



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Communication Server 1000E R7.6, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise to support KPN VaMo1 VoIP Connect Service – Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the KPN VaMo1 VoIP Connect service and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Session Border Controller Advanced for Enterprise, Avaya Aura® Session Manager and Avaya Communication Server 1000E. KPN is a member of the DevConnect 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 used to configure Session Initiation Protocol (SIP) trunking between KPN VaMo1 VoIP Connect service and an Avaya SIP-enabled Enterprise Solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise (Avaya SBCE), Avaya Aura® Session Manager and Avaya Communication Server 1000E (CS1000E). Customers using this Avaya SIP-enabled enterprise solution with KPN VaMo1 VoIP Connect service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise customer.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of CS1000E, Session Manager and Avaya SBCE. The enterprise site was configured to use the VaMo1 VoIP Connect service provided by KPN.

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

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from the PSTN routed to the DDI numbers assigned by KPN
- Incoming PSTN calls made to SIP, UniStim, Digital and Analog telephones at the enterprise
- Outgoing calls from the enterprise site completed via KPN to PSTN destinations
- Outgoing calls from the enterprise to the PSTN made from SIP, UniStim, Digital and Analog telephones
- Calls using the G.711A codec supported by KPN
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using T.38
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction
- Call coverage and call forwarding for endpoints at the enterprise site
- Transmission and response of SIP OPTIONS messages sent by KPN requiring Avaya response and sent by Avaya requiring KPN response
- 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 KPN VaMo1 VoIP Connect service with the following observations:

- As KPN do not support SIP UPDATE, the CS1000E default configuration will not allow a blind transfer to be executed if the parties involved do not support the SIP UPDATE method. With the installation of plugin 501 on the CS1000E, the blind transfer will be allowed and the call will be completed. The limitation of this plugin is that no ringback is provided to the originator of the call for the duration that the destination set is ringing. In addition to plugin 501, it is required that **VTRK SU version “cs1000-vtrk-7.50.17.16-15.i386.000.ntl”** or higher be used on all SSG signaling servers to ensure proper operation of the blind transfer feature. The use of plugin 501 does not restrict the use of the SIP UPDATE method of blind transfer to other parties that do happen to support the UPATE method, but rather extend support to those parties that do not
- 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
- All unwanted MIME was stripped on outbound calls using the Adaptation Module in Session Manager

2.3. Support

For technical support on KPN products please visit the website at www.kpn.nl or contact an authorized KPN representative.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to the KPN VaMo1 VoIP Connect Service. Located at the Enterprise site is an Avaya SBCE, Session Manager and CS1000E. Endpoints are Avaya 1140 series IP telephones, Avaya 1200 series 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.

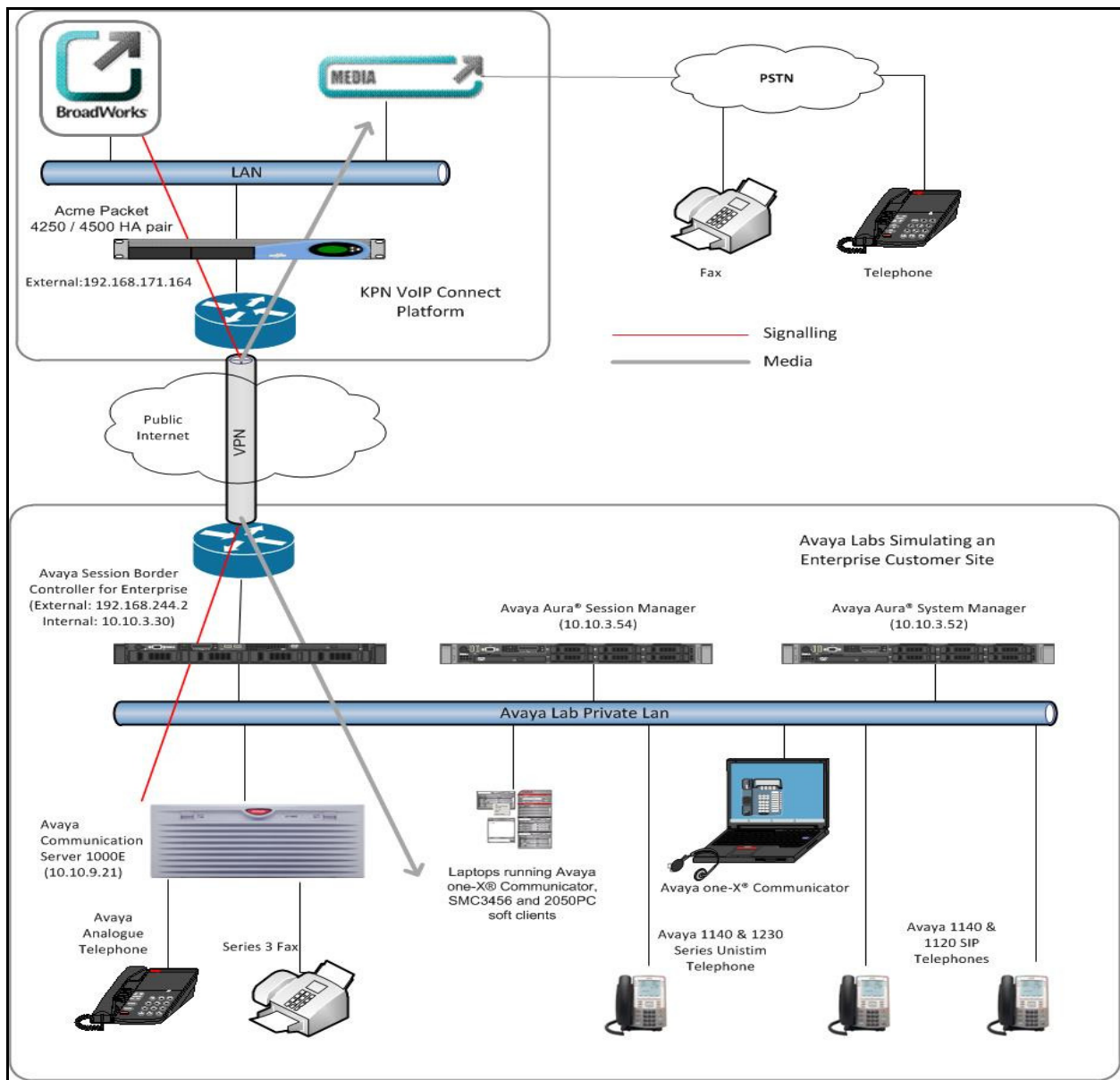


Figure 1: Test Setup KPN VaMo1 VoIP Connect to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment	Software
Avaya S8800 Media Server	Avaya Aura® Session Manager R6.3 Version – 6.3.3.0.633004
Avaya S8800 Media Server	Avaya Aura® System Manager R6.3.3.3 Build No. – 6.3.0.8.5682 – 6.3.8.1814
Dell R310 Server running Avaya Session Border Controller for Enterprise	Avaya Session Border Controller Advanced for Enterprise R6.2.0.Q48
Avaya Communication Server 1000E running on CP+PM server as co-resident configuration	Avaya Communication Server 1000E R7.6 Version 7.65.P Deplst: CPL_X21_07_65P All CS1000E patches listed in Appendix A
Avaya Communication Server 1000E Media Gateway	CSP Version: MGCC DC01 MSP Version: MGCM AB02 APP Version: MGCA BA18 FPGA Version: MGCF AA22 BOOT Version: MGCB BA18 DSP1 Version: DSP2 AB07
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 2050PC	Release 4.3.0081
Avaya Analog Telephone	N/A
Avaya M3904 Digital Telephone	N/A
KPN Equipment	Software
as1-sbc-s-2-1 ACME Net-Net 4500	SCX6.2.0 MR-6 Patch 2 (Build 876)
as1-sbc-s-1-1 ACME Net-Net 4250	SC6.2.0 MR-6 Patch 2 (Build 876)
Alcatel-Lucent-HPSS	v3.0.3
Broadsoft	v 17

5. Configure Avaya Communication Server 1000E

This section describes the steps for configuring Communication Server 1000E for SIP Trunking. SIP trunks are established between Communication Server 1000E and Session Manager. These SIP trunks will carry SIP Signalling associated with the KPNVaMo1 VoIP Connect Service. For incoming calls, the Session Manager receives SIP messages from the Avaya SBCE and directs the incoming SIP messages to Communication Server 1000E. Once the message arrives at Communication Server 1000E, 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 Communication Server 1000E and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Server 1000E selects a SIP trunk, the SIP signaling is routed to the Session Manager. The Session Manager directs the outbound SIP messages to the Session Border Controller at the enterprise site that then sends the SIP messages to the KPN network. Specific Communication Server 1000E configuration was performed using Element Manager and the system terminal interface. The general installation of the Communication Server 1000E, System Manager and Session Manager is presumed to have been previously completed and is not discussed here. **Appendix A** has a list of all CS1000E patches, deplist and service packs loaded on the system.

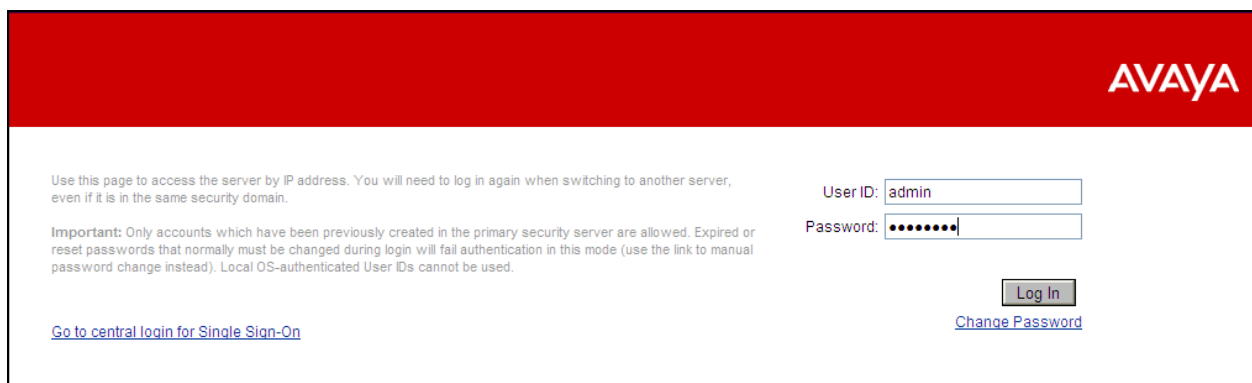
5.1. Logging into the Avaya Communication Server 1000E

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

Log in using SSH to the ELAN IP address of the Call Server 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 image shows the Avaya login web interface. At the top is a red header with the 'AVAYA' logo in white. Below the header, on the left, is a block of text: '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.' followed by an 'Important' note about account creation and password changes. On the right side, there are two input fields: 'User ID:' with 'admin' entered, and 'Password:' with masked characters. Below these fields is a 'Log In' button and a 'Change Password' link. At the bottom left, there is a link that says '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 cs1kv19**.

Host Name: 10.10.9.57 User Name: admin

Elements

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

<input type="checkbox"/>	Element Name	Element Type ▲	Release	Address	Description
1 <input type="checkbox"/>	smgrv9.avaya.com (primary)	Base OS	7.6	10.10.9.57	Base OS element.
2 <input type="checkbox"/>	EM on cs1kv19	CS1000	7.6	192.168.27.2	New element.
3 <input type="checkbox"/>	cs1kv19.avaya.com (member)	Linux Base	7.6	86.47.122.35	Base OS element.
4 <input type="checkbox"/>	192.168.27.3	Media Gateway Controller	7.6	192.168.27.3	New element.
5 <input type="checkbox"/>	NRSM on cs1kv19	Network Routing Service	7.6	192.168.27.2	New element.

5.2. Confirm System Features

The keycode installed on the Call Server controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity. Use the Communication Server 1000E system terminal and manually **load Overlay 22** to print the System Limits (the required command is **SLT**) and verify that the number of SIP Access Ports reported by the system is sufficient for the combination of trunks to KPN's 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 Communication Server 1000E.

```
Load Overlay 22
req: SLT

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      32767 LEFT 32752 USED 15
```

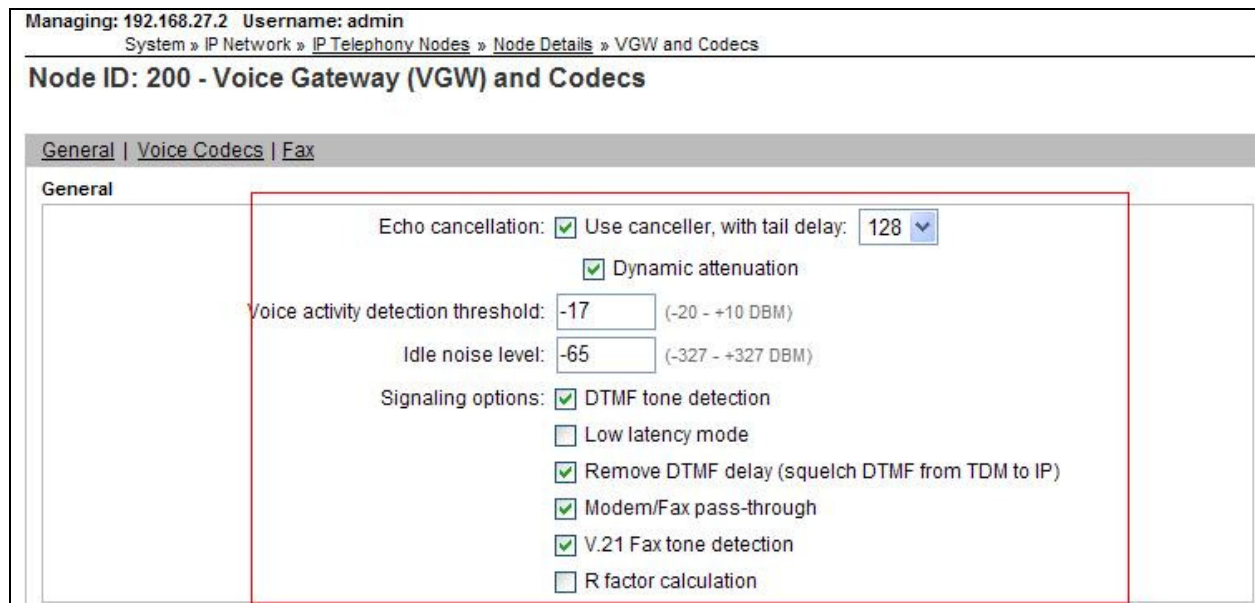
Load Overlay 21 and confirm the customer is setup to use **ISDN** trunks by typing the **PRT** and **NET_DATA** commands as shown below.

```
Load Overlay 21
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

KPN's SIP Trunk service supports G.711A voice codec and T.38 FAX transmissions. Using the Communication Server 1000E element manager sidebar, navigate to the **IP Network → IP Telephony Nodes → Node Details → Voice Gateway (VGW) and Codecs** property page and configure the Communication Server 1000E General codec settings as shown in the screenshot below. The values highlighted are required for correct operation; most of the options are turned on by default but its good practice to ensure that they are set as shown below.



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

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

General | Voice Codecs | Fax

General

Echo cancellation: ☒ Use canceller, with tail delay: 128

☒ Dynamic attenuation

Voice activity detection threshold: -17 (-20 - +10 DBM)

Idle noise level: -65 (-327 - +327 DBM)

Signaling options: ☒ DTMF tone detection

☐ Low latency mode

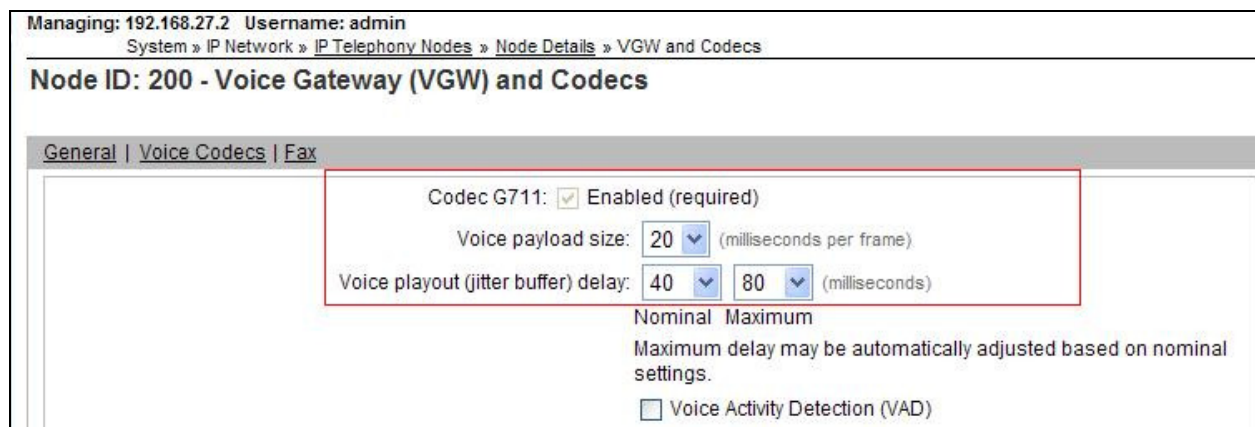
☒ Remove DTMF delay (squellch DTMF from TDM to IP)

☒ Modern/Fax pass-through

☒ V.21 Fax tone detection

☐ R factor calculation

Next, scroll down and configure the CS1000E to use **Codec G.711** only. Default values were configured. This aligns with what KPN support on their SIP network.



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

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

General | Voice Codecs | Fax

Codec G711: ☒ Enabled (required)

Voice payload size: 20 (milliseconds per frame)

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

Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

☐ Voice Activity Detection (VAD)

Finally, configure the **Fax** settings as in the highlighted section of the next screenshot with system defaults as shown below.

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 Communication Server 1000E 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 signaling server. The Node IPv4 address is the ip address that the IP phones use to register. This is also where the SIP trunk connection is made to the Session Manager. When an entity link is added in Session Manager for the CS1000E it is the Node IPv4 address that is used (see **Section 6.5 – Define SIP Entities** for more details).

Managing: 192.168.27.2 Username: admin

System » IP Network » IP Telephony Nodes » Node Details

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

Node ID: 200 * (0-9999)

Call server IP address: 192.168.27.2 *

TLAN address type: ☒ IPv4 only ☐ IPv4 and IPv6

Embedded LAN (ELAN)

Gateway IP address: 192.168.27.1 *

Telephony LAN (TLAN)

Node IPv4 address: 10.10.9.21 *

Subnet mask: 255.255.255.0 *

Node IPv6 address:

* Required Value.

Save Cancel

The next two screenshots show the SIP Virtual Trunk Gateway configuration, navigate to **System → IP Networks → IP Telephony Nodes → Node Details → Gateway (SIPGW) Virtual Trunk Configuration Details** and fill in the highlighted areas with the relevant settings.

- **Vtrk gateway application:** Provides option to select Gateway applications. The three supported modes are **SIP Gateway (SIPGw)**, **H.323Gw**, and **SIPGw and H.323Gw**
- **SIP domain name:** The SIP Domain Name is the SIP Service Domain. The SIP Domain Name configured in the Signaling Server properties must match the Service Domain name configured in the Session Manager, in this case **avaya.com**
- **Local SIP port:** The Local SIP Port is the port to which the gateway listens. The default value is **5060**
- **Gateway endpoint name:** This field cannot be left blank so a value is needed here. This field is used when a Network Routing Server is used for registration of the endpoint. In this network a Session Manager is used so any value can be put in here and will not be used
- **Application node ID:** This is a unique value that can be alphanumeric and is for the new Node that is being created, in this case **200**
- **Proxy or Redirect Server:** Primary TLAN IP address is the Security Module IP address of the Session Manager. The **Transport protocol** used for **SIP**, in this case is TCP
- **SIP URI Map:** **Public E.164 - National** and **Private - Unknown** are left blank. All other fields in the SIP URI Map are left with default values

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

Node ID: 200 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

Vtrk gateway application: ☒ Enable gateway service on this node

General

Vtrk gateway application: SIP Gateway (SIPGw) ▼

SIP domain name: avaya.com *

Local SIP port: 5060 * (1 - 65535)

Gateway endpoint name: cs1kv19 *

Gateway password: *

Application node ID: 200 * (0-9999)

Enable failsafe NRS: ☐

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

Virtual Trunk Network Health Monitor

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

Monitor IP: Add

Monitor addresses:

Remove

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	Private domain names
National: <input type="text" value=""/>	UDP: <input type="text" value="udp"/>
Subscriber: <input type="text" value="subscriber"/>	CDP: <input type="text" value="cdp.udp"/>
Special number: <input type="text" value="PublicSpecial"/>	Special number: <input type="text" value="PrivateSpecial"/>
Unknown: <input type="text" value="PublicUnknown"/>	Vacant number: <input type="text" value="PrivateUnknown"/>
	Unknown: <input type="text" value=""/>

5.5. Configure Bandwidth Zones

Bandwidth Zones are used for alternate call routing between IP stations and for Bandwidth Management. SIP trunks require a unique zone, not shared with other resources and best practice dictates that IP telephones and Media Gateways are all placed in separate zones. In the sample configuration SIP trunks use zone 01 and IP 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: 192.168.27.2 Username: admin
System » IP Network » Zones » Bandwidth Zones

Bandwidth Zones

[Add...](#) [Edit...](#) [Import...](#) [Export](#) [Maintenance...](#) [Delete](#)

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

5.6. Configure Incoming Digit Conversion Table

A limited number of Direct Dial Inwards (DDI) numbers were available. The 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: 192.168.27.2 Username: admin
Dialing and Numbering Plans » Incoming Digit Translation » Customer 00 » Digit Conversion Tree 0 Configuration

Digit Conversion Tree 0 Configuration

Regular IDC tree
Send calling party DID disabled

[Add...](#) [Delete IDC](#) [Delete IDC tree](#) [Refresh](#)

	Incoming Digits ▲	Converted Digits	CPND Name	CPND language
1	03024	6000		
2	03024	6002		
3	03024	6003		
4	03024	6003		
5	03024	6004		
6	03024	6005		

5.7. Configure SIP Trunks

Communication Server 1000E virtual trunks will be used for all inbound and outbound PSTN calls to KPN's SIP Trunk Service. Five separate steps are required to configure Communication Server 1000E virtual trunks:

- Configure a D-Channel Handler (DCH); configure using the Communication Server 1000E system terminal and overlay 17
- Configure a SIP trunk Route Data Block (RDB); configure using the Communication Server 1000E system terminal and overlay 16
- Configure SIP trunk members; configure using the Communication Server 1000E system terminal and overlay 14
- Configure a Route List Block (RLB); configure using the Communication Server 1000E system terminal and overlay 86
- Configure Special Prefix Numbers (SPN's); configure using the Communication Server 1000E system terminal and overlay 90

The following is an example DCH configuration for SIP trunks. **Load Overlay 17** at the Communication Server 1000E system terminal and enter the following values. The highlighted entries are required for correct SIP trunk operation. Exit overlay 17 when completed.

Load Overlay 17

```
ADAN      DCH 1
CTYP DCIP
DES  VIR_TRK
USR  ISLD
ISLM 4000
SSRC 1800
OTBF 32
NASA YES
IFC SL1
CNEG 1
RLS  ID  5
RCAP ND2
MBGA NO
H323
      OVLR NO
      OVLS NO
```

Next, configure the SIP trunk Route Data Block (RDB) using the Communication Server 1000E 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 **SIP_VTRK**. The remaining highlighted values are important for correct SIP trunk operation.

Load Overlay 16 TYPE: RDB CUST 00 ROUT 100 TYPE RDB CUST 00 ROUT 001 DES VIR_TRK TKTP TIE NPID_TBL_NUM 0 ESN NO RPA NO CNVT NO SAT NO RCLS EXT VTRK YES ZONE 00001 PCID SIP CRID NO NODE 200 DTRK NO ISDN YES MODE ISLD DCH 1 IFC SL1 PNI 00001 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 Communication Server 1000E system terminal and **Load Overlay 14**. Configure sufficient trunk members to carry both incoming and outgoing PSTN calls. The following example shows a single SIP trunk member configuration. **Load Overlay 14** at the system terminal and type **new X**, where *X* is the required number of trunks. Continue entering data until the overlay exits. The **RTMB** value is a combination of the **ROUT** value entered in the previous step and the first trunk member (usually 1). The remaining highlighted values are important for correct SIP trunk operation.

```
Load Overlay 14
new 30
TN 100 0 0 0
DATE
PAGE
DES VIR_TRK
TN 160 0 00 00 VIRTUAL
TYPE IPTI
CUST 0
XTRK VTRK
ZONE 00001
TIMP 600
BIMP 600
AUTO_BIMP NO
NMUS NO
TRK ANLG
NCOS 0
RTMB 100 1
CHID 1
TGAR 1
STRI/STRO WNK WNK
SUPN YES
AST NO
IAPG 0
CLS UNR DIP CND ECD WTA LPR APN THFD XREP SPCD MSBT
P10 NTC
TKID
AACR NO
```


Next, configure a Digit Manipulation data block (DGT) in overlay 86. Load **Overlay 86** at the system terminal and type **new**. The following example shows the values used. 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 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.

<pre> Load Overlay 86 new CUST 0 FEAT rlb RLI 10 ELC NO ENTR 0 LTER NO ROUT 001 TOD 0 ON 1 ON 2 ON 3 ON 4 ON 5 ON 6 ON 7 ON VNS NO SCNV NO CNV NO EXP NO FRL 0 DMI 10 CTBL 0 ISDM 0 </pre>	<pre> FCI 0 FSNI 0 BNE NO DORG NO SBOC NRR PROU 1 IDBB DBD IOHQ NO OHQ NO CBQ NO ISET 0 NALT 5 MFRL 0 OVLL 0 </pre>
---	--

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

TSC 00353	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 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 used in **Section 5.5** for **VIRTUALSETS**.

Load Overlay 20 IP Telephone configuration

```
DES 1140
TN 100 0 03 0 VIRTUAL
TYPE 1140
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00002
CUR_ZONE 00002
ERL 0
ECL 0
FDN 0
TGAR 0
LDN NO
NCOS 0
SGRP 0
RNPG 1
SCI 0
SSU
LNRS 16
XLST
SCPW
SFLT NO
CAC_MFC 0
CLS UNR FBA WTA LPR PUA MTD FNA HTA TDD HFA CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LNA CNDA
CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
ICDA CDMD LLCN MCTD CLBD AUTR
GPUD DPUD DNDA CFXA ARHD FITD CLTD ASCD
CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
UDI RCC HBTA AHD IPND DGGA NAMA MIND PRSD NRWD NRCD NROD
DRDD EXR0
USMD USRD ULAD CCBF RTDD RBDD RBHD PGND OCBF FLXD FTTC DNDY DNO3 MCBN
FDSD NOVD VOLA VOUD CDMR PRED RECA MCDD T87D SBMD KEM3 MSNV FRA PKCH MUTA MWTD
---continued on next page---
```

---continued from previous page---

```
DVLD CROD CROD
CPND_LANG ENG
RCO 0
HUNT 0
LHK 0
PLEV 02
PUID
DANI NO
AST 00
IAPG 1
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY 00 MCR 6000 0      MARP
      CPND
      CPND_LANG ROMAN
      NAME IP1140
      XPLN 10
      DISPLAY_FMT FIRST, LAST
01 MCR 6000 0
      CPND
      CPND_LANG ROMAN
      NAME IP1140
      XPLN 10
      DISPLAY_FMT FIRST, LAST
02
03 BSY
04 DSP
05
06
07
08
09
10
11
12
13
14
15
16
17 TRN
18 AO6
19 CFW 16
20 RGA
21 PRK
22 RNP
23
24 PRS
25 CHG
26 CPN
```

Digital telephones are configured using the **Overlay 20**, the following is a sample **3904** digital set configuration. Again, a unique number is entered for the **KEY 00** and **KEY 01** value.

Load Overlay 20 - Digital Set configuration

```
TYPE: 3904
DES 3904
TN 000 0 09 08 VIRTUAL
TYPE 3904
CDEN 8D
CTYP XDLC
CUST 0
MRT
ERL 0
FDN 0
TGAR 0
LDN NO
NCOS 0
SGRP 0
RNPG 1
SCI 0
SSU
LNRS 16
XLST
SCPW
SFLT NO
CAC_MFC 0
CLS UNR FBD WTA LPR PUA MTD FND HTD TDD HFA GRLD CRPA STSD
    MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
    POD SLKD CCSD SWD LNA CNDA
    CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
    ICDA CDMA LLCN MCTD CLBD AUTU
    GPUD DPUD DNDA CFXA ARHD FITD CNTD CLTD ASCD
    CPFA CPTA ABDA CFHD FICD NAID BUZZ AGRD MOAD
    UDI RCC HBTB AHA IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
    DRDD EXR0
    USMD USRD ULAD CCBF RTDD RBDD RBHD PGND OCBF FLXD FTTC DNDY DNO3 MCBN
    FDSD NOVD CDMR PRED RECA MCDD T87D SBMD PKCH CROD CROD
CPND_LANG ENG
RCO 0
HUNT
PLEV 02
PUID
DANI NO
SPID NONE
AST
IAPG 1
AACS
ACQ
ASID
SFNB
SFRB
USFB
CALB
FCTB
ITNA NO
DGRP
PRI 01
MLWU_LANG 0
```

---continued on next page---

---continued from previous page---

MLNG ENG

DNDR 0

KEY 00 MCR 6066 0 MARP

CPND

CPND_LANG ROMAN

NAME Digital Set

XPLN 10

DISPLAY_FMT FIRST, LAST

01 MCR 6066 0

CPND

CPND_LANG ROMAN

NAME Digital Set

XPLN 10

DISPLAY_FMT FIRST, LAST

02 DSP

03 MSB

04

05

06

07

08

09

10

11

12

13

14

15

16

17 TRN

18 AO6

19 CFW 16

20 RGA

21 PRK

22 RNP

23

24 PRS

25 CHG

26 CPN

27 CLT

28 RLT

29

30

31

Analog telephones are also configured using **Load Overlay 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.

Load Overlay 20 - Analog Telephone Configuration

```
DES 500
TN 004 0 03 03
TYPE 500
CDEN 4D
CUST 0
MRT

ERL 00000
WRLS NO
DN 6005
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 Communication Server 1000E system terminal and overlay 15 to activate SIP Line services, as in the following example where **SIPL_ON** is set to **YES**.

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

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

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

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

Node ID: 200 - SIP Line Configuration Details

General | SIP Line Gateway Settings | SIP Line Gateway Service

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

General

SIP domain name: *

SLG endpoint name:

SLG Group ID:

SLG Local Sip port: (1 - 65535)

SLG Local Tls port: (1 - 65535)

Virtual Trunk Network Health Monitor

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

5.10. Configure SIP Line Telephones

When SIP Line service configuration is completed, use the CS1000E system terminal and **Overlay 20** to add a Universal Extension (UEXT). See the following example of a SIP Line extension. The value for **UXTY** must be **SIPL**. This example is for an Avaya SIP telephone, so the value for **SIPN** is 1. The **SIPU** value is the username, **SCPW** is the logon password and these values are required to register the SIP telephone to the SLG. The value for **CFG_ZONE** is the value set for **SIPLINEZONE** 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 5.8**) value and the telephone number used in **KEY 00**.

```
Load Overlay 20 - SIP Telephone Configuration
DES  SIPD
TN    100 0 03 3  VIRTUAL
TYPE  UEXT
CDEN  8D
CTYP  XDLC
CUST  0
UXTY SIPL
MCCL  YES
SIPN 1
SIP3  0
FMCL  0
TLSV  0
SIPU 8889
NDID  200
SUPR  NO
SUBR  DFLT MWI RGA CWI MSB
UXID
NUID
NHTN
CFG_ZONE 00002
CUR_ZONE 00002
ERL   0
ECL   0
VSIT  NO
FDN
TGAR  0
LDN   NO
NCOS  0
SGRP  0
RNPG  0
SCI   0
SSU
XLST
SCPW 1234
SFLT  NO
CAC_MFC 0
CLS   UNR FBD WTA LPR MTD FNA HTA TDD HFD CRPD
      MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
      POD SLKD CCSD SWD LND CNDA
      CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
      ICDD CDMD LLCN MCTD CLBD AUTU
      GPUD DPUD DNDA CFXA ARHD FITD CLTD ASCD
      CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD

---continued on next page---
```


---continued from previous page---

```
UDI RCC HBTB AHA IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
DRDD 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 MCR 6002 0 MARP
    CPND
        CPND_LANG ROMAN
        NAME Sigma 1140
        XPLN 11
        DISPLAY_FMT FIRST, LAST*
01 HOT U 116002 MARP 0
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16
17 TRN
18 AO6
19 CFW 16
20 RGA
21 PRK
22 RNP
23 *
24 PRS
25 CHG
26 CPN
27
28
29
30
31
```

5.11. Save Configuration

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

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

The backup process will take several minutes to complete. Scroll to the bottom of the page to verify the backup process completed successfully as shown below.

```
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 Communication Server 1000E is complete.

6. Configuring Avaya Aura® Session Manager

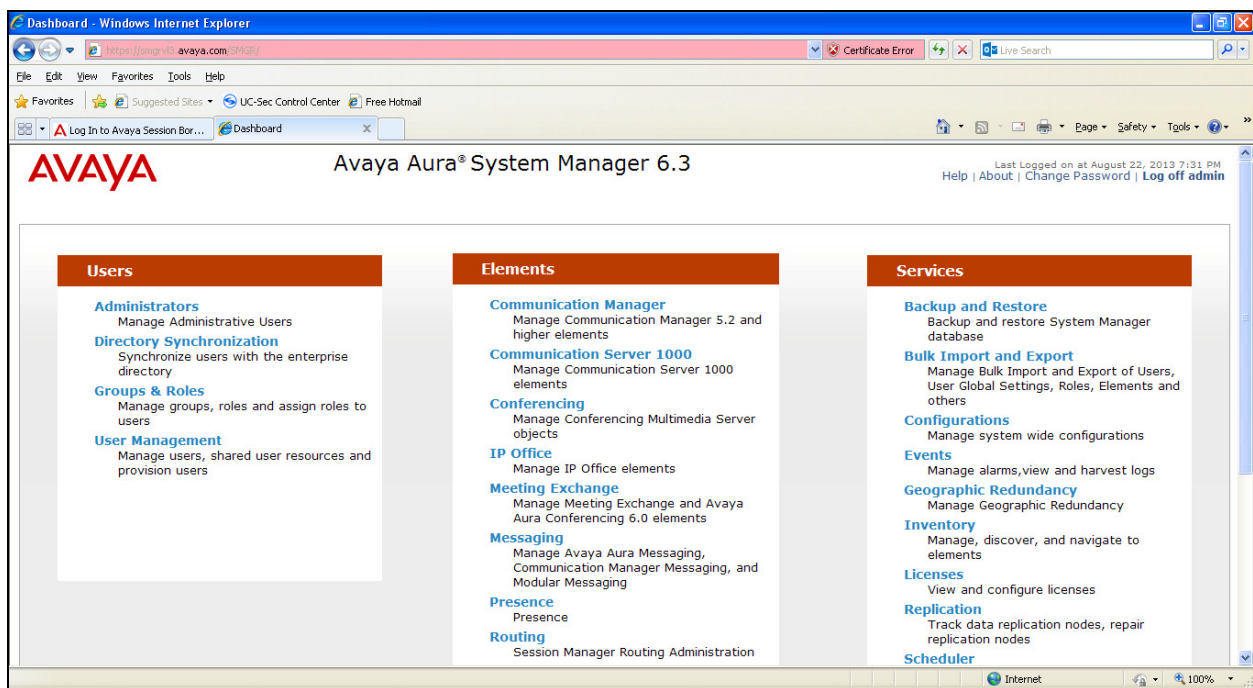
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

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

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

6.1. Log in to Avaya Aura® System Manager

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.



6.2. Administer SIP Domain

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

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

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



The screenshot shows the 'Domain Management' interface. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Domains'. Below this, the title 'Domain Management' is followed by a 'Help ?' link. A row of buttons includes 'Edit', 'New', 'Duplicate', 'Delete', and 'More Actions'. Below the buttons, it says '1 Item | Refresh' and 'Filter: Enable'. A table with the following columns is displayed: 'Name', 'Type', 'Default', and 'Notes'. The table contains one row with the values 'avaya.com', 'sip', and an unchecked checkbox for 'Default'. At the bottom left, there is a 'Select : All, None' option.

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

6.3. Administer Locations

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

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

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

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

- **IP Address Pattern:** Enter the logical pattern used to identify the location.
- **Notes:** Add a brief description [Optional].

Click **Commit** to save. The screenshot below shows the Location **SMGRVL3** defined for the compliance testing.

The screenshot shows the 'Location Details' configuration page for a location named 'SMGRVL3'. The page is divided into several sections:

- General:** Contains fields for 'Name' (set to 'SMGRVL3') and 'Notes'.
- Overall Managed Bandwidth:** Includes a dropdown for 'Managed Bandwidth Units' (set to 'Kbit/sec'), and input fields for 'Total Bandwidth' and 'Multimedia Bandwidth'. A checkbox for 'Audio Calls Can Take Multimedia Bandwidth' is checked.
- Per-Call Bandwidth Parameters:** Includes input fields for 'Maximum Multimedia Bandwidth (Intra-Location)' (1000 Kbit/Sec), 'Maximum Multimedia Bandwidth (Inter-Location)' (1000 Kbit/Sec), 'Minimum Multimedia Bandwidth' (64 Kbit/Sec), and 'Default Audio Bandwidth' (80 Kbit/sec).
- Location Pattern:** Features an 'Add' button, a 'Remove' button, and a table with 3 items. The table has columns for 'IP Address Pattern' and 'Notes'. The patterns listed are '10.10.3.*', '10.10.9.*', and '10.10.8.*'. Below the table is a 'Select' dropdown set to 'All, None'.

At the bottom right, there are 'Commit' and 'Cancel' buttons. A legend indicates that an asterisk (*) denotes 'Input Required'.

6.4. Administer Adaptations

To enable calls to be routed to stations on CS1000E, the Session Manager should be configured to modify the called party number to meet network requirements. 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
- **Module Name** Select **DigitConversionAdapter** 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 Commit Cancel

General

* Adaptation name: KPN

Module name: DigitConversionAdapter ▼

Module parameter: fromto=true MIME=no

Egress URI Parameters:

Notes:

In the **Digit Conversion for Incoming 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
- **Address to modify** Select **both**

Digit Conversion for Incoming Calls to SM

Add Remove

1 Item Refresh Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*+	*1	*36		*1	00	both ▼		

Select : All, None

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

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"/>	*6	*4	*36		*4	0302451400	both		

Select : All, None

6.5. Administer 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 Communication Server 1000E SIP entity and **Gateway** for the Session Border Controller SIP entity
- In the **Adaptation** field (not available for the Session Manager SIP Entity), select the appropriate Adaptation from the drop down menu
- In the **Location** field select the appropriate location from the drop down menu
- In the **Time Zone** field enter the time zone for the SIP Entity

In this configuration there are three SIP Entities:

- Avaya Aura® Session Manager SIP Entity
- Avaya Communication Server 1000E SIP Entity
- Avaya Session Border Controller Advanced for Enterprise 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: Home / Elements / Routing / SIP Entities. In the top right corner, there is a 'Help ?' link and 'Commit' and 'Cancel' buttons. The 'General' tab is selected. The configuration fields are as follows:

- 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)

The 'SIP Link Monitoring' section is expanded, showing the 'SIP Link Monitoring' dropdown menu set to 'Use Session Manager Configuration'.

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

Port

TCP Failover port:

TLS Failover port:

3 Items Refresh Filter: Enable

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

Select : All, None

6.5.2. Avaya Communication Server 1000E SIP Entity

The following screen shows the SIP entity for Communication Server 1000E. The **FQDN or IP Address** field is set to the Node IP address of the interface on CS1000E that will be providing SIP signaling, as shown in **Section 5.4**.

Home / Elements / Routing / SIP Entities Help ?

SIP Entity Details

General

* Name: CS1K_7.6

* FQDN or IP Address: 10.10.9.21

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

CommProfile Type Preference:

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.5.3. Avaya Session Border Controller Advanced for Enterprise SIP Entity

The following screen shows the SIP entity for the Avaya SBCE used for routing calls. The **FQDN or IP Address** field is set to the IP address of the private interfaces administered in **Section 7** of this document. Set the location to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.

The screenshot displays the 'SIP Entity Details' configuration page for the Avaya SBCE. The page has a breadcrumb trail at the top: 'Home / Elements / Routing / SIP Entities'. On the right, there are 'Commit', 'Cancel', and 'Help ?' buttons. The 'General' tab is selected. The configuration fields are as follows:

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

6.6. Administer Entity Links

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

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

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

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
* toAvaya SBCE	* Session Manager	TCP	* 5060	* Avaya SBCE	* 5060	Trusted	

* Input Required Commit Cancel

Home / Elements / Routing / Entity Links

Entity Links Commit Cancel Help ?

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	* Session Manager	* Session Manager	TCP	* 5060	* CS1K_7.6	* 5060	trusted	<input type="checkbox"/>	

Select : All, None

Commit Cancel

6.7. Administer Routing Policies

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

Under **General**:

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

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

The screenshot shows the 'Routing Policy Details' form for a policy named 'toCS1K_7.6'. The 'General' tab is active. The 'Name' field is 'toCS1K_7.6', 'Disabled' is unchecked, 'Retries' is '0', and 'Notes' is empty. Under 'SIP Entity as Destination', the 'Select' button is visible. Below, a table lists the destination:

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

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

The screenshot shows the 'Routing Policy Details' form for a policy named 'toAvaya SBCE'. The 'General' tab is active. The 'Name' field is 'toAvaya SBCE', 'Disabled' is unchecked, 'Retries' is '0', and 'Notes' is empty. Under 'SIP Entity as Destination', the 'Select' button is visible. Below, a table lists the destination:

Name	FQDN or IP Address	Type	Notes
Avaya SBCE	10.10.3.30	Gateway	

6.8. Administer Dial Patterns

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

Under **General**:

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

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

The following screen shows an example dial pattern configured for the Avaya SBCE which will route the calls out to the PSTN via the KPN VaMo1 VoIP Connect Service.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Help ?

Commit Cancel

General

* Pattern: 00353

* Min: 5

* Max: 36

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: 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	

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

Home / Elements / Routing / Dial Patterns

Help ?

Dial Pattern Details

Commit

Cancel

General

* Pattern: 0302451

* Min: 7

* Max: 36

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

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_7,6	0	<input type="checkbox"/>	CS1K_7,6	

Select : All, None

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. It is assumed that the Avaya SBCE software has already been installed..

7.1. Access Avaya Session Border Controller Advanced for Enterprise

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

Log In to Avaya Session Border Controller for Enterprise

AVAYA

Session Border Controller for Enterprise

Log In

Session expired, please sign in again.

Username:

Password:

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

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

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

© 2011 - 2013 Avaya Inc. All rights reserved.

The main page of the Avaya SBCE will appear.

Dashboard - Avaya Session Border Controller for Enterprise - Windows Internet Explorer

https://10.10.2.55/sbce/

File Edit View Favorites Tools Help

Dashboard - Avaya Session Border Controller for Enterprise

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

Dashboard

Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Domain Policies
TLS Management
Device Specific Settings

Information

System Time	11:23:03 AM GMT	Refresh
Version	6.2.0.Q36	
Build Date	Thu Feb 14 23:25:50 UTC 2013	

Alarms (past 24 hours)

None found.

Installed Devices

EMS
GSSCP_03

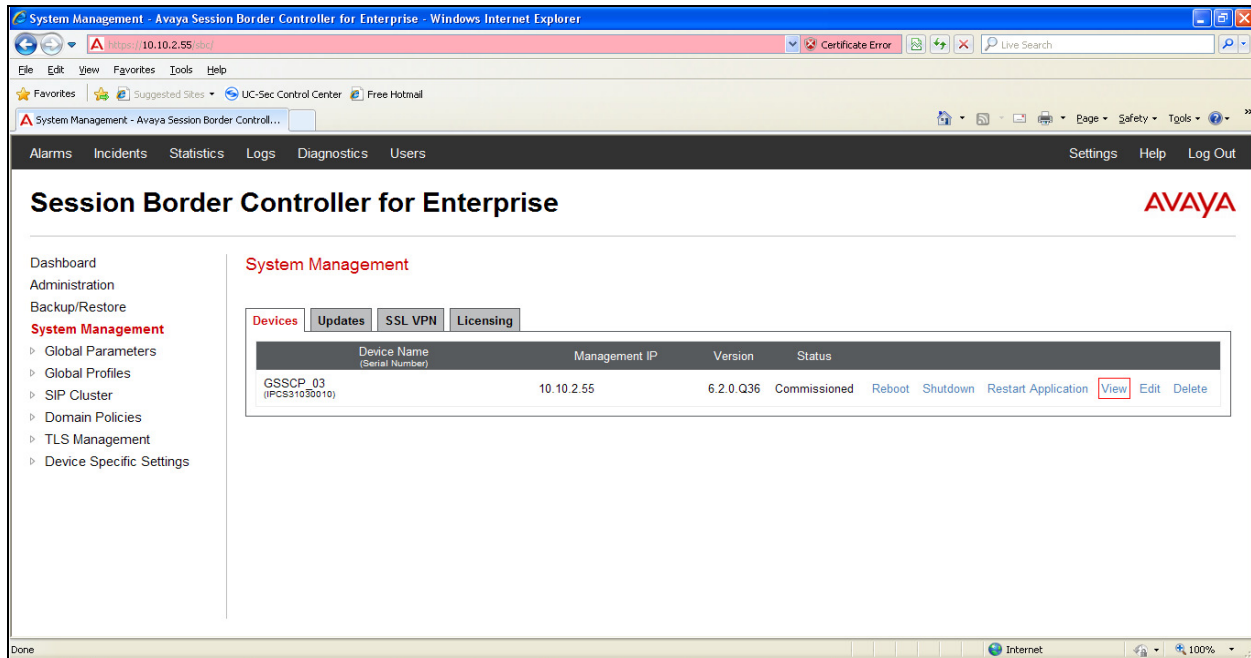
Incidents (past 24 hours)

GSSCP_03: Heartbeat Successful, Server is UP
GSSCP_03: Heartbeat Successful, Server is UP
GSSCP_03: Heartbeat Successful, Credentials are Invalid
GSSCP_03: Heartbeat Successful, Credentials are Invalid
GSSCP_03: Heartbeat Successful, Server is UP

[Add](#)

Notes

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



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

System Information: GSSCP_03				
General Configuration		Device Configuration		
Appliance Name	GSSCP_03	HA Mode	No	
Box Type	SIP	Two Bypass Mode	No	
Deployment Mode	Proxy			
Network Configuration				
IP	Public IP	Netmask	Gateway	Interface
10.10.3.30	10.10.3.30	255.255.255.0	10.10.3.1	A1
192.168.122.55	192.168.122.55	255.255.255.128	192.168.122.7	B1
DNS Configuration		Management IP(s)		
Primary DNS	10.10.7.100	IP	10.10.2.55	
Secondary DNS	10.10.101.115			
DNS Location	DMZ			
DNS Client IP	10.10.3.30			

7.2. Global Profiles

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

7.2.1. Server Internetworking - Avaya

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

Server Interworking and click on **Add Profile**.

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

The screenshot displays the configuration window for a profile named 'Avaya_SM'. The 'General' tab is active, showing several configuration options:

- Hold Support:** Set to 'None' (selected with a radio button). Other options are 'RFC2543 - c=0.0.0.0' and 'RFC3264 - a=sendonly'.
- 180 Handling:** Set to 'None' (selected with a radio button). Other options are 'SDP' and 'No SDP'.
- 181 Handling:** Set to 'None' (selected with a radio button). Other options are 'SDP' and 'No SDP'.
- 182 Handling:** Set to 'None' (selected with a radio button). Other options are 'SDP' and 'No SDP'.
- 183 Handling:** Set to 'None' (selected with a radio button). Other options are 'SDP' and 'No SDP'.
- Refer Handling:** Set to 'None' (checkbox is unchecked).
- 3xx Handling:** Set to 'None' (checkbox is unchecked).
- Diversion Header Support:** Set to 'None' (checkbox is unchecked).
- Delayed SDP Handling:** Set to 'None' (checkbox is unchecked).
- T.38 Support:** Set to 'Check' (checkbox is checked and highlighted with a red box).
- URI Scheme:** Set to 'SIP' (selected with a radio button). Other options are 'TEL' and 'ANY'.
- Via Header Format:** Set to 'RFC3261' (selected with a radio button). Other option is 'RFC2543'.

A 'Next' button is located at the bottom right of the configuration area.

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

Profile: Avaya_SM X

Record Routes	<input checked="" 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"/>
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"/>

Finish

7.2.2. Server Internetworking – KPN

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

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

Click on **Next** on the following screens and then **Finish**

Profile: KPN X

General

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

180 Handling ☒ None ☐ SDP ☐ No SDP

181 Handling ☒ None ☐ SDP ☐ No SDP

182 Handling ☒ None ☐ SDP ☐ No SDP

183 Handling ☒ None ☐ SDP ☐ No SDP

Refer Handling ☐

3xx Handling ☐

Diversion Header Support ☐

Delayed SDP Handling ☐

T.38 Support ☒

URI Scheme ☒ SIP ☐ TEL ☐ ANY

Via Header Format ☒ RFC3261 ☐ RFC2543

Next

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

Profile: KPN

X

Record Routes	<div><div><input checked="" type="radio"/></div>None</div> <div><div><input type="radio"/></div>Single Side</div> <div><div><input type="radio"/></div>Both Sides</div>
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"/>
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"/>

Finish

7.2.3. Routing

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

Routing information is required for routing to Session Manager on the internal side and the KPN VaMo1 VoIP addresses on the external side. The IP addresses and ports defined here will be used as the destination addresses for signaling. If no port is specified in the **Next Hop IP Address**, default 5060 is used.

Create a Routing Profile for both Session Manager and KPN VaMo1 VoIP 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, e.g., Session Manager
- **Next Hop Server 2:** (Optional) Enter the Domain Name or IP address of the secondary Next Hop server
- **Routing Priority Based on Next Hop Server:** Checked
- **Use Next Hop for In-Dialog Messages:** Select only if there is no secondary Next Hop server
- **Outgoing Transport:** Choose the protocol used for transporting outgoing signaling packets

Click **Finish**.

The following screen shows the Routing Profile to Session Manager

The screenshot shows the 'Routing Profiles: Avaya_SM' configuration page. On the left, a sidebar lists 'Routing Profiles' with 'default', 'Avaya_SM' (highlighted), and 'KPN'. The main area has a blue header with 'Click here to add a description.' and buttons for 'Rename', 'Clone', and 'Delete'. Below this is a 'Routing Profile' section with an 'Add' button. A table lists the profile details:

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	*	10.10.3.55	---	View Edit

The following screen shows the Routing Profile to KPN.

Routing Profiles: KPN

Add

Routing Profiles

default

Avaya_SM

KPN

Rename Clone Delete

Click here to add a description.

Routing Profile

Add

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	*	213.162.171.164	---	View Edit

7.2.4. Server Configuration – Avaya Aura® Session Manager

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

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow configuration and management of various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signaling parameters and some advanced options. From the left-hand menu select **Global Profiles** → **Server Configuration** and click on **Add Profile** and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Call Server**
- Enter **IP Addresses / Supported FQDNs** to **10.10.3.55** (Session Manager IP Address)
- For **Supported Transports**, check **TCP**
- **TCP Port** to **5060**
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs

The screenshot shows the 'Server Configuration Profile - General' window. It has several sections: 'Server Type' with a dropdown menu set to 'Call Server'; 'IP Addresses / Supported FQDNs' with a text area containing '10.10.3.55'; 'Supported Transports' with three checkboxes where 'TCP' is checked; 'TCP Port' with a text box containing '5060'; 'UDP Port' with an empty text box; and 'TLS Port' with an empty text box. A 'Finish' button is located at the bottom center of the window.

On the **Advanced** tab:

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

Server Configuration Profile - Advanced

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile Avaya_SM

Signaling Manipulation Script None

TCP Connection Type ☒ SUBID ☐ PORTID ☐ MAPPING

Finish

7.2.5. Server Configuration – KPN

To define the KPN VaMo1 VoIP Connect Trunk Server, navigate to select **Global Profiles** → **Server Configuration** and click on **Add Profile** and enter a descriptive name. On the **Add Server Configuration Profile** tab, click on **Edit** and set the following:

- Select **Server Type** as **Trunk Server**
- Set **IP Address** to **192.168.171.164** (KPN VaMo1 VoIP Connect)
- **Supported Transports**: Check **TCP**
- **TCP Port** to **5060**
- Hit **Next**
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs

Server Configuration Profile - General

Server Type Trunk Server

IP Addresses / Supported FQDNs
Separate entries with commas 192.168.171.164

Supported Transports ☒ TCP ☐ UDP ☐ TLS

TCP Port 5060

UDP Port

TLS Port

Finish

On the **Advanced** tab:

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

The screenshot shows a window titled "Server Configuration Profile - Advanced" with a close button (X) in the top right corner. The window contains several configuration options:

- Enable DoS Protection:** A checkbox that is currently unchecked.
- Enable Grooming:** A checkbox that is currently unchecked.
- Interworking Profile:** A dropdown menu with "KPN" selected. This dropdown is highlighted with a red rectangular border.
- Signaling Manipulation Script:** A dropdown menu with "None" selected.
- TCP Connection Type:** Three radio buttons labeled "SUBID", "PORTID", and "MAPPING". The "SUBID" radio button is selected.

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

7.2.6. Topology Hiding

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

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

- In the **Profile Name** field enter a descriptive name for Session Manager and click **Next**
- If the required Header is not shown, click on **Add Header**
- Select **Request-Line**, **To** and **From** as the required headers from the **Header** drop down menu
- Select the required action from the **Required Action** drop down menu, **Auto** was used for test

The screenshot shows the 'Topology Hiding Profiles: Avaya_SM' configuration page. On the left, a sidebar lists 'Topology Hiding Profiles' with options: 'default', 'cisco_th_profile', 'Avaya_SM' (selected), and 'KPN'. The main area has a blue header bar with 'Click here to add a description.' and buttons for 'Rename', 'Clone', and 'Delete'. Below this is a table titled 'Topology Hiding' with columns: 'Header', 'Criteria', 'Replace Action', and 'Overwrite Value'. The table contains six rows of configuration data. An 'Add' button is at the top left of the main area, and an 'Edit' button is at the bottom right.

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

To define Topology Hiding for the KPN VaMo1 VoIP Connect Service, navigate to **Global Profiles → Topology Hiding** in the **UC-Sec Control Center** menu on the left-hand side. Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- In the **Profile Name** field enter a descriptive name for the KPN and click **Next**
- If the required Header is not shown, click on **Add Header**
- Select **Request-Line**, **To** and **From** as the required headers from the **Header** drop down menu
- Select the required action from the **Required Action** drop down menu, **Auto** was used for test

Topology Hiding Profiles: KPN

Add

Rename

Clone

Delete

Topology Hiding Profiles

default

cisco_th_profile

Avaya_SM

KPN

Click here to add a description.

Topology Hiding

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

Edit

7.3. Define Network Information

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

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

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

Network Management: GSSCP_03

Devices
GSSCP_03

Network Configuration Interface Configuration

Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.

A1 Netmask 255.255.255.0 A2 Netmask B1 Netmask 255.255.255.240 B2 Netmask

Add Save Clear

IP Address	Public IP	Gateway	Interface	
10.10.3.30		10.10.3.1	A1	Delete
192.168.224.2		192.168.224.3	B1	Delete

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

Network Management: GSSCP_03

Devices
GSSCP_03

Network Configuration Interface Configuration

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

7.4. Define Interfaces

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

7.4.1. Signaling Interfaces

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

- Select **Add Signaling Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the internal signaling interface
- For **Signaling IP**, select an **internal** signaling interface IP address defined in **Section 7.3**
- Select **UDP** and **TCP** port numbers, **5060** is used for the Session Manager
- Select **Add Signaling Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the external signaling interface
- For **Signaling IP**, select an **external** signaling interface IP address defined in **Section 7.3**
- Select **UDP** and **TCP** port numbers, **5060** is used for KPN

Signaling Interface: GSSCP_03

Devices

GSSCP_03

Signaling Interface

Add

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Int_Sig	10.10.3.30	5060	5060	---	None	Edit Delete
Ext_Sig	192.168.224.2	5060	5060	---	None	Edit Delete

7.4.2. Media Interfaces

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

- Select **Add Media Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the internal media interface
- For **Media IP**, select an **internal** media interface IP address defined in **Section 7.3**
- Select **RTP port** ranges for the media path with the enterprise end-points
- Select **Add Media Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the external media interface
- For **Media IP**, select an **external** media interface IP address defined in **Section 7.3**
- Select **RTP port** ranges for the media path with KPN VaMo1 VoIP Connect Service

Media Interface: GSSCP_03

Devices

GSSCP_03

Media Interface

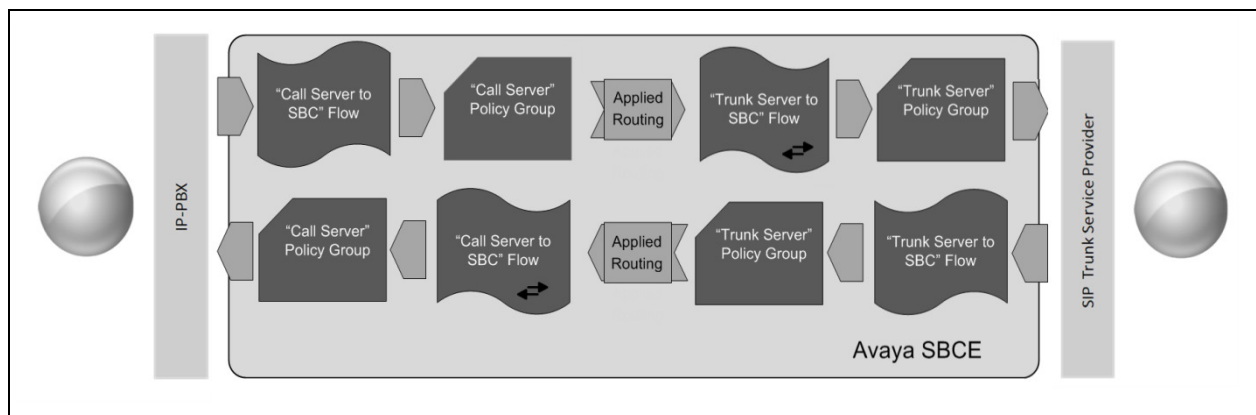
Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add

Name	Media IP	Port Range		
Int_Media	10.10.3.30	35000 - 40000	Edit	Delete
Ext_Media	192.168.224.2	35000 - 40000	Edit	Delete

7.5. Server 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.



This configuration ties all the previously entered information together so that calls can be routed from Session Manager to the KPN VaMo1 VoIP Connect Service and vice versa. The following screenshot shows both flows:

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

To define an outgoing Server Flow, navigate to **Device Specific Settings → End Point Flows**.

- Click on the **Server Flows** tab
- Select **Add Flow** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the outgoing server flow to the KPN VaMo1 VoIP Connect service
- In the **Received Interface** drop-down menu, select the internal SIP signaling interface defined in **Section 7.4.1**
- In the **Signaling Interface** drop-down menu, select the external SIP signaling interface defined in **Section 7.4.1**
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.4.2**
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 7.2.3**
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the KPN VaMo1 VoIP Connect Service defined in **Section 7.2.6** and click **Finish**

Flow: Trunk_Server	
Flow Name	Trunk_Server
Server Configuration	KPN
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig
Signaling Interface	Ext_Sig
Media Interface	Ext_Media
End Point Policy Group	default-low
Routing Profile	Avaya_SM
Topology Hiding Profile	KPN
File Transfer Profile	None

Finish

The incoming Server Flows are defined as a reversal of the outgoing Server Flows

- Click on the **Server Flows** tab
- Select **Add Flow** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the incoming server flow to Session Manager
- In the **Received Interface** drop-down menu, select the external SIP signaling interface defined in **Section 7.4.1**
- In the **Signaling Interface** drop-down menu, select the internal SIP signaling defined in **Section 7.4.1**
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.4.2**
- In the **Routing Profile** drop-down menu, select the routing profile of the KPN VaMo1 VoIP Connect Service defined in **Section 7.2.3**
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.2.6** and click **Finish**

Flow: Call_Server	
Flow Name	Call_Server
Server Configuration	Avaya_SM
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	KPN
Topology Hiding Profile	Avaya_SM
File Transfer Profile	None

Finish

8. KPN Configuration

The configuration of the KPN equipment used to support the KPN VaMo1 VoIP Connect Service is outside of the scope of these Application Notes and will not be covered. To obtain further information on KPN equipment and system configuration please contact an authorized KPN representative.

9. Verification Steps

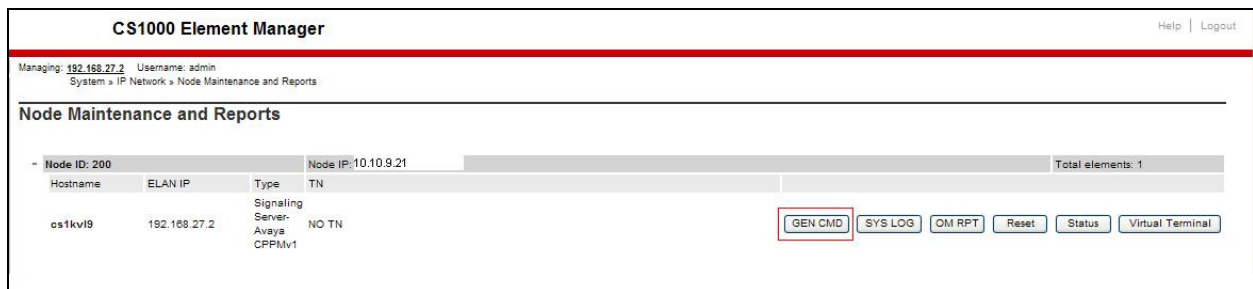
This section provides verification steps that may be performed in the field to verify that the solution is configured properly.

9.1. Avaya Communication Server 1000E Verification

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

9.1.1. IP Network Maintenance and Reports Commands

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



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

To check the status of the SIP Gateway to Session Manager in the sample configuration, select **Sip** from the Group menu and **SIPGwShow** from the **Command** menu. Click **Run**. The example output below shows that Session Manager (10.10.3.55, port 5060, TCP) has **SIPNPM Status** “Active”.

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

General Commands

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

Group: Sip Command: SIPGwShow SIP [v] RUN

IP address: 192.168.27.2 Number of pings: 3 PING

```

SIPPM Status      : Active
Primary Proxy IP address : 10.10.9.55
Primary Proxy port      : 5060
Primary Proxy Transport : TCP
Secondary Proxy IP address : 0.0.0.0
Secondary Proxy port     : 5060
Secondary Proxy Transport : TCP
Primary Proxy2 IP address : 10.10.9.55
Primary Proxy2 port      : 5060
Primary Proxy2 Transport : TCP
Active Proxy           : Primary :Register Not Supported
Time To Next Registration : 0 Seconds
Channels Busy / Idle / Total : 0 / 34 / 34
Stack version           : 5.5.0.13
TLS Security Policy      : Security Disabled
  
```

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

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

General Commands

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

Group: SipLine Command: sigSetShowAll RUN

IP address: 192.168.27.2 Number of pings: 3 PING

UserID	AuthId	TN	Clients	Calls	SetHandle	Pos ID	SIPL Type
----- IPv4 Endpoints -----							
6003	6003	100-00-03-03	1	0	0x91e82d0		SIP Lines
6002	6002	100-00-03-02	1	0	0x91c4158		SIP Lines
Total User Registered = 2 V4 Registered = 2 V6 Registered = 0							

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

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

General Commands

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

Group: Iset Command: isetShow Range: 0 500 RUN

IP address: 192.168.27.2 Number of pings: 3 PING

Set Information						
IP Address	NAT	Model Name	Type	RegType	State	Up
10.10.9.200	1230	IP Deskphone	1230	Regular	online	13
10.10.9.201	1140E	IP Deskphone	1140	Regular	online	13
Total sets = 2						

9.1.2. Verify Avaya Communication Server 1000E Operational Status

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

AVAYA CS1000 Element Manager

Managing: 192.168.1.5 Username: admin
System > Maintenance

Maintenance

☒ Select by Overlay ☐ Select by Functionality

<Select by Overlay>

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

<Select Group>

D-Channel Diagnostics
MSDL Diagnostics
TMDI Diagnostics

Select **Status for D-Channel (STAT DCH)** command and click **Submit** to verify status of virtual D-Channel as shown below. Verify the status of the following fields.

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

AVAYA CS1000 Element Manager

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_RECVP** **PDCH** **BDCH**

☐ 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** 
- **Service State** 

[Home](#) / [Elements](#) / [Session Manager](#) - Session Manager

Session Manager

Dashboard

Session Manager

Administration

Communication Profile Editor

Network Configuration

Device and Location Configuration

Application Configuration

System Status

System Tools

Home / Elements / Session Manager- Session Manager

Help ?


Session Manager Dashboard

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

Session Manager Instances

Service State Shutdown System As of 11:56 AM



1 Item Refresh Show Filter: Enable

<input type="checkbox"/>	Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Version
<input type="checkbox"/>	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.

1 Item Refresh Show Filter: Enable

	Details	Session Manager	Type	Status	Connections	IP Address	VLAN	Default Gateway	NIC Bonding	Entity Links (expected / actual)	Certificate Used
		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 a configuration window titled "Security Module" with a dropdown arrow. Inside the window, a red rectangular box highlights the following configuration fields:

- 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:** (field is empty)

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Communication Server R7.6, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise to KPN VaMo1 VoIP Connect Service. KPN VaMo1 VoIP Connect Service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.

11. References

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

- [1] *Implementing Avaya Aura® Session Manager*, Release 6.3
- [2] *Installing Service Packs for Avaya Aura® Session Manager*, Release 6.3
- [3] *Upgrading Avaya Aura® Session Manager*, Release 6.3
- [4] *Maintaining and Troubleshooting Avaya Aura® Session Manager Release 6.3*
- [5] *Installing and Configuring Avaya Aura® System Platform Release 6.3*, June 2013
- [6] *Implementing Avaya Aura® System Manager Release 6.3*, June 2013
- [7] *Upgrading Avaya Aura® System Manager to 6.3.2*, July 2013
- [8] *Avaya Communication Server 1000E Installation and Commissioning*, April 2012, Document Number NN43041-310.
- [9] *Feature Listing Reference Avaya Communication Server 1000*, November 2010, Document Number NN43001-111, 05.01.
- [10] *Linux Platform Base and Applications Installation and Commissioning Avaya Communication Server 1000*, April 2013, Document Number NN43001-315
- [11] *Unified Communications Management Common Servers Fundamentals Avaya Communication Server 1000*, February 2013, Document Number NN43001-116
- [12] *Software Input Output Reference – Maintenance Avaya Communication Server 1000*, April 2012, Document Number NN43001-711
- [13] *Signaling Server IP Line Applications Fundamentals Avaya Communication Server 1000*, October 2011, Document Number NN43001-125
- [14] *SIP Software for Avaya 1100 Series IP Deskphones-Administration*, December 2011, Document Number NN43170-600
- [15] RFC 3261 SIP: Session Initiation Protocol, <http://www.ietf.org/>

Appendix A

Avaya Communication Server 1000E Software

Communication Server 1000E call server patches and plug ins

TID: 46379

VERSION 4121

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

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

RELEASE 7

ISSUE 65 P +

IDLE_SET_DISPLAY NORTEL

DepList 1: core Issue: 01(created: 2013-05-28 04:19:50 (est))

MDP>LAST SUCCESSFUL MDP REFRESH :2013-09-12 14:50:17(Local Time)

MDP>USING DEPLIST ZIP FILE DOWNLOADED :2013-05-28 04:30:29(est)

SYSTEM HAS NO USER SELECTED PEPS IN-SERVICE

LOADWARE VERSION: PSWV 100+

INSTALLED LOADWARE PEPS : 1

PAT#	CR #	PATCH REF #	NAME	DATE	FILENAME
00	wi01057886	ISS1:10F1	DSP2AB07	13/09/2013	DSP2AB07.LW

ENABLED PLUGINS : 2

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

Communication Server 1000E call server deplists

VERSION 4121

RELEASE 7

ISSUE 65 P +

DepList 1: core Issue: 01 (created: 2013-05-28 04:19:50 (est))

IN-SERVICE PEPS

PAT#	CR #	PATCH REF #	NAME	DATE	FILENAME	SPECINS
000	wi01058359	ISS1:10F1	p32331_1	22/10/2013	p32331_1.cpl	NO
001	wi01064599	iss1:10f1	p32580_1	22/10/2013	p32580_1.cpl	NO
002	wi01056067	ISS1:10F1	p32457_1	22/10/2013	p32457_1.cpl	NO
003	wi01063263	ISS1:10F1	p32573_1	22/10/2013	p32573_1.cpl	NO
004	wi01065842	ISS1:10F1	p32478_1	22/10/2013	p32478_1.cpl	NO
005	wi01062607	ISS1:10F1	p32503_1	22/10/2013	p32503_1.cpl	NO
006	wi01070756	ISS1:10F1	p32444_1	22/10/2013	p32444_1.cpl	NO
007	wi01039280	ISS1:10F1	p32423_1	22/10/2013	p32423_1.cpl	NO
008	wi01087543	ISS1:10F1	p32662_1	22/10/2013	p32662_1.cpl	NO
009	wi00933195	ISS1:10F1	p32491_1	22/10/2013	p32491_1.cpl	NO
010	wi01071379	ISS1:10F1	p32522_1	22/10/2013	p32522_1.cpl	NO
011	wi01068669	ISS1:10F1	p32333_1	22/10/2013	p32333_1.cpl	NO

012	wi01066991	ISS1:10F1	p32449_1	22/10/2013	p32449_1.cpl	NO
013	wi01070474	iss1:1of1	p32407_1	22/10/2013	p32407_1.cpl	NO
014	WI0110261	ISS1:10F1	p32758_1	22/10/2013	p32758_1.cpl	NO
015	wi01094305	ISS1:10F1	p32640_1	22/10/2013	p32640_1.cpl	NO
016	wi01047890	ISS1:10F1	p32697_1	22/10/2013	p32697_1.cpl	NO
017	wi01055300	ISS1:10F1	p32543_1	22/10/2013	p32543_1.cpl	NO
018	wi01082456	ISS1:10F1	p32596_1	22/10/2013	p32596_1.cpl	NO
019	wi01058621	ISS1:10F1	p32339_1	22/10/2013	p32339_1.cpl	NO
020	wi01061484	ISS1:10F1	p32576_1	22/10/2013	p32576_1.cpl	NO
021	wi01078723	ISS1:10F1	p32532_1	22/10/2013	p32532_1.cpl	NO
022	wi01048457	ISS1:10F1	p32581_1	22/10/2013	p32581_1.cpl	NO
023	wi01075355	ISS1:10F1	p32594_1	22/10/2013	p32594_1.cpl	NO
024	wi01053597	ISS1:10F1	p32304_1	22/10/2013	p32304_1.cpl	NO
025	wi01045058	ISS1:10F1	p32214_1	22/10/2013	p32214_1.cpl	NO
026	wi01075359	ISS1:10F1	p32671_1	22/10/2013	p32671_1.cpl	NO
027	wi01025156	ISS1:10F1	p32136_1	22/10/2013	p32136_1.cpl	NO
028	wi01061481	ISS1:10F1	p32382_1	22/10/2013	p32382_1.cpl	NO
029	wi01035976	ISS1:10F1	p32173_1	22/10/2013	p32173_1.cpl	NO
030	wi01088775	ISS1:10F1	p32659_1	22/10/2013	p32659_1.cpl	NO
031	wi01070465	iss1:1of1	p32562_1	22/10/2013	p32562_1.cpl	NO
032	wi01088585	ISS1:10F1	p32656_1	22/10/2013	p32656_1.cpl	NO
033	wi01063864	ISS1:10F1	p32410_1	22/10/2013	p32410_1.cpl	YES
034	wi01034961	ISS1:10F1	p32144_1	22/10/2013	p32144_1.cpl	NO
035	wi01055480	ISS1:10F1	p32712_1	22/10/2013	p32712_1.cpl	NO
036	wi01034307	ISS1:10F1	p32615_1	22/10/2013	p32615_1.cpl	NO
037	wi01065118	ISS1:10F1	p32397_1	22/10/2013	p32397_1.cpl	NO
038	wi01075360	iss1:1of1	p32602_1	22/10/2013	p32602_1.cpl	NO
039	wi00884716	ISS1:10F1	p32517_1	22/10/2013	p32517_1.cpl	NO
040	wi01068851	ISS1:10F1	p32439_1	22/10/2013	p32439_1.cpl	NO
041	wi01053314	ISS1:10F1	p32555_1	22/10/2013	p32555_1.cpl	NO
042	wi01059388	iss1:1of1	p32628_1	22/10/2013	p32628_1.cpl	NO
043	wi01087528	ISS1:10F1	p32700_1	22/10/2013	p32700_1.cpl	NO
044	wi01072027	ISS1:10F1	p32689_1	22/10/2013	p32689_1.cpl	NO
045	wi01052428	ISS1:10F1	p32606_1	22/10/2013	p32606_1.cpl	NO
046	wi01053920	ISS1:10F1	p32303_1	22/10/2013	p32303_1.cpl	NO
047	wi01070468	iss1:1of1	p32418_1	22/10/2013	p32418_1.cpl	NO
048	wi01067822	ISS1:10F1	p32466_1	22/10/2013	p32466_1.cpl	YES
049	wi01060826	ISS1:10F1	p32379_1	22/10/2013	p32379_1.cpl	NO
050	wi01075352	ISS1:10F1	p32603_1	22/10/2013	p32603_1.cpl	NO
051	wi01043367	ISS1:10F1	p32232_1	22/10/2013	p32232_1.cpl	NO
052	wi01083584	ISS1:10F1	p32619_1	22/10/2013	p32619_1.cpl	NO
053	wi01060241	ISS1:10F1	p32381_1	22/10/2013	p32381_1.cpl	NO
054	wi01053195	ISS1:10F1	p32297_1	22/10/2013	p32297_1.cpl	NO
055	wi00897254	ISS1:10F1	p31127_1	22/10/2013	p31127_1.cpl	NO
056	wi01061483	ISS1:10F1	p32359_1	22/10/2013	p32359_1.cpl	NO
057	wi01085855	ISS1:10F1	p32658_1	22/10/2013	p32658_1.cpl	NO
058	wi01075353	ISS1:10F1	p32613_1	22/10/2013	p32613_1.cpl	NO
059	wi01070471	ISS1:10F1	p32415_1	22/10/2013	p32415_1.cpl	NO
060	wi01074003	ISS1:10F1	p32421_1	22/10/2013	p32421_1.cpl	NO
061	wi01060382	iss1:1of1	p32623_1	22/10/2013	p32623_1.cpl	YES
062	wi01068042	ISS1:10F1	p32669_1	22/10/2013	p32669_1.cpl	NO
063	wi01072023	ISS1:10F1	p32130_1	22/10/2013	p32130_1.cpl	YES
064	wi01065922	ISS1:10F1	p32516_1	22/10/2013	p32516_1.cpl	NO
065	wi01057403	ISS1:10F1	p32591_1	22/10/2013	p32591_1.cpl	NO
066	wi01069441	ISS1:10F1	p32097_1	22/10/2013	p32097_1.cpl	NO
067	wi01070473	ISS1:10F1	p32413_1	22/10/2013	p32413_1.cpl	NO
068	wi01056633	ISS1:10F1	p32322_1	22/10/2013	p32322_1.cpl	NO
069	wi01052968	ISS1:10F1	p32540_1	22/10/2013	p32540_1.cpl	NO
070	wi01072032	ISS1:10F1	p32448_1	22/10/2013	p32448_1.cpl	NO
071	wi01073100	ISS1:10F1	p32599_1	22/10/2013	p32599_1.cpl	NO
072	wi01035980	ISS1:10F1	p32558_1	22/10/2013	p32558_1.cpl	NO
073	wi01041453	ISS1:10F1	p32587_1	22/10/2013	p32587_1.cpl	NO
074	wi01032756	ISS1:10F1	p32673_1	22/10/2013	p32673_1.cpl	NO
075	wi01092300	ISS1:10F1	p32692_1	22/10/2013	p32692_1.cpl	NO
076	wi00996734	ISS1:10F1	p32550_1	22/10/2013	p32550_1.cpl	NO
077	wi01022599	ISS1:10F1	p32080_1	22/10/2013	p32080_1.cpl	NO
078	wi01060341	ISS1:10F1	p32578_1	22/10/2013	p32578_1.cpl	NO
079	wi01091447	ISS1:10F1	p32675_1	22/10/2013	p32675_1.cpl	NO
080	wi01070580	ISS1:10F1	p32380_1	22/10/2013	p32380_1.cpl	NO
081	wi01089519	ISS1:10F1	p32665_1	22/10/2013	p32665_1.cpl	NO

```

082 WI01077073      ISS1:10F1      p32534_1  22/10/2013  p32534_1.cpl  NO
083 wi01080753      ISS1:10F1      p32518_1  22/10/2013  p32518_1.cpl  NO
084 wi01065125      ISS1:10F1      p32416_1  22/10/2013  p32416_1.cpl  NO
MDP>LAST SUCCESSFUL MDP REFRESH :2013-09-12 14:50:17(Local Time)
MDP>USING DEPLIST ZIP FILE DOWNLOADED :2013-05-28 04:30:29(est)

```

Communication Server 1000E signaling server service updates

Product Release: 7.65.16.00

In system patches: 1

PATCH#	NAME	IN_SERVICE	DATE	SPECINS	TYPE	RPM
37	p31484_1	Yes	02/10/13	NO	FRU	cs1000-shared-general-7.65.16-00.i386

In System service updates: 29

PATCH#	IN_SERVICE	DATE	SPECINS	REMOVABLE	NAME
0	Yes	02/10/13	NO	YES	cs1000-patchWeb-7.65.16.21-06.i386.000
1	Yes	02/10/13	NO	yes	cs1000-cppmUtil-7.65.16.21-01.i686.000
2	Yes	27/09/13	NO	YES	cs1000-dmWeb-7.65.16.21-01.i386.000
4	Yes	27/09/13	NO	YES	cs1000-nrsm-7.65.16.00-03.i386.000
5	Yes	27/09/13	NO	YES	cs1000-oam-logging-7.65.16.01-01.i386.000
6	Yes	27/09/13	NO	yes	cs1000-cs1000WebService_6-0-7.65.16.21-386.000
8	Yes	27/09/13	NO	YES	cs1000-pd-7.65.16.21-00.i386.000
9	Yes	27/09/13	NO	YES	cs1000-shared-carrdtct-7.65.16.21-01.i386.000
10	Yes	27/09/13	NO	YES	cs1000-shared-tpselect-7.65.16.21-01.i386.000
11	Yes	27/09/13	NO	YES	cs1000-emWebLocal_6-0-7.65.16.21-01.i386.000
12	Yes	27/09/13	NO	yes	cs1000-dbcom-7.65.16.21-00.i386.000
14	Yes	27/09/13	NO	YES	cs1000-shared-xmsg-7.65.16.21-00.i386.000
17	Yes	27/09/13	NO	YES	cs1000-mscAnnc-7.65.16.21-02.i386.001
18	Yes	27/09/13	NO	YES	cs1000-mscAttn-7.65.16.21-04.i386.001
19	Yes	27/09/13	NO	YES	cs1000-mscConf-7.65.16.21-02.i386.001
20	Yes	27/09/13	NO	YES	cs1000-mscMusc-7.65.16.21-02.i386.001
21	Yes	27/09/13	NO	YES	cs1000-mscTone-7.65.16.21-03.i386.001
25	Yes	27/09/13	NO	yes	cs1000-cs-7.65.P.100-01.i386.001
26	Yes	02/10/13	YES	yes	cs1000-linuxbase-7.65.16.21-08.i386.000
27	Yes	02/10/13	NO	YES	cs1000-csmWeb-7.65.16.21-07.i386.000
28	Yes	02/10/13	NO	YES	cs1000-gk-7.65.16.21-01.i386.000
29	Yes	02/10/13	NO	yes	cs1000-Jboss-Quantum-7.65.16.21-7.i386.000
30	Yes	02/10/13	NO	YES	cs1000-snmp-7.65.16.21-00.i686.000
31	Yes	02/10/13	YES	yes	tzdata-2013c-1.el5.i386.001
32	Yes	02/10/13	NO	YES	cs1000-emWeb_6-0-7.65.16.21-09.i386.000
33	Yes	02/10/13	YES	yes	cs1000-tps-7.65.16.21-08.i386.000
34	Yes	02/10/13	NO	YES	cs1000-sps-7.65.16.21-7.i386.000
35	Yes	02/10/13	YES	YES	cs1000-bcc-7.65.16.21-31.i386.000
36	Yes	02/10/13	NO	YES	cs1000-vtrk-7.65.16.21-107.i386.000

Communication Server 1000E system software

Product Release: 7.65.16.00

Base Applications

base	7.65.16	[patched]
NTAFS	7.65.16	
sm	7.65.16	
cs1000-Auth	7.65.16	
Jboss-Quantum	n/a	[patched]
cnd	7.65.16	
lhmonitor	7.65.16	
baseAppUtils	7.65.16	
dfoTools	7.65.16	
cppmUtil	n/a	[patched]
oam-logging	n/a	[patched]
dmWeb	n/a	[patched]
baseWeb	7.65.16	
ipsec	7.65.16	
Snmp-Daemon-TrapLib	n/a	[patched]
ISECSH	7.65.16	
patchWeb	n/a	[patched]
EmCentralLogic	7.65.16	

Application configuration: CS+SS+NRS+EM

Packages:

CS+SS+NRS+EM

Configuration version:	7.65.16-00	
cs	7.65.16	[patched]
dbcom	7.65.16.21	[patched]
cslogin	7.65.16	
sigServerShare	7.65.16	[patched]
csv	7.65.16	
tps	7.65.16.21	[patched]
vtrk	7.65.16.21	[patched]
pd	7.65.16.21	[patched]
sps	7.65.16.21	[patched]
ncs	7.65.16	
gk	7.65.16.21	[patched]
nrsrm	7.65.16	[patched]
nrsrmWebService	7.65.16	
managedElementWebService	7.65.16	
EmConfig	7.65.16	
emWeb_6-0	7.65.16	[patched]
emWebLocal_6-0	7.65.16	[patched]
csmWeb	7.65.16	[patched]
bcc	7.65.16	[patched]
ftrpkg	7.65.16	
cs1000WebService_6-0	7.65.16	[patched]
mscAnnc	7.65.16.21	[patched]
mscAttn	7.65.16.21	[patched]
mscConf	7.65.16.21	[patched]
mscMusc	7.65.16.21	[patched]
mscTone	7.65.16.21	[patche

©2013 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.