



Avaya Solution & Interoperability Test Lab

Application Notes for IPC Unigy V2 with Avaya Modular Messaging 5.2 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 to interoperate with Avaya Modular Messaging 5.2 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 to interoperate with Avaya Modular Messaging 5.2 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 used SIP trunks to Avaya Aura® Session Manager, for IPC turret users to obtain voice messaging services from Avaya Modular Messaging. The Avaya Modular Messaging system in the Central site supported local subscribers from Avaya Aura® Communication Manager 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 Modular Messaging voicemail pilot to verify various call scenarios. The Avaya Modular Messaging Web Subscriber Options web-based interface was used to configure subscriber features such as Call Me.

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

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, call sender, and transfer.

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 server.

2.2. Test Results

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

- With shuffling on, the greeting stops in the middle of greeting, during retrieving messages. Recommends shuffling to be OFF.
- IPC does not offer the Coverage feature, therefore coverage to voicemail for the turret users were accomplished by setting the Modular Messaging pilot number as the Call Forwarding destination for the users.
- Receptionist/Personal Operator/Auto Attendant/Transfer – Issues were encountered when using the Receptionist/Personal Operator function provided by Modular Messaging. The “extension does not answer” message was heard when turret is the set to Auto Attendant.
- Find Me – When a turret is a Find Me station, the following symptoms were observed;
 - After the call goes to FindMe, the FindMe station can’t acknowledge the call. The DTMF digit (“#”) did not work.
 - During the Find Me message, the message cuts off and disconnects the call. Calling party was still connected to MM and directly goes to the called party VoiceMail.
- Call Me – When a Turret is a Call Me station, the following symptoms were observed;
 - During the message at the CallMe station, the message cuts off and disconnects the call.
 - When Called is Turret, Call Me feature did not work.
- Transfer – When a turret is a Transfer-to station, the same symptom were observed as Receptionist/Personal Operator/Auto Attendant test cases.

IPC does not expect their users to use these features, so the testing was passed. The issues are listed here for user awareness, and the above mentioned features are not supported with this solution.

2.3. Support

Technical support on IPC Unigy V2 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 consists of the Media Manager and Converged Communication Manager (HA system), and Turrets. SIP trunks are used from IPC Media Manager and Converged Communication Manager (virtual) to Session Manager, to reach Avaya Modular Messaging for voice messaging services.

The detailed administration of basic connectivity among Communication Manager, Session Manager, and Avaya Modular 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, 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 Modular Messaging.

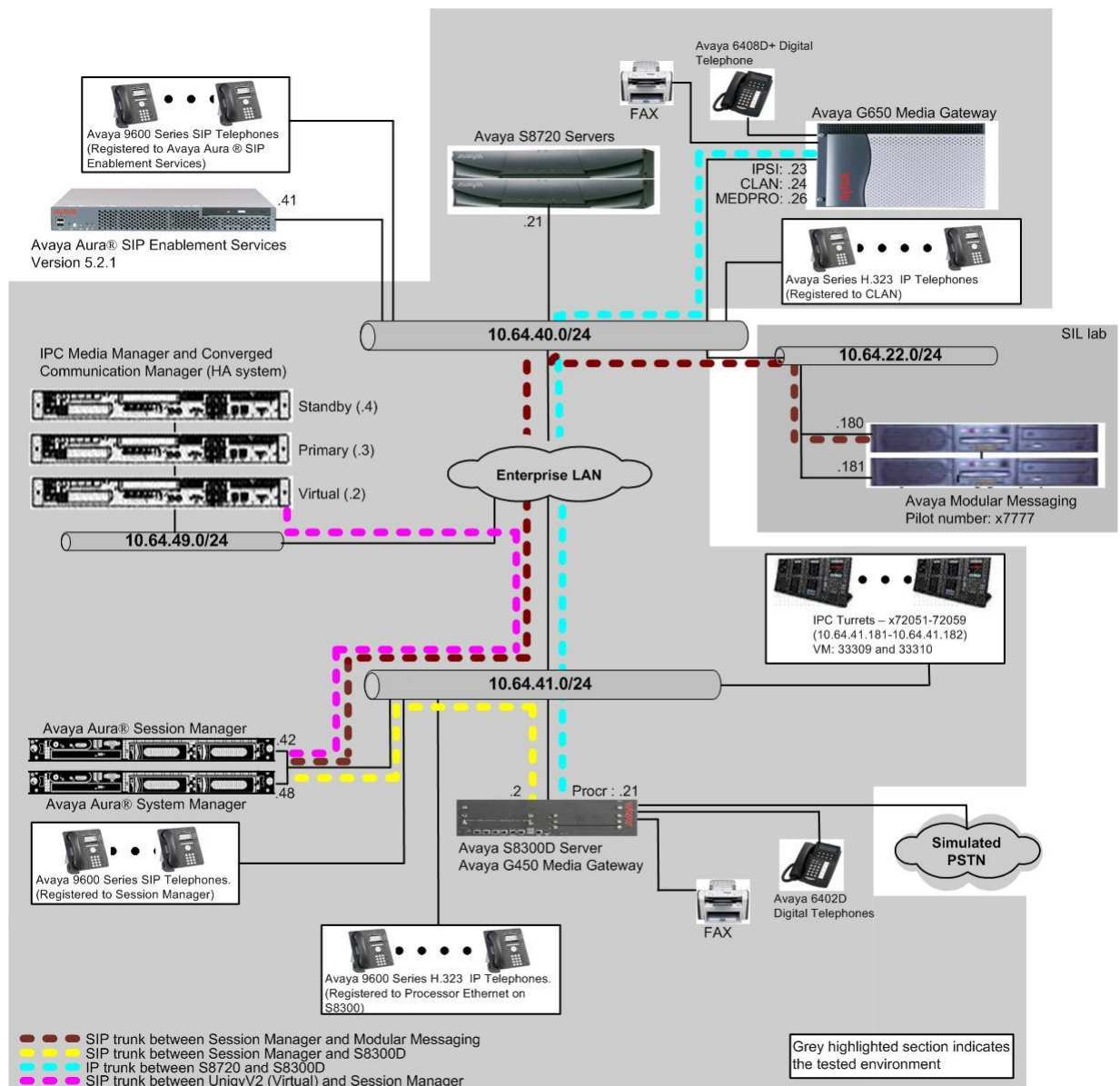


Figure 1: Test Configuration of IPC Unigy system with Avaya Modular Messaging

4. Equipment and Software Validated

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

Equipment	Software
Avaya Modular Messaging <ul style="list-style-type: none">• Messaging Storage Server• Messaging Application Server	5.2 SP9 5.2 SP9
Avaya Aura® Communication Manager on Avaya S8300D Server	6.3.4 (R016x.03.0.124-21291)
Avaya Aura® Session Manager	6.3.5.0.635005
Avaya Aura® System Manager	6.3.5.5.2017
Avaya A175 Desktop Video Device (SIP)	Hardware – 2.0
Avaya 96xx IP Telephone (H.323)	3.1
Avaya 96xx IP Telephone (SIP)	2.6.4
IPC Unigy V2 <ul style="list-style-type: none">• Media Manager• Converged Communication Manager• Turrets	02.00.00.07.0025 02.00.00.07.0025 02.00.00.07.0025

5. Configure Avaya Aura® Communication Manager

The configuration of Communication Manager is not a part of these Application Notes, since the test involves Avaya Modular Messaging. However, during the test, abnormal behavior was observed. During retrieving messages from IPC turrets, messages cut-off in the middle of greeting. To remedy the issue, the following topics are discussed:

- Configure hunt group
- Configure signaling group

5.1. Configure Hunt Group

This section describes the steps for administering a hunt group in Communication Manager, as a work-around solution. The following describes the call path that failed and a work-around.

Failed scenario:

- Turret → Session Manager → Avaya Modular Messaging (x7777)

Work-around solution:

- Turret → Session Manager → Communication Manager Hunt Group (x7776) → Session Manager → Avaya Modular Messaging (x7777)

Enter the **add hunt-group <h>** command; where **h** is an allocated hunt group number. The following fields were configured for the compliance test.

- Group Name – Enter a descriptive name
- Group Extension – Enter a group extension. This is the extension that IPC turrets will be used to retrieve calls.

```
add hunt-group 98                                     Page 1 of 60
                                                    HUNT GROUP

Group Number: 98                                     ACD? n
Group Name: ToMMviaSM                               Queue? n
Group Extension: 7776                               Vector? n
Group Type: ucd-mia                                Coverage Path:
TN: 1                                               Night Service Destination:
COR: 1                                             MM Early Answer? n
Security Code:                                     Local Agent Preference? n
ISDN/SIP Caller Display: mbr-name
```

On **Page 2**, provide the following information:

- Message Center – Enter **sip-adjunct**, indicating the type of messaging adjunct used for this hunt group.
- Voice Mail Number – Enter the Voice Mail Pilot Number, which is x7777.
- Voice Mail Handle – Enter the Voice Mail Handle which is the pilot number, x7777.
- Routing Digit (e.g. AAR/ARS Access Code) – Enter the AAR Access Code as defined in the Feature Access Code form.

display hunt-group 98		Page 2 of 60
HUNT GROUP		
Message Center: sip-adjunct		
Voice Mail Number	Voice Mail Handle	Routing Digits (e.g., AAR/ARS Access Code)
7777	7777	8

5.2. Configure Signaling Group

This section describes a step for disable shuffling (also known as IP-to-IP direct).

An assumption is made that the signaling group is already configured, and here, only shows the field that disables shuffling. Set to **n** on the **Direct IP-IP Audio Connections** field.

display signaling-group 92		Page 1 of 2
SIGNALING GROUP		
Group Number: 92	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? y	Priority Video? y	Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y	Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Near-end Node Name: procr	Far-end Node Name: SM-1	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	RFC 3389 Comfort Noise? y
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? n	
Session Establishment Timer(min): 3	IP Audio Hairpinning? n	
Enable Layer 3 Test? y	Alternate Route Timer(sec): 6	

6. Configure Avaya Modular Messaging MSS

This section provides the procedures for configuring IPC turret users as local subscribers on Avaya Modular Messaging. The subscriber management is configured on the Messaging Storage Server (MSS) component. The configuration procedures include the following areas:

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

6.1. Launch Messaging Administration

Access the MSS web interface by using the URL “http://ip-address” in an Internet browser window, where “ip-address” is the IP address of the MSS 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 **Messaging Administration** screen appears, as shown below.

The screenshot shows the 'Modular Messaging Messaging Administration' interface. The top right corner displays 'This server: 10.64.22.181'. The left sidebar contains a menu with 'Messaging Administration' (highlighted) and 'Server Administration'. The main content area is titled 'Messaging Administration' and contains the text: 'The Web Interface allows you to maintain, troubleshoot, and configure your Messaging System. Select a link from the left-side menu to display the corresponding page.'

6.2. Administer Subscriber Extension Ranges

Select **Messaging Administration** → **Networked Machines** from the left pane, to display the **Manage Networked Machines** screen. Select the MSS server from the table listing, and click **Edit the Selected Networked Machine** toward the bottom right of the screen.

The screenshot shows the 'Manage Networked Machines' screen. The left sidebar menu has 'Networked Machines' selected under 'Messaging Administration'. The main content area features a table with the following data:

Machine	IP Address	Machine Type	Total Subs ▼
alpinemss1	10.64.22.181	local	35

Below the table, there are several buttons: 'Display Report of Networked Machines', 'Delete the Selected Networked Machine', 'Add a New Networked Machine', 'Edit the Selected Networked Machine', 'Display Network Snapshot', and 'Display Report of Networked Machine Ranges'.

The **Edit Networked Machine** screen is displayed. Under the **MAILBOX NUMBER RANGES** section, locate an available entry line and enter the desired starting and ending mailbox numbers to be used for the IPC subscribers as necessary. In the compliance testing, the existing entry covered the 7205x extensions used by the IPC turret users.

Modular Messaging
Messaging Administration

Help Log Off
This server: 10.64.22.181

Messaging Administration

- Subscriber Management
- Activity Log Configuration
- Messaging Attributes
- Classes-of-Service
- Enhanced-Lists
- Sending Restrictions
- System Administration
- Request Remote Update
- Networked Machines
- Trusted Servers

Server Administration

- Configure Using DCT
- TCP/IP Network Configuration
- External Hosts
- MAS Host Setup
- MAS Host Send
- Windows Domain Setup
- Console Reboot Option
- Date/Time/NTP Server
- Syslog Server
- Modem/Terminal Display
- Modem/Terminal Configuration
- Modem/Terminal Removal
- TCP/IP Service Settings

IMAP/SMTP Administration

- SMTP Options
- Mail Options
- IMAP/SMTP Status

Server Information

- Server Status
- Alarm Summary
- Disk Information
- Server Notes
- CMOS Settings
- RAID Status
- Rebuild RAID Status
- Reboot Interval

Utilities

- Rebuild RAID 1 Array

Edit Networked Machine

Machine Name	<input type="text" value="alpinemss1"/>	Password	<input type="password"/>
		Confirm Password	<input type="password"/>
IP Address	<input type="text" value="10.64.22.181"/>	Machine Type	<input type="text" value="tcpip"/>
Mailbox Number Length	<input type="text" value="5"/>	Default Community	<input type="text" value="1"/>
Updates In	<input type="text" value="yes"/>	Updates Out	<input type="text" value="yes"/>
LDAP Port	<input type="text" value="56389"/>	Log Updates In	<input type="text" value="no"/>

MAILBOX NUMBER RANGES		
Prefix	Starting Mailbox Number	Ending Mailbox Number
<input type="text"/>	<input type="text" value="20000"/>	<input type="text" value="29999"/>
<input type="text"/>	<input type="text" value="72001"/>	<input type="text" value="79999"/>
<input type="text"/>	<input type="text" value="33301"/>	<input type="text" value="33310"/>
<input type="text"/>	<input type="text" value="42001"/>	<input type="text" value="49999"/>
<input type="text"/>	<input type="text" value="33201"/>	<input type="text" value="33210"/>

6.3. Administer Subscribers

Select **Messaging Administration** → **Subscriber Management** from the left pane, to display the **Manage Subscribers** screen. For the **Local Subscriber Mailbox Number** field toward the top of the screen, enter the first IPC turret user extension to add as a local subscriber, in this case “72051”. Click **Add or Edit**.

The screenshot shows the Avaya Modular Messaging Messaging Administration interface. The left pane contains a tree view with categories: Messaging Administration, Server Administration, and IMAP/SMTP Administration. The main pane is titled "Manage Subscribers" and displays a form for adding or editing a local subscriber mailbox number (72051). Below this, a table lists subscribers, categorized into Local and Remote. The table has columns for Machine Name, Local Subscriber Mailboxes, Total Subscribers, and Filtered Subscribers. The Local Subscribers row shows 34 local mailboxes, 35 total subscribers, and 35 filtered subscribers. The Remote Subscribers row shows 0 total subscribers and 0 filtered subscribers. A "Page Status" bar is at the bottom.

	Machine Name	Local Subscriber Mailboxes	Total Subscribers	Filtered Subscribers
• Local Subscribers	alpinemss1	34	35	35
• Remote Subscribers	internet		0	0

The **Add Local Subscriber** screen is displayed next. Enter the desired string into the **Last Name**, **First 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 **PBX 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** (not shown). Repeat this section to add all IPC subscribers.

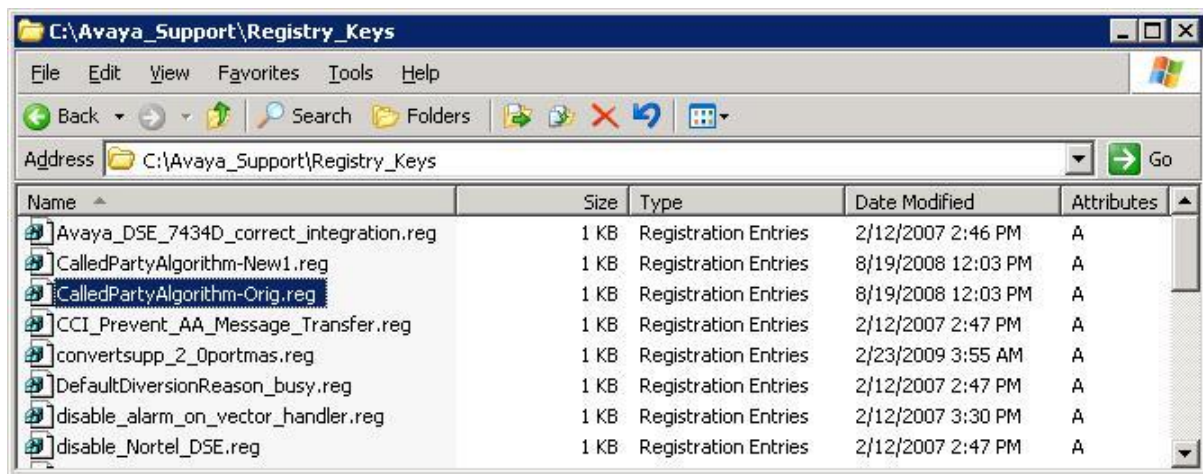
The screenshot shows the Avaya Modular Messaging Administration web interface. The title bar includes the Avaya logo, 'Modular Messaging', 'Messaging Administration', and 'This server: ms'. A navigation menu on the left lists various administration tasks. The main content area is titled 'Add Local Subscriber' and contains a form for adding a new subscriber. The form is titled 'BASIC INFORMATION * (Required Fields)' and includes the following fields:

Field Label	Value
*Last Name	Unigy-V2
First Name	72051
*Password	
*Mailbox Number	72051
*Numeric Address	72051
PBX Extension	72051
*Class Of Service	0 - class00
*Community ID	1

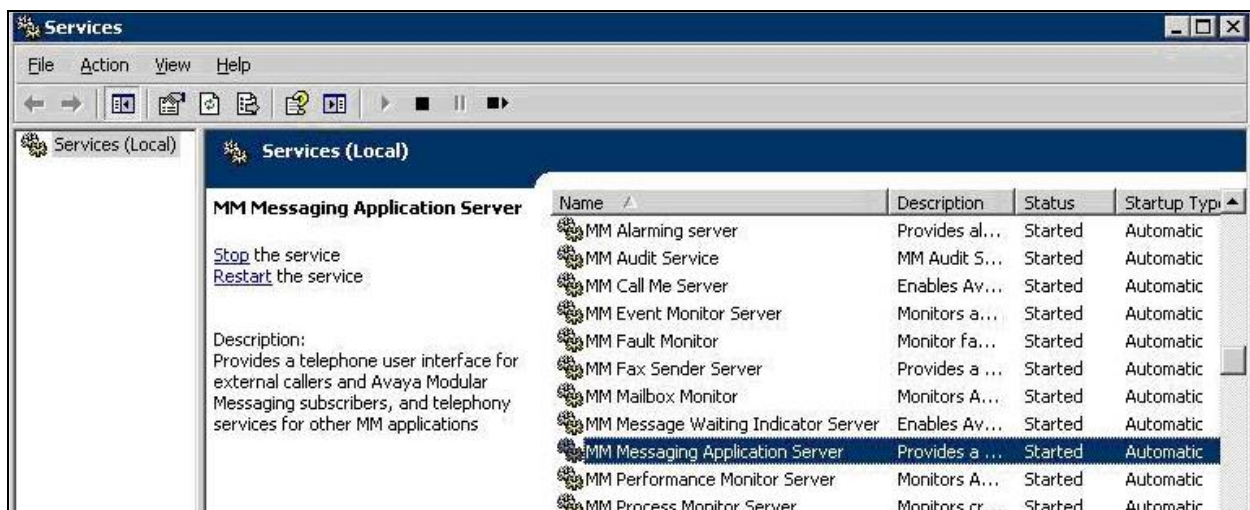
7. Configure Avaya Modular Messaging MAS

This section provides the procedures for configuring the Avaya Messaging Application Server (MAS) servers. A change is needed on each MAS server, to set the way Modular Messaging reads the SIP History Information records for proper integration with IPC. Note that enabling this setting has an impact on the proper identification of calling party number for Vectoring call scenarios.

From the first MAS server, navigate to the **C:\Avaya_Support\Registry_Keys** directory, and double-click on **CalledPartyAlgorithm-Orig.reg**. Confirm to add information in the file to the registry on the Registry Editor window (not shown).



Select **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Services**, to display the **Services** screen. Navigate to the **MM Messaging Application Server** entry, right-click on the entry and select **Restart**. Repeat these procedures on all MAS servers.



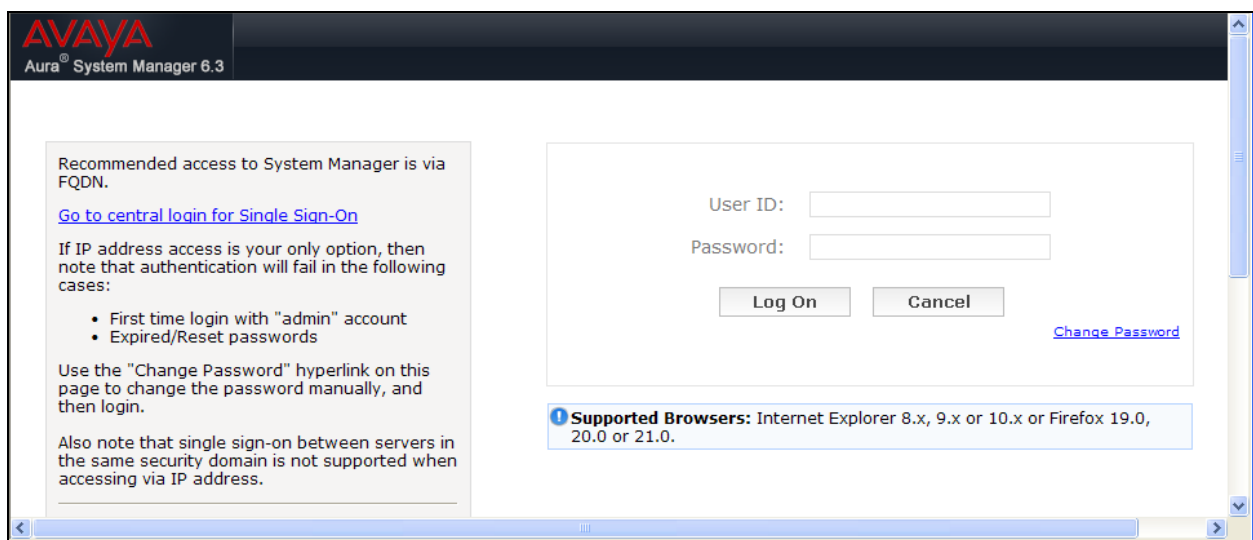
8. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer dial patterns

8.1. Launch System Manager

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



The screenshot shows the Avaya Aura System Manager 6.3 login interface. The header features the Avaya logo and the text "Aura® System Manager 6.3". The main content area is divided into two sections. The left section contains instructions: "Recommended access to System Manager is via FQDN." followed by a link "Go to central login for Single Sign-On". It then states: "If IP address access is your only option, then note that authentication will fail in the following cases:" followed by a bulleted list: "• First time login with 'admin' account" and "• Expired/Reset passwords". Below this, it says: "Use the 'Change Password' hyperlink on this page to change the password manually, and then login." and "Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address." The right section contains the login form with fields for "User ID:" and "Password:", "Log On" and "Cancel" buttons, and a "Change Password" link. At the bottom, a blue box lists "Supported Browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 19.0, 20.0 or 21.0." The browser's address bar is visible at the bottom, showing a URL starting with "https://".

8.2. Administer Dial Patterns

In the subsequent screen (not shown), select **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 Modular Messaging pilot number, in this case “7777”.

AVAYA
Aura® System Manager 6.3

Last Logged on at March 5, 2014 4:08 PM
Help | About | Change Password | Log off admin

Home Routing

Home / Elements / Routing / Dial Patterns

Dial Patterns

New Edit Delete Duplicate More Actions

16 Items Filter: Enable

Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
*	3	3				-ALL-	
#	1	3				-ALL-	
1303	10	12				-ALL-	
21	5	5				-ALL-	To Tom's CM for MWI
2200	5	5				-ALL-	
23	5	5				-ALL-	To Tom's CM for MWI
2800	5	5				-ALL-	
303	10	12				avaya.com	
332	5	5				-ALL-	Alliance via SI
4200	5	5				-ALL-	
7200	5	5				avaya.com	
7205	5	5				-ALL-	
7207	4	5				-ALL-	
7776	4	4				-ALL-	
7777	4	4				-ALL-	

Select : All, None Page 1 of 2

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 Modular 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

Last Logged on at March 5, 2014 4:08 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Home](#)
[Routing](#)

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](#)

2 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		<input type="checkbox"/>	ModularMessaging	
<input type="checkbox"/>	-ALL-		Route2AAM62		<input type="checkbox"/>	AAM62	

Select : [All](#), [None](#)

9. Configure IPC Unigy V2 Converged Communication Manager

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

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

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

9.1. Launch Unigy V2 Management System

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

The screen 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 screenshot shows the login interface for the IPC Unigy V2 Management System. It features the Unigy logo on the left. 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 link to 'Terms of Use'. A 'Login' button is positioned to the right of the checkbox. At the bottom of the form, the following text is displayed: 'IPC Unigy™ Management System', 'Unigy™ Version 02.00.00.07.0025', 'COP Version 02.00.00.00.1888', and '© Copyright 2011-2013 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', 'System Designer', 'Alerts', 'Tools', 'About', and 'Help'. The current page is 'Tools -> Monitoring'. The main content area is titled 'Enterprise' and features a 'Summary' tab. Below the tab, there are two tables: 'Instances' and 'Locations'. The 'Instances' table has columns for 'Instance', 'Total Devices', and 'Devices i...'. The 'Locations' table has columns for 'Location', 'Instance', 'Total D...', and 'Devices in ...'. A 'Refresh' button is located at the bottom right of the tables.

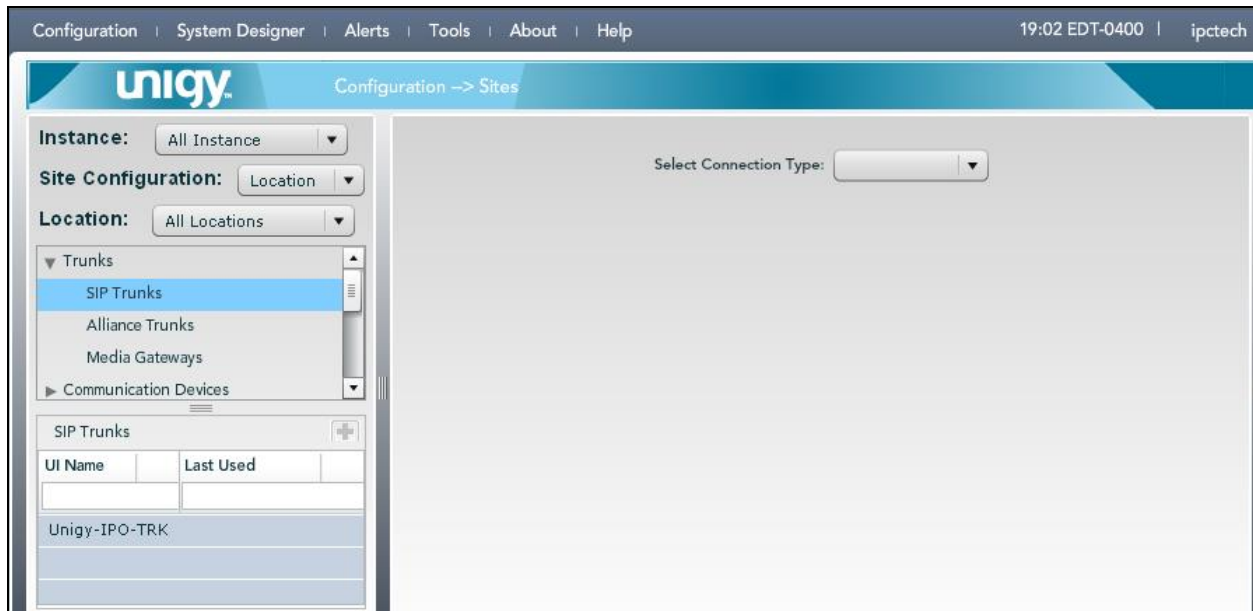
Instance	Total Devices	Devices i...
Default Instance	7	5

Location	Instance	Total D...	Devices in ... 1 ▼
Default Back Room	Default Instance	4	4
Default Front Room	Default Instance	3	1

Refresh

1.1. 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 shows the Unigy configuration interface. The top navigation bar includes the Unigy logo, the path "Configuration -> Sites", and a "Power" button. On the left, a sidebar contains a tree view with categories like "Trunks", "Alliance Trunks", "Media Gateways", "Communication Devices", "Servers", "Media Service", "Prototype Devices", "SNMP Forwarding", and "Routing". The "SIP Trunks" category is selected, showing a table with columns "UI Name" and "Last Used". The table lists "Unigy-IPO-TRK" and "Unigy-SIP-TRK-". The main content area is titled "Trunk: Unigy-SIP-TRK-SM63" and has tabs for "Basic" and "Advanced". The "Basic" tab is active, showing the "DialTone Trunk Configuration" section. This section contains various fields: "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", "A/B Side", "Distant End Name", "PBX Trunk Group Reference", "Trunk Info", "ReINVITE For Media Update" (checked), "Options Supported" (checked), and "Equipped" (checked). At the bottom right, there are buttons for "Delete", "Revert", and "Save".

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

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


Click **Save** at the bottom

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 tabs for 'Basic' and 'Advanced'. The 'Advanced' tab is active, showing the 'DialTone Trunk Configuration' section. The fields and their values are as follows:

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	
Diversion Header	History-Info
Indicate PRACK Support	<input checked="" type="checkbox"/>
Outgoing Transport Type	UDP

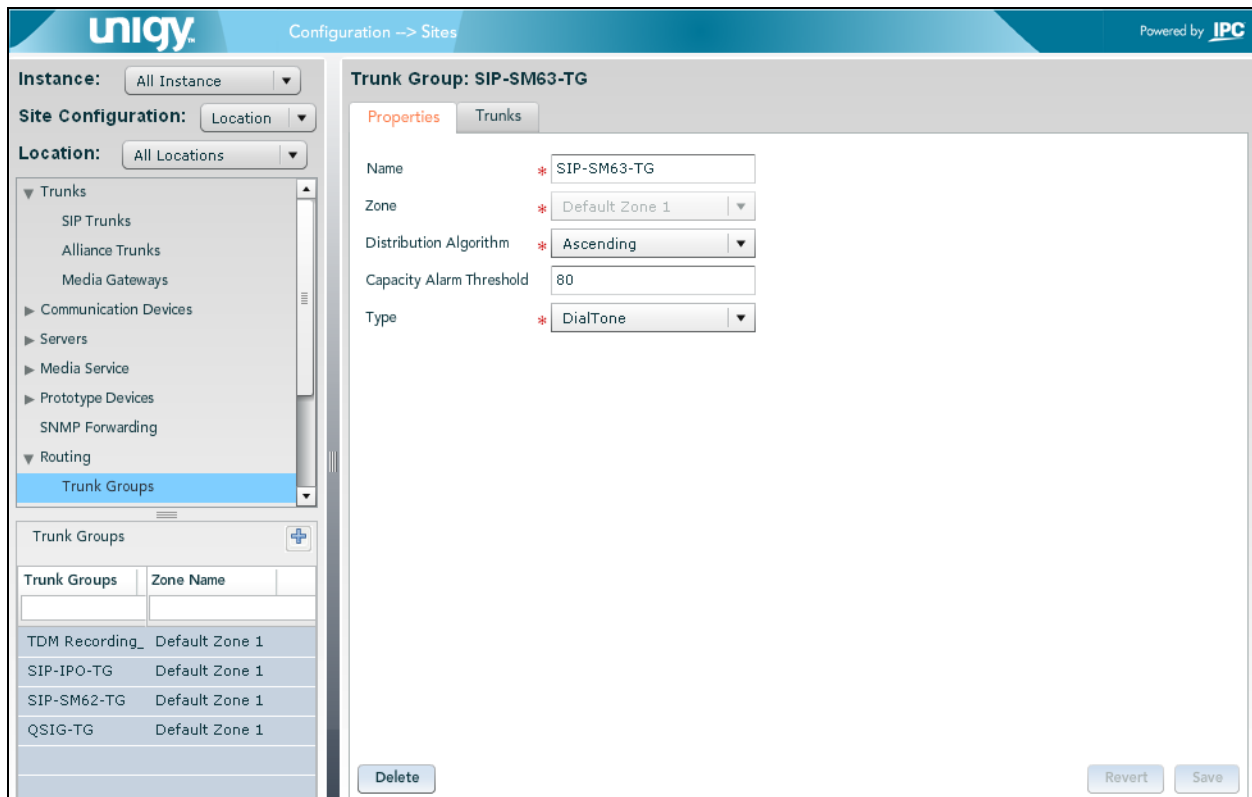
At the bottom right of the configuration area are three buttons: 'Delete', 'Revert', and 'Save'.

1.2. 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** tab, enter a descriptive **Name**, select “Default Zone 1” for the **Zone** field, select “Ascending” for the **Distribution Algorithm** field, and click **Save**.

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



The screenshot shows the UniQy Configuration -> Sites interface. The left pane displays a tree view with 'Trunk Groups' selected under 'Routing'. The right pane shows the 'Trunk Group: SIP-SM63-TG' configuration. The 'Properties' tab is active, showing fields for Name, Zone, Distribution Algorithm, Capacity Alarm Threshold, and Type. The 'Trunks' tab is also visible. At the bottom, there are 'Delete', 'Revert', and 'Save' buttons.

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

The screen is updated with three panes. In the rightmost pane, select the Trunks tab to display a list of trunks. Select the SIP trunk from **Section 1.1** in the rightmost pane and drag to the middle pane as shown below. Click **Save**.


The screenshot displays the Unigy configuration interface with the following components:

- Header:** "unigy" logo, "Configuration -> Sites", and "Powered by IPC".
- Left Pane:**
 - Instance: All Instance
 - Site Configuration: Location
 - Location: All Locations
 - Navigation tree with "Trunk Groups" selected.
 - Trunk Groups table:

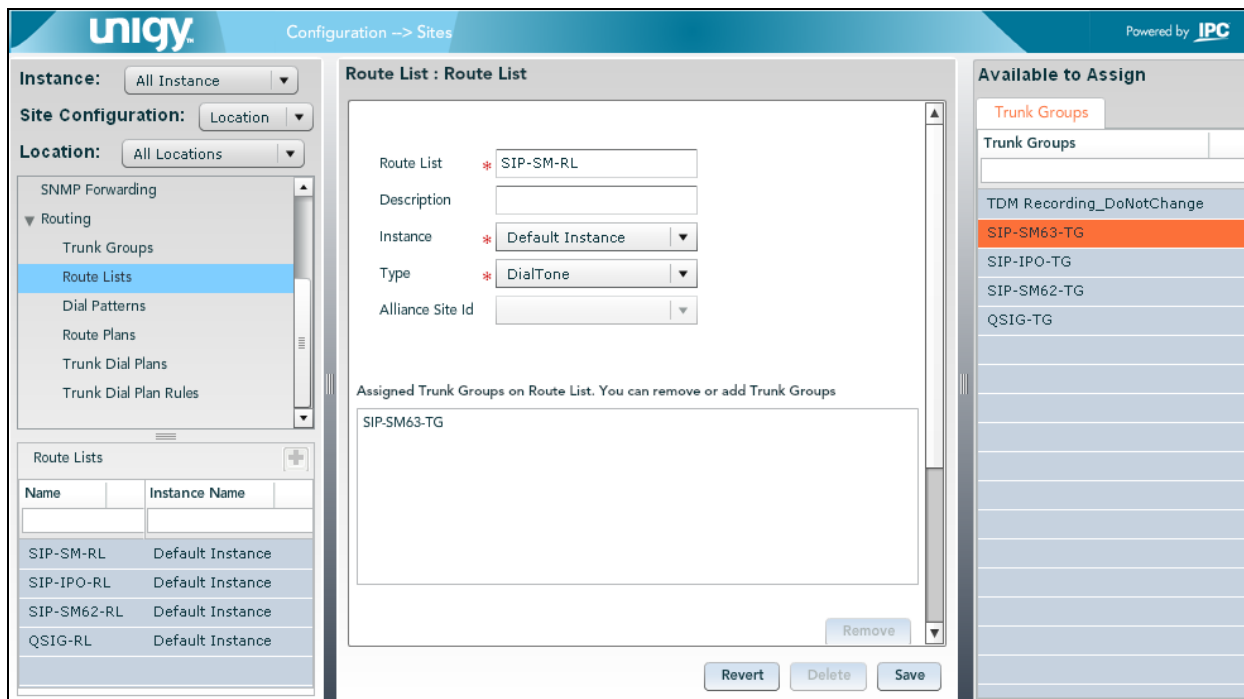
Trunk Groups	Zone Name
TDM Recording_	Default Zone 1
SIP-SM63-TG	Default Zone 1
SIP-IPO-TG	Default Zone 1
SIP-SM62-TG	Default Zone 1
QSIG-TG	Default Zone 1
- Middle Pane (Trunk Group: SIP-SM63-TG):**
 - Properties tab selected.
 - Table with columns "Name" and "Channels":

Name	Channels
Unigy-SIP-TRK-SM63	30
 - Buttons: Remove, Revert, Save.
- Right Pane (Available to Assign):**
 - Trunks tab selected.
 - Table with columns "Name" and "Channels" (empty).

1.3. 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 1.2** 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 UniQy configuration interface. The left pane displays 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: * SIP-SM-RL
Description:
Instance: * Default Instance
Type: * DialTone
Alliance Site Id:

Assigned Trunk Groups on Route List. You can remove or add Trunk Groups
SIP-SM63-TG

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

1.4. 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 UniQy Configuration -> Sites interface. The left pane contains a navigation tree with the following items: Trunks, Communication Devices, Servers, Media Service, Prototype Devices, SNMP Forwarding, Routing (expanded), Trunk Groups, Route Lists, **Dial Patterns** (selected), Route Plans, Trunk Dial Plans, and Trunk Dial Plan Rules. The right pane is titled "Dial Patterns" and contains a table with the following columns: Name, Pattern String, Description, and Zone Name. The table is currently empty. Below the table are "Add New" and "Delete" buttons. Below the table is a section titled "Dial pattern Details" with a "Properties" tab. The "Properties" tab contains the following fields: Name (ALL Dial Pattern), Zone (Default Zone 1), Description (all), and Pattern String (*). At the bottom right of the "Dial pattern Details" section are "Revert" and "Save" buttons.

Name	Pattern String	Description	Zone Name
------	----------------	-------------	-----------

Dial pattern Details

Properties

Name * ALL Dial Pattern

Zone * Default Zone 1

Description * all

Pattern String * *

Revert Save

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

1.5. Administer Route Plans

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

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. For **Called Party**, select the dial pattern for Avaya endpoints from **Section 1.4**. Select “Forward” for **Action**, and 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.

The screenshot shows the 'unigy' Configuration -> Sites interface. The left sidebar contains a navigation menu with the following items: Trunks, Communication Devices, Servers, Media Service, Prototype Devices, SNMP Forwarding, Routing (expanded), Trunk Groups, Route Lists, Dial Patterns, **Route Plans** (selected), Trunk Dial Plans, and Trunk Dial Plan Rules. The main content area is titled 'Route Plan' and contains a 'List of Route Plans' table. The table has columns for UI Name, Calling Party, Destination, Action, and Instance Name. The data rows are as follows:

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

Below the table are buttons for 'Delete', 'Add New', 'Revert', and 'Save Sequence Change'. The 'Route Plan Details' section below the table shows the following fields:

- Calling Party: *
- Destination: *
- Action: FORWARD
- RouteList: (empty text box)
- Trunk Group: (empty text box)

An 'Edit' button is located at the bottom right of the details section.

The screen is updated with three panes again, as shown below. In the right pane, select the route list from **Section 1.3** and drag into the **Route List** sub-section in the middle pane, as shown below. Click **Save** (not shown).

The screenshot displays the UniQy configuration interface for a Route Plan. The interface is organized into three main panes:

- Left Pane:** Contains navigation options. The 'Routing' section is expanded, and 'Route Plans' is selected.
- Middle Pane (Route Plan):** Titled 'Create New Route Plan', it includes the following fields:
 - UI Name: * Route2SM63
 - Description: Route to Session Manager
 - Calling Party: *
 - Destination: *
 - Action: * ForwardBelow these fields is a 'Route List' section with a table containing one entry: 'SIP-SM-RL'. A 'Remove' button is located at the bottom right of this section.
- Right Pane (Available to Assign):** Titled 'Route Lists', it shows a list of available route lists:
 - TDM Recording_DoNotChange
 - SIP-SM-RL (highlighted in orange)
 - SIP-IPO-RL
 - SIP-SM62-RL
 - QSIG-RL

10. Verification Steps

This section provides tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and IPC UnigyV2.

10.1. 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

10.2. 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. Click on the IPC entity name.

Avaya Aura® System Manager 6.3

Last Logged on at October 19, 2013 9:06 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Session Manager × Routing × Session Manager × Home

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

Help ?

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

Registration Summary

User Registrations

Session Counts

System Tools

Performance

SIP Entity Link Monitoring Status Summary

This page provides a summary of Session Manager SIP entity link monitoring status.

SIP Entities Status for All Monitoring Session Manager Instances

Run Monitor

1 Items | Refresh

Filter: Enable

<input type="checkbox"/>	Session Manager	Type	Monitored Entities					Deny	Total
			Down	Partially Up	Up	Not Monitored			
<input type="checkbox"/>	SM63	Core	3	2	6	0	0	11	

Select: All, None

All Monitored SIP Entities

Run Monitor

11 Items | Refresh

Filter: Enable

<input type="checkbox"/>	SIP Entity Name
<input type="checkbox"/>	SB300D-G450-TLS
<input type="checkbox"/>	SB300D-G450-TCP
<input type="checkbox"/>	IPC Uniqy HA

The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that **Conn. Status** and **Link Status** are “UP”, as shown below.

Avaya Aura® System Manager 6.3

Last Logged on at October 19, 2013 9:06 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

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
Registration Summary
User Registrations
Session Counts
System Tools
Performance

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

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: IPC Unigy HA

Status Details for the selected Session Manager:

Summary View

2 Items | Refresh

Filter: Enable

Session Manager I	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/> SM63	10.64.49.2	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/> SM63	10.64.49.2	5060	UDP	FALSE	UP	200 OK	UP

10.3. Verify IPC UnigyV2

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.

11. Conclusion

These Application Notes describe the configuration steps required for IPC Unigy V2 to successfully interoperate with Avaya Modular Messaging 5.2 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**.

12. Additional References

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

- [1] *Administering Avaya Aura® Communication Manager*, Release 6.3, October 2013, Issue 9, Document Number 03-300509
- [2] *Administering Avaya Aura® Session Manager*, Release 6.3, October 2013, Issue 3, Document Number 03-603324
- [3] *Administering Avaya Aura® System Manager*, Release 6.3, October 2013, Issue 3

The following document was provided by IPC

- [4] *Nexus Suite 2.0 SP1 Patch 11 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.