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 Communication Server 1000) 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 Communication Server 1000 IP (UNIStim and SIP), Digital and/or PSTN users.

2. General Test Approach and Test Results

The feature test cases were performed manually. Calls were manually established among Unigy turret users with Communication Server 1000 IP (UNIStim and SIP), 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.

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

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

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

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 S**ection 2.1** were verified and met. All tests were executed and passed with the following observations:

- Communication Server 1000 does not support the G722 Audio codec, hence on the Unigy CCM (Converged Communication Manager) side new codec and codec profiles should be created and should be assigned to Turret devices and Turret user profiles in following preferences, in order to work with Communication Server 1000: G711MU/G711A/G729A. A packet rate of 20ms is to be used with G.711 and G.729 codecs.

- Unigy MM (Media Manager) codec profile should be rearranged in following preferences, in order to work with Communication Server 1000: G711MU/G711A/G729A/telephone events.
- Set A (Unigy) calls Set B (Avaya SIP) which is All Calls Forwarded to Set C (Avaya) which is in busy state. Set A hears a mix of reorder and ring tone simultaneously instead of hearing only busy tone. This is a known limitation on an Avaya SIP phone where the preferred method for call forwarding would be directly from Communication Server 1000 using Flexible Feature Code rather than using phone based call forwarding.
- In the case of Attended and un-Attended call transfer, Calling Line ID does not update on the Avaya phones. It shows the Calling Line ID of the last Calling/Connected party, not the current Calling/Connected party. This is a known limitation on Avaya SIP trunks since it expects a re-INVITE message from the third party to trigger name and number modification and Unigy sends UPDATEs and not re-INVITEs to trigger name and number modifications.
- Observed Message Waiting Indicator (MWI) lamp delay approx. 60-80 second in case of Transfer and a few Diversion combinations, while it works instantly in the case of a point to point call.
- Set A (Avaya SIP) calls Set B (Unigy) and hangs up before Set B answers the call. As soon as Set A hangs up, ringing on Set B should cease however Set B keeps ringing till it times out. This scenario only occurs when Set A is an Avaya SIP phone. To overcome this problem, disable Ring Again No Answer (RNA) which is found under Option (OPT) field of the Features and Options (FTR) in Customer Data Block (CDB) of the Communication Server 1000.
- Since Unigy does not support UPDATE for call transfers, call transfer scenarios from Communication Server 1000 will fail unless firewall plug-in 501 is enabled in Communication Server 1000.
- 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**.

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

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, Communication Server 1000 and Avaya Aura® Session Manager are connected to each other through the lab network. SIP trunks are used from Unigy to Communication Server 1000 via the Avaya Aura® Session Manager, to reach users on Communication Server 1000 and on the PSTN.

A five digit Uniform Dial Plan (UDP) was used to facilitate dialing between Unigy and Communication Server 1000. During compliance testing, extension ranges 58xxx were associated with Communication Server 1000 users and 35xxx were associated with the Unigy turret users. The Avaya Call Pilot DN is 58888 and the PSTN number is 96139655570.

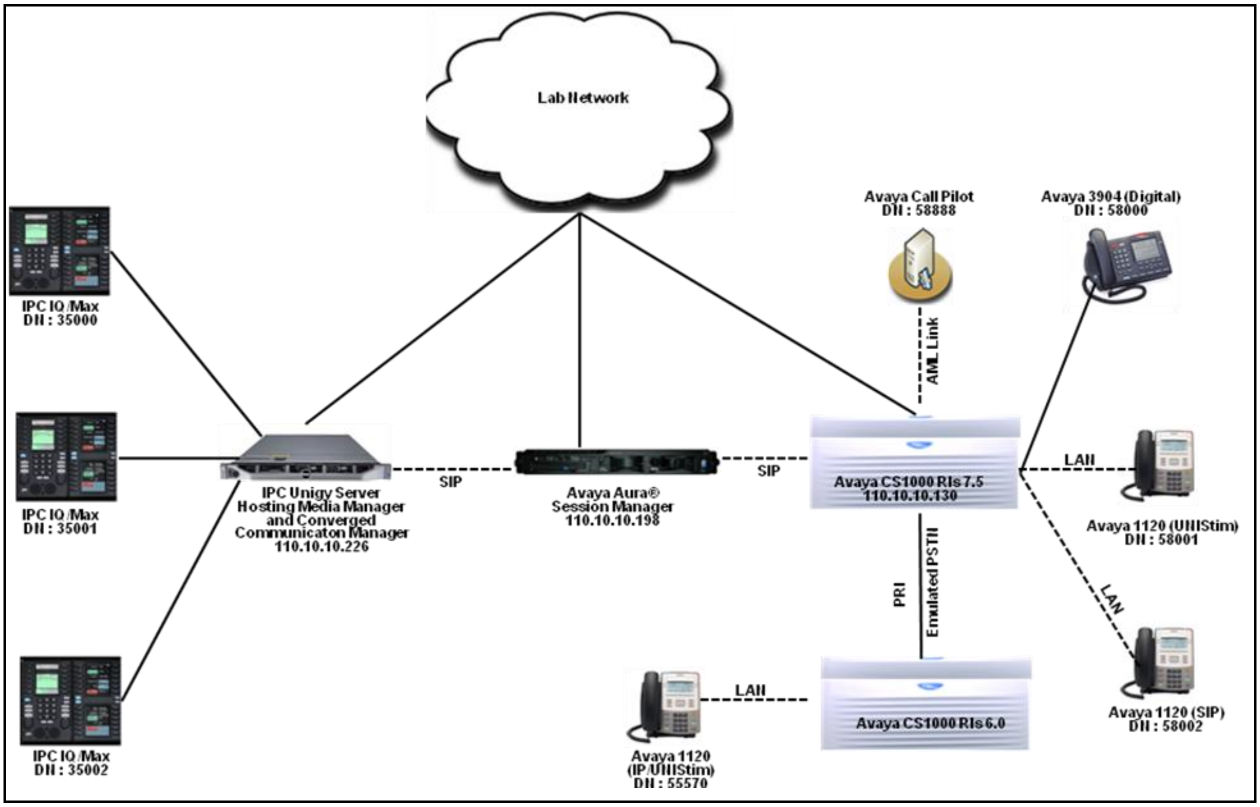


Figure 1: Compliance Test Setup in the lab

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)	5.00.41.143
Avaya Aura® Session Manager	6.1
Avaya Aura® System Manager	6.1
Avaya Digital user (3904)	NA
Avaya 1120 IP (SIP) Deskphone	04.03.12.00
Avaya 1120 IP (UNIStim) Deskphone	0624C8A
IPC Unigy • Media Manager • Converged Communication Manager • Turrets (IQ/Max)	 02.00.00.00.1536 02.00.00.00.1536 02.00.00.00.1536

5. Configure Avaya Communication Server 1000

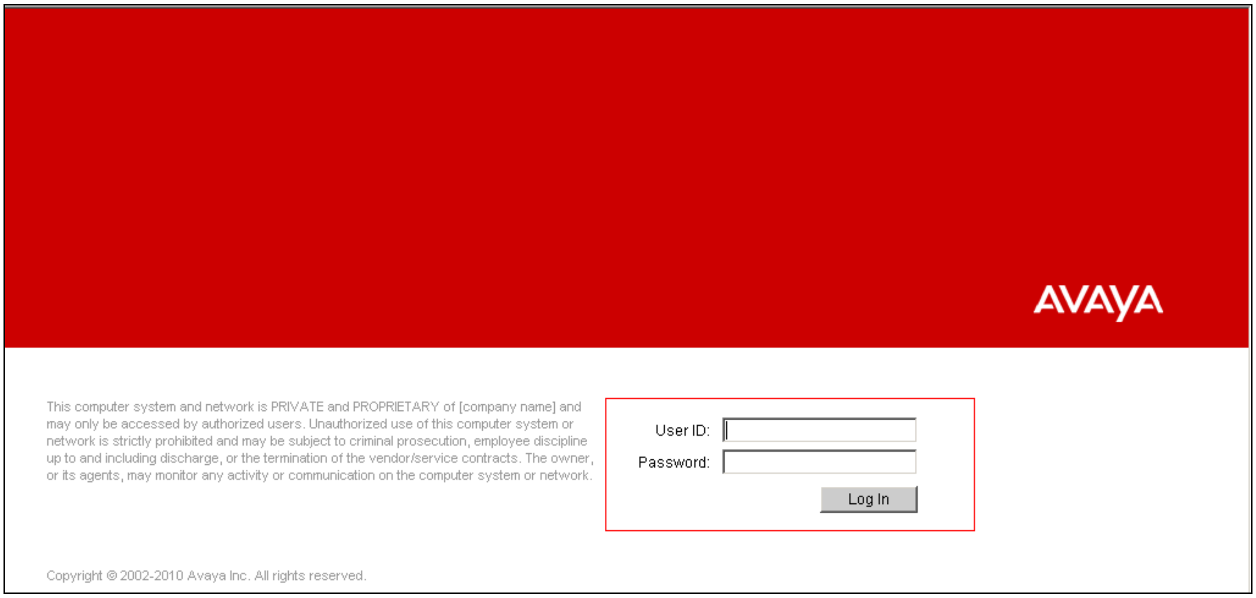
This section provides the procedures for configuring the Avaya Communication Server 1000 system. The procedures include the following areas:

- 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.

The assumption is made here that the Communication Server 1000 users are already created and also the PRI Trunk between Communication Server 1000 7.5 and Communication Server 1000 6.0 is configured for emulated PSTN setup during compliance testing. For configuration details of the Communication Server 1000 refer to the reference documentation in **Section 11**.

5.1. Logging into Element Manager via Unified Communication Manager

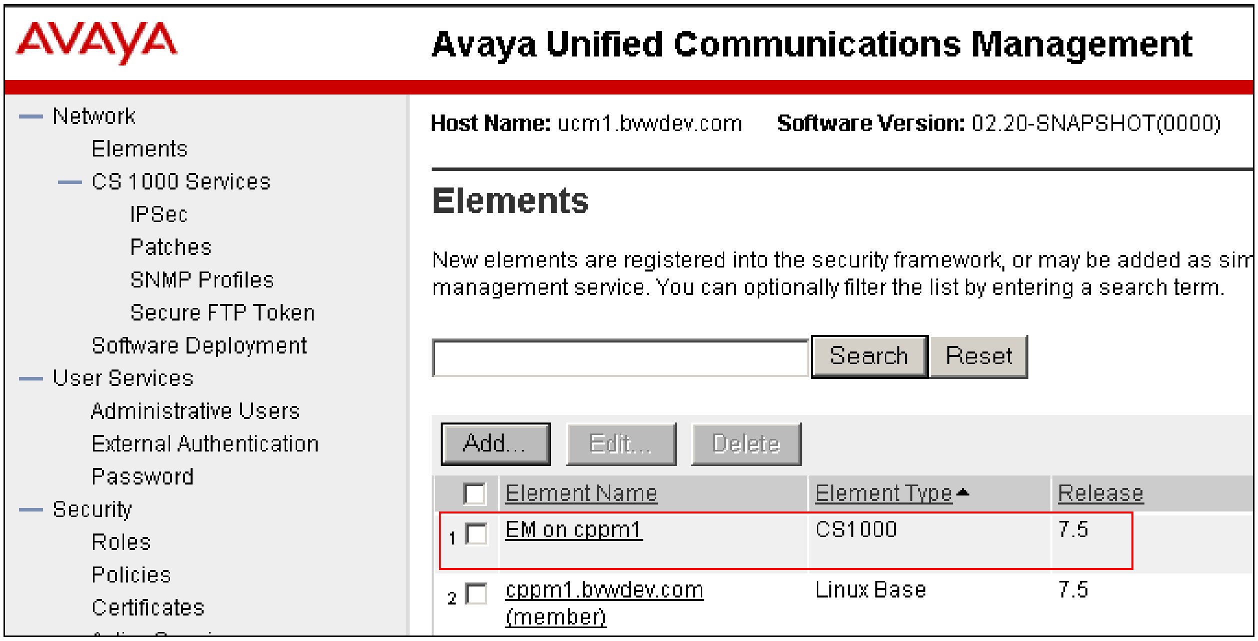
To login to the Unified Communications Manager (UCM) open an IE browser and type in the IP address of the UCM in the URL (not shown). The screen below shows the login screen of the UCM. Enter the **User ID** and **Password** credentials and click on **Log In** to continue.



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.

Copyright © 2002-2010 Avaya Inc. All rights reserved.

From the UCM main screen as shown below, click on the Element **EM on cppm1**. This is the element which is configured to access the Element Manager (EM) for the Communication Server 1000 Call Server.



Avaya Unified Communications Management

- Network
  - Elements
  - CS 1000 Services
    - IPSec
    - Patches
    - SNMP Profiles
    - Secure FTP Token
  - Software Deployment
- User Services
  - Administrative Users
  - External Authentication
  - Password
- Security
  - Roles
  - Policies
  - Certificates

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.

[ ] Search Reset

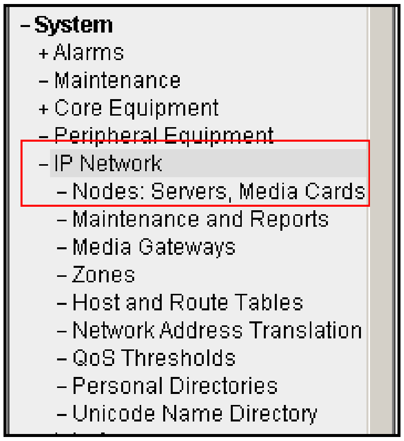
Add... Edit... Delete

	□	Element Name	Element Type ▲	Release
1	□	EM on cppm1	CS1000	7.5
2	□	cppm1.bwwdev.com (member)	Linux Base	7.5

5.2. Configuring the SIP Signaling Gateway

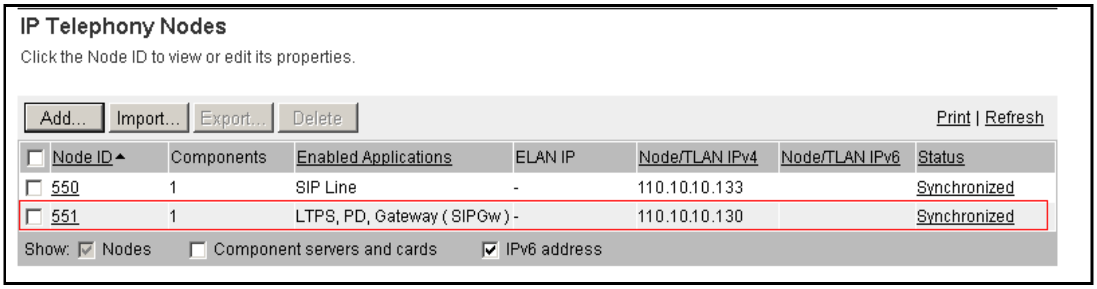
This section describes the configuration required on the SIP Signaling Gateway present on the Communication Server 1000 so that Communication Server 1000 can communicate with the Avaya Aura® Session Manager via SIP Trunks. The assumption is made here that the IP Telephony node is already added.

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



- 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
    - QoS Thresholds
    - Personal Directories
    - Unicode Name Directory

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



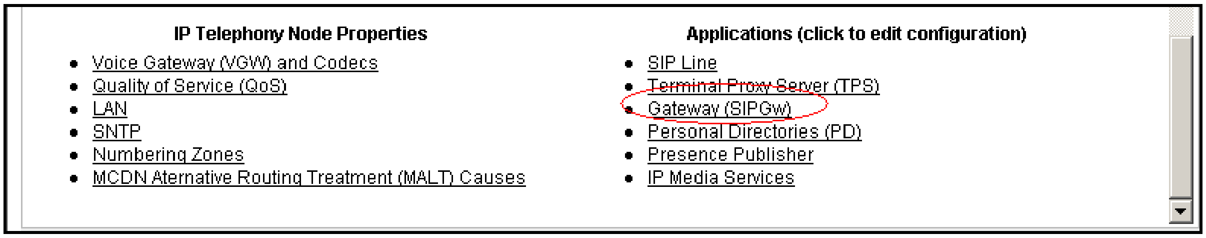
IP Telephony Nodes

Click the Node ID to view or edit its properties.

□ Node ID▲	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
□ 550	1	SIP Line	-	110.10.10.133		Synchronized
□ 551	1	LTPS, PD, Gateway (SIPGw)	-	110.10.10.130		Synchronized

Show: ☑ Nodes □ Component servers and cards ☑ IPv6 address

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



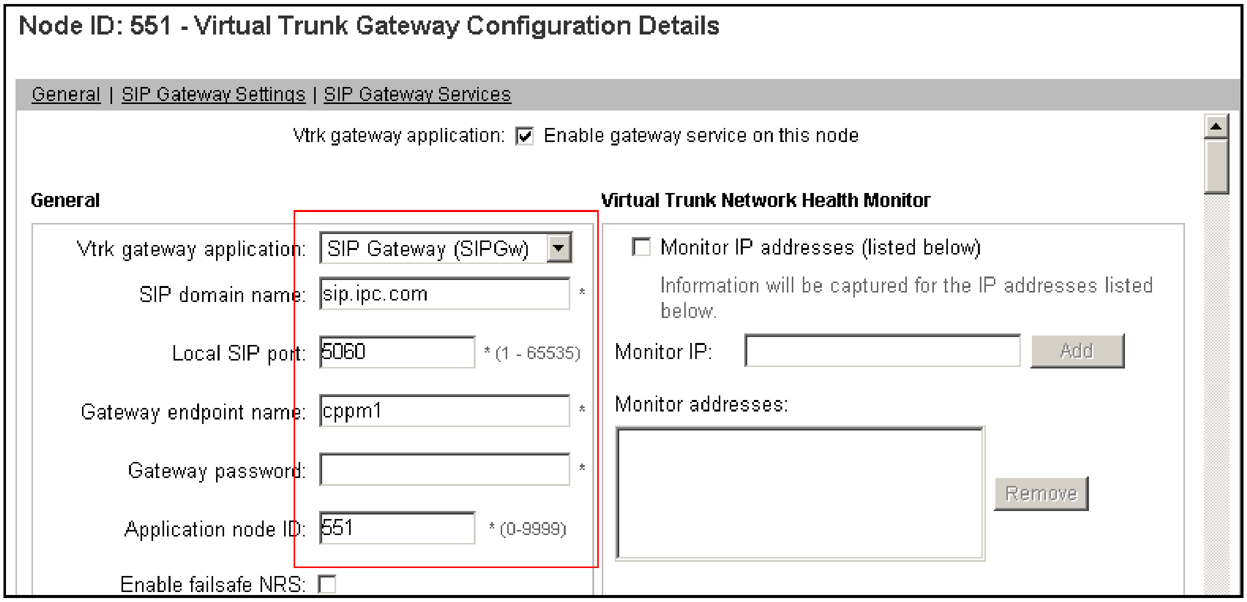
IP Telephony Node Properties

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

Applications (click to edit configuration)

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

In the **General** tab, select the values as shown 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

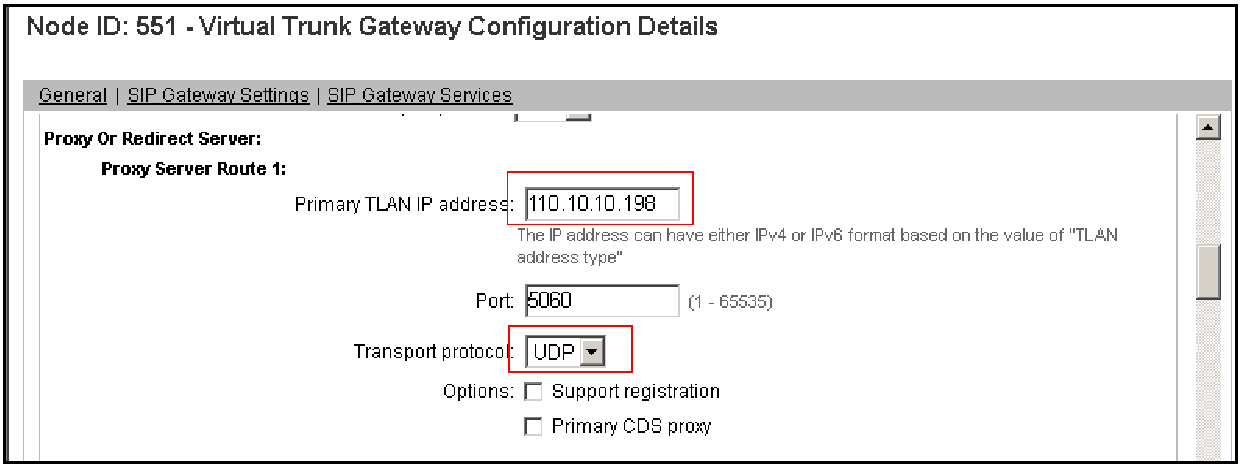
□ Monitor IP addresses (listed below)

Information will be captured for the IP addresses listed below.

Monitor IP:

Monitor addresses:

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 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

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"

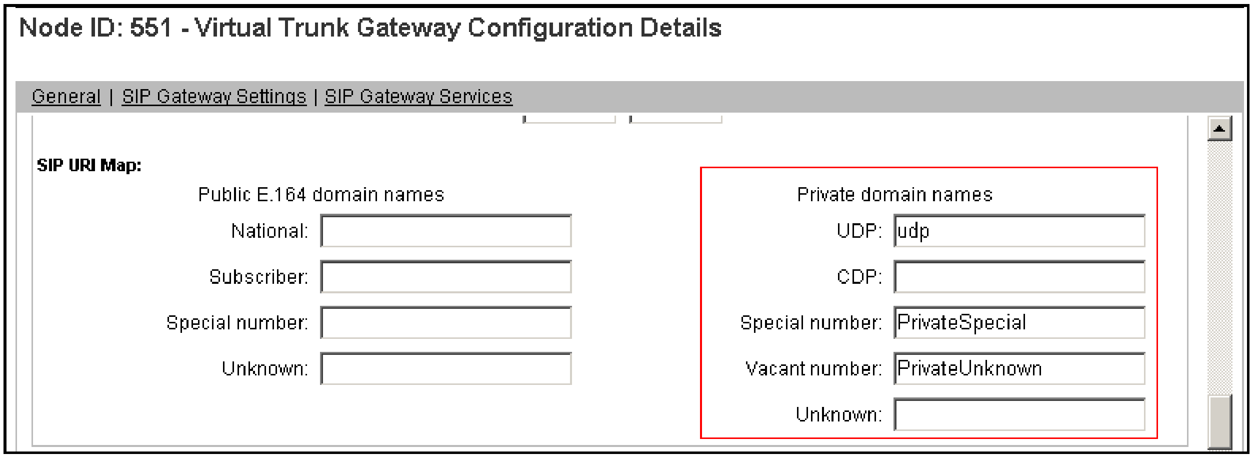
Port: 5060 (1 - 65535)

Transport protocol: UDP

Options: □ Support registration

□ Primary CDS proxy

In the **SIP URI Map** section, enter the values as shown below. These values need to be matched if integration is to be successful between Unigy and Communication Server 1000, since Unigy is only able to understand the values below in its SIP messaging properties.



Node ID: 551 - Virtual Trunk Gateway Configuration Details

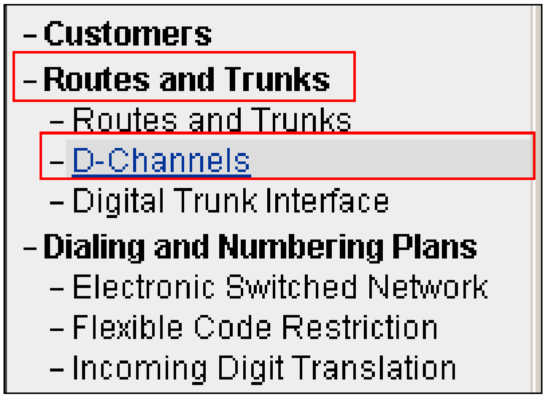
SIP URI Map:

Public E.164 domain names		Private domain names	
National:		UDP:	udp
Subscriber:		CDP:	
Special number:		Special number:	PrivateSpecial
Unknown:		Vacant number:	PrivateUnknown
		Unknown:	

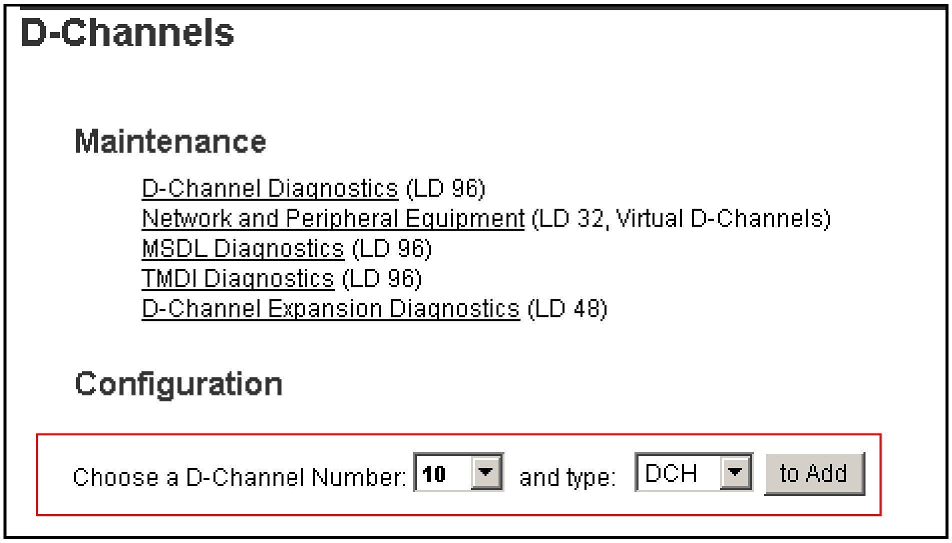
Save and transmit these Node properties to complete the SIPGw configuration (not shown).

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 below.


- 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

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


D-Channels

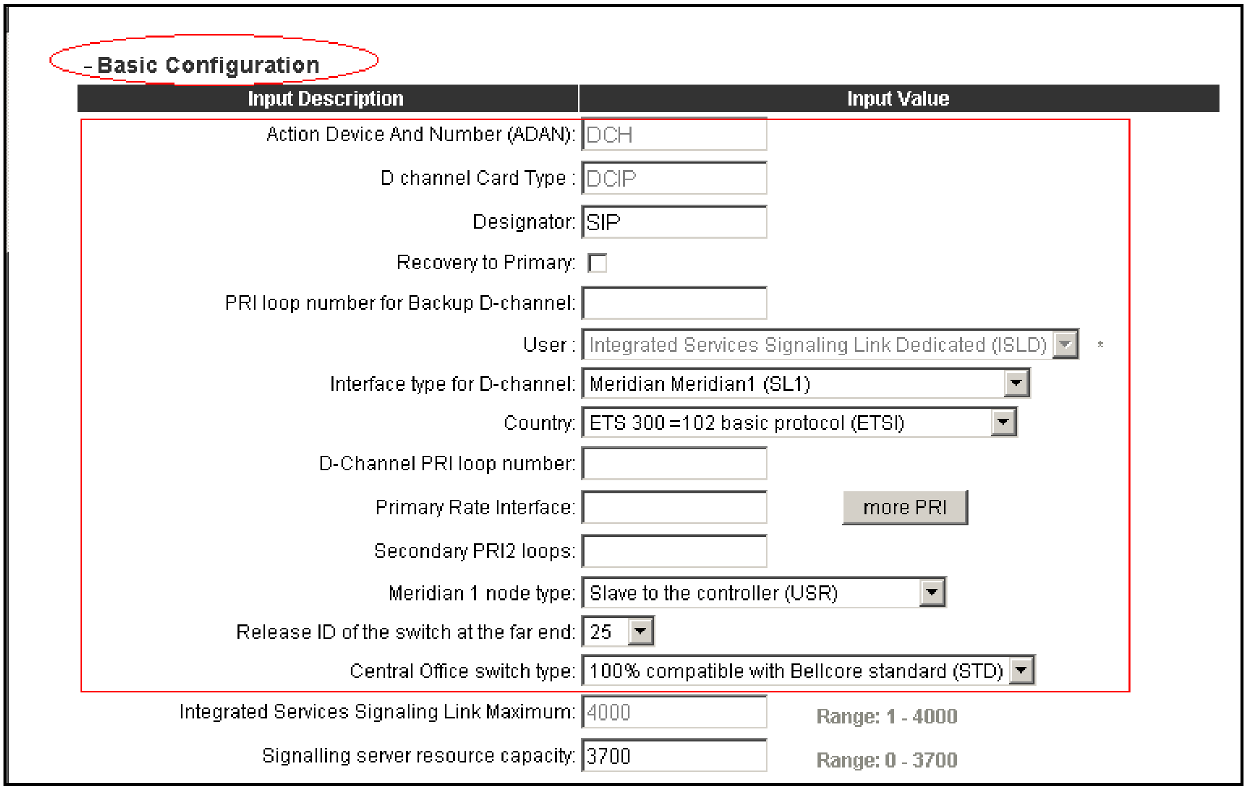
Maintenance

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

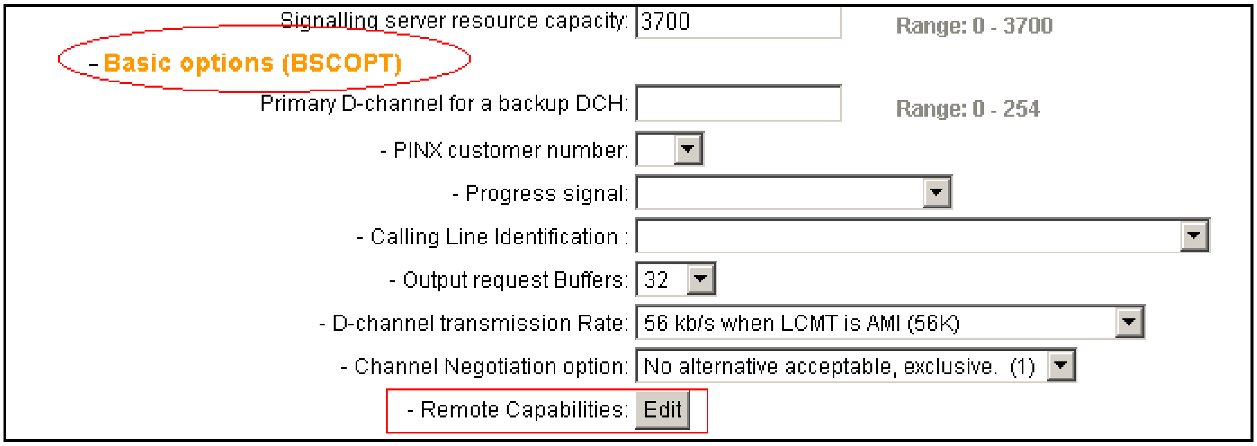
Configure the **Basic Configuration** values for the D-Channel as shown below.



- Basic Configuration

Input Description	Input Value
Action Device And Number (ADAN):	DCH
D channel Card Type :	DCIP
Designator:	SIP
Recovery to Primary:	□
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:	more PRI
Secondary PRI2 loops:	
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 Range: 1 - 4000
Signalling server resource capacity:	3700 Range: 0 - 3700

To edit the **Remote Capabilities** of the D-Channel, click on the **Edit** button in the **Basic options** section as shown 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:

- Progress signal:

- Calling Line Identification :

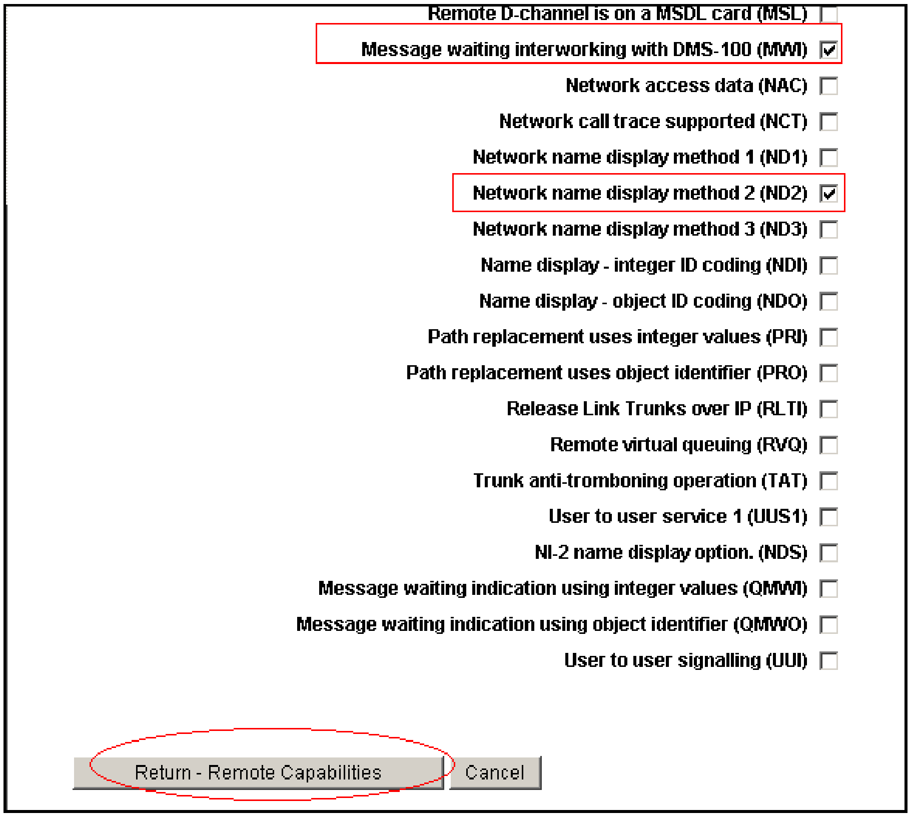
- Output request Buffers: 32

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

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

- Remote Capabilities: Edit

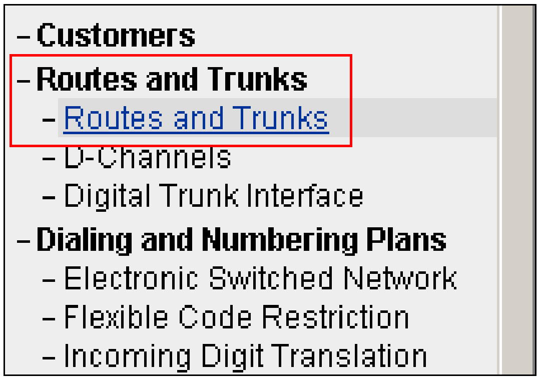
Select the boxes for the desired Remote Capabilities as shown below. Click on **Return - Remote Capabilities** button to return back to the main screen to complete the D-Channel configuration.



Remote D-channel is on a MSDL card (MSL) □
Message waiting interworking with DMS-100 (MWI) ☑
Network access data (NAC) □
Network call trace supported (NCT) □
Network name display method 1 (ND1) □
Network name display method 2 (ND2) ☑
Network name display method 3 (ND3) □
Name display - integer ID coding (NDI) □
Name display - object ID coding (NDO) □
Path replacement uses integer values (PRI) □
Path replacement uses object identifier (PRO) □
Release Link Trunks over IP (RLTI) □
Remote virtual queuing (RVQ) □
Trunk anti-tromboning operation (TAT) □
User to user service 1 (UUS1) □
NI-2 name display option. (NDS) □
Message waiting indication using integer values (QMWI) □
Message waiting indication using object identifier (QMWO) □
User to user signalling (UUI) □

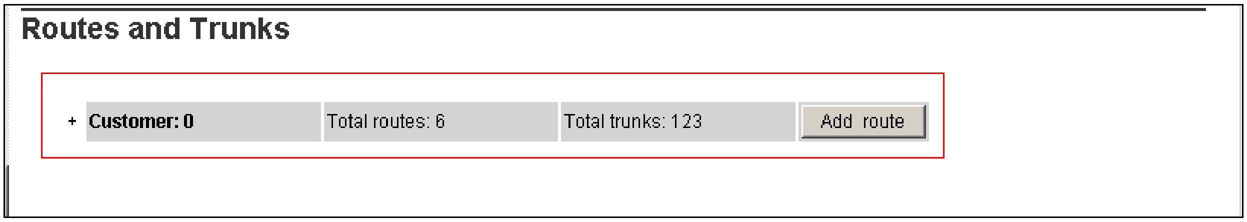
5.4. Configuring Routes and Trunks

This section explains the configuration of the SIP routes and trunks which will be used by Communication Server 1000 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 below.



- 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

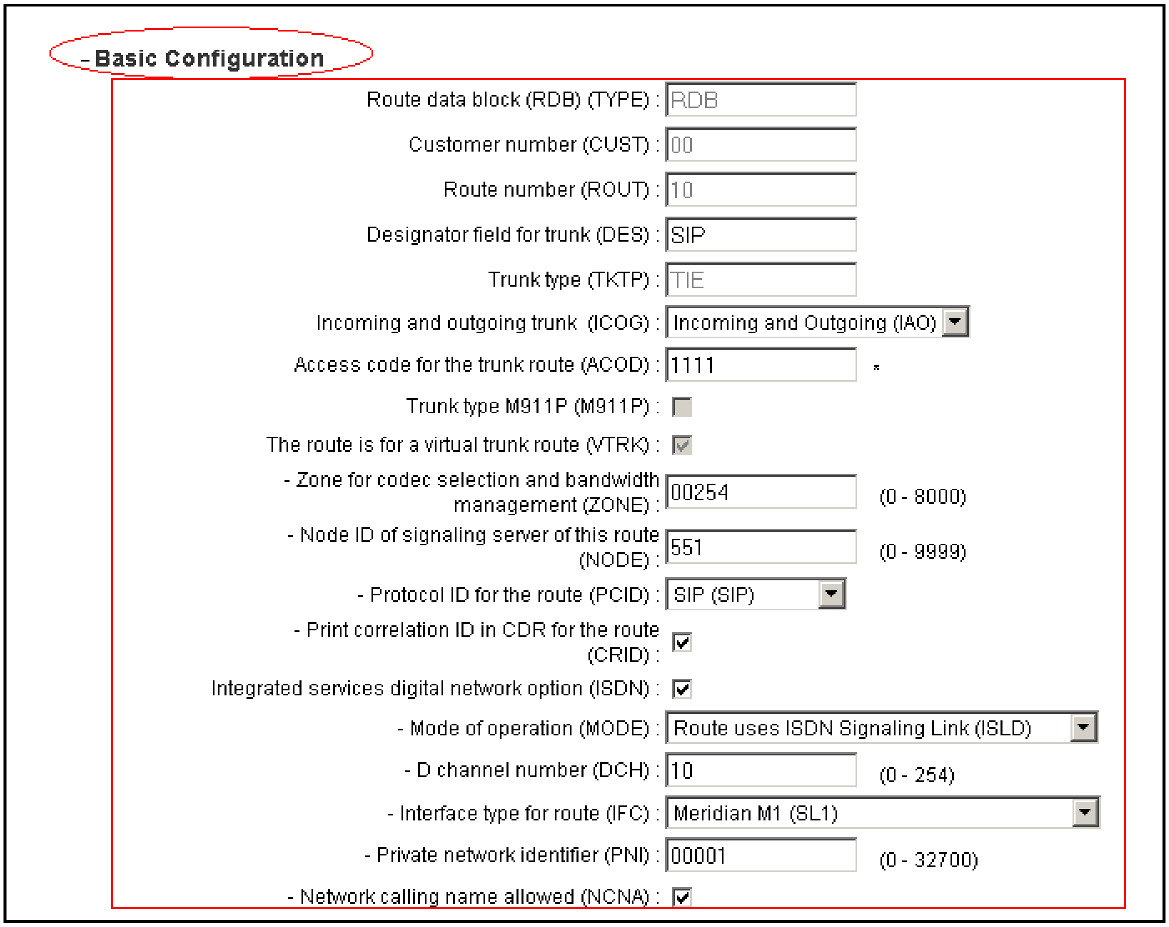
From the **Routes and Trunks** screen click on the **Add route** button to start configuring a new route as shown below.



Routes and Trunks

+ Customer: 0 | Total routes: 6 | Total trunks: 123 | Add route

During compliance testing **Route number 10** was added. Select the values from the drop down menu and configure the values as shown in the next three screens 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) : □

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

- 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) : ☑

Integrated services digital network option (ISDN) : ☑

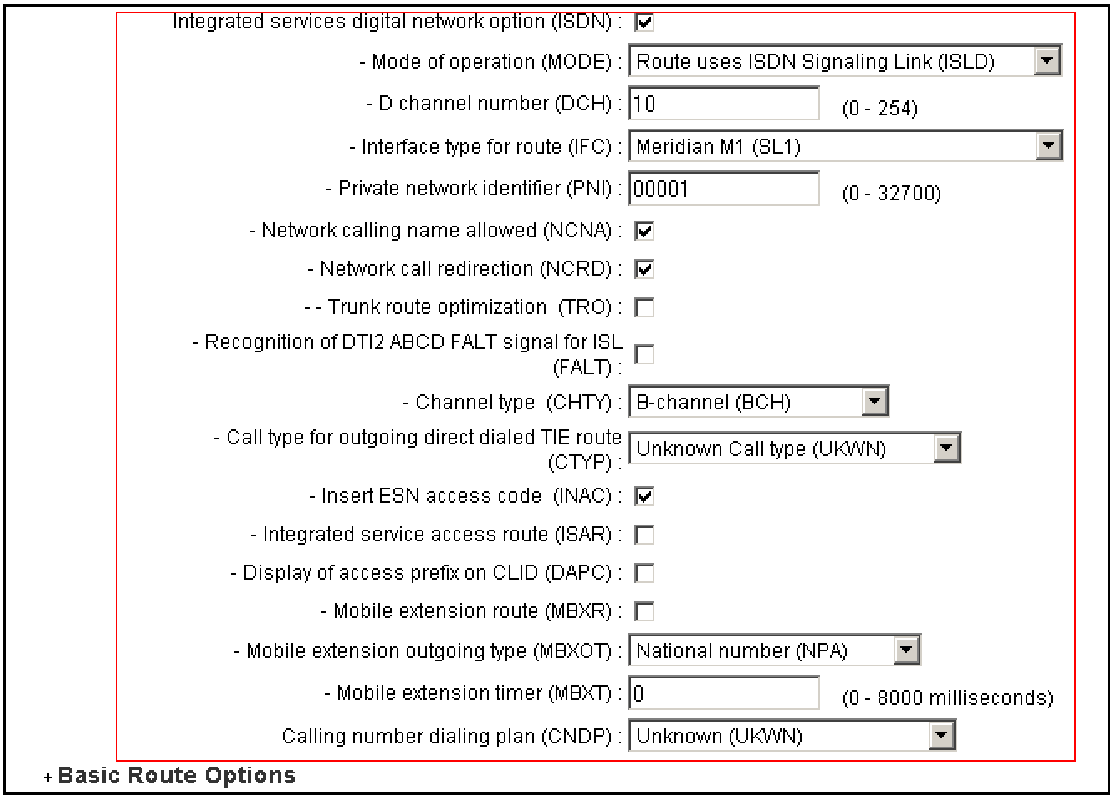
- Mode of operation (MODE) : Route uses ISDN Signaling Link (ISLD)

- D channel number (DCH) : 10 (0 - 254)

- Interface type for route (IFC) : Meridian M1 (SL1)

- Private network identifier (PNI) : 00001 (0 - 32700)

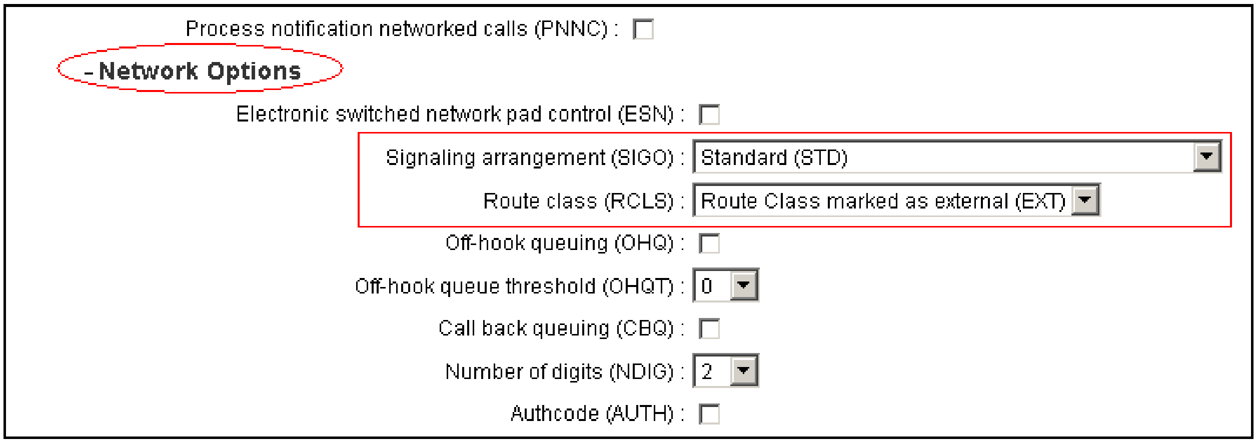
- Network calling name allowed (NCNA) : ☑



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) : ☑
- Network call redirection (NCRD) : ☑
- - Trunk route optimization (TRO) : □
- Recognition of DTI2 ABCD FALT signal for ISL (FALT) : □
- Channel type (CHTY) : B-channel (BCH)
- Call type for outgoing direct dialed TIE route (CTYP) : Unknown Call type (UKWN)
- 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) : Unknown (UKWN)



Process notification networked calls (PNNC) : □

Electronic switched network pad control (ESN) : □

Signaling arrangement (SIGO) : Standard (STD)

Route class (RCLS) : Route Class marked as external (EXT)

Off-hook queuing (OHQ) : □

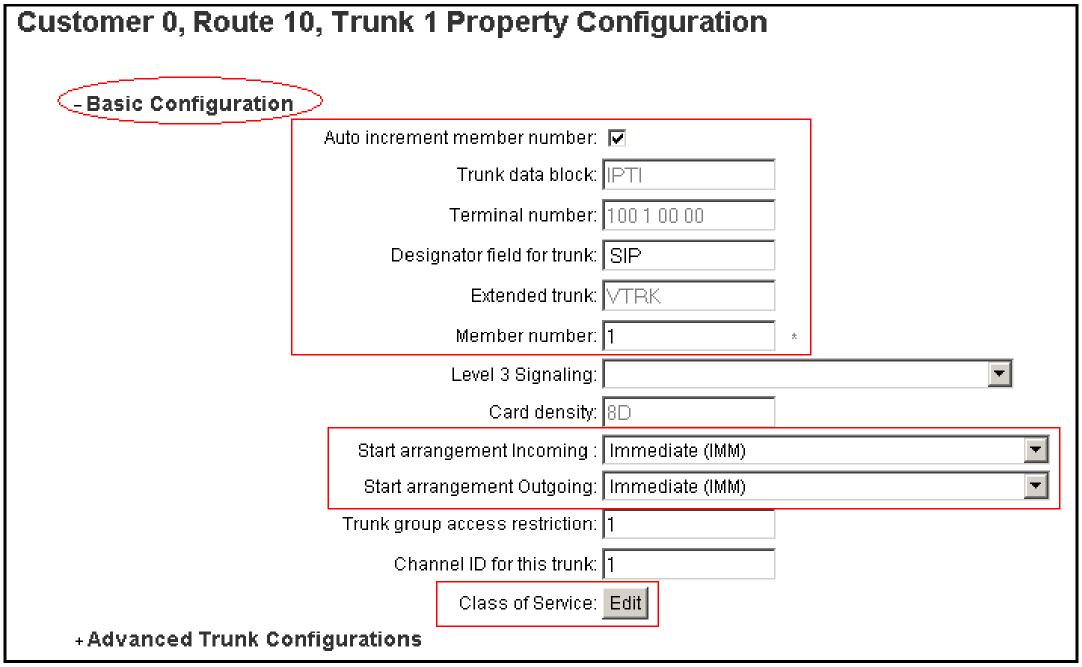
Off-hook queue threshold (OHQT) : 0

Call back queuing (CBQ) : □

Number of digits (NDIG) : 2

Authcode (AUTH) : □

Configure the trunk values as shown 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)

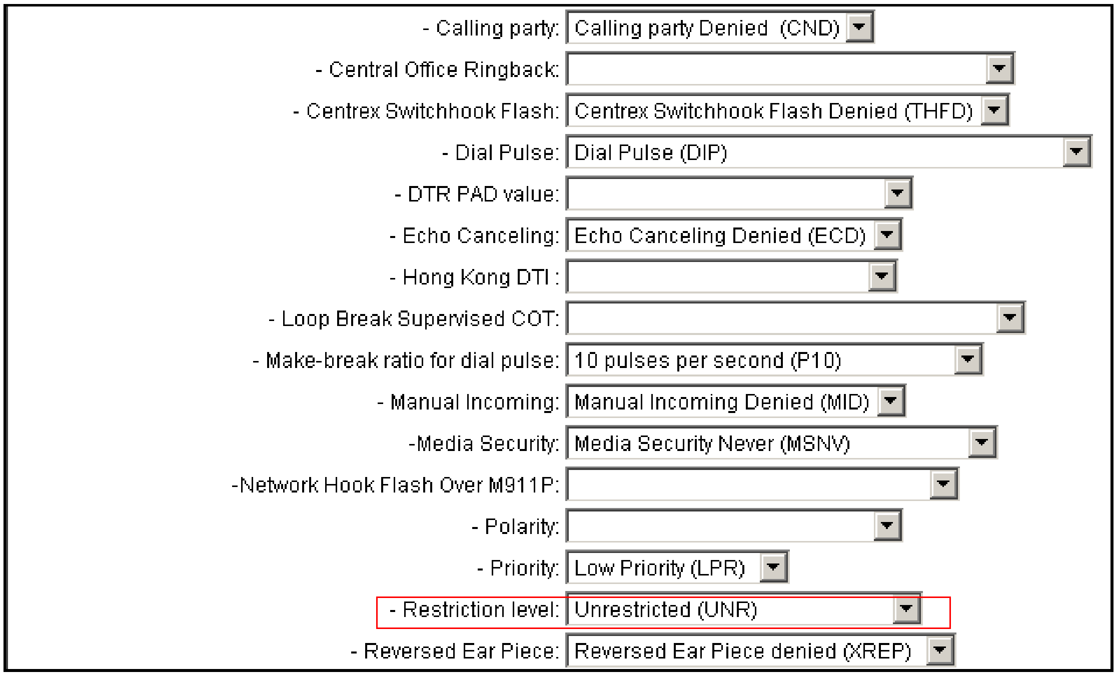
Trunk group access restriction: 1

Channel ID for this trunk: 1

Class of Service: Edit

+ Advanced Trunk Configurations

The screen below shows the **Class of Service** values selected for the compliance testing from the drop down menu. Click on the **Return Class of Service** (not shown) button to complete the trunk configuration.



- 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:

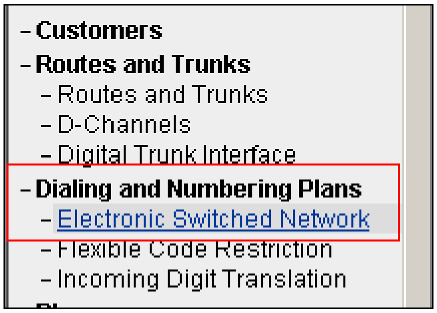
- Priority: Low Priority (LPR)

- Restriction level: Unrestricted (UNR)

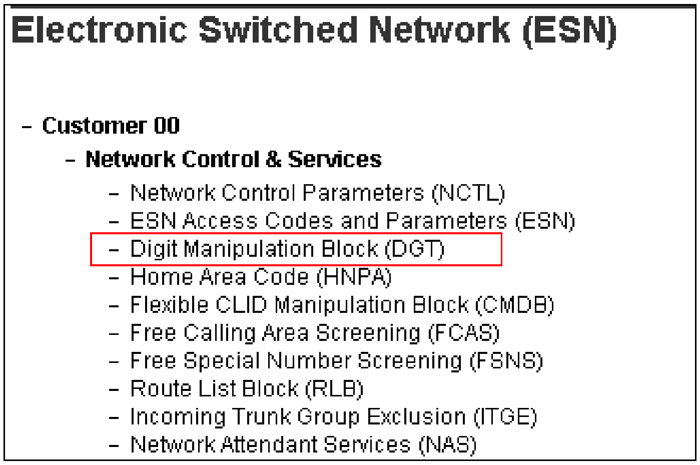
- Reversed Ear Piece: Reversed Ear Piece denied (XREP)

5.5. Configuring Digit Manipulation Block

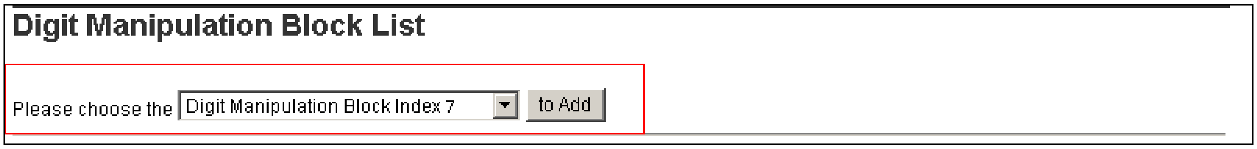
This section explains the digit manipulation block that is to be configured in the Communication Server 1000 dialing plan for its users to communicate with the Unigy system. From the EM navigator pane, navigate to **Dialing and Numbering Plans → Electronic Switched Network** as shown below.


- 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

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


Electronic Switched Network (ESN)
- Customer 00
- Network Control & Services
- Network Control Parameters (NCTL)
- ESN Access Codes and Parameters (ESN)
- Digit Manipulation Block (DGT)
- Home Area Code (HNPA)
- Flexible CLID Manipulation Block (CMDB)
- Free Calling Area Screening (FCAS)
- Free Special Number Screening (FSNS)
- Route List Block (RLB)
- Incoming Trunk Group Exclusion (ITGE)
- Network Attendant Services (NAS)

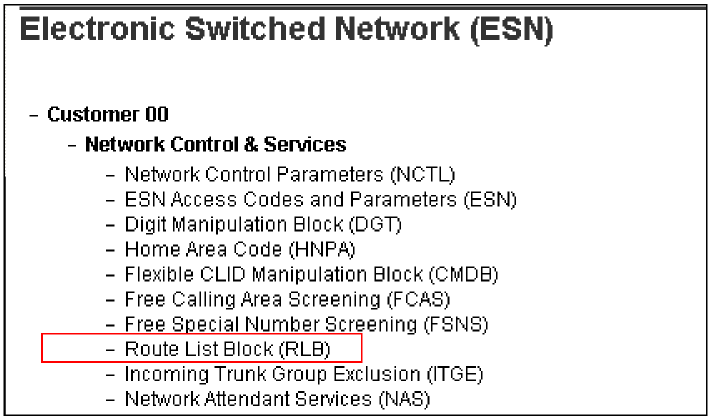
The screen below shows the Digit Manipulation Block Index users can add, which is **Digit Manipulation Block Index 7** (or any Index number other than the default value of **0**). During compliance testing, a **Digit Manipulation Block Index** of **0** was used which is already added in the Communication Server 1000 system by default.


Digit Manipulation Block List

Please choose the Digit Manipulation Block Index 7

5.6. Configuring Route List Block

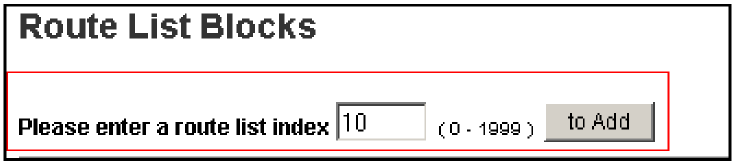
This section explains the route list block that is to be configured in the Communication Server 1000 dialing plan for its users to communicate with the Unigy system. From the EM navigator pane, navigate to **Dialing and Numbering Plans → Electronic Switched Network** as shown in **Section 5.5** above. Click on **Route List Block (RLB)** option as shown below.



Electronic Switched Network (ESN)

- Customer 00
  - Network Control & Services
    - Network Control Parameters (NCTL)
    - ESN Access Codes and Parameters (ESN)
    - Digit Manipulation Block (DGT)
    - Home Area Code (HNPA)
    - Flexible CLID Manipulation Block (CMDB)
    - Free Calling Area Screening (FCAS)
    - Free Special Number Screening (FSNS)
    - Route List Block (RLB)
    - Incoming Trunk Group Exclusion (ITGE)
    - Network Attendant Services (NAS)

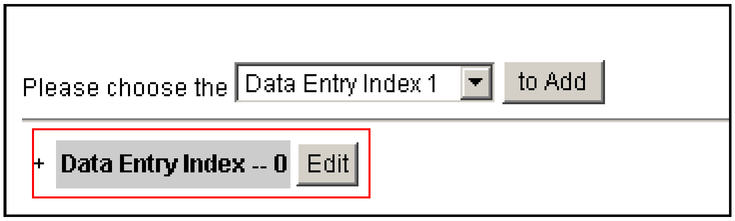
Start adding a **route list index** as shown below. During compliance testing, list index **10** was added. Click on **to Add** to continue.



Route List Blocks

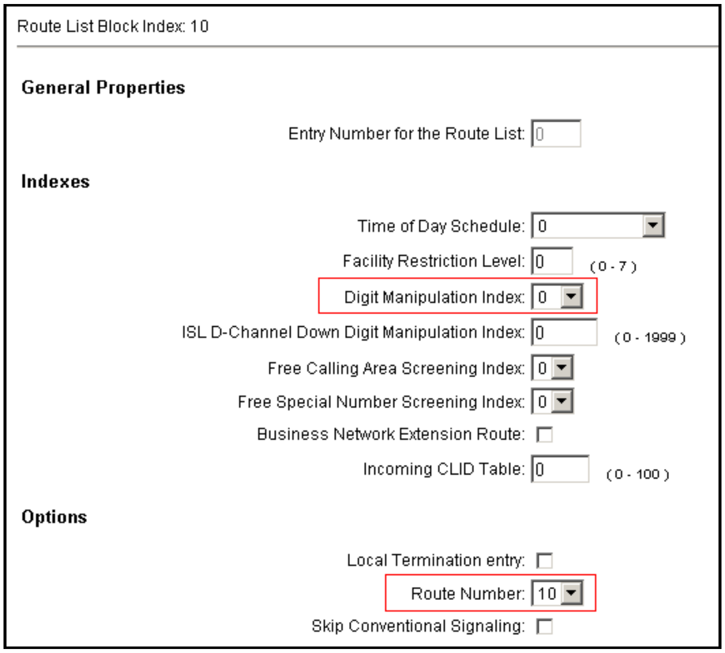
Please enter a route list index: 10 (0 - 1999)

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



Please choose the: Data Entry Index 1

Screen 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 on **Submit** (not shown) to complete the configuration.



Route List Block Index: 10

General Properties

Entry Number for the Route List: 0

Indexes

Time of Day Schedule: 0

Facility Restriction Level: 0 (0 - 7)

Digit Manipulation Index: 0

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

Free Calling Area Screening Index: 0

Free Special Number Screening Index: 0

Business Network Extension Route: □

Incoming CLID Table: 0 (0 - 100)

Options

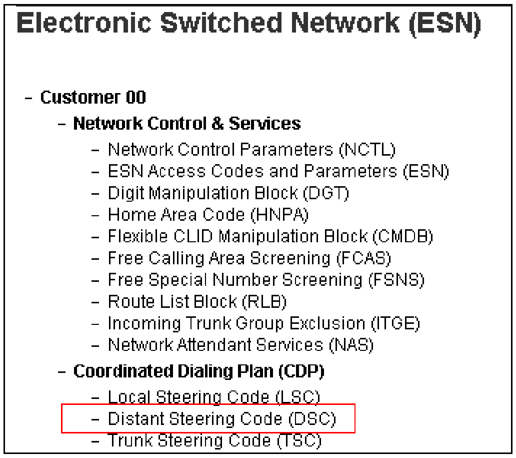
Local Termination entry: □

Route Number: 10

Skip Conventional Signaling: □

5.7. Configuring Distant Steering Code

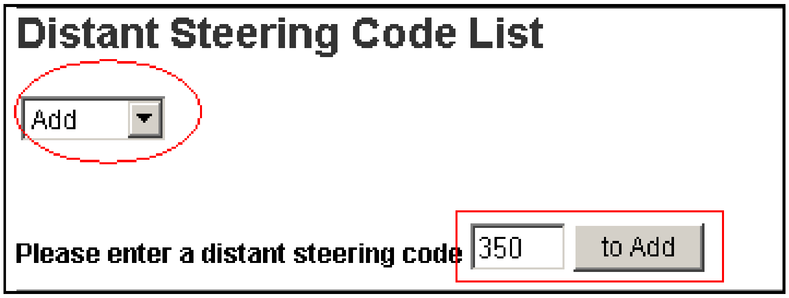
This section explains the **Distant Steering Code** that is to be configured in the Communication Server 1000 dialing plan for its users to communicate with the Unigy system. From the EM navigator pane, navigate to **Dialing and Numbering Plans → Electronic Switched Network** as shown in **Section 5.5** above. Click on the **Distant Steering Code (DSC)** option as shown below.



Electronic Switched Network (ESN)

- Customer 00
  - Network Control & Services
    - Network Control Parameters (NCTL)
    - ESN Access Codes and Parameters (ESN)
    - Digit Manipulation Block (DGT)
    - Home Area Code (HNPA)
    - Flexible CLID Manipulation Block (CMDB)
    - Free Calling Area Screening (FCAS)
    - Free Special Number Screening (FSNS)
    - Route List Block (RLB)
    - Incoming Trunk Group Exclusion (ITGE)
    - Network Attendant Services (NAS)
  - Coordinated Dialing Plan (CDP)
    - Local Steering Code (LSC)
    - Distant Steering Code (DSC)
    - Trunk Steering Code (TSC)

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

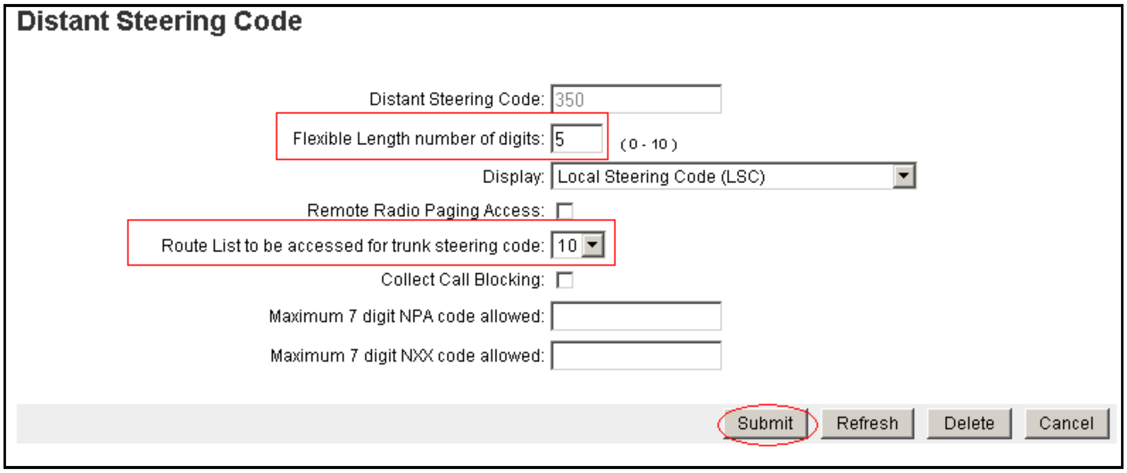


Distant Steering Code List

Add

Please enter a distant steering code 350

Enter the values as shown 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:

6. Configure Routing using Avaya Aura® System Manager

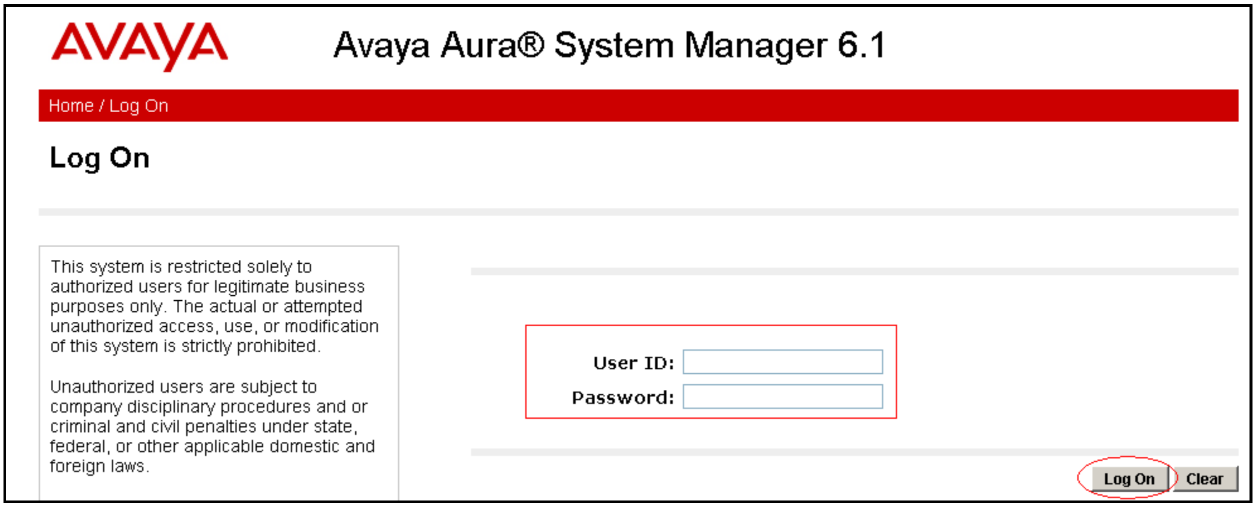
This section provides the procedures for configuring routing using Avaya Aura ® System Manager. The procedures include the following areas:

- 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). The screen below shows the Log On Screen. Type the required **User ID** and **Password** credentials and click **Log On** to continue.

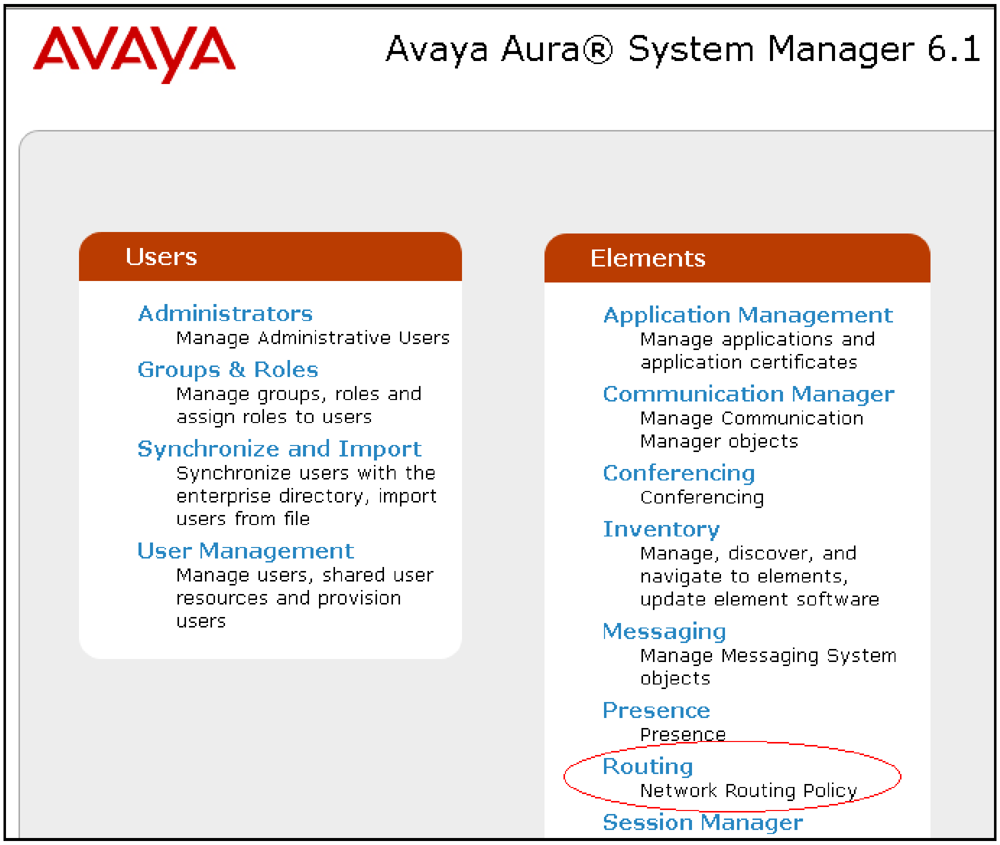


This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

User ID:
Password:

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


Avaya Aura® System Manager 6.1

Users

Administrators
Manage Administrative Users

Groups & Roles
Manage groups, roles and assign roles to users

Synchronize and Import
Synchronize users with the enterprise directory, import users from file

User Management
Manage users, shared user resources and provision users

Elements

Application Management
Manage applications and application certificates

Communication Manager
Manage Communication Manager objects

Conferencing
Conferencing

Inventory
Manage, discover, and navigate to elements, update element software

Messaging
Manage Messaging System objects

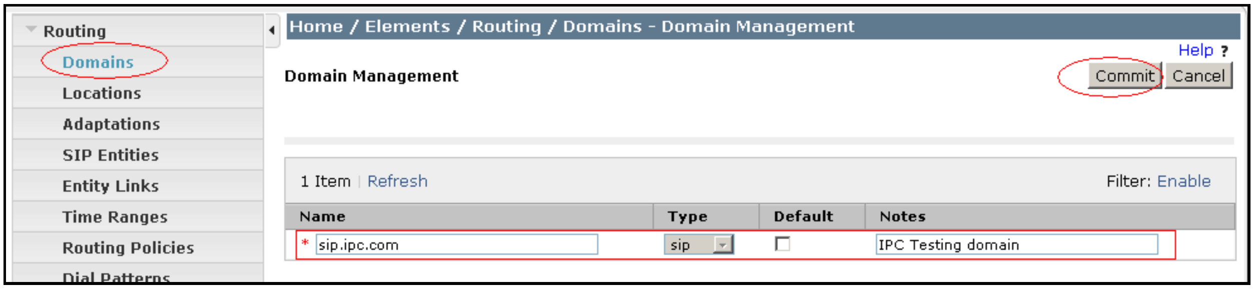
Presence
Presence

Routing
Network Routing Policy

Session Manager

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 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.



Home / Elements / Routing / Domains - Domain Management

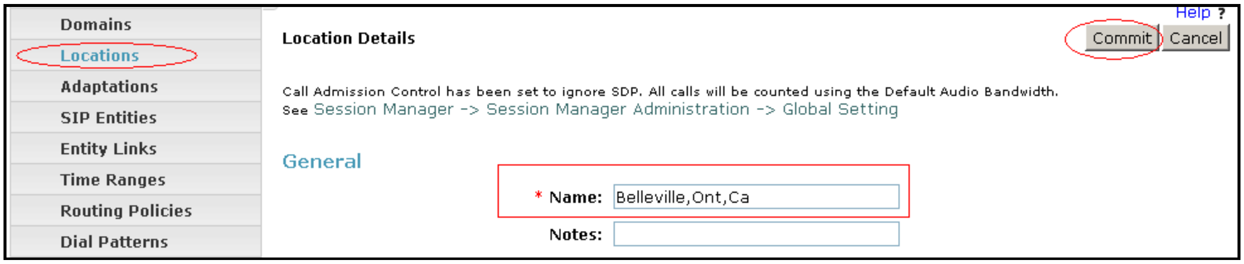
Domain Management

1 Item

Name	Type	Default	Notes
* sip.ipc.com	sip	□	IPC Testing domain

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 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.



Location Details

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.
See Session Manager -> Session Manager Administration -> Global Setting

General

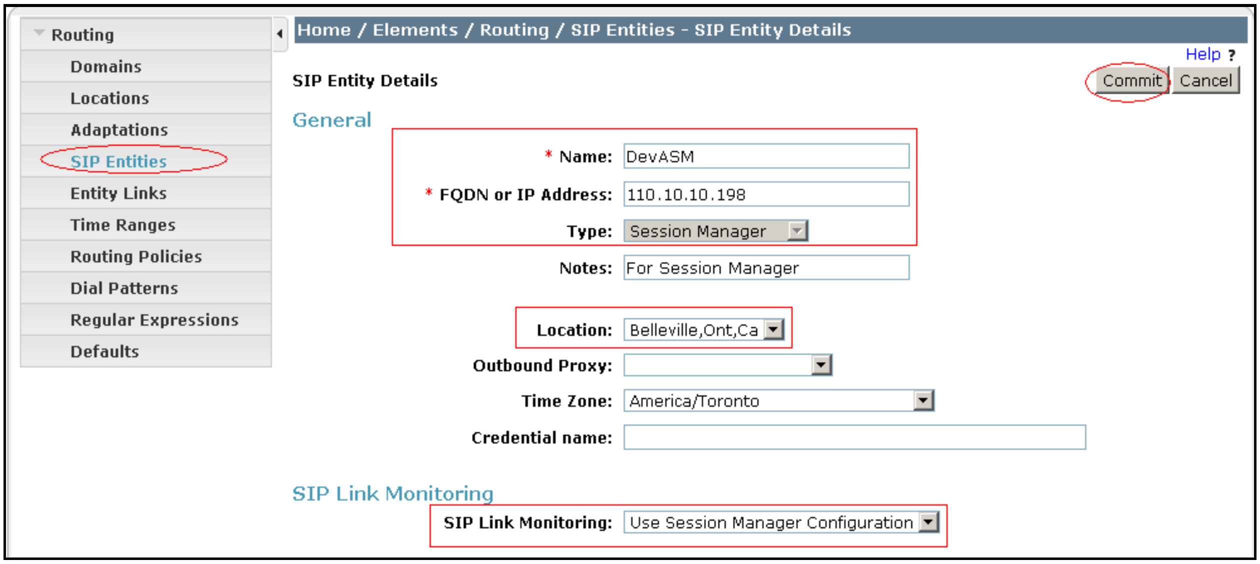
* Name: Belleville,Ont,Ca

Notes:

6.4. Adding SIP Entities

This section explains the adding of SIP entities to Session Manager, Unigy System and the Communication Server 1000 system routing. To add SIP Entities, select S**IP Entities** from the left hand window of the Routing screen and click on **New** (not shown).

The next two screens 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 the 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.



Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details

General

* Name: DevASM

* FQDN or IP Address: 110.10.10.198

Type: Session Manager

Notes: For Session Manager

Location: Belleville,Ont,Ca

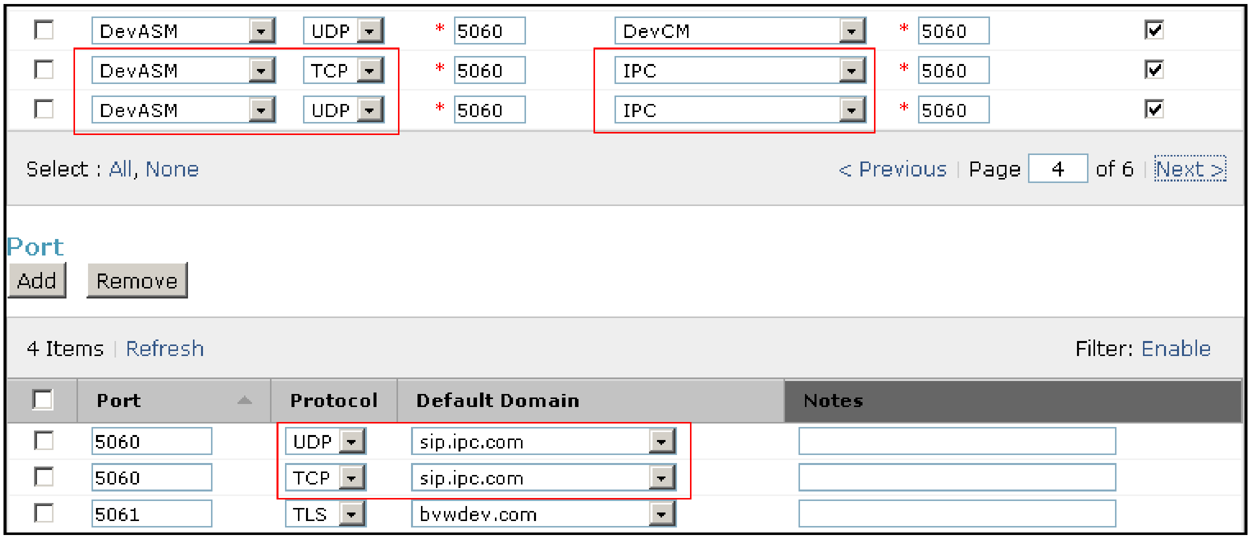
Outbound Proxy:

Time Zone: America/Toronto

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration



□	DevASM	UDP	* 5060	DevCM	* 5060	☑
□	DevASM	TCP	* 5060	IPC	* 5060	☑
□	DevASM	UDP	* 5060	IPC	* 5060	☑

Select : All, None

< Previous | Page 4 of 6 | Next >

Port

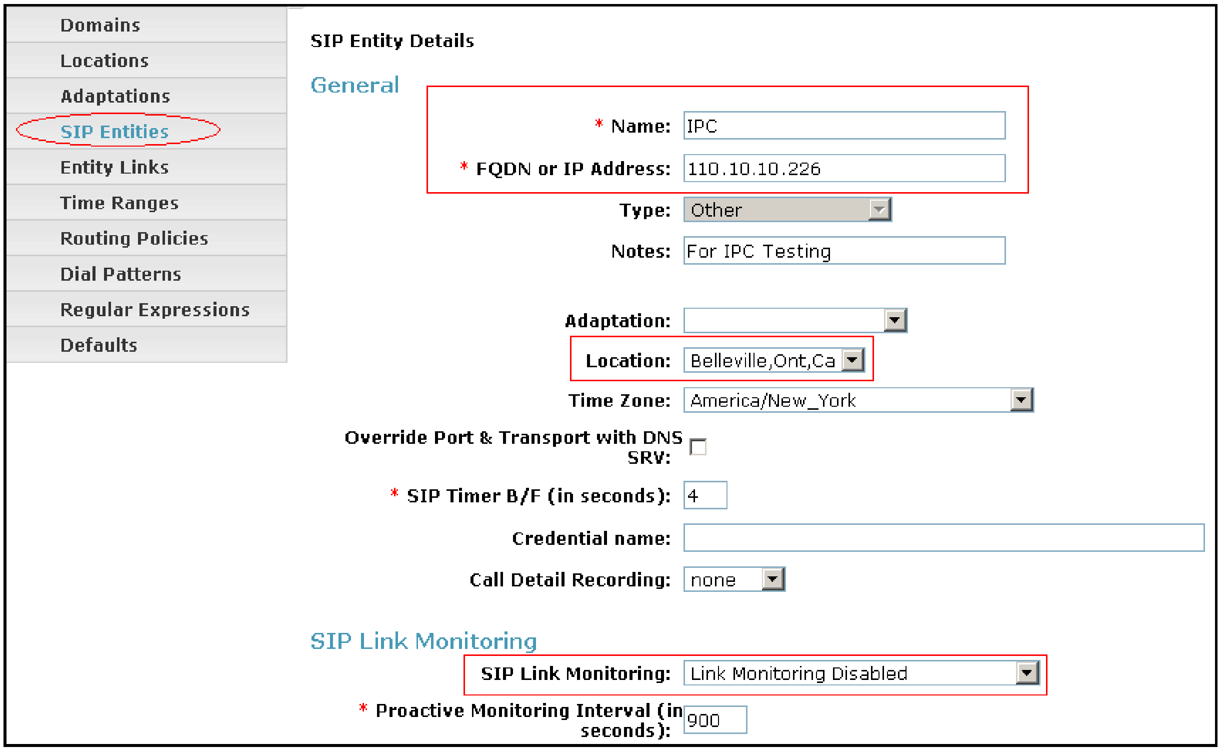
Add Remove

4 Items | Refresh

Filter: Enable

□	Port	Protocol	Default Domain	Notes
□	5060	UDP	sip.ipc.com	
□	5060	TCP	sip.ipc.com	
□	5061	TLS	bvwdev.com	

The next two screens 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** (not shown) since the 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

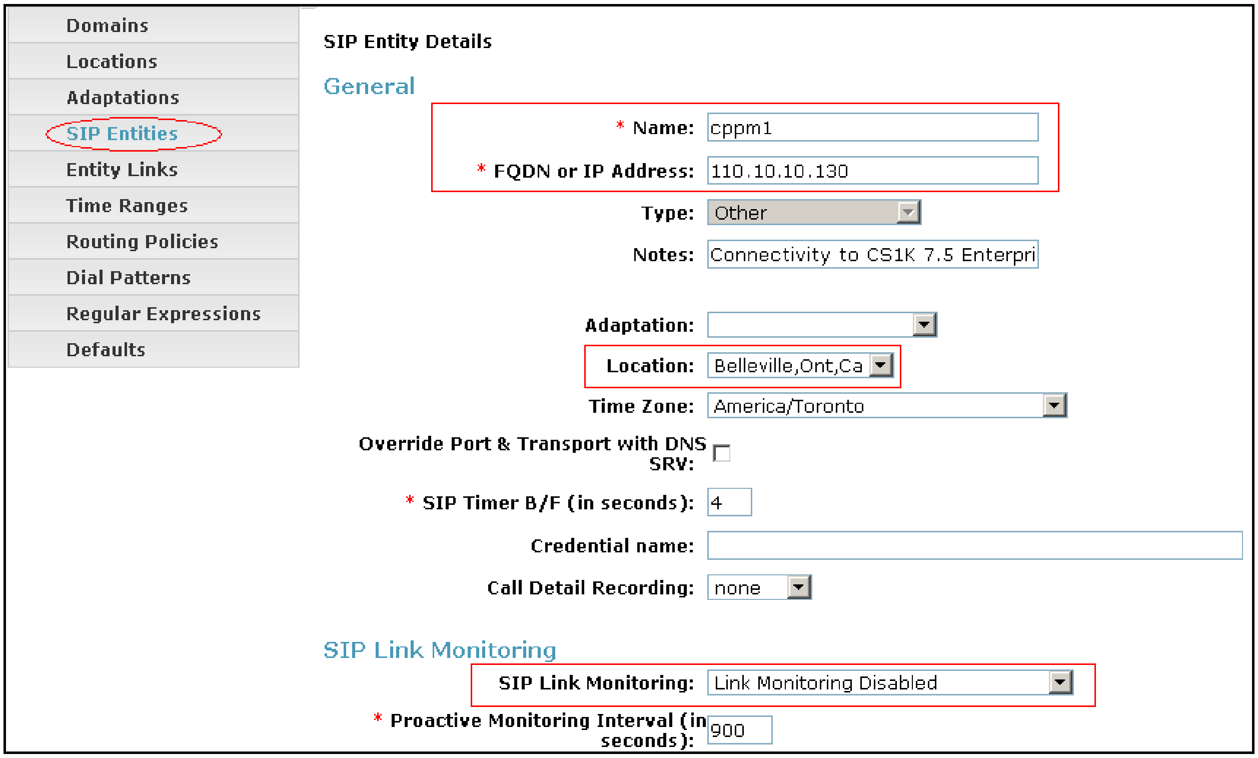
General

* Name:	IPC
* FQDN or IP Address:	110.10.10.226
Type:	Other
Notes:	For IPC Testing
Adaptation:	
Location:	Belleville,Ont,Ca
Time Zone:	America/New_York
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

The next two screens below show the SIP Entity Details for the Communication Server 1000 System routing. The **FQDN or IP Address** of **110.10.10.130** is the Node IP address of the SIP Signaling Gateway of the Communication Server 1000 System. Also note that both **TCP** and **UDP** protocols need to be selected in the Entity Links secton for **cppm1** since the 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.



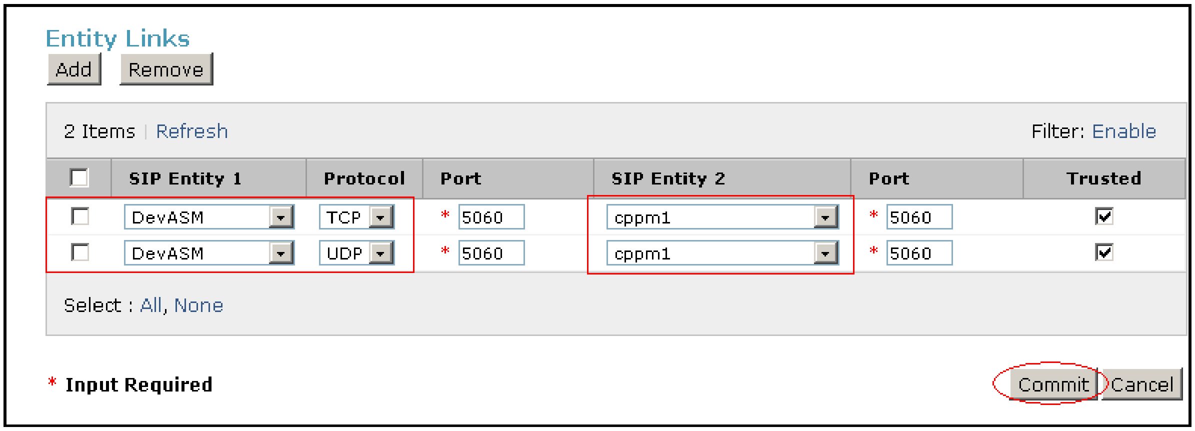
SIP Entity Details

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



Entity Links

2 Items

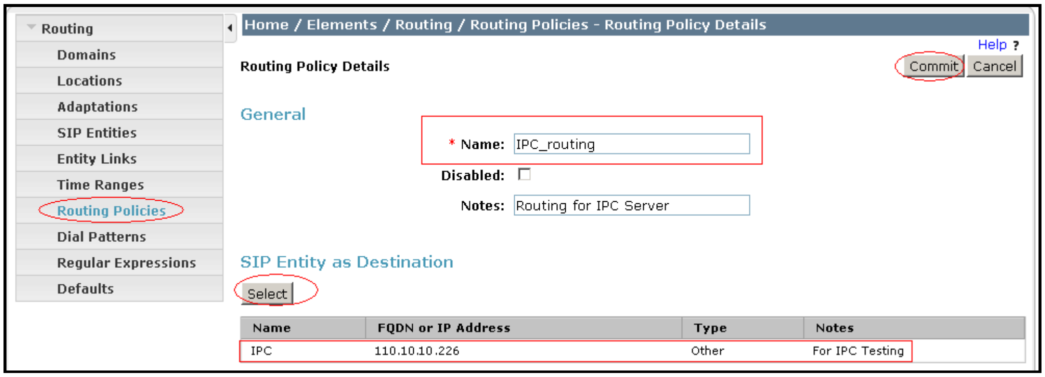
□	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
□	DevASM	TCP	* 5060	cppm1	* 5060	☑
□	DevASM	UDP	* 5060	cppm1	* 5060	☑

* Input Required

6.5. Adding Routing Policies

This section explains the Routing Policy configuration for the Unigy and Communication Server 1000 Systems. To add a routing policy, select **Routing Policies** from the left hand window of the Routing screen and click on **New** (not shown).

The next two screens below show the Routing Policy Details for the Unigy System. Select the Unigy System as the **SIP Entity as 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 Policy Details

General

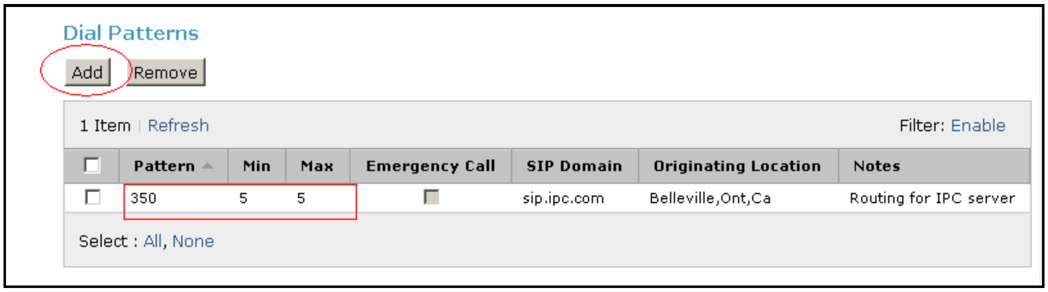
* Name: IPC_routing

Disabled: □

Notes: Routing for IPC Server

SIP Entity as Destination

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



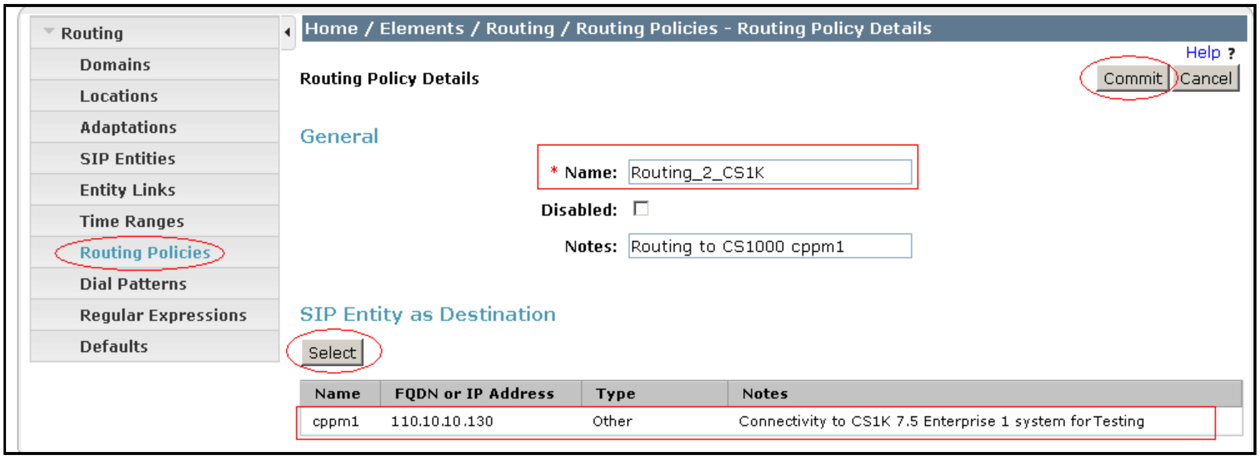
Dial Patterns

1 Item

□	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
□	350	5	5	□	sip.ipc.com	Belleville,Ont,Ca	Routing for IPC server

The next two screens below show the Routing Policy Details for the Communication Server 1000 System. Select the Communication Server 1000 System as the **SIP Entity as Destination** and add the Dial Pattern associated with the Communication Server 1000 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

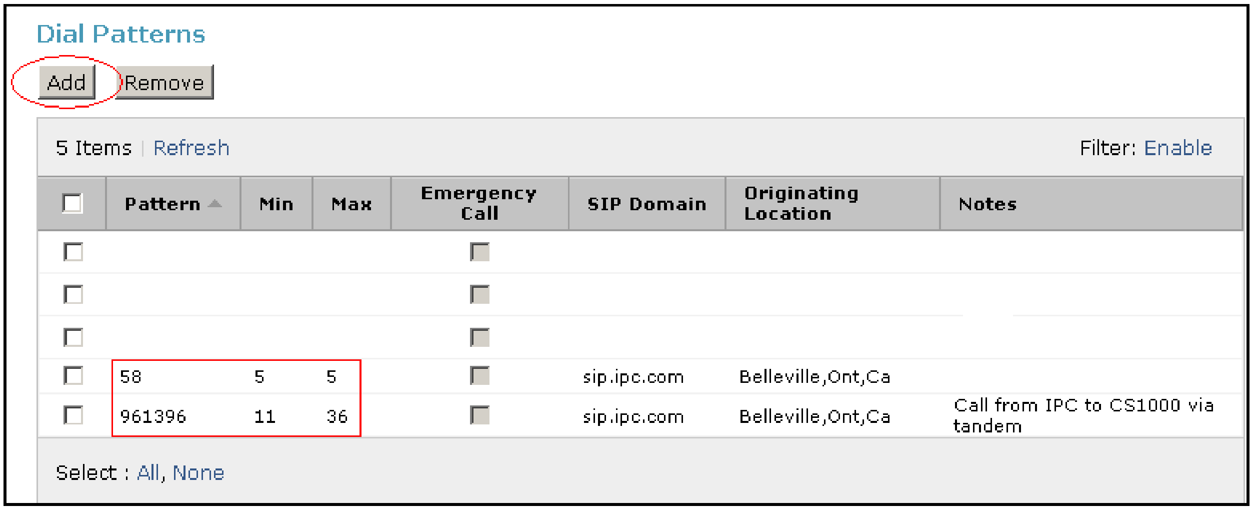
* Name: Routing_2_CS1K

Disabled: □

Notes: Routing to CS1000 cppm1

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
cppm1	110.10.10.130	Other	Connectivity to CS1K 7.5 Enterprise 1 system forTesting



Dial Patterns

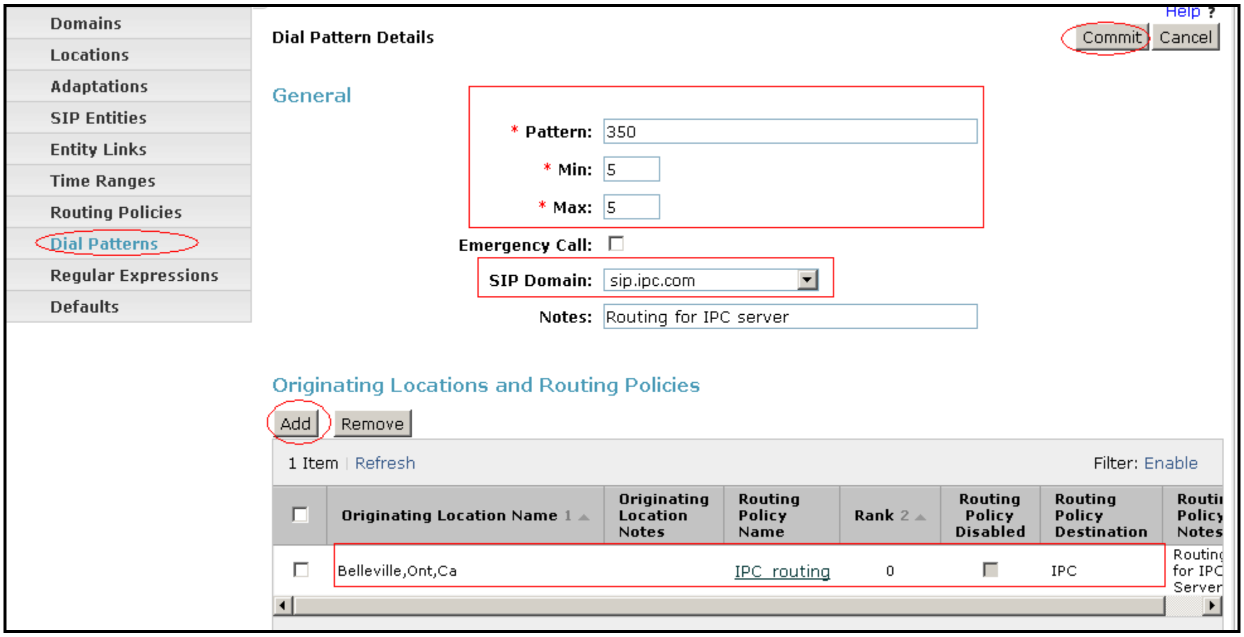
5 Items | Refresh

□	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

6.6. Adding Dial Patterns

This section explains the steps to add a Dial Pattern for the Unigy and Communication Server 1000 systems. To add a dial pattern, select **Dial Patterns** from the left hand window of the Routing screen and click on **New** (not shown).

The screen below 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

1 Item | Refresh

□	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routi Policy Notes
□	Belleville,Ont,Ca		IPC_routing	0	□	IPC	Routing for IPC Server

7. Configure IPC Converged Communications Manager

This section provides the procedures for configuring IPC Converged Communications 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.

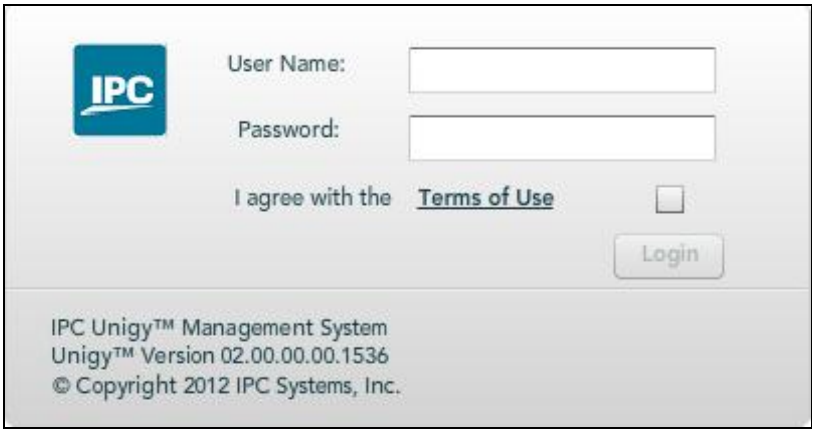
The configuration of Converged Communications Manager is typically performed by IPC installation technicians. The procedural steps are presented in these Application Notes for informational purposes. For detailed administration and configuration information for the Unigy system refer to the reference documentation in **Section 11**.

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 Converged Communications Manager. Log in using the appropriate credentials.

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

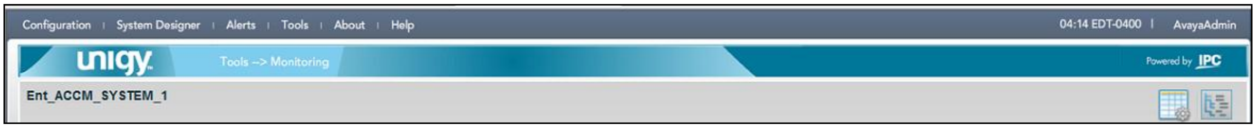
In the subsequent screen (not shown), click **Continue**.



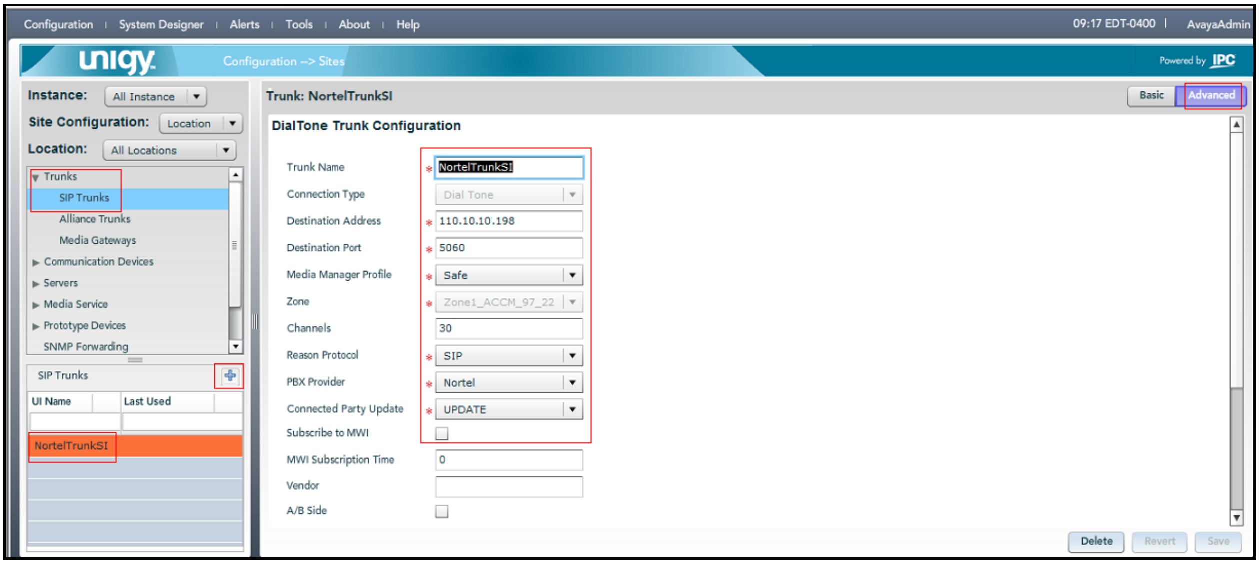
IPC Unigy™ Management System
Unigy™ Version 02.00.00.00.1536
© Copyright 2012 IPC Systems, Inc.

7.2. Administer SIP Trunks

The screen as shown below is displayed next. Select **Configuration → Sites** (not shown) from the top menu.



The two screens 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 **NortelTrunkSI** 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** to complete the configuration.



Instance: All Instance

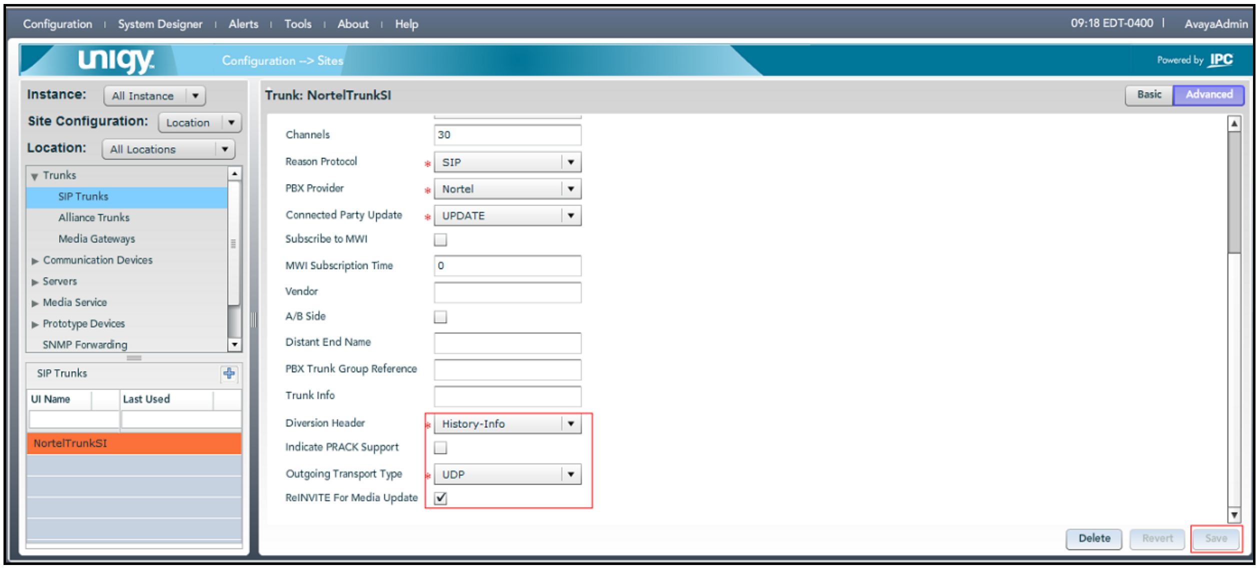
Site Configuration: Location

Location: All Locations

Trunk: NortelTrunkSI

DialTone Trunk Configuration

Trunk Name	* NortelTrunkSI
Connection Type	Dial Tone
Destination Address	* 110.10.10.198
Destination Port	* 5060
Media Manager Profile	* Safe
Zone	* Zone1_ACCM_97_22
Channels	30
Reason Protocol	* SIP
PBX Provider	* Nortel
Connected Party Update	* UPDATE
Subscribe to MWI	☐
MWI Subscription Time	0
Vendor	
A/B Side	☐



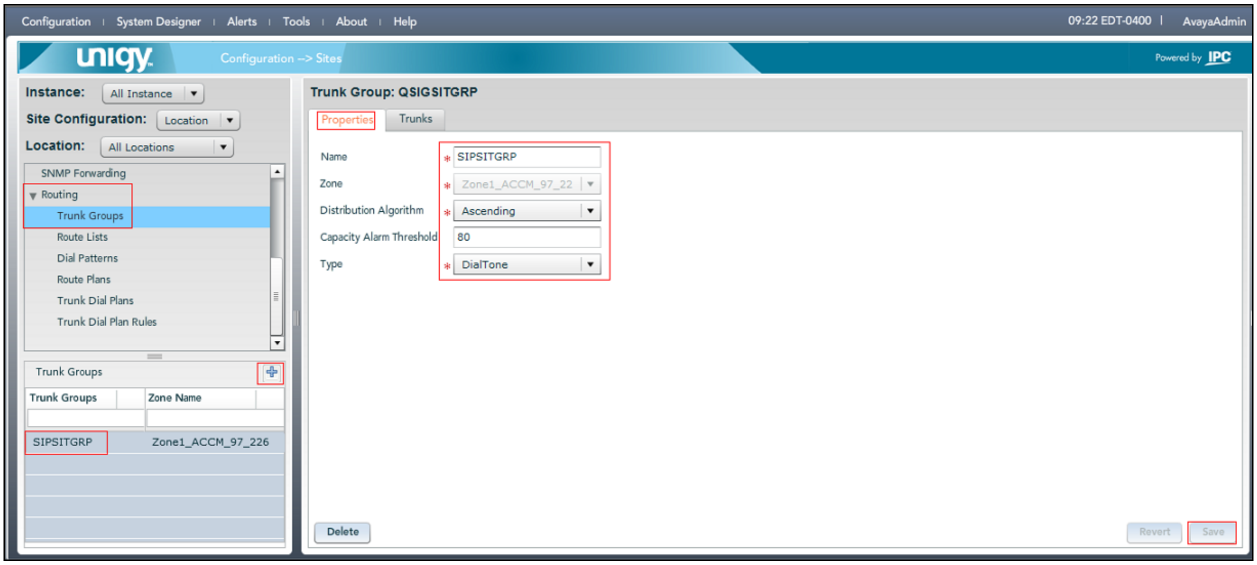
Trunk: NortelTrunkSI

Channels	30
Reason Protocol *	SIP
PBX Provider *	Nortel
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	☑

7.3. Administer Trunk Groups

From **Configuration → Sites**, 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 screen below.

The **Trunk Group** screen is displayed in the right pane. Select **Properties** tab, the screen shows the values configured for compliance testing. Click on **Save** to complete the configuration.

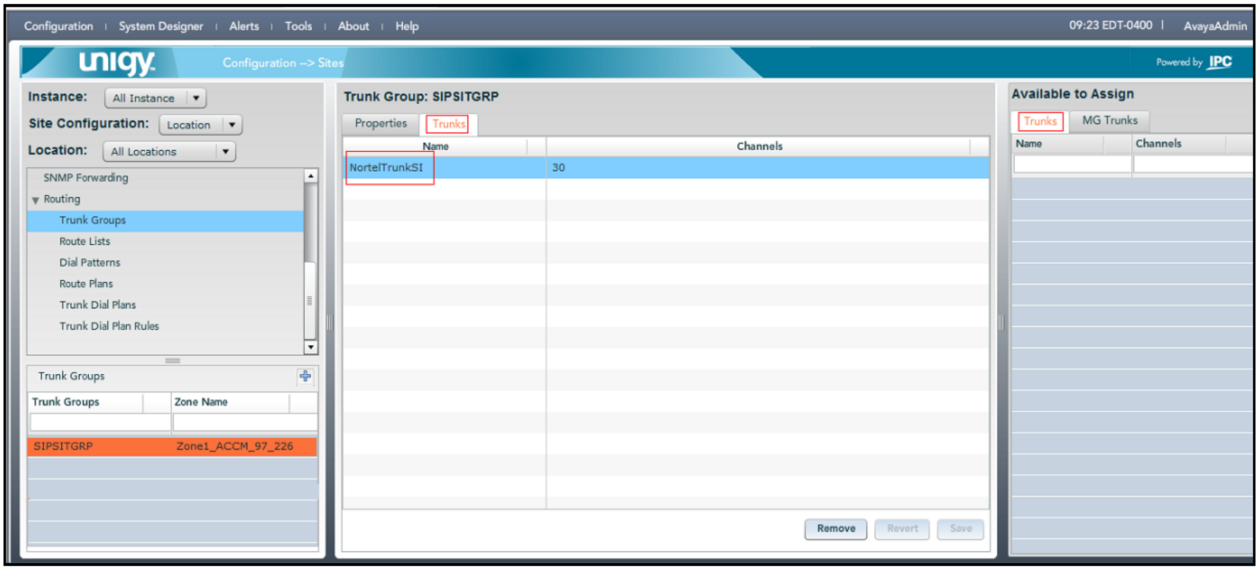


Trunk Groups	Zone Name
SIPSITGRP	Zone1_ACCM_97_226

Trunk Group: QSIGSITGRP

Name *	SIPSITGRP
Zone *	Zone1_ACCM_97_22
Distribution Algorithm *	Ascending
Capacity Alarm Threshold	80
Type *	DialTone

Select the **Trunks** tab in the right pane. The screen is updated with three panes. In the new right pane, select the **Trunks** tab as shown below. 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** to complete the configuration.



Instance: All Instance

Site Configuration: Location

Location: All Locations

Trunk Group: SIPSITGRP

Name	Channels
NortelTrunkSI	30

Trunk Groups

Trunk Groups	Zone Name
SIPSITGRP	Zone1_ACCM_97_226

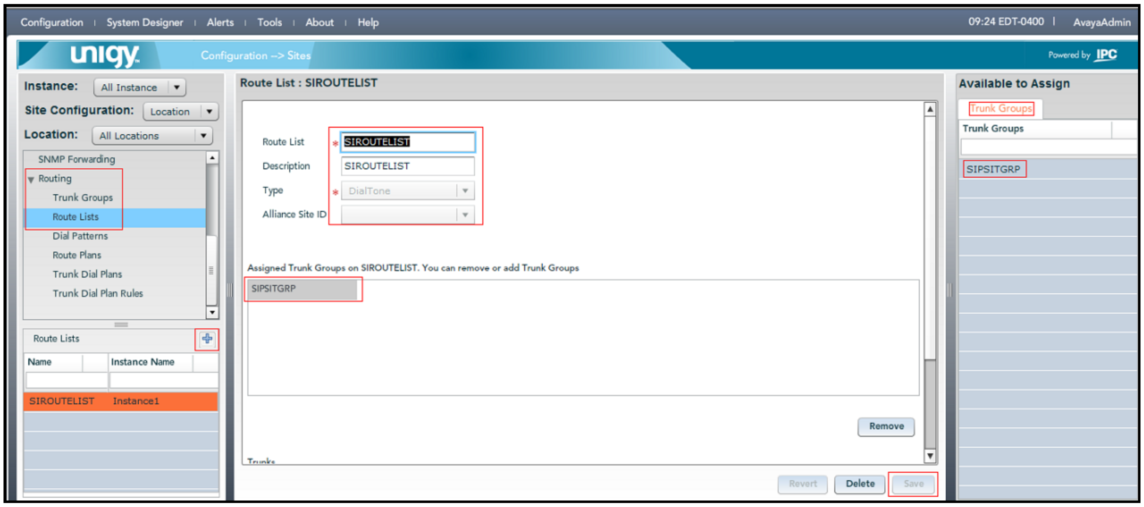
Available to Assign

Name	Channels

7.4. Administer Route Lists

Select **Routing → Route Lists** in the left pane from **Configuration → Sites**, and click the **"+"** icon in the lower left pane to add a new route list as shown in screen below.

The **Route List** screen is displayed in the middle pane. The screen shows the values configured for compliance testing. In the right pane, select the trunk group from **Section 7.3** and drag into the **Assigned Trunk Groups on SIROUTELIST** sub-section in the middle pane, as shown below. Click on **Save** to complete the configuration.



Instance: All Instance

Site Configuration: Location

Location: All Locations

Route List : SIROUTELIST

Route List * SIROUTELIST

Description SIROUTELIST

Type * DialTone

Alliance Site ID

Assigned Trunk Groups on SIROUTELIST. You can remove or add Trunk Groups

SIPSITGRP

Route Lists

Name	Instance Name
SIROUTELIST	Instance1

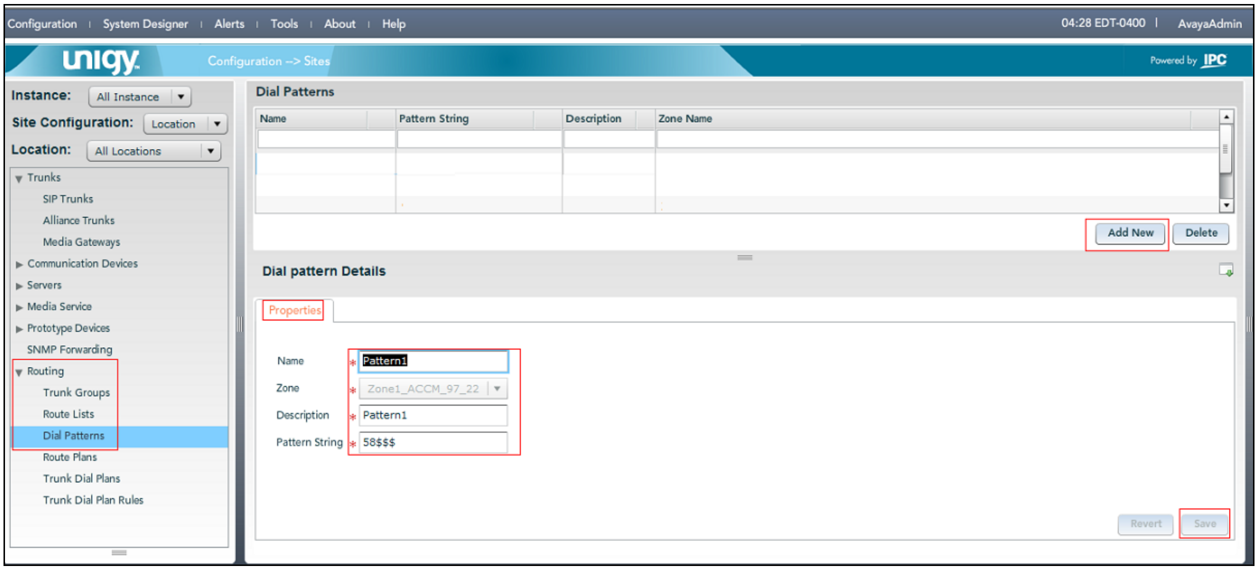
Available to Assign

Trunk Groups
SIPSITGRP

7.5. Administer Dial Patterns

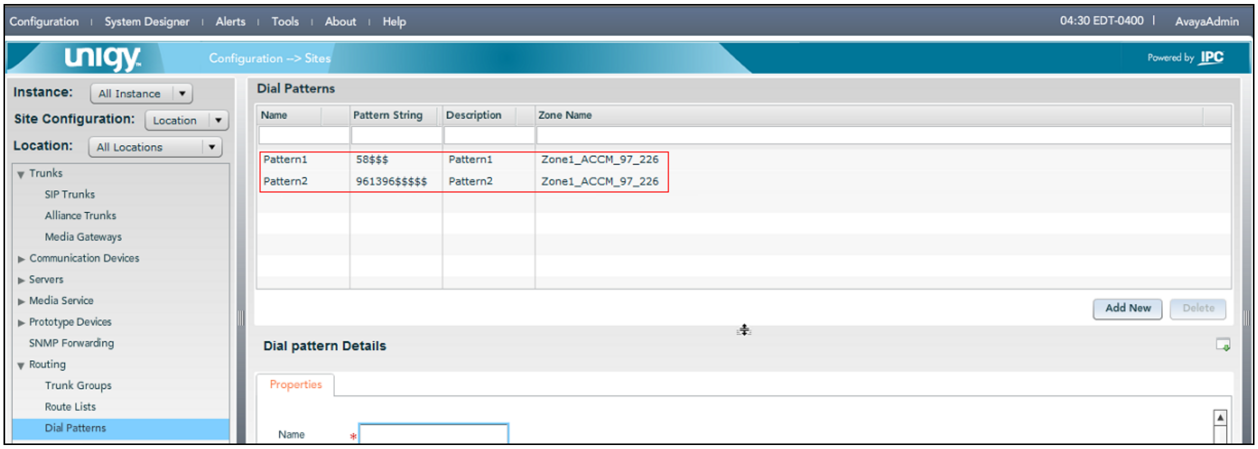
Select **Routing → Dial Patterns** in the left pane from **Configuration → Sites** to display the **Dial Patterns** screen in the right pane. Click **Add New** in the upper right pane as shown in the screen below.

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 the Avaya extensions, in this case **58$$$** with "$" matching to any digit. Click on **Save** to complete adding a dial pattern.



Name: Pattern1
Zone: Zone1_ACCM_97_22
Description: Pattern1
Pattern String: 58$$$

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

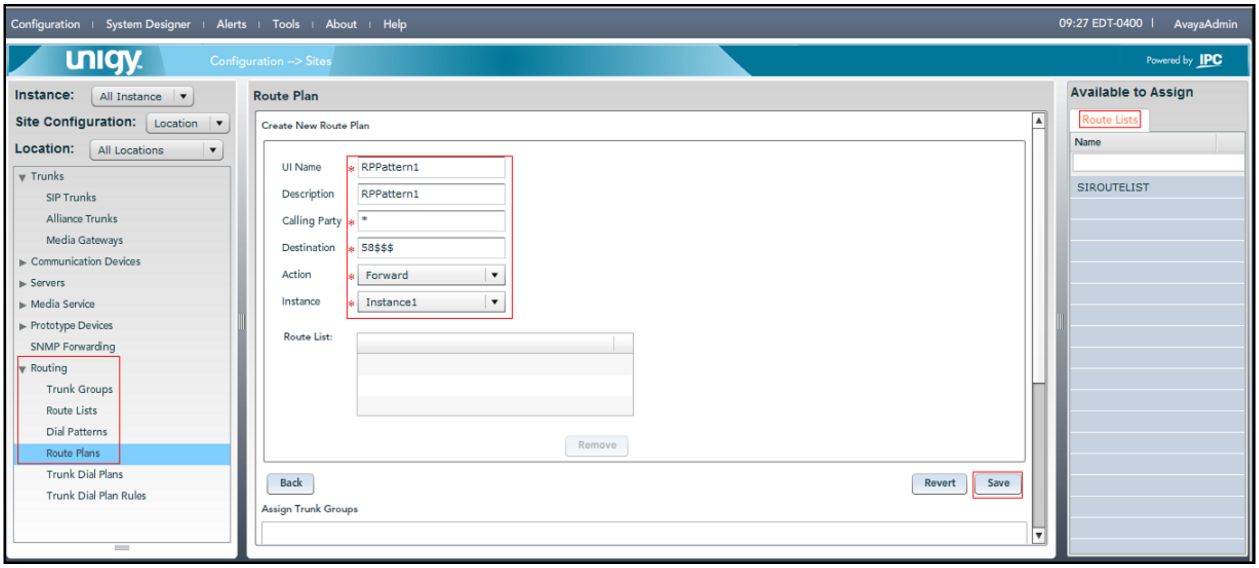


Name	Pattern String	Description	Zone Name
Pattern1	58$$$	Pattern1	Zone1_ACCM_97_226
Pattern2	961396$$$$$	Pattern2	Zone1_ACCM_97_226

7.6. Administer Route Plans

Select **Routing → Route Plans** in the left pane from **Configuration → Sites** and click **Add New** (not shown) in the right pane to create a new route plan as shown in screen below.

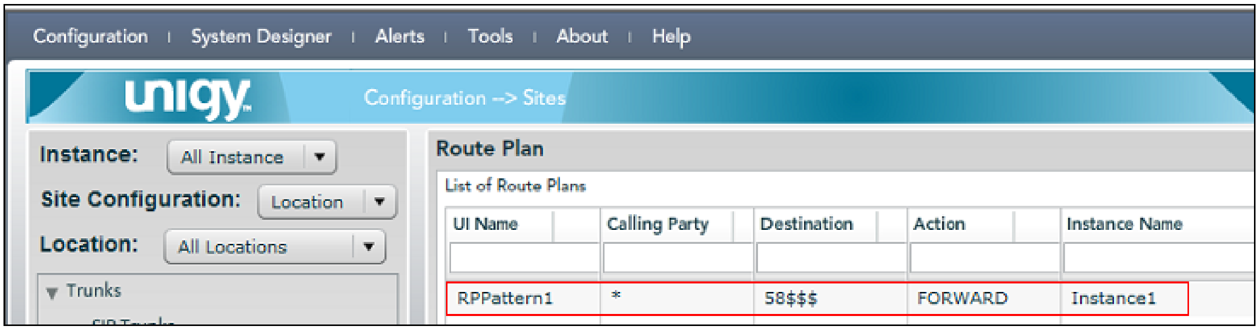
The screen is updated with three panes, as shown below. In the **Route Plan** middle pane, enter a descriptive **UI Name** and optional **Description**. For **Calling Party**, enter ***** to denote any calling party from Unigy. For **Destination**, select the dial pattern for the Avaya users from **Section 7.5**. Select **Forward** for **Action**, **Instance 1** for **Instance** and click on **Save**.



UI Name: RPPattern1
Description: RPPattern1
Calling Party: *
Destination: 58$$$
Action: Forward
Instance: Instance1

SIROUTELIST

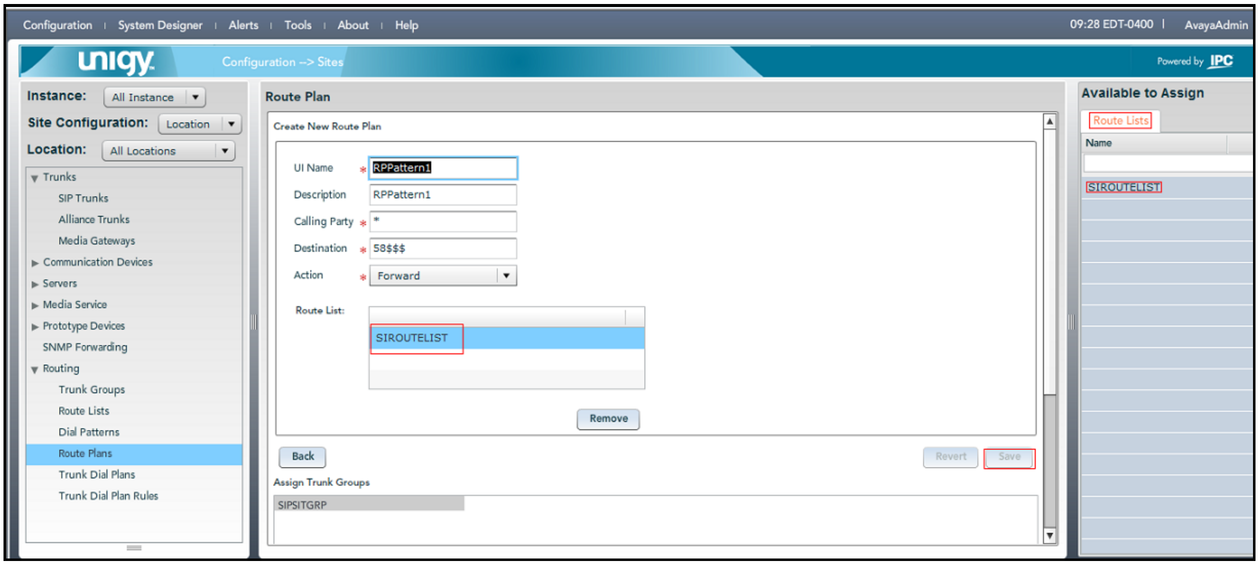
The screen is updated with the newly created route plan as shown in the screen below. Select the **Route Plan**, and click **Edit** toward the bottom of the screen (not shown).



List of Route Plans

UI Name	Calling Party	Destination	Action	Instance Name
RPPattern1	*	58$$$	FORWARD	Instance1

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



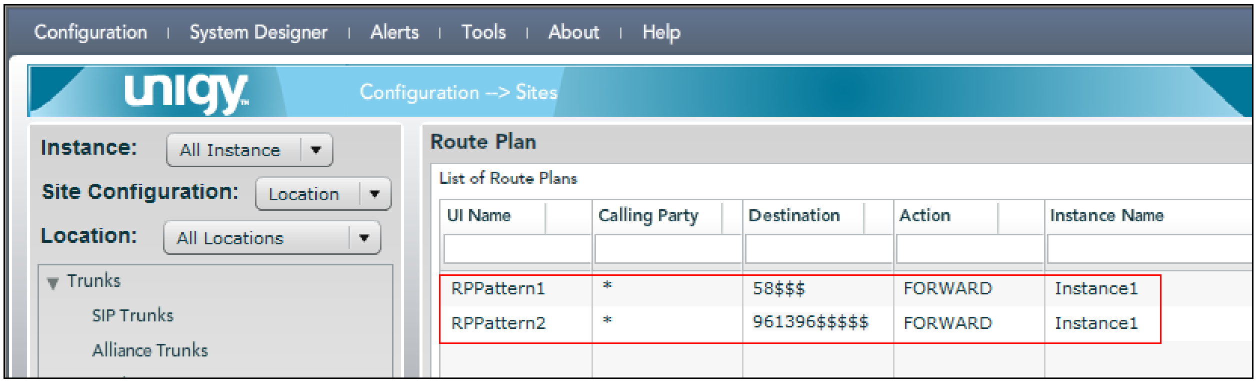
Instance: All Instance
Site Configuration: Location
Location: All Locations

UI Name: RPPattern1
Description: RPPattern1
Calling Party: *
Destination: 58$$$
Action: Forward
Route List: SIROUTELIST

Assign Trunk Groups: SIPSITGRP

SIROUTELIST

Repeat this section to add another **Route Plan** for the PSTN. During compliance testing, two Route Plans were created as shown below.


Configuration | System Designer | Alerts | Tools | About | Help
unigy
Configuration --> Sites
Trunks
SIP Trunks
Alliance Trunks

Instance: All Instance
Site Configuration: Location
Location: All Locations

Route Plan

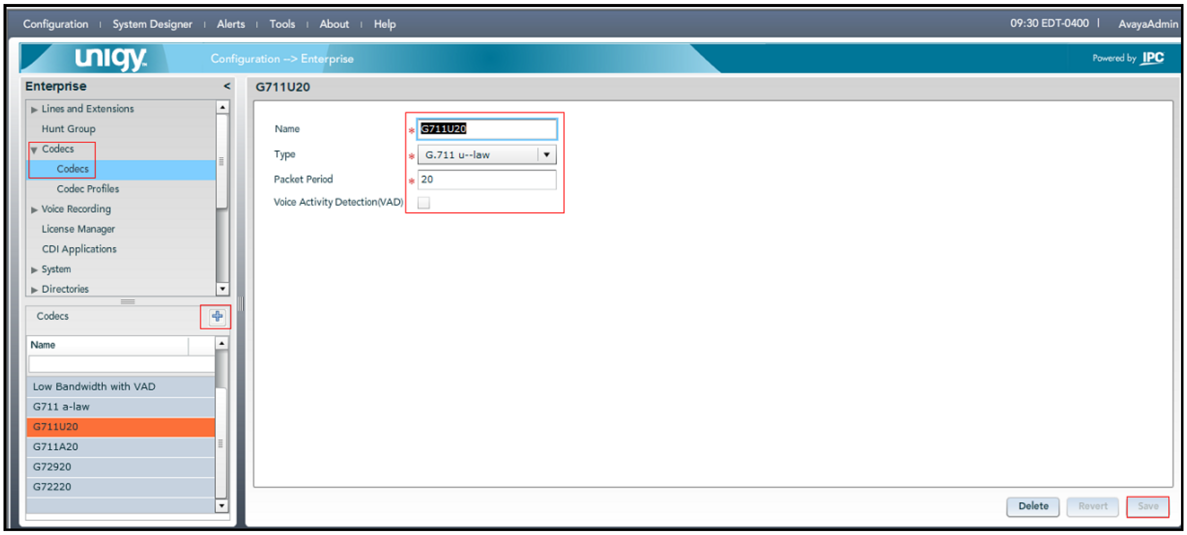
List of Route Plans

UI Name	Calling Party	Destination	Action	Instance Name
RPPattern1	*	58$$$	FORWARD	Instance1
RPPattern2	*	961396$$$$$	FORWARD	Instance1

7.7. Administer Codecs

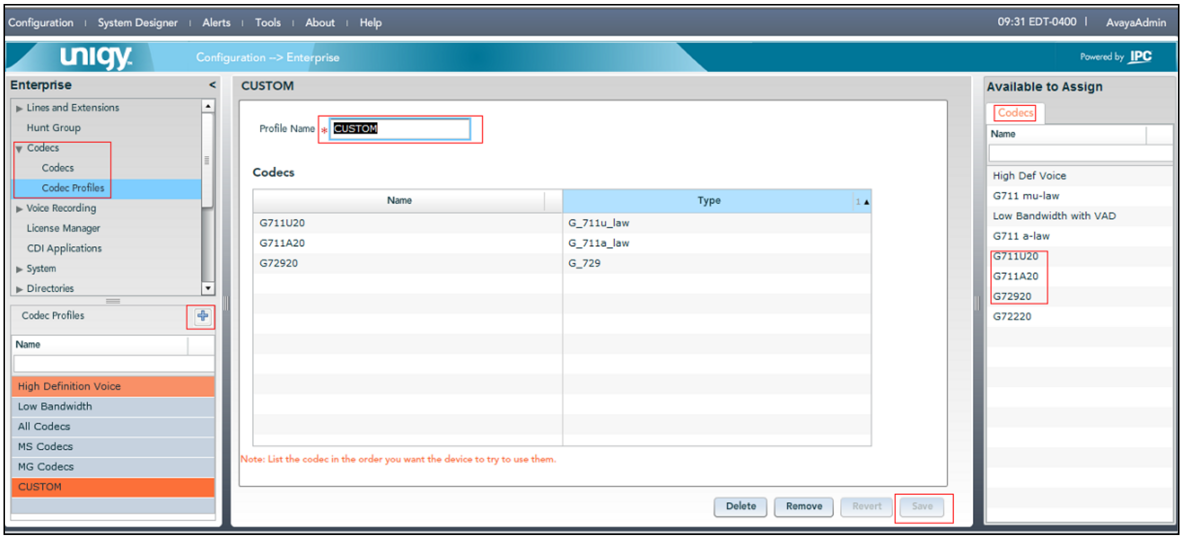
Select **Codecs → Codecs** in the left pane from **Configuration → Enterprise** (not shown), and click the “+” icon in the lower left pane to add a new codec as shown below.

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. The screen below shows the **G711U20** codec being added. Similarly other codecs can be added.



Name	G711U20
Type	G.711 u--law
Packet Period	20
Voice Activity Detection(VAD)	□

To configure a codec profile, select **Codecs → Codec Profiles** in the left pane from **Configuration → Enterprise**, and click on “+” to add a new profile. The screen below shows a profile that has been added during compliance testing called **CUSTOM, G711U20, G711A20** and **G72920** codecs have been added to this profile by dragging them into the middle pane from the right pane. Click on **Save** to complete this configuration.



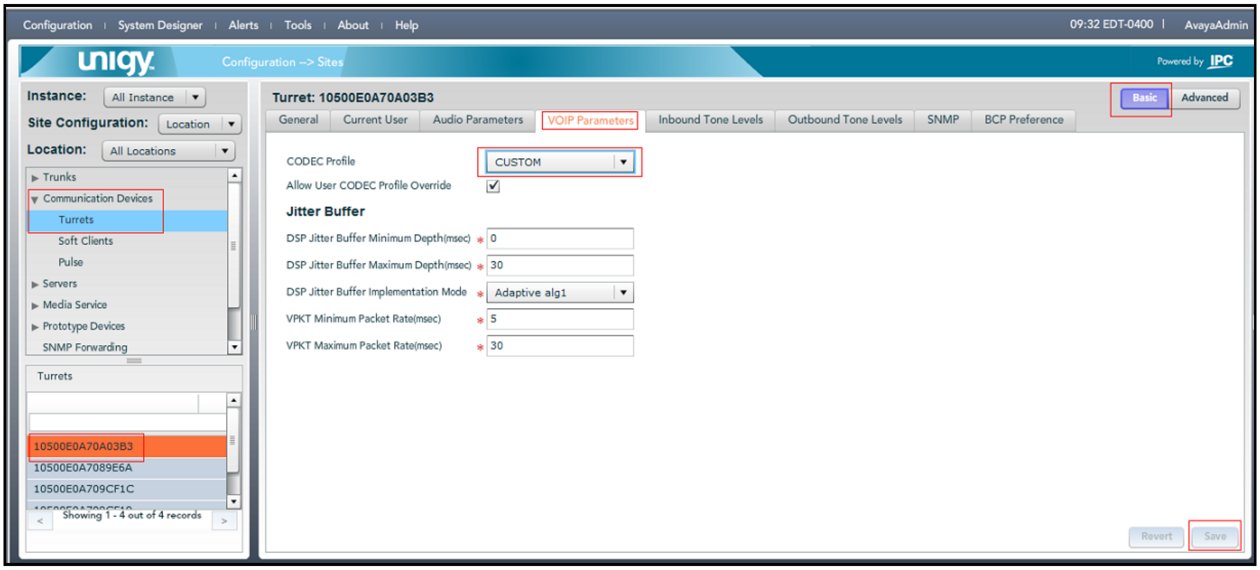
Profile Name: CUSTOM

Codecs

Name	Type
G711U20	G_711u_law
G711A20	G_711a_law
G72920	G_729

Note: List the codec in the order you want the device to try to use them.

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** from **Configuration → Sites** as shown 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. Retain default values for other fields and click on **Save** to complete this configuration.



Turret: 10500E0A70A03B3

CODEC Profile: CUSTOM

Allow User CODEC Profile Override ☑

Jitter Buffer

DSP Jitter Buffer Minimum Depth(msec) * 0

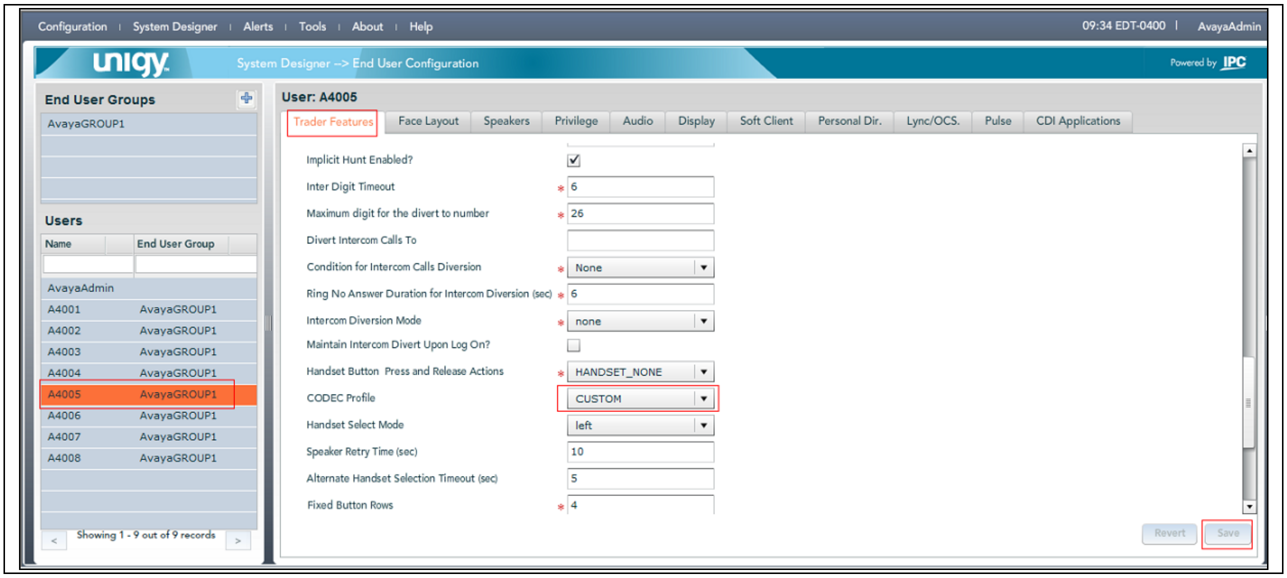
DSP Jitter Buffer Maximum Depth(msec) * 30

DSP Jitter Buffer Implementation Mode * Adaptive alg1

VPKT Minimum Packet Rate(msec) * 5

VPKT Maximum Packet Rate(msec) * 30

To include this profile in a user, navigate to **System Designer → End User Configuration** (not shown). From the screen shown below, select a user and access the **Trader Features** tab. Select the required profile from the drop down of the **CODEC Profile** field. Retain default values for other fields and click on **Save** to complete the configuration.



Name	End User Group
AvayaAdmin	
A4001	AvayaGROUP1
A4002	AvayaGROUP1
A4003	AvayaGROUP1
A4004	AvayaGROUP1
A4005	AvayaGROUP1
A4006	AvayaGROUP1
A4007	AvayaGROUP1
A4008	AvayaGROUP1

User: A4005

Implicit Hunt Enabled? ☑

Inter Digit Timeout * 6

Maximum digit for the divert to number * 26

Divert Intercom Calls To

Condition for Intercom Calls Diversion * None

Ring No Answer Duration for Intercom Diversion (sec) * 6

Intercom Diversion Mode * none

Maintain Intercom Divert Upon Log On? □

Handset Button Press and Release Actions * HANDSET_NONE

CODEC Profile: CUSTOM

Handset Select Mode: left

Speaker Retry Time (sec) 10

Alternate Handset Selection Timeout (sec) 5

Fixed Button Rows * 4

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

8. Configure IPC Media Manager

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

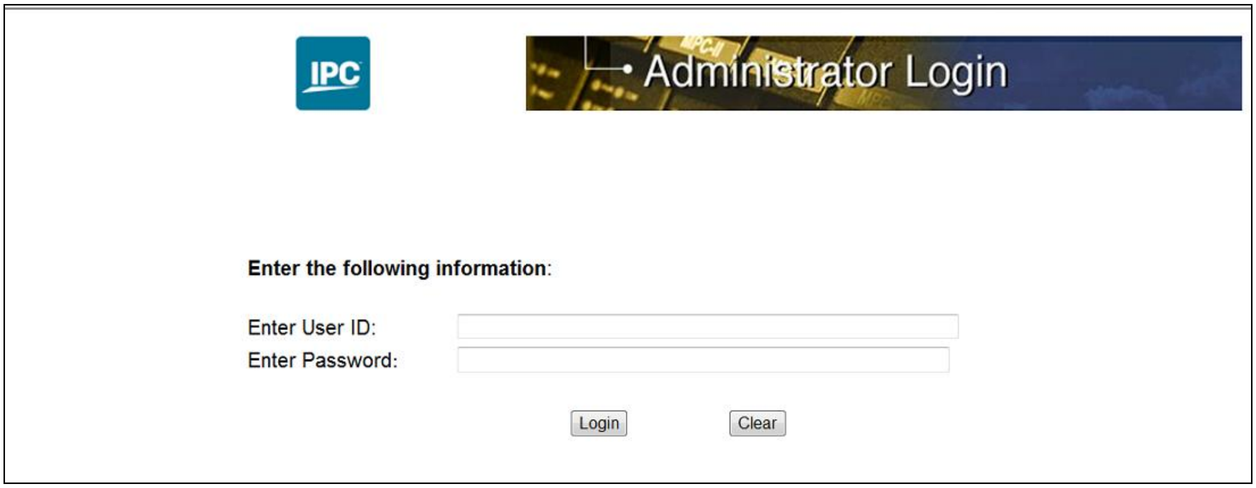
- Launch Unigy Media Manager web interface.
- Configure SIP Audio Codec List.

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 the reference documentation in **Section 11**.

8.1. Launch Unigy Media Manager web interface

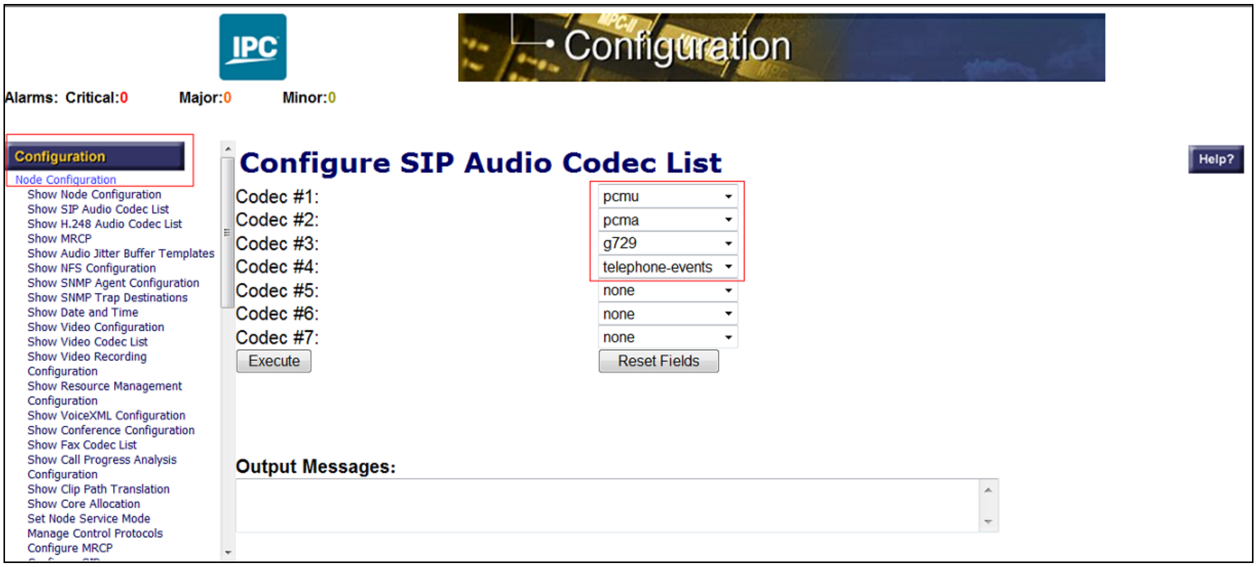
Access the Unigy Management System web interface by using the URL "http://ip-address/swms" in an Internet browser window, where "ip-address" is the IP address of the Media Manager. Log in using the appropriate credentials.

The screen as shown below is displayed. Enter the appropriate **User ID** and **Password** credentials and click **Login**.



8.2. Configure SIP Audio Codec List

Select **Configure SIP Audio Codec List** from **Configuration →Node Configuration** (not shown). The screen below is shown. Select the codec values from the drop down list for **Codec #1** to **Codec # 4** keeping it in synchronization with the codec list administered in **Section 7.7**.


IPC
Configuration
Alarms: Critical:0
Major:0
Minor:0
Configuration
Node Configuration
Show Node Configuration
Show SIP Audio Codec List
Show H.248 Audio Codec List
Show MRCP
Show Audio Jitter Buffer Templates
Show NFS Configuration
Show SNMP Agent Configuration
Show SNMP Trap Destinations
Show Date and Time
Show Video Configuration
Show Video Codec List
Show Video Recording Configuration
Show Resource Management Configuration
Show VoiceXML Configuration
Show Conference Configuration
Show Fax Codec List
Show Call Progress Analysis Configuration
Show Clip Path Translation
Show Core Allocation
Set Node Service Mode
Manage Control Protocols
Configure MRCP
Help?
Execute
Reset Fields
Output Messages:

Configure SIP Audio Codec List

Codec #1: pcmu
Codec #2: pcma
Codec #3: g729
Codec #4: telephone-events
Codec #5: none
Codec #6: none
Codec #7: none

9. Verification Steps

The following tests were conducted to verify the solution between the Communication Server 1000 and the Unigy system:

- All basic call features operate successfully between Communication Server 1000 and Unigy users.
- Connection between Unigy System and Avaya Aura® Session Manager is successfully established when the Ethernet connection is disconnected and reconnected back to the Unigy System.

10. 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 Communication Server 1000 Release 7.5 using Avaya Aura®.

11. Additional References

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

- *Software Input Output Reference — Administration Avaya Communication Server 1000 7.5* NN43001-611, Standard 05.13, September 2012, available at http://support.avaya.com.

- *Administering Avaya Aura® Session Manager*, Issue 1.1 03-603324, Release 6.1, November 2010, available at http://support.avaya.com.

- *Unigy System Configuration*, available upon request to IPC Support.

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.