Avaya Solution & Interoperability Test Lab

Application Notes for Configuring FCS Phoenix Voicemail System Release 2.0 with Avaya Communication Server 1000 Release 7.6 using SIP Trunk - Issue 1.0

Abstract

These Application Notes describe a solution for supporting interoperability between the FCS Phoenix Voicemail System Release 2.0 with Avaya Communication Server 1000 release 7.6 using a SIP trunk. Emphasis of the testing was to verify Voicemail and Auto Wake Up features of FCS Phoenix Voicemail System communicating to the Avaya Communication Server 1000 via the SIP trunk.

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 provide detail configurations for Avaya Communication 1000 (hereafter referred to as CS1000) FCS Phoenix Voicemail System (hereafter referred to as Phoenix) used during the compliance testing. Phoenix is a dynamic voice messaging system used in the hospitality industry and communicates with the CS1000 using a SIP trunk.

Phoenix will be connected to SIP trunks on the CS1000. The CS1000 takes care of the call processing (incoming and outgoing) tasks while the Real-time Protocol (RTP) sessions and Dual-tone multi-frequency (DTMF) transmission/processing are handled within the Phoenix system.

All the applicable voicemail and Auto Wake Up (AWU) features of Phoenix were executed to ensure the interoperability with CS1000.

2. General Test Approach and Test Results

The general test approach was to have Phoenix communicate to CS1000 SIP Signaling Gateway directly using SIP trunk. A Pilot Directory Number (DN) was assigned to Phoenix and CS1000 was configured so that Avaya phones can dial the Pilot DN to reach the Phoenix system over the SIP trunk. Phoenix is configured to handle voicemail and AWU features requested from the Avaya phones.

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

2.1. Interoperability Compliance Testing

The focus of this testing was to verify that the Phoenix server is able to communicate with CS1000 via a SIP trunk. The following areas were tested:

- To leave and retrieve voice messages from Avaya phones.
- To ensure if the Message Waiting Lamp (MWL) is turned on for a new voice message and turned off after all the messages have been retrieved.
- Able to delete voice messages.
- Able to leave or retrieve text messages (simulated, as there is no Hotel Property Management System (PMS) present).
- Able to forward a voice message.
- Able to change message greeting and mailbox password.
- Able to transfer call to operator.
- To ensure all AWU call features are functioning.
- Codec negotiation – G.711 and G.729.

2.2. Test Results

The objectives outlined in **Section 2.1** were verified. Phoenix was registered to CS1000 SIP Signaling Gateway successfully. All executed test cases passed with the following observations,

- The SIP Signaling Gateway (SSG) used for Phoenix cannot provide trunks for any other purpose (private trunks, Carrier trunks, other SIP applications). The dedicated SSG runs on a signaling server and can co-reside with UNIStim Terminal Proxy Server. Engineering recommendations should be consulted to ensure the co-resident services do not exceed the capacity of the signaling server.
- The SSG cannot co-reside on a signaling server with another SSG. If SIP trunks are needed for another purpose, then a second SSG must be provisioned on a separate signaling server.
- End points must support RFC2833 to convey caller key presses or pass through a media gateway which converts key presses to RFC2833 in the RTP stream. Key presses sent as SIP Info messages are not supported. Signaling and Media encryption protocols TLS and sRTP are not supported. CS1000 SIP trunks serving Phoenix must have media encryption disabled.
- CS1000 Automatic Call Distribution (ACD) DNs cannot overflow calls over SIP Trunks to Phoenix.
- Calling Party Name Display (CPND) and Calling Line Identification (CLID) are not updated for Call Transfer because none of the SIP IP Phones update the display upon receiving a REINVITE message. Only the Avaya 1120E and 1140E IP Deskphones update the display for simple calls and Call forward (CFW) calls. Due to CS1000 SIPL/SIP terminal limitations, Phoenix might experience incorrect message sender ID during call transfer scenarios.
- When a text message is left for a guest, the Hotel PMS will send a packet to Phoenix via Unicorn and Phoenix will then issue a command to activate the MWL. Conversely, once the guest has retrieved the text message, the Hotel PMS will send a corresponding packet to Phoenix via Unicorn and Phoenix will then issue a command to deactivate the MWL. But in the absence of the aforementioned interfaces, these scenarios were simulated using the Phoenix Web interface. This is achieved by first turning on the text message flag manually to indicate the presence of a text message. This will automatically trigger the system to activate the MWL. Then when the user calls in to check his messages, the prompt would say there is a written message. Since there is actually no text message deposited, proceed to manually turn off the text message flag from the Web. This will similarly trigger the system to deactivate the MWL.
- While attempting to leave a message for a checked out guest (Unicorn application provides check-in/out indications to Phoenix – not shown), Phoenix provides a message stating that the room is vacant and then transfers the call to a pre-defined operator. While trying to retrieve message for a checked out guest, Phoenix provides a message stating that it is an invalid extension. However, the system does keep checked-out guest messages for 2 days (by default) and guests can enlist the operator's help to retrieve their messages after checking out from the hotel via a special Telephone User Interface (TUI) option.

- When an AWU call is cancelled from a guest room, the record will be removed from the database and reflected on the web module of Phoenix. However, a report can be printed to check the history of AWU transactions, if necessary.
- When an AWU call is snoozed, the next call is made after 10 minutes of the original AWU set call time. This value is not configurable in Phoenix.

2.3. Support

Support for the Phoenix application can be obtained through contacting FCS via:

- Phone: +63 2 857 4000
- Email: FCS.Marketing@planet1world.com

3. Reference Configuration

Figure 1 illustrates the reference configuration used during compliance testing. Phoenix and Unicorn resided on the same server during compliance testing. Phoenix communicates directly with the SIP Signaling Gateway, which is a component of CS1000 using a SIP trunk.

FCS Unicorn is a Property Management System (PMS) that was used during compliance testing for the sole purpose of checking in, checking out and moving of guest rooms and providing this information to both CS1000 and Phoenix.

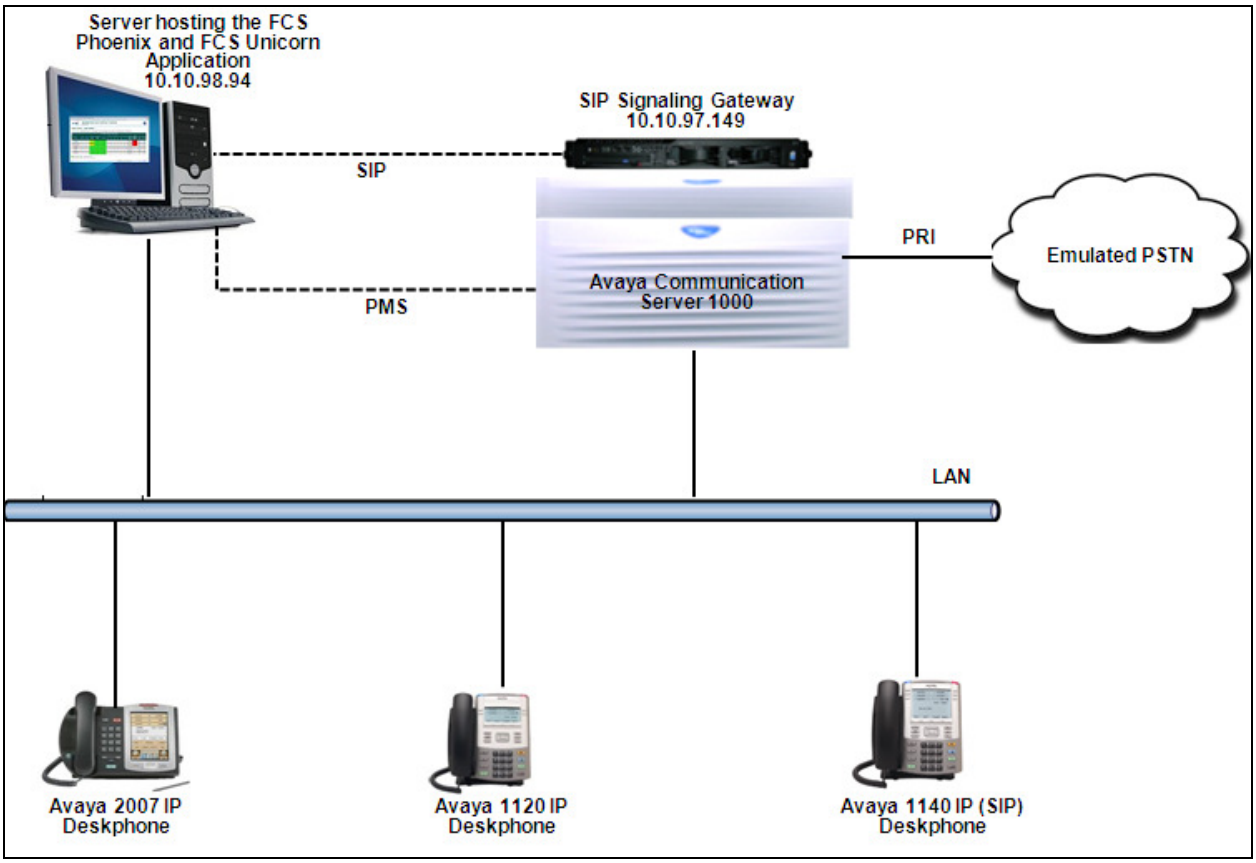


Figure 1: Network Configuration Diagram

4. Equipment and Software Validated

The following equipment and software/firmware were used for the reference configuration:

Equipment/Software	Release/Version
Avaya Communication Server 1000E Call Server SIP Signaling Gateway	7.65 P 7.65 P
Avaya CS1000 IP Phones: 2007 1120	 0621C8L 0624C8L
Avaya CS1000 SIP Phone: 1140	 04.03.12
FCS Phoenix and FCS Unicorn running on a Windows 2008 64 bit Server	2.02/1.2

5. Configure Avaya CS 1000

This section describes the steps to configure the Avaya CS1000 using the CS1000 Element Manager and command line interface (CLI) option for the integration with Phoenix. Any configuration required for CS1000 integration with Unicorn is beyond the scope of this document. For detailed information on how to configure and administer the CS1000, please refer to the **Section 9 [1]**. For detailed information on integration of Unicorn with CS1000, please refer to the **Section 9 [2]**.

The following is the summary of tasks that need to be completed in order to configure CS1000 to integrate with Phoenix:

- Log in to Unified Communications Management (UCM) and Element Manager (EM).
- Define a Listed Directory Number in the Customer Data Block.
- Define a Customer to support Integrated Services Digital Network.
- Configure the SIP Signaling Gateway.
- Create a D-Channel for SIP Signaling Gateway.
- Create a Virtual Trunk Zone.
- Create a SIP Route Data Block (RDB).
- Create SIP Virtual Trunks.
- Create Phoenix Pilot DN.
- Create a User Phone.
- Create an Automatic Call Distribution (ACD) Queue.

5.1. Prerequisite

This document assumes that the CS1000 SIP Signaling Gateway has been:

- Installed with CS 1000 Release 7.65 Linux Base.
- Joined CS 1000 Release 7.65 Security Domain.
- Deployed with SIP Signaling Gateway Application.

The following packages need to be 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 #	Descriptions	Package Type	Applicable market
BGD	99	Background Terminal	Existing package	Global
PMSI	103	Property Management System Interface	Existing package	Global
NMS	175	Network Message Services	Existing package	Global
SIP	406	SIP Gateway and Converged Desktop	New package	Global

Packages available on the CS1000 can be printed in the CLI using overlay 22 as shown in the screen below

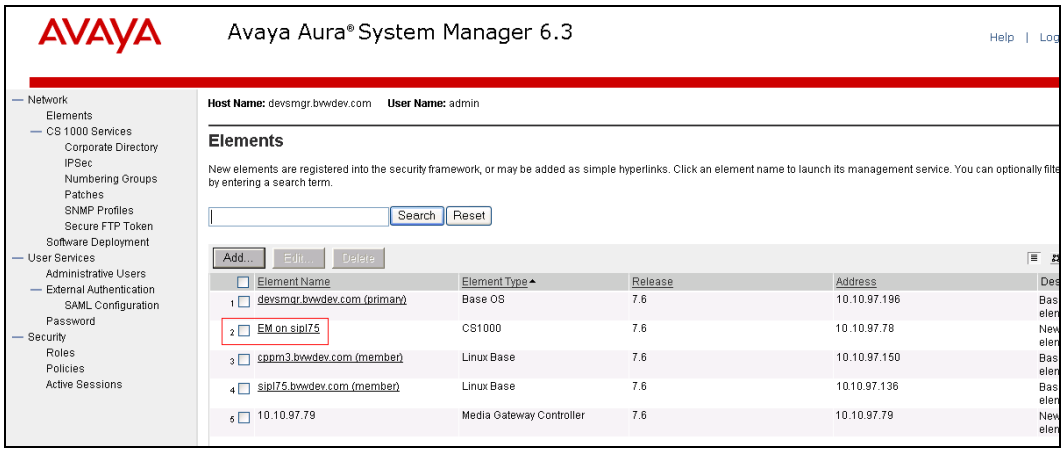
```
>ld 22
PT2000

REQ  prt
TYPE pkg
```

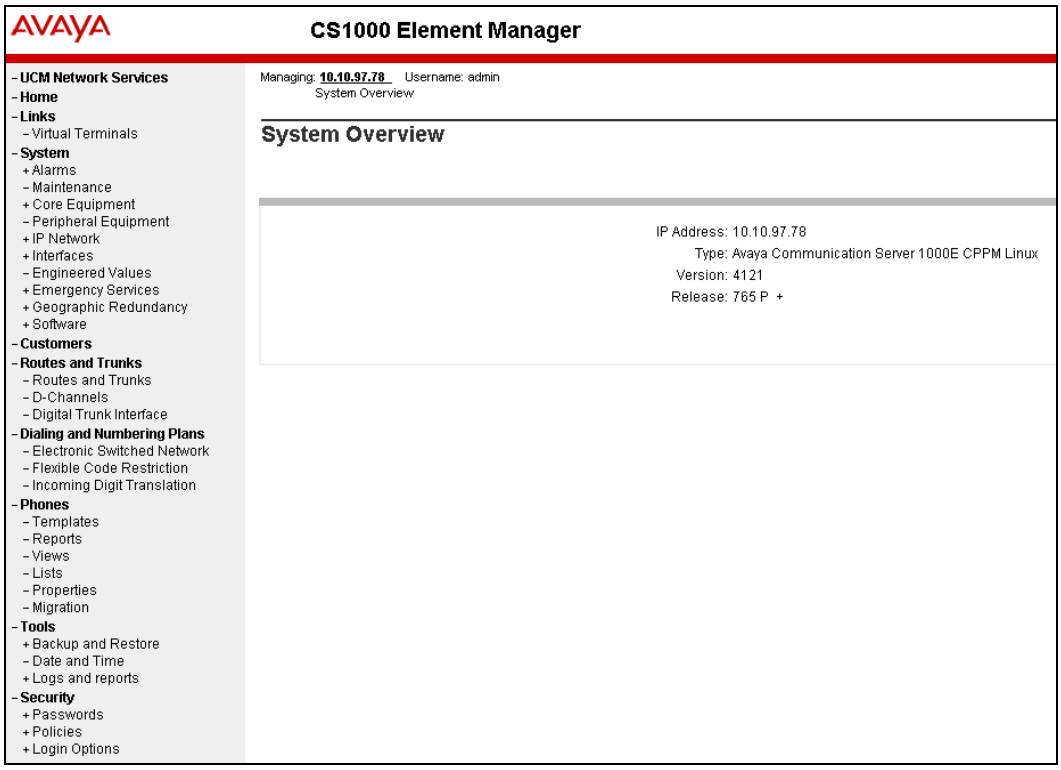
5.2. Log in to Unified Communications Management (UCM) and Element Manager (EM)

Use a web browser to launch the Avaya CS1000 UCM web portal at http://<IP Address or FQDN> where <IP address or FQDN> is the UCM Framework IP address or FQDN for UCM server. Login with the username/password which was defined during the primary security server configuration (not shown). For more information, see **Section 9[2].**

On the **Elements** page of Unified Communications Management, under the **Element Name** column, click the server name to navigate to Element Manager for that server.



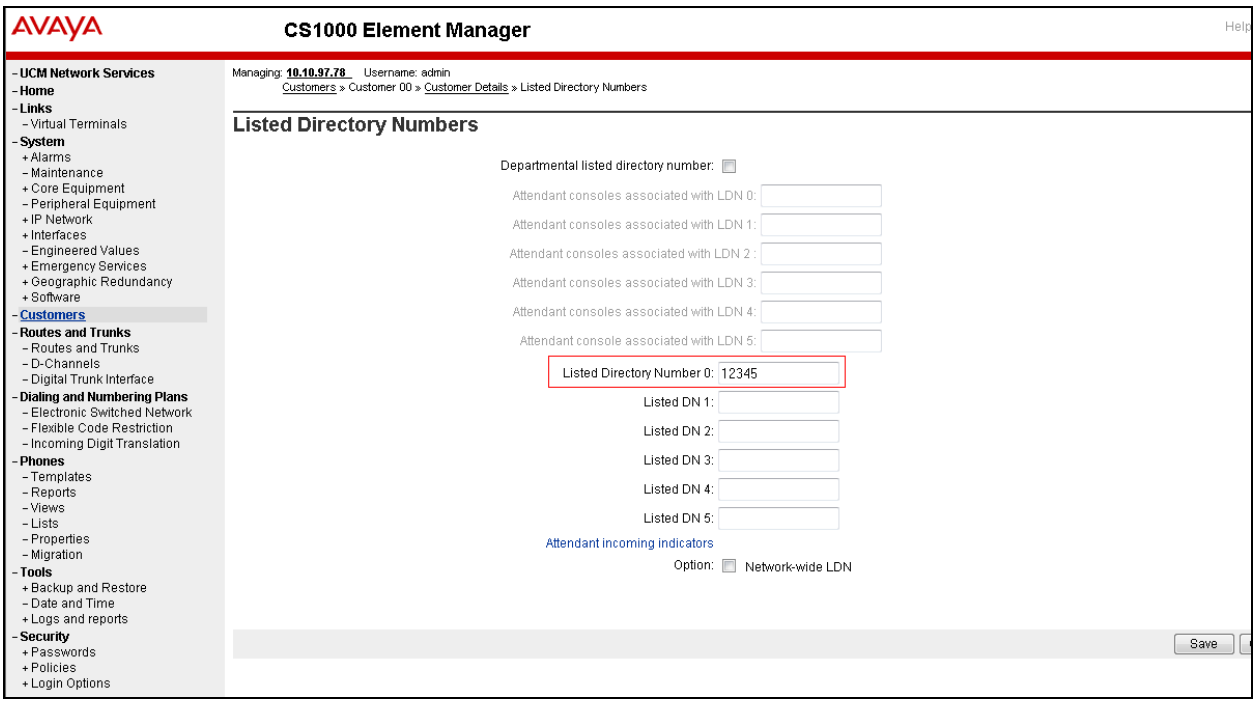
The Avaya CS1000 Element Manager (EM) page appears as shown.



5.3. Defining Listed Directory Number in the Customer Data Block

On the EM page (shown in **Section 5.2**), navigate to **Customers** on the left column menu; select the customer number configured (not shown) and click on **Listed Directory Number** (not shown) from the right column. The **Listed Directory Numbers** screen is seen as shown below. Enter the following,

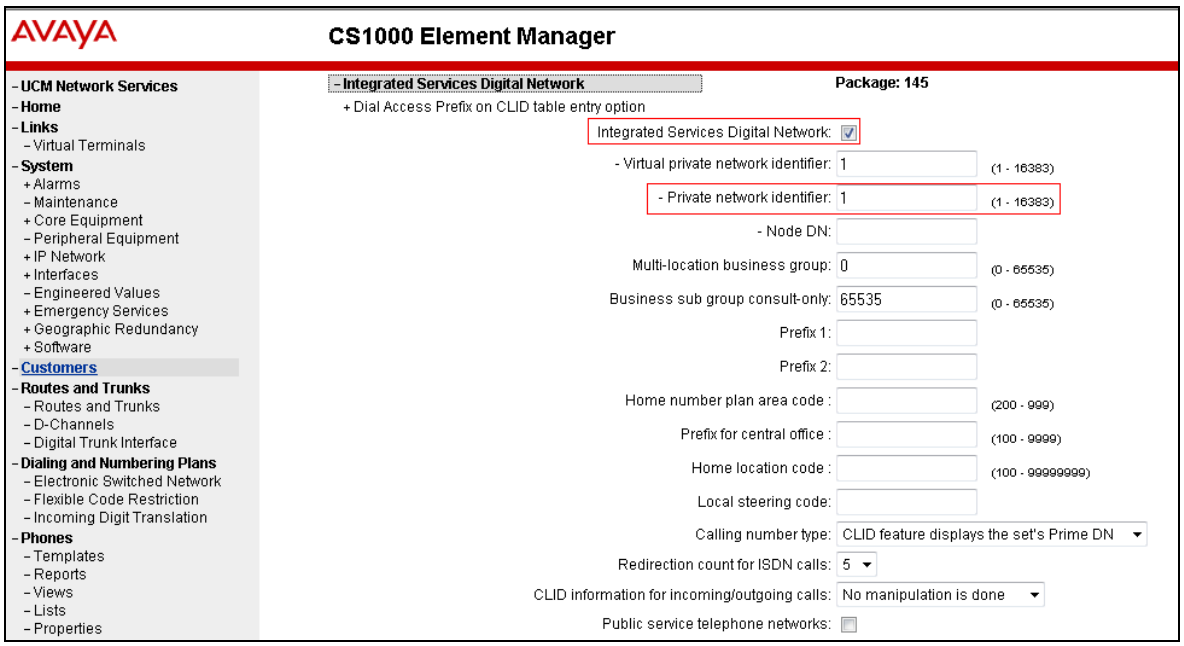
- **Listed Directory Number 0**: 12345; this value was used during compliance testing.
- Retain default values for all other fields.
- Click on **Save**.



5.4. Defining Customer to Support Integrated Services Digital Network

On the EM page (shown in **Section 5.2**), navigate to **Customers** on the left column menu; select the customer number configured (not shown) and click on **Feature Packages** (not shown) from the right column. The **Feature Packages** screen is seen and shown below. Expand the **Integrated Services Digital Network** and enter the following,

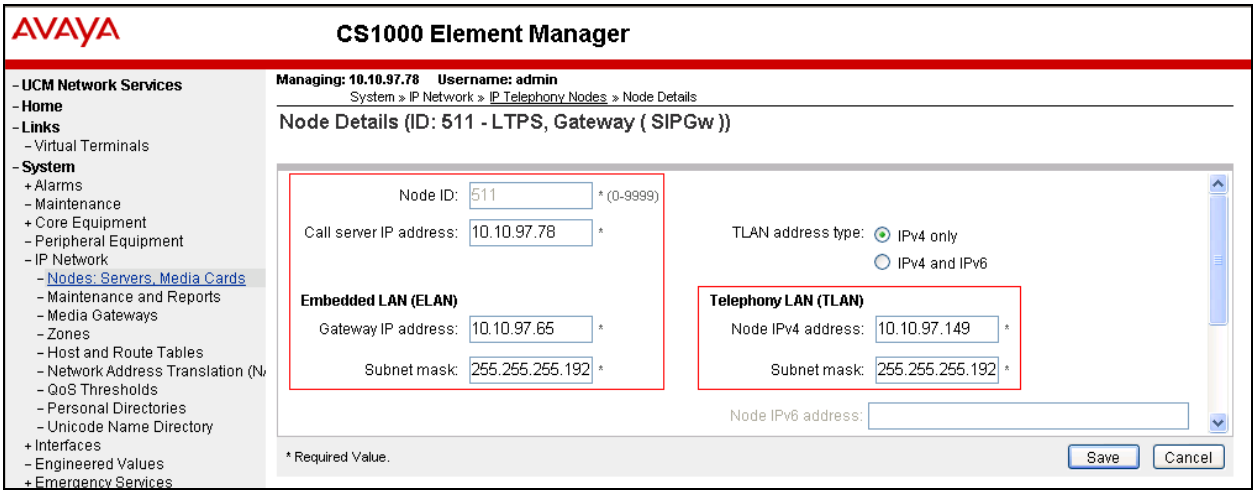
- **Integrated Services Digital Network**: Box is checked.
- **Private network identifier**: 1; this value was used during compliance testing.
- Retain default values for all other fields.
- Click on **Save** (not shown).



5.5. Configuring SIP Signaling Gateway

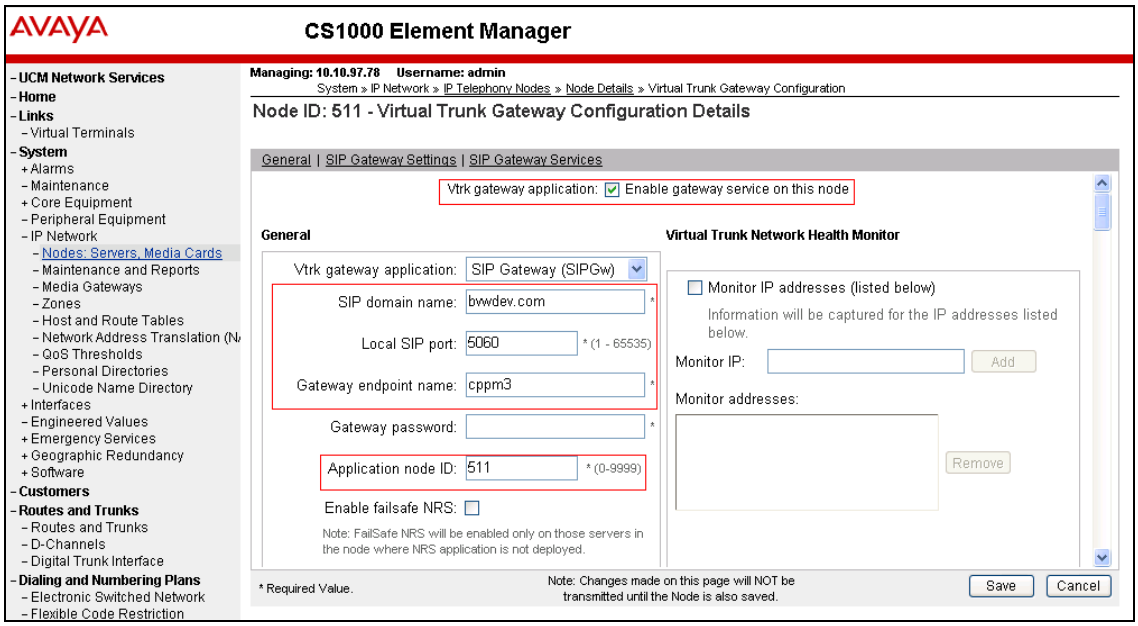
On the EM page (shown in **Section 5.2**), navigate to menu **System → IP Network → Nodes: Servers, Media Cards**. Click the **Add** button (not shown) to add a new SIP Signaling Gateway Node. The screen below shows an already configured node with the following values,

- **Node ID**: 511; this is the node ID of SIP Signaling Gateway used during compliance testing.
- **Call Server IP Address**: 10.10.97.78
- **Node IP Address**: 10.10.97.149; this is the IP address that Phoenix will use to communicate with the CS1000 via the SIP trunk.
- **Subnet Mask**: 255.255.255.192
- **Embedded LAN (ELAN) Gateway IP Address**: 10.10.97.65
- **Embedded LAN (ELAN) Subnet Mask** text box: 255.255.255.192.
- Click on **Save.**



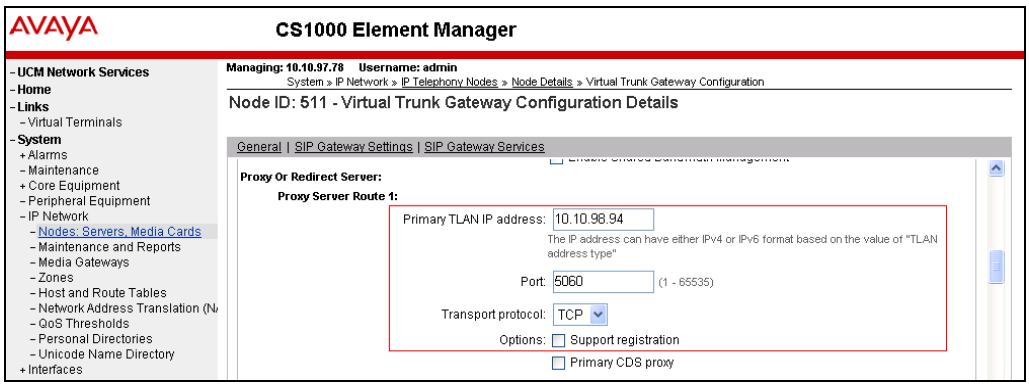
Click on **Gateway (SIPGw)** (now shown) to configure the newly added gateway. The screen below shows the Virtual Trunk Gateway Configuration Details under the **General** section with the following values,

- Check the **Enable gateway service on this node** box.
- **SIP Domain name**: bvwdev.com was used during compliance testing.
- **Local SIP port**: 5060.
- **Gateway endpoint name**: cppm3 was used during compliance testing.
- **Application node ID**: 511; this is the node ID created in **Section 5.5**.
- Retain default values for all other fields.



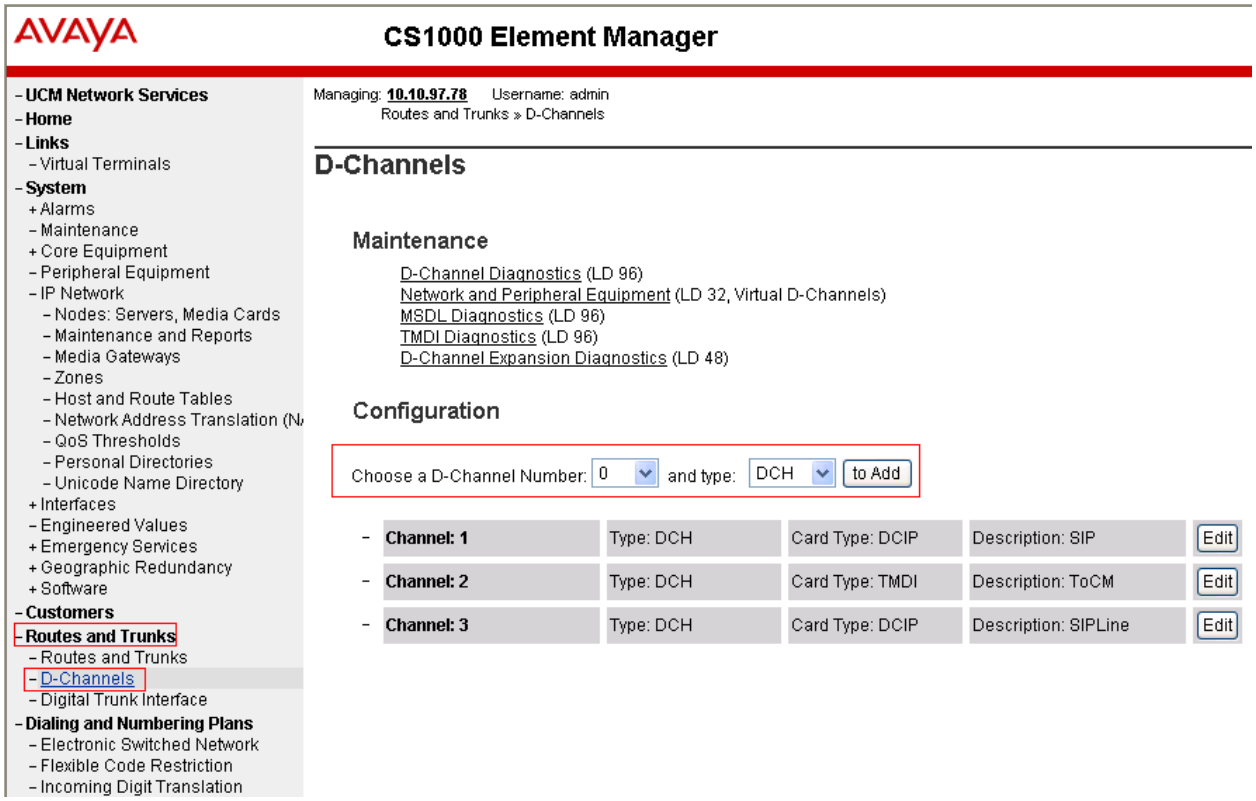
Under the **SIP Gateway Settings** section,

- **Primary TLAN IP address**: 10.10.98.94; this is the IP address of the Phoenix server.
- **Port**: 5060
- **Transport protocol**: TCP; ensure that Phoenix is also configured for the same protocol.
- **Options**: Do not check the **Support registration** box.
- Retain default values for all other fields.
- Click on **Save** (not shown).



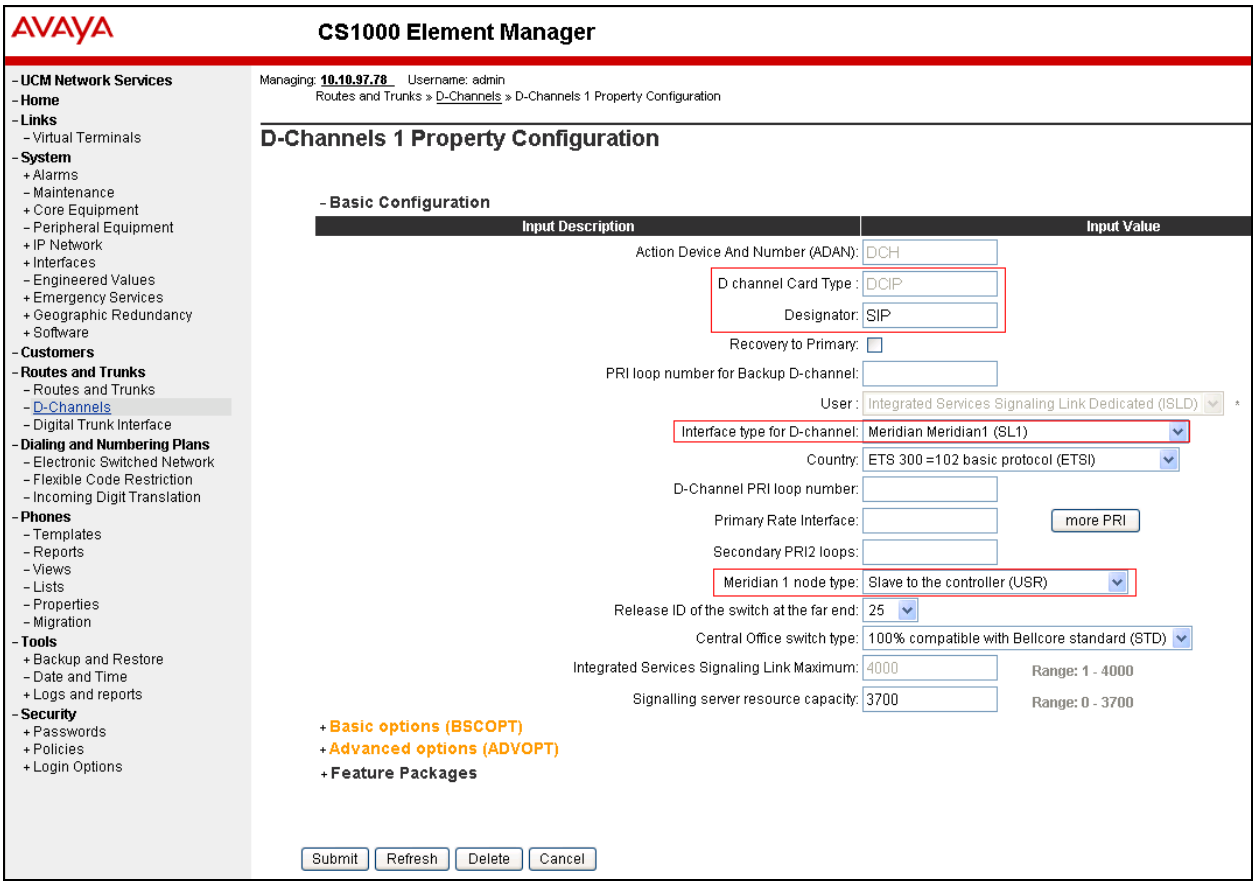
5.6. Create a D-Channel for SIP Signaling Gateway

On the EM page, on the left column menu navigate to **Routes and Trunks → D-Channels**. Under the **Configuration** section as shown below, select an available number in the **Choose a D-Channel Number** drop down menu, and click on the **to Add** button.



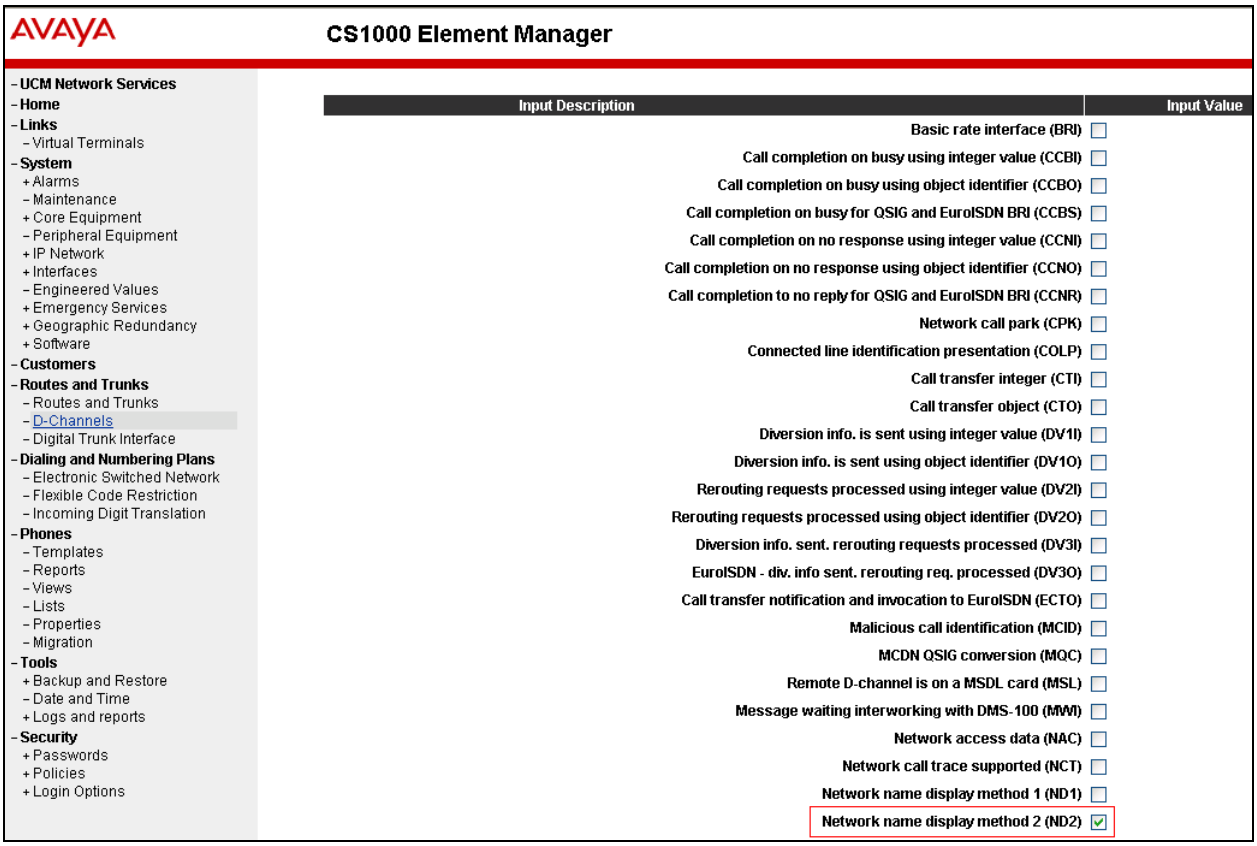
The screen below shows the **D-Channels 1 Property Configuration** page, which was configured during compliance testing. Configure the **Basic Configuration** section as follows,

- **D channel Card Type**: DCIP.
- **Designator:** A suitable description.
- **Interface type for D-channel**: Meridian Meridian1 (SL1).
- **Meridian 1 node type**: Slave to the controller (USR).
- Retain default values for rest of the fields.



Click on the **Basic options (BSCOPT)** link. The **Basic options (BSCOPT)** section expands (not shown). Click on **Edit** to configure **Remote Capabilities (RCAP)** (not shown). The **Remote Capabilities Configuration** page will appear as shown below.

- Select the **Network name display method 2 (ND2)** check box.
- Retain default values for all other fields.
- At the bottom of the **Remote Capabilities Configuration** page, click **Return - Remote Capabilities** (not shown) to return the **D-Channel 1 Property Configuration** page.



Click on the **Submit** button (not shown) of the D-Channel Property Configuration page to save changes.

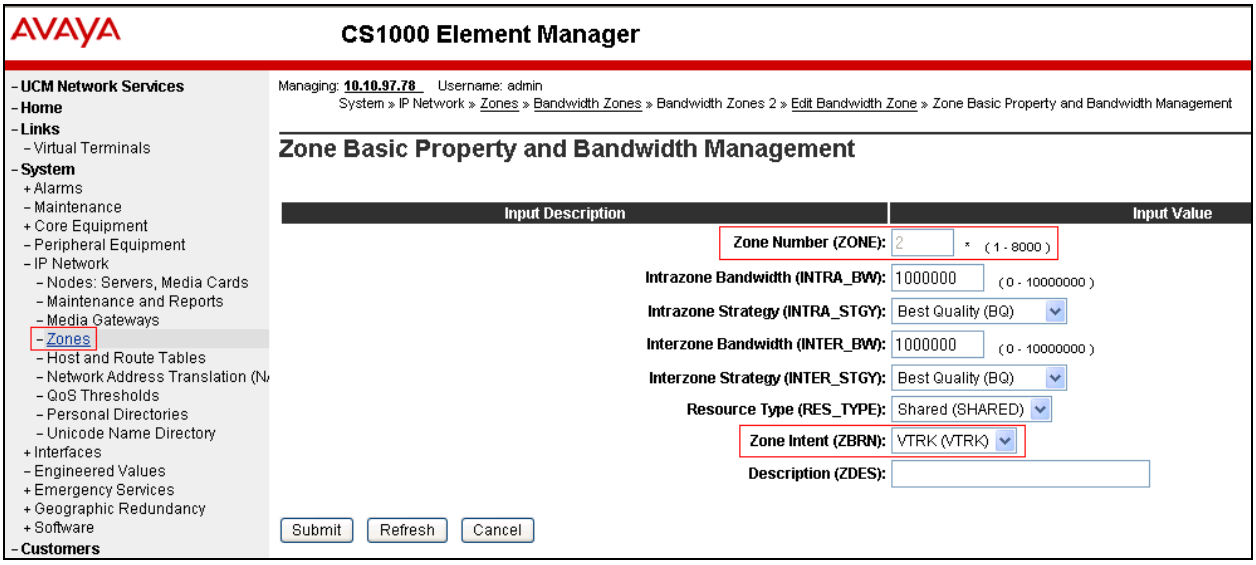
5.7. Create a Virtual Trunk Zone

On the EM page, navigate to menu **System → IP Network → Zones**. The **Zones** page appears on the right (not shown), in this page select **Bandwidth Zones** link.

On the **Bandwidth Zones** page, click on the **Add** button (not shown), the **Zone Basic Property and Bandwidth Management** page appears as shown below. The screen below shows configuration for Zone 2 that was configured during compliance testing.

- **Zone Number (Zone)**: 2
- **Zone Intent (ZBRN)**: VTRK (VTRK).
- Retain default values for all other fields.
- Click on the **Save** button to complete adding the Zone.

Note: Repeat the above step to create another zone for the SIP Line Gateway; however select **MO**, instead of **VTRK** in the **Zone Intent (ZBRN)** field.



5.8. Create a SIP Route Data Block (RDB)

On the EM page, navigate to the menu **Routes and Trunks → Routes and Trunks**; the **Routes and Trunks** page appears (not shown). In this page, click on the **Add route** button next to the customer number that the route will belong to. Route 1 was configured during compliance testing.

The **Customer ID, New Route Configuration** page appears, expand the **Basic Configuration** tab, and enter values below and as shown in next two figures.

- **Route Number (ROUT)**: 1; this is the value used during compliance testing.
- **Designator field for trunk (DES)**: Enter a descriptive name.
- **Trunk type(TKTP)**: TIE
- **Incoming and Outgoing trunk (ICOG)**: IAO
- **Access Code for Trunk group (ACOD)**: 8001; this is the value used during compliance testing.
- **The route is for a virtual trunk route (VTRK)**: Checked.
- **Zone for codec selection and bandwidth management (ZONE*)***: 2; this is the Virtual trunk zone number that was created in **Section 5.7**.
- **Node ID of signaling server of this route (NODE)**: 511; this is the node ID of the SIP Signaling Gateway that was created in **Section 5.5**.
- **Protocol ID for the route (PCID)**: SIP (SIP).
- **Integrated services digital network option (ISDN)**: Checked.
- **Mode of operation (MODE):** Route uses ISDN Signaling Link (ISLD).
- **D channel number (DCH)**: 1; the D-channel number that was created in **Section 5.6**.
- **Interface type for route (IFC)**: Meridian M1 (SL1).
- **Private network identifier (PNI):** 1; created in **Section 5.4**.
- **Network calling name allowed (NCNA)**: Checked.
- **Network call redirection (NCRD)**: Checked
- **Channel type (CHTP)**: B-channel (BCH).
- **Call type for outgoing direct dialed TIE route (CTYP)**: CDP.
- **Insert ESN access code (INAC)**: Checked.
- **Calling Number dialing plan (CNDP)**: CDP.

Leave default values for The **Basic Route Options, Network Options, General Options,** and **Advanced Configurations** sections.
Click **Submit** to complete adding the route and save configuration.

AVAYA **CS1000 Element Manager**

- 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 (N
    - 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

Managing: 10.10.97.78 Username: admin
Routes and Trunks » Routes and Trunks » Customer 0, Route 1 Property Configuration

Customer 0, Route 1 Property Configuration

- Basic Configuration

Route data block (RDB) (TYPE) :	RDB	
Customer number (CUST) :	00	
Route number (ROUT) :	1	
Designator field for trunk (DES) :	SIP	
Trunk type (TKTP) :	TIE	
Incoming and outgoing trunk (ICOG) :	Incoming and Outgoing (IAO)	
Access code for the trunk route (ACOD) :	8001	*
Trunk type M911P (M911P) :	☐	
The route is for a virtual trunk route (VTRK) :	☑	
- Zone for codec selection and bandwidth management (ZONE) :	00002	(0 - 8000)
- Node ID of signaling server of this route (NODE) :	511	(0 - 9999)
- Protocol ID for the route (PCID) :	SIP (SIP)	
- 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) :	Route uses ISDN Signaling Link (ISLD)	
- D channel number (DCH) :	1	(0 - 254)
- Interface type for route (IFC) :	Meridian M1 (SL1)	
- Private network identifier (PNI) :	00001	(0 - 32700)
- Network calling name allowed (NCNA) :	☑	
- Network call redirection (NCRD) :	☑	
- - Trunk route optimization (TRO) :	☐	
- Recognition of DTI2 ABCD FALT signal for ISL (FALT) :	☐	

- + 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

- Channel type (CHTY) :	B-channel (BCH)	
- Call type for outgoing direct dialed TIE route (CTYP) :	Coordinated Dialing Plan (CDP)	
- 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) :	National number (NPA)	
- Mobile extension timer (MBXT) :	0	(0 - 8000 milliseconds)
Calling number dialing plan (CNDP) :	Coordinated dialing plan (CDP)	

- + Basic Route Options
- + Network Options
- + General Options
- + Advanced Configurations

Submit Refresh Delete Cancel

5.9. Create SIP Virtual Trunks

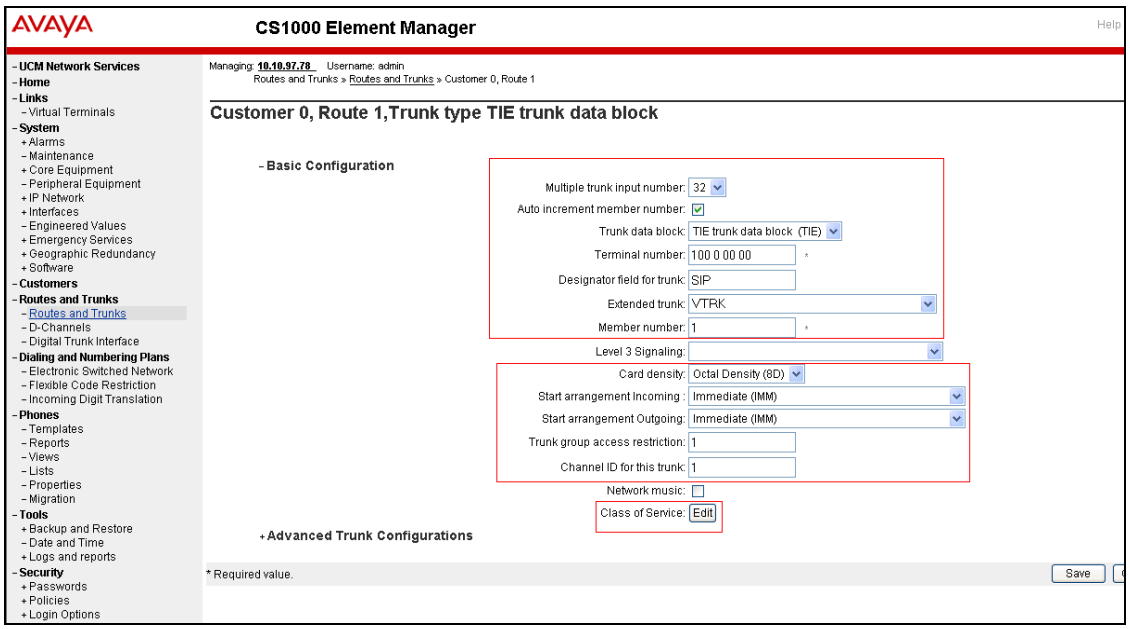
On the EM page, navigate to **Routes and Trunks → Routes and Trunks** and select the **Add trunk** button beside to the route that was created in **Section 5.8** above to create new trunks.

The **Customer 0, Route 1, and Trunk type TIE trunk data block** page appears as shown below, enter values for fields as shown below:

- **Multiple trunk input number (MTINPUT)**: 32; create 32 trunks.
- **Auto increment member number**: Checked.
- **Trunk data block:** TIE trunk data block (TIE).
- **Terminal Number (TN)**: Enter an available range. 100 0 00 00 was used during compliance testing.
- **Designator field for trunk**: Enter a descriptive name.
- **Extended trunk**: VTRK.
- **Member number**: 1; this is ID of trunk, just enter the first ID for first trunk; next ID will be automatically created and incremented.
- **Start arrangement Incoming**: Immediate (IMM).
- **Start arrangement Outgoing**: Immediate (IMM).
- **Trunk Group Access Restriction**: 1.
- **Channel ID for this trunk**: 1; this ID should be the same with the ID of Member Number.

Click on the **Edit** button under **Class of Service** and assign following class of services (not shown):

- **Media security**: Media Security Never (MSNV).
- **Restriction level**: Unrestricted.
- Retain default values for all other fields and click on the **Return Class of Service** button to return to the **Trunk type TIE trunk data block** page**.**
- Click **Save** to complete adding virtual trunks for SIP Signaling Gateway.

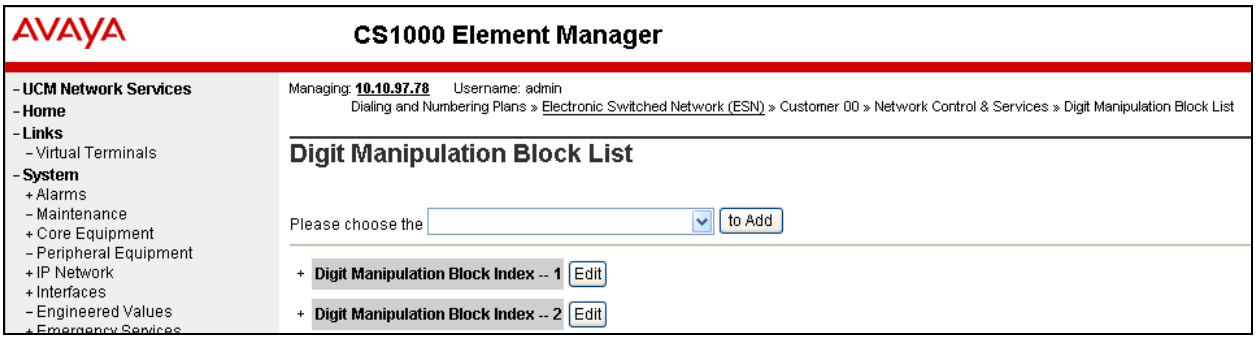


5.10. Create Phoenix Pilot Directory Number

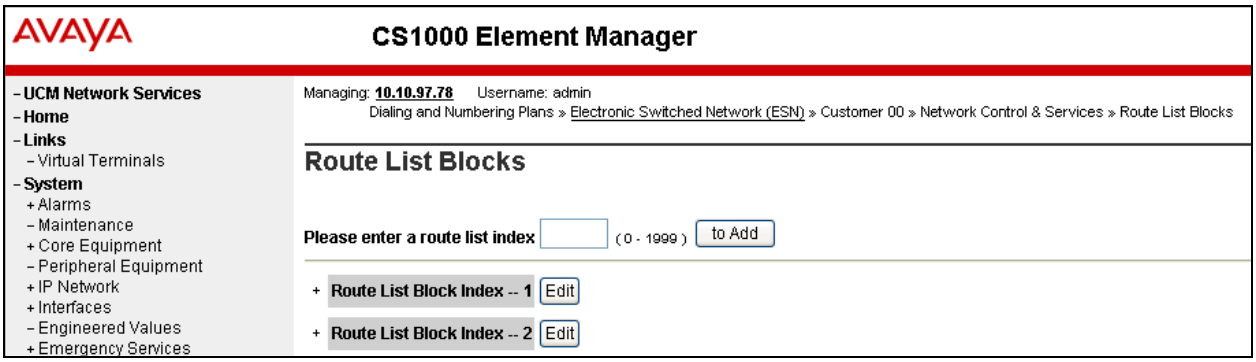
This is the primary number where all subscribers' calls should be forwarded to in Busy/No Answer situations. This number will also be the Night Call Forward (NCFW) destination for all Automatic Call Distribution (ACD) queues created to access Phoenix services.

From the EM navigator pane, navigate to **Dialing and Numbering Plans → Electronic Switched Network** (not shown). Click on **Digit Manipulation Block (DGT)** that is seen under **Network Control & Services** section (not shown).

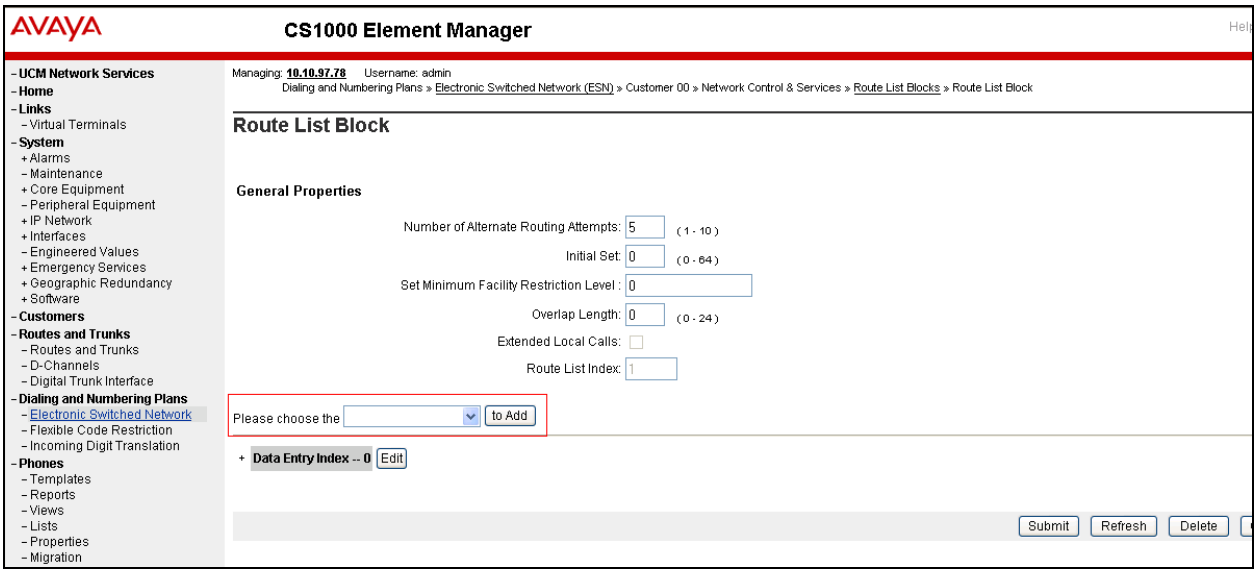
The screen below shows the Digit Manipulation Block Index that administrators can add. However during compliance testing **Digit Manipulation Block Index** of **0** was used which is already configured in CS1000 system by default.



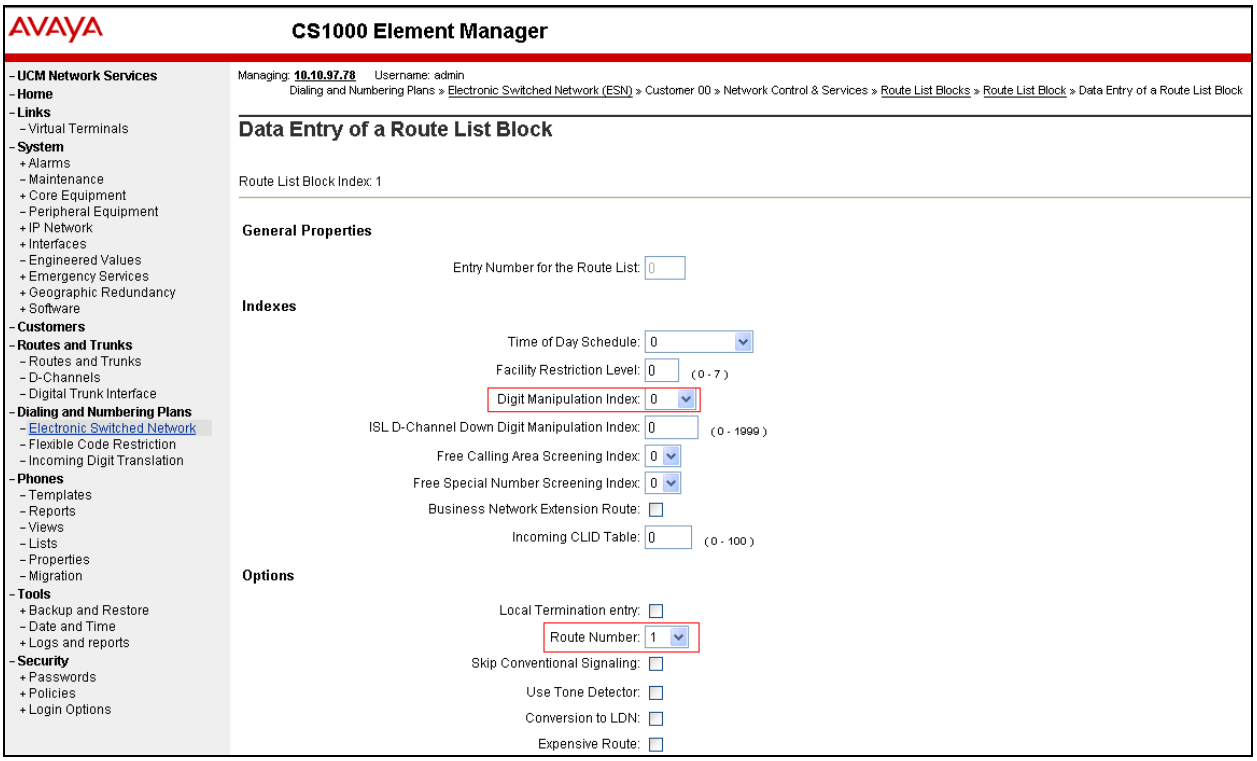
From the EM navigator pane, navigate to **Dialing and Numbering Plans → Electronic Switched Network** (not shown). Click on **Route List Block (RLB)** that is seen under **Network Control & Services** section (not shown). Start adding a **route list index** as shown below. During compliance testing list index **1** was added. Click on **to Add** to continue.



Click on **Edit** for **Data Entry Index 0** as shown below. This Data Entry Index value of 0 is already added in the CS1000 system by default.

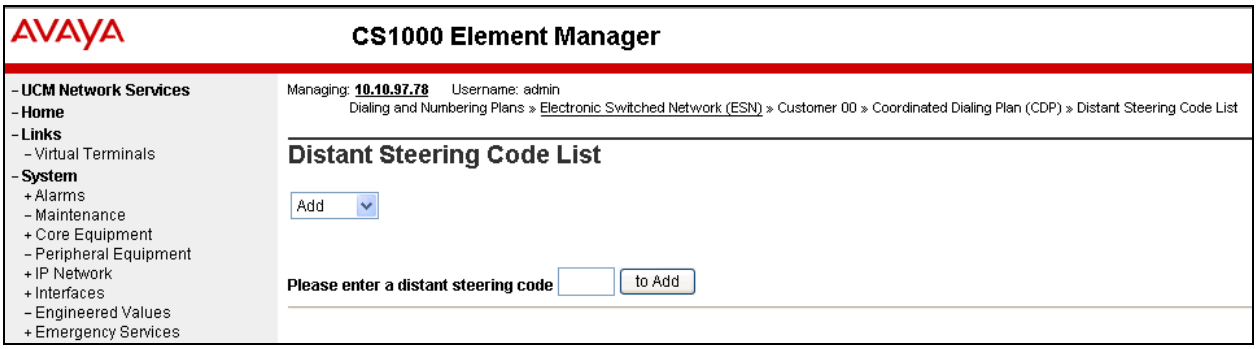


The screen below show the values configured for the index block used during compliance testing. **Route Number** of **1** and **Digit Manipulation Index** of **0** were selected as per the configuration explained above. Click the **Submit** button (not shown) to complete the configuration.



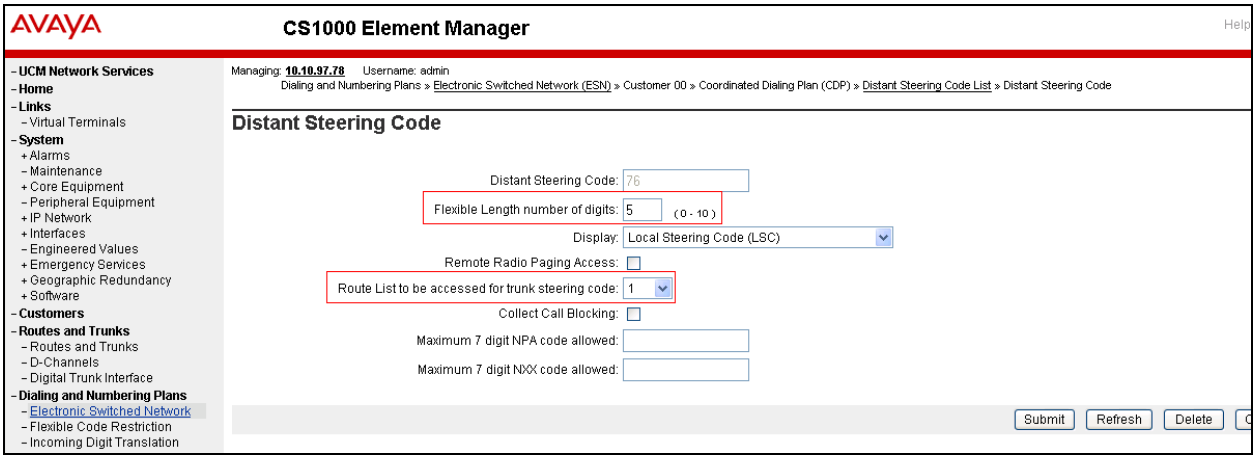
From the EM navigator pane, navigate to **Dialing and Numbering Plans → Electronic Switched Network** (not shown). Click on **Distant Steering Code (DSC)** that is seen under **Coordinated Dialing Plan (CDP)** section (not shown).

From the drop down menu select **Add** and enter a distant steering code to add as shown in below. During compliance testing a code of **76** was added since the Pilot DN assigned to the Phoenix server was 76000. Click on **to Add** to continue.



Enter the values as shown in the screen below.

- **Flexible Length number of digits**: 5; since the Pilot DN is 76000
- **Route List to be accessed for trunk steering code**: 1; configured earlier in this section.
- Retain default values for all other fields.
- Click on **Submit**.



5.11. Create a User Phone

To create a user phone on the Call Server, log in as administrator using the command line interface (CLI) and issue the overlay (LD) **11/20** as shown below.

The screen below shows a print out of the already configured guest phone. The bold fields must be properly inputted as they are configured on the Call Server, for other fields hit enter to leave it at default values. Similar users are to be created for hotel guests, administrators, operator, etc.

```
TYPE TNB
TN 96 0 1 6 → Terminal number on which the set is configured.
DATE
PAGE
DES

DES  2050PC → Description of the phone.
TN   096 0 01 06  VIRTUAL
TYPE 2050PC → Phone type.
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00001    → Zone configured on.
CUR_ZONE 00001
MRT
ERL
ECL  0
FDN  76000  → Forward DN to Phoenix service number.
TGAR 1
LDN  NO
NCOS 7      → Network Class of Service. Enter a value relevant to the user.
SGRP 0
..
..
CAC_MFC 0
CLS  CTD FBA WTA LPR MTD FNA HTA TDD HFA CRPD
     MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
     POD SLKD CCSD SWD LND CNDA
     CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBD
     ICDD CDMD LLCN MCTD CLBD AUTU
     GPUD DPUD DNDA CFXD ARHD CLTD ASCD
     CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
     UDI RCC HBTD AHD IPND  DDGA NAMA MIND PRSD NRWD NRCD NROD
     DRDD EXR0
     USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
     FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD
     KEM3 MSNV FRA  PKCH MUTA MWTD DVLD CROD ELCD VMSA
CPND_LANG ENG
RCO  0
HUNT 76000  → Hunt DN to Phoenix service number.
..
..
```

```
MLNG ENG
DNDR 0
KEY  00 SCR 54426 0     MARP  → Extension number for the phone.
        CPND
          CPND_LANG ROMAN
            NAME Guest 54426  → CLID information for the phone.
            XPLN 23
            DISPLAY_FMT FIRST,LAST
     01
     02
     03
     04
..
..
```

5.12. Create an Automatic Call Distribution (ACD) Queue

ACD Queues are used to access voicemail services – one ACD DN per service.
To create an ACD queue and have it call forwarded to the Phoenix service number, log in as administrator using the command line interface (CLI) and issue the overlay (LD) **23** as shown below.

The screen below shows a print out of the already configured ACD queue. The bold fields must be properly inputted as they are configured on the Call Server, for other fields hit enter to leave it at default values. Multiple queues can be created similarly for various hospitality services.

```
TYPE ACD    → Defining that the type is ACD.
CUST 0      → Customer number.
ACDN 77001  → ACD DN.
MWC  NO
DSAC NO
MAXP 1
SDNB NO
BSCW NO
ISAP NO
AACQ NO
RGAI NO
ACAA NO
FRRT
SRRT
NRRT
FROA NO
CALP POS
ICDD NO
NCFW 76000  → Night Call Forward to Phoenix directory number.
FNCF NO
CWTT NONE
..
..
```

6. Configure Phoenix

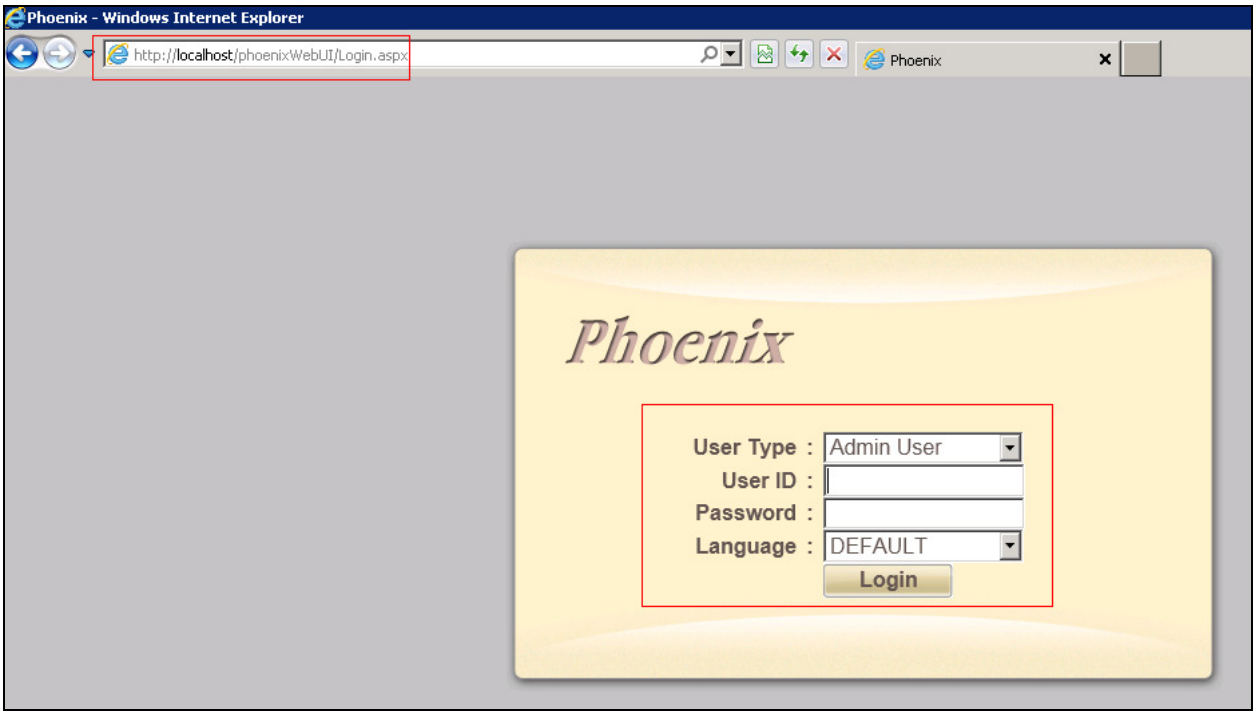
This section details the steps required to configure Phoenix Voicemail system to interoperate with Avaya Communication Server 1000. These Application Notes assume that the Phoenix server has been installed and configured by the FCS personnel and also integrated with the Unicorn PMS server. This section will only detail the steps required to configure Phoenix so it can communicate to CS1000 via a SIP trunk. For more details on installing and administering Phoenix, refer to **Section 9**.

6.1. Login to Phoenix Web Interface

Open a web browser and access the web interface of the Phoenix server by typing the following in the URL: http://localhost/phoenixWebUI/Login.aspx

During compliance testing the web interface was accessed from the same server where Phoenix was installed and therefore localhost was used as server name.

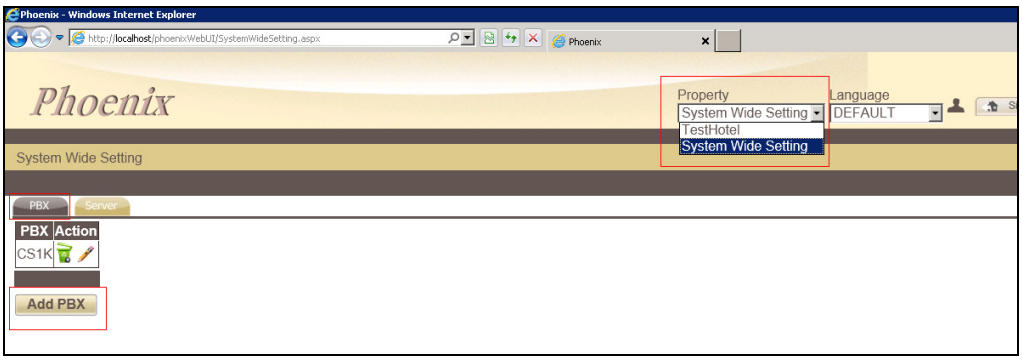
The screen below shows the Phoenix login screen. Enter the appropriate **User ID** and **Password** and click on **Login**.



6.2. Adding a PBX

This section explains the steps to add a PBX to the Phoenix server.

From the web interface, select **System Wide Setting** from the **Property** drop down menu as shown in the screen below. Click on the **PBX** tab and click on **Add PBX** button to add a new PBX.

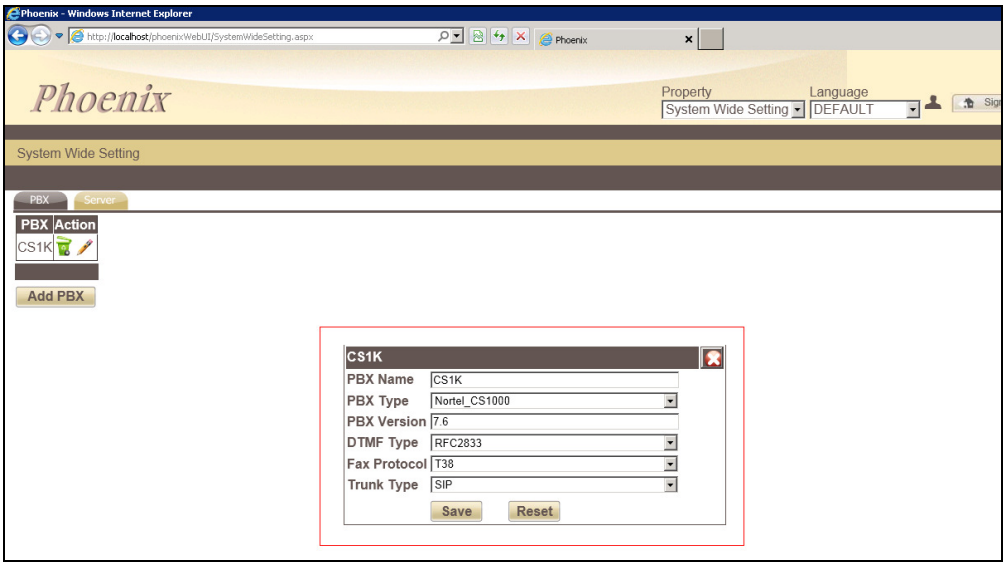


The screen below shows the information for the added PBX during compliance testing. Enter the following fields:

- **PBX Name**: Enter a descriptive name.
- **PBX Type**: Select a corresponding model from the drop down list.
- **PBX Version**: This is an optional field. Enter the version of the PBX.
- **DTMF Type**: Select the correct DTMF from the drop down list. In this case RFC2833
- **Fax Protocol**: If applicable, select the correct protocol from the drop-down list. Field was left at default value during compliance testing.
- **Trunk Type**: SIP, since the integration is using SIP trunk.

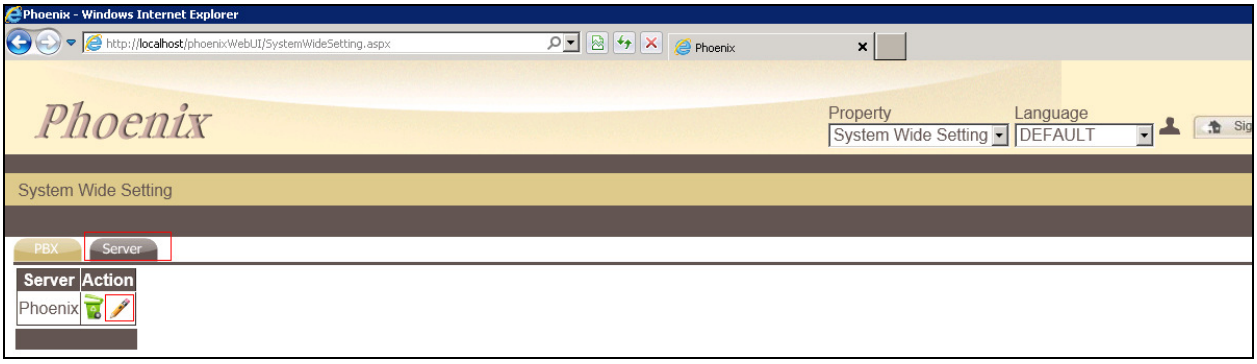
Click on **Save** to complete the adding of a PBX.

A confirmation message will then be shown indicating that the PBX has been added successfully (not shown).



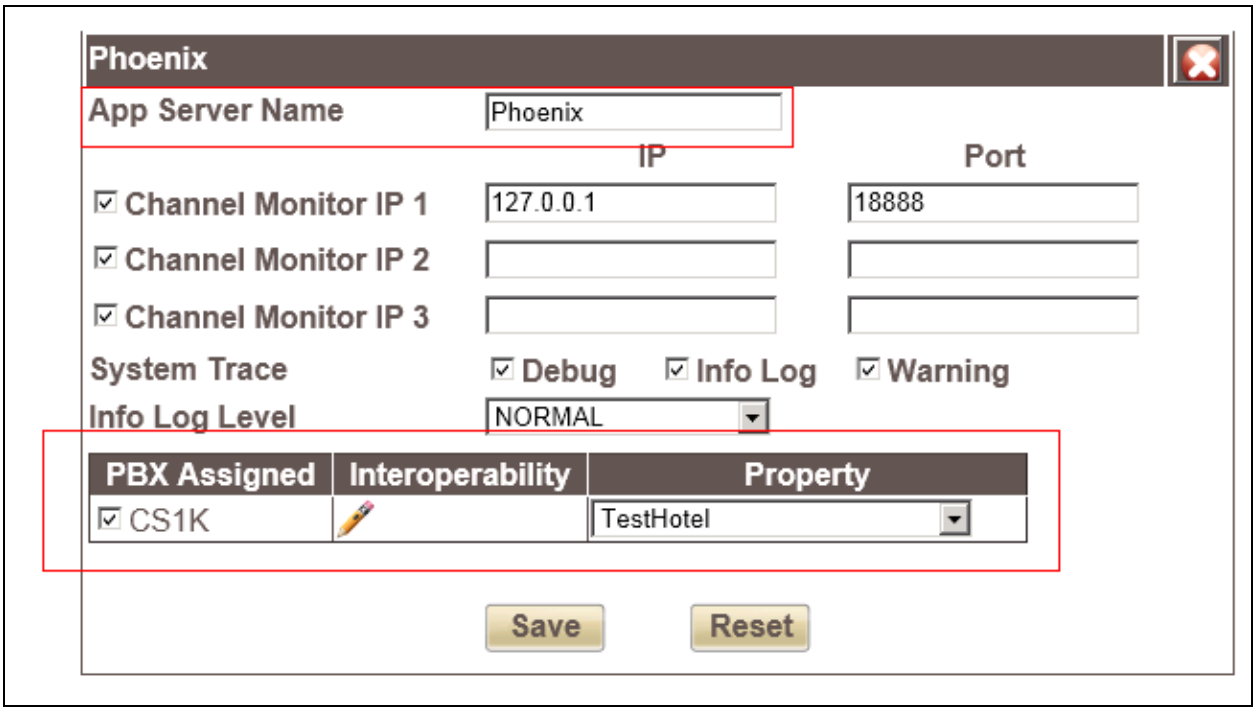
6.3. Adding a Server

From the web interface, select **System Wide Setting** from the **Property** drop down menu as shown in the screen below. Click on the **Server** tab; the number of servers that can be added is solely controlled by the activated license. Click the 'pencil' icon next to the server to edit as shown in the figure below.



Enter the following fields for the Server:

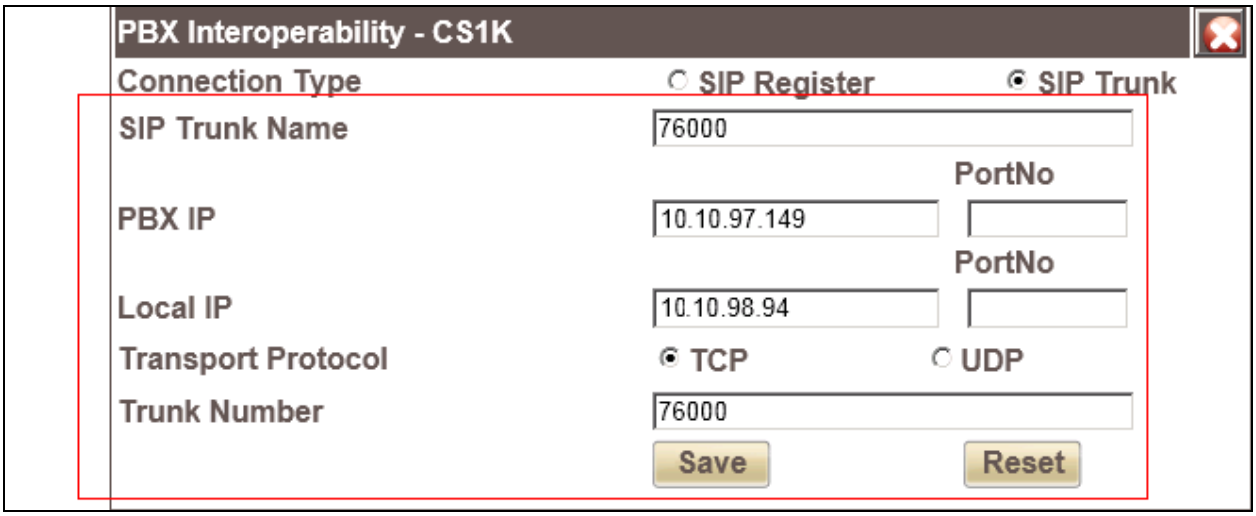
- **App Server Name**: Enter a descriptive name.
- Select the appropriate PBX (if there's more than one) from the **PBX Assigned** column and property from the **Property** column. Click on the "pencil" icon to start configuring the PBX SIP trunk properties.
- Retain default values for all other fields.



The screen below shows the **Connection Type** field. Select **SIP Trunk** radio button.

The screen below shows the SIP Trunk properties that were configured during compliance testing.

- **SIP Trunk Name**: Enter a descriptive name.
- **PBX IP**: This is the IP address of the SIP Signaling Gateway of the PBX.
- **Local IP**: This is the IP address of the Phoenix server.
- **PortNo fields**: Not required
- **Transport Protocol**: This value should match the value configured on the SIP Signaling Gateway of the PBX as explained in **Section 5.5**.
- **Trunk Number**: This is the Phoenix Pilot DN.
- Click on **Save**.



Click on **Save** (not shown) at the main server screen to complete the configuration. A confirmation message will then be shown informing that the server changes have been saved (not shown).

7. Verification Steps

This section includes some steps that can be followed to verify the configuration.

- Able to call into Phoenix via the service number provided from CS1000.
- Able to leave voice message for guests/admin.
- Guest/Admin phone MWI lamp is on when new message is available.
- Guest/Admin able to listen to voice message.
- Guest/Admin phone MWI lamp is off when no more new message.
- Web interface of Phoenix able to track guest/admin voice messages.
- Guest/Admin able to record own greeting message.
- Guest/Admin able to change mail box password.
- Guest can set Auto Wakeup Call (AWU) from phone.
- Web interface of Phoenix able to track and monitor AWU set by guest.
- AWU is triggered according to the date/time set by guest.
- Able to transfer call to operator.
- Able to terminate the call from either the phone or application.
- Able to call in to the various call flows based on specific numbers tied to entry points (numbers programmed as ACD queue in the PBX to call forward to Phoenix Pilot DN).

8. Conclusion

These Application Notes illustrate the procedures necessary for configuring the FCS Phoenix Voicemail system to interoperate with the Avaya Communication Server 1000. All feature functionality test cases described in **Section 2.1** passed. Please review the observations noted in **Section 2.2**.

9. Additional References

Product documentation for the Avaya CS 1000 products may be found at:
https://support.avaya.com/css/Products/

Product documentation for FCS Phoenix Voicemail system can be obtained by contacting FCS support mentioned in **Section 2.3**.

[1] Avaya CS1000 Documents:
Avaya Communication Server 1000E Installation and Commissioning.
Avaya Communication Server 1000 Element Manager System Reference – Administration.
Avaya Communication Server 1000 Co-resident Call Server and Signaling Server Fundamentals.
Avaya Communication Server 1000 Unified Communications Management Common Services Fundamentals.
Avaya Communication Server 1000 ISDN Primary Rate Interface Installation and Commissioning.

[2] Application Notes for Unicorn Version 1.1 with Avaya Communication Server 1000 Release 7.5 - Issue 1.1 - June 2013 can be found at the following URL:
https://devconnect.avaya.com/public/dyn/d_dyn.jsp?fn=831

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.