signaling and Switching	
LD 46 - Multifrequency Sender	
LD 48 - Link	
LD 54 - Multifrequency Signaling	
LD 60 - Digital Trunk Interface and Primary Rate Interface	
LD 75 - Digital Trunk	
LD 80 - Call Trace	
LD 96 - D-Channel	
LD 117 - Ethernet and Alarm Management	
LD 135 - Core Common Equipment	
LD 137 - Core Input/Output	
LD 143 - Centralized Software Upgrade	

Select Group	
D-Channel Diagnostics	
MSDL Diagnostics	
TMDI Diagnostics	

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**

The screenshot shows the AVAYA CS1000 Element Manager interface with the 'D-Channel Diagnostics' page. The 'Diagnostic Commands' table has 'Status for D-Channel (STAT DCH)' selected. The 'Command Parameters' table shows 'ALL' and 'FDL' options. The 'Action' column has a 'Submit' button. Below the table, the command 'STAT DCH' is shown to have been executed successfully.

Diagnostic Commands	Command Parameters	Action
Status for D-Channel (STAT DCH)		Submit
Disable Automatic Recovery (DIS AUTO)	<input type="checkbox"/> ALL	Submit
Enable Automatic Recovery (ENL AUTO)	<input type="checkbox"/> FDL	Submit
Test Interrupt Generation (TEST 100)		Submit
Establish D-Channel (EST DCH)		Submit

DCH	DES	APPL_STATUS	LINK_STATUS	AUTO_RECVP	PDCH	BDCH
C	001	SIP_DCH	OPER	EST ACTV	AUTO	

```

STAT DCH
-----
Command executed successfully.
    
```

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' page. At the top, the breadcrumb navigation is 'Home / Elements / Session Manager / Dashboard'. The page title is 'Session Manager Dashboard' with a 'Help ?' link. Below the title is a descriptive sentence: 'This page provides the overall status and health summary of each administered Session Manager.' The main content area is titled 'Session Manager Instances' and includes filters for 'Service State', 'Shutdown System', and 'As of 3:00 PM'. There is a '1 Item' indicator and a 'Show All' dropdown. A table lists the instances with columns for 'Session Manager', 'Type', 'Tests Pass', 'Alarms', 'Security Module', 'Service State', 'Entity Monitoring', 'Active Call Count', 'Registrations', 'Data Replication', 'User Data Storage Status', 'License Mode', and 'Version'. The table contains one row for 'Session Manager' with the following values: Type: Core, Tests Pass: 0/0/0, Alarms: 0/0/0, Security Module: Up, Service State: Accept New Service, Entity Monitoring: 0/5, Active Call Count: 0, Registrations: 2/2, Data Replication: ✓, User Data Storage Status: ✓, License Mode: Normal, Version: 7.0.1.2.701230. At the bottom, there is a 'Select : All, None' option.

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	2/2	✓	✓	Normal	7.0.1.2.701230

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. At the top, the breadcrumb navigation is 'Home / Elements / Session Manager / System Status / Security Module Status'. The page title is 'Security Module Status' with a 'Help ?' link. Below the title is a descriptive sentence: 'This page allows you to view the status of each Session Manager's Security Module and to perform certain actions.' The main content area includes buttons for 'Reset', 'Synchronize', and 'Connection Status', and a filter for 'As of 2:00 PM'. There is a '1 Item' indicator and a 'Show All' dropdown. A table lists the security module status with columns for 'Session Manager', 'Type', 'Status', 'Connections', 'IP Address', 'VLAN', 'Default Gateway', 'Entity Links (expected / actual)', and 'Certificate Used'. The table contains one row for 'Session Manager' with the following values: Type: SM, Status: Up, Connections: 18, IP Address: 10.10.3.42/24, VLAN: ---, Default Gateway: 10.10.3.1, Entity Links: 5/5, Certificate Used: SIP CA. At the bottom, there is a 'Select : None' option.

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

9.4. 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.

Type	ID	Date	Time	Category	Device	Cause
Routing Failure	686948871165253	7/15/13	2:15 PM	Policy	VLAN3_MicroSBC	Neither target nor source is Call Server, Sending 403 Forbidden
Routing Failure	686948811180314	7/15/13	2:13 PM	Policy	VLAN3_MicroSBC	Neither target nor source is Call Server, Sending 403 Forbidden
ACK Message Out of Dialog	686948761299324	7/15/13	2:12 PM	Protocol Discrepancy	VLAN3_MicroSBC	General Method not allowed Out-Of-Dialog
Message Dropped	686948761299222	7/15/13	2:12 PM	Policy	VLAN3_MicroSBC	No Subscriber Flow Matched
Call Denied	686948761263328	7/15/13	2:12 PM	Policy	VLAN3_MicroSBC	No Subscriber Flow Matched
Routing Failure	686948751195370	7/15/13	2:11 PM	Policy	VLAN3_MicroSBC	Neither target nor source is Call Server, Sending 403 Forbidden

9.4.2. Trace Settings

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

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

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

The screenshot shows the 'Trace: Micro_SBCE' interface. On the left, there is a 'Devices' sidebar with 'Micro_SBCE' selected. The main area has two tabs: 'Packet Capture' (active) and 'Captures'. The 'Packet Capture Configuration' section includes the following fields:

Status	Ready
Interface	B1
Local Address IP[:Port]	All : <input type="text"/>
Remote Address *, *:Port, IP, IP:Port	*
Protocol	All
Maximum Number of Packets to Capture	1000
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	test.pcap

At the bottom of the configuration section are two buttons: 'Start Capture' and 'Clear'.

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

The screenshot shows the 'Trace: Micro_SBCE' interface with the 'Captures' tab selected. A 'Refresh' button is located at the top right. Below it is a table listing the captured files:

File Name	File Size (bytes)	Last Modified	
test_20170622141913.pcap	0	June 22, 2017 2:19:48 PM IST	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 Sunrise Business Voice Direct SIP Trunk network.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Communication Server 1000 R7.65, Avaya Aura® Session Manager R7.1 and Avaya Session Border Controller for Enterprise R7.2 to Sunrise Business Voice Direct SIP Trunk. Sunrise Business Voice Direct 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] *Avaya Aura® System Manager using VMware® in the Virtualized Environment Deployment Guide* Release 7.1 May 2018.
- [2] *Implementing Avaya Aura® System Manager* Release 7.1, May 2018.
- [3] *Upgrading Avaya Aura® System Manager to Release 7.1*, May 2018.
- [4] *Administering Avaya Aura® System Manager* Release 7.1, Jun 2018
- [5] *Avaya Aura® Session Manager using VMware® in the Virtualized Environment Deployment Guide* Release 7.1, May 2018
- [6] *Implementing Avaya Aura® Session Manager* Release 7.1, May 2018.
- [7] *Upgrading Avaya Aura® Session Manager* Release 7.1, May 2018.
- [8] *Administering Avaya Aura® Session Manager* Release 7.1, May 2018.
- [9] *Avaya Communication Server 1000 Installation and Commissioning*, Document Number NN43041-310
- [10] *Linux Platform Base and Applications Installation and Commissioning Avaya Communication Server 1000*, Document Number NN43001-315
- [11] *Software Input Output Reference – Maintenance Avaya Communication Server 1000*, Document Number NN43001-711
- [12] *Deploying Avaya Session Border Controller for Enterprise* Release 7.2, Apr 2018.
- [13] *Upgrading Avaya Session Border Controller for Enterprise* Release 7.2, Apr 2018.
- [14] *Administering Avaya Session Border Controller for Enterprise* Release 7.2, Jun 2018.
- [15] *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

```

01/05/18
TID: 46379

VERSION 4121

System type is - Communication Server 1000E/CPPM Linux
CPM - 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: 2017-06-30 10:51:38 (est))

MDP>LAST SUCCESSFUL MDP REFRESH :2017-10-11 12:51:56(Local Time)
MDP>USING DEPLIST ZIP FILE DOWNLOADED :2017-06-30 11:39:15(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     ISS1:10F1      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 end

```

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     ISS1:10F1      p32331_1     15/03/2017   p32331_1.cpl  NO
001   wi01064599     iss1:10f1      p32580_1     15/03/2017   p32580_1.cpl  NO
002   wi01056067     ISS1:10F1      p32457_1     15/03/2017   p32457_1.cpl  NO
003   wi01063263     ISS1:10F1      p32573_1     15/03/2017   p32573_1.cpl  NO
004   wi01065842     ISS1:10F1      p32478_1     15/03/2017   p32478_1.cpl  NO
005   wi01062607     ISS1:10F1      p32503_1     15/03/2017   p32503_1.cpl  NO
006   wi01070756     ISS1:10F1      p32444_1     15/03/2017   p32444_1.cpl  NO
007   wi01039280     ISS1:10F1      p32423_1     15/03/2017   p32423_1.cpl  NO
008   wi01087543     ISS1:10F1      p32662_1     15/03/2017   p32662_1.cpl  NO
009   wi00933195     ISS1:10F1      p32491_1     15/03/2017   p32491_1.cpl  NO
010   wi01071379     ISS1:10F1      p32522_1     15/03/2017   p32522_1.cpl  NO
011   wi01068669     ISS1:10F1      p32333_1     15/03/2017   p32333_1.cpl  NO
012   wi01066991     ISS1:10F1      p32449_1     15/03/2017   p32449_1.cpl  NO
013   wi01070474     iss1:10f1      p32407_1     15/03/2017   p32407_1.cpl  NO
014   WI0110261     ISS1:10F1      p32758_1     15/03/2017   p32758_1.cpl  NO
015   wi01094305     ISS1:10F1      p32640_1     15/03/2017   p32640_1.cpl  NO
016   wi01047890     ISS1:10F1      p32697_1     15/03/2017   p32697_1.cpl  NO

```

017	wi01055300	ISS1:10F1	p32543_1	15/03/2017	p32543_1.cpl	NO
018	wi01082456	ISS1:10F1	p32596_1	15/03/2017	p32596_1.cpl	NO
019	wi01058621	ISS1:10F1	p32339_1	15/03/2017	p32339_1.cpl	NO
020	wi01061484	ISS1:10F1	p32576_1	15/03/2017	p32576_1.cpl	NO
021	wi01078723	ISS1:10F1	p32532_1	15/03/2017	p32532_1.cpl	NO
022	wi01048457	ISS1:10F1	p32581_1	15/03/2017	p32581_1.cpl	NO
023	wi01075355	ISS1:10F1	p32594_1	15/03/2017	p32594_1.cpl	NO
024	wi01053597	ISS1:10F1	p32304_1	15/03/2017	p32304_1.cpl	NO
025	wi01045058	ISS1:10F1	p32214_1	15/03/2017	p32214_1.cpl	NO
026	wi01075359	ISS1:10F1	p32671_1	15/03/2017	p32671_1.cpl	NO
027	wi01025156	ISS1:10F1	p32136_1	15/03/2017	p32136_1.cpl	NO
028	wi01061481	ISS1:10F1	p32382_1	15/03/2017	p32382_1.cpl	NO
029	wi01035976	ISS1:10F1	p32173_1	15/03/2017	p32173_1.cpl	NO
030	wi01088775	ISS1:10F1	p32659_1	15/03/2017	p32659_1.cpl	NO
031	wi01070465	iss1:10f1	p32562_1	15/03/2017	p32562_1.cpl	NO
032	wi01088585	ISS1:10F1	p32656_1	15/03/2017	p32656_1.cpl	NO
033	wi01063864	ISS1:10F1	p32410_1	15/03/2017	p32410_1.cpl	YES
034	wi01034961	ISS1:10F1	p32144_1	15/03/2017	p32144_1.cpl	NO
035	wi01055480	ISS1:10F1	p32712_1	15/03/2017	p32712_1.cpl	NO
036	wi01034307	ISS1:10F1	p32615_1	15/03/2017	p32615_1.cpl	NO
037	wi01065118	ISS1:10F1	p32397_1	15/03/2017	p32397_1.cpl	NO
038	wi01075360	iss1:10f1	p32602_1	15/03/2017	p32602_1.cpl	NO
039	wi00884716	ISS1:10F1	p32517_1	15/03/2017	p32517_1.cpl	NO
040	wi01068851	ISS1:10F1	p32439_1	15/03/2017	p32439_1.cpl	NO
041	wi01053314	ISS1:10F1	p32555_1	15/03/2017	p32555_1.cpl	NO
042	wi01059388	iss1:10f1	p32628_1	15/03/2017	p32628_1.cpl	NO
043	wi01087528	ISS1:10F1	p32700_1	15/03/2017	p32700_1.cpl	NO
044	wi01072027	ISS1:10F1	p32689_1	15/03/2017	p32689_1.cpl	NO
045	wi01052428	ISS1:10F1	p32606_1	15/03/2017	p32606_1.cpl	NO
046	wi01053920	ISS1:10F1	p32303_1	15/03/2017	p32303_1.cpl	NO
047	wi01070468	iss1:10f1	p32418_1	15/03/2017	p32418_1.cpl	NO
048	wi01067822	ISS1:10F1	p32466_1	15/03/2017	p32466_1.cpl	YES
049	wi01060826	ISS1:10F1	p32379_1	15/03/2017	p32379_1.cpl	NO
050	wi01075352	ISS1:10F1	p32603_1	15/03/2017	p32603_1.cpl	NO
051	wi01043367	ISS1:10F1	p32232_1	15/03/2017	p32232_1.cpl	NO
052	wi01083584	ISS1:10F1	p32619_1	15/03/2017	p32619_1.cpl	NO
053	wi01060241	ISS1:10F1	p32381_1	15/03/2017	p32381_1.cpl	NO
054	wi01053195	ISS1:10F1	p32297_1	15/03/2017	p32297_1.cpl	NO
055	wi00897254	ISS1:10F1	p31127_1	15/03/2017	p31127_1.cpl	NO
056	wi01061483	ISS1:10F1	p32359_1	15/03/2017	p32359_1.cpl	NO
057	wi01085855	ISS1:10F1	p32658_1	15/03/2017	p32658_1.cpl	NO
058	wi01075353	ISS1:10F1	p32613_1	15/03/2017	p32613_1.cpl	NO
059	wi01070471	ISS1:10F1	p32415_1	15/03/2017	p32415_1.cpl	NO
060	wi01074003	ISS1:10F1	p32421_1	15/03/2017	p32421_1.cpl	NO
061	wi01060382	iss1:10f1	p32623_1	15/03/2017	p32623_1.cpl	YES
062	wi01068042	ISS1:10F1	p32669_1	15/03/2017	p32669_1.cpl	NO
063	wi01072023	ISS1:10F1	p32130_1	15/03/2017	p32130_1.cpl	YES
064	wi01065922	ISS1:10F1	p32516_1	15/03/2017	p32516_1.cpl	NO
065	wi01057403	ISS1:10F1	p32591_1	15/03/2017	p32591_1.cpl	NO
066	wi01069441	ISS1:10F1	p32097_1	15/03/2017	p32097_1.cpl	NO
067	wi01070473	ISS1:10F1	p32413_1	15/03/2017	p32413_1.cpl	NO
068	wi01056633	ISS1:10F1	p32322_1	15/03/2017	p32322_1.cpl	NO
069	wi01052968	ISS1:10F1	p32540_1	15/03/2017	p32540_1.cpl	NO
070	wi01072032	ISS1:10F1	p32448_1	15/03/2017	p32448_1.cpl	NO
071	wi01073100	ISS1:10F1	p32599_1	15/03/2017	p32599_1.cpl	NO
072	wi01035980	ISS1:10F1	p32558_1	15/03/2017	p32558_1.cpl	NO
073	wi01041453	ISS1:10F1	p32587_1	15/03/2017	p32587_1.cpl	NO
074	wi01032756	ISS1:10F1	p32673_1	15/03/2017	p32673_1.cpl	NO
075	wi01092300	ISS1:10F1	p32692_1	15/03/2017	p32692_1.cpl	NO
076	wi00996734	ISS1:10F1	p32550_1	15/03/2017	p32550_1.cpl	NO
077	wi01022599	ISS1:10F1	p32080_1	15/03/2017	p32080_1.cpl	NO
078	wi01060341	ISS1:10F1	p32578_1	15/03/2017	p32578_1.cpl	NO
079	wi01091447	ISS1:10F1	p32675_1	15/03/2017	p32675_1.cpl	NO
080	wi01070580	ISS1:10F1	p32380_1	15/03/2017	p32380_1.cpl	NO
081	wi01089519	ISS1:10F1	p32665_1	15/03/2017	p32665_1.cpl	NO
082	WI01077073	ISS1:10F1	p32534_1	15/03/2017	p32534_1.cpl	NO
083	wi01080753	ISS1:10F1	p32518_1	15/03/2017	p32518_1.cpl	NO
084	wi01065125	ISS1:10F1	p32416_1	15/03/2017	p32416_1.cpl	NO

Communication Server 1000 signaling server service updates

Product Release: 7.65.16.00

In system patches: 9

PATCH#	NAME	IN_SERVICE	DATE	SPECINS	TYPE	RPM
37	p31484_1	Yes	02/10/13	NO	FRU	cs1000-shared-general-7.65.16-00.i386
46	p33384_1	Yes	15/10/15	NO	FRU	cs1000-OS-1.00.00.00-00.noarch
48	p33774_1	Yes	10/10/17	YES	FRU	cs1000-OS-1.00.00.00-00.noarch
56	p33125_1	Yes	14/07/14	NO	FRU	cs1000-OS-1.00.00.00-00.noarch
57	p33274_1	Yes	14/07/14	YES	FRU	initscripts-8.45.25-1.el5.i386
59	p33493_1	Yes	15/10/15	NO	FRU	cs1000-OS-1.00.00.00-00.noarch
61	p33557_1	Yes	15/10/15	YES	FRU	cs1000-OS-1.00.00.00-00.noarch
67	p33584_1	Yes	11/07/16	YES	FRU	cs1000-OS-1.00.00.00-00.noarch
68	p33673_1	Yes	11/07/16	NO	FRU	net-snmp-5.3.2.2-5.el5.i386

In System service updates: 46

PATCH#	IN_SERVICE	DATE	SPECINS	REMOVABLE	NAME
0	Yes	06/10/17	YES	YES	cs1000-linuxbase-7.65.16.23-35.i386.000
2	Yes	06/10/17	NO	YES	cs1000-Jboss-Quantum-7.65.16.23-12.i386.000
3	Yes	15/10/15	NO	YES	cs1000-sps-7.65.16.23-1.i386.000
4	Yes	11/07/16	YES	YES	cs1000-dmWeb-7.65.16.23-5.i386.000
5	Yes	10/10/17	YES	YES	cs1000-bcc-7.65.16.23-19.i386.000
6	Yes	11/07/16	YES	YES	cs1000-patchWeb-7.65.16.23-2.i386.000
7	Yes	14/07/14	YES	YES	cs1000-csoneksvrmgr-7.65.16.22-5.i386.000
9	Yes	27/09/13	NO	YES	cs1000-shared-carrdtct-7.65.16.21-.i386.000
10	Yes	10/10/17	NO	YES	cs1000-cs1000WebService_6-0-7.65.16.23-i386.000
11	Yes	14/07/14	YES	YES	cs1000-baseWeb-7.65.16.22-4.i386.000
13	Yes	11/07/16	NO	YES	cs1000-shared-tpselect-7.65.16.23-.i386.000
14	Yes	11/07/16	YES	YES	cs1000-csmWeb-7.65.16.23-2.i386.000
16	Yes	11/07/16	YES	YES	cs1000-nrsm-7.65.16.23-1.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	10/10/17	YES	YES	cs1000-dbcom-7.65.16.23-1.i386.000
20	Yes	10/10/17	YES	YES	cs1000-emWeb_6-0-7.65.16.23-8.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-2.6.26-1.25.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
25	Yes	11/07/16	YES	YES	cs1000-csv-7.65.16.23-4.i386.000
26	Yes	10/10/17	YES	YES	cs1000-mscAttn-7.65.16.23-15.i386.000
28	Yes	15/10/15	YES	YES	cs1000-ftprpkg-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	10/10/17	YES	YES	cs1000-oam-logging-7.65.16.23-1.i386.000
33	Yes	10/10/17	NO	YES	cs1000-pd-7.65.16.23-1.i386.000
34	Yes	10/10/17	YES	YES	cs1000-shared-pbx-7.65.16.23-3.i386.000
35	Yes	10/10/17	YES	YES	cs1000-tps-7.65.16.23-21.i386.000
36	Yes	10/10/17	YES	YES	cs1000-vtrk-7.65.16.23-123.i386.000
38	Yes	02/04/14	YES	YES	cs1000-emWebLocal_6-0-7.65.16.22-1.i386.000
40	Yes	02/04/14	YES	YES	cs1000-ipsec-7.65.16.22-1.i386.000
41	Yes	10/10/17	YES	YES	kernel-2.6.18-419.el5.i686.000
43	Yes	10/10/17	YES	YES	openssl-0.9.8e-40.el5_11.i386.000
44	Yes	10/10/17	NO	YES	pass_harden-7.65.16.23-2.i386.000
45	Yes	10/10/17	NO	YES	pcap-7.65.16.23-1.i386.000
47	Yes	10/10/17	NO	yes	tzdata-2016g-2.el5.i386.000
49	Yes	14/07/14	NO	YES	cs1000-gk-7.65.16.22-1.i386.000
50	Yes	11/07/16	YES	YES	cs1000-mscAnnc-7.65.16.23-1.i386.000
51	Yes	11/07/16	YES	YES	cs1000-mscConf-7.65.16.23-1.i386.000
52	Yes	11/07/16	YES	YES	cs1000-mscMusc-7.65.16.23-1.i386.000
53	Yes	14/07/14	YES	YES	cs1000-shared-xmsg-7.65.16.22-1.i386.000
55	Yes	11/07/16	YES	YES	cs1000-mscTone-7.65.16.23-1.i386.000
62	Yes	11/07/16	YES	YES	avaya-cs1000-cnd-4.0.48-1.el5.i386.000
63	Yes	11/07/16	NO	YES	libssh2-1.4.2-2.el5_7.1.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	[patched]
lhmonitor	7.65.16	
baseAppUtils	7.65.16	
dfoTools	7.65.16	[patched]
cppmUtil	n/a	[patched]
oam-logging	n/a	[patched]
dmWeb	n/a	[patched]
baseWeb	n/a	[patched]
ipsec	n/a	[patched]
Snmp-Daemon-TrapLib	n/a	[patched]
ISECSH	7.65.16	
patchWeb	n/a	[patched]
EmCentralLogic	7.65.16	

Application configuration: CS+SS+NRS+EM

Packages:

CS+SS+NRS+EM

Configuration version: 7.65.16-00

cs	7.65.16	[patched]
dbcom	7.65.16	[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	[patched]
sps	7.65.16	[patched]
ncs	7.65.16	
gk	7.65.16	[patched]
nrsrm	7.65.16	[patched]
nrsrmWebService	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]

©2018 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.