



Avaya Solution & Interoperability Test Lab

Application Notes for IPC Unigy V2.0.1 with Avaya Aura® Messaging 6.3 and Avaya Aura® Session Manager 6.3 in a Centralized Messaging Environment using SIP Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for IPC Unigy V2.0.1 to interoperate with Avaya Aura® Messaging 6.3 and Avaya Aura® Session Manager 6.3 in a centralized messaging environment using SIP trunks to Avaya Aura® Session Manager.

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 V2.0.1 to interoperate with Avaya Aura® Messaging 6.3 and Avaya Aura® Session Manager 6.3 in a centralized messaging environment using SIP trunks to Avaya Aura® Session Manager.

IPC Unigy is a trading communication solution. In the compliance testing, IPC Unigy V2.0.1 used SIP trunks to Avaya Aura® Session Manager, for IPC turret users to obtain voice messaging services from Avaya Aura® Messaging. The Avaya Aura® Messaging system in the Central site supported local subscribers from Avaya Aura® Communication Manager 6.3 at the Central site, and from IPC turret users at the Remote site.

2. General Test Approach and Test Results

The feature test cases were performed manually. Calls were manually established among IPC turret users with Avaya SIP, Avaya H.323, PSTN users, and/or the Avaya Aura® Messaging voicemail pilot to verify various call scenarios.

The serviceability test cases were performed manually by disconnecting and reconnecting the LAN connection to the IPC Unigy V2.0.1 servers.

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 consists of feature and serviceability testing.

The feature testing included subscriber login, greeting, voice message (leaving/retrieving), message waiting indicator, call forward, multiple call forward, personal operator, auto attendant, find me, call me, and call sender.

The serviceability testing focused on verifying the ability of IPC Unigy V2 to recover from adverse conditions, such as disconnecting/reconnecting the LAN connection to the IPC Unigy V2.0.1 server.

2.2. Test Results

All test cases were executed. The following were the observations from the compliance testing.

- IPC does not offer the Coverage feature, therefore coverage to voicemail for the turret users were accomplished by setting the Avaya Aura® Messaging pilot number as the Call Forwarding destination for the users.
- During the compliance test, shuffling was disabled, since issues were observed from the previous version, when shuffling was enabled.
- Issues were observed on transfer features from Avaya Aura® Messaging.
- An issue was observed on Multiple Call Forward without answer.

IPC does not expect their users to use these features, so the testing was passed. The issues listed here are for user awareness.

2.3. Support

Technical support on IPC Unigy V2.0.1 can be obtained through the following:

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

3. Reference Configuration

As shown in the test configuration below, **Figure 1**, IPC Unigy V2.0.1 consists of the Media Manager and Converged Communication Manager (HA system), and Turrets. SIP trunks are used from and the Virtual IP (VIP) of Converged Communication Manager to Session Manager, to reach Avaya Aura® Messaging for voice messaging services.

The detailed administration of basic connectivity among Communication Manager, Session Manager, and Avaya Aura® Messaging is not the focus of these Application Notes and will not be described.

The configuration of Session Manager is performed via the web interface of System Manager.

The detailed administration of SIP trunks between Session Manager, and IPC Unigy V2.0.1, to enable IPC turret users to reach users on Communication Manager and on the PSTN, is assumed to be in place with details described in [4].

These Application Notes will focus on the additional configuration required to support IPC turret users as local subscribers on Avaya Aura® Messaging.

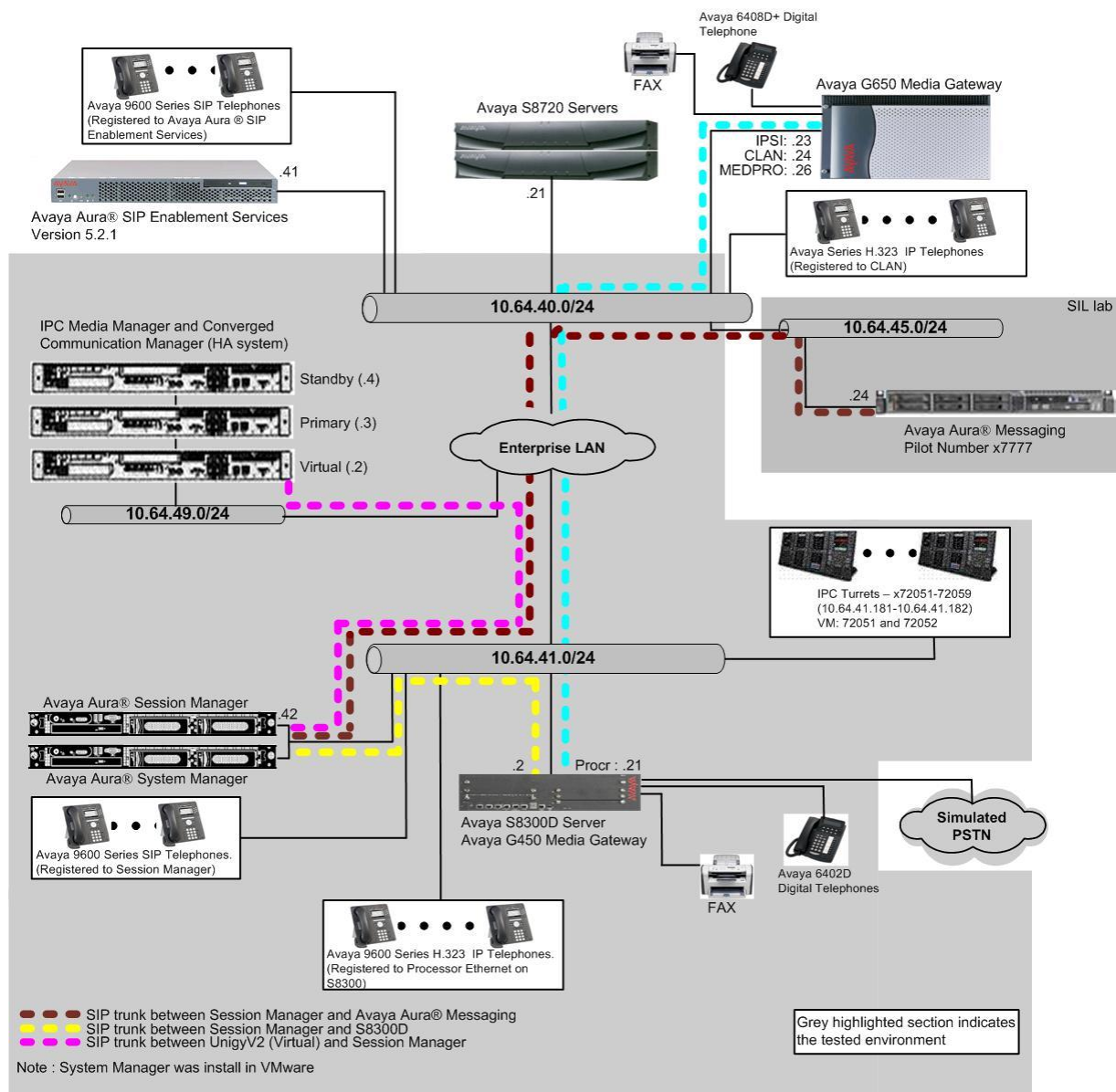


Figure 1: Test Configuration of IPC Unigy V2.0.1 with Avaya Aura® Messaging

4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Messaging	MSG-03.0.124.0-321_0103
Avaya Aura® Communication Manager on Avaya S8300D Server	6.3.7 (R016x.03.0.124-21754)
Avaya Aura® Session Manager	6.3.9.0.639011
Avaya Aura® System Manager	6.3.9.1.2482
Avaya 96xx IP Telephone (H.323)	3.1
Avaya 96x1 IP Telephone (H.323)	6.23
Avaya 96xx IP Telephone (SIP)	2.6.9.1
Avaya 96x1 IP Telephone (SIP)	6.3
IPC Unigy V2.0.1 <ul style="list-style-type: none">Media ManagerConverged Communication ManagerTurrets	02.00.01.02.0045 02.00.01.02.0045 02.00.01.02.0045

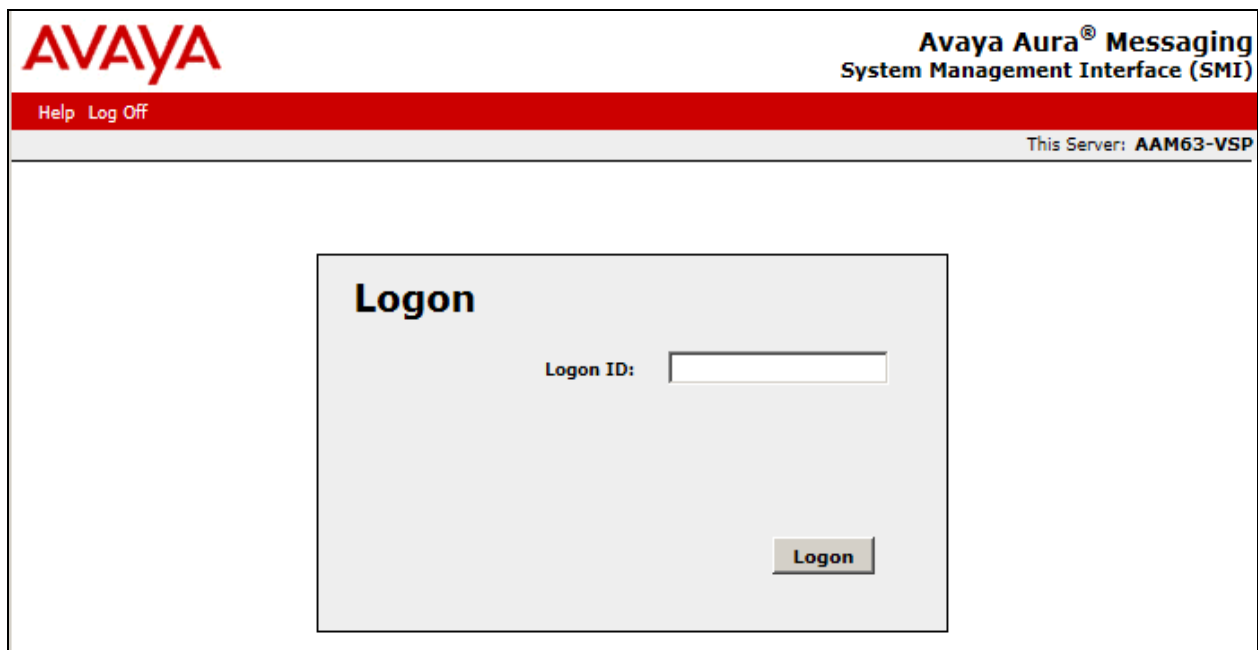
5. Configure Avaya Aura® Messaging

This section provides the procedures for configuring IPC turret users as local subscribers on Avaya Aura® Messaging. The configuration procedures include the following areas:

- Launch messaging administration
- Administer subscriber extension ranges
- Administer subscribers

5.1. Launch Messaging Administration

Access the Avaya Aura® Messaging web interface by using the URL “http://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Avaya Aura® Messaging server. The **Logon** screen is displayed. Log in using a valid user name and password. The **Password** field will appear after a value is entered into the **Username** field.



The screenshot displays the Avaya Aura® Messaging System Management Interface (SMI) web application. At the top left is the AVAYA logo. At the top right, the text reads "Avaya Aura® Messaging System Management Interface (SMI)". Below the logo, there are links for "Help" and "Log Off". On the right side of the header, it says "This Server: AAM63-VSP". The main content area features a "Logon" box with the title "Logon" in bold. Inside this box, there is a label "Logon ID:" followed by a text input field. Below the input field is a "Logon" button.

The **Messaging Administration** screen appears, as shown below. Navigate to **Administration** → **Messaging**.

AVAYA Avaya Aura® Messaging
System Management Interface (SMI)

Help Log Off Administration Licensing Messaging Server (Maintenance) This Server: AAM63-VSP

System Management Interface

© 2001-2013 Avaya Inc. All Rights Reserved.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at:
<http://support.avaya.com/ThirdPartyLicense/>

Trademarks

Avaya is a trademark of Avaya Inc.

Avaya Aura is a registered trademark of Avaya Inc.

MultiVantage is a trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

5.2. Administer Subscriber Extension Ranges

On the Messaging Administration page (not shown) select **Server Settings (Storage)** → **Networked Servers** from the left pane, to display the **Manage Networked Servers** screen. Select the Avaya Aura® Messaging server from the table listing, and click **Edit the Selected Networked Server** toward the bottom right of the screen.

AVAYA Avaya Aura® Messaging System Management Interface (SMI)

Help Log Off Administration This Server: AAM63-VSP

Administration / Messaging

System Status
Alarm Summary
Voice Channels (Application)
Cache Statistics (Application)
Outbound Fax (Storage)

Server Settings
Server Role / AxC Address
Server Settings (Storage)
External Hosts
Trusted Servers
Networked Servers
Request Remote Update

Server Settings (Application)
Dial Rules
Cluster
System Parameters
Languages
Log Configuration

IMAP/SMTP Settings (Storage)
General Options
Mail Options
IMAP/SMTP Status

Telephony Settings
Telephony Integration
Telephony Domains

Advanced (Application)
System Operations
Timeouts
Miscellaneous
Core Files

Utilities
Messaging DB Audits (Storage)
Start Messaging
Stop Messaging
LDAP Status/Restart (Storage)
Change LDAP Password (Storage)

Manage Networked Servers

The Manage Networked Servers page is used to add change or delete the Networked servers used by the messaging feature.

Server Name	IP Address	Server Type	ID	Total Subs
AAM63-VSP	10.64.45.24	local	0	6

Display Report of Servers

Add a New Networked Server

Display Network Snapshot

Help

Delete the Selected Networked Server

Edit the Selected Networked Server

The **Edit Messaging Server** screen is displayed. Select **5** using drop-down menu on the Mailbox Number Length field. In the compliance test, the 5 digit extensions were used by Avaya Aura® Messaging.

Click on **Save** at the bottom of the screen.

AVAYA Avaya Aura® Messaging System Management Interface (SMI)

Help Log Off Administration This Server: AAM63-VSP

Administration / Messaging

Edit Messaging Server

The Edit Messaging Server allows the changing of the local messaging server.

System Status
Alarm Summary
Voice Channels (Application)
Cache Statistics (Application)
Outbound Fax (Storage)

Server Settings
Server Role / AxC Address
Server Settings (Storage)
External Hosts
Trusted Servers
Networked Servers
Request Remote Update

Server Settings (Application)
Dial Rules
Cluster
System Parameters
Languages
Log Configuration

IMAP/SMTP Settings (Storage)
General Options
Mail Options
IMAP/SMTP Status

Telephony Settings
Telephony Integration
Telephony Domains

Server Name: AAM63-VSP Password:
Confirm Password:

IP Address: 10.64.45.24 Server Type: tcpip

Mailbox Number Length: 5

Updates In: no Default Community: 1

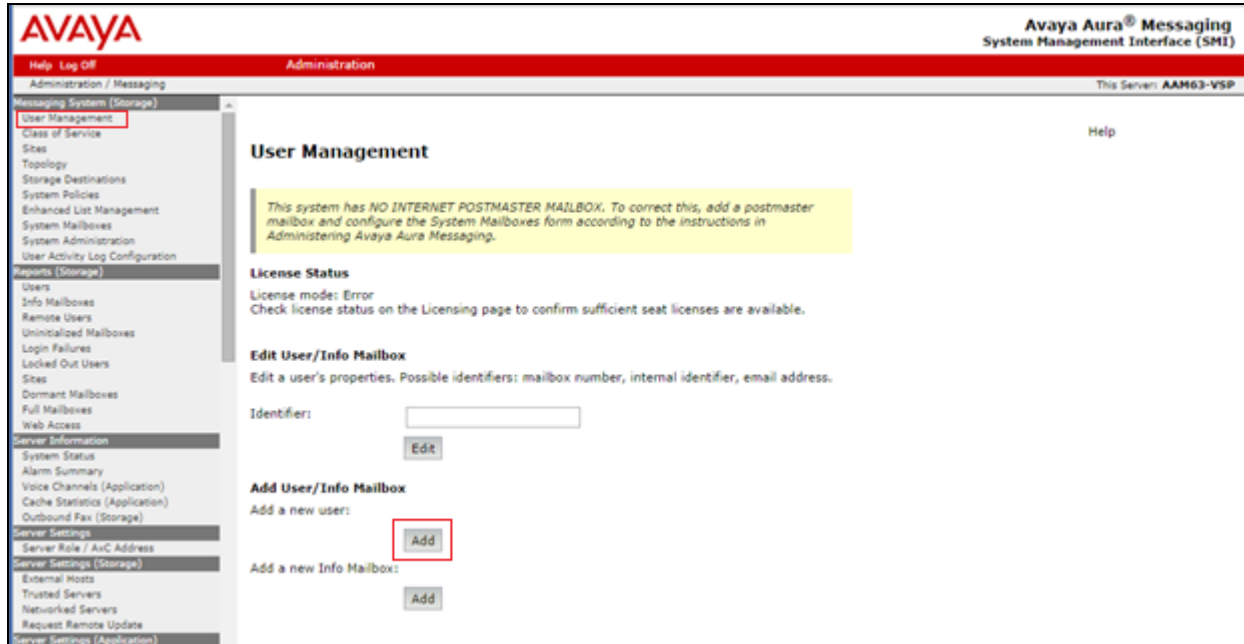
Remote LDAP Port: 56389 Updates Out: yes

Log Updates In: no

Back Save Help

5.3. Administer Subscribers

Select **Messaging System (Storage) → User Management** from the left pane, to display the **User Management** screen. Click **Add** under the **Add a new user** section.



The **User Management > Properties for New User** screen is displayed next. Enter the desired string into the **First Name**, **Last Name**, and **Password** fields.

In the compliance testing, the same telephone extensions for the IPC subscribers were used for the **Mailbox number**, **Numeric address**, and **Extension** fields. Select the appropriate **Class Of Service**, and retain the default values in the remaining fields.

Scroll down to the bottom of the screen and click **Save**.

The screenshot displays the Avaya Aura® Messaging System Management Interface (SMI) for server AAM63-VSI. The 'User Properties' configuration page is active, showing a comprehensive set of fields for user setup. The left navigation pane lists various system management tasks, with 'Users' currently selected. The main form area includes input fields for personal and contact information, a dropdown for site selection, and fields for mailbox and extension details. It also features a 'Class of Service' dropdown, a 'Pronounceable name' field, and a section for 'MWI enabled' settings. At the bottom, there are password fields and checkboxes for additional user management options. A 'Save' button is positioned at the bottom right of the configuration area.

Repeat this section to add all IPC subscribers. During the compliance test, 72051 and 72052 were used.

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. Prior to the solution test, the following sections were already configured, and not discussed in these application Notes.

- Domain
- SIP Entities
- Entity Links
- Routing Policy

The discussed procedures include the following areas:

- Launch System Manager
- Administer dial patterns

6.1. Launch System Manager

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

6.2. Administer Dial Patterns

In the subsequent screen (not shown), select **Home** → **Elements** → **Routing** to display the **Introduction to Network Routing Policy** screen (not shown). Click **Routing** → **Dial Patterns** from the left pane to display the **Dial Patterns** screen. Locate and click on the dial pattern that corresponds to the Avaya Aura® Messaging pilot number, in this case “7777”. The pilot number was configured prior to this solution test, and the following screen shows only for information purpose.

The screenshot shows the Avaya Aura Network Management console. The top navigation bar includes 'Home', 'Session Manager', and 'Routing'. The left sidebar lists various configuration categories, with 'Dial Patterns' highlighted. The main content area displays the 'Dial Patterns' screen, which includes a table of 13 items. The table columns are: Pattern, Min, Max, Emergency Call, Emergency Type, Emergency Priority, SIP Domain, and Notes. The row for pattern '7777' is highlighted with a red border. Below the table, there is a 'Select' dropdown menu set to 'All'.

Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
*	3	3	<input type="checkbox"/>			-ALL-	
12	3	3	<input type="checkbox"/>			-ALL-	
1303	10	12	<input type="checkbox"/>			-ALL-	
303	10	12	<input type="checkbox"/>			avaya.com	
332	5	5	<input type="checkbox"/>			-ALL-	
7200	5	5	<input type="checkbox"/>			-ALL-	
7205	5	5	<input type="checkbox"/>			-ALL-	
7207	5	5	<input type="checkbox"/>			-ALL-	
7208	5	5	<input type="checkbox"/>			-ALL-	
7209	5	5	<input type="checkbox"/>			-ALL-	
7776	4	4	<input type="checkbox"/>			-ALL-	
7777	4	4	<input type="checkbox"/>			avaya.com	
913	10	12	<input type="checkbox"/>			-ALL-	

The **Dial Pattern Details** screen is displayed. In the **Originating Locations and Routing Policies** sub-section, add or modify the entry as desired to allow IPC turret users to reach Avaya Aura® Messaging. In the compliance testing, a new entry was created to allow for call origination from the existing IPC location, as shown below.

AVAYA
Aura® System Manager 6.3

Session Manager x

Home / Elements / Routing / Dial Patterns

Dial Pattern Details Commit Cancel Help ?

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

3 Items Filter: Enable

<input type="checkbox"/>	Originating Location Name ^	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		Route2MM	0	<input checked="" type="checkbox"/>	Modular Messaging	
<input type="checkbox"/>	-ALL-		Route2AAM63-VMware	0	<input checked="" type="checkbox"/>	AAM63-VMware	
<input type="checkbox"/>	-ALL-		Rout2AAM63-VSP	0	<input type="checkbox"/>	AAM63-VSP	

Select : All, None

The following screen displays how to add **Originating Locations** and **Routing Policies**. During the compliance test, check the checkbox for **Apply The Selected Routing Policies to All Originating Locations**. For Routing Policy, check the checkbox for the **Rout2 AAM63-VSP**.

Click **Select**.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with options: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Routing' and contains two sections: 'Originating Location' and 'Routing Policies'.

In the 'Originating Location' section, there is a checkbox labeled 'Apply The Selected Routing Policies to All Originating Locations' which is checked. Below this is a table with 8 items, showing various subnets and their associated networks.

In the 'Routing Policies' section, there is a table with 7 items. The first item, 'Rout2AAM63-VSP', is selected. Its destination is 'AAM63-VSP', which is highlighted in the table.

Name	Notes
101-subnet	VMware Network
10-subnet	Ally network
22-Subnet	Modular Messaging Network
40-subnet	CM521 Network
41-subnet	CM63 Network
42-subnet	CM601 Network
45-subnet	
49-subnet	Unigy Network

Name	Disabled	Destination	Notes
Rout2AAM63-VSP	<input type="checkbox"/>	AAM63-VSP	
Route2AAM63-VMware	<input checked="" type="checkbox"/>	AAM63-VMware	
Route2Alliance system	<input type="checkbox"/>	Alliance	
Route2CM63	<input type="checkbox"/>	CM63	
Route2MM	<input checked="" type="checkbox"/>	Modular Messaging	
Route2Unigy system	<input type="checkbox"/>	Unigy	
Route-Keyur	<input checked="" type="checkbox"/>	CM63-Keyur	

There should be dial patterns for three routing policies:

- Route 2 Unigy system
- Route2CM63
- Rout2AAM63-VSP (included in this section)

Configure other dial patterns for two routing policies using above procedures.

7. Configure IPC Unigy V2.0.1 Converged Communication Manager

This section provides the procedures for configuring IPC Unigy V2.0.1 Converged Communication Manager. The procedures include the following areas:

- Launch Unigy V2.0.1 Management System
- Administer SIP trunks
- Administer trunk groups
- Administer route lists
- Administer dial patterns
- Administer route plans

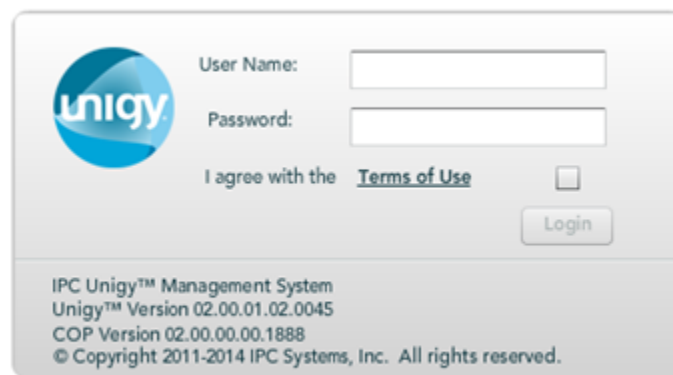
The configuration of Converged Communication Manager is typically performed by IPC installation technicians. The procedural steps are presented in these Application Notes for informational purposes.

7.1. Launch Unigy V2.0.1 Management System

Access the UnigyV2.0.1 Management System web interface by using the URL “http://ip-address” in an Internet browser window, where “ip-address” is the IP address of VIP. Log in using the appropriate credentials.

The screen 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 Unigy V2.0.1 Management System. On the left is the Unigy logo, a blue circle with the word 'unigy' in white. To the right of the logo are two input fields: 'User Name:' and 'Password:'. Below these fields is a checkbox labeled 'I agree with the' followed by a blue underlined link 'Terms of Use'. To the right of the checkbox is a small square icon. Below the checkbox and link is a 'Login' button. At the bottom of the form, there is a footer containing the following text: 'IPC Unigy™ Management System', 'Unigy™ Version 02.00.01.02.0045', 'COP Version 02.00.00.00.1888', and '© Copyright 2011-2014 IPC Systems, Inc. All rights reserved.'


The following screen (Tools -> Monitoring) displays. Navigate to **Configuration → Site**.

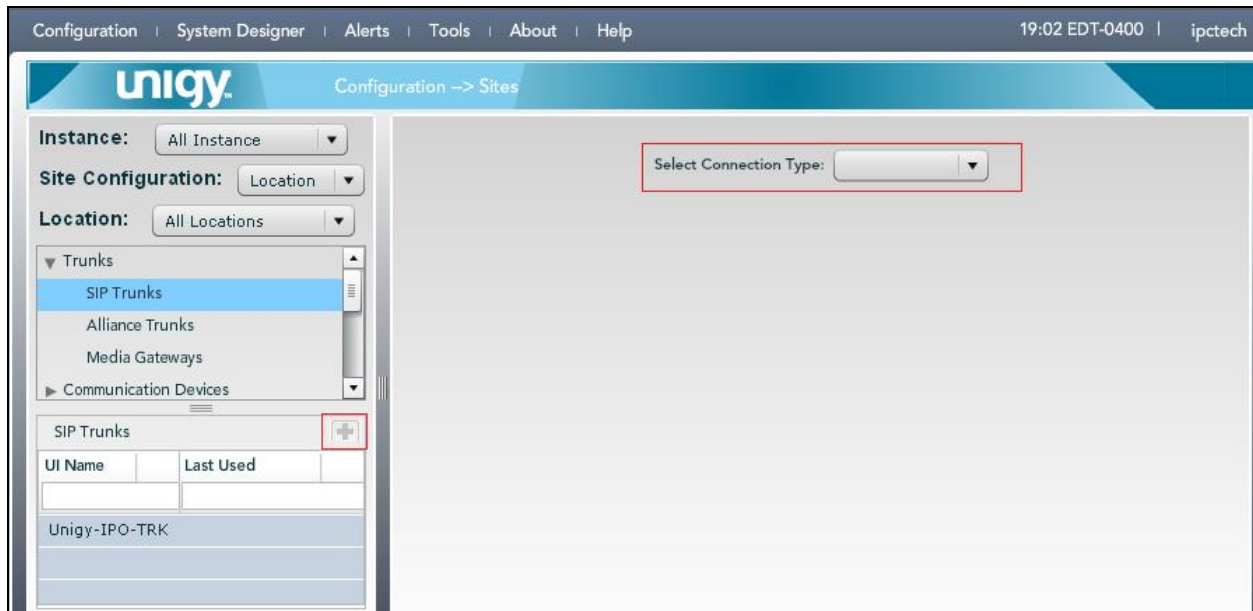
The screenshot shows the UniQy Enterprise monitoring interface. The top navigation bar includes 'Configuration' (highlighted with a red box), 'System Designer', 'Alerts', 'Tools', 'About', and 'Help'. The status bar shows a warning icon, the time '13:18 EDT-0400', and the user 'ipctech'. The main header displays the UniQy logo and the path 'Tools -> Monitoring'. Below the header, the 'Enterprise' section contains a 'Summary' tab and two data tables: 'Instances' and 'Locations'. The 'Instances' table has columns for Instance, Total Devices, Device Alerts High, and Dev Aler. The 'Locations' table has columns for Location, Instance, Total Devices, and Device Alerts Hig. Both tables show data for 'Default Instance' and 'Default Back R'.

Instance	Total Devices	Device Alerts High	Dev Aler
Default Instance	9	4	2

Location	Instance	Total Devices	Device Alerts Hig
Default Front R	Default Instanc	5	0
Default Back R	Default Instanc	4	4

7.2. Administer SIP Trunks

Select **Trunks** → **SIP Trunks** in the left pane, and click the **Add** icon () in the lower left pane to add a new SIP trunk. Select “Dial Tone” from the **Select Connection Type** drop-down list.



The screen below is displayed next. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Trunk Name:** A descriptive name.
- **Destination Address:** Enter the IP address of the Session Manager signaling interface.
- **Destination Port:** Enter the port number.
- **Zone:** An available zone, in this case “Default Zone 1”.
- **Channels:** Enter the number of SIP trunk group members.
- **Reason Protocol:** “SIP”
- **PBX Provider:** “Avaya”
- **Connected Party Update:** “UPDATE”

Retain the default values in the remaining fields.

The screenshot displays the Unigy configuration interface. The top navigation bar shows 'Configuration -> Sites'. On the left, a sidebar lists various configuration categories, with 'SIP Trunks' selected. The main area is titled 'Trunk: Unigy-SIP-TRK-SM63' and contains a 'DialTone Trunk Configuration' form. The form has two tabs: 'Basic' (selected) and 'Advanced'. The 'Basic' tab contains the following fields:

Field	Value
Trunk Name	Unigy-SIP-TRK-SM63
Connection Type	Dial Tone
Destination Address	10.64.41.42
Destination Port	5060
Media Manager Profile	Safe
Zone	Default Zone 1
Channels	30
Reason Protocol	SIP
PBX Provider	Avaya
Connected Party Update	UPDATE
Subscribe to MWI	<input checked="" type="checkbox"/>
MWI Subscription Time	0
Vendor	
A/B Side	<input type="checkbox"/>
Distant End Name	
PBX Trunk Group Reference	
Trunk Info	
ReINVITE For Media Update	<input checked="" type="checkbox"/>
Options Supported	<input checked="" type="checkbox"/>
Equipped	<input checked="" type="checkbox"/>

At the bottom of the form are three buttons: 'Delete', 'Revert', and 'Save'.

Select the **Advanced** tab in the upper right. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Diversion Header:** Select “History-Info”.
- **Outgoing Transport Type:** Select “UDP”.


Click the **Save** button at the bottom of this page.

The screenshot displays the Unigy configuration interface. The top header shows "unigy Configuration -> Sites" and "Powered by IPC". The left sidebar contains a tree view with categories like "Trunks", "Alliance Trunks", "Media Gateways", "Communication Devices", "Servers", "Media Service", "Prototype Devices", "SNMP Forwarding", "Routing", "Trunk Groups", "Route Lists", and "Dial Patterns". The "SIP Trunks" category is selected, and a table lists several trunks, with "Unigy-SIP-TRK-SM63" highlighted. The main configuration area is titled "Trunk: Unigy-SIP-TRK-SM63" and has two tabs: "Basic" and "Advanced". The "Advanced" tab is selected, showing the "DialTone Trunk Configuration" section. This section contains various fields with their current values: Trunk Name (Unigy-SIP-TRK-SM63), Connection Type (Dial Tone), Destination Address (10.64.41.42), Destination Port (5060), Media Manager Profile (Safe), Zone (Default Zone 1), Channels (30), Reason Protocol (SIP), PBX Provider (Avaya), Connected Party Update (UPDATE), Subscribe to MWI (checked), MWI Subscription Time (0), Vendor (empty), A/B Side (unchecked), Distant End Name (empty), PBX Trunk Group Reference (empty), Trunk Info (empty), Diversion Header (History-Info), Indicate PRACK Support (checked), and Outgoing Transport Type (UDP). At the bottom right, there are three buttons: "Delete", "Revert", and "Save".

UI Name	Last Used
Unigy-SIP-TRK-SM63	
Unigy-IPO-TRK	
Unigy-SIP-TRK-SM62	

Trunk Name	* Unigy-SIP-TRK-SM63
Connection Type	Dial Tone
Destination Address	* 10.64.41.42
Destination Port	* 5060
Media Manager Profile	* Safe
Zone	* Default Zone 1
Channels	30
Reason Protocol	* SIP
PBX Provider	* Avaya
Connected Party Update	* UPDATE
Subscribe to MWI	<input checked="" type="checkbox"/>
MWI Subscription Time	0
Vendor	
A/B Side	<input type="checkbox"/>
Distant End Name	
PBX Trunk Group Reference	
Trunk Info	
Diversion Header	* History-Info
Indicate PRACK Support	<input checked="" type="checkbox"/>
Outgoing Transport Type	* UDP

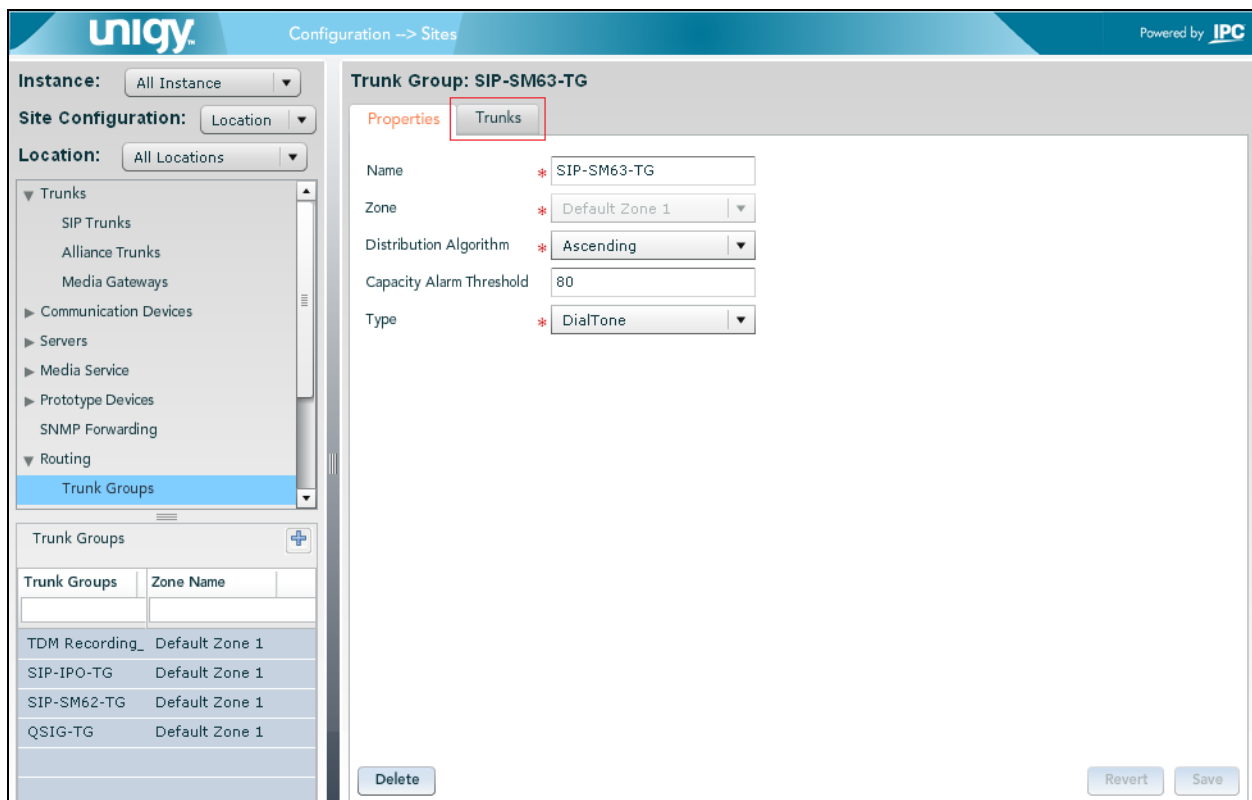
7.3. Administer Trunk Groups

Select **Routing** → **Trunk Groups** in the left pane, and click the **Add** icon () in the lower left pane to add a new trunk group.

The **Trunk Group** screen is displayed in the right pane. In the **Properties** (default) tab, enter a descriptive **Name**, select “Default Zone 1” for the **Zone** field, and select “Ascending” for the **Distribution Algorithm** field.

Click **Save**.

Select the **Trunks** tab in the right pane.



The screenshot displays the UniQy configuration interface. The left pane shows the navigation tree with 'Trunk Groups' selected under 'Routing'. The right pane shows the 'Trunk Group: SIP-SM63-TG' configuration. The 'Properties' tab is active, and the 'Trunks' sub-tab is highlighted. The configuration fields are as follows:

Field	Value
Name	SIP-SM63-TG
Zone	Default Zone 1
Distribution Algorithm	Ascending
Capacity Alarm Threshold	80
Type	DialTone

Below the configuration fields, there is a table listing existing trunk groups:


Trunk Groups	Zone Name
TDM Recording_	Default Zone 1
SIP-IPO-TG	Default Zone 1
SIP-SM62-TG	Default Zone 1
QSIG-TG	Default Zone 1

At the bottom of the right pane, there are buttons for 'Delete', 'Revert', and 'Save'.

Click **Save**.

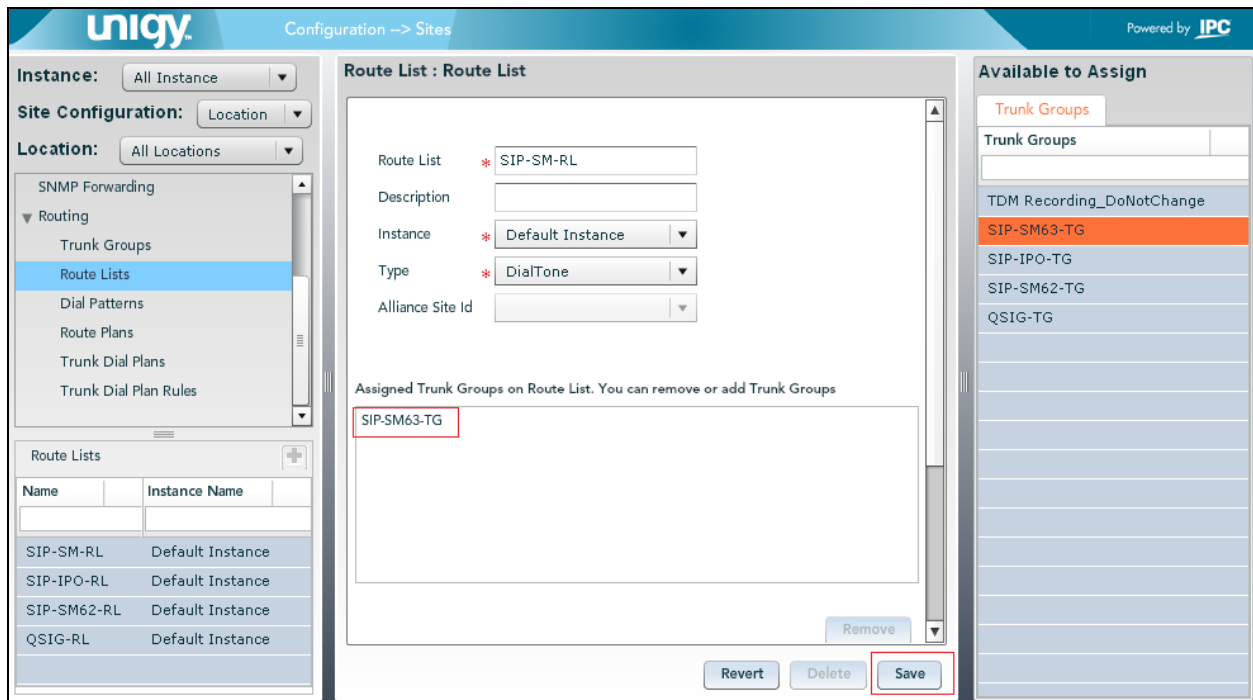
23 of 33
UniV2SM63AAM63

7.4. Administer Route Lists

Select **Routing** → **Route Lists** in the left pane, and click the **Add** icon () in the lower left pane to add a new route list.

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 **Save**.



The screenshot shows the UniGY configuration interface for Route Lists. The left pane shows the navigation menu with 'Route Lists' selected. The middle pane shows the 'Route List : Route List' configuration form. The right pane shows the 'Available to Assign' list of Trunk Groups.

Route List : Route List

Instance: Site Configuration: Location:

Route List: Description: Instance: Type: Alliance Site Id:

Assigned Trunk Groups on Route List. You can remove or add Trunk Groups

Remove

Revert Delete Save

Available to Assign

Trunk Groups

Trunk Groups
TDM Recording_DoNotChange
SIP-SM63-TG
SIP-IPO-TG
SIP-SM62-TG
QSIG-TG

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 right pane.

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 endpoints, in this case “*” meaning any digits will be sent to Session Manager.

Click **Save**.

Once the **Save** button is clicked, the newly created Dial pattern should be displayed under the Dial Patterns section.

The screenshot shows the Unigy Configuration -> Sites interface. The left pane displays a navigation tree with 'Dial Patterns' selected under the 'Routing' section. The right pane is divided into two sections: 'Dial Patterns' and 'Dial pattern Details'.

Dial Patterns Section:

Name	Pattern String	Description	Zone Name

Buttons: Add New, Delete

Dial pattern Details Section:

Properties

Name * ALL Dial Pattern

Zone * Default Zone 1

Description * all

Pattern String * *

Buttons: Revert, Save

Repeat this section to add another dial pattern to reach the PSTN, and include any required prefix by Communication Manager.

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

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 UnigyV2.0.1. For **Called Party**, select the dial pattern for Avaya endpoints from **Section 7.5**. Select “Forward” for **Action**.

Click Save.

[illegible]

The screen is updated with the newly created route plan. Select the route plan, and click **Edit** toward the bottom of the screen.

unigy Configuration -> Sites Powered by **IPC**

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

- Trunks
- Communication Devices
- Servers
- Media Service
- Prototype Devices
- SNMP Forwarding
- Routing
 - Trunk Groups
 - Route Lists
 - Dial Patterns
 - Route Plans**
 - Trunk Dial Plans
 - Trunk Dial Plan Rules

Route Plan

List of Route Plans

UI Name	Calling Party	Destination	Action	Instance Name
QSIG2CM601	*	*	FORWARD	Default Instance
Route-2-IPO	*	*	FORWARD	Default Instance
Route2SM62	*	*	FORWARD	Default Instance
Route2SM63	*	*	FORWARD	Default Instance

Delete Add New Revert Save Sequence Change

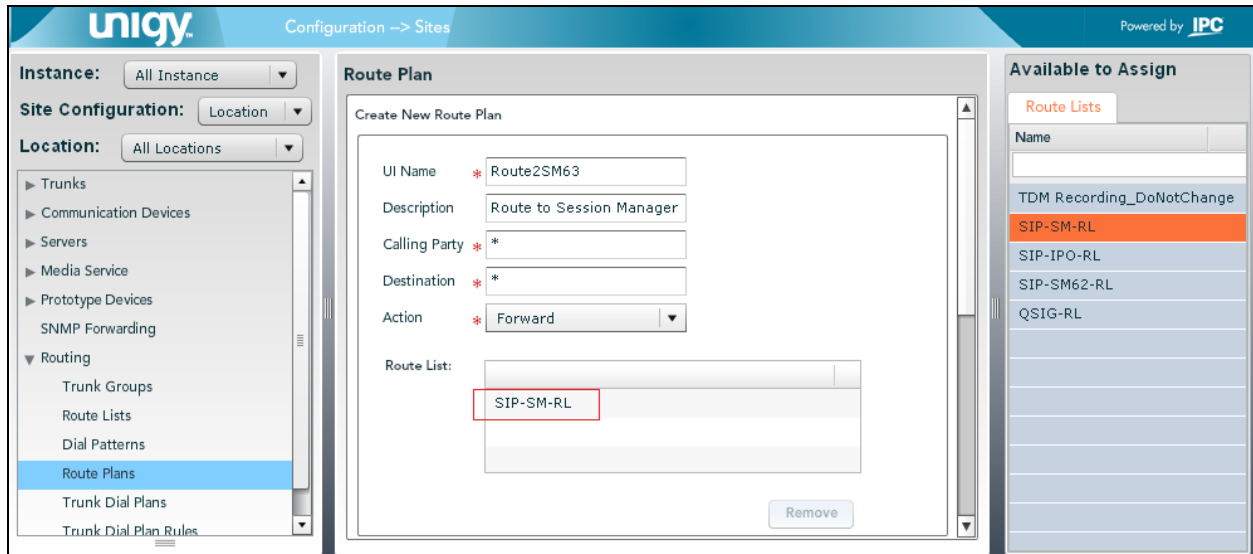
Route Plan Details

Calling Party : *
 Destination : *
 Action : FORWARD
 RouteList:
 Trunk Group:

Edit

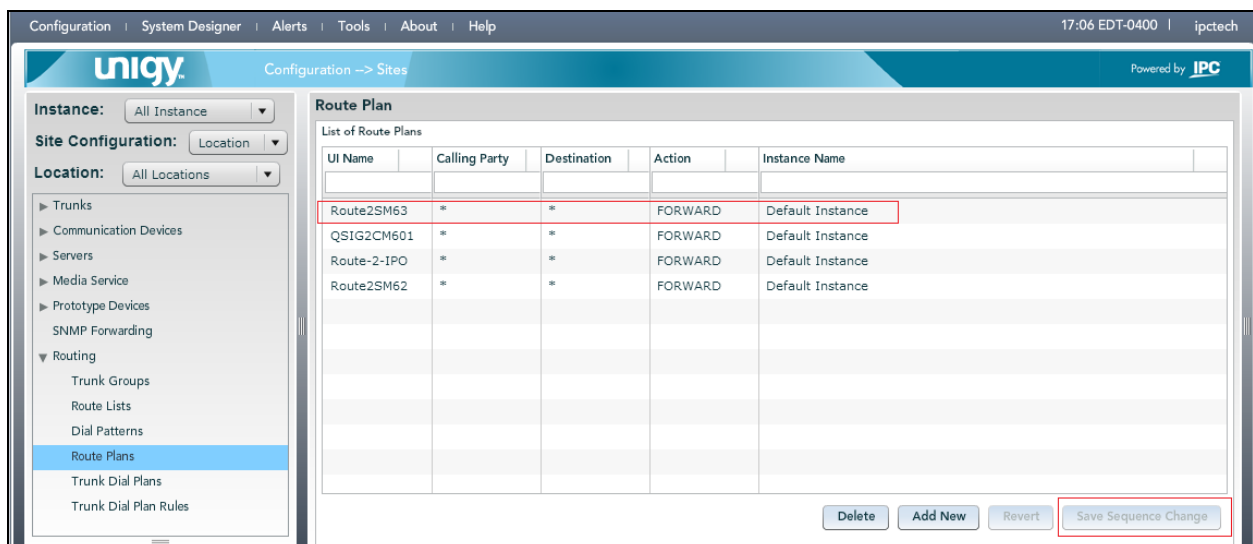
The screen is updated with three panes again, as shown below. In the right pane, select the route list from **Section 7.4** and drag into the **Route List** sub-section in the middle pane, as shown below.

Click **Save** (not shown).



Once the route plan configuration is completed, again select **Routing → Route Plans** in the left pane. List of route plans is displayed. Drag the latest route plan you've created, to the top.

Click the **Save Sequence Change** button to finish the Unigy V2.0.1 configuration.



8. Verification Steps

This section provides tests that may be performed to verify proper configuration of Communication Manager, Session Manager and IPC UnigyV2.0.1.

8.1. Verify Avaya Aura® Communication Manager

From the SAT interface, verify the status of the SIP trunk groups by using the “status trunk n” command, where “n” is the trunk group number administered in Communication Manager. Verify that all trunks are in the “in-service/idle” state as shown below.

```
status trunk 92
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0092/001	T00135	in-service/idle	no
0092/002	T00136	in-service/idle	no
0092/003	T00137	in-service/idle	no
0092/004	T00138	in-service/idle	no
0092/005	T00139	in-service/idle	no
0092/006	T00140	in-service/idle	no
0092/007	T00141	in-service/idle	no
0092/008	T00142	in-service/idle	no
0092/009	T00143	in-service/idle	no
0092/010	T00144	in-service/idle	no

Verify the status of the SIP signaling groups by using the “status signaling-group n” command, where “n” is the signaling group number administered in Communication Manager. Verify that the signaling group is “in-service” as indicated in the **Group State** field, shown below.

```
status signaling-group 92
```

STATUS SIGNALING GROUP	
Group ID:	92
Group Type:	sip
Group State:	in-service

8.2. Verify Avaya Aura® Session Manager

From the System Manager home page (not shown), select **Elements** → **Session Manager** to display the **Session Manager Dashboard** screen (not shown). Select **Session Manager** → **System Status** → **SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen.

Session Manager

Dashboard

Session Manager Administration

Communication Profile Editor

Network Configuration

Device and Location Configuration

Application Configuration

System Status

SIP Entity Monitoring

Managed Bandwidth Usage

Security Module Status

SIP Firewall Status

Registration Summary

User Registrations

Session Counts

User Data Storage

System Tools

Performance

Home / Elements / Session Manager / System Status / SIP Entity Monitoring

Help ?

Session Manager Entity Link Connection Status

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

All Entity Links for Session Manager: SM63

Status Details for the selected Session Manager:

Summary View

10 Items | Refresh

Filter: Enable

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	CM63	10.64.41.21	5060	TCP	FALSE	DOWN	408 Request Timeout	PARTIALLYU
<input type="radio"/>	CM63	10.64.41.21	5061	TLS	FALSE	UP	200 OK	PARTIALLYU
<input type="radio"/>	Modular Messaging	10.64.22.180	5060	TCP	FALSE	DOWN	408 Request Timeout	DOWN
<input type="radio"/>	Uniqv	10.64.49.2	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	Uniqv	10.64.49.2	5060	UDP	FALSE	UP	200 OK	UP
<input type="radio"/>	CM63-Keyur	10.64.10.67	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Alliance	10.64.10.114	5060	TCP	FALSE	UP	200 Options received from a non-SIPX UAC	UP
<input type="radio"/>	Alliance	10.64.10.114	5060	UDP	FALSE	UP	200 Options received from a non-SIPX UAC	UP
<input type="radio"/>	AAM63-VMware	10.64.101.215	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	AAM63-VSP	10.64.45.24	5060	TCP	FALSE	UP	200 OK	UP

Click on the entity names, **Unigy** and **AAM63-VSP**, and verify that **Conn. Status** and **Link Status** are “UP”, as shown below.

Session Manager Entity Link Connection Status

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

All Entity Links for Session Manager: SM63

Summary View

Status Details for the selected Session Manager:

10 Items | Refresh Filter: Enable

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	CM63	10.64.41.21	5060	TCP	FALSE	DOWN	408 Request Timeout	PARTIALLYU
<input type="radio"/>	CM63	10.64.41.21	5061	TLS	FALSE	UP	200 OK	PARTIALLYU
<input type="radio"/>	Modular Messaging	10.64.22.180	5060	TCP	FALSE	DOWN	408 Request Timeout	DOWN
<input type="radio"/>	Unigy	10.64.49.2	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	Unigy	10.64.49.2	5060	UDP	FALSE	UP	200 OK	UP
<input type="radio"/>	CM63-Keyur	10.64.10.67	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Alliance	10.64.10.114	5060	TCP	FALSE	UP	200 Options received from a non-SIPX UAC	UP
<input type="radio"/>	Alliance	10.64.10.114	5060	UDP	FALSE	UP	200 Options received from a non-SIPX UAC	UP
<input type="radio"/>	AAM63-VMware	10.64.101.215	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	AAM63-VSP	10.64.45.24	5060	TCP	FALSE	UP	200 OK	UP

8.3. Verify IPC Unigy V2.0.1

Make a call from/to an IPC turret user to an Avaya endpoint. Verify that the call can be connected with two-way talk paths.

9. Conclusion

These Application Notes describe the configuration steps required for IPC Unigy V2.0.1 to successfully interoperate with Avaya Aura® Messaging 6.3 and Avaya Aura® Session Manager 6.3 in a centralized messaging environment using SIP trunks to Avaya Aura® Session Manager. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

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

- [1] *Administering Avaya Aura® Communication Manager*, Release 6.3, June 2014, Issue 10, Document Number 03-300509
- [2] *Administering Avaya Aura® Session Manager*, Release 6.3, August 2014, Issue 6.
- [3] *Administering Avaya Aura® System Manager*, Release 6.3.9, August 2014.

The following document was provided by IPC

- [4] *Nexus Suite 2.0 SP1 Patch11 or Higher Deployment Guide*, Part Number B02200161, Revision Number 01, available upon request to IPC Support.

©2014 Avaya Inc. All Rights Reserved.

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

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