



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Vision 2020 3.1HA from Enghouse Interactive AB with Avaya Communication Server 1000 and Avaya Aura® Session Manager using a SIP Trunk connection – Issue 1.0

Abstract

These Application Notes describe how to configure an Avaya Communication Server 1000 and an Avaya Aura® Session Manager to interface with Vision 2020 3.1HA, which is operating as an attendant answering position. Vision 2020 3.1HA is a software application from Enghouse Interactive AB installed on a Windows server that interfaces with Avaya Communication Server 1000 using a SIP connection via Avaya Aura® Session Manager and provides users with the call functions of an attendant console without having to install a hardware attendant position.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect Compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the compliance tested configuration for Avaya Communication Server 1000E R7.6 and Avaya Aura® Session Manager R7.0 with Vision 2020 HA (hereafter referred as Vision) release 3.1 from Enghouse Interactive AB. Vision is a client/server based application running on Microsoft Windows 2012 Server operating systems. Vision provides users with an attendant answering position for Avaya Communication Server 1000E that does not require attendant telephony hardware e.g., Avaya 2250 attendant console. Vision connects to the Avaya Communication Server 1000 using a SIP connection via Avaya Aura® Session Manager.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise voice network using an Avaya Communication Server 1000E (Communication Server 1000). The Vision server uses a SIP connection to the Communication Server 1000 call server via Session Manager. See **Figure 1** for a network diagram. A basic Distance Steering Code configuration (DSC) was configured on the Communication Server 1000 to route all calls to the Vision attendant position. If a call is made from the Vision attendant console to the PSTN the call will route from the Vision console via a SIP trunk to Session Manager then to the PSTN. During compliance testing simulated PSTN PRI/T1 trunks were used. Vision can perform the usual range of attendant call functions, i.e., centralized answering position; extend PSTN calls to users, place PSTN calls on behalf of internal users, perform internal telephone directory lookups.

During tests, calls are placed to a number associated with the Vision attendant position. Session Manager routes all calls destined for the Vision server over the SIP connection. The Vision server then automatically places a call to the telephone the attendant is using for answering purposes. When the attendant answers the call, the Vision server bridges the two calls. When the attendant extends the call to another phone, Vision server performs a SIP Re-Invite to connect caller and called user directly. It is possible to have multiple Vision attendant positions on a Communication Server 1000 system.

A variety of Avaya telephones were installed and configured on the Communication Server 1000. The Vision attendant client provides a view of contacts, schedules, and communication tasks and was installed on the same server as the Vision Server, but can be installed on a separate platform if required.

Note: The Vision server places a call to the attendant's deskphone, for compliance testing an Avaya IP phone was used as the attendant's deskphone. When the attendant is called the Vision server calls the Avaya IP phone and bridges the call.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by

DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

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

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

For the testing associated with these Application Notes, the interface between Avaya systems and the Vision 2020 did not include use of any specific encryption features as requested by Enghouse Interactive AB.

2.1. Interoperability Compliance Testing

The compatibility tests included the following.

- Incoming internal and external calls
- Outgoing internal and external calls
- Blind and announced transfer with answer
- Directing calls to busy extensions
- Call queuing and retrieval

2.2. Test Results

Tests were performed to insure full interoperability between the Vision and the Communication Server 1000. The tests were all functional in nature and performance testing was not included. All the test cases passed successfully.

2.3. Support

For technical support for Enghouse Interactive AB products, please use the following web link.
<http://www.enghouseinteractive.com/solutions/>

Enghouse Interactive AB can also be contacted as follows.

Phone: +46 (0)8 457 30 00

Fax: +46 (0)8 31 87 00

E-mail: Visionsupport@enghouse.com

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of a Communication Server 1000, System Manager and Session Manager. The Vision 8020HA server connects the Communication Server 1000 using a SIP Trunk via Session Manager. An Avaya 1140 IP deskphone was used as the Vision 8030HA Attendant telephone during compliance testing. A PRI/T1 trunk on Media Gateway Controller (MGC) was configured to connect to the simulated PSTN.

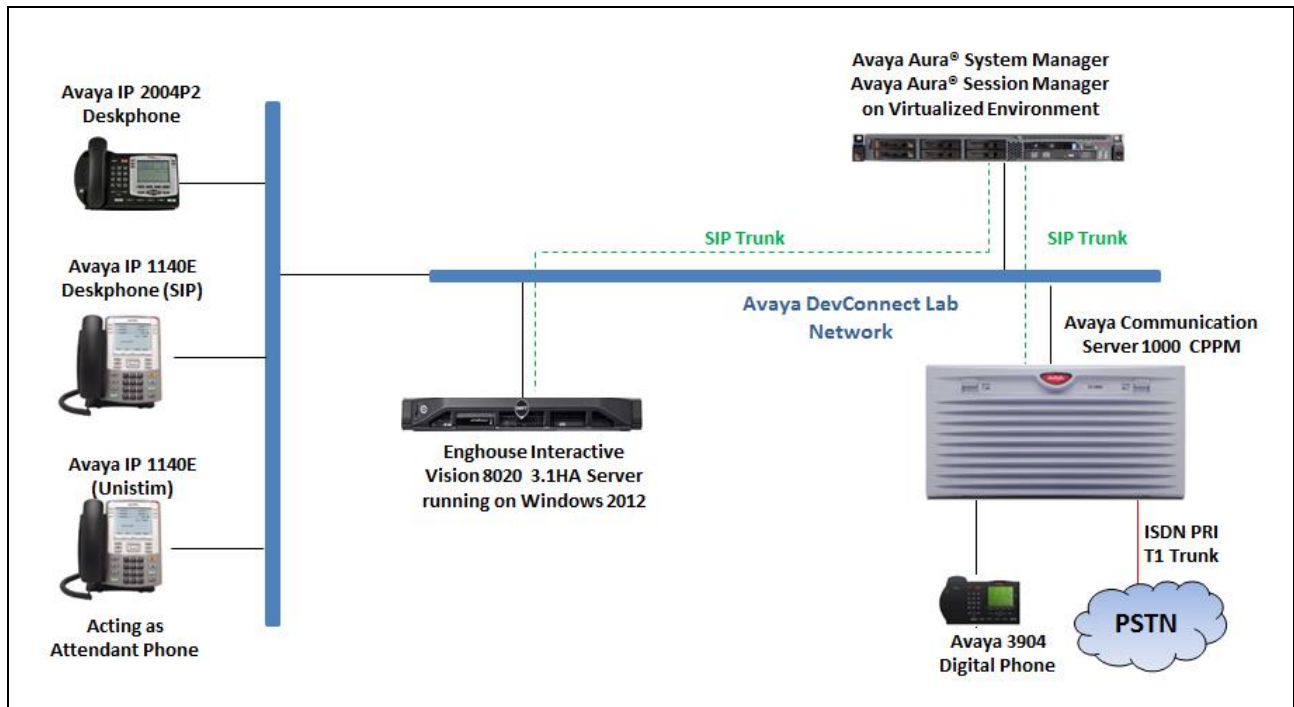


Figure 1: Configuration for Avaya Communication Server 1000, Avaya Aura® Session Manager and Enghouse Vision 2020 3.1HA

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Communication Server 1000	7.65 SP8
Avaya Aura® Session Manager running on virtualized environment	7.0.1.2.701114
Avaya Aura® System Manager running on virtualized environment	7.0.1.2 SP2
Avaya 11xx Series IP Telephone <ul style="list-style-type: none">• 1140 (UNISTim)• 1140 (SIP)	C95 4.03.09
Avaya 2004P2 IP Telephone	DCQ
Avaya 3904 Digital Telephone	-
Vision 2020 HA Server and Client running on Microsoft Windows 2012 R2 Server	3.1

5. Configure Avaya Communication Server 1000

The document assumes that route, trunk and dialing plan of the Avaya CS 1000 have been configured. This section only describes the details on how to configure the Avaya CS 1000 Signaling gateway to connect to the Session Manager via SIP trunk using the Element Manager.

Prerequisites: An Avaya CS1000 server which has been:

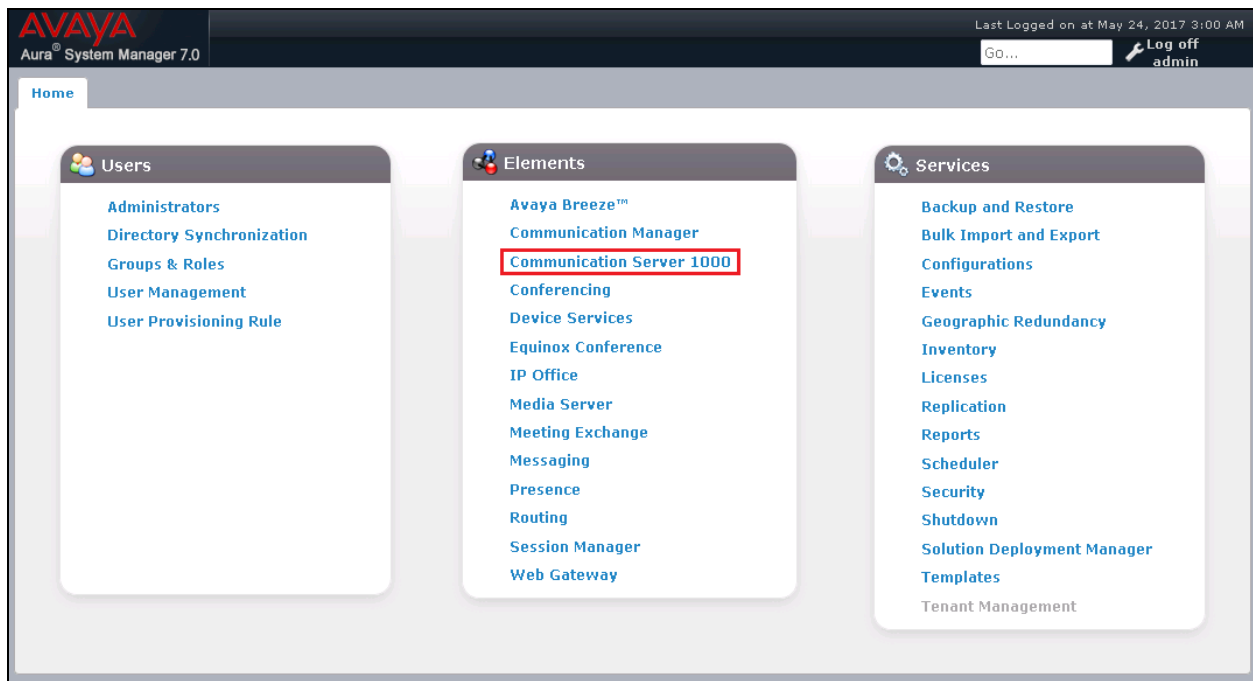
- Installed with CS 1000 Release 7.6 Linux Base.
- Joined CS 1000 Release 7.6 Security Domain.
- Deployed with SIP Trunk Application.

For more information on CS 1000 installation, maintenance, and upgrades, see **Section 10**. The following software packages are enabled in the key code. If any of these features have not been enabled, please contact your Avaya account team or Avaya technical support at <http://www.avaya.com>.

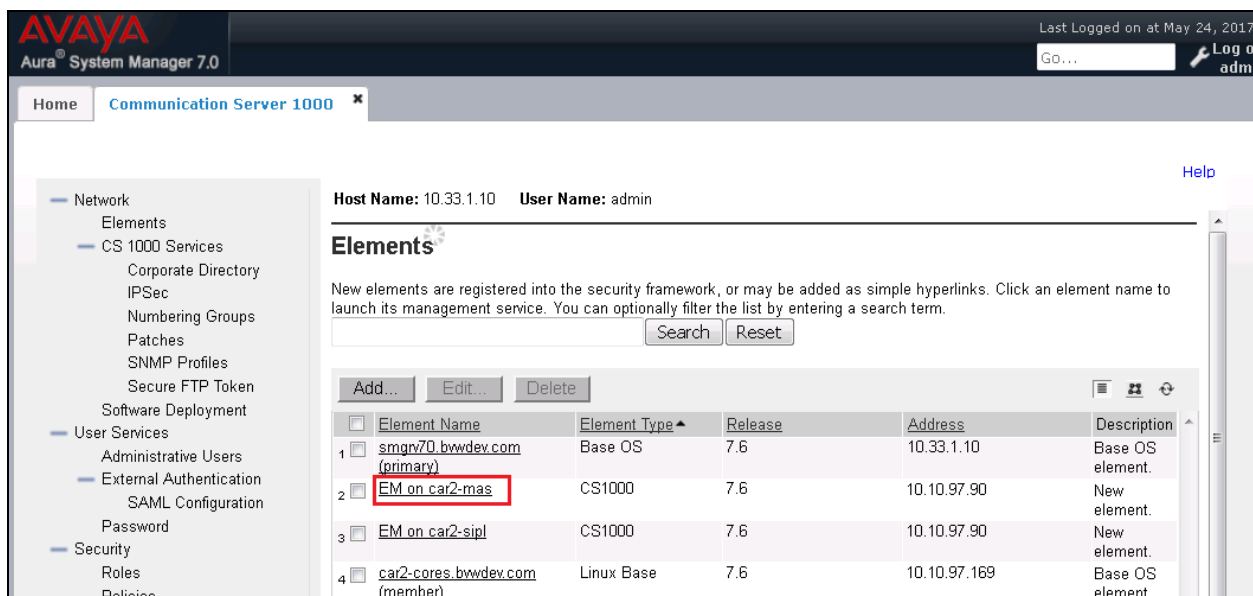
Package Mnemonic	Package Number	Package Description	Package Type (New or Existing or Dependency)	Applicable Market
SIP	406	SIP Service package	New package	Global
FFC	139	Flexible Feature Codes	Existing package	Global
SIPL_ Nortel	415	Avaya SIP Line	Existing package	-
SIPL_3ThirdParty	416	Third Party SIP Line	Existing package	-

5.1. Log in to Avaya Communication Server 1000 System

Since release 7.6 Avaya CS 1000 Elements is integrated to System Manager, to access the Element Manager of CS 1000 first log in the System Manager. The screen below shows the System Manager home page with **Communication Server 1000** entry in the Elements table. Click on the **Communication Server 1000** to access to CS 1000 Elements, the Elements webpage will be opened in the new window.



The **Elements** page is shown in the following screenshot. Click Element Name of the CS 1000 that needs to be accessed as highlighted in the red box.



5.2. Administer an IP Telephony Node

These application notes assume that the basic CS 1000 configuration has already been administered and that IP Telephony Node has already been created. This section describes the steps for configuring a Node (Node ID 2001) in CS 1000 IP network to work with Voice4net. Select **System** → **IP Network** → **Nodes: Servers, Media Cards** and then click on the **Node ID 2001** as shown below.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with 'Nodes: Servers, Media Cards' highlighted. The main content area displays a table of IP Telephony Nodes. The table has columns for Node ID, Components, Enabled Applications, ELAN IP, Node/TLAN IPv4, Node/TLAN IPv6, and Status. Node 2001 is highlighted, showing it is a LTPS Gateway (SIPGw) with ELAN IP 10.10.97.90 and Node/TLAN IPv4 10.10.97.170.

Node ID	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
2000	1	LTPS, Gateway (SIPGw)	-	10.10.97.168	-	Synchronized
2001	1	LTPS, Gateway (SIPGw)	-	10.10.97.170	-	Synchronized
2003	1	SIP Line, LTPS, Gateway (SIPGw)	-	10.10.97.158	-	Synchronized
2004	1	SIP Line, LTPS, PD, Gateway (SIPGw)	-	10.10.97.190	-	Synchronized
2005	1	SIP Line	-	10.10.97.188	-	Synchronized

The **Node Details** page will appear. Scroll down under the **Applications**, click on the **Gateway (SIPGw)** link, the **Virtual Trunk Gateway Configuration Details** page will appear in the next two screenshots. The node IP address 10.10.97.170 is used to establish SIP trunk with Session Manager.

The screenshot shows the AVAYA CS1000 Element Manager interface with the 'Node Details' page for Node ID 2001. The page is titled 'Node Details (ID: 2001 - LTPS, Gateway (SIPGw))'. It contains fields for Node ID, Call server IP address, Embedded LAN (ELAN) Gateway IP address and Subnet mask, and Telephone LAN (TLAN) Node IPv4 address and Subnet mask. The 'Applications' section lists various services, with 'Gateway (SIPGw)' highlighted.

Node ID: 2001 * (0-9999)

Call server IP address: 10.10.97.90 *

Embedded LAN (ELAN)

Gateway IP address: 10.10.97.65 *

Subnet mask: 255.255.255.192 *

Telephone LAN (TLAN)

Node IPv4 address: 10.10.97.170 *

Subnet mask: 255.255.255.192 *

Node IPv6 address: *

IP Telephony Node Properties

- Voice Gateway (VGW) and Codecs
- Quality of Service (QoS)
- LAN
- SNTP
- Numbering Zones
- MCDN Alternative Routing Treatment (MALT) Causes

Applications (click to edit configuration)

- SIP Line
- Terminal Proxy Server (TPS)
- Gateway (SIPGw)
- Personal Directories (PD)
- Presence Publisher
- IP Media Services

In the **Node ID: 2001- Virtual Trunk Gateway Configuration Details**, enter the information highlighted in the red-box for the **General** and **SIP Gateway Settings**. All other fields are kept at default. Click **Save**. Note: SIP domain name **bwvdev.com** should be matched with SIP domain created in **Section 6.2**.

AVAYA CS1000 Element Manager

Managing: 135.10.97.90 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 2001 - 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: bwvdev.com *

Local SIP port: 5060 * (1 - 65535)

Gateway endpoint name: car2-cores *

Gateway password: *

Application node ID: 2001 * (0-9999)

Enable failsafe NRS: ☐

Note: FailSafe NRS will be enabled only on those servers in

Virtual Trunk Network Health Monitor

☐ Monitor IP addresses (listed below)

Information will be captured for the IP a below.

Monitor IP:

Monitor addresses:

Copyright © 2002-2013 Avaya Inc. All rights reserved.

Enter the IP address **10.33.1.12** of signaling Session Manager in the **Primary TLAN IP address** field, port **5061** in the Port field and select **TLS** in the Transport protocol dropdown menu.

AVAYA CS1000 Element Manager

Help | Logout

General | SIP Gateway Settings | SIP Gateway Services

Transport protocol: TLS ▼

Shared Bandwidth Management:

☐ Enable Shared Bandwidth Management

Proxy Or Redirect Server:

Proxy Server Route 1:

Primary TLAN IP address: 10.33.1.12

The IP address can have either IPv4 or IPv6 format based on the val address type"

Port: 5061 (1 - 65535)

Transport protocol: TLS ▼

Options: ☐ Support registration
☐ Primary CDS proxy

Secondary TLAN IP address: 0.0.0.0

The IP address can have either IPv4 or IPv6 format based on the val address type"

On the same page, scroll-down the parameters box to the **SIP URI Map** section. Under the **Public E.164 domain names** and **Private domain names** subsections, leave all fields as blank, which remove the phone context in Invite message sent from CS 1000.

The screenshot shows the AVAYA CS1000 Element Manager interface. The breadcrumb trail is: System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration. The page title is "Node ID: 2001 - Virtual Trunk Gateway Configuration Details". The left sidebar shows a tree view with "Nodes: Servers, Media Car" selected. The main content area has tabs for "General", "SIP Gateway Settings", and "SIP Gateway Services". The "SIP URI Map" section is highlighted with a red box. It contains two subsections: "Public E.164 domain names" and "Private domain names". Each subsection has four input fields: "National", "Subscriber", "Special number", and "Unknown". The "SIP Gateway Services" tab is also visible at the bottom.

Afterwards, click **Save**, the system will bring back the **Node ID** page (not shown). Then click **Save** button on the **Node ID** page and that will take the user to the **Node Saved** page (not shown). Click on the **Transfer Now** button, when finished it will bring the user to the **Synchronize Configuration Files** page. Then click **Start Sync** button (not shown) to complete the configuration saved process.

The screenshot shows the "Synchronize Configuration Files (Node ID <2001>)" page. The breadcrumb trail is: System » IP Network » IP Telephony Nodes » Synchronize Configuration Files. A note in a yellow box states: "Note: Select components to synchronize their configuration files with call server data. This process transfers server INI files to selected components, and requires a restart* of applications on affected server(s) when complete." Below the note are three buttons: "Start Sync", "Cancel", and "Restart Applications". There is also a "Print | Refresh" link. A table lists the components to be synchronized:

<input checked="" type="checkbox"/>	Hostname	Type	Applications	Synchronization Status
<input checked="" type="checkbox"/>	car2-cores	Signaling_Server	SIP Line, LTPS, Gateway (SIP/H323), PD, Presence Publisher, IP Media Services	Sync required

* Application restart is only required for initial system configuration or if changes have been made to general LAN configurations, SNMP settings, SIP and H323 Gateway settings, network connectivity related parameters like ports and IP address, enabling or disabling services, or adding or removing application servers.

5.3. Administer D-Channel for SIP Trunk

From the homepage of Element Manager, expand the menu **Routes and Trunks** → **D-Channels** and select the **D-Channels** tab. The **D-Channel 101** as shown below was used for the compliance test.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation menu with the following items: Host and Route Tables, Network Address Translation, QoS Thresholds, Personal Directories, Unicode Name Directory, Interfaces, Engineered Values, Emergency Services, Geographic Redundancy, Software, Customers, Routes and Trunks (expanded), D-Channels (highlighted), Digital Trunk Interface, Dialing and Numbering Plans, Electronic Switched Network, Flexible Code Restriction, Incoming Digit Translation, Phones, Templates, Reports, Views, Lists, and Properties. The main content area is titled 'D-Channels' and shows a list of D-Channels. The 'Channel: 101' entry is highlighted with a red box. The 'Edit' button for Channel 101 is also highlighted. The 'Configuration' section shows a table with the following data:

Channel	Type	Card Type	Description	Action
Channel: 10	DCH	TMDI	TMDI	Edit
Channel: 100	DCH	DCIP	CenturyLink	Edit
Channel: 101	DCH	DCIP	SIPTrk	Edit

Click **Edit** button on the **D-channel 101**. The screen below shows the **Basic Configuration** section of this D-channel. Select **D-Channel is over IP (DCIP)** in the **D-Channel Card Type**, enter a description in the **Designator** box and keep all other values at their defaults.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation menu with the following items: Zones, Host and Route Tables, Network Address Translation, QoS Thresholds, Personal Directories, Unicode Name Directory, Interfaces, Engineered Values, Emergency Services, Geographic Redundancy, Software, Customers, Routes and Trunks (expanded), D-Channels (highlighted), Digital Trunk Interface, Dialing and Numbering Plans, Electronic Switched Network, Flexible Code Restriction, Incoming Digit Translation, Phones, Templates, Reports, Views, Lists, Properties, Migration, Tools, Backup and Restore, Date and Time, Logs and reports, Security, Passwords, and Policies. The main content area is titled 'D-Channels 101 Property Configuration' and shows the 'Basic Configuration' section. The 'D channel Card Type' is set to 'DCIP' and the 'Designator' is 'SIPTrk'. The 'Release ID of the switch at the far end' is set to '25' and the 'Central Office switch type' is set to '100% compatible with Bellcore standard (STD)'. The 'Integrated Services Signaling Link Maximum' is set to '4000' and the 'Signalling server resource capacity' is set to '3700'.

Continue to expand the **Basic options (BSCOPT)** section. Keep all fields at default and click on **Edit** button in the **Remote Capabilities** field.

- Basic options (BSCOPT)

Primary D-channel for a backup DCH: Range: 0 - 254

- PINX customer number:

- Progress signal:

- Calling Line Identification:

- Output request Buffers: 32

- D-channel transmission Rate: 56 kb/s when LCMT is AMI (56K)

- Channel Negotiation option: No alternative acceptable, exclusive. (1)

- Remote Capabilities: **Edit**

+ - Change protocol timer value (TIMR)

The **Remote Capabilities Configuration** page is displayed. Make sure that **Message waiting interworking with DMS-100 (MWI)** and **Network name display method 2 (ND2)** check boxes checked. Click on **Return – Remote Capabilities** button to return to the D-Channel page.

Message waiting interworking with DMS-100 (MWI) ☒

Network access data (NAC) ☐

Network call trace supported (NCT) ☐

Network name display method 1 (ND1) ☐

Network name display method 2 (ND2) ☒

Network name display method 3 (ND3) ☐

Name display - integer ID coding (NDI) ☐

Name display - object ID coding (NDO) ☐

Path replacement uses integer values (PRI) ☐

Path replacement uses object identifier (PRO) ☐

Release Link Trunks over IP (RLTI) ☐

Remote virtual queuing (RVQ) ☐

Trunk anti-tromboning operation (TAT) ☐

User to user service 1 (UUS1) ☐

NI-2 name display option. (NDS) ☐

Message waiting indication using integer values (QMWI) ☐

Message waiting indication using object identifier (QMWO) ☐

User to user signalling (UUI) ☐

Return - Remote Capabilities **Cancel**

Keep all values at default for the **Change protocol time value (time)** and **Advanced options (ADVOPT)** sections. Click on the **Submit** button in the bottom of the D-channel configuration page to save and complete.

5.4. Administer Zone Bandwidth

To configure a Zone, from the homepage of Element Manager expand the menu **System** → **IP Network** → **Zones** and select the **Zones** tab. The **Zones** page is displayed in the right-hand side as shown below.

AVAYA CS1000 Element Manager Help | Logout

Managing: **10.97.90** Username: admin
System » IP Network » Zones

Zones

Zones are used to group related information for either bandwidth or dial plan numbering purposes.

Bandwidth Zones
Bandwidth zones are used for alternate routing of calls between IP stations and also for bandwidth management.

Numbering Zones
Numbering zones are used to route calls through a centralized call server.

Click on the **Bandwidth Zones** link. The **Bandwidth Zones** page is displayed (screen not shown) and clicks on the **Add** button to add a new zone. The **Zone Basic Property and Bandwidth Management** page is displayed. Enter number **255** in the **Zone Number**, select **Zone Intent (ZBRN)** as **VTRK** (this zone is intended to use for virtual trunks) and keep other fields at their defaults. Click on **Save** button to save changes and complete to add the new zone.

Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	255 * (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	1000000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ) ▼
Interzone Bandwidth (INTER_BW):	1000000 (0 - 10000000)
Interzone Strategy (INTER_STGY):	Best Quality (BQ) ▼
Resource Type (RES_TYPE):	Shared (SHARED) ▼
Zone Intent (ZBRN):	VTRK (VTRK) ▼
Description (ZDES):	

* Required value.

Save **Cancel**

5.5. Administer SIP Route

To configure a SIP Route, from the homepage of Element Manager, navigate to **Routes and Trunks** → **Routes and Trunks**. The **Routes and Trunks** page is displayed in the right-hand side. In the compliance test, the route and trunks were created in the **Customer 1**. Expand the **Customer: 1** there is SIP route **101** already created and used for the compliance test as shown in the screen below.

The screenshot shows the Avaya CS1000 Element Manager interface. The left sidebar contains a navigation menu with categories like Emergency Services, Geographic Redundancy, Software, Customers, Routes and Trunks, D-Channels, Digital Trunk Interface, Dialing and Numbering Plans, Electronic Switched Network, Flexible Code Restriction, Incoming Digit Translation, Phones, Templates, Reports, Views, and Lists. The main content area is titled 'Routes and Trunks' and displays a summary table for two customers. The 'Customer: 1' row is highlighted with a red box. Below this, a detailed list of routes for Customer 1 is shown, with 'Route: 101' highlighted by a red box.

Routes and Trunks			
+ Customer: 0	Total routes: 2	Total trunks: 32	Add route
- Customer: 1	Total routes: 4	Total trunks: 89	Add route
+ Route: 10 Type: DID Description: TMDI Edit Add trunk			
+ Route: 51 Type: MUS Description: MUS Edit Add trunk			
+ Route: 101 Type: TIE Description: SIPTRK Edit Add trunk			
+ Route: 111 Type: TIE Description: SIPL Edit Add trunk			

Click on **Edit** button on the route **101** to show the configuration of this route. All necessary parameters of the **Basic Configuration** section are shown in the screenshot below.

AVAYA

CS1000 Element Manager

Help | Logout

- UCM Network Services
- Home
- Links
 - Virtual Terminals
- System
 - + Alarms
 - Maintenance
 - + Core Equipment
 - Peripheral Equipment
 - IP Network
 - Nodes: Servers, Media Cards
 - Maintenance and Reports
 - Media Gateways
 - Zones
 - Host and Route Tables
 - Network Address Translation (NAT)
 - QoS Thresholds
 - Personal Directories
 - Unicode Name Directory
 - + Interfaces
 - Engineered Values
 - + Emergency Services
 - + Geographic Redundancy
 - + Software
- Customers
- Routes and Trunks
 - [Routes and Trunks](#)
 - D-Channels
 - Digital Trunk Interface
- Dialing and Numbering Plans
 - Electronic Switched Network
 - Flexible Code Restriction
 - Incoming Digit Translation
- Phones
 - Templates
 - Reports
 - Views
 - Lists
 - Properties
 - Migration
- Tools
 - + Backup and Restore
 - Date and Time
 - + Logs and reports
- Security
 - + Passwords
 - + Policies
 - + Login Options

Customer 1, Route 101 Property Configuration

- Basic Configuration

Route data block (RDB) (TYPE) :

Customer number (CUST) :

Route number (ROUT) :

Designator field for trunk (DES) :

Trunk type (TKTP) :

Incoming and outgoing trunk (ICOG) :

Access code for the trunk route (ACOD) : *

Trunk type M911P (M911P) : ☐

The route is for a virtual trunk route (VTRK) : ☒

- Zone for codec selection and bandwidth management (ZONE) : (0 - 8000)

- Node ID of signaling server of this route (NODE) : (0 - 9999)

- Protocol ID for the route (PCID) :

- Print correlation ID in CDR for the route (CRID) : ☐

- Enable Shared Bandwidth Management for the route (SBWM) : ☐

Integrated services digital network option (ISDN) : ☒

- Mode of operation (MODE) :

- D channel number (DCH) : (0 - 254)

- Interface type for route (IFC) :

- Private network identifier (PNI) : (0 - 32700)

- Network calling name allowed (NCNA) : ☒

- Network call redirection (NCRD) : ☒

- - Trunk route optimization (TRO) : ☐

- Recognition of DTI2 ABCD FALT signal for ISL (FALT) : ☐

- Channel type (CHTY) :

- Call type for outgoing direct dialed TIE route (CTYP) :

- Insert ESN access code (INAC) : ☒

- Integrated service access route (ISAR) : ☐

- Display of access prefix on CLID (DAPC) : ☐

- Mobile extension route (MBXR) : ☐

- Mobile extension outgoing type (MBXOT) :

- Mobile extension timer (MBXT) : (0 - 8000 milliseconds)

Calling number dialing plan (CNDP) :

Keep all values at default for the **Basic Route Options**, **Network Options**, **General Options**, and **Advanced Configurations** sections as shown in the screenshots below.

AVAYA
CS1000 Element Manager

Help
Logout

- UCM Network Services
- Home
- Links
- Virtual Terminals
+ System
- Customers
+ Routes and Trunks
- Dialing and Numbering Plans
- Electronic Switched Network
- Flexible Code Restriction
- Incoming Digit Translation
+ Phones
- Tools
+ Backup and Restore
- Date and Time
+ Logs and reports
- Security
+ Passwords
+ Policies
+ Login Options

Managing: **135.10.97.90** Username: admin
Routes and Trunks » Routes and Trunks » Customer 1, Route 101 Property Configuration

Customer 1, Route 101 Property Configuration

+ Basic Configuration

- Basic Route Options

Attendant announcement (ATAN) : No Attendant Announcement. (NO)
Billing number required (BILN) :
Call detail recording (CDR) :
North American toll scheme (NATL) :
Controls or timers (CNTL) :
Conventional (Tie trunk only) (CNVT) :
Incoming DID digit conversion on this route (IDC) :
Multifrequency compelled or MFC signaling (MFC) : No MFC (NO)
Process notification networked calls (PNNC) :

- Network Options


Electronic switched network pad control (ESN) :
Signaling arrangement (SIGO) : Standard (STD)
Route class (RCLS) : Route Class marked as external (EXT)
Off-hook queuing (OHQ) :
Off-hook queue threshold (OHQT) : 0
Call back queuing (CBQ) :
Number of digits (NDIG) : 2
Authcode (AUTH) :

- General Options

M1 is the only controlling party on incoming calls (CPDC) :
Dial tone on originating calls (DLTN) :
Hold failure threshold (HOLD) : 02 02 40
Trunk access restriction group (TARG) : 01
Alternate trunk route for outgoing trunks (STEP) : (0 - 511)
Actual outgoing toll digits to be ignored for code restriction (OABS) :
Display IDC name (DNAM) :
Enable equal access restrictions (EQAR) :
ACD DNIS route (DNIS) :
Include DNIS number in CDR records (DCDR) :

+ Advanced Configurations

The screen below shows the parameters of the **Advanced Configurations** section of the route 101.



CS1000 Element Manager

[Help](#) | [Logout](#)

- UCM Network Services
- Home
- Links
 - Virtual Terminals
- + System
- Customers
- + Routes and Trunks
- Dialing and Numbering Plans
 - Electronic Switched Network
 - Flexible Code Restriction
 - Incoming Digit Translation
- + Phones
- Tools
 - + Backup and Restore
 - Date and Time
 - + Logs and reports
- Security
 - + Passwords
 - + Policies
 - + Login Options

- Advanced Configurations

Malicious call trace alarm is allowed for external calls (ALRM) : ☐

Allow last re-directing number (ARDN) : ARDN (NO) ▼

ANI identifier number (ANTK) :

AC15 timed reminder recall (ATTR) : ☐

Auto terminate (AUTO) : ☐

Collect call blocking allowed (CCBA) : ☐

Call forward restriction (CFWR) : ☐

Maximum number of CNL digits (CLEN) : 10 ▼

Time (in seconds) that an extension is allowed to ring or be On-hold or Call Park before the trunk is disconnected (DCTI) : (0 - 511)

North American distinctive ringing for incoming calls (DRNG) : ☐

Home local number (HLCL) :

Home national number (HNTN) :

In-band automatic number identification route (IANI) : ☐

Incoming identifier send (ICIS) : ☒

Internal/external definition (IDEF) : Use network info (NET) ▼

Identify originating party (IDOP) : ☐

Insert (INST) :

Manual outgoing trunk route (MANO) : ☐

Manual route (MNL) : ☐

Music on-hold (MUS) : ☒

- Music route number (MRT) : (0 - 511)

Outgoing identifier send (OGIS) : ☒

Off-hook timer delay (OHTD) : ☐

Outpulsing route (OPR) : ☐

Pseudo answer (PANS) : ☒

Periodic clearing signal (PECL) : ☐

Privacy indicator ignored (PII) : ☐

Auxiliary application (AUXP) : ☐

Priority level (PLEV) : 2 ▼

Protocol selection (PSEL) : DM-DM Protocol Selection (DMDM) ▼

Preference trunk usage threshold (PTUT) : (0 - 510)

Port type at far end (PTYP) : Analog TIE trunks (ATT) ▼

Route traffic information in ACD Reports (RACD) : ☐

Radio paging route (RPA) : ☐

5.6. Administer SIP Trunks

To configure SIP trunks, from the homepage of Element Manager, navigate to **Routes and Trunks** → **Routes and Trunks**. The **Routes and Trunks** page is displayed in the right-hand side. In the compliance test, the route and trunks were created in the **Customer 1**. Expand the **Customer: 1** and the SIP route **101** there are 32 SIP trunks already created as shown below.

Customer	Total routes	Total trunks	Action
Customer: 0	2	32	Add route
Customer: 1	4	89	Add route

Route	Type	Description	Action
Route: 10	DID	TMDI	Edit Add trunk
Route: 51	MUS	MUS	Edit Add trunk
Route: 101	TIE	SIPTRK	Edit Add trunk

Trunk	TN	Description	Action
Trunk: 1 - 32	Total trunks: 32		
Trunk: 1	100 0 01 00	Description: XO	Edit Multi-Del
Trunk: 2	100 0 01 01	Description: XO	Edit
Trunk: 3	100 0 01 02	Description: XO	Edit
Trunk: 4	100 0 01 03	Description: XO	Edit
Trunk: 5	100 0 01 04	Description: XO	Edit
Trunk: 6	100 0 01 05	Description: XO	Edit

Click on **Edit** button on **Trunk: 1** to show configuration of this SIP trunk. The configuration of the trunk 1 is the same for the rest of SIP trunks. The screen below shows the **Basic Configuration** of the SIP trunk. Keep all values at default for the **Advance Trunk Configurations** section.

Customer 1, Route 101, Trunk 1 Property Configuration

- Basic Configuration

Auto increment member number: ☒

Trunk data block:

Terminal number:

Designator field for trunk:

Extended trunk:

Member number: *

Level 3 Signaling:

Card density:

Start arrangement Incoming:

Start arrangement Outgoing:

Trunk group access restriction:

Channel ID for this trunk:

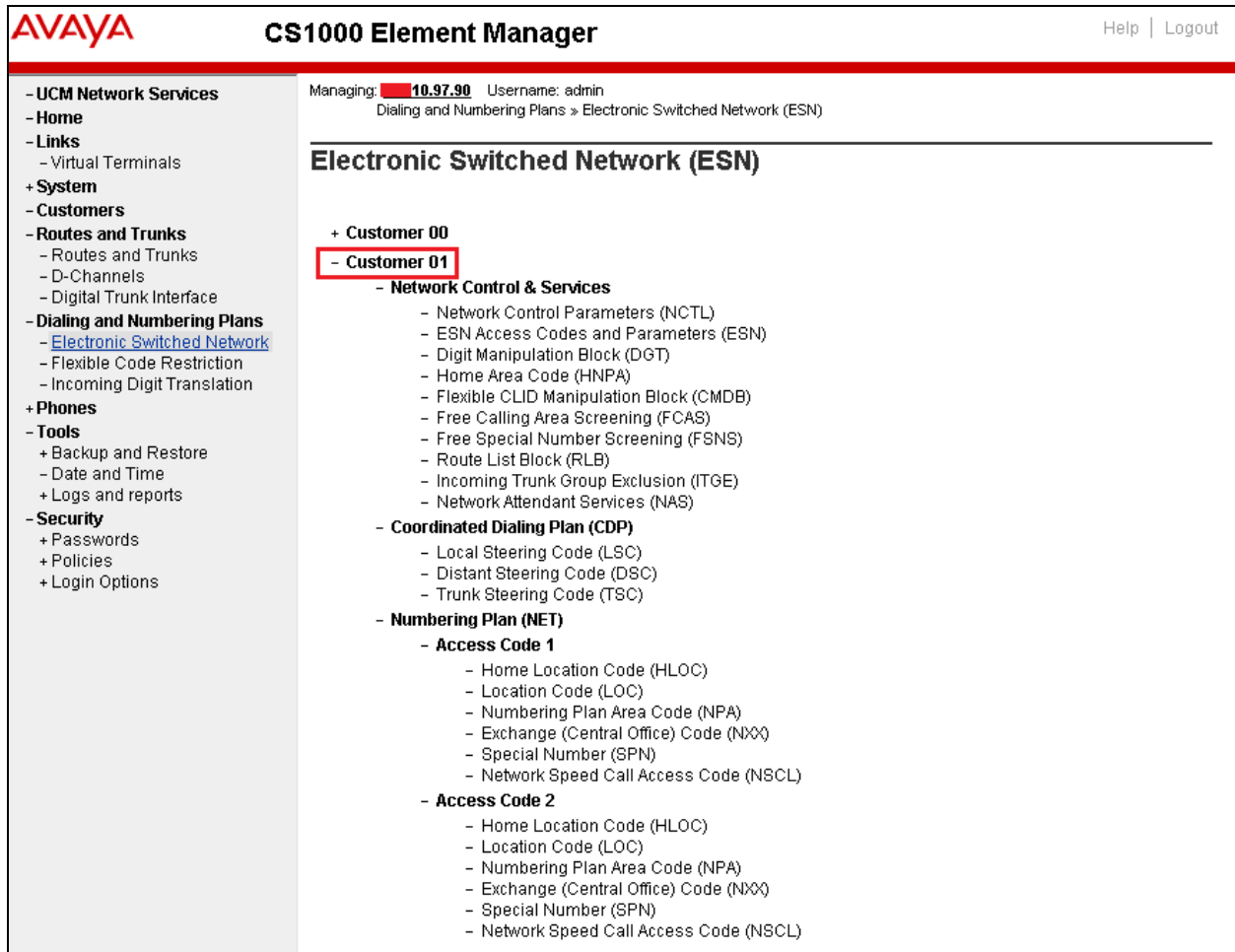
Class of Service:

5.7. Administer CDP Dialing Plan

This section provides the steps on how to create a new Route List Index (RLI) and a new Distant Steering Code (DSC) for the Coordinated Dialing Plan (CDP) dialing plan.

5.7.1. Configure Route List Index (RLI)

To configure Route List Index, from the home page of Element Manger, navigate to **Dialing and Numbering Plan → Electronic Switched Network**. The **Electronic Switched Network (ESN)** page is displayed; expand the **Customer 01** which the RLI will be created.



AVAYA CS1000 Element Manager Help | Logout

Managing: **10.97.90** Username: admin
Dialing and Numbering Plans > Electronic Switched Network (ESN)

Electronic Switched Network (ESN)

- + Customer 00
- Customer 01**
 - Network Control & Services
 - Network Control Parameters (NCTL)
 - ESN Access Codes and Parameters (ESN)
 - Digit Manipulation Block (DGT)
 - Home Area Code (HNPA)
 - Flexible CLID Manipulation Block (CMDB)
 - Free Calling Area Screening (FCAS)
 - Free Special Number Screening (FSNS)
 - Route List Block (RLB)
 - Incoming Trunk Group Exclusion (ITGE)
 - Network Attendant Services (NAS)
 - Coordinated Dialing Plan (CDP)
 - Local Steering Code (LSC)
 - Distant Steering Code (DSC)
 - Trunk Steering Code (TSC)
 - Numbering Plan (NET)
 - Access Code 1
 - Home Location Code (HLOC)
 - Location Code (LOC)
 - Numbering Plan Area Code (NPA)
 - Exchange (Central Office) Code (NXX)
 - Special Number (SPN)
 - Network Speed Call Access Code (NSCL)
 - Access Code 2
 - Home Location Code (HLOC)
 - Location Code (LOC)
 - Numbering Plan Area Code (NPA)
 - Exchange (Central Office) Code (NXX)
 - Special Number (SPN)
 - Network Speed Call Access Code (NSCL)

Click on the **Route List Block (RLB)** link, the **Route List Blocks** page is displayed as the screen below. In the testing, the Route Link Block Index **101** was created and used the route **101** as configured in **Section 5.5**.

AVAYA **CS1000 Element Manager** Help | Logout

Managing: **10.97.90** Username: admin
Dialing and Numbering Plans » [Electronic Switched Network \(ESN\)](#) » Customer 01 » Network Control & Services » Route List Blocks

Route List Blocks

Please enter a route list index (0 - 1999)

- + Route List Block Index -- 1
- + Route List Block Index -- 10
- + Route List Block Index -- 11
- + Route List Block Index -- 12
- **Route List Block Index -- 101**
 - Initial Set: 0
 - Number of Alternate Routing Attempts: 5
 - Set Minimum Facility Restriction Level : 0
 - Data Entry Index -- 0
 - Route Number: 101**
 - Expensive Route: N
 - Facility Restriction Level: 0
 - Digit Manipulation Index: 0
 - ISL D-Channel Down Digit Manipulation Index: 0
 - Free Calling Area Screening Index: 0
 - Free Special Number Screening Index: 0
 - Business Network Extension Route: NO
- + Route List Block Index -- 102

5.7.2. Create a Distant Steering Code (DSC)

In the **Customer 01** of the Electronic Switch Network (ESN) page, select **Distant Steering Code (DSC)** under **Coordinated Dialing Plan (CDP)**.

AVAYA CS1000 Element Manager Help | Logout

Managing: **10.97.90** Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN)

Electronic Switched Network (ESN)

- + Customer 00
- **Customer 01**
 - Network Control & Services
 - Network Control Parameters (NCTL)
 - ESN Access Codes and Parameters (ESN)
 - Digit Manipulation Block (DGT)
 - Home Area Code (HNPA)
 - Flexible CLID Manipulation Block (CMDB)
 - Free Calling Area Screening (FCAS)
 - Free Special Number Screening (FSNS)
 - Route List Block (RLB)
 - Incoming Trunk Group Exclusion (ITGE)
 - Network Attendant Services (NAS)
 - Coordinated Dialing Plan (CDP)
 - Local Steering Code (LSC)
 - **Distant Steering Code (DSC)**
 - Trunk Steering Code (TSC)
 - Numbering Plan (NET)
 - Access Code 1
 - Home Location Code (HLOC)
 - Location Code (LOC)
 - Numbering Plan Area Code (NPA)
 - Exchange (Central Office) Code (NXX)
 - Special Number (SPN)
 - Network Speed Call Access Code (NSCL)
 - Access Code 2
 - Home Location Code (HLOC)
 - Location Code (LOC)
 - Numbering Plan Area Code (NPA)
 - Exchange (Central Office) Code (NXX)
 - Special Number (SPN)
 - Network Speed Call Access Code (NSCL)

The **Distant Steering Code List** page is displayed. In the testing, the distant steering code **45** was configured for routing call from CS 1000 to Vision. The distant steering code contains 4 digits and used the route list index **101** as configured in **Section 5.7.1** above.

The screenshot shows the AVAYA CS1000 Element Manager web interface. The top header includes the AVAYA logo, the title "CS1000 Element Manager", and links for "Help" and "Logout". A left-hand navigation menu lists various system services and configuration options. The main content area displays the "Distant Steering Code" configuration page. At the top of this page, it shows the current user session: "Managing: 10.97.90 Username: admin" and the navigation path: "Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 01 » Coordinated Dialing Plan (CDP) » Distant Steering Code List » Distant Steering Code". The configuration fields include: "Distant Steering Code" set to 45, "Flexible Length number of digits" set to 4 (with a range of 0-10), "Display" set to "Local Steering Code (LSC)", "Remote Radio Paging Access" as an unchecked checkbox, "Route List to be accessed for trunk steering code" set to 101, "Collect Call Blocking" as an unchecked checkbox, and two empty text boxes for "Maximum 7 digit NPA code allowed" and "Maximum 7 digit NXX code allowed". At the bottom right, there are four buttons: "Submit", "Refresh", "Delete", and "Cancel".

AVAYA CS1000 Element Manager Help | Logout

Managing: 10.97.90 Username: admin
Dialing and Numbering Plans » [Electronic Switched Network \(ESN\)](#) » Customer 01 » Coordinated Dialing Plan (CDP) » [Distant Steering Code List](#) » Distant Steering Code

Distant Steering Code

Distant Steering Code: 45

Flexible Length number of digits: 4 (0 - 10)

Display: Local Steering Code (LSC) ▼

Remote Radio Paging Access: ☐

Route List to be accessed for trunk steering code: 101 ▼

Collect Call Blocking: ☐

Maximum 7 digit NPA code allowed:

Maximum 7 digit NXX code allowed:

Submit Refresh Delete Cancel

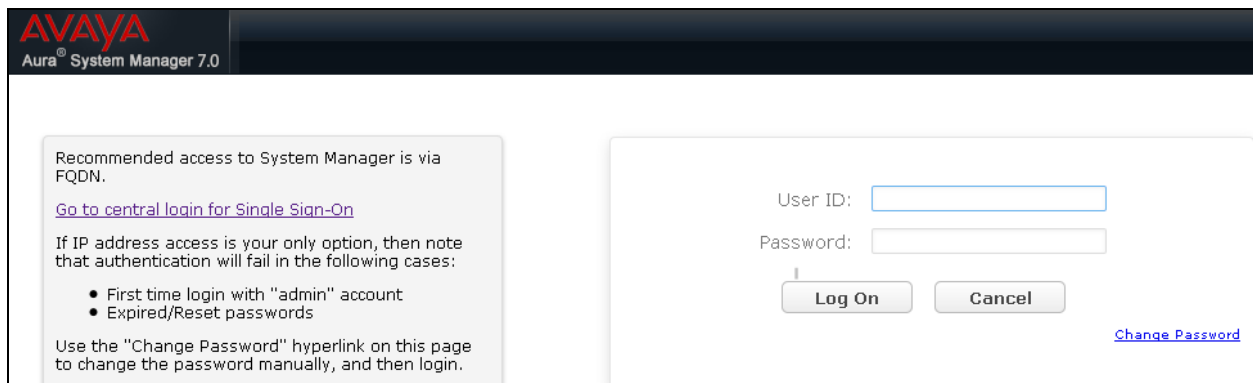
6. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer Domain
- Administer locations
- Administer Adaptation
- Administer SIP entities
- Administer routing policies
- Administer dial patterns

6.1. Launch System Manager

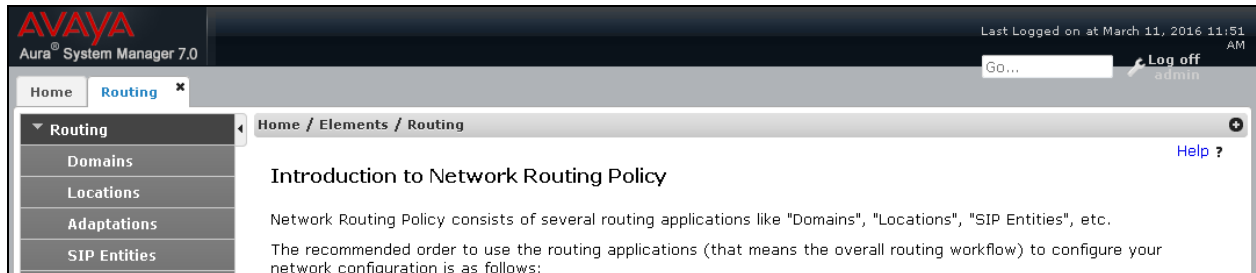
Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.



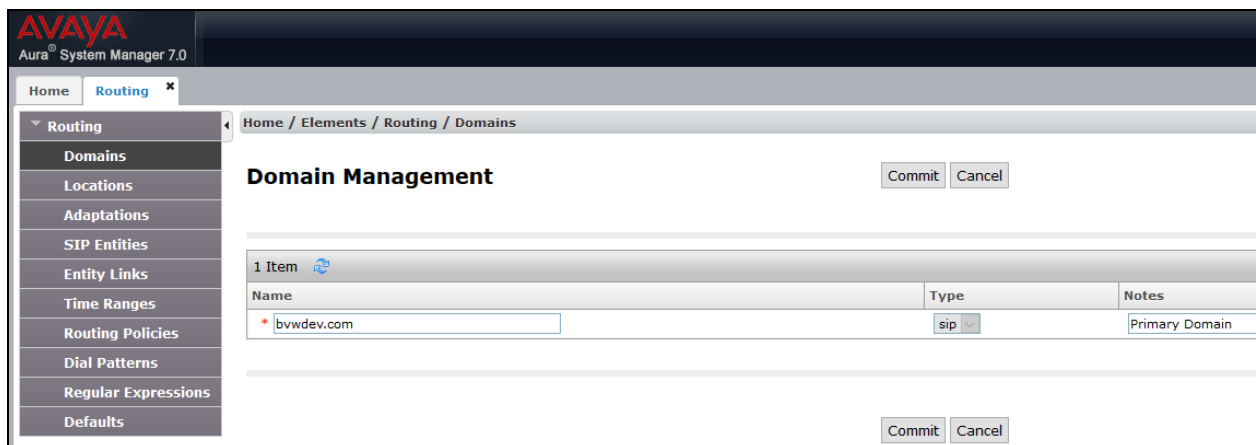
The screenshot shows the Avaya Aura System Manager 7.0 login interface. The header features the Avaya logo and the text "Aura® System Manager 7.0". The main content area is divided into two sections. The left section contains instructions: "Recommended access to System Manager is via FQDN." followed by a link "Go to central login for Single Sign-On". Below this, it states "If IP address access is your only option, then note that authentication will fail in the following cases:" and lists two bullet points: "• First time login with 'admin' account" and "• Expired/Reset passwords". It also mentions "Use the 'Change Password' hyperlink on this page to change the password manually, and then login." The right section contains the login form with fields for "User ID:" and "Password:", and "Log On" and "Cancel" buttons. A "Change Password" link is located at the bottom right of the login form.

6.2. Administer Domain

In the subsequent screen (not shown), select **Elements → Routing** to display the **Introduction to Network Routing Policy** screen below. Select **Routing → Domains** from the left pane, and click **New** in the subsequent screen (not shown) to add a new domain



The **Domain Management** screen is displayed. In the **Name** field enter the domain name, select *sip* from the **Type** drop down menu and provide any optional **Notes**.



6.3. Administer Locations

Select **Routing** → **Locations** from the left pane, and click **New** in the subsequent screen (not shown) to add a new location for Vision.

The **Location Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name** and optional **Notes**. Retain the default values in the remaining fields.

AVAYA
Aura® System Manager 7.0

Last Logged on at May 23, 201

Home Routing

Home / Elements / Routing / Locations

Location Details

Commit Cancel

General

* Name: BvwDevSIL

Notes:

Scroll down to the **Location Pattern** sub-section, click **Add** and enter the IP address of all devices involved in the compliance testing in **IP Address Pattern**, as shown below. Retain the default values in the remaining fields.

Location Pattern

Add Remove

4 Items Filter: Enable

IP Address Pattern	Notes
* 10.10.5.*	
* 10.10.97.*	
* 10.10.98.*	
*	

Select : All, None

Commit Cancel

6.4. Administer Adaptation

During compliance test, in order to make the call from and to Communication Server 1000 via Session Manager, Adaptation to translate IP address into domain name is used for Trio SIP entity. Here is step on how to create Adaptation. Select **Adaptations** on the left panel menu and then click on the **New** button in the main window (not shown). Enter the following for the Trio Adaptation.

- **Adaptation Name** An informative name (e.g., **change IP to Domain Trio**)
- **Module Name** Select **DigitConversionAdapter**
- **Module Parameter Type** Select Name-Value Parameter

Click **Add** to add a new row for the following values as shown below table:

Name	Value
fromto	true
iodstd	Enter the domain name of system, ex: bvwddev.com
iosrcd	Enter the domain name of system, ex: bvwddev.com
odstd	Enter IP address of Trio, ex: 10.10.98.8
osrcd	Enter IP Address of Session Manager, ex: 10.33.1.12

Once the correct information is entered click the **Commit** button. Here is the screenshot show Adaptation created for Trio.

AVAYA
Aura® System Manager 7.0

Last Logged on at May 23, 201

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel

General

* Adaptation Name: Trio Adapt

* Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

Name	Value
fromto	true
iodstd	bvwddev.com
iosrcd	bvwddev.com

(Continue) the screenshot show Adaptation created for Trio:

The screenshot displays the Avaya Aura System Manager 7.0 interface. The top header shows the Avaya logo and 'Aura System Manager 7.0'. The user is logged in as 'admin' on May 23, 2017. The left sidebar contains a navigation menu with 'Routing' selected, showing sub-items like Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Adaptation Details' and shows the 'General' tab. The 'Adaptation Name' is 'Trio Adapt'. The 'Module Name' is 'DigitConversionAdapter' and the 'Module Parameter Type' is 'Name-Value Parameter'. Below this is a table with two rows: 'odstd' with value '10.10.98.8' and 'osrcd' with value '10.33.1.12'. The table has 'Add' and 'Remove' buttons. The bottom of the page shows 'Page 2 of 2'.

AVAYA
Aura System Manager 7.0

Last Logged on at May 23, 2017

Home Routing

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel

General

* Adaptation Name: Trio Adapt

* Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

Name	Value
odstd	10.10.98.8
osrcd	10.33.1.12

Select : All, None

Page 2 of 2

6.5. Administer SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes Communication Server 1000 and Vision.

6.5.1. SIP Entity for Session Manager

Navigate to **Routing** → **SIP Entities** in the left 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:** Select *Session Manager* for Session Manager.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager** if Adaptations were to be created, here is where they would be applied to the entity.
- **Location:** Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of the *Session Manager* SIP Entity for Session Manager. The IP address of the Session Manager Security Module is entered in the **FQDN or IP Address** field.

The screenshot displays the Avaya Aura System Manager 7.0 web interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 7.0', and a 'Last Logged on at May 23, 2017' timestamp. Below the navigation bar, there are tabs for 'Home', 'Session Manager', and 'Routing'. The 'Routing' tab is active, and the breadcrumb trail shows 'Home / Elements / Routing / SIP Entities'. On the left, a vertical navigation pane lists various configuration options: Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and has a 'General' sub-section. It contains several input fields: 'Name' (with a red asterisk) containing 'ASM70A', 'FQDN or IP Address' (with a red asterisk) containing '10.33.1.12', 'Type' (a dropdown menu set to 'Session Manager'), 'Notes' (an empty text area), 'Location' (a dropdown menu set to 'BvwDevSIL'), 'Outbound Proxy' (an empty text area), 'Time Zone' (a dropdown menu set to 'America/Toronto'), and 'Credential name' (an empty text area). At the bottom, there is a 'SIP Link Monitoring' section with a dropdown menu set to 'Use Session Manager Configuration'. 'Commit' and 'Cancel' buttons are located at the top right of the form area.

6.5.2. SIP Entity for Communication Server 1000

Select **Routing** → **SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for Communication Server 1000. Note that this SIP entity is used for integration with Vision.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The node IP address of Communication Server 1000 SIP Gateway as mentioned in **Section 5.2**.
- **Type:** Select “SIP Trunk” in the dropdown list.
- **Notes:** Any desired notes.
- **Location:** Select the applicable location for Communication Server 1000.
- **Time Zone:** Select the applicable time zone.

AVAYA
Aura® System Manager 7.0

Last Logged on at May 24, 2017 9:18
GO... Log off admin

Home Routing

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel Help ?

General

* Name: Car2-cores

* FQDN or IP Address: 10.10.97.170

Type: SIP Trunk

Notes: CS1000 Node 2001

Adaptation:

Location: BvwDevSIL

Time Zone: America/Toronto

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

Credential name:

Securable: ☐

Call Detail Recording: none

6.5.3. SIP Entity for Vision

Select **Routing** → **SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for Vision.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of the Vision server.
- **Type:** Select “SIP Trunk” in the dropdown list.
- **Notes:** Any desired notes.
- **Adaptation:** Select the adaptation configured in **Section 6.4**
- **Location:** Select the applicable location from **Section 6.3**.
- **Time Zone:** Select the applicable time zone.

The screenshot displays the Avaya Aura System Manager 7.0 interface. The top header shows the Avaya logo and 'Aura System Manager 7.0'. The user is logged in as 'admin' on May 24, 2017, at 9:18. The left navigation pane has 'Routing' selected, with a sub-menu showing 'SIP Entities' as the active option. The main content area is titled 'SIP Entity Details' and has a 'General' tab selected. The form contains the following fields and values:

- Name:** VisionHA
- * FQDN or IP Address:** 10.10.98.8
- Type:** SIP Trunk
- Notes:** (empty)
- Adaptation:** Trio Adapt
- Location:** BvwDevSIL
- Time Zone:** America/Toronto
- * SIP Timer B/F (in seconds):** 4
- Credential name:** (empty)
- Securable:** ☐
- Call Detail Recording:** none

Buttons for 'Commit' and 'Cancel' are visible in the top right of the form area. A 'Help ?' link is also present.

6.6. Administer Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the Communication Server 1000 and one to Vision. To add an Entity Link, select to **Routing → Entity Links** in the left 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 Session Manager from the drop-down menu.
- **Protocol:** Select applicable transport protocol.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.
- **SIP Entity 2:** Select the name of the other systems from the drop-down menu.
- **Port:** Port number on which the other system receives SIP requests from Session Manager.
- **Connection Policy:** Select **Trusted** to allow calls from the associated SIP Entity.

The screens below show the Entity Link to Communication Server 1000 and Vision. During the compliance test, **TLS** transport with port **5061** was used between Session Manager and Communication Server 1000.

The screenshot shows the 'Entity Links' configuration page. The breadcrumb trail is 'Home / Elements / Routing / Entity Links'. The page title is 'Entity Links'. There are 'Commit' and 'Cancel' buttons. A table with 1 item is displayed. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, and Port. The row shows: Name: *ASM70_Car2-cores_50, SIP Entity 1: *ASM70A, Protocol: TLS, Port: *5061, SIP Entity 2: *Car2-cores, DNS Override: ☐, Port: *5061. The 'Select' dropdown is set to 'All, None'.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port
*ASM70_Car2-cores_50	*ASM70A	TLS	*5061	*Car2-cores	<input type="checkbox"/>	*5061

The Entity Link to Vision is shown below; **UDP** transport and port **5060** were used.

The screenshot shows the 'Entity Links' configuration page. The breadcrumb trail is 'Home / Elements / Routing / Entity Links'. The page title is 'Entity Links'. There are 'Commit' and 'Cancel' buttons. A table with 1 item is displayed. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, and Port. The row shows: Name: *ASM70A_VisionHA_506, SIP Entity 1: *ASM70A, Protocol: UDP, Port: *5060, SIP Entity 2: *VisionHA, DNS Override: ☐, Port: *5060. The 'Select' dropdown is set to 'All, None'.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port
*ASM70A_VisionHA_506	*ASM70A	UDP	*5060	*VisionHA	<input type="checkbox"/>	*5060

6.7. Administer Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies were added: an incoming policy with Communication Server 1000 as the destination, and an incoming policy to Vision. To add a routing policy, select to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed:

- In the **General** section, enter a descriptive **Name** and add a brief description under **Notes** (optional).
- In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Choose the appropriate SIP entity to which this routing policy applies (**Section 6.5**) and click **Select**. The selected SIP Entity displays on the **Routing Policy Details** page as shown below.
- Use default values for remaining fields.
- Click **Commit** to save.

The following screens show the Routing Policy for Communication Server 1000.

The screenshot displays the Avaya Aura System Manager 7.0 web interface. The left navigation pane shows the 'Routing' menu expanded, with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and contains two sections: 'General' and 'SIP Entity as Destination'. In the 'General' section, the 'Name' field is set to 'To-Car2-Cores', 'Disabled' is unchecked, 'Retries' is set to 0, and the 'Notes' field is empty. In the 'SIP Entity as Destination' section, a table lists the selected SIP entity: 'Car2-cores' with FQDN or IP Address '10.10.97.170', Type 'Other', and Notes 'CS1000 Node 2001'. The interface includes a 'Commit' button and a 'Cancel' button at the top right of the form area.

Name	FQDN or IP Address	Type	Notes
Car2-cores	10.10.97.170	Other	CS1000 Node 2001

The following screens show the Routing Policy for Vision.

The screenshot displays the Avaya Aura System Manager 7.0 web interface. The top header shows the Avaya logo and 'Aura System Manager 7.0'. The right side of the header indicates 'Last Logged on at May 24, 2017' and includes a 'GO...' button. The left sidebar contains a navigation menu with options: Home, Routing (selected), Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies (highlighted), Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Routing Policy Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' tab, the following fields are visible: '* Name: To-VisionHA', 'Disabled: ☐', '* Retries: 0', and 'Notes:'. Below this is the 'SIP Entity as Destination' section, which includes a 'Select' button and a table with the following data:

Name	FQDN or IP Address	Type	Notes
VisionHA	10.10.98.8	SIP Trunk	

6.8. Administer Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Server 1000 to Vision 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.

6.8.1. Dial Pattern for Vision

Select **Routing** → **Dial Patterns** from the left pane, and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach Vision. The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern:** A dial pattern to match, in this case “45”.
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.
- **SIP Domain:** The signaling group domain name from **Section 6.2**.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching Vision. In the compliance testing, the entry allowed for call originations from all Communication Server 1000 endpoints in the location “BvwDevSIL”. The Vision routing policy from **Section 6.7** was selected as shown below.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details [Help ?](#)

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

1 Item [Filter: Enable](#)

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	BvwDevSIL		To-VisionHA	0	<input type="checkbox"/>	VisionHA	

6.8.2. Dial Pattern for Communication Server 1000

Select **Routing** → **Dial Patterns** from the left pane, and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach Communication Server 1000. The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern:** A dial pattern to match, in this case “46”.
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.
- **SIP Domain:** The signaling group domain name from **Section 6.2**.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching Communication Server 1000. In the compliance testing, the entry allowed for call originations from all Vision endpoints in locations “BvwDevSIL”. The Communication Server 1000 routing policy from **Section 6.5** was selected as shown below.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details Commit Cancel [Help ?](#)

General

* **Pattern:** 46

* **Min:** 4

* **Max:** 4

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: bvwddev.com

Notes: Dial Pattern to CS1K Cores

Originating Locations and Routing Policies

Add Remove

1 Item [Filter: Enable](#)

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	BvwDevSIL		To-Car2-Cores	0	<input type="checkbox"/>	Car2-cores	

7. Configure Enghouse Vision 8030HA

This section shows how to configure Vision 8030HA to successfully connect to Session Manager. The installation of the Vision 8030HA software is assumed to be completed and the correct licence is installed.

7.1. Configure SIP Trunk

Using SSH connect to the Vision 8030HA server and login with as root with the appropriate password.

```
CentOS release 6.4 (Final)
Kernel 2.6.32-042stab072.10 on an x86_64

localhost login: root
Password: _
```

At the **root@localhost** prompt start the configuration program using the **install_setup** command.

```
CentOS release 6.4 (Final)
Kernel 2.6.32-042stab072.10 on an x86_64

localhost login: root
Password:
[root@localhost ~]# install_setup _
```

Select option **4** to configure the **SIP trunk**.

```
---- System Settings ----  
  
1. General  
2. Current DHCP Network  
3. Current DHCP DNS  
4. SIP trunk  
5. Additional features  
6. Update/Import  
Change section 1-6 or (E)xit: 4_
```

Select option 1

```
---- SIP Trunk Settings ----  
  
1. T1 PBX IP addr: 1.2.3.4  
2. T1 PBX port: 5060  
3. SIP domain:  
Change 1-3 or (B)ack: 1_
```

Enter the signaling IP address of Session Manager.

```
---- SIP Trunk Settings ----  
  
1. T1 PBX IP addr: 1.2.3.4  
2. T1 PBX port: 5060  
3. SIP domain:  
Change 1-3 or (B)ack: 1  
IP or name: 10.33.1.12_
```

Select option 3.

```
---- SIP Trunk Settings ----  
1. T1 PBX IP addr: 10.33.1.12  
2. T1 PBX port: 5060  
3. SIP domain:  
Change 1-3 or (B)ack: 3_
```

Enter the SIP domain **bwdev.com** as configured in **Section 6.2**.

```
---- SIP Trunk Settings ----  
1. T1 PBX IP addr: 10.33.1.12  
2. T1 PBX port: 5060  
3. SIP domain:  
Change 1-3 or (B)ack: 3  
SIP domain: bwdev.com_
```

Return back to the previous menu.

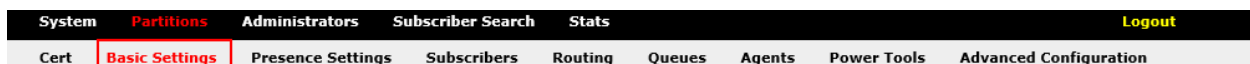
```
---- SIP Trunk Settings ----  
1. T1 PBX IP addr: 10.33.1.12  
2. T1 PBX port: 5060  
3. SIP domain: bwdev.com  
Change 1-3 or (B)ack: b_
```

Exit from the setup and reboot the server.

```
[root@localhost ~]#  
[root@localhost ~]#  
[root@localhost ~]#  
[root@localhost ~]#  
[root@localhost ~]# shutdown -r now
```

7.2. Configure Operator queue

Log on to the partition manager and go to the “Basic Settings” tab.



Enter the queue number, in this scenario the queue number was **4500**. Click **Save** when done.

The screenshot shows the 'Basic Settings' form for a partition. The 'Incoming calls' section has a 'Welcome message' dropdown and a 'Number to operator' text box containing '4500', which is highlighted with a red box. Below this is the 'Provisioning defaults' section with checkboxes for 'Presence diversion', 'Voicemail', and 'Calendar integration'. The 'Extra partition features' section has a checkbox for 'Statistics export'. At the bottom left, there is a 'Save' button highlighted with a red box.

Browse to the “Queues” tab and select to create a new queue.

The screenshot shows the 'Queues' tab selected in the sub-navigation bar. The main content area shows a table with columns: Queue Type, Size, SLA (Max time), Say est. time, Say cur. pos., Opening hours, Night action, Overflow action, Callback, and IVR feature. Below the table, it says 'No Queues defined for this partition'. At the bottom left, there is a 'Create new Queue' button highlighted with a red box.

Give the queue a suitable name, and select queue type “Operator Queue”. Click **Create** when done.

The screenshot shows the 'Create new queue' form. The 'Name' text box contains 'Main queue' and the 'Queue type' dropdown is set to 'Operator Queue (with auto generated IVR)', both highlighted with a red box. At the bottom left, there are 'Create' and 'Cancel' buttons, with the 'Create' button highlighted with a red box.

Set the queue preferences and click **Save**.

System **Partitions** **Administrators** **Subscriber Search** **Stats** **Logout**

dok **Basic Settings** **Presence Settings** **Subscribers** **Routing** **Queues** **Agents** **Power Tools** **Advanced Configuration**

Base settings for "Main queue"

Max size:

Say queue position:

Estimated queue time:

Preparation time:

Clerical time:

Max time (SLA):

Outgoing A-number: (Activated per agent)

Callback settings

Offer callback:

(Activation condition) Min. queue:

(Activation condition) Min. est. queue time:

Actions & Overflow

Night action:

Overflow action:

IVR feature:

Agent **Optional activation delay (time - count)**

Save **Cancel**

7.3. Configure routing to queue

Go to the "Routing" tab and select **Add**.

System **Partitions** **Administrators** **Subscriber Search** **Stats** **Logout**

dok **Basic Settings** **Presence Settings** **Subscribers** **Routing** **Queues** **Agents** **Power Tools** **Advanced Configuration**

Main Number **Name** **Routed to**

No Main Numbers defined for this partition

Add

Enter the number to route, give the route a suitable name and select where to route the call. In this scenario number 4500 is given the name "Main number" and is routed to the "Main queue". Click **Create** when done.

System **Partitions** **Administrators** **Subscriber Search** **Stats** **Logout**

dok **Basic Settings** **Presence Settings** **Subscribers** **Routing** **Queues** **Agents** **Power Tools** **Advanced Configuration**

Create new Main Number

Number:

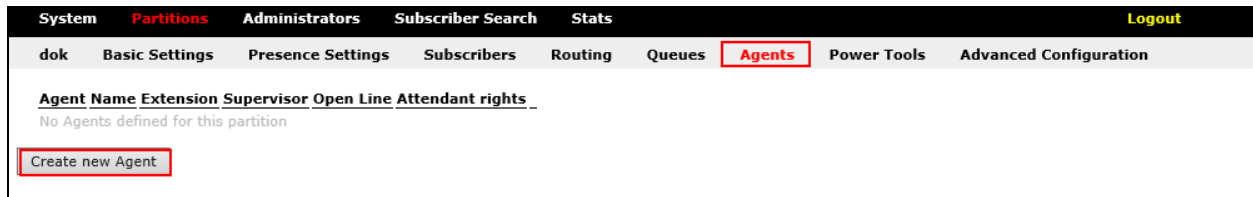
Name:

Route to:

Create **Cancel**

7.4. Setting up attendant

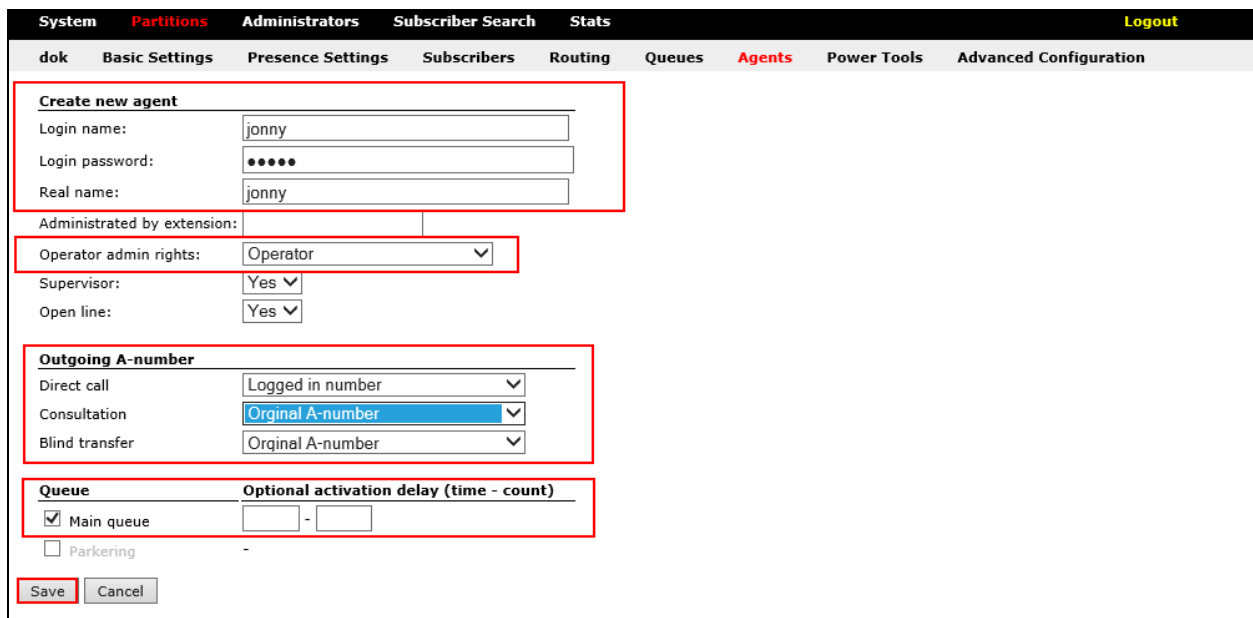
Go to the “Agents tab and select to create a new agent.



The screenshot shows the top navigation bar with tabs: System, Partitions, Administrators, Subscriber Search, Stats, and Logout. Below this is a secondary bar with: dok, Basic Settings, Presence Settings, Subscribers, Routing, Queues, Agents (highlighted with a red box), Power Tools, and Advanced Configuration. The main content area has a header with links: Agent Name, Extension, Supervisor, Open Line, and Attendant rights. Below the header, it says "No Agents defined for this partition". At the bottom, there is a red-bordered button labeled "Create new Agent".

In the **Create new agent** section, enter the attendant a login name in the **Login name** field, in this scenario “jonny” and enter the attendant a password in the **Login password** field. Select the rights to “Operator” in the **Operator admin rights** dropdown menu.

In the **Outgoing A-number** section, specify A-number settings in this scenario attendant uses logged in number for spontaneous calls and original a-number for transfers. Select which queue the attendant will service, in this scenario “Main queue”. Click **Save** when done.

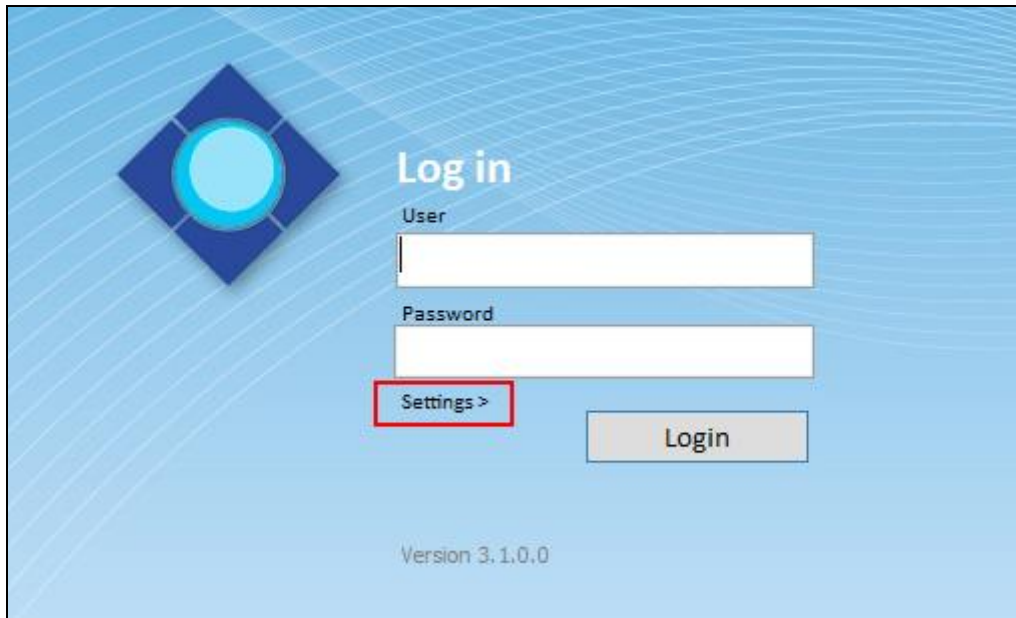


The screenshot shows the "Create new agent" form. The top navigation bar is the same as the previous screenshot. The "Agents" tab is active. The form has several sections, each highlighted with a red box:

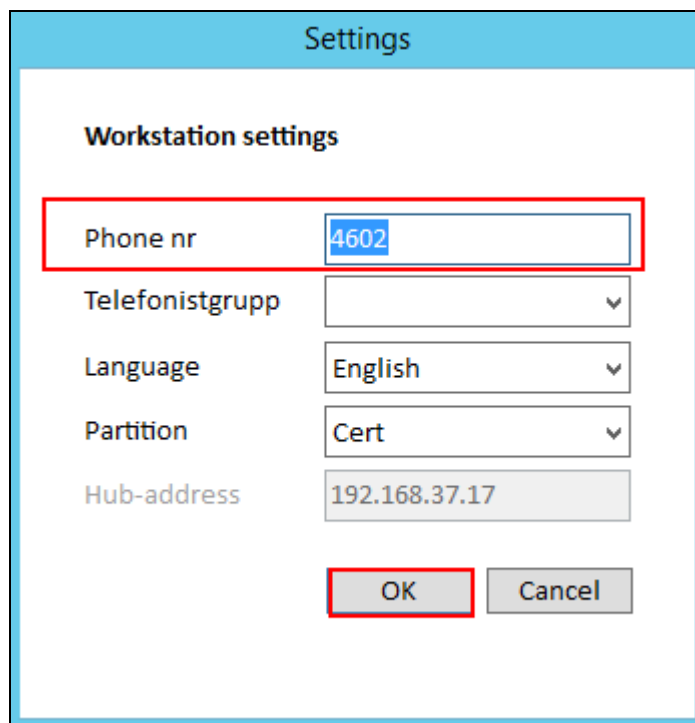
- Create new agent**: Contains fields for "Login name:" (value: jonny), "Login password:" (value: •••••), and "Real name:" (value: jonny).
- Operator admin rights**: A dropdown menu with "Operator" selected.
- Supervisor**: A dropdown menu with "Yes" selected.
- Open line**: A dropdown menu with "Yes" selected.
- Outgoing A-number**: Contains three dropdown menus: "Direct call" (value: Logged in number), "Consultation" (value: Original A-number), and "Blind transfer" (value: Original A-number).
- Queue**: A section with a checkbox "Main queue" (checked) and a field for "Optional activation delay (time - count)" (value: -).
- Parking**: A checkbox "Parking" (unchecked).
- Buttons**: "Save" and "Cancel" buttons at the bottom.

7.5. Running the attendant client

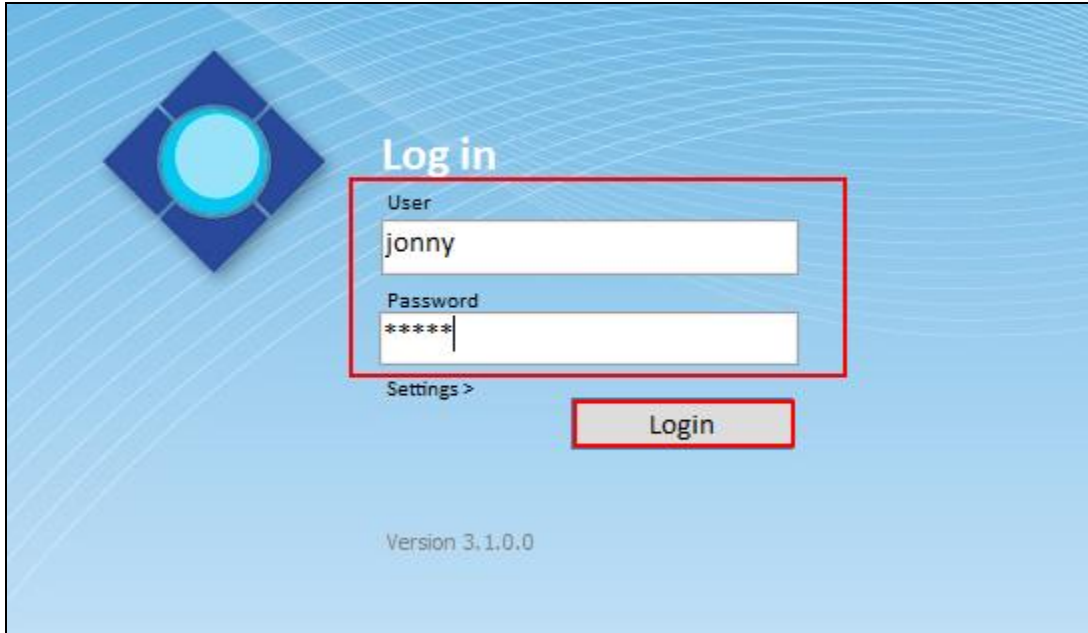
Start the “svara” application and click settings.



Select which telephone number in the Communication Server 1000 to be used as attendant phone in this case the number is **4602**, and click **OK**.

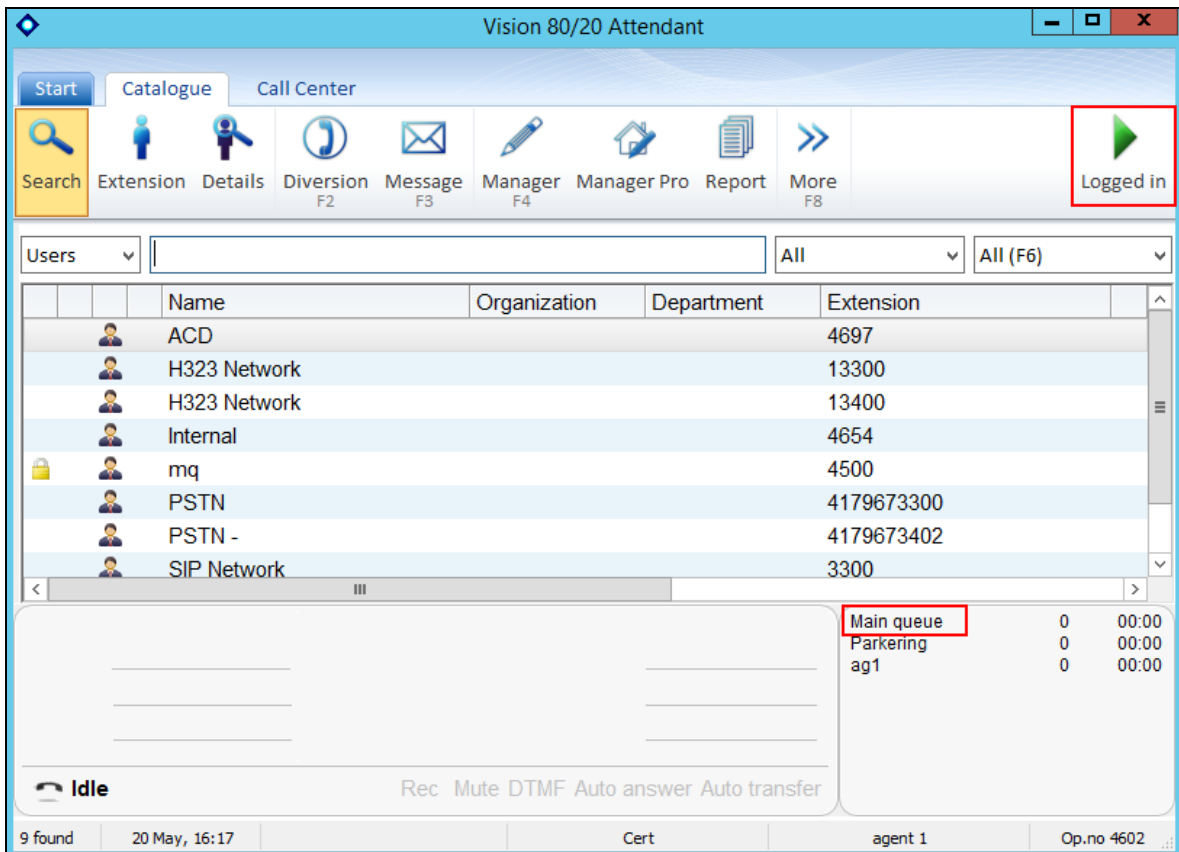


Enter the credentials as configured in the step above and click **Login**.



The login screen features a blue background with a diamond-shaped logo on the left. The title "Log in" is centered at the top. Below it, a red rectangular box highlights the "User" and "Password" input fields. The "User" field contains the text "jonny", and the "Password" field contains "*****". Below these fields is a "Settings >" link. A "Login" button is positioned below the password field. At the bottom center, the text "Version 3.1.0.0" is displayed.

When logged in it should be able to see which queue the attendant is servicing



The interface is titled "Vision 80/20 Attendant". It includes a top navigation bar with tabs for "Start", "Catalogue", and "Call Center". Below this is a toolbar with icons for "Search", "Extension", "Details", "Diversion", "Message", "Manager", "Manager Pro", "Report", and "More". A "Logged in" status indicator is shown in the top right corner. The main area displays a table of users with columns for "Name", "Organization", "Department", and "Extension". The table lists several users, including "ACD", "H323 Network", "Internal", "mq", "PSTN", "PSTN -", and "SIP Network". A "Main queue" section is visible on the right, showing "Main queue", "Parkering", and "ag1" with associated counts and times. The bottom status bar shows "9 found", "20 May, 16:17", "Cert", "agent 1", and "Op.no 4602".

Name	Organization	Department	Extension
ACD			4697
H323 Network			13300
H323 Network			13400
Internal			4654
mq			4500
PSTN			4179673300
PSTN -			4179673402
SIP Network			3300

Queue	Count	Time
Main queue	0	00:00
Parkering	0	00:00
ag1	0	00:00

8. Verification Steps

This section provides the tests that can be performed to verify correct configuration of Communication Server 1000 and Vision with Session Manager.

8.1. Verify Session Manager

Log in to System Manager. Under the **Elements** section, navigate to **Session Manager** → **System Status** → **SIP Entity Monitoring**. Click the Session Manager instance (**ASM70A** in the example below).

The screenshot shows the Avaya Aura System Manager 7.0 interface. The top navigation bar includes the Avaya logo, the text "Aura® System Manager 7.0", and a "Last Logged on at May 23, 2017 10:09 AM" timestamp. Below the navigation bar, there is a breadcrumb trail: "Home / Elements / Session Manager / System Status / SIP Entity Monitoring". The main content area is titled "SIP Entity Link Monitoring Status Summary" and includes a description: "This page provides a summary of Session Manager SIP entity link monitoring status." Below this, there is a section titled "SIP Entities Status for All Monitoring Session Manager Instances" with a "Run Monitor" button. A table displays the status of three monitored entities. The table has columns for "Session Manager", "Type", "Down", "Partially Up", "Up", "Not Monitored", "Deny", and "Total". The first row, for "ASM70A", is highlighted with a red border. The second row is for "ASM70B" and the third is for "Branch-ASM70".

	Session Manager	Type	Monitored Entities					Total
			Down	Partially Up	Up	Not Monitored	Deny	
<input type="checkbox"/>	ASM70A	Core	15	0	10	1	1	27
<input type="checkbox"/>	ASM70B	Core	0	0	4	0	1	5
<input type="checkbox"/>	Branch-ASM70	BSM	---	---	---	---	---	---

Verify that the state of the Session Manager links to Communication Server 1000 and Vision under the **Conn. Status** and **Link Status** columns is **UP**, like shown on the screen below.

Session Manager Entity Link Connection Status

This page displays detailed connection status for all entity links from a Session Manager.

All Entity Links for Session Manager: ASM70A

Summary View

Status Details for the selected Session Manager:

27 Items | Refresh Filter: Enable

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	ACM-Trunk3-Public	10.33.1.6	5067	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Trio	10.10.98.9	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	Breeze	10.33.1.16	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	VisionHA	10.10.98.8	5060	UDP	FALSE	UP	200 OK	UP
<input type="radio"/>	Presence70	10.33.1.16	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	ACM-Trunk1-Private	10.33.1.6	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Avaya-SBCE-A1	10.33.1.51	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Car2-cores	10.10.97.170	5061	TLS	FALSE	UP	200 OK	UP

Other Session Manager useful verification and troubleshooting tools include:

- **traceSM** – Session Manager command line tool for traffic analysis. Login to the Session Manager command line management interface to run this command.
- **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, from the System Manager Home screen navigate to **Elements → Session Manager → System Tools → Call Routing Test**. Enter the requested data to run the test.

9. Conclusion

These Application Notes describe the configuration steps required for Vision 2020 3.1HA from Enghouse Interactive AB to successfully interoperate with Avaya Communication Server 1000 and Avaya Aura® Session Manager using SIP trunks. Vision passed all compliance testing successfully; please see **Section 2.2** of these Application Notes for results and observations if any.

10. Additional References

This section references the product documentation relevant to these Application Notes. Product documentation for Avaya products may be found at <http://support.avaya.com>.

Avaya:

1. *Communication Server 1000E Installation and Commissioning*, Release 7.6, NN43041-310
2. *Element Manager System Reference – Administration - Avaya Communication Server 1000*, Release 7.6, NN43001-632.
3. *Avaya Communication Server 1000 Co-resident Call Server and Signaling Server Fundamentals* Release 7.6, NN43001-509.
4. *Avaya Communication Server 1000 Unified Communications Management Common Services Fundamentals -*, Release 7.6, NN43001-116.
5. *Avaya Communication Server 1000 - Software Input Output Reference — Administration* Release 7.6, NN43001-611.
6. *Avaya Communication Server 1000 - ISDN Primary Rate Interface Installation and Commissioning*, Release 7.6, NN43001-301.
7. *Implementing Avaya Aura® Session Manager* Document ID 03-603473.
8. *Administering Avaya Aura® Session Manager*, Doc ID 03-603324.
9. *Deploying Avaya Aura® System Manager*, Release 7.0.
10. *Administering Avaya Aura® System Manager for Release 7.0*, Release 7.0.

All information on the product installation and configuration Vision Server can be found at <http://enghouseinteractive.com>

©2017 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.