



Avaya Solution & Interoperability Test Lab

Application Notes for IPC Alliance 16 with Avaya Aura® Communication Manager 6.3 via QSIG, and Avaya Aura® Messaging 6.3 via Avaya Aura® Session Manager 6.3 in a Centralized Messaging Environment – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for IPC Alliance 16 to interoperate with Avaya Aura® Communication Manager via QSIG, and Avaya Aura® Messaging 6.3 via Avaya Aura® Session Manager 6.3 in a centralized messaging environment.

IPC Alliance 16 is a trading communication solution. In the compliance testing, IPC Alliance MX used E1 QSIG trunks to Avaya Aura® Communication Manager, for IPC turret users to obtain voice messaging services from Avaya Aura® Messaging. E1 QSIG trunks were used from IPC Alliance 16 to Avaya Aura® Communication Manager, and SIP trunks were used from Avaya Aura® Communication Manager to Avaya Aura® Session Manager to reach Avaya Aura® Messaging. The Avaya Aura® 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.

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 Alliance 16 to interoperate with Avaya Aura® Communication Manager via QSIG, and Avaya Aura® Messaging 6.3 via Avaya Aura® Session Manager 6.3 in a centralized messaging environment.

IPC Alliance 16 is a trading communication solution. In the compliance testing, IPC Alliance 16 used E1 QSIG trunks to Avaya Aura® Communication Manager, for IPC turret users to obtain voice messaging services from Avaya Aura® Messaging. E1 QSIG trunks were used from IPC Alliance 16 to Avaya Aura® Communication Manager, and SIP trunks were used from Avaya Aura® Communication Manager to Avaya Aura® Session Manager to reach Avaya Aura® Messaging. The Avaya Aura® 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 Aura® Messaging voicemail pilot to verify various call scenarios. The Avaya Aura® 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 E1 connection to IPC.

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 subscriber login, greeting, voice message, message waiting indicator, call forward, multiple call forward, personal operator, live attendant, find me (reach me), notify me (call me), call sender, transfer, and vector.

The serviceability testing focused on verifying the ability of IPC Alliance 16 to recover from adverse conditions, such as disconnecting/reconnecting the E1 connection to IPC Alliance 16.

2.2. Test Results

All test cases were executed and passed. 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 Aura® Messaging pilot number as the Call Forwarding destination for the users.

2.3. Support

Technical support on IPC Alliance 16 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, IPC Alliance 16 system at the Remote Site consisted of the System Center, Switching Center and Turrets. E1 QSIG trunks were used from the switching center to Avaya Aura® Communication Manager, and SIP trunks were used from Avaya Aura® Communication Manager to Avaya Aura® Session Manager to reach Avaya Aura® Messaging. In the test configuration, QSIG allowed IPC turret users at the Remote Site to “cover” to Avaya Aura® Messaging at the Central site for voice messaging services.

The configuration of Avaya Aura® Session Manager is performed via the web interface of Avaya Aura® System Manager. The detailed administration of basic connectivity among Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Aura® Messaging is not the focus of these Application Notes and will not be described. These Application Notes will focus on the additional configuration required to support IPC turret users as local subscribers on Avaya Aura® Messaging.

The detailed administration of E1 QSIG trunks between Avaya Aura® Communication Manager and IPC Alliance 16, to enable IPC turret users to reach users on Avaya Aura® Communication Manager and on the PSTN, is assumed to be in place with details described in [3].

A five digit Uniform Dial Plan (UDP) was used to facilitate dialing between the Central and Remote sites. Unique extension ranges were associated with Avaya Aura® Communication Manager user(s) at the Central site (720xx), and IPC turret users at the Remote site (333xx). The Avaya Aura® Messaging pilot number was 7777.

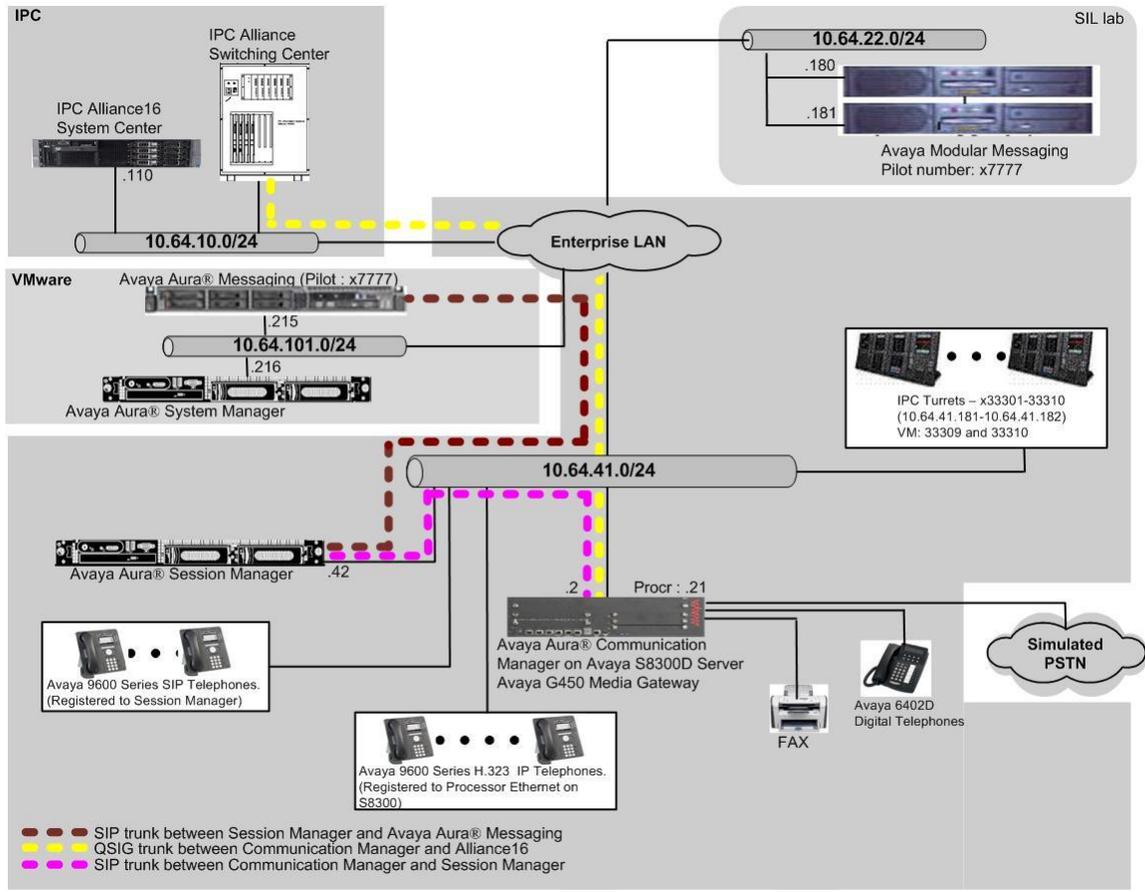


Figure 1: Test Configuration of IPC Alliance with Avaya Aura® Messaging

4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Messaging	6.3 (S016x.03.0.124-21591)
Avaya Aura® Communication Manager on Avaya S8300D Server	6.3 (R016x.03.0.124.0-21754)
Avaya G450 Media Gateway	36.9
Avaya Aura® Session Manager	6.3.9.0.639011
Avaya Aura® System Manager	6.3.9
Avaya 9600 Series IP Telephone (H.323)	3.2.2
Avaya 96x1 Series IP Telephone (H.323)	6.2.3
Avaya 9600 Series IP Telephone (SIP)	2.6.12
Avaya 96x1 Series IP Telephone (SIP)	6.4.1
IPC Alliance 16 <ul style="list-style-type: none">One Management System (OneMS)	16.02.01.09

5. Configure Avaya Aura® Communication Manager

For a QSIG trunk configuration between Communication Manager and IPC Alliance, please refer to [3]. Otherwise, there is no special configuration in Communication Manager.

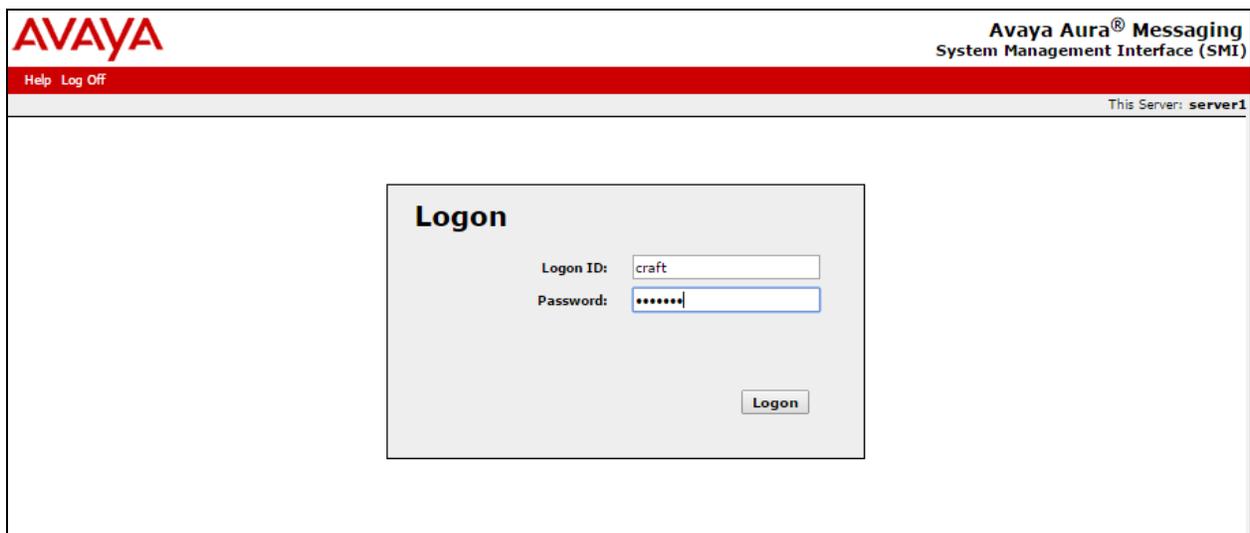
6. Configure Avaya Aura® Messaging

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

6.1. 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 interface. At the top left is the AVAYA logo. At the top right, it reads "Avaya Aura® Messaging System Management Interface (SMI)". Below the logo, there are links for "Help" and "Log Off". In the bottom right corner, it says "This Server: server1". The main content area is a light gray box titled "Logon". Inside this box, there are two input fields: "Logon ID:" with the value "craft" and "Password:" with masked characters "*****". Below these fields 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 This Server: server1

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

6.2. 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: server1

Administration / Messaging

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
server1	10.64.101.215	local	0	13

Buttons: Display Report of Servers, Delete the Selected Networked Server, Add a New Networked Server, Edit the Selected Networked Server, Display Network Snapshot, Help

Left Sidebar Navigation:

- Server Information
 - 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)
 - CallPilot Migration
 - Octel Aria Migration

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: server1

Administration / Messaging

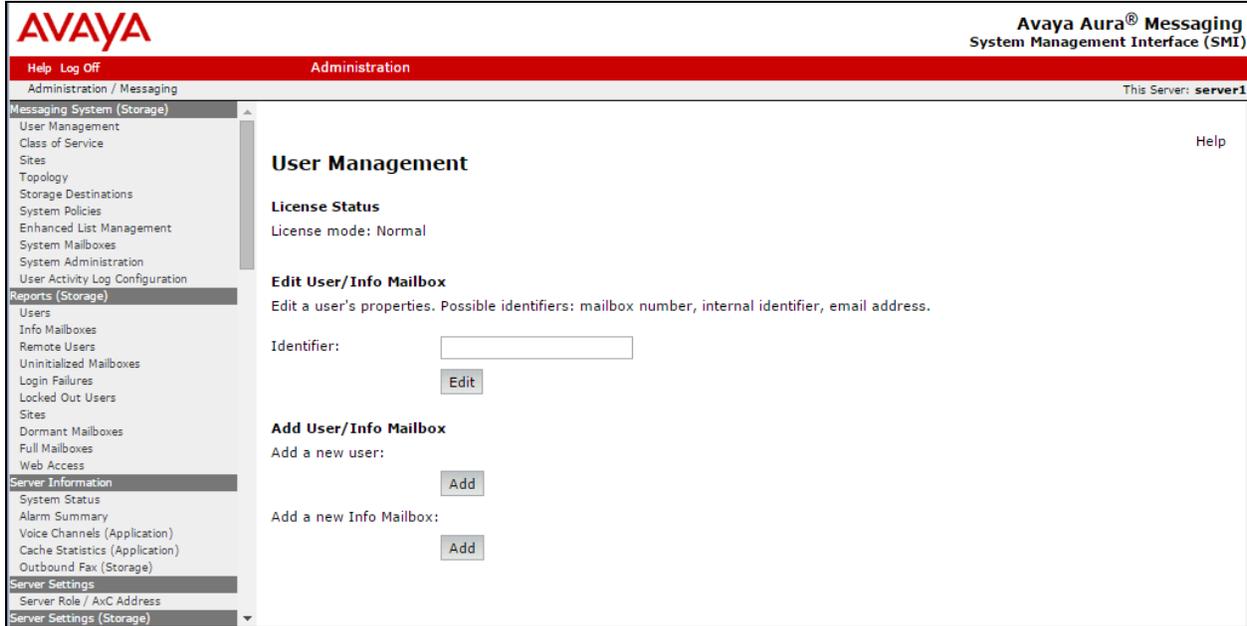
Edit Messaging Server

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

Server Name	<input type="text" value="server1"/>	Password	<input type="password"/>
		Confirm Password	<input type="password"/>
IP Address	<input type="text" value="10.64.101.215"/>	Server 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"/>
Remote LDAP Port	<input type="text" value="56389"/>	Log Updates In	<input type="text" value="no"/>

6.3. 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 Administration / Messaging. The main window is titled "User Management > Properties for New User". The left sidebar contains a navigation menu with categories such as "User Management", "Reports (Storage)", "Server Information", "Server Settings", "Server Settings (Storage)", "Server Settings (Application)", "IMAP/SMTP Settings (Storage)", "Telephony Settings", "Advanced (Application)", "Utilities", and "Logs". The main content area is titled "User Properties" and contains the following fields and options:

- First name:
- Last name:
- Display name:
- ASCII name:
- Site:
- Mailbox number:
- Numeric address:
- Extension:
- Include in Auto Attendant directory
- Additional extension 1:
- Additional extension 2:
- Additional extension 3:
- Additional extension 4:
- Additional extension 5:
- Additional extension 6:
- Additional extension 7:
- Class of Service:
- Pronounceable name:
- MWI enabled:
- Miscellaneous 1:
- Miscellaneous 2:
- New password:
- Confirm password:
- User must change voice messaging password at next login
- Voice messaging password expired
- Locked out from voice messaging

A "Save" button is located at the bottom of the configuration area.

Repeat this section to add all IPC subscribers. During the compliance test, 33309 and 33310 were used.

7. 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

7.1. 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.

Note: During the compliance the System Manager was installed on VMware.

AVAYA
Aura® System Manager 6.3

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

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.

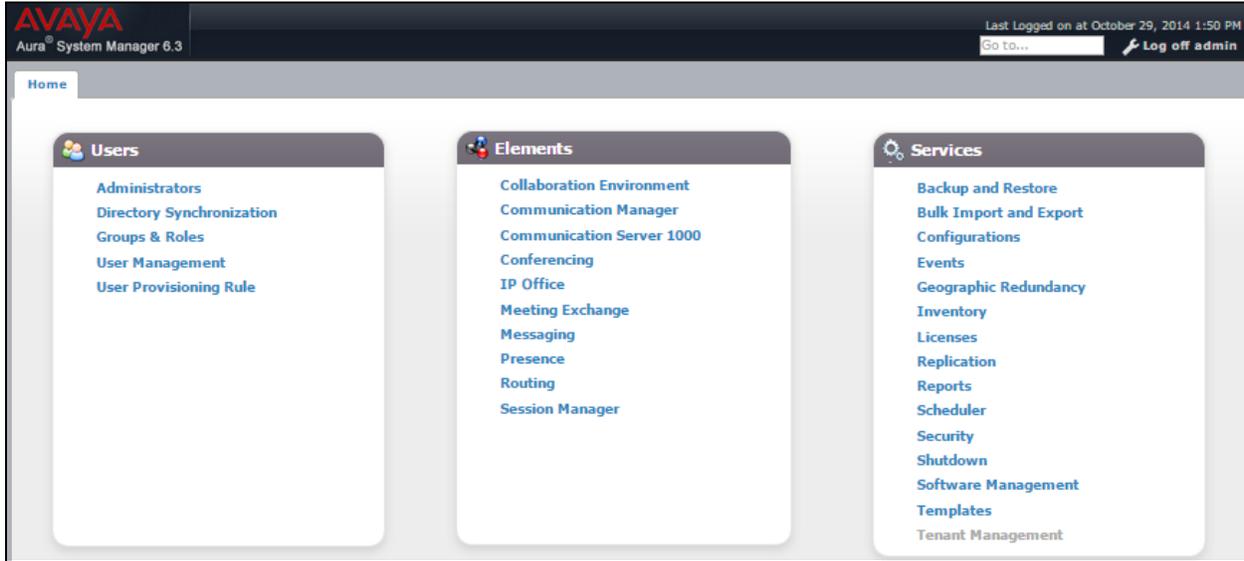
User ID:

Password:

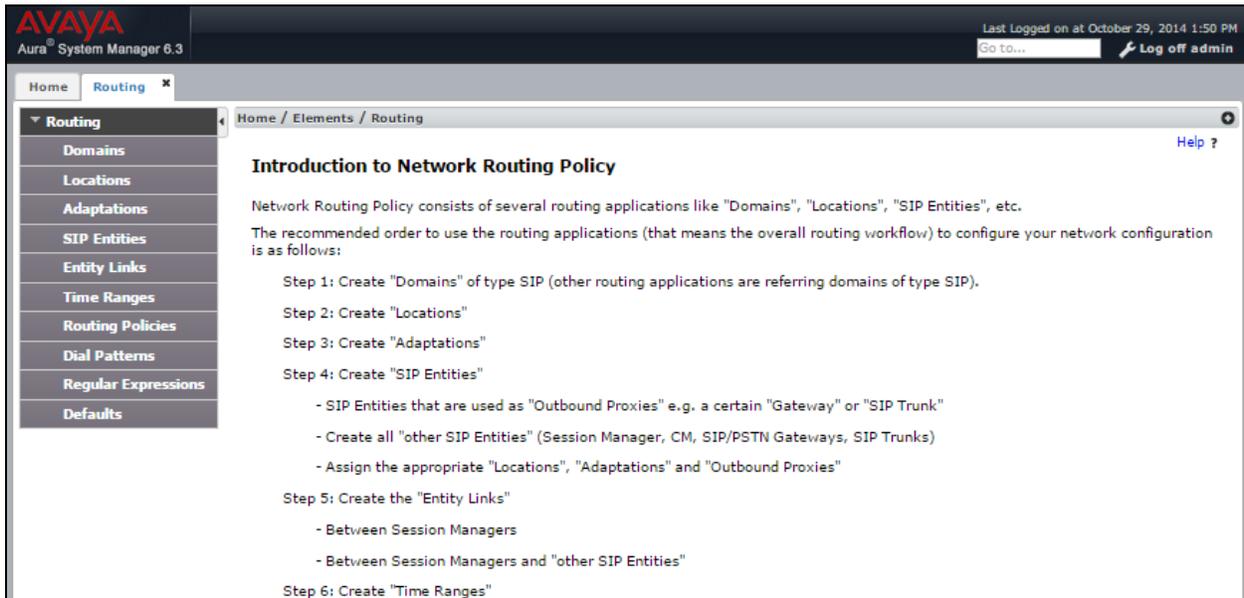
[Change Password](#)

Supported Browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 26.0, 27.0 and 28.0.

The **Main** screen is displayed. Navigate to **Elements** → **Routing**



The **Introduction to Network Routing Policy** screen is displayed next. Navigate to **Routing** → **Dial Patterns** from the left pane.



7.2. Administer Dial Patterns

On the **Dial Pattern Details** screen, click **New** in the subsequent screen (not shown) to add a new dial pattern for Aura® Messaging to reach IPC turret users.

The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern:** A dial pattern to match.
- **Min:** The minimum number of digits to be matched.
- **Max:** The maximum number of digits to be matched.
- **SIP Domain:** Select the applicable SIP domain for the relevant Communication Manager.
- **Notes:** Any desired description.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create a new policy for reaching IPC turret users with extensions 333xx. In the compliance testing, “Apply The Selected Routing Policies to All Originating Locations” was selected as the Originating Location, and the Routing Policies is set to Route2CM63.. Retain the default values in the remaining fields. Aura® Messaging will dial out to IPC turret users for features such as Call Sender, and the call will be delivered as SIP from Aura® Messaging to Session Manager, and SIP from Session Manager to Communication Manager, and then QSIG from Communication Manager to Alliance 16.

The screenshot displays the Avaya Aura System Manager 6.3 interface. The top navigation bar includes 'Home' and 'Routing'. The left sidebar lists various configuration options, with 'Dial Patterns' selected. The main content area is titled 'Dial Pattern Details' and contains a 'General' section with the following fields:

- Pattern:** 333
- Min:** 5
- Max:** 5
- Emergency Call:**
- Emergency Priority:** 1
- Emergency Type:** (empty)
- SIP Domain:** -ALL-
- Notes:** To Alliance using QSIG via CM

Below the 'General' section is the 'Originating Locations and Routing Policies' section, which includes an 'Add' button and a table with one item:

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
-ALL-		Route2CM63	0	<input type="checkbox"/>	CM63	

The table also includes a 'Filter: Enable' button and a 'Select: All, None' option at the bottom.

The following screen shows the dial pattern for the pilot number, 7777, to Aura® Messaging.

AVAYA
Aura® System Manager 6.3

Last Logged on at January 6, 2015 4:07 PM
Go to... Log off admin

Home Routing *
Home / Elements / Routing / Dial Patterns

Dial Pattern Details Commit Cancel [Help ?](#)

General

* Pattern: 7777
 * Min: 4
 * Max: 4
 Emergency Call:
 Emergency Priority: 1
 Emergency Type:
 SIP Domain: avaya.com
 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 type="checkbox"/>	AAM63-VMware	
<input type="checkbox"/>	-ALL-		Route2AAM63-VSP	0	<input checked="" type="checkbox"/>	AAM63-VSP	

Select : All, None

8. Configure IPC Alliance 16

For the compliance test, no special configuration is needed for the IPC Alliance 16. For a QSIG trunk configuration between Communication Manager and IPC Alliance, please refer to [3].

9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Aura® Messaging, Avaya Aura® Session Manager, and IPC Alliance 16.

Place a call from an IPC turret user to the Aura® Messaging pilot number. Verify that Aura® Messaging recognizes the calling party as a local subscriber.

10. Conclusion

These Application Notes describe the configuration steps required for IPC Alliance 16 to successfully interoperate with Avaya Aura® Messaging 6.3 and Avaya Aura® Session Manager 6.3 in a centralized messaging environment using QSIG trunks to Avaya Aura® Communication Manager 6.3. All feature and serviceability test cases were completed with an observation noted in **Section 2.2**.

11. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Release 6.3, Issue 10, June 2014, available at <http://support.avaya.com>
2. *Administering Avaya Aura® Messaging*, Release 6.3.2, Issue 1, December 2014, available at <http://support.avaya.com>
3. *Application Notes for IPC Alliance 16 with Avaya Aura® Communication Manager 6.3 using QSIG Trunks*, Issue 1.0

©2015 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.