



Avaya Solution & Interoperability Test Lab

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

Abstract

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

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

1. Introduction

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

2. General Test Approach and Test Results

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

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

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming PSTN calls were made to Unistim, SIP, Digital and Analog telephones at the enterprise
- Incoming calls to the enterprise site from the PSTN routed to the DDI numbers assigned by Colt
- Outgoing calls from the enterprise to the PSTN were made from Unistim, SIP, Digital and Analog telephones
- Outgoing calls from the enterprise site completed via Colt to PSTN destinations
- Calls using the G.711A, G729 codec's supported by Colt
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using the T.38 mode
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls
- User features such as hold and resume, transfer, conference, call forwarding, etc
- Caller ID Presentation and Caller ID Restriction
- Call coverage and call forwarding for endpoints at the enterprise site
- Mobile-X call features
- Off-net call forwarding and mobility (extension to mobile)

2.2. Test Results

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

- All unwanted MIME was stripped on outbound calls using the Adaptation Module in Session Manager
- No inbound toll free numbers were tested as none were available from the Service Provider
- No Emergency Services numbers tested as test calls to these numbers should be pre-arranged with the Operator

2.3. Support

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

For technical support on Colt products please contact the Colt authorized representative at:

www.colt.net

or

Colt Local Support numbers.

Austria	0800 880 990	Belgium	0800 507 01
Germany	0800 111 1230	France	0800 948 888
Italy	192090	Netherlands	0800 265 8023
Portugal	808 780 222	Spain	901 888400
Switzerland	0800 560 560	UK	0800 136 166

3. Reference Configuration

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

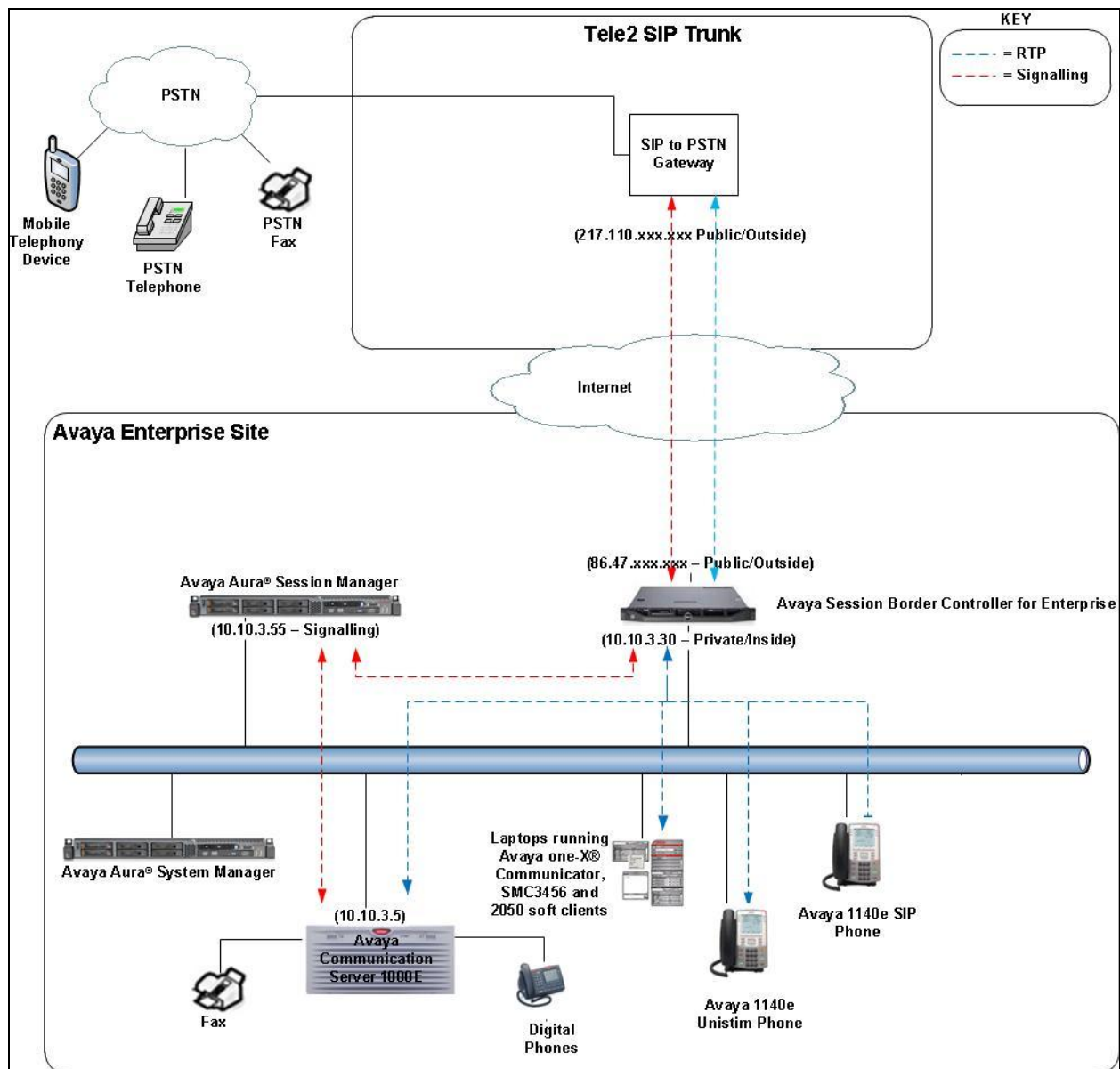


Figure 1: Test Setup Colt SIP Trunk Service to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Session Manager running on Avaya S8800 server	R6.2 Build: 6.2.2.0.622005
Avaya Aura® System Manager running on Avaya S8800 server	R6.2 Load: 6.2.0.0.15669 Service Pack 2
Avaya Communication Server 1000E running on CP+PM server as co-resident configuration	R7.5, Version 7.50.17 Service Update: 7.50_16Jul12 Deplist: X21 07.50Q
Avaya Session Border Controller for Enterprise on Dell R210 V2 server	Build: 4.0.5.Q09
Avaya Communication Server 1000E Media Gateway	CSP Version: MGCC CD02 MSP Version: MGCM AB01 APP Version: MGCA BA07 FPGA Version: MGCF AA18 BOOT Version: MGCB BA15 DSP1 Version: DSP1 AB04
Avaya 1140e and 1230 Unistim Telephones	FW: 0625C8A
Avaya 1140e and 1230 SIP Telephones	FW: 04.01.13.00.bin
Avaya SMC 3456	Version 2.6 build 53715
Avaya one-X® Communicator	Version cs6.1.0.10
Avaya Analogue Telephone	N/A
Avaya M3904 Digital Telephone	N/A
Colt SIP Trunk Service	Sonus GSX 9000 (SBC)8.4.2 Sonus PSX 8.4.2

5. Configure Avaya Communication Server 1000E

This section describes the steps required to configure CS1000E for SIP Trunking and also the necessary configuration for terminals (analog, SIP and IP phones). SIP trunks are established between CS1000E and Session Manager. These SIP trunks carry SIP Signaling associated with Colt SIP Trunk Service. For incoming calls, the Session Manager receives SIP messages from the Avaya SBCE; through which Colts SIP Service directs incoming SIP messages to CS1000E (see **Figure 1**). Once a SIP message arrives at CS1000E, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within CS1000E and may be first subject to outbound features such as route selection, digit manipulation and class of service restrictions. Once CS1000E selects a SIP trunk, the SIP signaling is routed to the Session Manager. The Session Manager directs the outbound SIP messages to the Avaya SBCE and on to Colts network. Specific CS1000E configuration was performed using Element Manager and the system terminal interface. The

general installation of the CS1000E, System Manager and Session Manager is presumed to have been previously completed and is not discussed here.

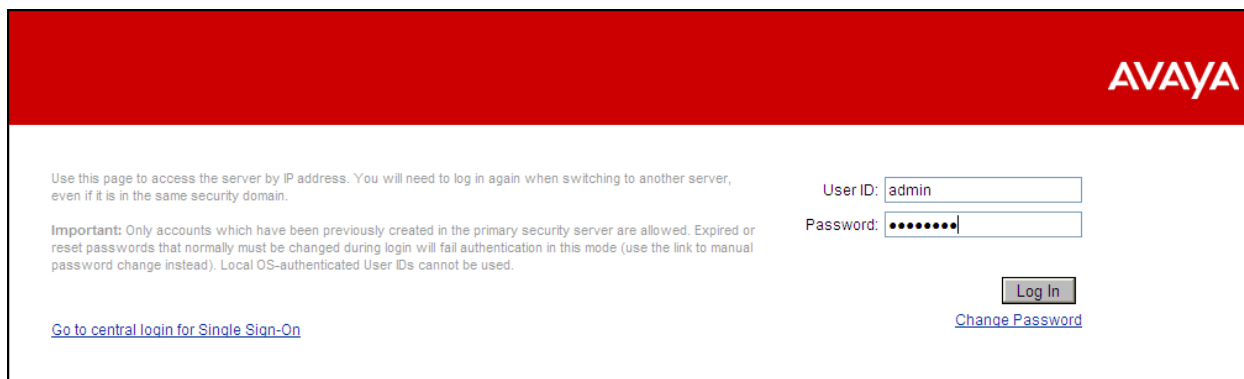
5.1. Log in to the Avaya Communication Server 1000E

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

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

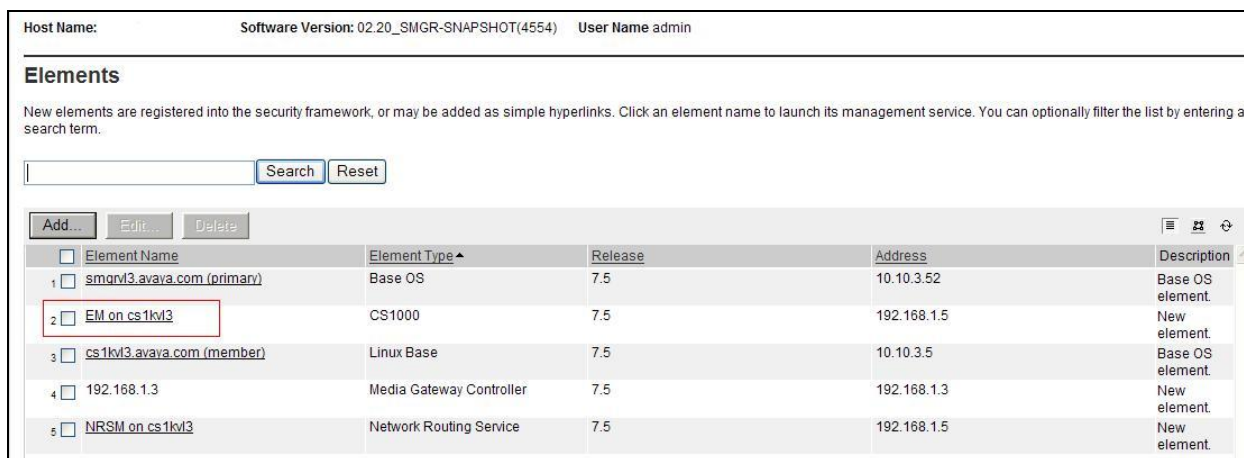
Log in using the web based Avaya Unified Communications Management GUI. The Avaya Unified Communications Management GUI may be launched directly via <http://<ipaddress>> where the relevant <ipaddress> is the TLAN ip address of the CS1000E.

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



The login screen features a red header with the AVAYA logo. Below the header, 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." To the right of this message are input fields for "User ID:" (containing "admin") and "Password:" (masked with dots). Below these fields are "Log In" and "Change Password" buttons. An "Important:" note states: "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." At the bottom left is a link: "Go to central login for Single Sign-On".

The Avaya Unified Communications Management Elements page will be used for configuration. Click on the Element Name corresponding to CS1000E in the Element Type column. In the abridged screen below, the user would click on the Element Name **EM on cs1kv13**.



The Elements page shows a table of system components. At the top, it displays "Host Name:", "Software Version: 02.20_SMGR-SNAPSHOT(4554)", and "User Name admin". Below the title "Elements", a message states: "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 bar with "Search" and "Reset" buttons. Below the search bar are "Add...", "Edit...", and "Delete" buttons. The table has columns: "Element Name", "Element Type", "Release", "Address", and "Description".

	Element Name	Element Type	Release	Address	Description
1	smgrv13.avaya.com (primary)	Base OS	7.5	10.10.3.52	Base OS element.
2	EM on cs1kv13	CS1000	7.5	192.168.1.5	New element.
3	cs1kv13.avaya.com (member)	Linux Base	7.5	10.10.3.5	Base OS element.
4	192.168.1.3	Media Gateway Controller	7.5	192.168.1.3	New element.
5	NRSM on cs1kv13	Network Routing Service	7.5	192.168.1.5	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 CS1000E system terminal and manually load overlay **LD 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 Colts network, and any other SIP trunks needed. See the following screenshot for a typical System Limits printout. The value of **SIP ACCESS PORTS** defines the maximum number of SIP trunks for the CS1000E.

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

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

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

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

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

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

5.3. Configure Codec's for Voice and FAX Operation

Colts SIP Trunk service supports G.711A and T.38 FAX transmissions. Using the CS1000E element manager sidebar, navigate to the **IP Network → IP Telephony Nodes → Node Details → VGW Gateway (VGW) and Codec's** property page and configure the CS1000E General codec settings as in the next screenshot

The screenshot shows the 'General' tab of the configuration page for Node ID: 100 - Voice Gateway (VGW) and Codecs. The page has three tabs: General, Voice Codecs, and Fax. The General tab is active. The following settings are highlighted with red boxes:

- Echo cancellation: ☒ Use canceller, with tail delay: 128 (dropdown)
- ☒ Dynamic attenuation
- Voice activity detection threshold: -17 (range: -20 - +10 DBM)
- Idle noise level: -65 (range: -327 - +327 DBM)
- Signaling options:
 - ☒ DTMF tone detection
 - ☐ Low latency mode
 - ☒ Remove DTMF delay (squelch DTMF from TDM to IP)
 - ☒ Modem/Fax pass-through
 - ☒ V.21 Fax tone detection
 - ☐ R factor calculation

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

The screenshot shows the 'Voice Codecs' tab of the configuration page for Node ID: 100 - Voice Gateway (VGW) and Codecs. The page has three tabs: General, Voice Codecs, and Fax. The Voice Codecs tab is active. The following settings are highlighted with a red box:

- Codec G711: ☒ Enabled (required)
- Voice payload size: 20 (milliseconds per frame)
- Voice playout (jitter buffer) delay: 40 (Nominal) 80 (Maximum) (milliseconds)

Below the highlighted settings, there is a note: "Maximum delay may be automatically adjusted based on nominal settings." and a checkbox for "Voice Activity Detection (VAD)" which is currently unchecked.

Next, scroll down and configure the **Codec G.729**. The relevant settings are highlighted in the following screenshot.

Managing: 192.168.1.5 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » VGW and Codecs

Node ID: 100 - Voice Gateway (VGW) and Codecs

General | Voice Codecs | Fax

Codec G729: ☒ Enabled

Voice payload size: 20 (milliseconds per frame)

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

Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

☐ Voice Activity Detection (VAD)

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

Managing: 192.168.1.5 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » VGW and Codecs

Node ID: 100 - Voice Gateway (VGW) and Codecs

General | Voice Codecs | Fax

Codec G723.1: ☐ Enabled

Voice payload size: 30 (milliseconds per frame)

Voice playout (jitter buffer) delay: 60 120 (milliseconds)

Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

Coding rate: 5.3 (kbps)

Fax

Codec name: T.38 FAX

Maximum rate: 14400 (bps)

Fax TCF method: 2

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

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

Packet size: 30 (bps)

5.4. Virtual Trunk Gateway Configuration

Use CS1000E Element Manager to configure the system node properties. Navigate to the **System → IP Networks → IP Telephony Nodes → Node Details** and verify the highlighted section is completed with the correct IP addresses and subnet masks of the Node. At this stage the call server has an IP address and so too does the signalling server. The Node IP (**10.10.3.6**) is the IP address that the IP phones use to register. This is also where the SIP trunk connection is made to the Session Manager. When an entity link is added in Session Manager for the CS1000E it is the Node IP that is used (please see **Section 6.5** – Define SIP Entities for more details).

Managing: 192.168.1.5 Username: admin
System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 100 - SIP Line, LTPS, Gateway (SIPGw))

Node ID:	<input type="text" value="100"/>	* (0-9999)	
Call server IP address:	<input type="text" value="192.168.1.5"/>	TLAN address type:	<input checked="" type="radio"/> IPv4 only <input type="radio"/> IPv4 and IPv6
Embedded LAN (ELAN)		Telephony LAN (TLAN)	
Gateway IP address:	<input type="text" value="192.168.1.1"/>	Node IPv4 address:	<input type="text" value="10.10.3.6"/>
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"/>

* Required Value.

Associated Signaling Servers & Cards

[Print](#) | [Refresh](#)

<input type="checkbox"/> Hostname ▲	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/> cs1kv3	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	192.168.1.5	10.10.3.5	Leader

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 outlined in **Section 6.2**.
- **Local SIP port:** The Local SIP Port is the port to which the gateway listens. The default value is **5060**.
- **Gateway endpoint name:** This field cannot be left blank so a value is needed here. This field is used when a Network Routing Server is used for registration of the endpoint. In this network a Session Manager is used so any value can be put in here and will not be used.
- **Application node ID:** This is a unique value that can be alphanumeric and is for the new Node that is being created, in this case **100**.
- **Proxy or Redirect Server:** Primary TLAN IP address is the Security Module IP address of the Session Manager. The **Transport protocol** used for **SIP**, in this case is TCP
- **SIP URI Map:** **Public National** and **Private Unknown** are left blank. All other fields in the SIP URI Map are left with default values.

Node ID: 100 - 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: *

Local SIP port: * (1 - 65535)

Gateway endpoint name: *

Gateway password: *

Application node ID: * (0-9999)

Enable failsafe NRS: ☐

SIP ANAT: ☒ IPv4

☐ IPv6

Virtual Trunk Network Health Monitor

☐ Monitor IP addresses (listed below)

Information will be captured for the IP addresses listed below.

Monitor IP:

Monitor addresses:

* Required Value.

Note: Changes made on this page will NOT be transmitted until the Node is also saved.

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

SIP URI Map:

Public E.164 domain names

National:

Subscriber:

Special number:

Unknown:

Private domain names

UDP:

CDP:

Special number:

Vacant number:

Unknown:

5.5. Configure Bandwidth Zones

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

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

Managing: 192.168.1.5 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 IDC table was configured to translate incoming PSTN numbers to five digit local telephone extension numbers. The digits of the actual PSTN DDI number are obscured for security reasons. The following screenshot shows the incoming PSTN numbers converted to local extension numbers. These were altered during testing to map to various SIP, Analog, Digital or Unistim telephones depending on the particular test case being executed.

Managing: 192.168.1.5 Username: admin
Dialing and Numbering Plans » Incoming Digit Translation » Customer 00 » Digit Conversion Tree 1 Configuration

Digit Conversion Tree 1 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 44207	5000		
2 44207	5001		
3 44207	5003		
4 44207	5004		
5 44207	5005		
6 44207	5006		

5.7. Configure SIP Trunks

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

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

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

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

Next, configure the SIP trunk Route Data Block (RDB) using the CS1000E system terminal and overlay 16. Load **Overlay 16**, enter **RDB** at the prompt, press return and commence configuration. The value for **DCH** is the same as previously entered in overlay 17. The value for **NODE** should match the node value in **Section 5.4**. The value for **ZONE** should match that used in **Section 5.5** for **VTRK (Zone 01)**. The remaining highlighted values are important for correct SIP trunk operation.

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

Next, configure virtual trunk members using the CS1000E system terminal and Overlay **LD 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 **LD 14** at the system terminal and type **new X**, where X is the required number of trunks. Continue entering data until the overlay exits. The **RTMB** value is a combination of the **ROUT** value entered in the previous step and the first trunk member (usually 1). The remaining highlighted values are important for correct SIP trunk operation.

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


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

```

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

```

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

```

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

```

```

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

ISET 0
NALT 5
MFRL 0
OVLL 0

```

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

TSC 00353	TSC 18	TSC 800	TSC 08
FLEN 0	FLEN 0	FLEN 0	FLEN 0
RRPA NO	RRPA NO	RRPA NO	RRPA NO
RLI 10	RLI 10	RLI 10	RLI 10
CCBA NO	CCBA NO	CCBA NO	CCBA NO

5.8. Configure Analog, Digital and IP Telephones

A variety of telephone types were used during the testing, the following is the configuration for the Avaya 1140e Unistim IP telephone. Load overlay **LD 20** at the system terminal and enter the following values. A unique four digit number is entered for the **KEY 00** and **KEY 01** value. The value for **CFG_ZONE** is the same value configured in **Section 5.5** for IP/SIP telephones (**Zone 02**).

Overlay 20 IP Telephone configuration

```
DES 1140
TN 100 0 01 0 VIRTUAL
TYPE 1140
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00002
CUR_ZONE 00002
ERL 0
ECL 0
FDN 0
TGAR 0
LDN NO
NCOS 0
SGRP 0
RNPG 1
SCI 0
SSU
LNRS 16
XLST
SCPW
SFLT NO
CAC_MFC 0
CLS UNR FBA WTA LPR PUA MTD FNA HTA TDD HFA CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LNA CNDA
CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
ICDA CDMD LLCN MCTD CLBD AUTR
GPUD DPUD DNDA CFXA ARHD FITD CLTD ASCD
CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
UDI RCC HBTA AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
DRDD EXR0
USMD USRD ULAD CCBF RTDD RBDD RBHD PGND OCBF FLXD FTTC DNDY DNO3 MCBN
FDSF 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 5000 0      MARP
      CPND
        CPND_LANG ROMAN
        NAME IP1140
        XPLN 10
        DISPLAY_FMT FIRST, LAST
01 MCR 5000 0
      CPND
        CPND_LANG ROMAN
        NAME IP1140
        XPLN 10
        DISPLAY_FMT FIRST, LAST
02
03 BSY
04 DSP
05
06
07
08
09
10
11
12
13
14
15
16
17 TRN
18 AO6
19 CFW 16
20 RGA
21 PRK
22 RNP
23
24 PRS
25 CHG
26 CPN
```

Digital telephones are configured using the overlay **LD20**, the following is a sample **3904** digital set configuration. Again, a unique number is entered for the **KEY 00** and **KEY 01** value.

Overlay 20 - Digital Set configuration

TYPE: 3904

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

---continued on next page---

---continued from previous page----

MLNG ENG

DNDR 0

KEY 00 MCR **5008** 0 MARP

CPND

CPND_LANG ROMAN

NAME Digital Set

XPLN 10

DISPLAY_FMT FIRST, LAST

01 MCR **5008** 0

CPND

CPND_LANG ROMAN

NAME Digital Set

XPLN 10

DISPLAY_FMT FIRST, LAST

02

03

04

05

06

07

08

09

10

11

12

13

14

15

16

17 TRN

18 AO6

19 CFW 16

20 RGA

21 PRK

22 RNP

23

24 PRS

25 CHG

26 CPN

27 CLT

28 RLT

29

30

31

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

Overlay 20 – Analog Telephone Configuration

```
DES 500
TN 04 0 03 00
TYPE 500
CDEN 4D
CUST 0
MRT

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

5.9. Configure the SIP Line Gateway Service

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

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

To configure the SIP Line Gateway Service, use Element Manager and navigate to the **IP Network → IP Telephony Nodes → Node Details → SIP Line Gateway Configuration** page. See the following screenshot for highlighted critical parameters.

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

The screenshot displays the CS1000 Element Manager interface. At the top, it shows 'Managing: 192.168.1.5 Username: admin' and a breadcrumb trail: 'System » IP Network » IP Telephony Nodes » Node Details » SIP Line Configuration'. The main heading is 'Node ID: 100 - SIP Line Configuration Details'. Below this, there are three tabs: 'General', 'SIP Line Gateway Settings', and 'SIP Line Gateway Service'. The 'SIP Line Gateway Service' tab is active, showing 'SIP Line Gateway Application: ☒ Enable gateway service on this node'. A red box highlights the 'General' section on the left, which contains the following fields: 'SIP domain name: avaya.com', 'SLG endpoint name: cs1kv13', 'SLG Group ID: [empty]', 'SLG Local Sip port: 5070 (1 - 65535)', and 'SLG Local Tls port: 5071 (1 - 65535)'. To the right of the 'General' section is the 'Virtual Trunk Network Health Monitor' section, which includes a checkbox for 'Monitor IP addresses (listed below)', a text area for 'Information will be captured for the IP addresses listed below.', a 'Monitor IP:' field with an 'Add' button, and a 'Monitor addresses:' field with a 'Remove' button.

5.10. Configure SIP Line Telephones

When SIP Line service configuration is completed, use the CS1000E system terminal and overlay **LD 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 configured for IP, SIP telephones (**Zone 02**) in **Section 5.5**. A unique telephone number is entered for value **KEY 00**. The value for **KEY 01** is comprised of the **UAPR** (set in **Section 5.9**) value and the telephone number used in **KEY 00**.

Overlay 20 – SIP Telephone Configuration

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

---continued on next page---

---continued from previous page---

```

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

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

5.11. Save Configuration

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

The screenshot shows the AVAYA CS1000 Element Manager web interface. On the left is a navigation tree with categories like 'Host and Route Tables', 'Network Address Translation', 'QoS Thresholds', 'Personal Directories', 'Unicode Name Directory', 'Interfaces', 'Engineered Values', 'Emergency Services', 'Software', 'Customers', 'Routes and Trunks', 'Dialing and Numbering Plans', 'Phones', and 'Tools'. The 'Tools' category is expanded, showing 'Backup and Restore' and 'Call Server'. The main content area is titled 'Call Server Backup'. It includes a breadcrumb trail: 'Managing: 192.168.1.5 Username: admin' followed by 'Tools » Backup and Restore » Call Server Backup and Restore » Call Server Backup'. Below the title, there is an 'Action' dropdown menu set to 'Backup', and two buttons: 'Submit' (highlighted with a red box) and 'Cancel'.

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.

```
Backing up reten.bkp to "/var/opt/nortel/cs/fs/cf2/backup/single"  
Database backup Complete!  
TEMU207  
Backup process to local Removable Media Device ended successfully.
```

Configuration of CS1000E is complete.

6. Configure Avaya Aura® Session Manager

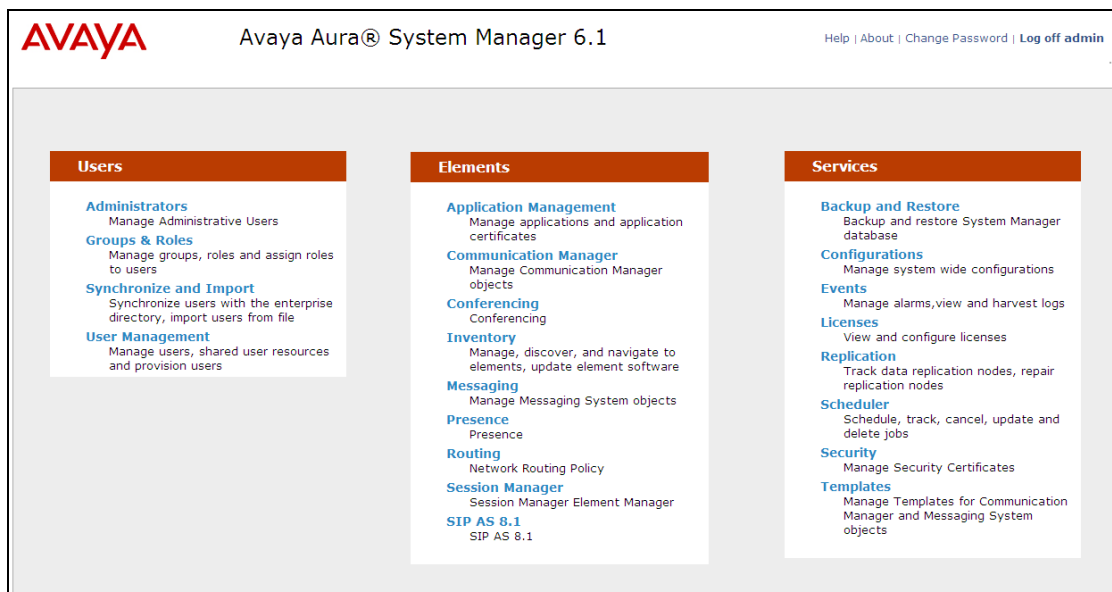
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

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

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

6.1. Avaya Aura® System Manager Login and Navigation

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



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.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Home

Home /Elements / Routing- Introduction to Network Routing Policy

Introduction to Network Routing Policy

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.

The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

- Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
- Step 2: Create "Locations"
- Step 3: Create "Adaptations"
- Step 4: Create "SIP Entities"

- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)

6.2. Define SIP Domain

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

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

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

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off

Routing x

Home /Elements / Routing / Domains- Domain Management

Domain Management

Warning: SIP Domain name change will cause login failure for Communication Address handles with this domain. Consult release notes or Support for steps to reset login credentials.

1 Item Refresh Filter: E

Name	Type	Default	Notes
* avaya.com	sip	<input type="checkbox"/>	

* Input Required

Commit

6.3. Define Location for Avaya Communication Server 1000E

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

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

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

In the **Location Pattern** section, click **Add** and enter the following values.

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

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

Home / Elements / Routing / Locations - Location Details

Location Details Help ? Commit Cancel

General

* Name:

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): Kbit/Sec

Minimum Multimedia Bandwidth: Kbit/Sec

* Default Audio Bandwidth: Kbit/sec

Location Pattern

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.10.3.*	<input type="text"/>

Select : All, None

* Input Required Commit Cancel

6.4. Configure Adaptation Module

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

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

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

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

Home / Elements / Routing / Adaptations- Adaptation Details

Adaptation Details

Help ?

Commit Cancel

General

* Adaptation name: COLT

Module name: DigitConversionAdaptor

Module parameter: MIME=no fromto=true

Egress URI Parameters:

Notes:

In the **Digit Conversion for Outgoing 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**

Digit Conversion for Outgoing Calls from SM

Add
Remove

1 Item Refresh
Filter: Enable

<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*00	*2	*36		*2	+	both ▼		

Select : All, None

* Input Required
Commit
Cancel

6.5. Define SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to the Session Manager. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown). The following will need to be entered for each SIP Entity.

Under **General**:

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

In this configuration there are three SIP Entities.

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

6.5.1. Avaya Aura® Session Manager SIP Entity

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

The screenshot shows the 'SIP Entity Details' configuration page for a Session Manager SIP Entity. The page has a breadcrumb trail at the top: 'Home / Elements / Routing / SIP Entities - SIP Entity Details'. On the left, there is a sidebar with 'SIP Entity Details' and 'General' (selected). A 'Commit' button is in the top right corner. The main form area contains the following fields:

- Name:** Session Manager
- FQDN or IP Address:** 10.10.3.55
- Type:** Session Manager (dropdown menu)
- Notes:** (empty text field)
- Location:** SMGRVL3 (dropdown menu)
- Outbound Proxy:** (empty dropdown menu)
- Time Zone:** Europe/Dublin (dropdown menu)
- Credential name:** (empty text field)
- SIP Link Monitoring:** Use Session Manager Configuration (dropdown menu)

At the bottom left of the sidebar, there is a link for 'SIP Link Monitoring'.

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

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

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

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

6.5.2. Avaya Aura® Communication Server 10000E SIP Entity

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

SIP Entity Details

General

* Name: CS1K

* FQDN or IP Address: 10.10.3.6

Type: Other

Notes:

Adaptation:

Location: SMGRVL3

Time Zone: Europe/Dublin

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

SIP Link Monitoring: Use Session Manager Configuration

6.5.3. Avaya Session Border Controller for Enterprise SIP Entities

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

The screenshot displays the 'SIP Entity Details' configuration page for 'Avaya SBCE'. The page has a breadcrumb trail at the top: 'Home / Elements / Routing / SIP Entities'. On the right, there are 'Commit' and 'Cancel' buttons, and a 'Help ?' link. The left sidebar shows 'General' as the active tab, with 'SIP Link Monitoring' below it. The main content area contains the following fields:

- Name:** Avaya SBCE
- FQDN or IP Address:** 10.10.3.30
- Type:** Gateway (dropdown)
- Notes:** (empty text field)
- Adaptation:** COLT (dropdown)
- Location:** SMGRVL3 (dropdown)
- Time Zone:** Europe/Dublin (dropdown)
- Override Port & Transport with DNS SRV:** ☐
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none (dropdown)
- SIP Link Monitoring:** Use Session Manager Configuration (dropdown)

6.6. Define Entity Links

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

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

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

Entity Link to CS1000E.

Home / Elements / Routing / Entity Links - Entity Links

Entity Links Help ? Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* CS1K	* Session Manager	TCP	* 5060	* CS1K	* 5060	Trusted	toCS1K

* Input Required Commit Cancel

Entity Link to Avaya SBCE.

Home / Elements / Routing / Entity Links

Entity Links Help ? Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* Avaya SBCE	* Session Manager	TCP	* 5060	* Avaya SBCE	* 5060	Trusted	

* Input Required Commit Cancel

6.7. Define Routing Policies

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

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

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

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

The following screenshot shows the Routing Policy for CS1000E.

Home / Elements / Routing / Routing Policies - Routing Policy Details

Routing Policy Details

Help ?

Commit Cancel

General

* Name: toCS1K

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CS1K	10.10.3.6	Other	

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

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

Home / Elements / Routing / Routing Policies

Routing Policy Details

Help ?

Commit Cancel

General

* Name: toAvaya SBCE

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Avaya SBCE	10.10.3.30	Gateway	

6.8. Define Dial Patterns

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

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

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

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

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

The first example shows that minimum **6** digit dialed numbers that begin with **442071** originating from **SMGRVL3** uses route policy **toCS1K**. This will allow DID numbers assigned to the enterprise from Colt SIP Trunk Service to route to CS1000E.

Home / Elements / Routing / Dial Patterns- Dial Pattern Details

Dial Pattern Details

Help ?

Commit Cancel

General

* Pattern: 442071

* Min: 6

* Max: 36

Emergency Call: ☐

SIP Domain: avaya.com

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh 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"/>	SMGRVL3		toCS1K	0	<input type="checkbox"/>	CS1K	

Select : All, None

The second example shows that a minimum **5** digit dialed numbers that begin with **00353** originating from **SMGRVL3** uses route policy **toAvaya SBCE**. This will allow outbound calls to route from the CS1000E to PSTN test numbers in the Avaya enterprise lab.

General

* Pattern: 00353

* Min: 5

* Max: 36

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

AddRemove

1 Item RefreshFilter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	SMGRVL3		toAvaya SBCE	0	<input type="checkbox"/>	Avaya SBCE	

Select : All, None

7. Configure Avaya Session Border Controller for Enterprise

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

7.1. Access Avaya Session Border Controller for Enterprise

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



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



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

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 10:17:32 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

- Welcome
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
- SIP Cluster
- Domain Policies
- Device Specific Settings
- Troubleshooting
- TLS Management
- IM Logging

Securing your real-time unified communications

A comprehensive IP Communications Security product, the Sipera UC-Sec offers a complete suite of security, enablement and compliance features for protecting and deploying unified communications such as Voice-over-IP (VoIP), instant messaging (IM), multimedia, and collaboration applications.

If you need support, please call our toll free number at (866) 861-3113 or e-mail support@sipera.com.

Alarms (Past 24 Hours)	Incidents (Past 24 Hours)
None found.	Sipera: Server Heartbeat is UP
	Sipera: Server Heartbeat is failed
	Sipera: Server Heartbeat is UP
	Sipera: Server Heartbeat is UP
	Sipera: Server Heartbeat is UP

Administrator Notes [Add]
No notes posted.

UC-Sec Devices	Network Type
Sipera	DMZ_ONLY

Quick Links

- Sipera Website
- Sipera VIPER Labs
- Contact Support

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

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 5:40:27 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

- Welcome
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
- SIP Cluster
- Domain Policies
- Device Specific Settings
- Troubleshooting
- TLS Management
- IM Logging

System Management

Installed Updates

Device Name	Serial Number	Version	Status
ASBCE	IPCS31020130	4.0.5.Q09	Commissioned

Icons: [Green Checkmark] [Red X] [Yellow Warning] [Monitor] [Pencil] [Red X]

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

System Information: GSSCP_03

Network Configuration

General Settings

Appliance Name	GSSCP_03
Box Type	SIP
Deployment Mode	Proxy

Device Settings

HA Mode	NO
Secure Channel Mode	NONE
Two Bypass Mode	NO

Network Settings

IP	Public IP	Netmask	Gateway	Interface
10.10.3.30	10.10.3.30	255.255.255.0	10.10.3.1	A1
86.47.xxx.xxx	86.47.xxx.xxx	255.255.255.128	86.47.xxx.xxx	B1

DNS Configuration

Primary DNS	8.8.8.8
Secondary DNS	
DNS Location	DMZ
DNS Client IP	86.47.xxx.xxx

Management IP(s)

IP	10.10.2.55
----	------------

7.2. Global Profiles

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

7.2.1. Server Interworking - Avaya Side

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

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

Click **Next** to continue.

Profile: SM3_CS	
General	
Hold Support	<input type="radio"/> None <input checked="" 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"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<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
Next	

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

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

DTMF	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO

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

Advanced Settings	
Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
SLIC Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>

7.2.2. Server Interworking – Colt Side

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

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

Click **Next** to continue.

Profile: SP_Trunk	
General	
Hold Support	<input type="radio"/> None <input checked="" 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 type="radio"/> None <input type="radio"/> SDP <input checked="" type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<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

Next

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

The screenshot shows a configuration window titled "Profile: SP_Trunk". It contains two main sections: "Privacy" and "DTMF".

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

DTMF	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO

At the bottom, there are two buttons: "Back" and "Finish".

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

The screenshot shows a configuration window titled "Profile: SP_Trunk" with the "Advanced Settings" section selected. It contains a list of settings with checkboxes or radio buttons.

Advanced Settings	
Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
SLIC Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>

At the bottom, there is a "Finish" button.

7.2.3. Routing

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

Create a Routing Profile for Session Manager and a Routing Profile for Colt SIP Trunk. To add a routing profile, navigate to **UC-Sec Control Center → Global Profiles → Routing** and select **Add Profile**. Enter a **Profile Name** and click **Next** to continue.

In the new window that appears, enter the following values. Use default values for all remaining fields:

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

Click **Finish**.

The following screen shows the Routing Profile to Session Manager. The **Next Hop Server 1** IP address must match the IP address of the Session Manager Security Module in **Section 9.2.3**.

Global Profiles > Routing: Call Server

Add Profile Rename Profile Clone Profile Delete Profile

Click here to add a description.

Routing Profile

Add Routing Rule

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	10.10.3.55	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TCP

The following screen shows the Routing Profile to Colt.

Global Profiles > Routing: Trunk Server

Add Profile

Routing Profiles

default

Call Server

Trunk Server

Rename Profile

Clone Profile

Delete Profile

Click here to add a description.

Routing Profile

Add Routing Rule

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport	
1	*	217.110.xxx.xxx	217.110.xxx.xxxx	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	UDP	

7.2.4. Server - Configuration

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

7.2.4.1 Server - Configuration – Avaya Side

To add a Server Configuration Profile for Session Manager navigate to **UC-Sec Control Center** → **Global Profiles** → **Server Configuration** and click on **Add Profile** (not shown). Enter name as **SM3_Call-Server**. In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Server Type:** Select **Call Server** from the drop-down box
- **IP Addresses / Supported FQDNs:** Enter the IP address of the Session Manager signaling interface. This should match the IP address of the Session Manager Security Module in **Section 9.2.3**
- **Supported Transports:** Select the transport protocol used to create the Avaya SBCE Entity Link on Session Manager in **Section 6.6**
- **TCP Port:** Port number on which to send SIP requests to Session Manager. This should match the port number used in the Avaya SBCE Entity Link on Session Manager in **Section 6.6**

Click **Finish** to continue.

Server Configuration Profile - General	
Server Type	Call Server
IP Addresses / Supported FQDNs Comma seperated list	10.10.3.55
Supported Transports	<input checked="" type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	5060
UDP Port	5060
TLS Port	
Finish	

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



Server Configuration Profile - Authentication	
Enable Authentication	<input type="checkbox"/>
User Name	<input type="text"/>
Realm	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
Finish	

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



Configuration Profile - Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SM3_CS
Signaling Manipulation Script	None
TCP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING
UDP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING
Finish	

7.2.4.2 Server - Configuration - Colt

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

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

Click **Finish** to continue.

The screenshot shows a window titled "Server Configuration Profile - General". It contains several fields for configuration:

- Server Type:** A dropdown menu with "Trunk Server" selected.
- IP Addresses / Supported FQDNs:** A text area with a comma-separated list: "217.110.xxx.xxx,217.110.xxx.xxx".
- Supported Transports:** Three checkboxes: "TCP" (unchecked), "UDP" (checked), and "TLS" (unchecked).
- TCP Port:** A text box, currently empty.
- UDP Port:** A text box containing the value "5060".
- TLS Port:** A text box, currently empty.

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

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

Server Configuration Profile - Authentication	
Enable Authentication	<input type="checkbox"/>
User Name	<input type="text"/>
Realm	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>

Finish

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

Server Configuration Profile - Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP_Trunk
Signaling Manipulation Script	None
UDP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING

Finish

7.2.5. Topology Hiding – Avaya Side

The **Topology Hiding** screen manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks. Navigate to **Global Profiles → Topology Hiding** (not shown).

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

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

Global Profiles > Topology Hiding: SM3_CS

Add Profile

Rename ProfileClone ProfileDelete Profile

Topology Hiding Profiles

default

cisco_th_profile

SM3_CS

SP_Trunk

Click here to add a description.

Topology Hiding

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

Edit

7.2.6. Topology Hiding – Colt Side

The **Topology Hiding** screen manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks. Navigate to **Global Profiles → Topology Hiding** (not shown).

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

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

Global Profiles > Topology Hiding: SP_Trunk

Add Profile

Rename Profile Clone Profile Delete Profile

Topology Hiding Profiles

default

cisco_th_profile

SM3_CS

SP_Trunk

Click here to add a description.

Topology Hiding

Header	Criteria	Replace Action	Overwrite Value
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Request-Line	IP/Domain	Next Hop	---
To	IP/Domain	Next Hop	---
From	IP/Domain	Next Hop	---
SDP	IP/Domain	Auto	---

Edit

7.3. Device Specific Settings

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

7.3.1. Network Management

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

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

IP Address	Public IP	Gateway	Interface
10.10.3.30		10.10.3.1	A1
86.47.xxx.xxx		86.47.xxx.xxx	B1

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

Name	Administrative Status	Toggle State
A1	Enabled	Toggle State
A2	Disabled	Toggle State
B1	Enabled	Toggle State
B2	Disabled	Toggle State

7.3.2. Media Interface

The Media Interface screen allows the IP address and ports to be set for transporting Media over the SIP trunk. The Avaya SBCE listens for SIP media on the defined ports.

To create a new Media Interface, navigate to **UC-Sec Control Center → Device Specific Settings → Media Interface** and click **Add Media Interface**

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

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

Device Specific Settings > Media Interface: GSSCP_03

UC-Sec Devices
GSSCP_03

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 Media Interface

Name	Media IP	Port Range		
Int_Media	10.10.3.30	35000 - 40000		
Ext_Media	86.47.xxx.xxx	35000 - 40000		

7.3.3. Signalling Interface

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

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

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

Device Specific Settings > Signaling Interface: GSSCP_03

UC-Sec Devices
GSSCP_03

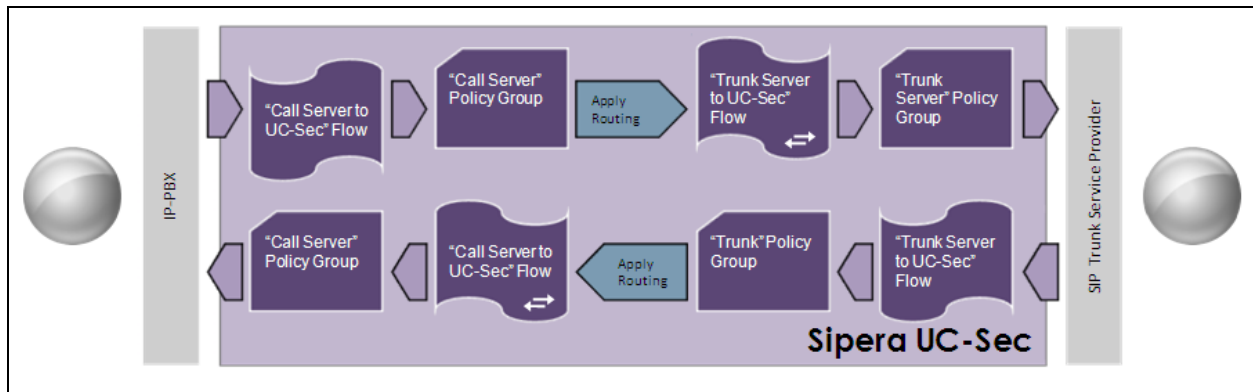
Signaling Interface

Add Signaling Interface

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Int_Sig	10.10.3.30	5060	5060	---	None		
Ext_Sig	86.47.xxx.xxx	5060	5060	---	None		

7.3.4. End Point Flows

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



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

- **Flow Name:** Enter a descriptive name
- **Server Configuration:** Select a Server Configuration created in **Section 7.2.4** to assign to the Flow
- **Received Interface:** Select the Signaling Interface the Server Configuration is allowed to receive SIP messages from
- **Signaling Interface:** Select the Signaling Interface used to communicate with the Server Configuration
- **Media Interface:** Select the Media Interface used to communicate with the Server Configuration.
- **End Point Policy Group:** Select the policy assigned to the Server Configuration
- **Routing Profile:** Select the profile the Server Configuration will use to route SIP messages to
- **Topology Hiding Profile:** Select the profile to apply toward the Server Configuration

Click **Finish** to save and exit.

The following screen shows the Sever Flow for Session Manager.

Flow: SM3_Call_Server	
Criteria	
Flow Name	SM3_Call_Server
Server Configuration	SM3_Call_Server
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig
Signaling Interface	Int_Sig
Media Interface	Int_Media
End Point Policy Group	default-low
Routing Profile	Trunk Server
Topology Hiding Profile	SM3_CS
File Transfer Profile	None
Finish	

The following screen shows the Sever Flow for Colt.

Flow: SP_Trunk_Server	
Criteria	
Flow Name	SP_Trunk_Server
Server Configuration	SP_Trunk_Server
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig
Signaling Interface	Ext_Sig
Media Interface	Ext_Media
End Point Policy Group	default-low
Routing Profile	Call Server
Topology Hiding Profile	SP_Trunk
File Transfer Profile	None
Finish	

8. Colt SIP Service Provider Configuration

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

9. Verification

9.1. Verify Avaya Communication Server 1000E Operational Status

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

The screenshot displays the AVAYA CS1000 Element Manager web interface. The left navigation pane shows the 'System' menu expanded, with 'Maintenance' selected. The main content area is titled 'Maintenance' and shows two selection methods: '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 lists 'D-Channel Diagnostics', 'MSDL Diagnostics', and 'TMDI Diagnostics'.

AVAYA CS1000 Element Manager																							
Navigation Pane: <ul style="list-style-type: none">- UCM Network Services- Home- Links- Virtual Terminals- System<ul style="list-style-type: none">- Alarms- Maintenance (selected)- Core Equipment- Peripheral Equipment- IP Network- Interfaces- Engineered Values- Emergency Services- Software- Customers- Routes and Trunks<ul style="list-style-type: none">- Routes and Trunks- D-Channels- Digital Trunk Interface- Dialing and Numbering Plans<ul style="list-style-type: none">- Electronic Switched Network- Flexible Code Restriction- Incoming Digit Translation- Phones<ul style="list-style-type: none">- Templates- Reports- Views- Lists- Properties- Migration	Main Content Area: <p>Managing: 192.168.1.5 Username: admin System > Maintenance</p> <p>Maintenance</p> <p><input checked="" type="radio"/> Select by Overlay <input type="radio"/> Select by Functionality</p> <table border="1"><caption><Select by Overlay></caption><tbody><tr><td>LD 30 - Network and Signaling</td></tr><tr><td>LD 32 - Network and Peripheral Equipment</td></tr><tr><td>LD 34 - Tone and Digit Switch</td></tr><tr><td>LD 36 - Trunk</td></tr><tr><td>LD 37 - Input/Output</td></tr><tr><td>LD 38 - Conference Circuit</td></tr><tr><td>LD 39 - Intergroup Switch and System Clock</td></tr><tr><td>LD 45 - Background Signaling and Switching</td></tr><tr><td>LD 46 - Multifrequency Sender</td></tr><tr><td>LD 48 - Link</td></tr><tr><td>LD 54 - Multifrequency Signaling</td></tr><tr><td>LD 60 - Digital Trunk Interface and Primary Rate Interface</td></tr><tr><td>LD 75 - Digital Trunk</td></tr><tr><td>LD 80 - Call Trace</td></tr><tr><td>LD 96 - D-Channel</td></tr><tr><td>LD 117 - Ethernet and Alarm Management</td></tr><tr><td>LD 135 - Core Common Equipment</td></tr><tr><td>LD 137 - Core Input/Output</td></tr><tr><td>LD 143 - Centralized Software Upgrade</td></tr></tbody></table> <table border="1"><caption><Select Group></caption><tbody><tr><td>D-Channel Diagnostics</td></tr><tr><td>MSDL Diagnostics</td></tr><tr><td>TMDI Diagnostics</td></tr></tbody></table>	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	D-Channel Diagnostics	MSDL Diagnostics	TMDI Diagnostics
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																							
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**

Managing: 192.168.1.5 Username: admin
System > Maintenance > D-Channel Diagnostics

D-Channel Diagnostics

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

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

STAT DCH

 Command executed successfully.

9.2. Verify Avaya Aura® Session Manager Operational Status

9.2.1. Verify Avaya Aura® Session Manager is Operational

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

• **Tests Pass** ✓

• **Security Module** Up

• **Service State** Accept New Service

Home / Elements / Session Manager- Session Manager

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

Service State: Up Shutdown System: Accept New Service As of 11:56 AM

Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Version
Session Manager	Core	0/0/2	✓	Up	Accept New Service	0/3	1	0	6.1.0.0.610023

Select : All, None

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.

Reset

Synchronize

Certificate Management ▾

Connection Status

1 Item

Refresh

Show

ALL ▾

Filter: Enable

	Details	Session Manager	Type	Status	Connections	IP Address	VLAN	Default Gateway	NIC Bonding	Entity Links (expected / actual)	Certificate Used
<div>C</div>	<div>► Show</div>	Session Manager	SM	Up	6	10.10.3.55/24	---	10.10.3.1	Disabled	3/3	SIP CA

Select : None

9.2.2. Verify SIP Entity Link Status

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

SIP Entity, Entity Link Connection Status							
This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.							
All Entity Links to SIP Entity: CS1K							
Summary View							
1 Item Refresh Filter: Enable							
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	Session Manager	10.10.3.6	5060	TCP	Up	200 OK	Up

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

SIP Entity, Entity Link Connection Status							
This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.							
All Entity Links to SIP Entity: Sipera							
Summary View							
1 Item Refresh Filter: Enable							
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	Session Manager	10.10.3.30	5060	TCP	Up	200 OK	Up

9.2.3. Verify Avaya Aura® Session Manager Instance

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

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

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

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

Home / Elements / Session Manager / Session Manager Administration - Session Manager Administration

Help ?

View Session Manager

Return

General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |
Expand All | Collapse All

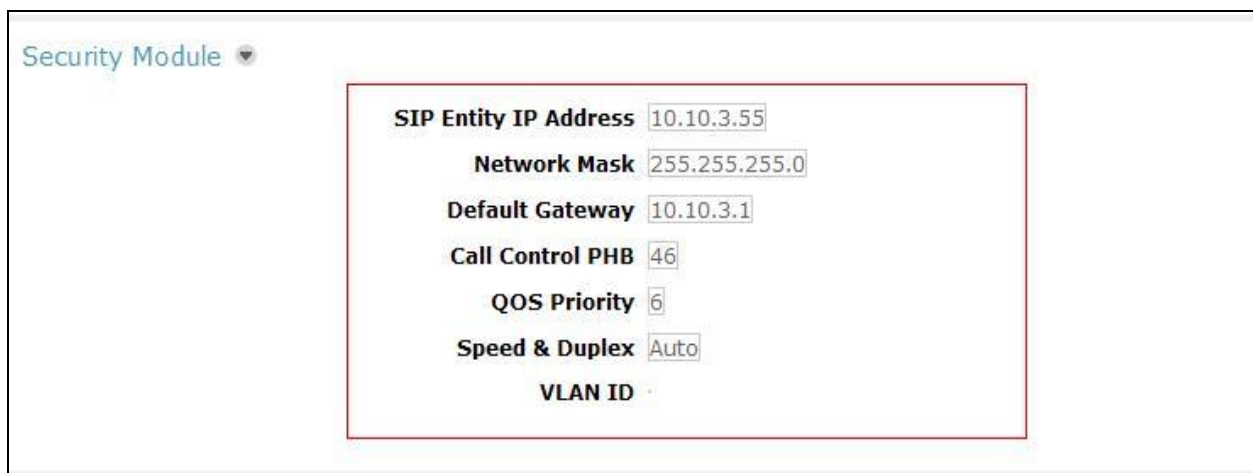
General ▾

SIP Entity Name	Session Manager
Description	Session Manager
Management Access Point Host Name/IP	10.10.3.54
Direct Routing to Endpoints	Enable

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

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

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



The screenshot displays the 'Security Module' configuration page. A red rectangular box highlights the following fields and their values:

Field	Value
SIP Entity IP Address	10.10.3.55
Network Mask	255.255.255.0
Default Gateway	10.10.3.1
Call Control PHB	46
QOS Priority	6
Speed & Duplex	Auto
VLAN ID	

10. Conclusion

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

11. Additional References

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

- [1] Avaya Aura® Session Manager Overview, Doc ID 03-603323, available at <http://support.avaya.com>
- [2] Installing and Configuring Avaya Aura® Session Manager, available at <http://support.avaya.com>.
- [3] Avaya Aura® Session Manager Case Studies, available at <http://support.avaya.com>
- [4] Maintaining and Troubleshooting Avaya Aura® Session Manager, Doc ID 03-603325, available at <http://support.avaya.com>
- [5] Administering Avaya Aura® Session Manager, Doc ID 03-603324, available at <http://support.avaya.com>
- [6] IP Peer Networking Installation and Commissioning, Release 7.5, Document Number NN43001-313, available at <http://support.avaya.com>
- [7] Network Routing Service Fundamentals, Release 7.5, Document Number NN43001-130, Issue 03.02, available at <http://support.avaya.com>
- [8] Co-resident Call Server and Signaling Server Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-509, available at <http://support.avaya.com>
- [9] Signaling Server and IP Line Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-125, available at <http://support.avaya.com>
- [10] E-SBC (Avaya Session Border Controller for Enterprise) Administration Guide, November 2011
- [11] RFC 3261 SIP: Session Initiation Protocol, <http://www.ietf.org/>

Appendix A – Avaya Communication Server 1000E Software

Avaya Communication Server 1000E call server patches and plug ins

TID: 46379

VERSION 4121

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

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

RELEASE 7

ISSUE 50 Q +

IDLE_SET_DISPLAY NORTEL

DepList 1: core Issue: 01(created: 2012-05-16 12:51:18 (est))

MDP>LAST SUCCESSFUL MDP REFRESH :2012-06-06 15:58:07(Local Time)

MDP>USING DEPLIST ZIP FILE DOWNLOADED :2012-06-06 11:11:47(est)

SYSTEM HAS NO USER SELECTED PEPS IN-SERVICE

LOADWARE VERSION: PSWV 100+

INSTALLED LOADWARE PEPS : 3

PAT#	CR #	PATCH REF #	NAME	DATE	FILENAME
00	wi00890367	ISS1:10F1	MGCCCD02	24/04/2012	MGCCCD02.LW
01	wi00832543	ISS1:10F1	DSP1AB04	24/04/2012	DSP1AB04.LW
02	wi00946113	ISS1:10F1	MGCBB15	24/04/2012	MGCBB15.LW

ENABLED PLUGINS : 0

Avaya Communication Server 1000E call server deplists

VERSION 4121

RELEASE 7

ISSUE 50 Q +

DepList 1: core Issue: 01 (created: 2012-05-16 12:51:18 (est))

IN-SERVICE PEPS

PAT#	CR #	PATCH REF #	NAME	DATE	FILENAME	SPECINS
000	wi00832106	ISS1:10F1	p30550_1	01/10/2012	p30550_1.cpl	NO
001	wi00835294	ISS1:10F1	p30565_1	01/10/2012	p30565_1.cpl	NO
002	wi00897176	ISS1:10F1	p30418_1	01/10/2012	p30418_1.cpl	NO
003	wi00925218	ISS1:10F1	p30675_1	01/10/2012	p30675_1.cpl	NO
004	wi00839821	ISS1:10F1	p30619_1	01/10/2012	p30619_1.cpl	NO
005	wi00937672	ISS1:10F1	p31276_1	01/10/2012	p31276_1.cpl	NO
006	wi00842409	ISS1:10F1	p30621_1	01/10/2012	p30621_1.cpl	NO
007	wi00838073	ISS1:10F1	p30588_1	01/10/2012	p30588_1.cpl	NO
008	wi00937114	ISS1:10F1	p31310_1	01/10/2012	p31310_1.cpl	NO
009	wi00841980	ISS1:10F1	p30618_1	01/10/2012	p30618_1.cpl	NO
010	wi00955753	ISS1:10F1	p31733_1	01/10/2012	p31733_1.cpl	NO
011	wi00839255	ISS1:10F1	p30591_1	01/10/2012	p30591_1.cpl	NO
012	wi00843623	ISS1:10F1	p30731_1	01/10/2012	p30731_1.cpl	YES
013	wi00843571	ISS1:10F1	p30627_1	01/10/2012	p30627_1.cpl	NO
014	wi00871739	ISS1:10F1	p30856_1	01/10/2012	p30856_1.cpl	NO
015	wi00852365	ISS1:10F1	p30707_1	01/10/2012	p30707_1.cpl	NO
016	wi00852389	ISS1:10F1	p30641_1	01/10/2012	p30641_1.cpl	NO
017	wi00839134	ISS1:10F1	p30698_1	01/10/2012	p30698_1.cpl	YES
018	wi00856702	ISS1:10F1	p30573_1	01/10/2012	p30573_1.cpl	NO
019	wi00857566	ISS1:10F1	p30766_1	01/10/2012	p30766_1.cpl	NO
020	wi00850521	ISS1:10F1	p30709_1	01/10/2012	p30709_1.cpl	YES

021	wi00903381	ISS1:10F1	p30421_1	01/10/2012	p30421_1.cpl	NO
022	wi00863876	ISS1:10F1	p30787_1	01/10/2012	p30787_1.cpl	NO
023	WI00853473	ISS1:10F1	p30625_1	01/10/2012	p30625_1.cpl	NO
024	wi00854130	ISS1:10F1	p30443_1	01/10/2012	p30443_1.cpl	NO
025	wi00875425	ISS1:10F1	p30943_1	01/10/2012	p30943_1.cpl	NO
026	wi00978883	ISS1:10F1	p31770_1	01/10/2012	p31770_1.cpl	NO
027	wi00875701	ISS1:10F1	p30942_1	01/10/2012	p30942_1.cpl	NO
028	wi00936935	ISS1:10F1	p31362_1	01/10/2012	p31362_1.cpl	NO
029	wi00877367	ISS1:10F1	p30534_1	01/10/2012	p30534_1.cpl	NO
030	wi00871969	ISS1:10F1	p30768_1	01/10/2012	p30768_1.cpl	NO
031	wi00886321	ISS1:10F1	p31009_1	01/10/2012	p31009_1.cpl	NO
032	WI00836334	ISS1:10F1	p30481_1	01/10/2012	p30481_1.cpl	NO
033	wi00836182	ISS1:10F1	p30450_1	01/10/2012	p30450_1.cpl	NO
034	wi00858335	ISS1:10F1	p30819_1	01/10/2012	p30819_1.cpl	NO
035	wi00860279	ISS1:10F1	p30789_1	01/10/2012	p30789_1.cpl	NO
036	wi00953900	ISS1:10F1	p31494_1	01/10/2012	p31494_1.cpl	NO
037	wi00854415	ISS1:10F1	p30593_1	01/10/2012	p30593_1.cpl	NO
038	WI00836292	ISS1:10F1	p30554_1	01/10/2012	p30554_1.cpl	NO
039	WI00839794	ISS1:10F1	p28647_1	01/10/2012	p28647_1.cpl	NO
040	wi00824257	ISS1:10F1	p30447_1	01/10/2012	p30447_1.cpl	NO
041	wi00827950	ISS2:10F1	p30471_2	01/10/2012	p30471_2.cpl	NO
042	wi00949273	ISS1:10F1	p31411_1	01/10/2012	p31411_1.cpl	NO
043	WI00854150	ISS1:10F1	p30468_1	01/10/2012	p30468_1.cpl	NO
044	wi00873382	ISS1:10F1	p30832_1	01/10/2012	p30832_1.cpl	NO
045	wi00853178	ISS1:10F1	p30719_1	01/10/2012	p30719_1.cpl	NO
046	wi00869695	ISS1:10F1	p30654_1	01/10/2012	p30654_1.cpl	NO
047	wi00834382	ISS1:10F1	p30548_1	01/10/2012	p30548_1.cpl	NO
048	wi00951427	ISS1:10F1	p31478_1	01/10/2012	p31478_1.cpl	NO
049	wi00946558	ISS1:10F1	p31358_1	01/10/2012	p31358_1.cpl	NO
050	wi00903369	ISS1:10F1	p31165_1	01/10/2012	p31165_1.cpl	NO
051	wi00927321	ISS1:10F1	p31286_1	01/10/2012	p31286_1.cpl	YES
052	wi00923899	ISS1:10F1	p31270_1	01/10/2012	p31270_1.cpl	NO
053	wi00949627	ISS1:10F1	p31462_1	01/10/2012	p31462_1.cpl	NO
054	wi00990993	ISS1:10F1	p31825_1	01/10/2012	p31825_1.cpl	NO
055	wi00865477	ISS1:10F1	p30894_1	01/10/2012	p30894_1.cpl	YES
056	wi00962211	ISS1:10F1	p31580_1	01/10/2012	p31580_1.cpl	NO
057	wi00883604	ISS1:10F1	p30973_1	01/10/2012	p30973_1.cpl	NO
058	wi00898327	ISS1:10F1	p31136_1	01/10/2012	p31136_1.cpl	NO
059	wi00856410	ISS1:10F1	p30749_1	01/10/2012	p30749_1.cpl	NO
060	wi00932948	ISS1:10F1	p31077_1	01/10/2012	p31077_1.cpl	NO
061	wi00905600	ISS1:10F1	p31201_1	01/10/2012	p31201_1.cpl	NO
062	wi00979591	ISS1:10F1	p31746_1	01/10/2012	p31746_1.cpl	NO
063	wi00879526	ISS1:10F1	p31007_1	01/10/2012	p31007_1.cpl	NO
064	wi00962955	ISS1:10F1	p31585_1	01/10/2012	p31585_1.cpl	NO
065	wi00984178	ISS1:10F1	p31786_1	01/10/2012	p31786_1.cpl	NO
066	wi00907707	ISS1:10F1	p31228_1	01/10/2012	p31228_1.cpl	NO
067	wi00857362	ISS1:10F1	p30782_1	01/10/2012	p30782_1.cpl	NO
068	wi00974635	ISS1:10F1	p31695_1	01/10/2012	p31695_1.cpl	YES
069	wi00894443	ISS1:10F1	p31093_1	01/10/2012	p31093_1.cpl	NO
070	wi00942734	ISS1:10F1	p31409_1	01/10/2012	p31409_1.cpl	NO
071	wi00841273	ISS1:10F1	p30713_1	01/10/2012	p30713_1.cpl	NO
072	wi00974272	ISS1:10F1	p31690_1	01/10/2012	p31690_1.cpl	YES
073	wi00948931	ISS1:10F1	p31407_1	01/10/2012	p31407_1.cpl	NO
074	wi00891626	ISS1:10F1	p31051_1	01/10/2012	p31051_1.cpl	YES
075	wi00929140	ISS1:10F1	p31284_1	01/10/2012	p31284_1.cpl	NO
076	wi00925208	ISS1:10F1	p30986_1	01/10/2012	p30986_1.cpl	NO
077	wi00958776	ISS1:10F1	p31542_1	01/10/2012	p31542_1.cpl	YES
078	wi00880836	ISS1:10F1	p30976_1	01/10/2012	p30976_1.cpl	NO
079	WI00927300	ISS1:10F1	p30999_1	01/10/2012	p30999_1.cpl	NO
080	wi00943172	ISS1:10F1	p31402_1	01/10/2012	p31402_1.cpl	NO
081	wi00826075	ISS1:10F1	p30452_1	01/10/2012	p30452_1.cpl	NO
082	wi00881777	ISS1:10F1	p25747_1	01/10/2012	p25747_1.cpl	NO
083	wi00948274	ISS1:10F1	p31365_1	01/10/2012	p31365_1.cpl	NO
084	wi00908933	ISS1:10F1	p31239_1	01/10/2012	p31239_1.cpl	NO
085	wi00865477	ISS1:10F1	p30892_1	01/10/2012	p30892_1.cpl	YES
086	wi00968531	ISS1:10F1	p31645_1	01/10/2012	p31645_1.cpl	NO
087	wi00961267	ISS1:10F1	p30288_1	01/10/2012	p30288_1.cpl	NO
088	wi00930864	ISS1:10F1	p31325_1	01/10/2012	p31325_1.cpl	NO
089	wi00898200	ISS1:10F1	p31274_1	01/10/2012	p31274_1.cpl	NO
090	wi00946876	ISS1:10F1	p31430_1	01/10/2012	p31430_1.cpl	NO

091	wi00936714	ISS1:10F1	p31379_1	01/10/2012	p31379_1.cpl	NO
092	wi00959457	ISS1:10F1	p31551_1	01/10/2012	p31551_1.cpl	NO
093	wi00969581	ISS1:10F1	p31661_1	01/10/2012	p31661_1.cpl	YES
094	wi00956885	ISS1:10F1	p31489_1	01/10/2012	p31489_1.cpl	NO
095	wi00973241	ISS1:10F1	p31715_1	01/10/2012	p31715_1.cpl	NO
096	wi00946282	ISS1:10F1	p31204_1	01/10/2012	p31204_1.cpl	NO
097	wi00840590	ISS1:10F1	p30767_1	01/10/2012	p30767_1.cpl	NO
098	wi00897082	ISS1:10F1	p31124_1	01/10/2012	p31124_1.cpl	NO
099	wi00896394	ISS1:10F1	p30807_1	01/10/2012	p30807_1.cpl	NO
100	wi00909476	ISS1:10F1	p31340_1	01/10/2012	p31340_1.cpl	NO
101	wi00887744	ISS2:10F1	p31026_2	01/10/2012	p31026_2.cpl	NO
102	wi00865477	ISS1:10F1	p30896_1	01/10/2012	p30896_1.cpl	YES
103	wi00957252	ISS1:10F1	p31530_1	01/10/2012	p31530_1.cpl	NO
104	wi00859123	ISS1:10F1	p30648_1	01/10/2012	p30648_1.cpl	NO
105	wi00895181	ISS1:10F1	p31106_1	01/10/2012	p31106_1.cpl	NO
106	wi00938555	ISS1:10F1	p30881_1	01/10/2012	p30881_1.cpl	YES
107	wi00993648	ISS1:10F1	p31867_1	01/10/2012	p31867_1.cpl	NO
108	wi00931028	ISS1:10F1	p31354_1	01/10/2012	p31354_1.cpl	YES
109	wi00907697	ISS1:10F1	p31227_1	01/10/2012	p31227_1.cpl	NO
110	wi00905660	ISS1:10F1	p27968_1	01/10/2012	p27968_1.cpl	NO
111	wi00900096	ISS1:10F1	p31006_1	01/10/2012	p31006_1.cpl	NO
112	wi00900766	ISS1:10F1	p31159_1	01/10/2012	p31159_1.cpl	NO
113	wi00865477	ISS1:10F1	p30898_1	01/10/2012	p30898_1.cpl	YES
114	wi00906022	ISS1:10F1	p31202_1	01/10/2012	p31202_1.cpl	NO
115	wi00856991	ISS1:10F1	p17588_1	01/10/2012	p17588_1.cpl	NO
116	wi00880386	ISS1:10F1	p30977_1	01/10/2012	p30977_1.cpl	NO
117	wi00688381	ISS1:10F1	p30104_1	01/10/2012	p30104_1.cpl	NO
118	wi00908598	ISS1:10F1	p31235_1	01/10/2012	p31235_1.cpl	NO
119	wi00890475	p30952	p31048_1	01/10/2012	p31048_1.cpl	NO
120	wi00868729	ISS1:10F1	p31163_1	01/10/2012	p31163_1.cpl	NO
121	wi00956788	ISS1:10F1	p31638_1	01/10/2012	p31638_1.cpl	NO
122	wi00859499	ISS1:10F1	p30694_1	01/10/2012	p30694_1.cpl	NO
123	wi00895090	ISS1:10F1	p31105_1	01/10/2012	p31105_1.cpl	NO
124	wi00869243	ISS1:10F1	p30848_1	01/10/2012	p30848_1.cpl	NO
125	wi00930649	ISS1:10F1	p31570_1	01/10/2012	p31570_1.cpl	NO
126	wi00899584	ISS1:10F1	p30809_1	01/10/2012	p30809_1.cpl	NO
127	wi00932204	ISS2:10F1	p31305_2	01/10/2012	p31305_2.cpl	NO
128	wi00951837	ISS1:10F1	p31485_1	01/10/2012	p31485_1.cpl	NO
129	wi00865477	ISS1:10F1	p30893_1	01/10/2012	p30893_1.cpl	YES
130	wi00946477	ISS1:10F1	p31426_1	01/10/2012	p31426_1.cpl	NO
131	wi00959284	ISS1:10F1	p31531_1	01/10/2012	p31531_1.cpl	NO
132	wi00855423	ISS1:10F1	p31328_1	01/10/2012	p31328_1.cpl	YES
133	wi00900668	ISS1:10F1	p30456_1	01/10/2012	p30456_1.cpl	NO
134	wi00862574	iss1:10f1	p30870_1	01/10/2012	p30870_1.cpl	NO
135	wi00894243	ISS1:10F1	p31087_1	01/10/2012	p31087_1.cpl	NO
136	wi00959820	ISS1:10F1	p31562_1	01/10/2012	p31562_1.cpl	NO
137	WI00889786	ISS1:10F1	p30750_1	01/10/2012	p30750_1.cpl	NO
138	wi00943748	ISS1:10F1	p31516_1	01/10/2012	p31516_1.cpl	NO
139	wi00959463	ISS1:10F1	p31528_1	01/10/2012	p31528_1.cpl	NO
140	WI00928455	ISS1:10F1	p31297_1	01/10/2012	p31297_1.cpl	NO
141	wi00896680	ISS1:10F1	p30357_1	01/10/2012	p30357_1.cpl	NO
142	wi00925141	ISS1:10F1	p30802_1	01/10/2012	p30802_1.cpl	NO
143	wi00968157	ISS1:10F1	p31637_1	01/10/2012	p31637_1.cpl	NO
144	wi00884699	ISS1:10F1	p31000_1	01/10/2012	p31000_1.cpl	YES
145	wi00932958	ISS1:10F1	p31115_1	01/10/2012	p31115_1.cpl	NO
146	wi00921295	ISS1:10F1	p31265_1	01/10/2012	p31265_1.cpl	NO
147	wi00906163	ISS1:10F1	p31205_1	01/10/2012	p31205_1.cpl	NO
148	wi00903437	ISS1:10F1	p31167_1	01/10/2012	p31167_1.cpl	NO
149	wi00960133	ISS2:10F1	p31557_2	01/10/2012	p31557_2.cpl	NO
150	wi00879322	ISS1:10F1	p30954_1	01/10/2012	p30954_1.cpl	NO
151	wi00896420	ISS1:10F1	p30867_1	01/10/2012	p30867_1.cpl	NO
152	wi00924886	ISS1:10F1	p31062_1	01/10/2012	p31062_1.cpl	YES
153	wi00877592	ISS1:10F1	p30880_1	01/10/2012	p30880_1.cpl	NO
154	wi00981711	ISS1:10F1	p31766_1	01/10/2012	p31766_1.cpl	NO
155	wi00882293	ISS1:10F1	p31010_1	01/10/2012	p31010_1.cpl	NO
156	wi00905297	ISS1:10F1	p31195_1	01/10/2012	p31195_1.cpl	NO
157	wi00968353	ISS1:10F1	p31412_1	01/10/2012	p31412_1.cpl	NO
158	wi00975133	ISS1:10F1	p31731_1	01/10/2012	p31731_1.cpl	NO
159	wi00897096	ISS1:10F1	p30676_1	01/10/2012	p30676_1.cpl	NO
160	wi00969890	ISS1:10F1	p31664_1	01/10/2012	p31664_1.cpl	YES

161	wi00967510	ISS1:10F1	p31147_1	01/10/2012	p31147_1.cpl	NO
162	wi00891621	ISS1:10F1	p31037_1	01/10/2012	p31037_1.cpl	NO
163	wi00968448	ISS1:10F1	p31648_1	01/10/2012	p31648_1.cpl	YES
164	wi00945997	ISS1:10F1	p31641_1	01/10/2012	p31641_1.cpl	NO
165	wi00967509	ISS1:10F1	p31294_1	01/10/2012	p31294_1.cpl	NO
166	wi00969208	ISS1:10F1	p31656_1	01/10/2012	p31656_1.cpl	NO
167	wi00976209	ISS1:10F1	p31717_1	01/10/2012	p31717_1.cpl	YES
168	wi00969039	ISS1:10F1	p31643_1	01/10/2012	p31643_1.cpl	NO
169	wi00977436	ISS1:10F1	p31834_1	01/10/2012	p31834_1.cpl	NO
170	wi00950575	ISS1:10F1	p31724_1	01/10/2012	p31724_1.cpl	NO
171	wi00975659	ISS1:10F1	p31707_1	01/10/2012	p31707_1.cpl	NO
172	wi00949410	ISS1:10F1	p31248_1	01/10/2012	p31248_1.cpl	NO
173	wi00977978	ISS1:10F1	p31831_1	01/10/2012	p31831_1.cpl	NO
174	wi00965285	ISS1:10F1	p31476_1	01/10/2012	p31476_1.cpl	NO
175	wi00979414	ISS1:10F1	p31748_1	01/10/2012	p31748_1.cpl	YES
176	wi00982243	ISS1:10F1	p31797_1	01/10/2012	p31797_1.cpl	NO
177	wi00960809	ISS1:10F1	p31564_1	01/10/2012	p31564_1.cpl	NO
178	wi00964006	ISS1:10F1	p31595_1	01/10/2012	p31595_1.cpl	YES
179	wi00965838	ISS1:10F1	p31623_1	01/10/2012	p31623_1.cpl	NO
180	wi00977393	ISS1:10F1	p31744_1	01/10/2012	p31744_1.cpl	YES
181	wi00994044	ISS1:10F1	p31871_1	01/10/2012	p31871_1.cpl	NO
182	wi00988285	ISS1:10F1	p31824_1	01/10/2012	p31824_1.cpl	NO
183	wi00982566	ISS1:10F1	p31774_1	01/10/2012	p31774_1.cpl	NO
184	wi00906350	ISS1:10F1	p31219_1	01/10/2012	p31219_1.cpl	NO
185	wi00983007	ISS1:10F1	p31778_1	01/10/2012	p31778_1.cpl	YES
186	wi00998121	ISS1:10F1	p31897_1	01/10/2012	p31897_1.cpl	NO
187	wi01003999	ISS1:10F1	p31946_1	01/10/2012	p31946_1.cpl	YES
188	wi00973270	ISS1:10F1	p31751_1	01/10/2012	p31751_1.cpl	NO
189	wi00992974	ISS1:10F1	p31889_1	01/10/2012	p31889_1.cpl	NO
190	wi00989828	ISS1:10F1	p31836_1	01/10/2012	p31836_1.cpl	NO
191	wi00985153	ISS1:10F1	p31859_1	01/10/2012	p31859_1.cpl	NO
192	wi00996639	ISS1:10F1	p31886_1	01/10/2012	p31886_1.cpl	NO
193	wi00944019	ISS1:10F1	p31874_1	01/10/2012	p31874_1.cpl	NO
194	wi00971029	ISS1:10F1	p31794_1	01/10/2012	p31794_1.cpl	NO
195	wi00971209	ISS1:10F1	p31750_1	01/10/2012	p31750_1.cpl	NO
196	wi00986337	ISS1:10F1	p31803_1	01/10/2012	p31803_1.cpl	NO
197	wi00991892	ISS1:10F1	p31853_1	01/10/2012	p31853_1.cpl	NO
198	wi00983505	ISS1:10F1	p31758_1	01/10/2012	p31758_1.cpl	NO
199	wi00996630	ISS1:10F1	p31789_1	01/10/2012	p31789_1.cpl	NO
200	wi00984652	ISS1:10F1	p31792_1	01/10/2012	p31792_1.cpl	NO
201	wi00974856	ISS1:10F1	p31823_1	01/10/2012	p31823_1.cpl	NO
202	wi00967512	ISS1:10F1	p31384_1	01/10/2012	p31384_1.cpl	NO
203	wi00957235	ISS1:10F1	p31798_1	01/10/2012	p31798_1.cpl	NO
204	wi00991523	ISS1:10F1	p31603_1	01/10/2012	p31603_1.cpl	NO
205	wi00984888	ISS1:10F1	p31795_1	01/10/2012	p31795_1.cpl	NO
206	wi00997559	ISS1:10F1	p31898_1	01/10/2012	p31898_1.cpl	NO
207	wi00980476	ISS1:10F1	p31387_1	01/10/2012	p31387_1.cpl	NO
208	wi00987089	ISS1:10F1	p31809_1	01/10/2012	p31809_1.cpl	NO
209	wi00985760	ISS1:10F1	p31913_1	01/10/2012	p31913_1.cpl	NO
210	wi00981928	ISS1:10F1	p31869_1	01/10/2012	p31869_1.cpl	NO
211	wi00987424	ISS1:10F1	p31815_1	01/10/2012	p31815_1.cpl	NO
212	wi00992921	ISS1:10F1	p31878_1	01/10/2012	p31878_1.cpl	NO
213	wi00993377	ISS1:10F1	p31860_1	01/10/2012	p31860_1.cpl	NO
214	wi00978064	ISS1:10F1	p31760_1	01/10/2012	p31760_1.cpl	NO

MDP>LAST SUCCESSFUL MDP REFRESH :2012-06-06 15:58:07 (Local Time)

MDP>USING DEPLIST ZIP FILE DOWNLOADED :2012-06-06 11:11:47(est)

Avaya Communication Server 1000E signaling server service updates

Product Release: 7.50.17.00

In system patches: 1

PATCH#	NAME	IN_SERVICE	DATE	SPECINS	TYPE	RPM
2	p30260_1	No	15/06/12	NO	FRU	cs1000-pi-control-1.00.00.00-00.noarch

In System service updates: 26

PATCH#	IN_SERVICE	DATE	SPECINS	REMOVABLE	NAME
0	No	06/06/12	NO	YES	cs1000-tps-7.50.17.16-19.i386.000
1	Yes	27/03/12	NO	YES	cs1000-ftrpkg-7.50.17.16-9.i386.000
3	Yes	01/03/12	NO	YES	cs1000-csmWeb-7.50.17.16-3.i386.000
4	Yes	18/04/11	NO	YES	cs1000-dbcom-7.50.17-02.i386.000
5	Yes	01/03/12	NO	YES	cs1000-mscAnnc-7.50.17.16-1.i386.000
6	Yes	01/03/12	NO	YES	cs1000-mscTone-7.50.17.16-1.i386.000
7	Yes	01/03/12	NO	YES	cs1000-mscMusc-7.50.17.16-2.i386.000
8	Yes	21/06/12	NO	YES	cs1000-vtrk-7.50.17.16-64.i386.000
11	Yes	17/01/12	NO	YES	cs1000-baseWeb-7.50.17.16-1.i386.001
12	Yes	17/01/12	NO	YES	cs1000-shared-pbx-7.50.17.16-1.i386.000
13	Yes	17/01/12	NO	YES	cs1000-kcv-7.50.17.16-1.i386.000
14	Yes	27/03/12	NO	YES	cs1000-sps-7.50.17.16-4.i386.000
15	Yes	17/01/12	NO	YES	cs1000-ipsec-7.50.17.16-1.i386.000
19	Yes	17/01/12	NO	YES	ipsec-tools-0.6.5-14.el5.3_avaya_1.i386.000
20	Yes	17/01/12	NO	YES	spiritAgent-6.1-1.0.0.108.208.i386.000
23	No	06/06/12	NO	YES	cs1000-pd-7.50.17.16-1.i386.000
24	Yes	06/06/12	NO	YES	cs1000-patchWeb-7.50.17.16-6.i386.000
25	No	06/06/12	NO	YES	cs1000-csmWeb-7.50.17.16-4.i386.000
26	Yes	06/06/12	NO	YES	cs1000-linuxbase-7.50.17.16-10.i386.000
27	Yes	06/06/12	NO	YES	cs1000-ncs-7.50.17.16-1.i386.000
28	Yes	06/06/12	NO	YES	cs1000-bcc-7.50.17.16-62.i386.000
29	Yes	06/06/12	NO	YES	cs1000-dmWeb-7.50.17.16-3.i386.000
30	Yes	06/06/12	NO	YES	cs1000-Jboss-Quantum-7.50.17.16-24.i386.000
31	Yes	06/06/12	NO	YES	cs1000-EmCentralLogic-7.50.17.16-2.i386.000
32	Yes	06/06/12	NO	YES	cs1000-emWeb_6-0-7.50.17.16-27.i386.000
33	Yes	06/06/12	NO	YES	cs1000-emWebLocal_6-0-7.50.17.16-1.i386.000

Avaya Communication Server 1000E system software

Product Release: 7.50.17.00

Base Applications

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

Application configuration: CS+SS+EM

Packages:

CS+SS+EM

Configuration version:	7.50.17-00
cs	7.50.17
dbcom	7.50.17
cslogin	7.50.17
sigServerShare	7.50.17
csv	7.50.17

tps	7.50.17.16	
vtrk	7.50.17.16	[patched]
pd	7.50.17.16	
sps	7.50.17.16	[patched]
ncs	7.50.17.16	[patched]
gk	7.50.17	
EmConfig	7.50.17	
emWeb 6-0	7.50.17	[patched]
emWebLocal_6-0	7.50.17	[patched]
csmWeb	n/a	[patched]
bcc	7.50.17	[patched]
ftrpkg	7.50.17	[patched]
cs1000WebService_6-0	7.50.17	
managedElementWebService	7.50.17	
mscAnnc	7.50.17.16	[patched]
mscAttn	7.50.17	
mscConf	7.50.17	
mscMusc	7.50.17.16	[patched]
mscTone	7.50.17.16	[patched]

©2012 Avaya Inc. All Rights Reserved.

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

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