



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

Abstract

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

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

1. Introduction

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Vodafone FMC Trunk 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). The Vodafone FMC Trunk is a fixed and mobile voice connectivity solution. Customers using this can enjoy the benefits of integration of the mobile network with an Avaya SIP-enabled enterprise solution. This allows the user to place PSTN calls as well as the ability to place and receive calls directly to mobile devices on the Vodafone network via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks and 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 FMC Trunk service provided by Vodafone. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1**.

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

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from mobile phones using the FMC Trunk provided by Vodafone, calls made to Unistim, SIP, Digital and Analog telephones at the enterprise
- Incoming calls to the enterprise site from the PSTN routed to the DDI numbers assigned by Vodafone
- Outgoing fixed and mobile calls from the enterprise site completed via Vodafone to PSTN and mobile destinations, were made from Unistim, SIP, Digital and Analog telephones
- Calls using the G.711A and G.729 codec's supported by Vodafone
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls
- User features such as hold and resume, transfer, conference, call forwarding, etc
- Caller ID Presentation and Caller ID Restriction
- Call coverage and call forwarding for endpoints at the enterprise site
- Mobile-X call features
- Off-net call forwarding and mobility (extension to mobile)

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Vodafone FMC Trunk service with the following observations:

- 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.
- When calls are placed on-hold on both inbound and outbound, Vodafone FMC Trunk service requires a RTP stream to be sent in both directions. If no RTP stream is received by Vodafone FMC Trunk, after 2 minutes a BYE is sent from the Vodafone FMC Trunk service and the call is dropped. During testing, music on-hold was configured to ensure RTP was sent in both directions during the call-hold scenario and the call-hold test-cases passed successfully.
- T.38 Fax is not supported by Vodafone UK FMC Trunk service.
- All unwanted MIME was stripped on outbound calls using the Adaptation Module in Session Manager.
- No inbound toll free numbers were tested as none were available from the Service Provider.
- No Emergency Services numbers tested as test calls to these numbers should be pre-arranged with the Operator.

2.3. Support

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

For technical support on Vodafone products please visit the website at <http://www.vodafone.co.uk/business/business-solutions/unified-communications/index.htm> or contact an authorized Vodafone representative.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the Vodafone FMC Trunk service. Located at the enterprise site are Session Manager, Avaya SBCE and CS1000E. Endpoints are Avaya 1140 series IP telephones, Avaya 1200 series (not shown in **Figure 1**) IP telephones (with Unistim and SIP firmware), Avaya IP Softphones (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.

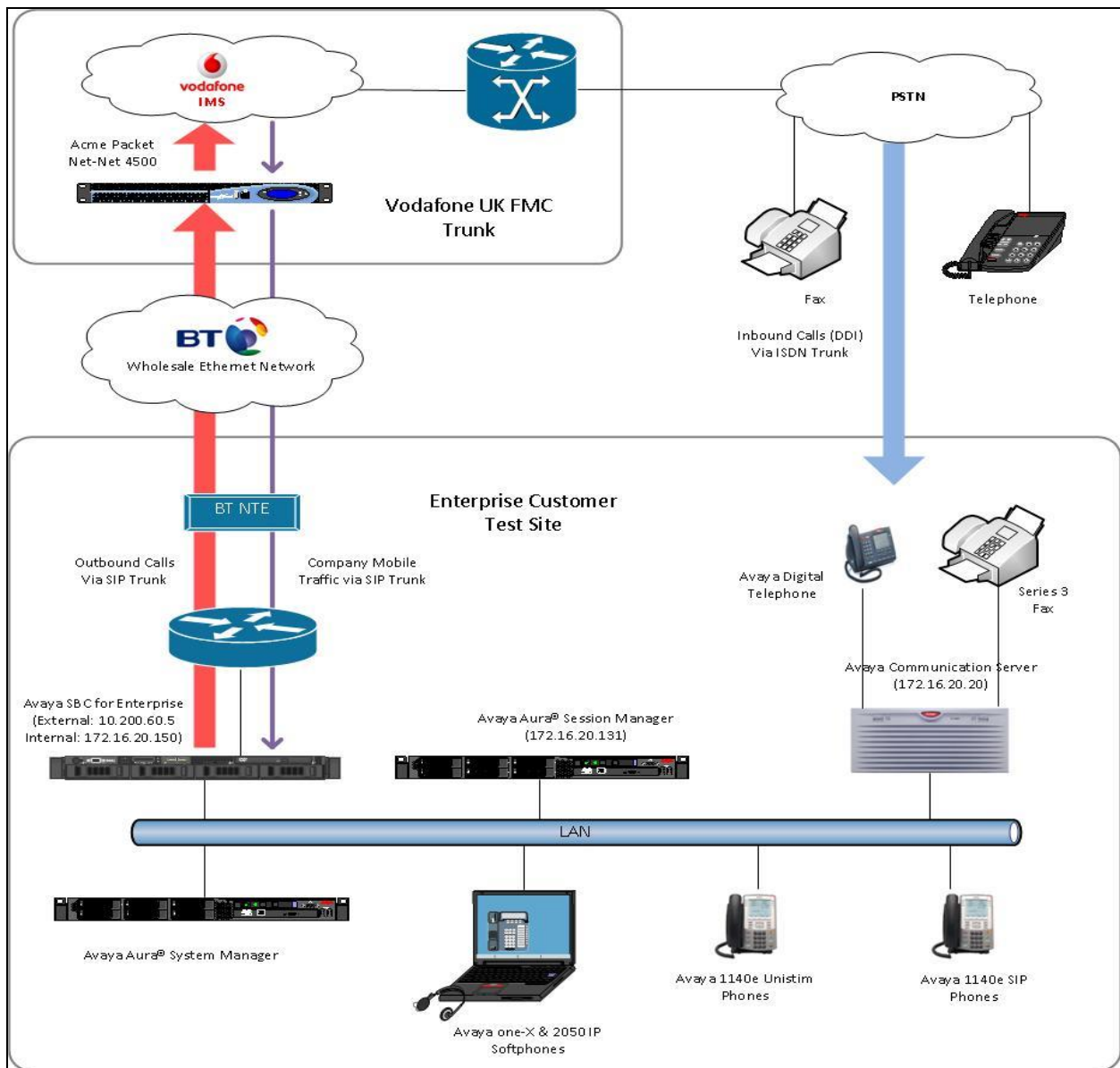


Figure 1: Test Setup Vodafone FMC Trunk to Avaya Enterprise

4. Equipment and Software Validated

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

| Equipment/Software | Release/Version |
|---|---|
| Avaya Aura® Session Manager running on Avaya S8800 server | R6.2 Build: 6.2.3.0.623006 |
| Avaya Aura® System Manager running on Avaya S8800 server | R6.2 Load: 6.2.0.0.15669 Service Pack 4 |
| Avaya Communication Server 1000E | R7.5, Version 7.50.17 Service Update: 7.50_16May12 Deplist: X21 07.50Q |
| Avaya Communication Server 1000E Media Gateway | CSP Version: MGCC CD03 MSP Version: MGCM AB01 APP Version: MGCA BA15 FPGA Version: MGCF AA19 BOOT Version: MGCB BA15 DSP1 Version: DSP1 AB06 |
| Avaya Session Border Controller for Enterprise on Dell R210 V2 server | Build: 4.0.5.Q09 |
| Avaya 1140e and 1220 Unistim Telephones | FW: 0625C8A & 062AC8A |
| Avaya 1140e and 1220 SIP Telephones | FW: 02.02.21.00.bin |
| Avaya 2050PC Softphone | 4.3 |
| Avaya one-X® Communicator | Version cs6.1.0.10-GA-26321 |
| Avaya Analogue Telephone | N/A |
| Avaya M3904 Digital Telephone | N/A |
| Vodafone | |
| SBC ACME Net-Net 4500 | 6.1 |
| CelFocus IP Trunking AS | R11.2 |
| Lucent SIPTRANS UA | V2.2 |

5. Configure Avaya Communication Server 1000E

This section describes the steps required to configure CS1000E for SIP Trunking and also the necessary configuration for telephones (analog, SIP and IP phones). SIP trunks are established between CS1000E and Session Manager. These SIP trunks will carry SIP signalling associated with the Vodafone SIP Trunk service. For incoming calls, Session Manager receives SIP messages from the Avaya SBCE and directs the incoming SIP messages to the CS1000E. Once the message arrives at the CS1000E, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within the CS1000E and may be first subject to outbound features such as route selection, digit manipulation and class of service restrictions. Once the CS1000E selects a SIP trunk, the SIP signalling is routed to Session Manager. Session Manager directs the outbound SIP messages to the Avaya SBCE at the enterprise site that then sends the SIP messages to Vodafone SIP Trunk service. Specific CS1000E configuration was performed using Element

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

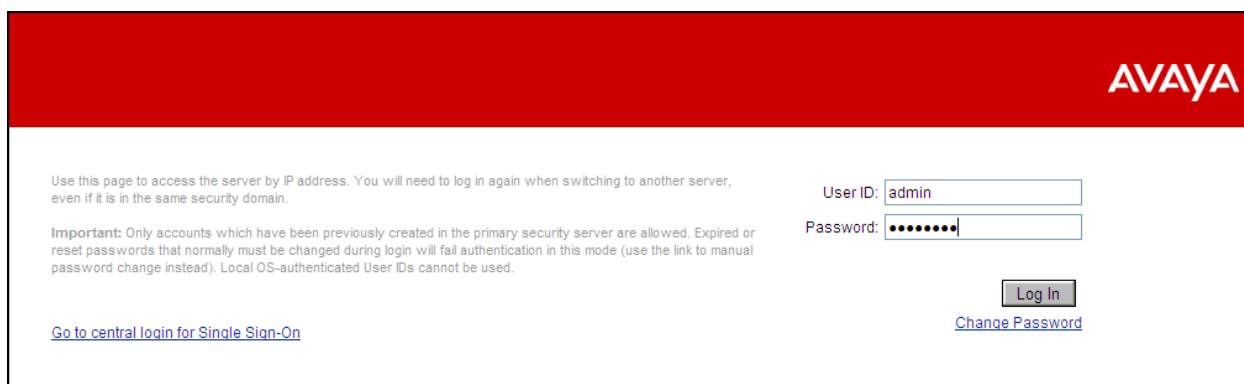
5.1. Log in to the Avaya Communication Server 1000E

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

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

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

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



The login screen features a red header with the AVAYA logo. Below the header, there is a message: "Use this page to access the server by IP address. You will need to log in again when switching to another server, even if it is in the same security domain." To the right of this message are input fields for "User ID:" (containing "admin") and "Password:" (containing "*****"). Below these fields are "Log In" and "Change Password" buttons. At the bottom left, there is a link: "Go to central login for Single Sign-On".

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

Host Name:

Software Version: 02.20_SMGR-SNAPSHOT(4554)

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.

Search

Reset

Add... Edit... Delete

| <input type="checkbox"/> | Element Name | Element Type ^ | Release | Address | Description |
|--------------------------|--|--------------------------|---------|-------------|------------------|
| 1 | smgrv3.avaya.com (primary) | Base OS | 7.5 | 10.10.3.52 | Base OS element. |
| 2 | EM on cs1kv13 | CS1000 | 7.5 | 192.168.1.5 | New element. |
| 3 | cs1kv13.avaya.com (member) | Linux Base | 7.5 | 10.10.3.5 | Base OS element. |
| 4 | 192.168.1.3 | Media Gateway Controller | 7.5 | 192.168.1.3 | New element. |
| 5 | NRSML on cs1kv13 | Network Routing Service | 7.5 | 192.168.1.5 | New element. |

5.2. Confirm System Features

The keycode installed on the Call Server controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity. Use the CS1000E system terminal and manually load overlay 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 Vodafone'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 CS1000E.

| | | | | | |
|--|-----------|-------------|----------|-------------|-----------|
| System type is - Communication Server 1000E/CPPM Linux | | | | | |
| CPPM - Pentium M 1.4 GHz | | | | | |
| IPMGs Registered: 1 | | | | | |
| IPMGs Unregistered: 0 | | | | | |
| IPMGs Configured/unregistered: 0 | | | | | |
| TRADITIONAL TELEPHONES | 11 | LEFT | 1 | USED | 10 |
| DECT USERS | 0 | LEFT | 0 | USED | 0 |
| IP USERS | 116 | LEFT | 110 | USED | 6 |
| BASIC IP USERS | 0 | LEFT | 0 | USED | 0 |
| TEMPORARY IP USERS | 0 | LEFT | 0 | USED | 0 |
| DECT VISITOR USER | 0 | LEFT | 0 | USED | 0 |
| ACD AGENTS | 10 | LEFT | 10 | USED | 0 |
| MOBILE EXTENSIONS | 200 | LEFT | 199 | USED | 1 |
| TELEPHONY SERVICES | 100 | LEFT | 97 | USED | 3 |
| CONVERGED MOBILE USERS | 0 | LEFT | 0 | USED | 0 |
| AVAYA SIP LINES | 5 | LEFT | 3 | USED | 2 |
| THIRD PARTY SIP LINES | 2 | LEFT | 2 | USED | 0 |
| | | | | | |
| PCA | 240 | LEFT | 240 | USED | 0 |
| ITG ISDN TRUNKS | 0 | LEFT | 0 | USED | 0 |
| H.323 ACCESS PORTS | 0 | LEFT | 0 | USED | 0 |
| AST | 474 | LEFT | 474 | USED | 0 |
| SIP CONVERGED DESKTOPS | 0 | LEFT | 0 | USED | 0 |
| SIP CTI TR87 | 120 | LEFT | 120 | USED | 0 |
| SIP ACCESS PORTS | 78 | LEFT | 4 | USED | 74 |

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

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

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

5.3. Configure Codec's for Voice and FAX Operation

Vodafone FMC Trunk service supports G.711A and G.729 codec's. Using the CS1000E element manager sidebar, navigate to the **IP Network → IP Telephony Nodes → Node Details → VGW Gateway (VGW) and Codec's** property page and configure the CS1000E General codec settings as in the next screenshot.

Managing: 172.21.0.11 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » VGW and Codecs

Node ID: 4201 - 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 (squelch DTMF from TDM to IP)
☒ Modem/Fax pass-through
☒ V.21 Fax tone detection
☐ R factor calculation

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

Voice Codecs

Codec G711: ☒ Enabled (required)

Voice payload size: 20 (milliseconds per frame)

Voice playout (jitter buffer) delay: 40 80 (milliseconds)
Nominal Maximum
Maximum delay may be automatically adjusted based on nominal settings.

☐ Voice Activity Detection (VAD)

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



Settings:

Codec G729: ☒ Enabled

Voice payload size: 20 (milliseconds per frame)

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

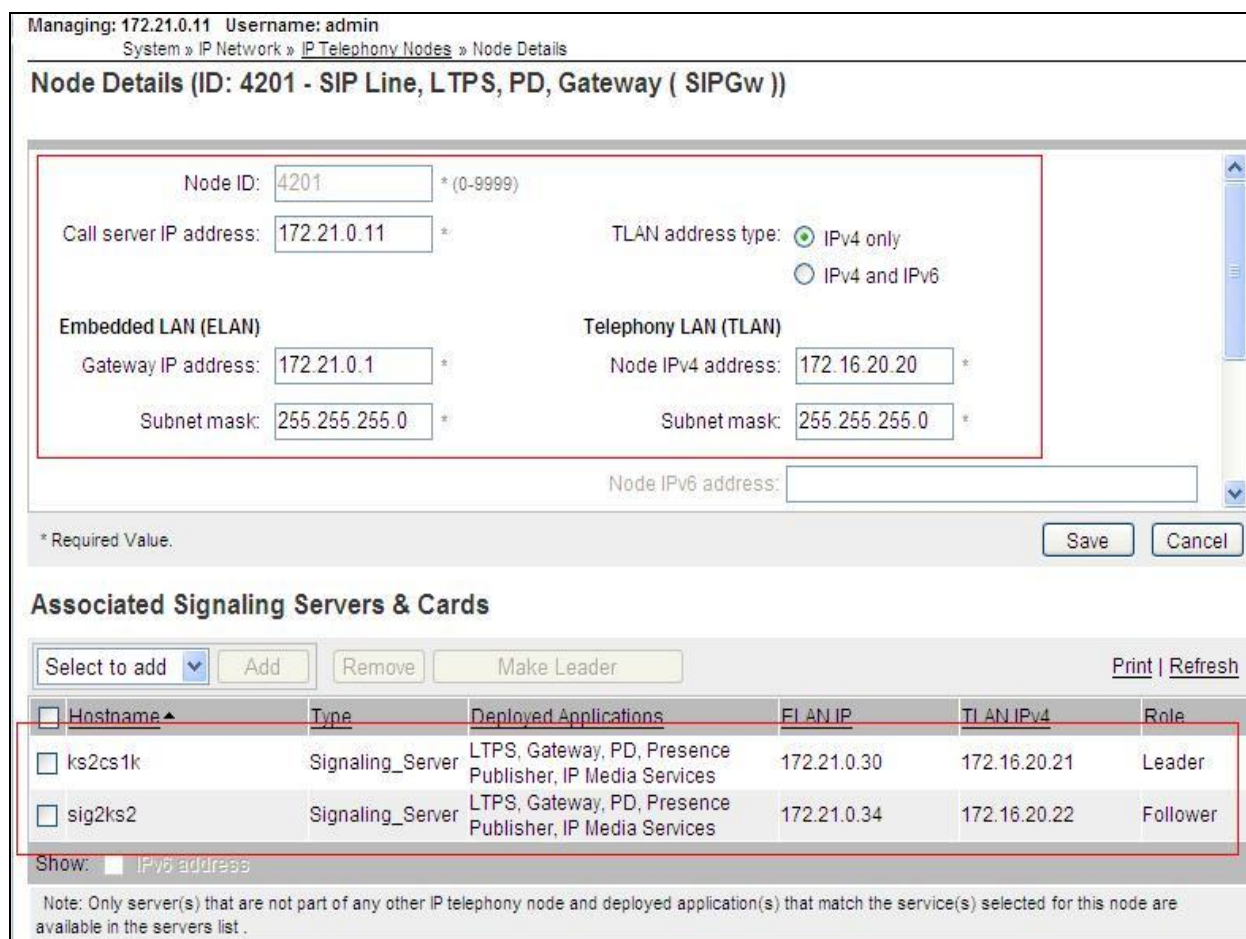
Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

☐ Voice Activity Detection (VAD)

5.4. Virtual Trunk Gateway Configuration

Use CS1000E Element Manager to configure the system node properties. Navigate to the **System → IP Networks → IP Telephony Nodes → Node Details** and verify the highlighted section is completed with the correct IP addresses and subnet masks of the Node. The Node IP 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 (please see **Section 6.5 – Define SIP Entities** for more details).



Managing: 172.21.0.11 Username: admin

System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 4201 - SIP Line, LTPS, PD, Gateway (SIPGw))

Node ID: 4201 * (0-9999)

Call server IP address: 172.21.0.11 *

TLAN address type: ☒ IPv4 only ☐ IPv4 and IPv6

Embedded LAN (ELAN)

Gateway IP address: 172.21.0.1 *

Subnet mask: 255.255.255.0 *

Telephony LAN (TLAN)

Node IPv4 address: 172.16.20.20 *

Subnet mask: 255.255.255.0 *

Node IPv6 address:

* Required Value.

Save Cancel

Associated Signaling Servers & Cards

Select to add Add Remove Make Leader Print Refresh

| Hostname | Type | Deployed Applications | ELAN IP | TLAN IPv4 | Role |
|----------------------------------|------------------|--|-------------|--------------|----------|
| <input type="checkbox"/> ks2cs1k | Signaling_Server | LTPS, Gateway, PD, Presence Publisher, IP Media Services | 172.21.0.30 | 172.16.20.21 | Leader |
| <input type="checkbox"/> sig2ks2 | Signaling_Server | LTPS, Gateway, PD, Presence Publisher, IP Media Services | 172.21.0.34 | 172.16.20.22 | Follower |

Show: ☐ IPv6 address

Note: Only server(s) that are not part of any other IP telephony node and deployed application(s) that match the service(s) selected for this node are available in the servers list.

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 & H323Gw**.
- **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. **vf1.ims.vodafone.co.uk** was used in the compliance testing.
- **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 **4201**.
- **Proxy or Redirect Server:** Primary TLAN IP address is the Security Module IP address of the Session Manager. The **Transport protocol** used for **SIP**, in this case is TCP.
- **SIP URI Map:** **Public National** and **Private Unknown** are left blank. All other fields in the SIP URI Map are left with default values.

Node ID: 4201 - 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: vf1.ims.vodafone.co.uk *

Local SIP port: 5060 * (1 - 65535)

Gateway endpoint name: ks2cs1k *

Gateway password: *

Application node ID: 4201 * (0-9999)

Enable failsafe NRS: ☐

Proxy Server Route 1:

Primary TLAN IP address: 172.16.20.131

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

Port: 5060 (1 - 65535)

Transport protocol: TCP

Options: ☐ Support registration

☐ Primary CDS proxy

Virtual Trunk Network Health Monitor

☐ Monitor IP addresses (listed below)

Information will be captured for the IP addresses listed below.

Monitor IP:

Monitor addresses:

SIP URI Map:

Public E.164 domain names

National:

Subscriber:

Special number:

Unknown:

Private domain names

UDP:

CDP:

Special number:

Vacant number:

Unknown:

5.5. Configure Bandwidth Zones

Bandwidth Zones are used for alternate call routing between IP stations and for Bandwidth Management. SIP trunks require a unique zone, not shared with other resources and best practice dictates that IP telephones and Media Gateways are all placed in separate zones. In the sample configuration SIP trunks use zone 14 and IP & SIP telephones use zone 01, system defaults were used for each zone other than the parameter configured for **Zone Intent**. For SIP Trunks (zone 14), **VTRK** is configured for **Zone Intent**. For IP and SIP Telephones (zone 01), **MO** is configured for **Managed Office**.

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

Managing: 172.21.0.11 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 | 100000 | BQ | SHARED | MO | HSET_VGWI |
| 2 14 | 1000000 | BQ | 100000 | BQ | SHARED | VTRK | IPTI |

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

Managing: 172.21.0.11 Username: admin
Dialing and Numbering Plans » Incoming Digit Translation » Customer 00 » Digit Conversion Tree 2 Configuration

Digit Conversion Tree 2 Configuration

Regular IDC tree
Send calling party DID disabled

Add... Delete IDC Delete IDC tree Refresh

| Incoming Digits | Converted Digits | CPND Name | CPND language |
|-----------------|------------------|-----------|---------------|
| 1 107 | 75 | | |
| 2 910121 | 121 | | |

5.7. Configure SIP Trunks

CS1000E virtual trunks will be used for all inbound and outbound PSTN calls to Vodafone's FMC Trunk service. Six separate steps are required to configure CS1000E virtual trunks.

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

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

```
Overlay 17
ADAN      DCH 66
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 CS1000E system terminal and overlay 16. Load **Overlay 16**, enter **RDB** at the prompt, press return and commence configuration. The value for **DCH** is the same as previously entered in overlay 17. The value for **NODE** should match the node value in **Section 5.4**. The value for **ZONE** should match that used in **Section 5.5** for **VTRK**. The remaining highlighted values are important for correct SIP trunk operation.

| | | |
|---|---|---|
| Overlay 16 TYPE: RDB CUST 00 ROUT 1 TYPE RDB CUST 00 ROUT 66 DES SIPRT TKTP TIE NPID_TBL_NUM 0 ESN NO RPA NO CNVT NO SAT NO RCLS EXT VTRK YES ZONE 00014 PCID SIP CRID NO NODE 4201 DTRK NO ISDN YES MODE ISLD DCH 66 IFC SL1 PNI 00001 NCNA YES NCRD YES TRO YES FALT NO CTYP UKWN INAC NO ISAR NO DAPC NO MBXR YES MBXOT NPA MBXT 0 PTYP ATT CNDP UKWN AUTO NO DNIS NO DCDR NO ICOG IAO SRCH LIN TRMB YES STEP | ACOD 89966 TCPP NO PII NO AUXP NO TARG CLEN 1 BILN NO OABS INST IDC YES DCNO 2 NDNO 2 * DEXT NO DNAM NO SIGO STD STYP SDAT MFC NO ICIS YES OGIS YES TIMR ICF 1920 OGF 1920 EOD 13952 LCT 256 DSI 34944 NRD 10112 DDL 70 ODT 4096 RGV 640 GTO 896 GTI 896 SFB 3 PRPS 800 NBS 2048 NBL 4096 IENB 5 TFD 0 VSS 0 VGD 6 EESD 1024 SST 5 0 DTD NO SCDT NO 2 DT NO NEDC ORG FEDC ORG | CPDC NO DLTN NO HOLD 02 02 40 SEIZ 02 02 SVFL 02 02 DRNG NO CDR NO NATL YES SSL CFWR NO IDOP NO VRAT NO MUS YES MRT 21 PANS YES RACD NO MANO NO FRL 0 0 FRL 1 0 FRL 2 0 FRL 3 0 FRL 4 0 FRL 5 0 FRL 6 0 FRL 7 0 OHQ NO OHQT 00 CBQ NO AUTH NO TTBL 0 ATAN NO OHTD NO PLEV 2 OPR NO ALRM NO ART 0 PECL NO DCTI 0 TIDY 1600 100 ATRR NO TRRL NO SGRP 0 ARDN NO CTBL 0 AACR NO |
|---|---|---|

Next, configure virtual trunk members using the CS1000E system terminal and **Overlay 14**. Configure sufficient trunk members to carry both incoming and outgoing PSTN calls. The following example shows a single SIP trunk member configuration. Load **Overlay 14** at the system terminal and type **new X**, where X is the required number of trunks. Continue entering data until the overlay exits. The **RTMB** value is a combination of the **ROUT** value entered in the previous step and the first trunk member (usually 1). The remaining highlighted values are important for correct SIP trunk operation.

```

Overlay 14
TN    100 0 0 0
DATE
PAGE
DES   SIP_TRK
TN    100 0 00 00  VIRTUAL
TYPE IPTI
CDEN  8D
CUST  0
XTRK VTRK
ZONE 00014
TIMP  600
BIMP  600
AUTO_BIMP NO
NMUS  NO
TRK   ANLG
NCOS  0
RTMB 66 1
CHID  1
TGAR  1
STRI/STRO WNK WNK
SUPN  YES
AST   NO
IAPG  0
CLS   UNR DTN 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 0
DEL 0
ISPN NO
CTYP INTL

```

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> Overlay 86 CUST 0 FEAT rlb RLI 2 ELC NO ENTR 0 LTER NO ROUT 66 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 0 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 OVL 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 003 | TSC 009 | TSC 0128320 | TSC 0128327 |
| FLEN 16 | FLEN 16 | FLEN 11 | FLEN 11 |
| RRPA NO | RRPA NO | RRPA NO | RRPA NO |
| RLI 2 | RLI 2 | RLI 2 | RLI 2 |

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**. The value for **CFG_ZONE** is the value used in **Section 5.5** for IP and SIP Telephones.

Overlay 20 IP Telephone configuration

```
DES 1140
TN 248 0 00 02 VIRTUAL
TYPE 1140
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00001
CUR_ZONE 00001
ERL 0
ECL 0
FDN 0
TGAR 0
LDN NO
NCOS 0
SGRP 0
RNPG 1
SCI 0
SSU
LNRS 16
XLST
SCPW
SFLT NO
CAC_MFC 0
CLS UNR FBA WTA LPR PUA MTD FNA HTA TDD HFA CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LNA CNDA
CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
ICDA CDMD LLCN MCTD CLBD AUTR
GPUD DPUD DNDA CFXA ARHD FITD CLTD ASCD
CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
UDI RCC HBTA AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
DRDD EXR0
USMD USRD ULAD CCBF RTDD RBDD RBHD PGND OCBF FLXD FTTC DNDY DNO3 MCBN
FDSD NOVD VOLA VOUD CDMR PRED RECA MCDD T87D SBMD KEM3 MSNV FRA PKCH MUTA MWTD
```

---continued on next page---

---continued from previous page---

```
DVLD CROD CROD
CPND_LANG ENG
RCO 0
HUNT 0
LHK 0
PLEV 02
PUID
DANI NO
AST 00
IAPG 1
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY 00 MCR 7520 0      MARP
      CPND
      CPND_LANG ROMAN
      NAME IP1140
      XPLN 10
      DISPLAY_FMT FIRST, LAST
01 HNDO
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** value.

Overlay 20 - Digital Set configuration

TYPE: 3904

```
DES 3904
TN 000 0 01 02 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 7526 0 MARP

CPND

CPND_LANG ROMAN

NAME Digital Set

XPLN 10

DISPLAY_FMT FIRST, LAST

02

03

04

05

06

07

08

09

10

11

12

13

14

15

16

17 TRN

18 AO6

19 CFW 16

20 RGA

21 PRK

22 RNP

23

24 PRS

25 CHG

26 CPN

27 CLT

28 RLT

29

30

31

Analog telephones are also configured using **Overlay 20**, the following example shows an analog port configured for Plain Ordinary Telephone Service (POTS). A unique value is entered for **DN**, this is the extension number. **DTN** is required if the telephone uses DTMF dialing.

Overlay 20 - Analog Telephone Configuration

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

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

5.9. Configure the SIP Line Gateway Service

SIP terminal operation requires the Communication Server node to be configured as a SIP Line Gateway (SLG) before SIP telephones can be configured. Prior to configuring the SIP Line node properties, the SIP Line service must be enabled in the customer data block. Use the CS1000E system terminal and **Overlay 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: 172.21.0.11 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » SIP Line Configuration

Node ID: 4201 - 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: vf1.ims.vodafone *

SLG endpoint name:

SLG Group ID:

SLG Local Sip port: 5070 (1 - 65535)

SLG Local Tls port: 5071 (1 - 65535)

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

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 used in **Section 5.5** for IP and SIP Telephones. A unique telephone number is entered for value **KEY 00**. The value for **KEY 01** is comprised of the **UAPR** (set in **Section 5.8**) value and the telephone number used in **KEY 00**.

Overlay 20 - SIP Telephone Configuration

```
DES  SIPD
TN    100 0 01 10  VIRTUAL
TYPE  UEXT
CDEN  8D
CTYP  XDLC
CUST  0
UXTY SIPL
MCCL  YES
SIPN 1
SIP3  0
FMCL  0
TLSV  0
SIPU 7528
NDID 4201
SUPR  NO
SUBR  DFLT MWI RGA CWI MSB
UXID
NUID  100
NHTN  100 0 01 10
CFG_ZONE 00001
CUR_ZONE 00001
ERL   0
ECL   0
VSIT  NO
FDN
TGAR  0
LDN   NO
NCOS  0
SGRP  0
RNPG  0
SCI   0
SSU
XLST
SCPW 1234
SFLT  NO
CAC   MFC 0
CLS   UNR FBD WTA LPR MTD FNA HTA TDD HFD CRPD
      MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
      POD SLKD CCSD SWD LND CNDA
      CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
      ICDD CDMD LLCN MCTD CLBD AUTU
      GPUD DPUD DNDA CFXA ARHD FITD CLTD ASCD
      CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
```

---continued on next page---

---continued from previous page---

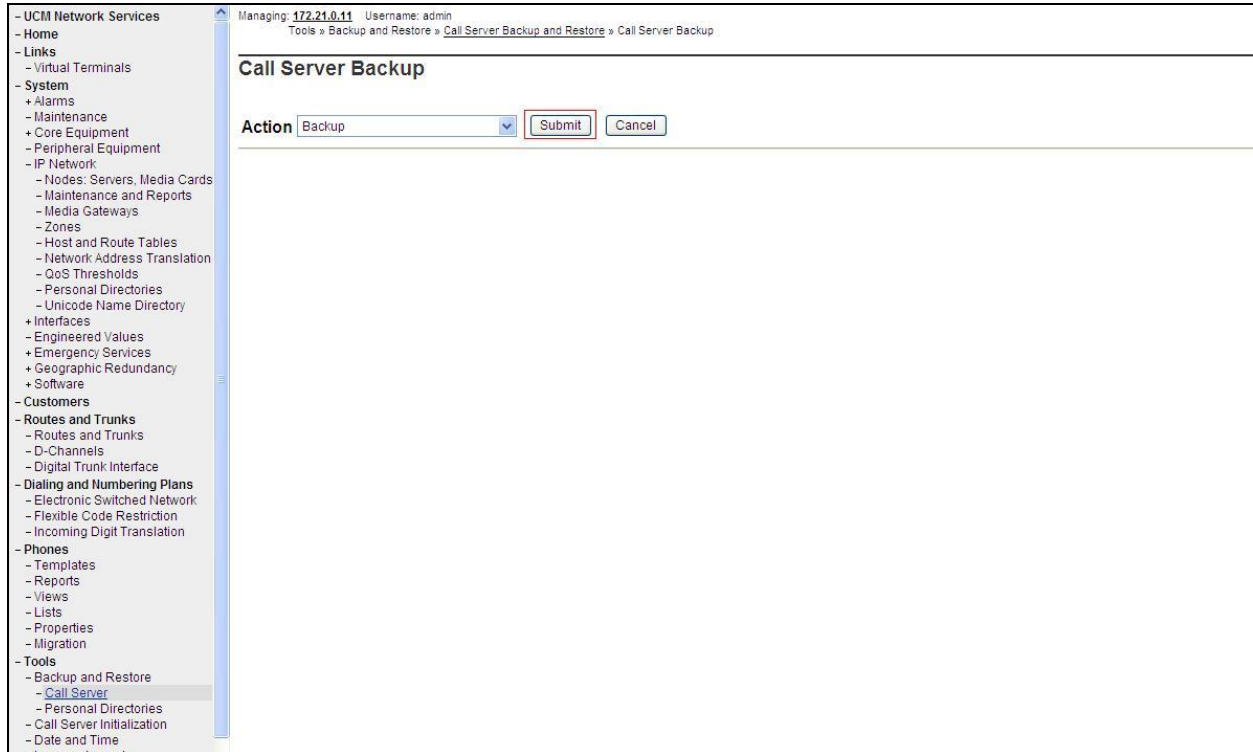
```

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

AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY 00 SCR 7528 0      MARP
    CPND
        CPND_LANG ROMAN
        NAME Sigma 1140
        XPLN 11
        DISPLAY_FMT FIRST, LAST*
01 HOT U 117528 MARP 0
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16
17 TRN
18 AO6
19 CFW 16
20 RGA
21 PRK
22 RNP
23 *
24 PRS
25 CHG
26 CPN
27
28
29
30
31
```

5.11. Save Configuration

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



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.



Configuration of CS1000E is complete.

6. Configure Avaya Aura® Session Manager

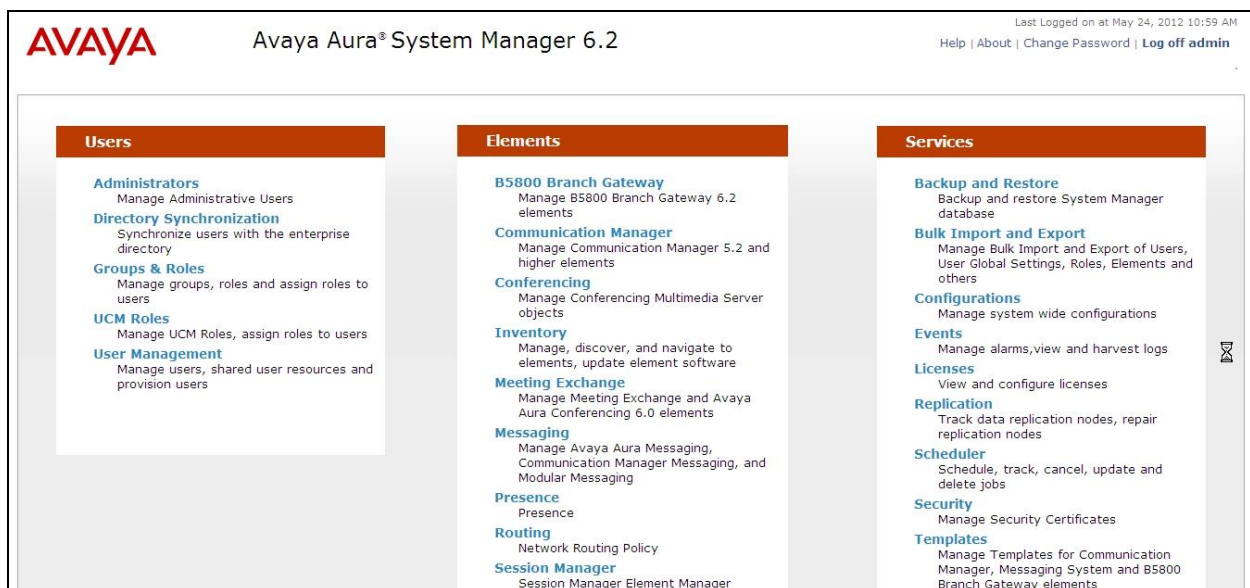
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

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

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

6.1. Avaya Aura® System Manager Login and Navigation

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



Most of the configuration items are performed in the Routing Element. Click on **Routing** in the Elements column shown above to bring up the Introduction to Network Routing Policy screen.

Avaya Aura® System Manager 6.2

Help | About | Change Password | Log o

Routing x

Home / Elements / Routing

Introduction to Network Routing Policy

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

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

- Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
- Step 2: Create "Locations"
- Step 3: Create "Adaptations"
- Step 4: Create "SIP Entities"
 - SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
 - Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
 - Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"
- Step 5: Create the "Entity Links"
 - Between Session Managers
 - Between Session Managers and "other SIP Entities"
- Step 6: Create "Time Ranges"

6.2. Define SIP Domain

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

- **Name** Enter the Domain Name specified for the SIP Gateway in **Section 5.4**. In the sample configuration, **vf1.ims.vodafone.co.uk** 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.

Home / Elements / Routing / Domains

Help ?

Domain Management

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

Commit Cancel

1 Item Refresh Filter: Enable

| Name | Type | Default | Notes |
|--------------------------|------|--------------------------|-------|
| * vf1.ims.vodafone.co.uk | sip | <input type="checkbox"/> | |

* Input Required

Commit Cancel

6.3. Define Location for Avaya Communication Server 1000E

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

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

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

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

- **IP Address Pattern** Enter the logical pattern used to identify the location. For the sample configuration, **172.16.20.*** was used
- **Notes** Add a brief description [Optional]

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

The screenshot displays the 'Home / Elements / Routing / Locations' configuration page. It features two main sections: 'Location' and 'Location Pattern'.

Location Section:

- Buttons: Edit, New, Duplicate, Delete, More Actions.
- Table with 1 item: KS2. The table has columns for Name and Notes.
- Filter: Enable
- Select: All, None

Location Pattern Section:

- Buttons: Add, Remove.
- Table with 1 item: *172.16.20.*. The table has columns for IP Address Pattern and Notes.
- Filter: Enable
- Select: All, None

At the bottom, there is a red asterisk icon and the text '* Input Required', along with Commit and Cancel buttons.

6.4. Configure Adaptation Module

Adaptations can be used to modify the called and calling party numbers to meet the requirements of the service. The called party number present in the SIP INVITE Request URI is modified by the **Digit Conversion** in the Adaptation. **MIME=no** strips MIME message bodies on egress from Session Manager to the Avaya SBCE. Additionally, the called and calling party numbers can be modified using **Digit Conversion** when **fromto=true** is entered in the **Module Parameters**.

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

The screenshot shows the 'Adaptation Details' form in the Session Manager interface. The breadcrumb navigation at the top reads 'Home / Elements / Routing / Adaptations'. On the right, there are 'Commit' and 'Cancel' buttons, and a 'Help ?' link. The 'General' tab is selected. The form fields are as follows:

- * Adaptation name:** CS1K
- Module name:** DigitConversionAdapter (selected from a dropdown menu)
- Module parameter:** fromto=true MIME=no
- Egress URI Parameters:** (empty text field)
- Notes:** (empty text field)

6.5. Define SIP Entities

A SIP Entity must be added for Session Manager and for each SIP server connected to it, which includes CS1000E and Avaya SBCE. Navigate to **Routing → SIP Entities** in the left-hand navigation pane and click on 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
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling
- **Type:** Enter **Session Manager** for Session Manager, **Other** for CS1000E and **Gateway** for Avaya SBCE
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the **Adaptation Name** that will be applied to this entity
- **Location:** Select one of the locations defined previously
- **Time Zone:** Select the time zone for the location above

In the **SIP Link Monitoring** section:

- **SIP Link Monitoring** Select **Use Session Manager**

The following screen shows the addition of Session Manager. The IP address of the Session Manager signaling interface is entered for **FQDN or IP Address**.

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

* Name: ks2-asm

* FQDN or IP Address: 172.16.20.131

Type: Session Manager

Notes: Session Manager

Location: KS2

Outbound Proxy:

Time Zone: Etc/GMT

Credential name:

SIP Link Monitoring: Use Session Manager Configuration

Commit Cancel Help ?

To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities. This section defines a default set of ports that Session Manager will use to listen for SIP requests, typically from registered SIP endpoints. Session Manager can also listen on additional ports defined elsewhere such as the ports specified in the SIP Entity Link definition in **Section 6.6**.

In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:

- **Port:** Port number on which Session Manager can listen for requests
- **Protocol:** Transport protocol to be used to send SIP requests
- **Default Domain:** The domain used for the enterprise

Defaults can be used for the remaining fields. Click **Commit** to save.

Port

TCP Failover port:

TLS Failover port:

8 Items Refresh Filter: Enable

| <input type="checkbox"/> | Port | Protocol | Default Domain | Notes |
|--------------------------|------|----------|------------------------|----------------------|
| <input type="checkbox"/> | 5060 | TCP | vf1.ims.vodafone.co.uk | <input type="text"/> |
| <input type="checkbox"/> | 5060 | UDP | vf1.ims.vodafone.co.uk | <input type="text"/> |

The following screen shows the addition of CS1000E SIP Entity. The **FQDN or IP Address** field is set to the TLAN Node IP address defined in **Section 5.4**.

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds):

Credential name:

Call Detail Recording:

CommProfile Type Preference:

SIP Link Monitoring

SIP Link Monitoring:

[Help ?](#)

The following screen shows the addition of Avaya SBCE SIP Entity. The **FQDN or IP Address** field is set to the IP address of its private network interface.

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

- Name:** ks2-sbc
- * FQDN or IP Address:** 172.16.20.150
- Type:** Other (dropdown menu)
- Notes:** Sipera SBC
- Adaptation:** CS1K (dropdown menu)
- Location:** KS2 (dropdown menu)
- Time Zone:** Europe/London (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)
- CommProfile Type Preference:** (empty dropdown menu)
- SIP Link Monitoring:** Use Session Manager Configuration (dropdown menu)

6.6. Define Entity Links

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

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

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

Entity Link to CS1000E.

The screenshot shows the 'Entity Links' configuration page. At the top, there are 'Add' and 'Remove' buttons. Below them is a table with the following columns: 'SIP Entity 1', 'Protocol', 'Port', 'SIP Entity 2', 'Port', and 'Connection Policy'. A single row is displayed with the following values: 'ks2-asm' for SIP Entity 1, 'TCP' for Protocol, '5060' for Port, 'ks2cs1k' for SIP Entity 2, '5060' for Port, and 'Trusted' for Connection Policy. A red box highlights the row. At the bottom, there is a 'Select : All, None' dropdown.

| SIP Entity 1 | Protocol | Port | SIP Entity 2 | Port | Connection Policy |
|--------------|----------|------|--------------|------|-------------------|
| ks2-asm | TCP | 5060 | ks2cs1k | 5060 | Trusted |

Entity Link to Avaya SBCE.

Entity Links

Add Remove

2 Items Refresh Filter: Enable

| <input type="checkbox"/> | SIP Entity 1 | Protocol | Port | SIP Entity 2 | Port | Connection Policy |
|--------------------------|--------------|----------|-------|--------------|-------|-------------------|
| <input type="checkbox"/> | ks2-asm | UDP | *5060 | ks2-sbc | *5060 | Trusted |
| <input type="checkbox"/> | ks2-asm | TCP | *5060 | ks2-sbc | *5060 | Trusted |

Select : All, None

6.7. Define Routing Policies

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

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

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

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

The following screenshot shows the Routing Policy for CS1000E.

Home / Elements / Routing / Routing Policies

Routing Policy Details [Help ?](#)

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

| Name | FQDN or IP Address | Type | Notes |
|---------|--------------------|-------|-------|
| ks2cs1k | 172.16.20.20 | Other | CS1K |

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

The following screenshot shows the Routing Policy for Avaya SBCE – Vodafone’s FMC Trunk service.

Home / Elements / Routing / Routing Policies

Routing Policy Details [Help ?](#)

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

| Name | FQDN or IP Address | Type | Notes |
|---------|--------------------|-------|------------|
| ks2-sbc | 172.16.20.150 | Other | Sipera SBC |

6.8. Define Dial Patterns

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

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

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

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

An example of a dial pattern used for the compliance test is shown below.

The screenshot shows the 'Dial Pattern Details' form in the Session Manager web interface. The form is divided into two sections: 'General' and 'Originating Locations and Routing Policies'.

General Section:

- Pattern:** +
- Min:** 1
- Max:** 36
- Emergency Call:** ☐
- Emergency Priority:** 1
- Emergency Type:**
- SIP Domain:** -ALL-
- Notes:**

Originating Locations and Routing Policies Section:

Buttons: Add, Remove

5 Items 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"/> | KS2 | KS2 Burton | Avaya CS1K | 0 | <input type="checkbox"/> | ks2cs1k | |
| <input type="checkbox"/> | KS2 | KS2 Burton | Sipera SBC | 0 | <input type="checkbox"/> | ks2-sbc | |

7. Configure Avaya Session Border Controller for Enterprise

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

7.1. Access Avaya Session Border Controller for Enterprise

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



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



7.2. Global Profiles

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

7.2.1. Server Interworking - Avaya Side

Server Internetworking configures and manages various SIP call server specific capabilities such as call hold and T.38. In this case, the Avaya SBCE is connected as the Trunk Server and the Session Manager is connected as the Call Server.

To define server interworking on the Avaya SBCE, navigate to **Global Profiles → Server Interworking** and click on **Add Profile** (Not Shown).

- Enter profile name such as **Avaya SM** and click **Next** (Not Shown)
- Check **T.38 Support** (not required but checked to avoid restriction on SBC)
- All other options on the **General** Tab can be left at default

Click **Next** to continue.

| Profile: Avaya SM | |
|--------------------------|--|
| General | |
| Hold Support | <input type="radio"/> None <input checked="" type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly |
| 180 Handling | <input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP |
| 181 Handling | <input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP |
| 182 Handling | <input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP |
| 183 Handling | <input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP |
| Refer Handling | <input type="checkbox"/> |
| 3xx Handling | <input type="checkbox"/> |
| Diversion Header Support | <input type="checkbox"/> |
| Delayed SDP Handling | <input type="checkbox"/> |
| T.38 Support | <input checked="" type="checkbox"/> |
| URI Scheme | <input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY |
| Via Header Format | <input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543 |

Next

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

The screenshot shows a window titled "Profile: Avaya SM" with a close button in the top right corner. The window contains two sections: "Privacy" and "DTMF".

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

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

At the bottom of the window are two buttons: "Back" and "Finish".

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

The screenshot shows a window titled "Profile: Avaya SM" with a close button in the top right corner. The window contains an "Advanced Settings" section.

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

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

7.2.2. Server Interworking – Vodafone Side

Server Interworking configures and manages various SIP call server specific capabilities such as call hold and T.38. In this case, the Avaya SBCE is connected as the Trunk Server and the Session Manager is connected as the Call Server.

To define server interworking on the Avaya SBCE, navigate to **Global Profiles → Server Interworking** and click on **Add Profile** (Not Shown).

- Enter profile name such as **Vodafone ONE** and click **Next** (Not Shown)
- Check **Hold Support= RFC2543**
- Check **T.38 Support** (not required but checked to avoid restriction on SBC)
- All other options on the **General** Tab can be left at default

Click **Next** to continue.

| Profile: Vodafone ONE | |
|--------------------------|--|
| General | |
| Hold Support | <input type="radio"/> None <input checked="" type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly |
| 180 Handling | <input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP |
| 181 Handling | <input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP |
| 182 Handling | <input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP |
| 183 Handling | <input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP |
| Refer Handling | <input type="checkbox"/> |
| 3xx Handling | <input type="checkbox"/> |
| Diversion Header Support | <input type="checkbox"/> |
| Delayed SDP Handling | <input type="checkbox"/> |
| T.38 Support | <input checked="" type="checkbox"/> |
| URI Scheme | <input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY |
| Via Header Format | <input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543 |
| Next | |

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

The screenshot shows a window titled "Profile: Vodaone ONE" with a close button in the top right corner. The window contains two sections: "Privacy" and "DTMF".

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

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

At the bottom of the window are two buttons: "Back" and "Finish".

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

The screenshot shows a window titled "Profile: Vodaone ONE" with a close button in the top right corner. The window contains an "Advanced Settings" section with a list of settings and their values.

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

At the bottom of the window is a button: "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 the Session Manager on the internal side and the Avaya SBCE on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop IP Address**, default 5060 is used.

Create a Routing Profile for Session Manager and a Routing Profile for Vodafone FMC Trunk service. 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 (not shown), enter the following values. Use default values for all remaining fields:

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

Click **Finish** (not shown).

The following screen shows the Routing Profile to Session Manager. The **Next Hop Server 1** IP address must match the IP address of the Session Manager Security Module in **Section 6.5**.

| Priority | URI Group | Next Hop Server 1 | Next Hop Server 2 | Next Hop Priority | NAPTR | SRV | Next Hop in Dialog | Ignore Route Header | Outgoing Transport |
|----------|-----------|-------------------|-------------------|-------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------|
| 1 | * | 172.16.20.131 | --- | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | TCP |

The following screen shows the Routing Profile to Vodafone.

Global Profiles > Routing: Vodafone ONE

[Add Profile](#) [Rename Profile](#) [Clone Profile](#) [Delete Profile](#)

Click here to add a description.

Routing Profile

[Add Routing Rule](#)

| Priority | URI Group | Next Hop Server 1 | Next Hop Server 2 | Next Hop Priority | NAPTR | SRV | Next Hop in Dialog | Ignore Route Header | Outgoing Transport |
|----------|-----------|-------------------|-------------------|-------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------|
| 1 | * | 192.168.2.158 | --- | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | UDP |

7.2.4. Server - Configuration

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

7.2.4.1 Server - Configuration – Avaya Side

Servers are defined for each server connected to the Avaya SBCE. In this case, the Vodafone SBC is connected as the Trunk Server and the Session Manager is connected as the Call Server. To add a Server Configuration Profile for Session Manager, navigate to **UC-Sec Control Center** → **Global Profiles** → **Server Configuration** and click on **Add Profile** (not shown). In the new window that appears, enter the following values. Use default values for all remaining fields:

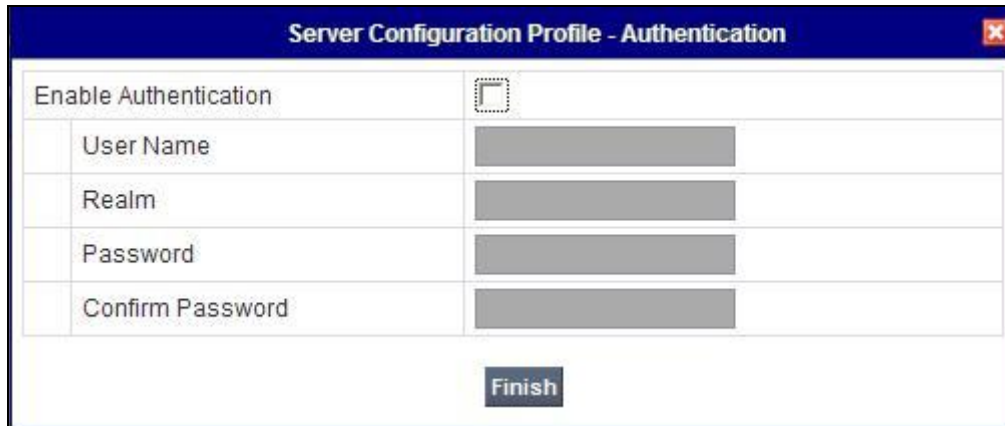
- **Server Type:** Select **Call Server** from the drop-down box
- **IP Addresses / Supported FQDNs:** Enter the IP address of the Session Manager signaling interface. This should match the IP address of the Session Manager Security Module in **Section 6.5**
- **Supported Transports:** Select the transport protocol used to create the Avaya SBCE Entity Link on Session Manager in **Section 6.6**
- **TCP/UDP Port:** Port number on which to send SIP requests to Session Manager. This should match the port number used in the Avaya SBCE Entity Link on Session Manager in **Section 6.6**

Click **Finish** to continue.

Server Configuration Profile - General

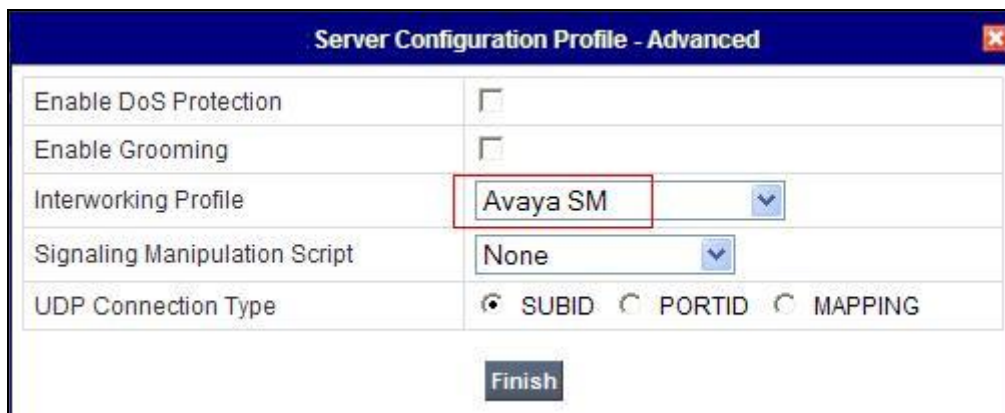
| | |
|--|--|
| Server Type | Call Server |
| IP Addresses / Supported FQDNs Comma separated list | 172.16.20.131 |
| Supported Transports | <input checked="" type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS |
| TCP Port | 5060 |
| UDP Port | 5060 |
| TLS Port | |
| Finish | |

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



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

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



| Server Configuration Profile - Advanced | |
|---|---|
| Enable DoS Protection | <input type="checkbox"/> |
| Enable Grooming | <input type="checkbox"/> |
| Interworking Profile | Avaya SM <input type="button" value="v"/> |
| Signaling Manipulation Script | None <input type="button" value="v"/> |
| UDP Connection Type | <input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING |
| Finish | |

7.2.4.2 Server - Configuration - Vodafone

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

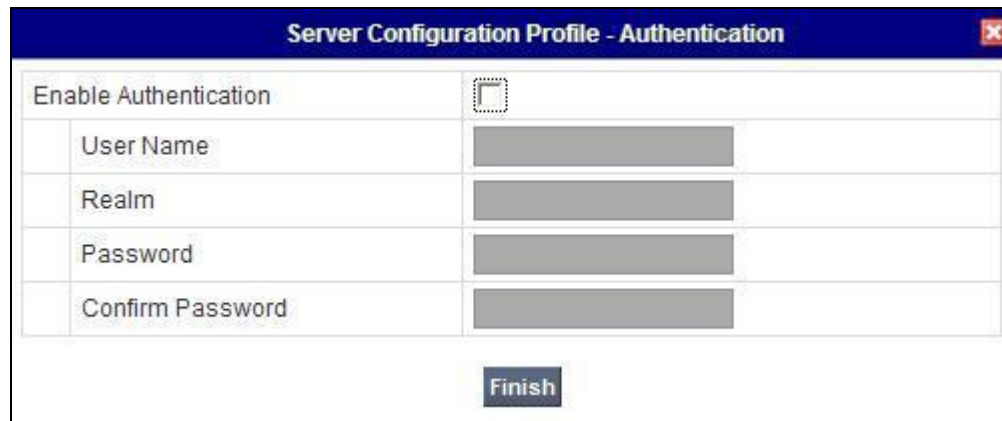
- **Server Type:** Select **Trunk Server** from the drop-down box
- **IP Addresses / Supported FQDNs:** Enter the IP address(es) of the SIP proxy(ies) of the service provider. This will associate the inbound SIP messages from Vodafone to this Sever Configuration
- **Supported Transports:** Select the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

Click **Finish** to continue.

The screenshot shows a window titled "Server Configuration Profile - General" with a close button in the top right corner. The window contains several fields and checkboxes:

- Server Type:** A dropdown menu with "Trunk Server" selected.
- IP Addresses / Supported FQDNs:** A text area with "192.168.2.158" entered. Below the text area is a label "Comma seperated list".
- Supported Transports:** Three checkboxes: "TCP" (unchecked), "UDP" (checked), and "TLS" (unchecked).
- TCP Port:** A text field that is currently empty.
- UDP Port:** A text field with "5060" entered.
- TLS Port:** A text field that is currently empty.
- Finish:** A button at the bottom center of the window.

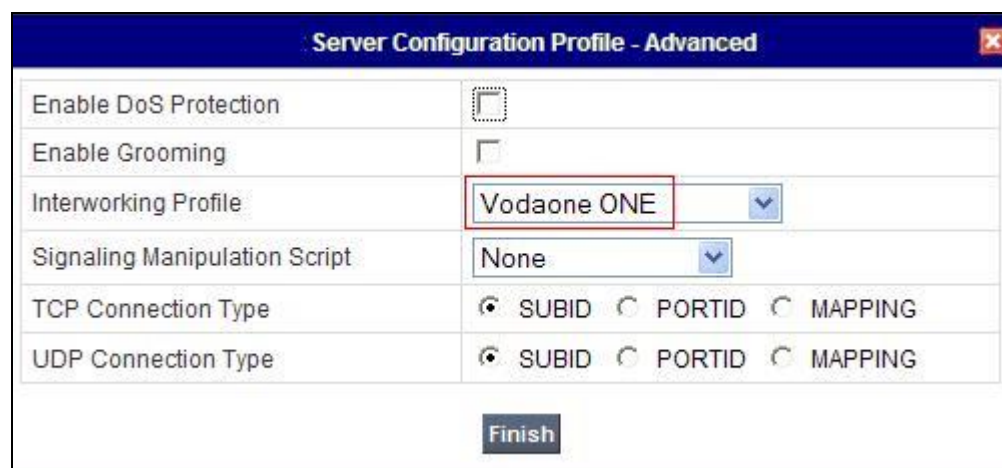
In the new window that appears, verify **Enable Authentication** is unchecked as Vodafone do not require authentication. Click **Finish**.



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

Finish

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



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

Finish

7.2.5. 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 the Session Manager and click **Next**
- If the **Request-Line**, **Record-Route** and **Via** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu
- For both of the above headers, leave the **Replace Action** at the default value of **Auto**
- If the **From** and **To** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu
- For each of the above headers, select **IP** from the **Criteria** drop down menu (important for the **From** header so that the "anonymous.invalid" domain name for restricted CLI is not overwritten)
- For each of the headers leave the **Replace Action** at the default value of **Auto**

Global Profiles > Topology Hiding: Avaya SM

Buttons: Add Profile, Rename Profile, Clone Profile, Delete Profile

Topology Hiding Profiles

- default
- cisco_th_profile
- Avaya SM
- Vodafone ONE

Click here to add a description.

Topology Hiding

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

Edit

Note: The use of **Auto** results in an IP address being inserted in the host portion of the Request-URI as opposed to a domain name. If a domain name is required, the action **Overwrite** must be used where appropriate, and the required domain names entered in the **Overwrite Value** field. Different domain names could be used for the enterprise and the Vodafone network.

To define Topology Hiding for the Vodafone SBC, 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 Vodafone SBC and click **Next**
- If the **Request-Line**, **Record-Route** and **Via** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu
- For each of the above headers, leave the **Replace Action** at the default value of **Auto**
- If the **From** and **To** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu
- For each of the above headers, select **IP** from the **Criteria** drop down menu (important for the **From** header so that the "anonymous.invalid" domain name for restricted CLI is not overwritten)
- For each of the headers leave the **Replace Action** at the default value of **Auto**

Global Profiles > Topology Hiding: Vodafone ONE

Buttons: Add Profile, Rename Profile, Clone Profile, Delete Profile

Click here to add a description.

Topology Hiding

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

Edit

7.3. Device Specific Settings

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

7.3.1. Network Management

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

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

The screenshot shows the 'Device Specific Settings > Network Management: Pathway_SBC_E' window. On the left, a sidebar lists 'UC-Sec Devices' with 'Pathway_SBC_E' selected. The main area has two tabs: 'Network Configuration' (active) and 'Interface Configuration'. A yellow warning banner states: '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.' Below this, there are input fields for 'A1 Netmask' (255.255.255.0), 'A2 Netmask' (empty), 'B1 Netmask' (255.255.255.252), and 'B2 Netmask' (empty). There are 'Add IP', 'Save Changes', and 'Clear Changes' buttons. A table below shows IP configurations:

| IP Address | Public IP | Gateway | Interface |
|---------------|-----------|-------------|-----------|
| 172.16.20.150 | | 172.16.20.1 | A1 |
| 10.200.60.5 | | 10.200.60.6 | B1 |

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

The screenshot shows the same 'Device Specific Settings > Network Management: Pathway_SBC_E' window, but with the 'Interface Configuration' tab selected. The 'Network Configuration' tab is now inactive. The interface displays a table with the following data:

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

7.3.2. Media Interface

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

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

- Select **Add Media Interface**
- **Name: Avaya SM**
- **Media IP: 172.16.20.150** (Internal address for calls toward CS1000E)
- **Port Range: 35000-40000**
- Click **Finish**
- Select **Add Media Interface**
- **Name: Vodafone ONE**
- **Media IP: 10.200.60.5** (External address for calls toward Vodafone)
- **Port Range: 35000-40000**
- Click **Finish**

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

Device Specific Settings > Media Interface: Pathway_SBC_E

UC-Sec Devices

Pathway_SBC_E

Media Interface

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

Add Media Interface

| Name | Media IP | Port Range | | |
|--------------|---------------|---------------|--|--|
| Avaya SM | 172.16.20.150 | 35000 - 40000 | | |
| Vodafone ONE | 10.200.60.5 | 35000 - 40000 | | |

7.3.3. Signalling Interface

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

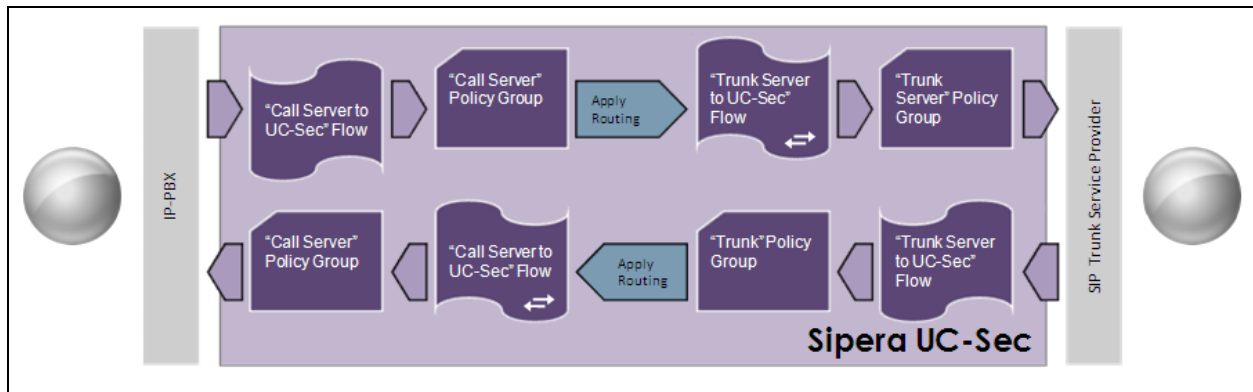
- **Name: Avaya SM**
- **Signaling IP: 172.16.20.150** (Internal address for calls toward CS1000E)
- **TCP Port: 5060**
- **UDP Port: 5060**
- Click **Finish**
- Select **Add Signaling Interface**
- **Name: Vodafone ONE**
- **Signaling IP: 10.200.60.5** (External address for calls toward Vodafone)
- **TCP Port: 5060**
- **UDP Port: 5060**
- Click **Finish**

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

| Name | Signaling IP | TCP Port | UDP Port | TLS Port | TLS Profile | | |
|--------------|---------------|----------|----------|----------|-------------|--|--|
| Avaya SM | 172.16.20.150 | 5060 | 5060 | --- | None | | |
| Vodafone ONE | 10.200.60.5 | 5060 | 5060 | --- | None | | |

7.3.4. End Point Flows

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



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



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

Click **Finish** to save and exit.

The following screen shows the Sever Flow for Session Manager.

| Server Configuration: Avaya SM | | | | | | | | | | | | | |
|--------------------------------|--------------|-----------|-----------|---------------|--------------------|---------------------|-----------------|------------------------|-----------------|-------------------------|-----------------------|---|---|
| Priority | Flow Name | URI Group | Transport | Remote Subnet | Received Interface | Signaling Interface | Media Interface | End Point Policy Group | Routing Profile | Topology Hiding Profile | File Transfer Profile | | |
| 1 | Inbound Flow | * | * | * | Vodafone ONE | Avaya SM | Avaya SM | default-low | Vodafone ONE | Avaya SM | None |  |  |

The following screen shows the Sever Flow for Vodafone.

| Server Configuration: Vodafone ONE | | | | | | | | | | | | | |
|------------------------------------|---------------|-----------|-----------|---------------|--------------------|---------------------|-----------------|------------------------|-----------------|-------------------------|-----------------------|---|---|
| Priority | Flow Name | URI Group | Transport | Remote Subnet | Received Interface | Signaling Interface | Media Interface | End Point Policy Group | Routing Profile | Topology Hiding Profile | File Transfer Profile | | |
| 1 | Outbound Flow | * | * | * | Avaya SM | Vodafone ONE | Vodafone ONE | default-low | Avaya SM | Vodafone ONE | None |  |  |

8. Vodafone FMC Trunk Service Provider Configuration

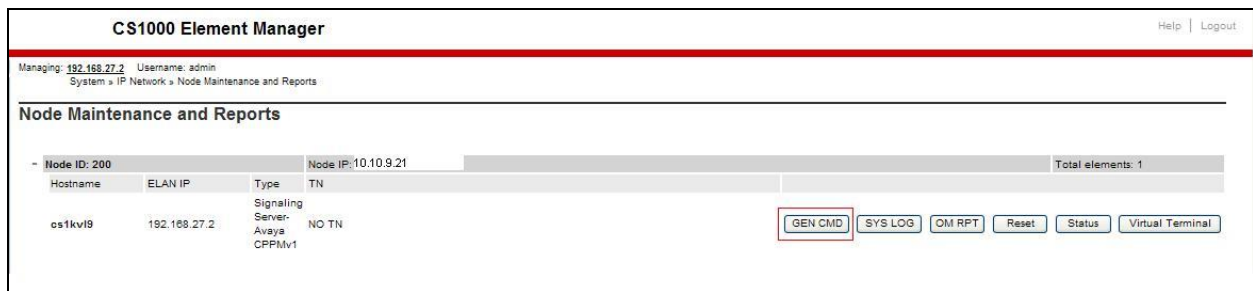
The configuration of the Vodafone equipment used to support the Vodafone FMC Trunk service is outside of the scope of these Application Notes and will not be covered. To obtain further information on Vodafone equipment and system configuration please contact an authorised Vodafone representative.

9. Verification

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

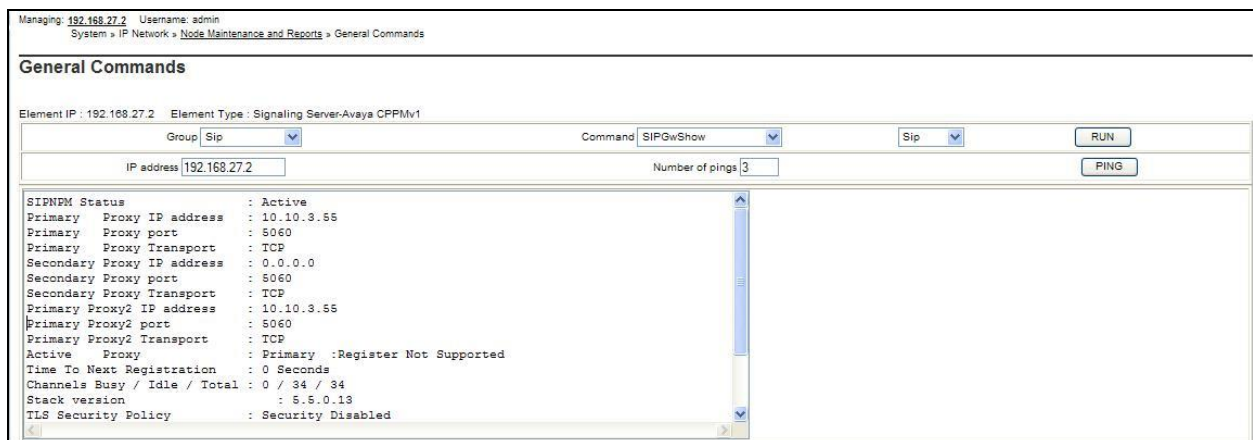
9.1.1. IP Network Maintenance and Reports Commands

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”.



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

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

General Commands

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

Group SipLine

Command sigSetShowAll

RUN

IP address 192.168.27.2

Number of pings 3

PING

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

The following screen shows a means to view IP UNISTim 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 | | | | | | |

9.2. 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_REC** **PDCH** **BDCH**

001 SIP_DCH OPER EST ACTV AUTO

STAT DCH

Command executed successfully.

9.3. Verify Avaya Aura® Session Manager Operational Status

9.3.1. Verify Avaya Aura® Session Manager is Operational

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

The screenshot shows the 'Session Manager Dashboard' with a sidebar on the left containing links like Dashboard, Session Manager, Administration, etc. The main content area has a title 'Session Manager Dashboard' and a subtitle 'This page provides the overall status and health summary of each administered Session Manager.' Below this is a section titled 'Session Manager Instances' with filters for 'Service State' and 'Shutdown System', and a timestamp 'As of 11:56 AM'. A table lists the instances, with one item shown: 'Session Manager' of type 'Core', with 0/0/2 alarms, tests passing, security module 'Up', service state 'Accept New Service', 0/3 entity monitoring, 1 active call count, 0 registrations, and version 6.1.0.0.610023.

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

Navigate to **Elements** → **Session Manager** → **System Status** → **Security Module Status** (not shown) to view more detailed status information on the status of Security Module for the specific Session Manager. Verify the **Status** column displays **Up** as shown below.

The screenshot shows the 'Security Module Status' page with buttons for 'Reset', 'Synchronize', 'Certificate Management', and 'Connection Status'. Below these is a table with columns: Details, Session Manager, Type, Status, Connections, IP Address, VLAN, Default Gateway, NIC Bonding, Entity Links (expected / actual), and Certificate Used. One item is shown: 'Session Manager' of type 'SM', status 'Up', 6 connections, IP 10.10.3.55/24, VLAN ---, Default Gateway 10.10.3.1, NIC Bonding Disabled, Entity Links 3/3, and Certificate Used SIP CA.

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

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Communication Server 1000E, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise to Vodafone FMC Trunk Service. Vodafone FMC Trunk 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. Additional 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, December 2013.
- [2] *Installing Service Packs for Avaya Aura® Session Manager*, Release 6.3, December 2013.
- [3] *Upgrading Avaya Aura® Session Manager*, Release 6.3, December 2013.
- [4] *Maintaining and Troubleshooting Avaya Aura® Session Manager Release 6.3*, December 2013.
- [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

Avaya Communication Server 1000E call server patches and plug ins

TID: 008809193

VERSION 4021

System type is - Communication Server 1000E/CP PMCP PM - Pentium M 1.4 GHz

IPMGs Registered: 1

IPMGs Unregistered: 0

IPMGs Configured/unregistered: 0

RELEASE 7

ISSUE 50 Q +

IDLE SET DISPLAY Vodafone One

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

IN-SERVICE PEPs

| CR # | PATCH REF # | NAME | DATE | FILENAME | SPECINS |
|------------|-------------|----------|------------|--------------|---------|
| wi00996889 | ISS1:10F1 | p31933_1 | 10/04/2013 | p31933_1.cpm | NO |
| wi01025511 | ISS1:10F1 | p32114_1 | 10/04/2013 | p32114_1.cpm | NO |

MDP>LAST SUCCESSFUL MDP REFRESH :2012-05-24 13:36:57(Local Time)

MDP>USING DEPLIST ZIP FILE DOWNLOADED :2012-05-21 11:49:19(est)

LOADWARE VERSION: PSWV 100+

INSTALLED LOADWARE PEPs : 11

| PAT# | CR # | PATCH REF # | NAME | DATE | FILENAME |
|------|------------|-------------|----------|------------|-------------|
| 00 | wi00839337 | ISS1:10F1 | DSP1AB06 | 24/01/2013 | DSP1AB06.LW |
| 01 | wi00839337 | ISS1:10F1 | DSP2AB06 | 24/01/2013 | DSP2AB06.LW |
| 02 | wi00839337 | ISS1:10F1 | DSP3AB06 | 24/01/2013 | DSP3AB06.LW |
| 03 | wi00839337 | ISS1:10F1 | DSP4AB06 | 24/01/2013 | DSP4AB06.LW |
| 04 | wi00839337 | ISS1:10F1 | DSP5AB06 | 24/01/2013 | DSP5AB06.LW |
| 05 | | | mgcfaa19 | 24/01/2013 | MGCFAA19.LD |
| 06 | wi00946109 | ISS1:10F1 | MGCABA15 | 24/01/2013 | MGCABA15.LW |
| 07 | wi00946113 | ISS1:10F1 | MGCBA15 | 24/01/2013 | MGCBA15.LW |
| 08 | Q01820502 | ISS1:10F1 | MGCMA01 | 24/01/2013 | MGCMA01.LW |
| 09 | WI00998702 | ISS1:10F1 | MGCCCD03 | 24/01/2013 | MGCCCD03.LW |
| 20 | Q01981776 | ISS1:10F1 | udtcab14 | 12/06/2012 | udtcab14.lw |

ENABLED PLUGINS : 1

| PLUGIN | STATUS | PRS/CR_NUM | MPLR_NUM | DESCRIPTION |
|--------|---------|------------|-----------|---|
| 501 | ENABLED | Q02138637 | MPLR30070 | Enables blind transfer to a SIP endpoint even if SIP UPDATE is not supported by the far end |

Avaya Communication Server 1000E call server deplists

VERSION 4021

RELEASE 7

ISSUE 50 Q +

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

IN-SERVICE PEPs

| PAT# | CR # | PATCH REF # | NAME | DATE | FILENAME | SPECINS |
|------|------------|-------------|----------|------------|--------------|---------|
| 000 | wi00856991 | ISS1:10F1 | p17588_1 | 10/04/2013 | p17588_1.cpm | NO |
| 001 | wi00950857 | ISS1:10F1 | p24307_1 | 10/04/2013 | p24307_1.cpm | NO |
| 002 | wi00881777 | ISS1:10F1 | p25747_1 | 10/04/2013 | p25747_1.cpm | NO |
| 003 | wi00905660 | ISS1:10F1 | p27968_1 | 10/04/2013 | p27968_1.cpm | NO |
| 004 | WI00839794 | ISS1:10F1 | p28647_1 | 10/04/2013 | p28647_1.cpm | NO |
| 005 | wi00688381 | ISS1:10F1 | p30104_1 | 10/04/2013 | p30104_1.cpm | NO |
| 006 | wi00961267 | ISS1:10F1 | p30288_1 | 10/04/2013 | p30288_1.cpm | NO |
| 007 | wi00896680 | ISS1:10F1 | p30357_1 | 10/04/2013 | p30357_1.cpm | NO |
| 008 | wi00825488 | ISS1:10F1 | p30371_1 | 10/04/2013 | p30371_1.cpm | NO |

| | | | | | | |
|-----|------------|-----------|----------|------------|--------------|-----|
| 009 | wi00825486 | ISS1:10F1 | p30382_1 | 10/04/2013 | p30382_1.cpm | NO |
| 010 | wi00897176 | ISS1:10F1 | p30418_1 | 10/04/2013 | p30418_1.cpm | NO |
| 011 | wi00903381 | ISS1:10F1 | p30421_1 | 10/04/2013 | p30421_1.cpm | NO |
| 012 | wi00854130 | ISS1:10F1 | p30443_1 | 10/04/2013 | p30443_1.cpm | NO |
| 013 | wi00824257 | ISS1:10F1 | p30447_1 | 10/04/2013 | p30447_1.cpm | NO |
| 014 | wi00836182 | ISS1:10F1 | p30450_1 | 10/04/2013 | p30450_1.cpm | NO |
| 015 | wi00826075 | ISS1:10F1 | p30452_1 | 10/04/2013 | p30452_1.cpm | NO |
| 016 | WI00900668 | ISS1:10F1 | p30456_1 | 10/04/2013 | p30456_1.cpm | NO |
| 017 | wi00854150 | ISS1:10F1 | p30468_1 | 10/04/2013 | p30468_1.cpm | NO |
| 018 | wi00827950 | ISS2:10F1 | p30471_2 | 10/04/2013 | p30471_2.cpm | NO |
| 019 | WI00836334 | ISS1:10F1 | p30481_1 | 10/04/2013 | p30481_1.cpm | NO |
| 020 | wi00877367 | ISS1:10F1 | p30534_1 | 10/04/2013 | p30534_1.cpm | NO |
| 021 | wi00834382 | ISS1:10F1 | p30548_1 | 10/04/2013 | p30548_1.cpm | NO |
| 022 | wi00832106 | ISS1:10F1 | p30550_1 | 10/04/2013 | p30550_1.cpm | NO |
| 023 | WI00836292 | ISS1:10F1 | p30554_1 | 10/04/2013 | p30554_1.cpm | NO |
| 024 | wi00835294 | ISS1:10F1 | p30565_1 | 10/04/2013 | p30565_1.cpm | NO |
| 025 | wi00856702 | ISS1:10F1 | p30573_1 | 10/04/2013 | p30573_1.cpm | NO |
| 026 | wi00838073 | ISS1:10F1 | p30588_1 | 10/04/2013 | p30588_1.cpm | NO |
| 027 | wi00839255 | ISS1:10F1 | p30591_1 | 10/04/2013 | p30591_1.cpm | NO |
| 028 | wi00854415 | ISS1:10F1 | p30593_1 | 10/04/2013 | p30593_1.cpm | NO |
| 029 | wi00841980 | ISS1:10F1 | p30618_1 | 10/04/2013 | p30618_1.cpm | NO |
| 030 | wi00839821 | ISS1:10F1 | p30619_1 | 10/04/2013 | p30619_1.cpm | NO |
| 031 | wi00842409 | ISS1:10F1 | p30621_1 | 10/04/2013 | p30621_1.cpm | NO |
| 032 | WI00853473 | ISS1:10F1 | p30625_1 | 10/04/2013 | p30625_1.cpm | NO |
| 033 | WI00843571 | ISS1:10F1 | p30627_1 | 10/04/2013 | p30627_1.cpm | NO |
| 034 | wi00852389 | ISS1:10F1 | p30641_1 | 10/04/2013 | p30641_1.cpm | NO |
| 035 | wi00859123 | ISS1:10F1 | p30648_1 | 10/04/2013 | p30648_1.cpm | NO |
| 036 | wi00869695 | ISS1:10F1 | p30654_1 | 10/04/2013 | p30654_1.cpm | NO |
| 037 | wi00897096 | ISS1:10F1 | p30676_1 | 10/04/2013 | p30676_1.cpm | NO |
| 038 | wi00859449 | ISS1:10F1 | p30694_1 | 10/04/2013 | p30694_1.cpm | NO |
| 039 | wi00839134 | ISS1:10F1 | p30698_1 | 10/04/2013 | p30698_1.cpm | YES |
| 040 | wi00852365 | ISS1:10F1 | p30707_1 | 10/04/2013 | p30707_1.cpm | NO |
| 041 | wi00850521 | ISS1:10F1 | p30709_1 | 10/04/2013 | p30709_1.cpm | YES |
| 042 | wi00841273 | ISS1:10F1 | p30713_1 | 10/04/2013 | p30713_1.cpm | NO |
| 043 | wi00853178 | ISS1:10F1 | p30719_1 | 10/04/2013 | p30719_1.cpm | NO |
| 044 | wi00843623 | ISS1:10F1 | p30731_1 | 10/04/2013 | p30731_1.cpm | YES |
| 045 | wi00856410 | ISS1:10F1 | p30749_1 | 10/04/2013 | p30749_1.cpm | NO |
| 046 | WI00889786 | ISS1:10F1 | p30750_1 | 10/04/2013 | p30750_1.cpm | NO |
| 047 | wi00857566 | ISS1:10F1 | p30766_1 | 10/04/2013 | p30766_1.cpm | NO |
| 048 | wi00840590 | ISS1:10F1 | p30767_1 | 10/04/2013 | p30767_1.cpm | NO |
| 049 | wi00871969 | ISS1:10F1 | p30768_1 | 10/04/2013 | p30768_1.cpm | NO |
| 050 | wi00857362 | ISS1:10F1 | p30782_1 | 10/04/2013 | p30782_1.cpm | NO |
| 051 | wi00863876 | ISS1:10F1 | p30787_1 | 10/04/2013 | p30787_1.cpm | NO |
| 052 | wi00860279 | ISS1:10F1 | p30789_1 | 10/04/2013 | p30789_1.cpm | NO |
| 053 | wi00859305 | ISS1:10F1 | p30792_1 | 10/04/2013 | p30792_1.cpm | NO |
| 054 | wi00925141 | ISS1:10F1 | p30802_1 | 10/04/2013 | p30802_1.cpm | NO |
| 055 | wi00896394 | ISS1:10F1 | p30807_1 | 10/04/2013 | p30807_1.cpm | NO |
| 056 | wi00899584 | ISS1:10F1 | p30809_1 | 10/04/2013 | p30809_1.cpm | NO |
| 057 | wi00858335 | ISS1:10F1 | p30819_1 | 10/04/2013 | p30819_1.cpm | NO |
| 058 | wi00873382 | ISS1:10F1 | p30832_1 | 10/04/2013 | p30832_1.cpm | NO |
| 059 | wi00932942 | ISS1:10F1 | p30843_1 | 10/04/2013 | p30843_1.cpm | NO |
| 060 | wi00869243 | ISS1:10F1 | p30848_1 | 10/04/2013 | p30848_1.cpm | NO |
| 061 | wi00871739 | ISS1:10F1 | p30856_1 | 10/04/2013 | p30856_1.cpm | NO |
| 062 | wi00896420 | ISS1:10F1 | p30867_1 | 10/04/2013 | p30867_1.cpm | NO |
| 063 | wi00862574 | iss1:10f1 | p30870_1 | 10/04/2013 | p30870_1.cpm | NO |
| 064 | wi00877592 | ISS1:10F1 | p30880_1 | 10/04/2013 | p30880_1.cpm | NO |
| 065 | wi00938555 | ISS1:10F1 | p30881_1 | 10/04/2013 | p30881_1.cpm | YES |
| 066 | wi00865477 | ISS1:10F1 | p30892_1 | 10/04/2013 | p30892_1.cpm | YES |
| 067 | wi00865477 | ISS1:10F1 | p30893_1 | 10/04/2013 | p30893_1.cpm | YES |
| 068 | wi00865477 | ISS1:10F1 | p30894_1 | 10/04/2013 | p30894_1.cpm | YES |
| 069 | wi00865477 | ISS1:10F1 | p30896_1 | 10/04/2013 | p30896_1.cpm | YES |
| 070 | wi00865477 | ISS1:10F1 | p30898_1 | 10/04/2013 | p30898_1.cpm | YES |
| 071 | wi00875701 | ISS1:10F1 | p30942_1 | 10/04/2013 | p30942_1.cpm | NO |
| 072 | wi00875425 | ISS1:10F1 | p30943_1 | 10/04/2013 | p30943_1.cpm | NO |
| 073 | wi00879322 | ISS1:10F1 | p30954_1 | 10/04/2013 | p30954_1.cpm | NO |
| 074 | wi00883604 | ISS1:10F1 | p30973_1 | 10/04/2013 | p30973_1.cpm | NO |
| 075 | wi00882884 | ISS1:10F1 | p30975_1 | 10/04/2013 | p30975_1.cpm | NO |
| 076 | wi00880836 | ISS1:10F1 | p30976_1 | 10/04/2013 | p30976_1.cpm | NO |
| 077 | wi00880386 | ISS1:10F1 | p30977_1 | 10/04/2013 | p30977_1.cpm | NO |
| 078 | wi00925208 | ISS1:10F1 | p30986_1 | 10/04/2013 | p30986_1.cpm | NO |

| | | | | | | |
|-----|------------|-----------|----------|------------|--------------|-----|
| 079 | WI00927300 | ISS1:10F1 | p30999_1 | 10/04/2013 | p30999_1.cpm | NO |
| 080 | wi00884699 | ISS1:10F1 | p31000_1 | 10/04/2013 | p31000_1.cpm | YES |
| 081 | wi00953811 | ISS1:10F1 | p31002_1 | 10/04/2013 | p31002_1.cpm | NO |
| 082 | wi00900096 | ISS1:10F1 | p31006_1 | 10/04/2013 | p31006_1.cpm | NO |
| 083 | wi00879526 | ISS1:10F1 | p31007_1 | 10/04/2013 | p31007_1.cpm | NO |
| 084 | wi00886321 | ISS1:10F1 | p31009_1 | 10/04/2013 | p31009_1.cpm | NO |
| 085 | wi00882293 | ISS1:10F1 | p31010_1 | 10/04/2013 | p31010_1.cpm | NO |
| 086 | wi00887744 | ISS2:10F1 | p31026_2 | 10/04/2013 | p31026_2.cpm | NO |
| 087 | wi00889088 | ISS1:10F1 | p31036_1 | 10/04/2013 | p31036_1.cpm | NO |
| 089 | wi00890036 | ISS1:10F1 | p31044_1 | 10/04/2013 | p31044_1.cpm | NO |
| 090 | wi00890475 | p30952 | p31048_1 | 10/04/2013 | p31048_1.cpm | NO |
| 091 | wi00891626 | ISS1:10F1 | p31051_1 | 10/04/2013 | p31051_1.cpm | YES |
| 092 | wi00880221 | ISS1:10F1 | p31054_1 | 10/04/2013 | p31054_1.cpm | NO |
| 093 | wi00877365 | ISS1:10F1 | p31060_1 | 10/04/2013 | p31060_1.cpm | NO |
| 094 | wi00924886 | ISS1:10F1 | p31062_1 | 10/04/2013 | p31062_1.cpm | YES |
| 095 | wi00932948 | ISS1:10F1 | p31077_1 | 10/04/2013 | p31077_1.cpm | NO |
| 096 | wi00894243 | ISS1:10F1 | p31087_1 | 10/04/2013 | p31087_1.cpm | NO |
| 097 | wi00893131 | ISS1:10F1 | p31089_1 | 10/04/2013 | p31089_1.cpm | NO |
| 098 | wi00894443 | ISS1:10F1 | p31093_1 | 10/04/2013 | p31093_1.cpm | NO |
| 099 | wi00895090 | ISS1:10F1 | p31105_1 | 10/04/2013 | p31105_1.cpm | NO |
| 100 | wi00895181 | ISS1:10F1 | p31106_1 | 10/04/2013 | p31106_1.cpm | NO |
| 101 | wi00932958 | ISS1:10F1 | p31115_1 | 10/04/2013 | p31115_1.cpm | NO |
| 102 | wi00897082 | ISS1:10F1 | p31124_1 | 10/04/2013 | p31124_1.cpm | NO |
| 103 | wi00898327 | ISS1:10F1 | p31136_1 | 10/04/2013 | p31136_1.cpm | NO |
| 104 | wi00967510 | ISS1:10F1 | p31147_1 | 10/04/2013 | p31147_1.cpm | NO |
| 105 | wi00900766 | ISS1:10F1 | p31159_1 | 10/04/2013 | p31159_1.cpm | NO |
| 106 | wi00868729 | ISS1:10F1 | p31163_1 | 10/04/2013 | p31163_1.cpm | NO |
| 107 | wi00903369 | ISS1:10F1 | p31165_1 | 10/04/2013 | p31165_1.cpm | NO |
| 108 | wi00903437 | ISS1:10F1 | p31167_1 | 10/04/2013 | p31167_1.cpm | NO |
| 109 | wi00905297 | ISS1:10F1 | p31195_1 | 10/04/2013 | p31195_1.cpm | NO |
| 110 | wi00905600 | ISS1:10F1 | p31201_1 | 10/04/2013 | p31201_1.cpm | NO |
| 111 | wi00906022 | ISS1:10F1 | p31202_1 | 10/04/2013 | p31202_1.cpm | NO |
| 112 | wi00906098 | ISS1:10F1 | p31203_1 | 10/04/2013 | p31203_1.cpm | YES |
| 113 | wi00946282 | ISS1:10F1 | p31204_1 | 10/04/2013 | p31204_1.cpm | NO |
| 114 | wi00906163 | ISS1:10F1 | p31205_1 | 10/04/2013 | p31205_1.cpm | NO |
| 115 | wi00906350 | ISS1:10F1 | p31219_1 | 10/04/2013 | p31219_1.cpm | NO |
| 116 | wi00907403 | ISS1:10F1 | p31225_1 | 10/04/2013 | p31225_1.cpm | NO |
| 117 | wi00907697 | ISS1:10F1 | p31227_1 | 10/04/2013 | p31227_1.cpm | NO |
| 118 | wi00907707 | ISS1:10F1 | p31228_1 | 10/04/2013 | p31228_1.cpm | NO |
| 119 | wi00908598 | ISS1:10F1 | p31235_1 | 10/04/2013 | p31235_1.cpm | NO |
| 120 | wi00908933 | ISS1:10F1 | p31239_1 | 10/04/2013 | p31239_1.cpm | NO |
| 121 | wi00949410 | ISS1:10F1 | p31248_1 | 10/04/2013 | p31248_1.cpm | NO |
| 122 | wi00921295 | ISS1:10F1 | p31265_1 | 10/04/2013 | p31265_1.cpm | NO |
| 123 | wi00923899 | ISS1:10F1 | p31270_1 | 10/04/2013 | p31270_1.cpm | NO |
| 124 | wi00898200 | ISS1:10F1 | p31274_1 | 10/04/2013 | p31274_1.cpm | NO |
| 125 | wi00937672 | ISS1:10F1 | p31276_1 | 10/04/2013 | p31276_1.cpm | NO |
| 126 | wi00929140 | ISS1:10F1 | p31284_1 | 10/04/2013 | p31284_1.cpm | NO |
| 127 | wi00927321 | ISS1:10F1 | p31286_1 | 10/04/2013 | p31286_1.cpm | YES |
| 128 | wi00967509 | ISS1:10F1 | p31294_1 | 10/04/2013 | p31294_1.cpm | NO |
| 129 | WI00928455 | ISS1:10F1 | p31297_1 | 10/04/2013 | p31297_1.cpm | NO |
| 130 | wi00932204 | ISS2:10F1 | p31305_2 | 10/04/2013 | p31305_2.cpm | NO |
| 131 | wi00937114 | ISS1:10F1 | p31310_1 | 10/04/2013 | p31310_1.cpm | NO |
| 132 | wi00925033 | ISS1:10F1 | p31320_1 | 10/04/2013 | p31320_1.cpm | NO |
| 133 | wi00930864 | ISS1:10F1 | p31325_1 | 10/04/2013 | p31325_1.cpm | NO |
| 134 | wi00855423 | ISS1:10F1 | p31328_1 | 10/04/2013 | p31328_1.cpm | YES |
| 135 | wi00909476 | ISS1:10F1 | p31340_1 | 10/04/2013 | p31340_1.cpm | NO |
| 136 | wi00931028 | ISS1:10F1 | p31354_1 | 10/04/2013 | p31354_1.cpm | YES |
| 137 | wi00946558 | ISS1:10F1 | p31358_1 | 10/04/2013 | p31358_1.cpm | NO |
| 138 | wi00936935 | ISS1:10F1 | p31362_1 | 10/04/2013 | p31362_1.cpm | NO |
| 139 | wi00948274 | ISS1:10F1 | p31365_1 | 10/04/2013 | p31365_1.cpm | NO |
| 140 | wi00892954 | ISS1:10F1 | p31378_1 | 10/04/2013 | p31378_1.cpm | NO |
| 141 | wi00936714 | ISS1:10F1 | p31379_1 | 10/04/2013 | p31379_1.cpm | NO |
| 142 | wi00967512 | ISS1:10F1 | p31384_1 | 10/04/2013 | p31384_1.cpm | NO |
| 143 | wi00980476 | ISS1:10F1 | p31387_1 | 10/04/2013 | p31387_1.cpm | NO |
| 144 | wi00932929 | ISS1:10F1 | p31392_1 | 10/04/2013 | p31392_1.cpm | YES |
| 145 | wi00943172 | ISS1:10F1 | p31402_1 | 10/04/2013 | p31402_1.cpm | NO |
| 146 | wi00948931 | ISS1:10F1 | p31407_1 | 10/04/2013 | p31407_1.cpm | NO |
| 147 | wi00942734 | ISS1:10F1 | p31409_1 | 10/04/2013 | p31409_1.cpm | NO |
| 148 | wi00949273 | ISS1:10F1 | p31411_1 | 10/04/2013 | p31411_1.cpm | NO |
| 149 | wi00968353 | ISS1:10F1 | p31412_1 | 10/04/2013 | p31412_1.cpm | NO |

| | | | | | | |
|-----|------------|-----------|----------|------------|--------------|-----|
| 150 | wi00946477 | ISS1:10F1 | p31426_1 | 10/04/2013 | p31426_1.cpm | NO |
| 151 | wi00946876 | ISS1:10F1 | p31430_1 | 10/04/2013 | p31430_1.cpm | NO |
| 152 | wi00949627 | ISS1:10F1 | p31462_1 | 10/04/2013 | p31462_1.cpm | NO |
| 153 | wi00965285 | ISS1:10F1 | p31476_1 | 10/04/2013 | p31476_1.cpm | NO |
| 154 | wi00951427 | ISS1:10F1 | p31478_1 | 10/04/2013 | p31478_1.cpm | NO |
| 155 | wi00951837 | ISS1:10F1 | p31485_1 | 10/04/2013 | p31485_1.cpm | NO |
| 156 | wi00956885 | ISS1:10F1 | p31489_1 | 10/04/2013 | p31489_1.cpm | NO |
| 157 | wi00953900 | ISS1:10F1 | p31494_1 | 10/04/2013 | p31494_1.cpm | NO |
| 158 | wi00955541 | ISS1:10F1 | p31501_1 | 10/04/2013 | p31501_1.cpm | NO |
| 159 | wi00943748 | ISS1:10F1 | p31516_1 | 10/04/2013 | p31516_1.cpm | NO |
| 160 | wi00959463 | ISS1:10F1 | p31528_1 | 10/04/2013 | p31528_1.cpm | NO |
| 161 | wi00957252 | ISS1:10F1 | p31530_1 | 10/04/2013 | p31530_1.cpm | NO |
| 162 | wi00959284 | ISS1:10F1 | p31531_1 | 10/04/2013 | p31531_1.cpm | NO |
| 163 | wi00958776 | ISS1:10F1 | p31542_1 | 10/04/2013 | p31542_1.cpm | YES |
| 164 | wi00957316 | ISS1:10F1 | p31547_1 | 10/04/2013 | p31547_1.cpm | NO |
| 165 | wi00959457 | ISS1:10F1 | p31551_1 | 10/04/2013 | p31551_1.cpm | NO |
| 166 | wi00960133 | ISS2:10F1 | p31557_2 | 10/04/2013 | p31557_2.cpm | NO |
| 167 | wi00959820 | ISS1:10F1 | p31562_1 | 10/04/2013 | p31562_1.cpm | NO |
| 168 | wi00960809 | ISS1:10F1 | p31564_1 | 10/04/2013 | p31564_1.cpm | NO |
| 169 | wi00930649 | ISS1:10F1 | p31570_1 | 10/04/2013 | p31570_1.cpm | NO |
| 170 | wi00962211 | ISS1:10F1 | p31580_1 | 10/04/2013 | p31580_1.cpm | NO |
| 171 | wi00962955 | ISS1:10F1 | p31585_1 | 10/04/2013 | p31585_1.cpm | NO |
| 172 | wi00967205 | ISS1:10F1 | p31592_1 | 10/04/2013 | p31592_1.cpm | NO |
| 173 | wi00991523 | ISS1:10F1 | p31603_1 | 10/04/2013 | p31603_1.cpm | NO |
| 174 | wi00965724 | ISS1:10F1 | p31606_1 | 10/04/2013 | p31606_1.cpm | NO |
| 175 | wi00965838 | ISS1:10F1 | p31623_1 | 10/04/2013 | p31623_1.cpm | NO |
| 176 | wi00968157 | ISS1:10F1 | p31637_1 | 10/04/2013 | p31637_1.cpm | NO |
| 177 | wi00956788 | ISS1:10F1 | p31638_1 | 10/04/2013 | p31638_1.cpm | NO |
| 178 | wi00945997 | ISS1:10F1 | p31641_1 | 10/04/2013 | p31641_1.cpm | NO |
| 179 | wi00969039 | ISS1:10F1 | p31643_1 | 10/04/2013 | p31643_1.cpm | NO |
| 180 | wi00968531 | ISS1:10F1 | p31645_1 | 10/04/2013 | p31645_1.cpm | NO |
| 181 | wi00968448 | ISS1:10F1 | p31648_1 | 10/04/2013 | p31648_1.cpm | YES |
| 182 | wi00969208 | ISS1:10F1 | p31656_1 | 10/04/2013 | p31656_1.cpm | NO |
| 183 | wi00969581 | ISS1:10F1 | p31661_1 | 10/04/2013 | p31661_1.cpm | YES |
| 184 | wi00969890 | ISS1:10F1 | p31664_1 | 10/04/2013 | p31664_1.cpm | YES |
| 185 | wi00962982 | ISS1:10F1 | p31685_1 | 10/04/2013 | p31685_1.cpm | NO |
| 186 | wi00974272 | ISS1:10F1 | p31690_1 | 10/04/2013 | p31690_1.cpm | YES |
| 187 | wi00974635 | ISS1:10F1 | p31695_1 | 10/04/2013 | p31695_1.cpm | YES |
| 188 | wi00975150 | ISS1:10F1 | p31703_1 | 10/04/2013 | p31703_1.cpm | NO |
| 189 | wi00975659 | ISS1:10F1 | p31707_1 | 10/04/2013 | p31707_1.cpm | NO |
| 190 | wi00973241 | ISS1:10F1 | p31715_1 | 10/04/2013 | p31715_1.cpm | NO |
| 191 | wi00976209 | ISS1:10F1 | p31717_1 | 10/04/2013 | p31717_1.cpm | YES |
| 192 | wi00950575 | ISS1:10F1 | p31724_1 | 10/04/2013 | p31724_1.cpm | NO |
| 193 | wi00975133 | ISS1:10F1 | p31731_1 | 10/04/2013 | p31731_1.cpm | NO |
| 194 | wi00955753 | ISS1:10F1 | p31733_1 | 10/04/2013 | p31733_1.cpm | NO |
| 195 | wi00977393 | ISS1:10F1 | p31744_1 | 10/04/2013 | p31744_1.cpm | YES |
| 196 | wi00979591 | ISS1:10F1 | p31746_1 | 10/04/2013 | p31746_1.cpm | NO |
| 197 | wi00979414 | ISS1:10F1 | p31748_1 | 10/04/2013 | p31748_1.cpm | YES |
| 198 | wi00971209 | ISS1:10F1 | p31750_1 | 10/04/2013 | p31750_1.cpm | NO |
| 199 | wi00973270 | ISS1:10F1 | p31751_1 | 10/04/2013 | p31751_1.cpm | NO |
| 200 | wi00980531 | ISS1:10F1 | p31755_1 | 10/04/2013 | p31755_1.cpm | NO |
| 201 | wi00983505 | ISS1:10F1 | p31758_1 | 10/04/2013 | p31758_1.cpm | NO |
| 202 | wi00978064 | ISS1:10F1 | p31760_1 | 10/04/2013 | p31760_1.cpm | NO |
| 203 | wi00981711 | ISS1:10F1 | p31766_1 | 10/04/2013 | p31766_1.cpm | NO |
| 204 | wi00978883 | ISS1:10F1 | p31770_1 | 10/04/2013 | p31770_1.cpm | NO |
| 205 | wi00982566 | ISS1:10F1 | p31774_1 | 10/04/2013 | p31774_1.cpm | NO |
| 206 | wi00983007 | ISS1:10F1 | p31778_1 | 10/04/2013 | p31778_1.cpm | YES |
| 207 | wi00996630 | ISS1:10F1 | p31789_1 | 10/04/2013 | p31789_1.cpm | NO |
| 208 | wi00984652 | ISS1:10F1 | p31792_1 | 10/04/2013 | p31792_1.cpm | NO |
| 209 | wi00971029 | ISS1:10F1 | p31794_1 | 10/04/2013 | p31794_1.cpm | NO |
| 210 | wi00984888 | ISS1:10F1 | p31795_1 | 10/04/2013 | p31795_1.cpm | NO |
| 211 | wi00982243 | ISS1:10F1 | p31797_1 | 10/04/2013 | p31797_1.cpm | YES |
| 212 | wi00957235 | ISS1:10F1 | p31798_1 | 10/04/2013 | p31798_1.cpm | NO |
| 213 | wi00986337 | ISS1:10F1 | p31803_1 | 10/04/2013 | p31803_1.cpm | NO |
| 214 | wi00987089 | ISS1:10F1 | p31809_1 | 10/04/2013 | p31809_1.cpm | NO |
| 215 | wi00987424 | ISS1:10F1 | p31815_1 | 10/04/2013 | p31815_1.cpm | NO |
| 216 | wi00982851 | ISS1:10F1 | p31822_1 | 10/04/2013 | p31822_1.cpm | NO |
| 217 | wi00974856 | ISS1:10F1 | p31823_1 | 10/04/2013 | p31823_1.cpm | NO |
| 218 | wi00988285 | ISS1:10F1 | p31824_1 | 10/04/2013 | p31824_1.cpm | NO |
| 219 | wi00990993 | ISS1:10F1 | p31825_1 | 10/04/2013 | p31825_1.cpm | NO |

| | | | | | | |
|-----|------------|-----------|----------|------------|--------------|-----|
| 220 | WI00977978 | ISS1:10F1 | p31831_1 | 10/04/2013 | p31831_1.cpm | NO |
| 221 | wi00977436 | ISS1:10F1 | p31834_1 | 10/04/2013 | p31834_1.cpm | NO |
| 222 | wi00989828 | ISS1:10F1 | p31836_1 | 10/04/2013 | p31836_1.cpm | NO |
| 223 | wi00991892 | ISS1:10F1 | p31853_1 | 10/04/2013 | p31853_1.cpm | NO |
| 224 | wi00985153 | ISS1:10F1 | p31859_1 | 10/04/2013 | p31859_1.cpm | NO |
| 225 | wi00993377 | ISS1:10F1 | p31860_1 | 10/04/2013 | p31860_1.cpm | NO |
| 226 | wi00993648 | ISS1:10F1 | p31867_1 | 10/04/2013 | p31867_1.cpm | NO |
| 227 | wi00981928 | ISS1:10F1 | p31869_1 | 10/04/2013 | p31869_1.cpm | NO |
| 228 | wi00994044 | ISS1:10F1 | p31871_1 | 10/04/2013 | p31871_1.cpm | NO |
| 229 | wi00944019 | ISS1:10F1 | p31874_1 | 10/04/2013 | p31874_1.cpm | NO |
| 230 | wi00992921 | ISS1:10F1 | p31878_1 | 10/04/2013 | p31878_1.cpm | NO |
| 231 | wi00992974 | ISS1:10F1 | p31889_1 | 10/04/2013 | p31889_1.cpm | NO |
| 232 | wi00998121 | ISS1:10F1 | p31897_1 | 10/04/2013 | p31897_1.cpm | NO |
| 233 | wi00997559 | ISS1:10F1 | p31898_1 | 10/04/2013 | p31898_1.cpm | NO |
| 234 | wi00985760 | ISS1:10F1 | p31913_1 | 10/04/2013 | p31913_1.cpm | NO |
| 235 | wi01003999 | ISS1:10F1 | p31946_1 | 10/04/2013 | p31946_1.cpm | YES |
| 237 | wi00996889 | ISS1:10F1 | p31933_1 | 10/04/2013 | p31933_1.cpm | NO |
| 238 | wi01025511 | ISS1:10F1 | p32114_1 | 10/04/2013 | p32114_1.cpm | NO |

MDP>LAST SUCCESSFUL MDP REFRESH :2012-05-24 13:36:57(Local Time)

MDP>USING DEPLIST ZIP FILE DOWNLOADED :2012-05-21 11:49:19(est)

Avaya Communication Server 1000E signaling server service updates

In System service updates: 33

| PATCH# | IN_SERVICE | DATE | SPECINS | REMOVABLE | NAME |
|--------|------------|----------|---------|-----------|---|
| 3 | Yes | 20/01/12 | NO | YES | cs1000-dbcom-7.50.17-02.i386.000 |
| 4 | Yes | 18/12/12 | NO | yes | tzdata-2011h-2.el5.i386.000 |
| 5 | Yes | 20/01/12 | NO | YES | cs1000-shared-pbx-7.50.17.16-1.i386.000 |
| 6 | Yes | 20/01/12 | NO | YES | cs1000-kcv-7.50.17.16-1.i386.000 |
| 7 | Yes | 20/01/12 | NO | YES | cs1000-nrsmWebService-7.50.17.16-1.i386.000 |
| 9 | Yes | 02/10/12 | YES | YES | cs1000-baseWeb-7.50.17.16-2.i386.000 |
| 10 | Yes | 20/01/12 | NO | YES | cs1000-ipsec-7.50.17.16-1.i386.000 |
| 11 | Yes | 02/10/12 | NO | yes | avaya-cs1000-cnd-4.0.20-00.i386.000 |
| 12 | Yes | 02/10/12 | NO | YES | cs1000-pd-7.50.17.16-1.i386.000 |
| 13 | Yes | 02/10/12 | NO | YES | cs1000-ncs-7.50.17.16-1.i386.000 |
| 14 | Yes | 20/01/12 | NO | YES | ipsec-tools-0.6.5-14.el5.3 avaya 1.i386.000 |
| 15 | Yes | 20/01/12 | NO | YES | spiritAgent-6.1-1.0.0.108.208.i386.000 |
| 16 | No | 18/12/12 | NO | YES | cs1000-tps-7.50.17.16-24.i386.000 |
| 17 | Yes | 02/10/12 | NO | YES | cs1000-EmCentralLogic-7.50.17.16-2.i386.000 |
| 20 | Yes | 02/10/12 | NO | YES | cs1000-cs1000WebService 6-0-7.50.17.16-1.i386.000 |
| 21 | Yes | 02/10/12 | NO | YES | cs1000-mscMusc-7.50.17.16-11.i386.000 |
| 22 | Yes | 02/10/12 | NO | YES | cs1000-mscAnnc-7.50.17.16-10.i386.000 |
| 23 | No | 18/12/12 | NO | YES | cs1000-sps-7.50.17.16-10.i386.000 |
| 24 | Yes | 27/03/12 | NO | YES | cs1000-mscTone-7.50.17.16-1.i386.000 |
| 25 | No | 18/12/12 | NO | YES | cs1000-ftrpkg-7.50.17.16-11.i386.000 |
| 26 | Yes | 18/12/12 | NO | YES | cs1000-dmWeb-7.50.17.16-6.i386.000 |
| 27 | Yes | 02/10/12 | NO | YES | cs1000-csoneksvrmgr-7.50.17.16-1.i386.000 |
| 28 | No | 18/12/12 | NO | YES | cs1000-dbcom-7.50.17.16-1.i386.000 |
| 29 | No | 18/12/12 | NO | YES | cs1000-vtrk-7.50.17.16-131.i386.001 |
| 30 | Yes | 27/03/12 | NO | YES | cs1000-sps-7.50.17.16-4.i386.000 |
| 31 | Yes | 18/12/12 | NO | YES | cs1000-linuxbase-7.50.17.16-13.i386.000 |
| 32 | Yes | 18/12/12 | NO | YES | cs1000-mscAttn-7.50.17.16-3.i386.000 |
| 35 | Yes | 02/10/12 | YES | YES | cs1000-nrsm-7.50.17.16-4.i386.000 |
| 36 | Yes | 02/10/12 | NO | YES | cs1000-csmWeb-7.50.17.16-6.i386.000 |
| 37 | Yes | 02/10/12 | NO | YES | cs1000-mscConf-7.50.17.16-1.i386.000 |
| 38 | Yes | 02/10/12 | NO | YES | cs1000-emWeb 6-0-7.50.17.16-34.i386.000 |
| 40 | Yes | 02/10/12 | NO | YES | cs1000-Jboss-Quantum-7.50.17.16-30.i386.000 |
| 42 | Yes | 02/10/12 | NO | YES | cs1000-emWebLocal 6-0-7.50.17.16-3.i386.000 |

Avaya Communication Server 1000E system software

Product Release: 7.50.17.00

Base Applications

| | | |
|-------|---------|-----------|
| base | 7.50.17 | [patched] |
| NTAFS | 7.50.17 | |
| sm | 7.50.17 | |

| | | |
|----------------------------------|------------|-----------|
| cs1000-Auth | 7.50.17 | |
| Jboss-Quantum | 7.50.17 | [patched] |
| cnd | n/a | [patched] |
| lhmonitor | 7.50.17 | |
| baseAppUtils | 7.50.17 | [patched] |
| dfoTools | 7.50.17 | |
| nnnm | 7.50.17 | |
| cppmUtil | 7.50.17 | |
| oam-logging | 7.50.17 | [patched] |
| dmWeb | n/a | [patched] |
| baseWeb | n/a | [patched] |
| ipsec | n/a | [patched] |
| Snmp-Daemon-TrapLib | 7.50.17 | [patched] |
| ISECSH | 7.50.17 | |
| patchWeb | n/a | [patched] |
| EmCentralLogic | n/a | [patched] |
| Application configuration: SS_EM | | |
| Packages: | | |
| SS | | |
| EM | | |
| Configuration version: | 7.50.17-00 | |
| dbcom | 7.50.17.16 | [patched] |
| cslogin | 7.50.17 | |
| sigServerShare | 7.50.17 | [patched] |
| csv | 7.50.17 | |
| tps | 7.50.17.16 | [patched] |
| vtrk | 7.50.17.16 | [patched] |
| pd | 7.50.17.16 | [patched] |
| sps | 7.50.17.16 | [patched] |
| ncs | 7.50.17.16 | [patched] |
| gk | 7.50.17 | |
| EmConfig | 7.50.17 | |
| emWeb_6-0 | 7.50.17 | [patched] |
| emWebLocal_6-0 | 7.50.17 | [patched] |
| csmWeb | 7.50.17 | [patched] |
| bcc | 7.50.17 | [patched] |
| ftrpkg | 7.50.17 | [patched] |
| cs1000WebService 6-0 | 7.50.17 | [patched] |
| managedElementWebService | 7.50.17 | |
| mscAnnc | 7.50.17.16 | [patched] |
| mscAttn | 7.50.17.16 | [patched] |
| mscConf | 7.50.17.16 | [patched] |
| mscMusc | 7.50.17.16 | [patched] |
| mscTone | 7.50.17.16 | [patched] |

©2014 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.