



Avaya Solution & Interoperability Test Lab

Application Notes for IPC Alliance MX 15.03 with Avaya Modular Messaging 5.2 and 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 MX 15.03 to interoperate with Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3, and Avaya Modular Messaging 5.2 in a centralized messaging environment.

IPC Alliance MX 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 Modular Messaging. SIP trunks were used from Avaya Aura® Communication Manager to Avaya Aura® Session Manager to reach 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.

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 MX 15.03 to interoperate with Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3, and Avaya Modular Messaging 5.2 in a centralized messaging environment.

IPC Alliance MX 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 Modular Messaging. SIP trunks were used from Avaya Aura® Communication Manager to Avaya Aura® Session Manager to reach 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 E1 connection to IPC Alliance MX.

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, auto attendant, find me, call me, call sender, and transfer.

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

2.2. Test Results

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

- 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.
- During For multiple call forward scenarios involving calls forwarded to the called party's forward-to extension and then covered subsequently to Modular Messaging based on the coverage setting at the forward-to extension, the call does not get the called party greeting, instead, it keeps ringing at the forward-to station.

2.3. Support

Technical support on IPC Alliance MX can be obtained through the following:

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

3. Reference Configuration

As shown in the reference configuration below, IPC Alliance MX at the Remote Site consisted of the Alliance MX, System Center, and Turrets. E1 QSIG trunks were used from IPC Alliance MX to Avaya Aura® Communication Manager, and SIP trunks were used from Avaya Aura® Communication Manager to Avaya Aura® Session Manager to reach Avaya Modular Messaging. In the test configuration, QSIG allowed IPC turret users at the Remote Site to “cover” to Avaya Modular 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 Modular 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 Modular Messaging.

The detailed administration of E1 QSIG trunks between Avaya Aura® Communication Manager and IPC Alliance MX, 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 (72xxx), and IPC turret users at the Remote site (33xxx). The Avaya Modular Messaging pilot number was 7777.

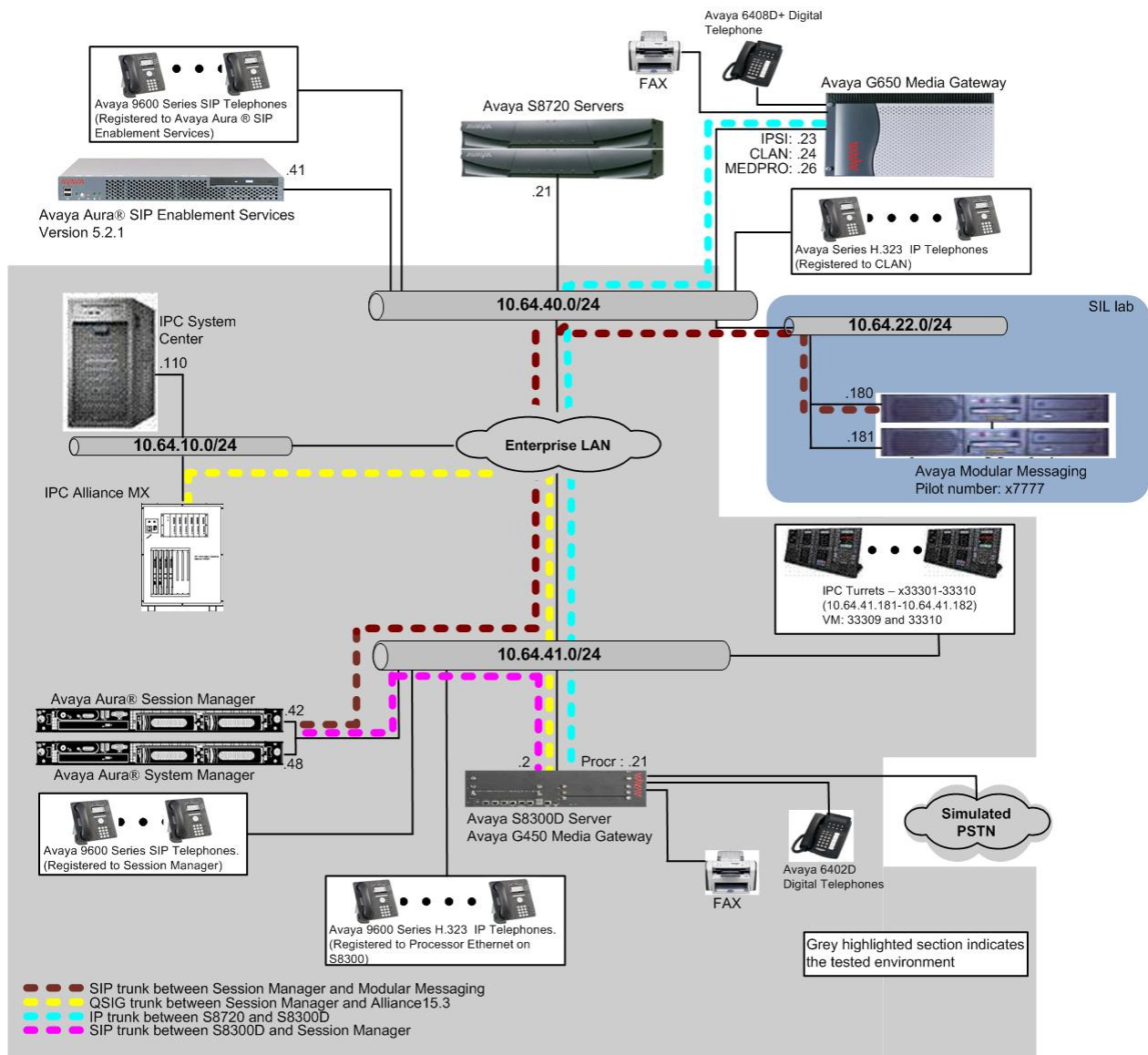


Figure 1: Test Configuration of IPC Alliance with Avaya Modular Messaging

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 ServerMessaging Application Server	5.2 SP9 5.2 SP9
Avaya Aura® Communication Manager on Avaya S8300D Server	6.3 (R016x.03.0.124.0-20553)
Avaya G450 Media Gateway	33.13
Avaya Aura® Session Manager	6.3.2.0.632023
Avaya Aura® System Manager	6.3.2.4.1529
Avaya 9600 Series IP Telephone (H.323)	3.1
Avaya 9600 Series IP Telephone (SIP)	2.6.4
Avaya A175 Desktop Video Device (SIP)	1.1.1
IPC <ul style="list-style-type: none">System CenterQSIG Line Card	15.03.00.18c 15.03.00.17a

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.

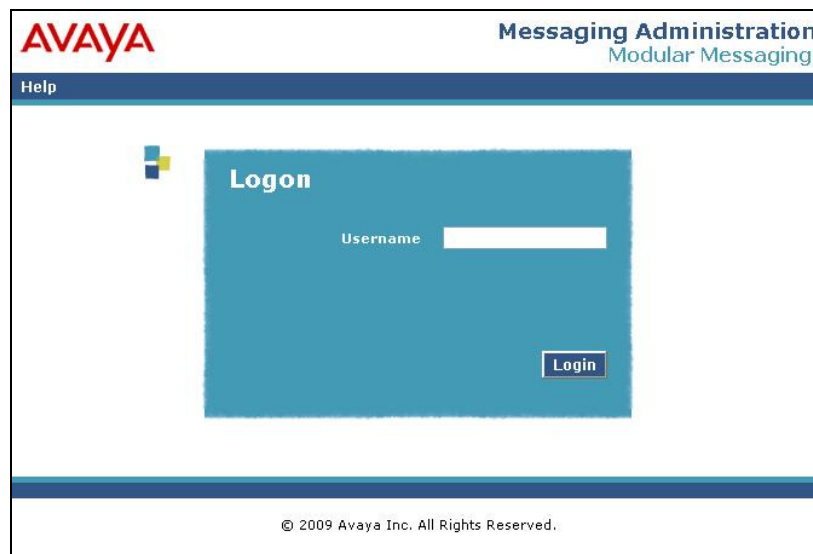
6. Configure Avaya Modular Messaging MSS

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 screenshot displays the Avaya Messaging Administration web interface. At the top left is the AVAYA logo. To its right, the text "Messaging Administration" and "Modular Messaging" is displayed. Below this is a "Help" link. The main content area features a blue "Logon" box with a "Username" label and a text input field. A "Login" button is located at the bottom right of the box. A small Avaya logo icon is positioned to the left of the Logon box. At the bottom of the page, a copyright notice reads: "© 2009 Avaya Inc. All Rights Reserved."

The **Messaging Administration** screen appears, as shown below.

The screenshot shows the Avaya Modular Messaging Messaging Administration interface. The top header includes the Avaya logo, the title 'Modular Messaging Messaging Administration', and the server name 'This server: mss1'. A navigation menu on the left lists various options under 'Messaging Administration' and 'Server Administration'. The main content area is titled 'Messaging Administration' and contains a brief description of the web interface's purpose.

AVAYA Modular Messaging
Messaging Administration
This server: mss1

Help Log Off

▼ 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

Messaging Administration

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 in the Avaya Modular Messaging interface. The left navigation menu is expanded to show 'Networked Machines' under the 'Messaging Administration' section. The main area features a table with columns for Machine, IP Address, Machine Type, and Total Subs. A single entry, 'alpinemss1', is listed. Below the table are several action buttons for managing the networked machines.

AVAYA Modular Messaging
Messaging Administration
This server: mss1

Help Log Off

▼ 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

Manage Networked Machines


Machine	IP Address	Machine Type	Total Subs
alpinemss1	10.64.22.181	local	28

Display Report of Networked Machines Delete the Selected Networked Machine

Add a New Networked Machine Edit the Selected Networked Machine

Display Network Snapshot Display Report of Networked Machine Ranges

The **Edit Networked Machine** screen is displayed. Under the **MAILBOX NUMBER RANGES** sub-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 33xxx extensions used by the IPC turret users.



Modular Messaging
 Messaging Administration

[Help](#) [Log Off](#)
This server: mss1

- ▼ **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

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"/>

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 “33309”. Click **Add or Edit**.

The screenshot shows the Avaya Modular Messaging Messaging Administration interface. The left pane contains a tree view with 'Messaging Administration' expanded, showing 'Subscriber Management' selected. The main area is titled 'Manage Subscribers'. At the top, there is a field for 'Local Subscriber Mailbox Number' with the value '33309' and an 'Add or Edit' button. Below this is a table with columns: 'Machine Name', 'Local Subscriber Mailboxes', 'Total Subscribers', and 'Filtered Subscribers'. The table lists two categories: 'Local Subscribers' and 'Remote Subscribers'. The 'Local Subscribers' row shows 'alpinemss1' with 27 local mailboxes, 28 total subscribers, and 28 filtered subscribers. The 'Remote Subscribers' row shows 'internet' with 0 local mailboxes, 0 total subscribers, and 0 filtered subscribers. Each row has a 'Filter' button and a 'Manage' button. The bottom of the interface includes a 'Help' button and a status bar indicating 'This server: mss1'.

	<u>Machine Name</u>	<u>Local Subscriber Mailboxes</u>	<u>Total Subscribers</u>	<u>Filtered Subscribers</u>
• Local Subscribers	alpinemss1	27	28	28
• 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**, **PBX Extension**, and **Email Handle** fields. Select the appropriate **Class Of Service**, and retain the default values in the remaining fields. Repeat this section to add all IPC subscribers.

AVAYA Modular Messaging
Messaging Administration
This server: mss1

Help Log Off

Add Local Subscriber

BASIC INFORMATION
* (Required Fields)

*Last Name	IPC	First Name	33309
*Password	*Mailbox Number	33309
*Numeric Address	33309	PBX Extension	
*Class Of Service	0 - class00	*Community ID	1

SUBSCRIBER DIRECTORY

Email Handle	33309 @alpinemss1.avaya.com	Telephone Number	
Common Name		ASCII Version of Name	

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.

The screenshot shows the Avaya Aura System Manager 6.3 login interface. At the top, the Avaya logo is on the left and the text "Avaya Aura® System Manager 6.3" is on the right. Below this is a red navigation bar with the text "Home / Log On". The main heading is "Log On". On the left, there is a box with the following text: "Recommended access to System Manager is via FQDN." followed by a link "Go to central login for Single Sign-On". Below this, it says "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". To the right of this box are two input fields: "User ID:" and "Password:". At the bottom right, there are two buttons: "Log On" and "Cancel", and a link "Change Password" below them.

AVAYA Avaya Aura® System Manager 6.3

Home / Log On

Log On

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

User ID:

Password:

[Change Password](#)

7.2. Administer Dial Patterns

Select **Routing** → **Dial Patterns** (not shown) from the left pane, and click **New** in the subsequent screen (not shown) to add a new dial pattern for Modular 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 domain for the relevant Communication Manager.
- **Notes:** Any desired description.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create a dial pattern for reaching IPC turret users with extensions 33xxx. In the compliance testing, the policy allowed for call origination from all location, and the destination is Communication Manager, as shown below. Retain the default values in the remaining fields. Modular Messaging will dial out to IPC turret users for features such as Call Sender, and the call will be delivered as SIP from Modular Messaging to Session Manager, and SIP from Session Manager to Communication Manager, and then QSIG from Communication Manager to Alliance MX.

Avaya Aura® System Manager 6.3

Last Logged on at August 19, 2013 3:05 PM
Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Dial Patterns

Dial Pattern Details [Commit] [Cancel] Help ?

General

* Pattern: 333

* Min: 5

* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes: Alliance Turret thru QSIG

Originating Locations and Routing Policies

[Add] [Remove]

1 Item Refresh Filter: Enable

	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		Route2G450		<input type="checkbox"/>	S8300D-G450-63	

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

Avaya Aura® System Manager 6.3

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

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: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

2 Items Refresh

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-		Route2AAM		<input checked="" type="checkbox"/>	AAM	

8. Configure IPC Alliance MX

For the compliance test, no special configuration is needed for the IPC Alliance MX. 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 Modular Messaging, Avaya Aura® Session Manager, and IPC Alliance MX.

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

10. Conclusion

These Application Notes describe the configuration steps required for IPC Alliance MX 15.03 to successfully interoperate with Avaya Modular Messaging 5.2 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, May 2013, available at <http://support.avaya.com>.
2. *Avaya Modular Messaging for the Avaya Message Store Server (MSS) Configuration*, Release 5.0, February 2009, available at <http://support.avaya.com>.
3. *Application Notes for IPC Alliance MX 15.03 with Avaya Aura® Communication Manager 6.3 using QSIG Trunks*, Issue 1.0, available at <http://support.avaya.com>.

©2013 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.