



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for configuring IPC Unigy with Avaya Communication Server 1000 7.5 and Avaya Aura® Session Manager 6.1 using SIP Trunks – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for IPC Unigy to interoperate with Avaya Communication Server 1000 7.5 using SIP trunks.

IPC Unigy is a trading communication solution. In the compliance testing, IPC Unigy used SIP trunks to Avaya Communication Server 1000 via Avaya Aura® Session Manager, for turret users on IPC to reach users on Avaya Communication Server 1000 and on the PSTN.

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 configuration steps required for IPC Unigy to interoperate with Avaya Communication Server 1000 7.5 using SIP trunks.

IPC Unigy (hereafter referred to as Unigy) is a trading communication solution. In the compliance testing, IPC Unigy used SIP trunks to Avaya Communication Server 1000 7.5 (hereafter referred to as CS1000) via Avaya Aura® Session Manager, for turret users on IPC Unigy to reach users on Avaya Communication Server 1000 and on the PSTN.

This solution covered CS1000 IP (UNISTim), Digital and/or PSTN users. SIP endpoints are currently not supported due to an issue with blind transfer.

## 2. General Test Approach and Test Results

The feature test cases were performed manually. Calls were manually established among Unigy turret users with CS1000 IP (UNISTim), Digital and/or PSTN users. Call controls were performed from various users to verify the call scenarios.

The serviceability test cases were performed manually by disconnecting and reconnecting the network connection to Unigy.

### 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing included basic calls, basic display, G.711, G.729, DTMF, hold/reconnect, call forwarding unconditional/ring-no-answer/busy, blind/attended transfer, and attended conference.

The serviceability testing focused on verifying the ability of Unigy to recover from adverse conditions, such as disconnecting/reconnecting the network connection to Unigy.

### 2.2. Test Results

The objectives outlined in **Section 2.1** were verified and met. All tests were executed and passed with the following observations.

- Blind transfer of a call from Unigy to an Avaya SIP endpoint fails. For example, Set A (Avaya) calls Set B (Unigy). Set B does a blind transfer to Set C (Avaya SIP endpoint). When Set C answers the call, Set A gets disconnected. Issue is not seen if Set C is a non SIP endpoint.
- Set A (Unigy) calls Set B (Avaya) with name and number restricted. Set B does an unattended transfer to Set C (Unigy). Set C sees the Calling Line Identification (CLID) of Set B rather than Set A. This is because Avaya CS1000 design does not support CLID update while doing a transfer to a third party system.
- Set A (Avaya) calls Set B (Unigy) which is setup so that all calls forward to Set C (Avaya) which is setup so that all calls forward to a voice mail system. Set A is leaving a

voice mail to Set B mailbox and not to the mailbox for Set C. This is the CS1000 design intent since original call from Set A was made to Set B.

- Set A (Avaya) calls Set B (Unigy) which has calls forward if busy to Set C's (Avaya) voice mail. Set A hears the voice mail greeting right away with no ringing indication.
- Set A (Unigy) calls Set B (Unigy) which has calls forward if busy to an invalid extension on Avaya CS1000. As per design call fails however the line on Set A freezes and has to be force cleared. Unigy design is investigating this issue.
- Set A (Unigy) calls Set B (Avaya) which has calls forward on no answer to Set C (Unigy) which has all calls forward to a PSTN number. Even though Unigy documentation claims to use the UDP protocol only, during diversions like the example mentioned above, it changes the protocol to TCP. Therefore, for calls to be successful, Avaya Aura® Session Manager needs to be configured for both UDP and TCP protocols when integrating with the Unigy system. Details of the configuration are explained in **Section 6**.
- Set A (Unigy) calls Set B (Unigy). Set B does a blind transfer to Set C (Unigy) which has calls forward on no answer to a voice mail system. The call between Set A and the voice mail system is active however there is no speech path and Set A cannot hear any mail box greetings or commands. Issue has been raised with Avaya CS1000 design.
- Uncheck PRACK in Unigy system so that Unigy users can access the Avaya Call Pilot voice mail system that is hosted on the Avaya CS1000 system.
- G.722 codec is not supported and therefore should not be configured on Unigy.
- A packet rate of 20ms is to be used with G.711 and G.729 codecs.

## 2.3. Support

Technical support on IPC Unigy can be obtained through the following:

- **Phone:** (800) NEEDIPC, (203) 339-7800
- **Email:** [systems.support@ipc.com](mailto:systems.support@ipc.com)

### 3. Reference Configuration

As shown in **Figure 1** below, the Unigy configuration consists of the Media Manager, Converged Communication Manager, and Turrets. The Media Manager and Converged Communication Manager are typically deployed on separate servers. In the compliance testing, the same server hosted the Media Manager and Converged Communication Manager.

Unigy, CS1000 and Avaya Aura® Session Manager are connected to each other through the lab network. SIP trunks are used from Unigy to Avaya CS1000 via the Avaya Aura® Session Manager, to reach users on CS1000 and on the PSTN.

A five digit Uniform Dial Plan (UDP) was used to facilitate dialing between Unigy and CS1000. During compliance testing, extension ranges 58xxx were associated with CS1000 users and 35xxx were associated with the Unigy turret users. Avaya Call Pilot DN is 58888 and the PSTN number is 9613965570.

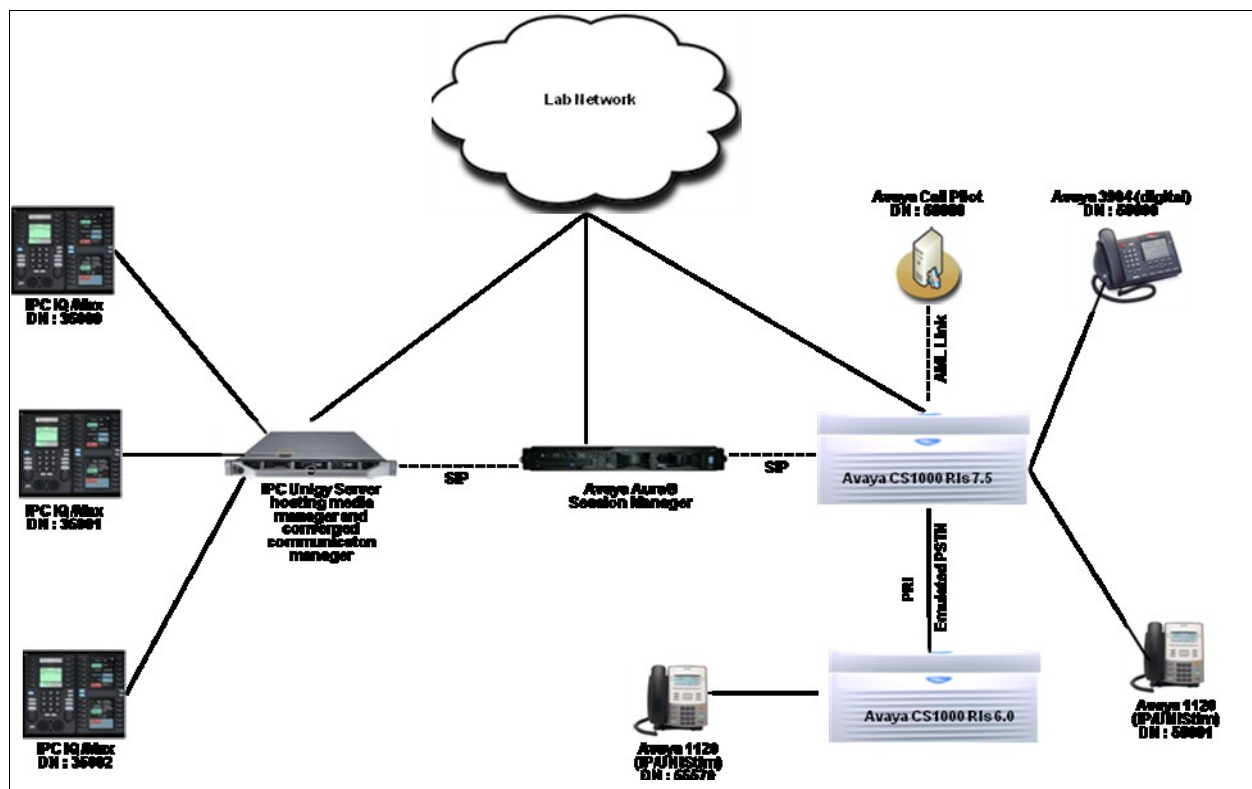


Figure 1: Compliance Test Setup in the lab

## 4. Equipment and Software Validated

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

Equipment	Software
Avaya Communication Server 1000	7.50.17
Avaya Communication Server 1000 (for emulated PSTN)	6.0
Avaya Call Pilot (600r)	5.00.41
Avaya Aura® Session Manager	6.1 SP2
Avaya Aura® System Manager	6.1 SP2
Avaya Digital user (3904)	NA
Avaya IP (UNISTim) user (1120)	0624C8A
IPC Unigy <ul style="list-style-type: none"><li>• Media Manager</li><li>• Converged Communication Manager</li><li>• Turrets (IQ/Max)</li></ul>	01.00.00.04.0003 01.00.00.04.0003 01.00.00.04.0003

## 5. Configure Avaya CS1000

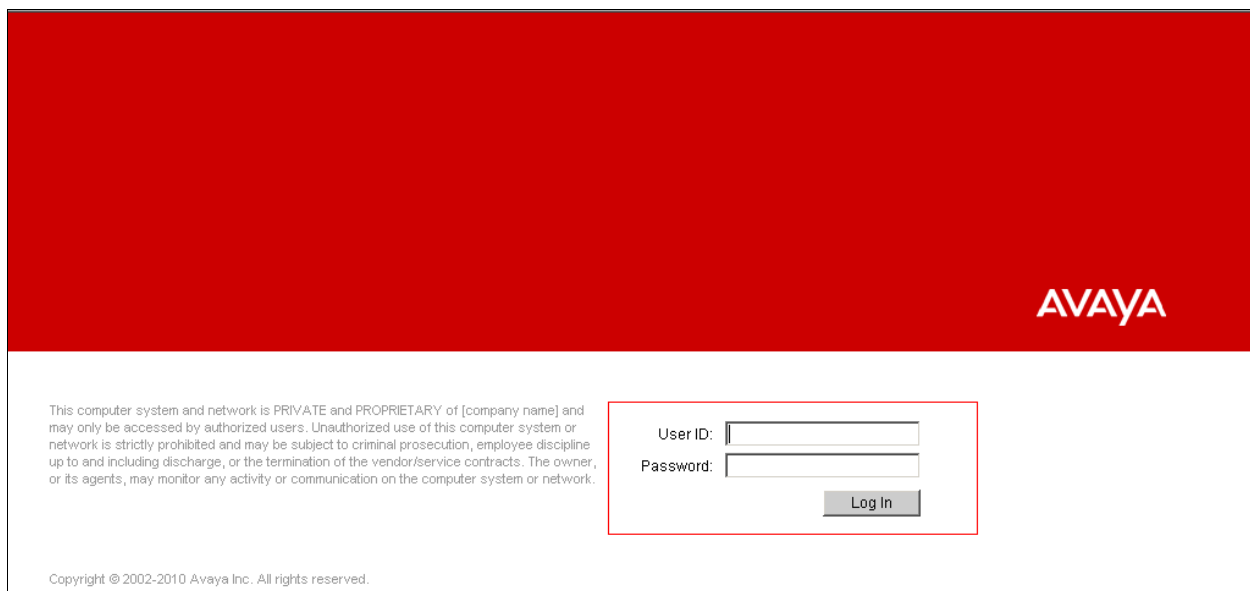
This section provides the procedures for configuring the Avaya CS1000 system. The procedures include the following areas:

- Logging into the Element Manager via Unified Communications Manager.
- Configuring the SIP Signaling Gateway.
- Configuring a D-Channel.
- Configuring Routes and Trunks.
- Configuring Digit Manipulation Block.
- Configuring Route List Block.
- Configuring Distant Steering Code.

Assumption is made here that the CS1000 users are already created and also the PRI Trunk between CS1000 7.5 and CS1000 6.0 is configured for emulated PSTN setup during compliance testing. For configuration details of the CS1000 refer to **Section 10[1]**.

### 5.1. Logging into Element Manager via Unified Communication Manager

To login to the Unified Communications Manager (UCM) open an IE browser and type in the IP address of the UCM in the URL (not shown). **Figure 2** below shows the login screen of the UCM. Enter the **User ID** and **Password** credentials and click on **Log In** to continue.

The image shows the login screen of the Unified Communications Manager (UCM). It features a red header bar with the "AVAYA" logo in white on the right. Below the header, on the left, is a disclaimer: "This computer system and network is PRIVATE and PROPRIETARY of [company name] and may only be accessed by authorized users. Unauthorized use of this computer system or network is strictly prohibited and may be subject to criminal prosecution, employee discipline up to and including discharge, or the termination of the vendor/service contracts. The owner, or its agents, may monitor any activity or communication on the computer system or network." In the center, there is a login form with two input fields: "User ID:" and "Password:". Below these fields is a "Log In" button. The entire login form area is enclosed in a red rectangular border. At the bottom left of the page, there is a copyright notice: "Copyright © 2002-2010 Avaya Inc. All rights reserved."

**Figure 2: UCM Login Screen**

From the UCM main screen as shown in **Figure 3** below, click on the Element **EM on cppm1**. This is the element which is configured to access the Element Manager (EM) for the CS1000 Call Server.

# Avaya Unified Communications Management

Host Name: ucm1.bwwdev.com    Software Version: 02.20-SNAPSHOT(0000)

## Elements

New elements are registered into the security framework, or may be added as sim management service. You can optionally filter the list by entering a search term.

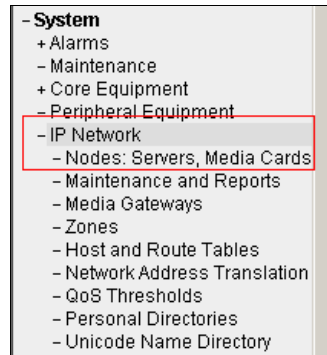
<input type="checkbox"/>	Element Name	Element Type ▲	Release
1 <input type="checkbox"/>	EM on cppm1	CS1000	7.5
2 <input type="checkbox"/>	cppm1.bwwdev.com (member)	Linux Base	7.5

**Figure 3: UCM Main Screen**

## 5.2. Configuring the SIP Signaling Gateway

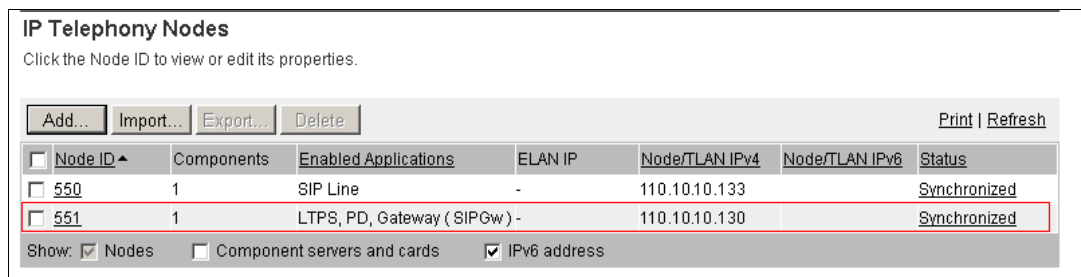
This section describes the configuration required on the SIP Signaling Gateway present on the CS1000 so that CS1000 can communicate with the Avaya Aura® Session Manager via SIP Trunks. Assumption is made here that the IP Telephony node is already added.

To access the Node in the EM left navigator screen, navigate to **IP Network > Nodes: Servers, Media Cards** as shown in **Figure 4** below.



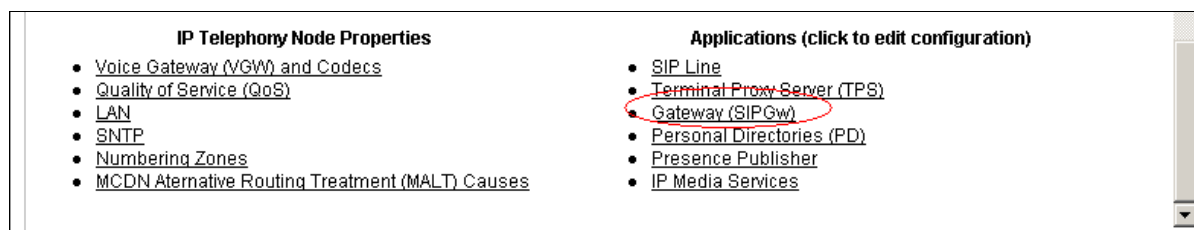
**Figure 4: EM Screen showing navigation tree to Nodes**

During compliance testing Node **551** was already created. Click on this Node as shown in **Figure 5** below.



**Figure 5: Accessing the Node**

Open the SIP Signaling Gateway configuration by clicking on **Gateway (SIPGw)** as shown in **Figure 6** below.



**Figure 6: Accessing the SIP Signaling Gateway**



In the **General** tab, select the values as shown in **Figure 7** below. A **SIP domain name** of **sip.ipc.com** was chosen since this is the domain name that will be configured on the Avaya Aura® Session Manager. Similarly, **cppm1** was configured as the **Gateway endpoint name**.

Node ID: 551 - 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: sip.ipc.com \*  
Local SIP port: 5060 \* (1 - 65535)  
Gateway endpoint name: cppm1 \*  
Gateway password: \*  
Application node ID: 551 \* (0-9999)  
Enable failsafe NRS: ☐

**Virtual Trunk Network Health Monitor**

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

**Figure 7: SIPGw General tab Configuration**

Under the **Proxy or Redirect Server** section, enter the IP address of the Avaya Aura® Session Manager and select **UDP** as the Transport protocol as shown in **Figure 8** below. Leave the remaining values at their default settings. During compliance testing **110.10.10.198** was the IP address of the Avaya Aura® Session Manager.

Node ID: 551 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

**Proxy Or Redirect Server:**

**Proxy Server Route 1:**

Primary TLAN IP address: 110.10.10.198  
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"  
Port: 5060 (1 - 65535)  
Transport protocol: UDP  
Options: ☐ Support registration  
☐ Primary CDS proxy

**Figure 8: Proxy or Redirect Server Configuration**

In the **SIP URI Map** section, enter the values as shown in **Figure 9** below. These values need to be matched if integration is to be successful between Unigy and CS1000, since Unigy is only able to understand the values below in its SIP messaging properties.

**Node ID: 551 - Virtual Trunk Gateway Configuration Details**

General | SIP Gateway Settings | SIP Gateway Services

**SIP URI Map:**

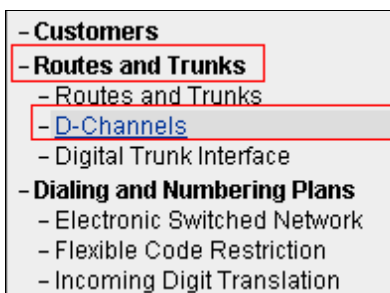
Public E.164 domain names	Private domain names
National: <input type="text"/>	UDP: <input type="text" value="udp"/>
Subscriber: <input type="text"/>	CDP: <input type="text"/>
Special number: <input type="text"/>	Special number: <input type="text" value="PrivateSpecial"/>
Unknown: <input type="text"/>	Vacant number: <input type="text" value="PrivateUnknown"/>
	Unknown: <input type="text"/>

**Figure 9: SIP URI Map Configuration**

Save and transmit these Node properties to complete the SIPGw configuration (not shown).

### 5.3. Configuring D-Channel

This section explains the configuration of a D-Channel for SIP Trunking. From the EM navigation screen, navigate to **Routes and Trunks > D-Channels** as shown in **Figure 10** below.



**Figure 10: EM Screen showing navigation tree to D-Channels**

Choose a D-Channel number to add as shown in **Figure 11** below. During compliance testing D-Channel number **10** was selected. Click on **to Add** to continue.

## D-Channels

### Maintenance

[D-Channel Diagnostics \(LD 96\)](#)  
[Network and Peripheral Equipment \(LD 32, Virtual D-Channels\)](#)  
[MSDL Diagnostics \(LD 96\)](#)  
[TMDI Diagnostics \(LD 96\)](#)  
[D-Channel Expansion Diagnostics \(LD 48\)](#)

### Configuration

Choose a D-Channel Number: 10 and type: DCH to Add

**Figure 11: Adding D-Channel**

Configure the **Basic Configuration** values for the D-Channel as shown in **Figure 12** below.

### - Basic Configuration

Input Description	Input Value
Action Device And Number (ADAN):	DCH
D channel Card Type :	DCIP
Designator:	SIP
Recovery to Primary:	<input type="checkbox"/>
PRI loop number for Backup D-channel:	
User :	Integrated Services Signaling Link Dedicated (ISLD) *
Interface type for D-channel:	Meridian Meridian1 (SL1)
Country:	ETS 300 =102 basic protocol (ETSI)
D-Channel PRI loop number:	
Primary Rate Interface:	<input type="text"/> <span>more PRI</span>
Secondary PRI2 loops:	<input type="text"/>
Meridian 1 node type:	Slave to the controller (USR)
Release ID of the switch at the far end:	25
Central Office switch type:	100% compatible with Bellcore standard (STD)
Integrated Services Signaling Link Maximum:	4000 <span>Range: 1 - 4000</span>
Signalling server resource capacity:	3700 <span>Range: 0 - 3700</span>

**Figure 12: D-Channel Basic Configuration**

To edit the **Remote Capabilities** of the D-Channel, click on the **Edit** button as shown in **Figure 13** below.

Signalling server resource capacity: 3700 Range: 0 - 3700

**- Basic options (BSCOPT)**

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

- PINX customer number: [dropdown]

- Progress signal: [dropdown]

- Calling Line Identification : [dropdown]

- Output request Buffers: 32 [dropdown]

- D-channel transmission Rate: 56 kb/s when LCMT is AMI (56k) [dropdown]

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

- Remote Capabilities: **Edit**

**Figure 13: Editing Remote Capabilities Screen**

Select the boxes for the desired Remote Capabilities as shown in **Figures 14** below. Click on **Return - Remote Capabilities** button to return back to the main screen to complete the D-Channel configuration.

Remote D-channel is on a MSDL card (MSL) ☐

**Message waiting interworking with DMS-100 (MM)** ☒

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) ☐

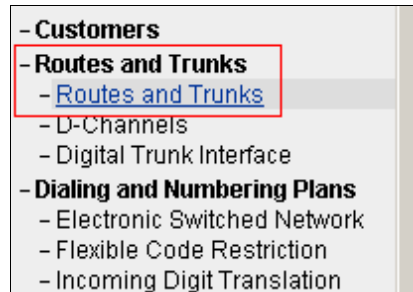
User to user signalling (UUI) ☐

**Return - Remote Capabilities** Cancel

**Figure 14: Remote Capabilities Values**

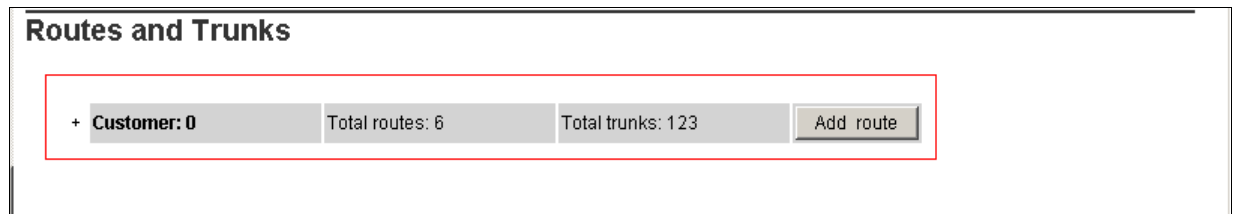
## 5.4. Configuring Routes and Trunks

This section explains the configuration of the SIP routes and trunks which will be used by CS1000 and Unigy to communicate between them. To add a new route, navigate to **Routes and Trunks > Routes and Trunks** from the EM left hand navigator window as shown in **Figure 15** below.



**Figure 15: EM Screen showing navigation tree to Routes and Trunks**

From the Routes and Trunks screen click on the **Add route** button to start configuring a new route as shown in **Figure 16** below.



**Figure 16: Adding a new Route**

During compliance testing **Route number 10** was added. Select the values from the drop down menu and configure the values as shown in **Figures 17a, 17b and 17c** below.

**- Basic Configuration**

Route data block (RDB) (TYPE):	RDB
Customer number (CUST):	00
Route number (ROUT):	10
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):	1111 *
Trunk type M911P (M911P):	<input type="checkbox"/>
The route is for a virtual trunk route (VTRK):	<input checked="" type="checkbox"/>
- Zone for codec selection and bandwidth management (ZONE):	00254 (0 - 8000)
- Node ID of signaling server of this route (NODE):	551 (0 - 9999)
- Protocol ID for the route (PCID):	SIP (SIP)
- Print correlation ID in CDR for the route (CRID):	<input checked="" type="checkbox"/>
Integrated services digital network option (ISDN):	<input checked="" type="checkbox"/>
- Mode of operation (MODE):	Route uses ISDN Signaling Link (ISLD)
- D channel number (DCH):	10 (0 - 254)
- Interface type for route (IFC):	Meridian M1 (SL1)
- Private network identifier (PNI):	00001 (0 - 32700)
- Network calling name allowed (NCNA):	<input checked="" type="checkbox"/>

**Figure 17a: Route Basic Configuration values**

Integrated services digital network option (ISDN): ☒

- Mode of operation (MODE):	Route uses ISDN Signaling Link (ISLD)
- D channel number (DCH):	10 (0 - 254)
- Interface type for route (IFC):	Meridian M1 (SL1)
- Private network identifier (PNI):	00001 (0 - 32700)
- Network calling name allowed (NCNA):	<input checked="" type="checkbox"/>
- Network call redirection (NCRD):	<input checked="" type="checkbox"/>
- Trunk route optimization (TRO):	<input type="checkbox"/>
- Recognition of DT12 ABCD FALT signal for ISL (FALT):	<input type="checkbox"/>
- Channel type (CHTY):	B-channel (BCH)
- Call type for outgoing direct dialed TIE route (CTYP):	Unknown Call type (UKWN)
- Insert ESN access code (INAC):	<input checked="" type="checkbox"/>
- Integrated service access route (ISAR):	<input type="checkbox"/>
- Display of access prefix on CLID (DAPC):	<input type="checkbox"/>
- Mobile extension route (MBXR):	<input type="checkbox"/>
- Mobile extension outgoing type (MBXOT):	National number (NPA)
- Mobile extension timer (MBXT):	0 (0 - 8000 milliseconds)
Calling number dialing plan (CNDP):	Unknown (UKWN)

**+ Basic Route Options**

**Figure 17b: Route Network Options values**

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) : ☐

**Figure 17c: Route Network Options values**

Configure the trunk values as shown in **Figure 18** below. During compliance testing the **Terminal number** used was **100 1 00 00** since it is a virtual trunk. Click on the **Edit** button to configure the required **Class of Service** for the trunks.

**Customer 0, Route 10, Trunk 1 Property Configuration**

**- Basic Configuration**

Auto increment member number: ☒

Trunk data block: IPTI

Terminal number: 100 1 00 00

Designator field for trunk: SIP

Extended trunk: VTRK

Member number: 1 \*

Level 3 Signaling:

Card density: 8D

Start arrangement Incoming : Immediate (IMM)

Start arrangement Outgoing : Immediate (IMM)

Trunk group access restriction: 1

Channel ID for this trunk: 1

Class of Service: Edit

**+ Advanced Trunk Configurations**

**Figure 18: Trunk Properties**

**Figure 19** shows the **Class of Service** values selected for the compliance testing from the drop down menu. Click on **Return Class of Service** button to complete the trunks configuration.

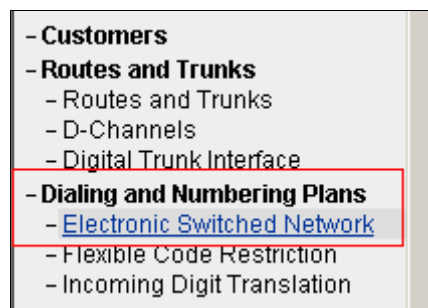
The screenshot shows the 'Trunk Class of Service' configuration interface. It contains the following configuration items:

- Calling party: Calling party Denied (CND)
- Central Office Ringback:
- Centrex Switchhook Flash: Centrex Switchhook Flash Denied (THFD)
- Dial Pulse: Dial Pulse (DIP)
- DTR PAD value:
- Echo Canceling: Echo Canceling Denied (ECD)
- Hong Kong DTI:
- Loop Break Supervised COT:
- Make-break ratio for dial pulse: 10 pulses per second (P10)
- Manual Incoming: Manual Incoming Denied (MID)
- Media Security: Media Security Never (MSNV)
- Network Hook Flash Over M911P:
- Polarity:
- Priority: Low Priority (LPR)
- Restriction level: Unrestricted (UNR)
- Reversed Ear Piece: Reversed Ear Piece denied (XREP)

**Figure 19: Trunk Class of Service**

## 5.5. Configuring Digit Manipulation Block

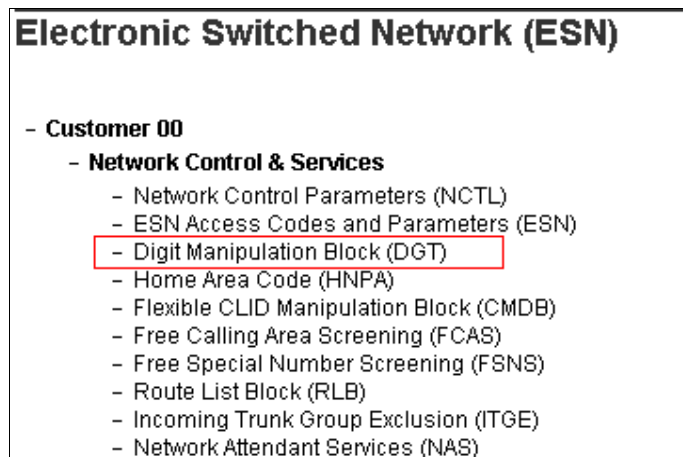
This section explains the digit manipulation block that is to be configured in the CS1000 dialing plan for its users to communicate with the Unigy system. From the EM navigator pane, navigate to **Dialing and Numbering Plans > Electronic Switched Network** as shown in **Figure 20** below.



**Figure 20: EM Screen showing navigation tree to Electronic Switched Network**

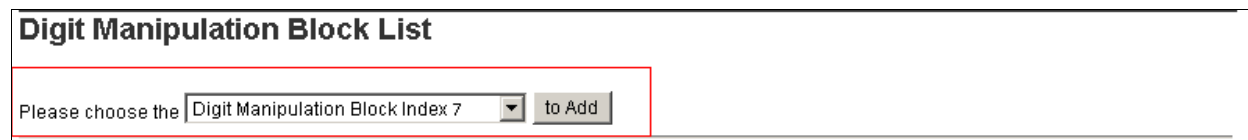


Click on the **Digit Manipulation Block (DGT)** option as shown in **Figure 21** below.



**Figure 21: Accessing Digit Manipulation Block**

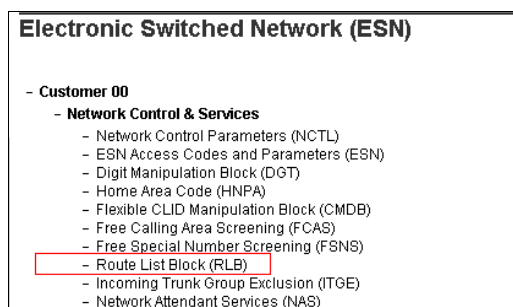
**Figure 22** below shows the Digit Manipulation Block Index users can add. However, during compliance testing **Digit Manipulation Block Index** of **0** was used which is already added in the CS1000 system by default.



**Figure 22: Adding a Digit Manipulation Block Index**

## 5.6. Configuring Route List Block

This section explains the route list block that is to be configured in the CS1000 dialing plan for its users to communicate with the Unigy system. From the EM navigator pane, navigate to **Dialing and Numbering Plans > Electronic Switched Network** as shown in **Figure 20** above. Click on **Route List Block (RLB)** option as shown in **Figure 23** below.



**Figure 23: Accessing Route List Block**

Start adding a **route list index** as shown in **Figure 24** below. During compliance testing, list index **10** was added. Click on **to Add** to continue.

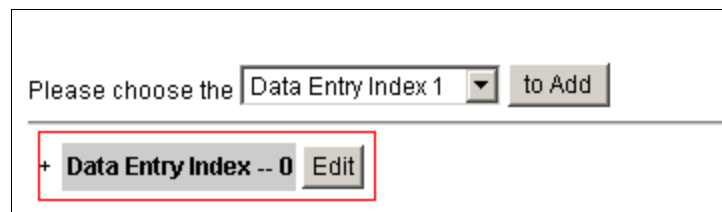


**Route List Blocks**

Please enter a route list index  (0 - 1999)

**Figure 24: Adding Route List Index**

Click on **Edit** for **Data Entry Index 0** as shown in **Figure 25** below.

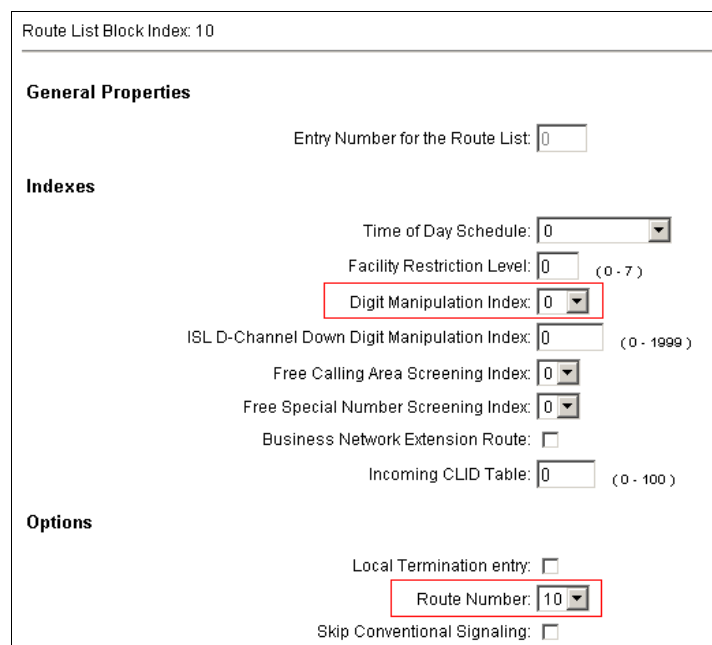


Please choose the

+ Data Entry Index -- 0

**Figure 25: Adding Data Entry Index**

**Figure 26** below shows the values configured for the index block used during compliance testing. A **Route Number** of **10** and **Digit Manipulation Index** of **0** were selected as per the configuration explained in **Sections 5.4** and **5.5** respectively. Click **Submit** (not shown) to complete the configuration.



Route List Block Index: 10

**General Properties**

Entry Number for the Route List:

**Indexes**

Time of Day Schedule:

Facility Restriction Level:  (0 - 7)

Digit Manipulation Index:

ISL D-Channel Down Digit Manipulation Index:  (0 - 1999)

Free Calling Area Screening Index:

Free Special Number Screening Index:

Business Network Extension Route: ☐

Incoming CLID Table:  (0 - 100)

**Options**

Local Termination entry: ☐

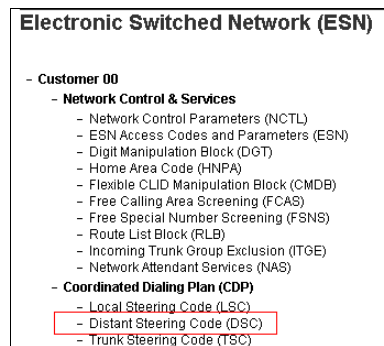
Route Number:

Skip Conventional Signaling: ☐

**Figure 26: Route List Block properties**

## 5.7. Configuring Distant Steering Code

This section explains the distant steering code that is to be configured in the CS1000 dialing plan for its users to communicate with the Unigy system. From the EM navigator pane, navigate to **Dialing and Numbering Plans > Electronic Switched Network** as shown in **Figure 20** above. Click on the **Distant Steering Code (DSC)** option as shown in **Figure 27** below.



**Figure 27: Accessing Distant Steering Code**

From the drop down menu select **Add** and enter a distant steering code to add as shown in **Figure 28** below. During compliance testing a code of **350** was added since the Unigy extension range started with 350xx. Click on **Add** to continue.



**Figure 28: Adding a Distant Steering Code**

Enter the values as shown in **Figure 29** below. Note that the **Route List to be accessed for trunk steering code** value selected is **10** based on the configuration explained in **Section 5.6** above. Click on **Submit** to complete the configuration.

Distant Steering Code

Distant Steering Code: 350

Flexible Length number of digits: 5 (0 - 10)

Display: Local Steering Code (LSC)

Remote Radio Paging Access: ☐

Route List to be accessed for trunk steering code: 10

Collect Call Blocking: ☐

Maximum 7 digit NPA code allowed:

Maximum 7 digit NXX code allowed:

Submit Refresh Delete Cancel

**Figure 29: Distant Steering Code properties**

## 6. Configure Routing using Avaya Aura® System Manager

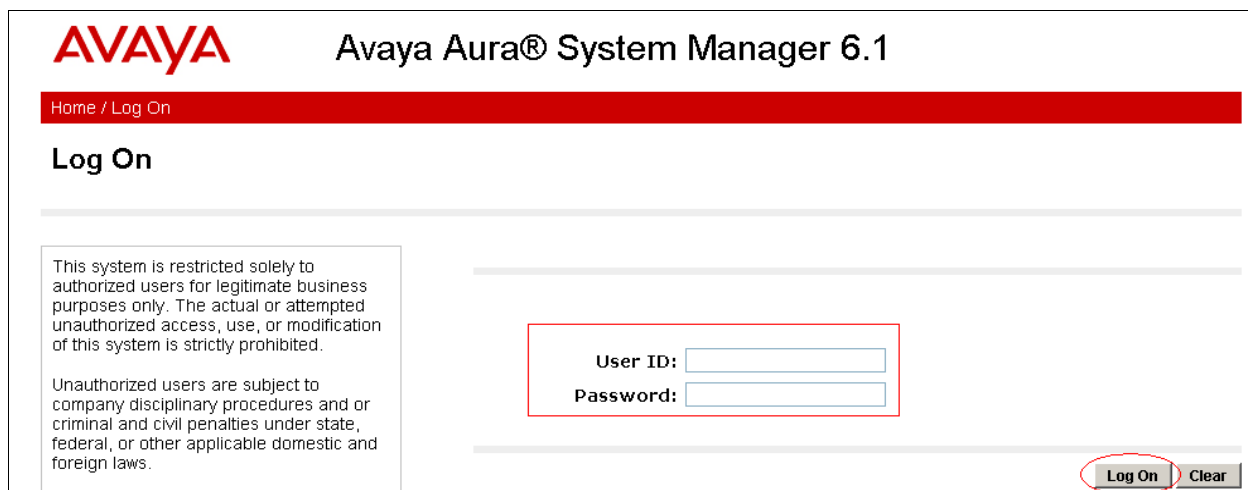
This section provides the procedures for configuring routing using Avaya Aura® System Manager. The procedures include the following areas:

- Logging into the Avaya Aura® System Manager.
- Adding a Domain.
- Adding a Location.
- Adding SIP entities.
- Adding Routing Policies.
- Adding Dial Patterns.

### 6.1. Logging into the Avaya Aura® System Manager

This section explains the steps to launch the login screen of System Manager, and then access the Network Routing Policy.

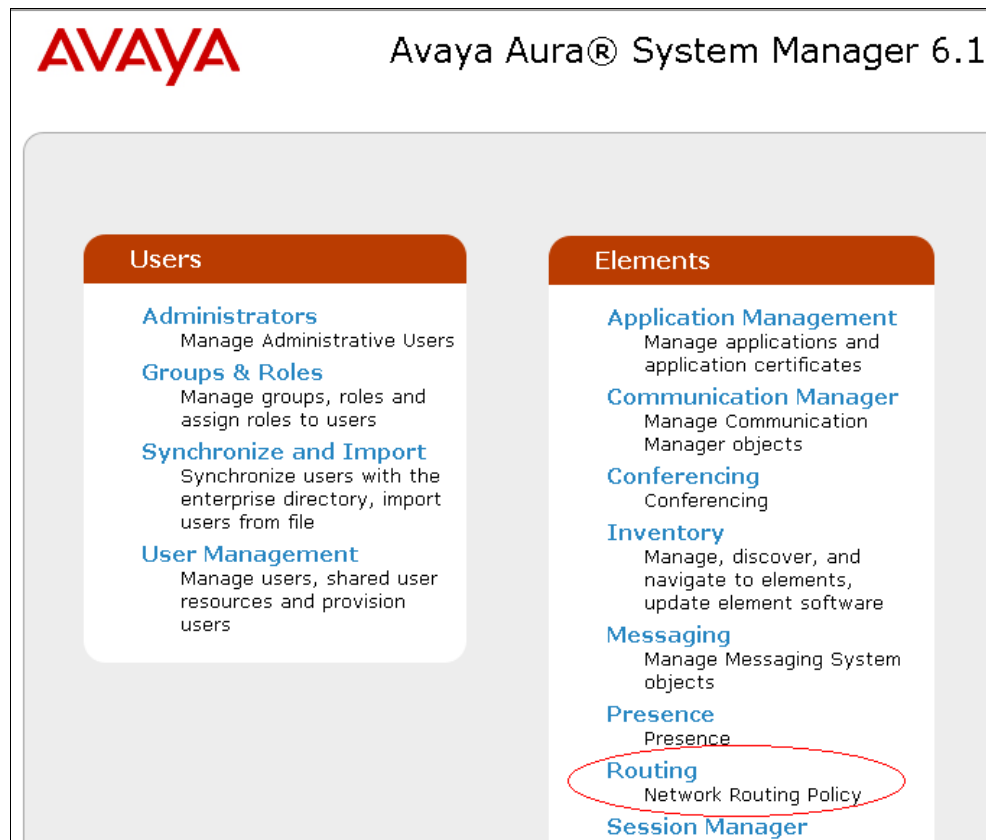
To launch the System Manager Login screen, start an IE browser and type the IP address of System Manager in the URL (not shown). **Figure 30** below shows the Log On Screen. Type the required **User ID** and **Password** credentials and click **Log On** to continue.



The screenshot shows the Avaya Aura® System Manager 6.1 login interface. At the top left is the Avaya logo, and to its right is the title 'Avaya Aura® System Manager 6.1'. Below this is a red navigation bar with the text 'Home / Log On'. The main heading is 'Log On'. On the left side, there is a text box containing a disclaimer: 'This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.' In the center, there is a red-outlined box containing two input fields: 'User ID:' and 'Password:'. At the bottom right, there are two buttons: 'Log On' (which is circled in red) and 'Clear'.

**Figure 30: Avaya Aura® System Manager Login Screen**

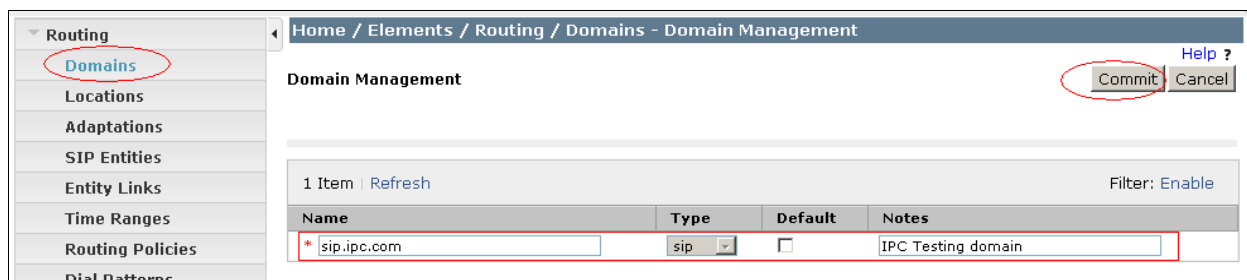
From the main screen of System Manager access the Network Routing Policy by selecting **Routing** as shown in **Figure 31** below.



**Figure 31: Avaya Aura® System Manager Main Screen**

## 6.2. Adding a Domain

To add a domain, select **Domains** from the left hand window of the Routing screen and click on **New** (not shown). Configure the Domain in the **Name** field as shown in **Figure 32** below and click on **Commit** to complete adding a domain. During compliance testing a domain name of **sip.ipc.com** was used. Additional domains can be added in a similar fashion.



**Figure 32: Domain Management**

### 6.3. Adding a Location

To add a location, select **Locations** from the left hand window of the Routing screen and click on **New** (not shown). Configure the Location **Name** as shown in **Figure 33** below and click on **Commit** to add the Location. During compliance testing a location name of **Belleville,Ont,Ca** was used. Click on **Commit** to complete adding a location. Additional locations can be added in a similar fashion.

The screenshot shows the 'Location Details' form. The left sidebar has 'Locations' selected. The main area has a 'General' tab. A red box highlights the 'Name' field with the value 'Belleville,Ont,Ca'. The 'Notes' field is empty. At the top right, 'Commit' and 'Cancel' buttons are visible, with 'Commit' circled in red.

Figure 33: Location Details

### 6.4. Adding SIP Entities

This section explains the adding of SIP entities to Session Manager, Unigy System and the CS1000 system routing. To add SIP Entities, select **SIP Entities** from the left hand window of the Routing screen and click on **New** (not shown).

**Figures 34a and 34b** show the SIP Entity Details for the Session Manager routing. The **FQDN or IP Address** of **110.10.10.198** is the IP address of the Session Manager. Also note that both **TCP** and **UDP** protocols need to be selected for the Entity Links and Ports to **IPC** and **sip.ipc.com** respectively, since Unigy System changes protocols for various diversions. If only the **UDP** protocol is selected then the integration will fail. Click on **Commit** to complete adding the SIP Entity.

The screenshot shows the 'SIP Entity Details' form. The left sidebar has 'SIP Entities' selected. The main area has a 'General' tab. A red box highlights the 'Name' field with the value 'DevASM' and the 'FQDN or IP Address' field with the value '110.10.10.198'. The 'Type' dropdown is set to 'Session Manager'. The 'Notes' field contains 'For Session Manager'. Below this, the 'Location' dropdown is set to 'Belleville,Ont,Ca'. The 'Outbound Proxy' field is empty. The 'Time Zone' dropdown is set to 'America/Toronto'. The 'Credential name' field is empty. At the bottom, the 'SIP Link Monitoring' dropdown is set to 'Use Session Manager Configuration'. At the top right, 'Commit' and 'Cancel' buttons are visible, with 'Commit' circled in red.

Figure 34a: SIP Entity Details for Session Manager

<input type="checkbox"/>	DevASM	UDP	* 5060	DevCM	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	DevASM	TCP	* 5060	IPC	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	DevASM	UDP	* 5060	IPC	* 5060	<input checked="" type="checkbox"/>

Select : All, None < Previous | Page 4 of 6 | Next >

**Port**  
Add Remove

4 Items Refresh Filter: Enable

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

**Figure 34b: SIP Entity Details for Session Manager (cont'd)**

**Figures 35a and 35b** show the SIP Entity Details for the Unigy System routing. The **FQDN or IP Address** of **110.10.10.226** is the IP address of the Unigy System. Also note that both **TCP** and **UDP** protocols need to be selected in the Entity Links section for **IPC** since Unigy System changes protocols for various diversions. If only **UDP** protocol is selected then the integration will fail. Click on **Commit** to complete adding the SIP Entity.

Domains	<p><b>SIP Entity Details</b></p> <p><b>General</b></p> <p>* Name: IPC</p> <p>* FQDN or IP Address: 110.10.10.226</p> <p>Type: Other</p> <p>Notes: For IPC Testing</p> <p>Adaptation:</p> <p>Location: Belleville,Ont,Ca</p> <p>Time Zone: America/New_York</p> <p>Override Port &amp; Transport with DNS <input type="checkbox"/></p> <p>SRV:</p> <p>* SIP Timer B/F (in seconds): 4</p> <p>Credential name:</p> <p>Call Detail Recording: none</p> <p><b>SIP Link Monitoring</b></p> <p>SIP Link Monitoring: Link Monitoring Disabled</p> <p>* Proactive Monitoring Interval (in seconds): 900</p>
Locations	
Adaptations	
<b>SIP Entities</b>	
Entity Links	
Time Ranges	
Routing Policies	
Dial Patterns	
Regular Expressions	
Defaults	

**Figure 35a: SIP Entity Details for Unigy System**

**Entity Links**

Add Remove

2 Items | Refresh Filter: Enable

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	DevASM	TCP	* 5060	IPC	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	DevASM	UDP	* 5060	IPC	* 5060	<input checked="" type="checkbox"/>

Select : All, None

\* Input Required

Commit Cancel

**Figure 35b: SIP Entity Details for Unigy System (cont'd)**

**Figures 36a and 36b** show the SIP Entity Details for the CS1000 System routing. The **FQDN or IP Address** of **110.10.10.130** is the Node IP address of the SIP Signaling Gateway of the CS1000 System. Also note that both **TCP** and **UDP** protocols need to be selected in the Entity Links section for **cppm1** since Unigy System changes protocols for various diversions. If only **UDP** protocol is selected then the integration will fail. Click on **Commit** to complete adding the SIP Entity.

**SIP Entity Details**

**General**

\* Name: cppm1

\* FQDN or IP Address: 110.10.10.130

Type: Other

Notes: Connectivity to CS1K 7.5 Enterpri

Adaptation:

Location: Belleville,Ont,Ca

Time Zone: America/Toronto

Override Port & Transport with DNS ☐

SRV: ☐

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

Credential name:

Call Detail Recording: none

**SIP Link Monitoring**

SIP Link Monitoring: Link Monitoring Disabled

\* Proactive Monitoring Interval (in seconds): 900

**Figure 36a: SIP Entity Details for CS1000 System**



**Entity Links**  
Add Remove

2 Items Refresh Filter: Enable

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	DevASM	TCP	* 5060	cppm1	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	DevASM	UDP	* 5060	cppm1	* 5060	<input checked="" type="checkbox"/>

Select : All, None

\* Input Required

Commit Cancel

**Figure 36b: SIP Entity Details for CS1000 System (cont'd)**

## 6.5. Adding Routing Policies

This section explains the Routing Policy configuration for the Unigy and CS1000 Systems. To add a routing policy, select **Routing Policies** from the left hand window of the Routing screen and click on **New** (not shown).

**Figures 37a and 37b** show the Routing Policy Details for the Unigy System. Select the Unigy System as the SIP Entity Destination and add the dial pattern associated with the Unigy System. A dial pattern can be added once it has been configured as explained in **Section 6.6** below. Click on **Commit** to complete adding a routing policy.

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

Routing Policy Details

General

\* Name: IPC\_routing

Disabled: ☐

Notes: Routing for IPC Server

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
IPC	110.10.10.226	Other	For IPC Testing

Commit Cancel

**Figure 37a: Routing Policy Details for Unigy System**

**Dial Patterns**  
Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/>	350	5	5	<input type="checkbox"/>	sip.ipc.com	Belleville,Ont,Ca	Routing for IPC server

Select : All, None

**Figure 37b: Routing Policy Details for Unigy System (cont'd)**

**Figures 38a and 38b** show the Routing Policy Details for the CS1000 System. Select the CS1000 System as the SIP Entity Destination and add the dial pattern associated with the CS1000 System. A dial pattern can be added once it has been configured as explained in **Section 6.6** below. Click on **Commit** to complete adding a routing policy.

Additional routing policies can be configured as required in a similar fashion.

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

Routing Policy Details

General

\* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
cppm1	135.10.97.130	Other	Connectivity to CS1K 7.5 Enterprise 1 system for Skype Testing

**Figure 38a: Routing Policy Details for CS1000**

Dial Patterns

5 Items | Refresh Filter: Enable

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
58	5	5		sip.ipc.com	Belleville,Ont,Ca	
961396	11	36		sip.ipc.com	Belleville,Ont,Ca	Call from IPC to CS1000 via tandem

Select : All, None

**Figure 38b: Routing Policy Details for CS1000 (cont'd)**

## 6.6. Adding Dial Patterns

This section explains the steps to add a dial pattern for the Unigy and CS1000 systems. To add a dial pattern, select **Dial Patterns** from the left hand window of the Routing screen and click on **New** (not shown).

**Figure 39** shows the Dial Pattern Details for the Unigy System. During compliance testing, the extension range on the Unigy System started with 350xx and therefore **350** is used in the **Pattern** field. The minimum and maximum size of the extension is defined as **5**. Add the **IPC routing** policy as configured in **Section 6.5** above. Click on **Commit** to complete adding the dial pattern. Additional dial patterns can be configured as required in a similar fashion.

**Dial Pattern Details**

**General**

\* Pattern: 350

\* Min: 5

\* Max: 5

Emergency Call: ☐

SIP Domain: sip.ipc.com

Notes: Routing for IPC server

**Originating Locations and Routing Policies**

**Add** **Remove**

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville, Ont, Ca		IPC_routing	0	<input type="checkbox"/>	IPC	Routing for IPC Server

**Figure 39: Dial Pattern Details**

## 7. Configure IPC Media Manager

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

- Launch Unigy Management System.
- Administer SIP Trunks.
- Administer trunk groups.
- Administer route lists.
- Administer dial patterns.
- Administer route plans.
- Administer Codecs.

The configuration of Media Manager is typically performed by IPC installation technicians. The procedural steps are presented in these Application Notes for informational purposes. For detailed administration and configuration information for the Unigy system refer to **Section 10 [2]**.

### 7.1. Launch Unigy Management System

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

The screen as shown in **Figure 40** below is displayed. Enter the appropriate credentials. Check **I agree with the Terms of Use**, and click **Login**.

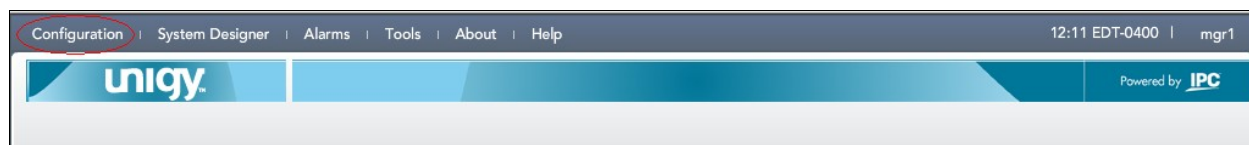
In the subsequent screen (not shown), click **Continue**.

The image shows a web-based login interface for the IPC Unigy Management System. On the left is the IPC logo. To its right are labels for 'User Name:' and 'Password:'. The corresponding input fields are highlighted with a red rectangle. Below these fields is a checkbox labeled 'I agree with the' followed by a blue underlined link 'Terms of Use'. The 'Login' button is highlighted with a red circle. At the bottom, the text reads: 'IPC Unigy™ Management System', 'Unigy™ Version 01.00.00.04.0003', and '© Copyright 2011 IPC Systems, Inc.'

**Figure 40: Unigy Management System Login Screen**

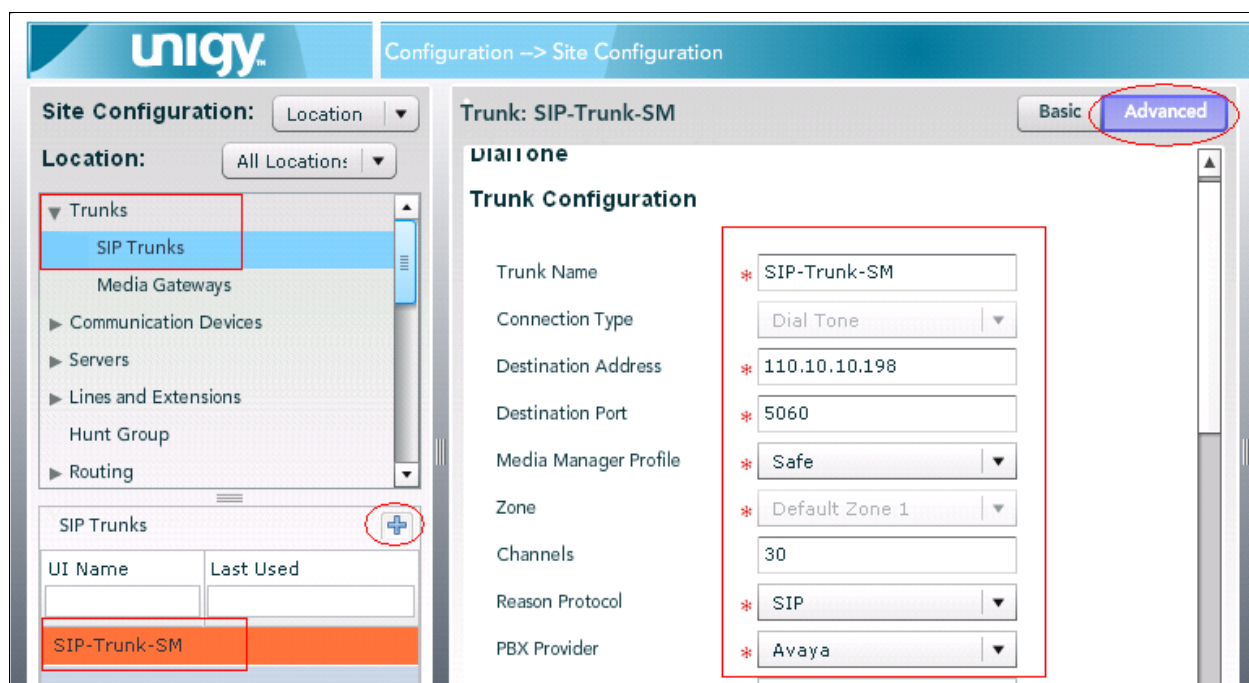
## 7.2. Administer SIP Trunks

The screen as shown in **Figure 41** below is displayed next. Select **Configuration > Site Configuration** from the top menu.



**Figure 41: Unigy Management System Login Screen**

**Figures 42a and 42b** below show the **Site Configuration** information displayed in the left pane. Select **Trunks > SIP Trunks** and click the “+” icon in the lower left pane to add a new SIP trunk group. Click on the **Advanced** tab to configure the trunk. During compliance testing a SIP trunk by the name **SIP-Trunk-SM** was added with the required values as shown below. The IP address **110.10.10.198** is the IP address of the Avaya Aura® Session Manager. Values shown in the red box were used during compliance testing. Click on **Save** (not shown) to complete the configuration.



**Figure 42a: Adding a SIP Trunk**

unigy™ Configuration -> Site Configuration

**Site Configuration:** Location ▾

**Location:** All Location: ▾

▼ Trunks

- SIP Trunks
- Media Gateways
  - Communication Devices
  - Servers
  - Lines and Extensions
- Hunt Group
- Routing

SIP Trunks +

UI Name	Last Used
SIP-Trunk-SM	

**Trunk: SIP-Trunk-SM** Basic Advanced

Connected Party Update \* UPDATE ▾

Subscribe to MWI ☐

MWI Subscription Time 0

Vendor

A/B Side ☐

Distant End Name

PBX Trunk Group Reference

Trunk Info

Diversion Header \* History-Info ▾

Indicate PRACK Support ☐

Outgoing Transport Type \* UDP ▾

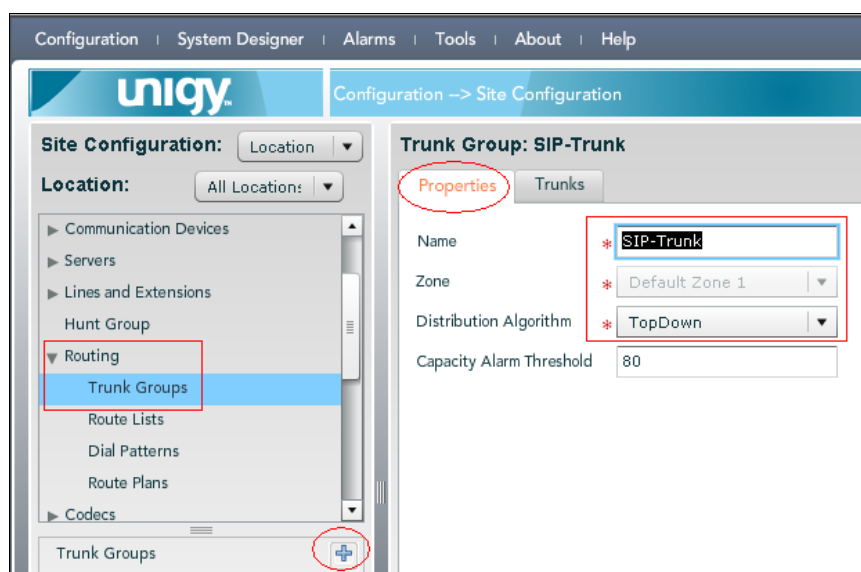
ReINVITE For Media Update ☐

**Figure 42b: Adding a SIP Trunk (cont'd)**

### 7.3. Administer Trunk Groups

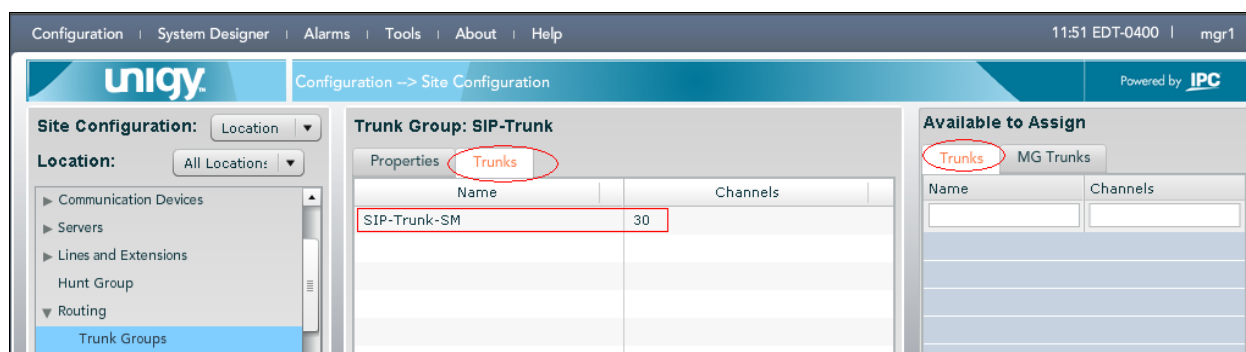
Select **Routing > Trunk Groups** in the left pane, and click the “+” icon in the lower left pane to add a new trunk group as shown in **Figure 43** below.

The **Trunk Group** screen is displayed in the right pane. In the **Properties** tab, enter a descriptive **Name**, leave the remaining values as default and click **Save** (not shown).



**Figure 43: Adding Trunk Group**

Select the **Trunks** tab in the right pane as shown in **Figure 44** below. The screen is updated with three panes. In the right pane, select the **Trunks** tab. In the listing, select and expand the applicable trunk (not shown) from **Section 7.2**, and drag the selection to the **Name** column in the middle pane as shown below. Click on **Save** (not shown) to complete the configuration.

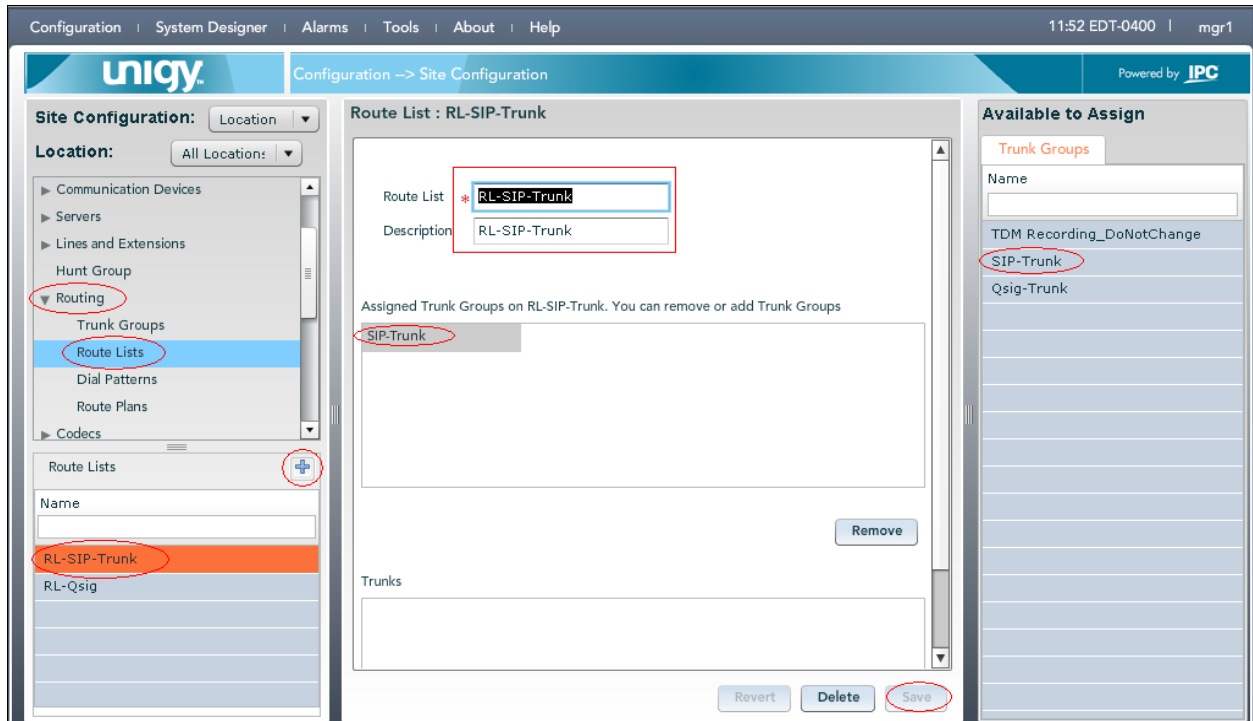


**Figure 44: Adding Trunk Group (cont'd)**

## 7.4. Administer Route Lists

Select **Routing > Route Lists** in the left pane, and click the “+” icon in the lower left pane to add a new route list as shown in **Figure 45** below.

The **Route List** screen is displayed in the middle pane. For **Route List**, enter a descriptive name. In the right pane, select the trunk group from **Section 7.3** and drag into the **Assigned Trunk Groups on Route List** sub-section in the middle pane, as shown below. Click on **Save** to complete the configuration.



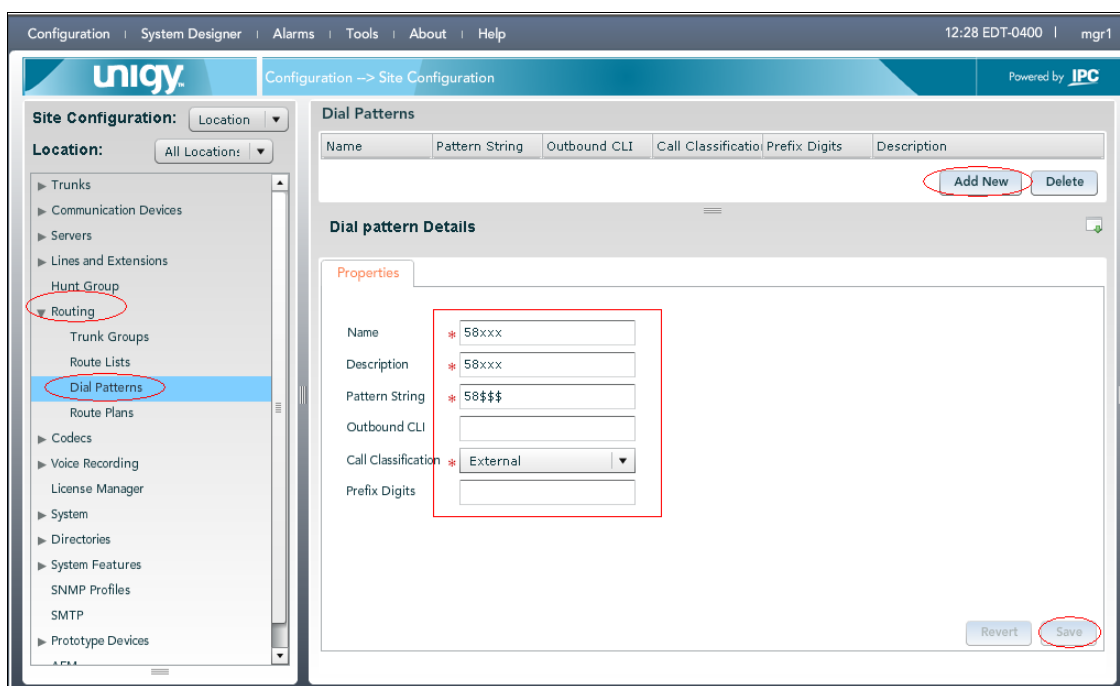
**Figure 45: Adding Route List**



## 7.5. Administer Dial Patterns

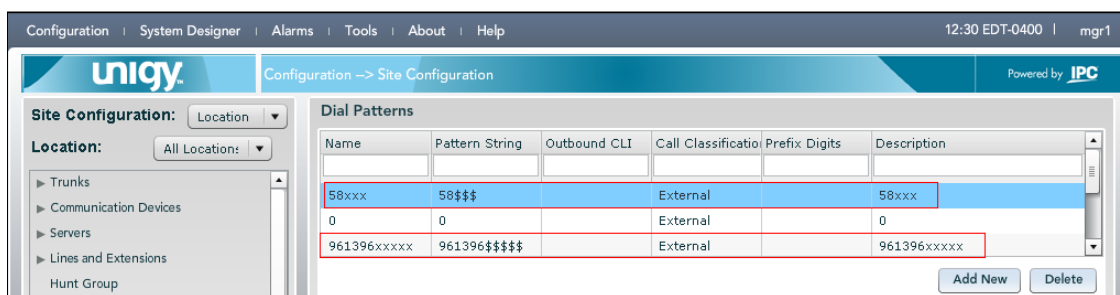
Select **Routing > Dial Patterns** in the left pane to display the **Dial Patterns** screen in the right pane. Click **Add New** in the upper right pane as shown in **Figure 46** below.

In the **Dial pattern Details** sub-section in the lower right pane, enter the desired **Name** and **Description**. For **Pattern String**, enter the dial pattern to match for Avaya CS1000 extensions, in this case **58\$\$\$** with “\$” matching to any digit. For **Call Classification**, select **External**. Click on **Save** to complete adding a dial pattern.



**Figure 46: Adding a Dial Pattern**

Repeat this section to add another dial pattern to reach the PSTN, and include any required prefix by Avaya CS1000. In the compliance testing, two dial patterns were created as shown in **Figure 47** below.



**Figure 47: Extension and PSTN Dial Patterns**

## 7.6. Administer Route Plans

Select **Routing > Route Plans** in the left pane, and click **Add New** (not shown) in the right pane to create a new route plan as shown in **Figure 48** below.

The screen is updated with three panes, as shown below. In the **Route Plan** middle pane, enter a descriptive **UI Name** and an optional **Description**. For **Calling Party**, enter \* to denote any calling party from Unigy. For **Called Party**, select the dial pattern for the CS1000 users from **Section 7.5**. Select **Forward** for **Action**, and click on **Save**.

The screenshot shows the Unigy configuration interface. The left pane shows the 'Site Configuration' menu with 'Routing' and 'Route Plans' highlighted. The middle pane shows the 'Create New Route Plan' form with the following fields: UI Name (58xxx), Description, Calling Party (\*), Called Party (58xxx), and Action (Forward). The 'Save' button is highlighted. The right pane shows the 'Available to Assign' section with a list of route plans.

**Figure 48: Creating a new Route plan**

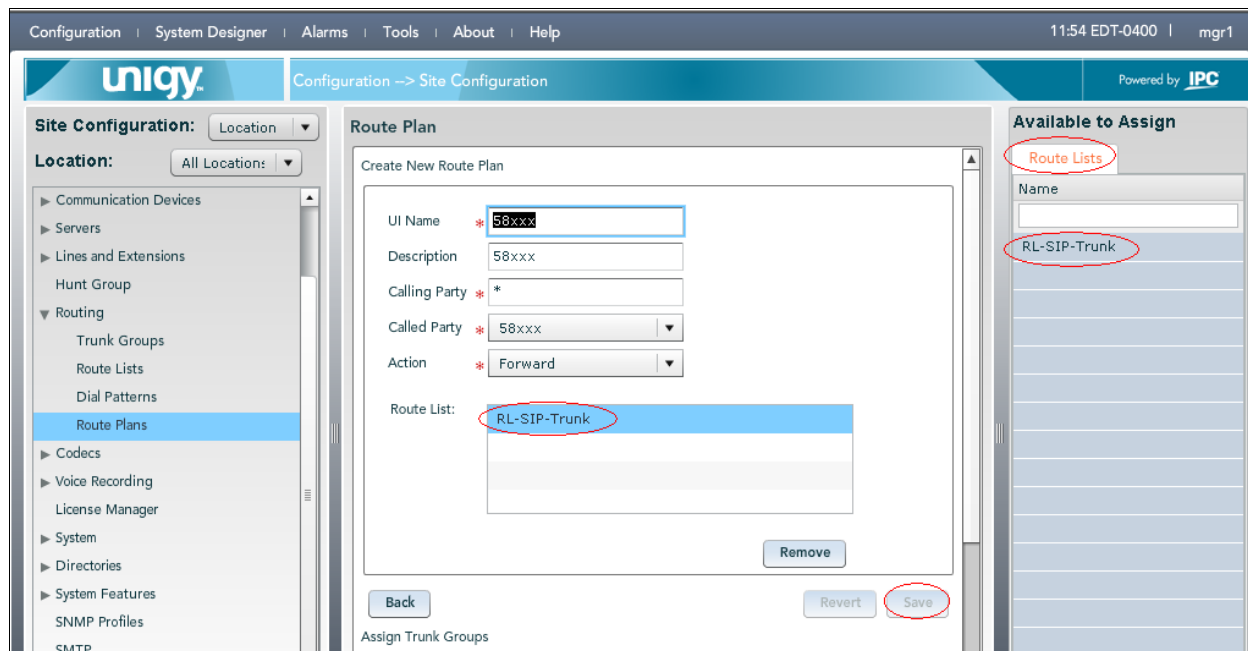
The screen is updated with the newly created route plan as shown in **Figure 49** below. Select the route plan, and click **Edit** toward the bottom of the screen (not shown).

The screenshot shows the Unigy configuration interface. The left pane shows the 'Site Configuration' menu with 'Routing' and 'Route Plans' highlighted. The middle pane shows the 'List of Route Plans' table with the following data:

UI Name	Calling Party	Called Party	Action
58xxx	*	58xxx	FORWARD

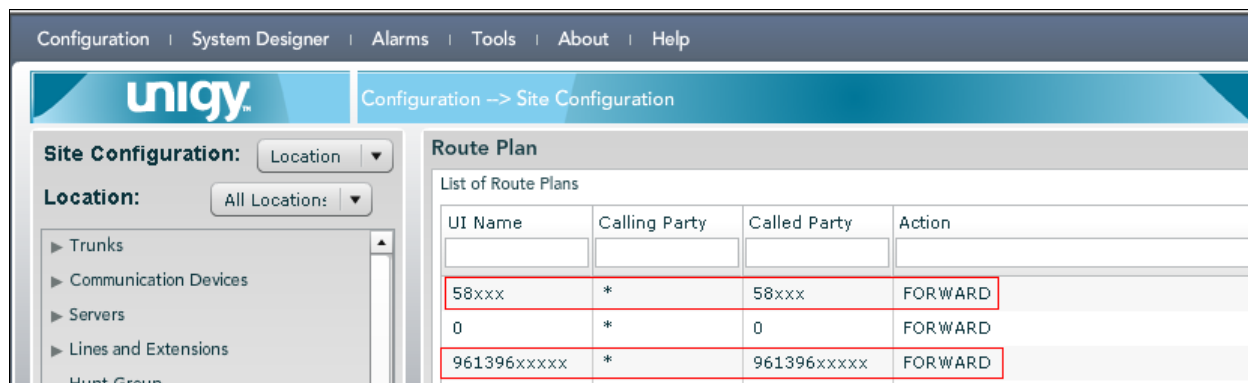
**Figure 49: New Route Plan**

The screen is updated with three panes again, as shown in **Figure 50** below. In the right pane, select the route list from **Section 7.4** and drag into the **Route List** sub-section in the middle pane, as shown below. Click on **Save** to complete the configuration.



**Figure 50: Adding Route List to Route Plan**

Repeat this section to add another route plan for the PSTN. During compliance testing, two route plans were created as shown in **Figure 51** below.



**Figure 51: Extension and PSTN Route Plan**

## 7.7. Administer Codecs

Select **Codecs** > **Codecs** in the left pane, and click the “+” icon in the lower left pane to add a new codec as shown in **Figure 52** below.

Enter a **Name** for the Codec, select a codec **Type** from the drop down and enter 20 for the **Packet Period**. Click on **Save** to complete the configuration. **Figure 52** below shows the G.711 u-law codec being added. Similarly another codec for G.729 can be added.

The screenshot shows the UniQy configuration interface. On the left, the 'Site Configuration' pane has a tree view with 'Codecs' selected. Below it, a list of existing codecs is shown: 'High Def Voice G\_722', 'G711 mu-law G\_711u\_law', and 'Low Bandwidth G\_729'. A red box highlights the 'G711 mu-law' entry. In the main pane, the 'G711 mu-law' configuration form is displayed. It has fields for 'Name' (containing 'G711 mu-law'), 'Type' (a dropdown menu showing 'G.711 u-law'), and 'Packet Period' (containing '20'). A red box highlights these three fields. At the bottom right of the main pane, there are buttons for 'Delete', 'Revert', and 'Save', with the 'Save' button highlighted by a red circle.

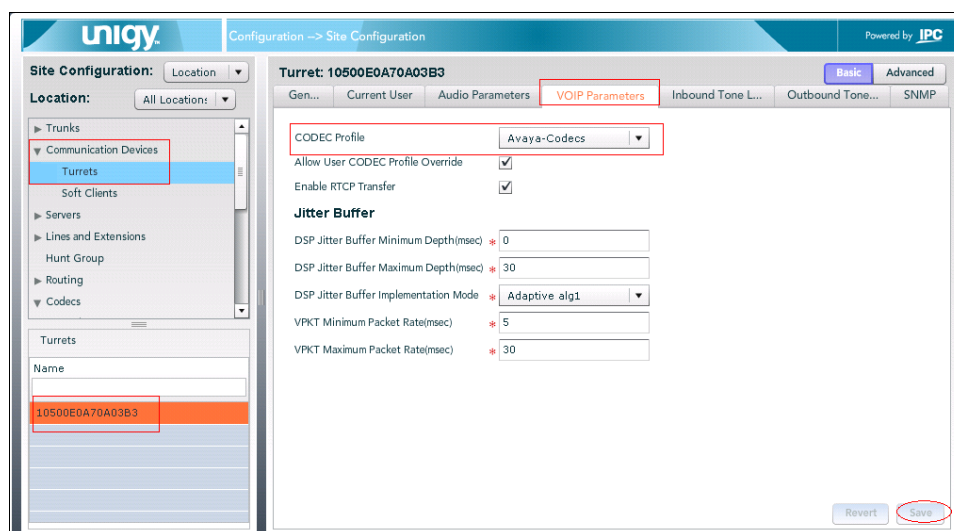
**Figure 52: Adding a Codec**

The two codecs added above will be used during compliance testing however they need to be included into a codec profile. Select **Codecs** > **Codec Profiles** and click on “+” to add a new profile. **Figure 53** below shows a profile that has been added during compliance testing called **Avaya-Codecs** and **G711 a-law** and **G.729** codecs has been added to this profile by dragging it into the middle pane from the right pane. Click on **Save** to complete this configuration.

The screenshot shows the UniQy configuration interface for creating a codec profile. On the left, the 'Site Configuration' pane has a tree view with 'Codec Profiles' selected. Below it, a list of existing profiles is shown: 'Low Bandwidth', 'All Codecs', 'MS Codecs', 'MG Codecs', and 'Avaya-Codecs'. A red box highlights the 'Avaya-Codecs' entry. In the main pane, the 'Avaya-Codecs' configuration form is displayed. It has a 'Profile Name' field (containing 'Avaya-Codecs') and a table for 'Codecs'. The table has two columns: 'Name' and 'Type'. It contains two rows: 'G711 mu-law' with type 'G\_711u\_law' and 'G.729' with type 'G\_729'. A red box highlights the 'G711 mu-law' entry. At the bottom of the main pane, there are buttons for 'Delete', 'Remove', 'Revert', and 'Save', with the 'Save' button highlighted by a red circle. On the right, the 'Available to Assign' pane shows a list of codecs: 'High Def Voice', 'G711 mu-law', 'Low Bandwidth with VAD', 'G711 a-law', and 'G.729'. A red box highlights the 'G711 a-law' and 'G.729' entries.

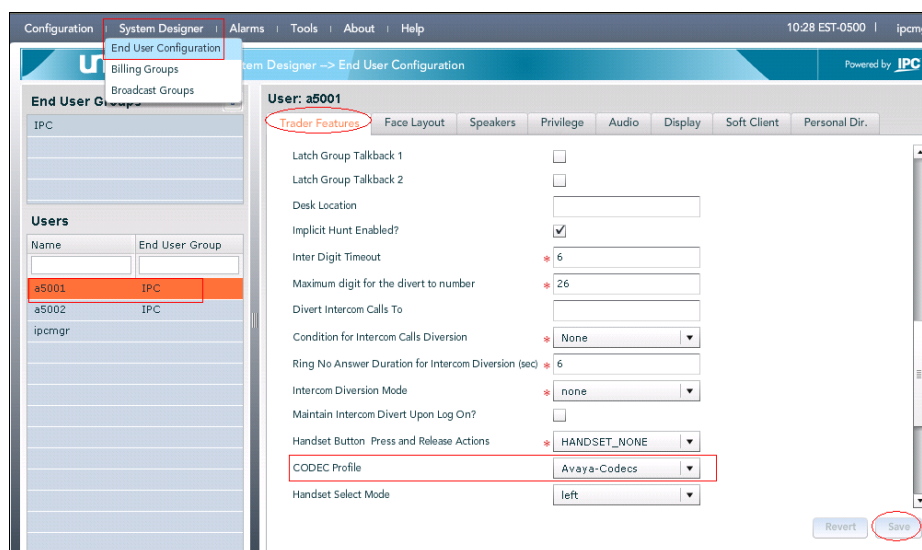
**Figure 54: Creating a Codec Profile**

The created Codec profile needs to be added at the Turret and User level. To include this profile in a turret, select **Communication Devices > Turrets** as shown in **Figure 55** below. Select a turret and in the **VOIP Parameters** tab select the created codec profile from the drop down seen under the **CODEC Profile** field. Click on **Save** to complete this configuration.



**Figure 55: Selecting CODEC Profile for a Turret**

To include this profile in a user, navigate to **System Designer > End User Configuration**. Select a user and access the **Trader Features** tab. Select the required profile from the drop down of the **CODEC Profile** field as shown below. Click on **Save** to complete the configuration.



**Figure 56: Selecting CODEC Profile for a User**

Note that after configuring the Codecs, the turrets will need to be rebooted.

## 8. Verification Steps

The following tests were conducted to verify the solution between the CS1000 and Unigy system:

- All basic call features operate successfully between CS1000 and Unigy users.
- Connection between Unigy System and Avaya Aura® Session Manager is successfully established when the Ethernet connection is disconnected and connected back to the Unigy System.

## 9. Conclusion

These Application Notes describe the configuration steps required for IPC Unigy to successfully interoperate with Avaya Communication Server 1000 7.5 using SIP trunks. All executed test cases have passed and met the objectives outlined in **Section 2** along with the observations as noted in **Section 2.2**. The Unigy System is considered compliant with Avaya CS1000 Release 7.5 using Avaya Aura®.

## 10. Additional References

This section references the product documentation relevant to these Application Notes.

1. *CS1000 7.50 Administering and System Programming documents*, available at <http://support.avaya.com>.
2. *Unigy 1.1 System Configuration*, Part Number B02200187, Release 00, upon request to IPC Support.

---

**©2012 Avaya Inc. All Rights Reserved.**

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

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