



Avaya Solution & Interoperability Test Lab

Application Notes for IPC Alliance MX 15.03 with Avaya Aura® Messaging 6.2 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 Aura® Messaging 6.2 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 Aura® Messaging. 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 MX 15.03 to interoperate with Avaya Aura® Messaging 6.2 and Avaya Aura® Session Manager 6.3 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 Aura® Messaging. 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 Sender.

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, operator/live attendant, 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 Aura® 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 Aura® 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 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 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 (333xx). The Avaya Aura® Messaging pilot number was 7777.

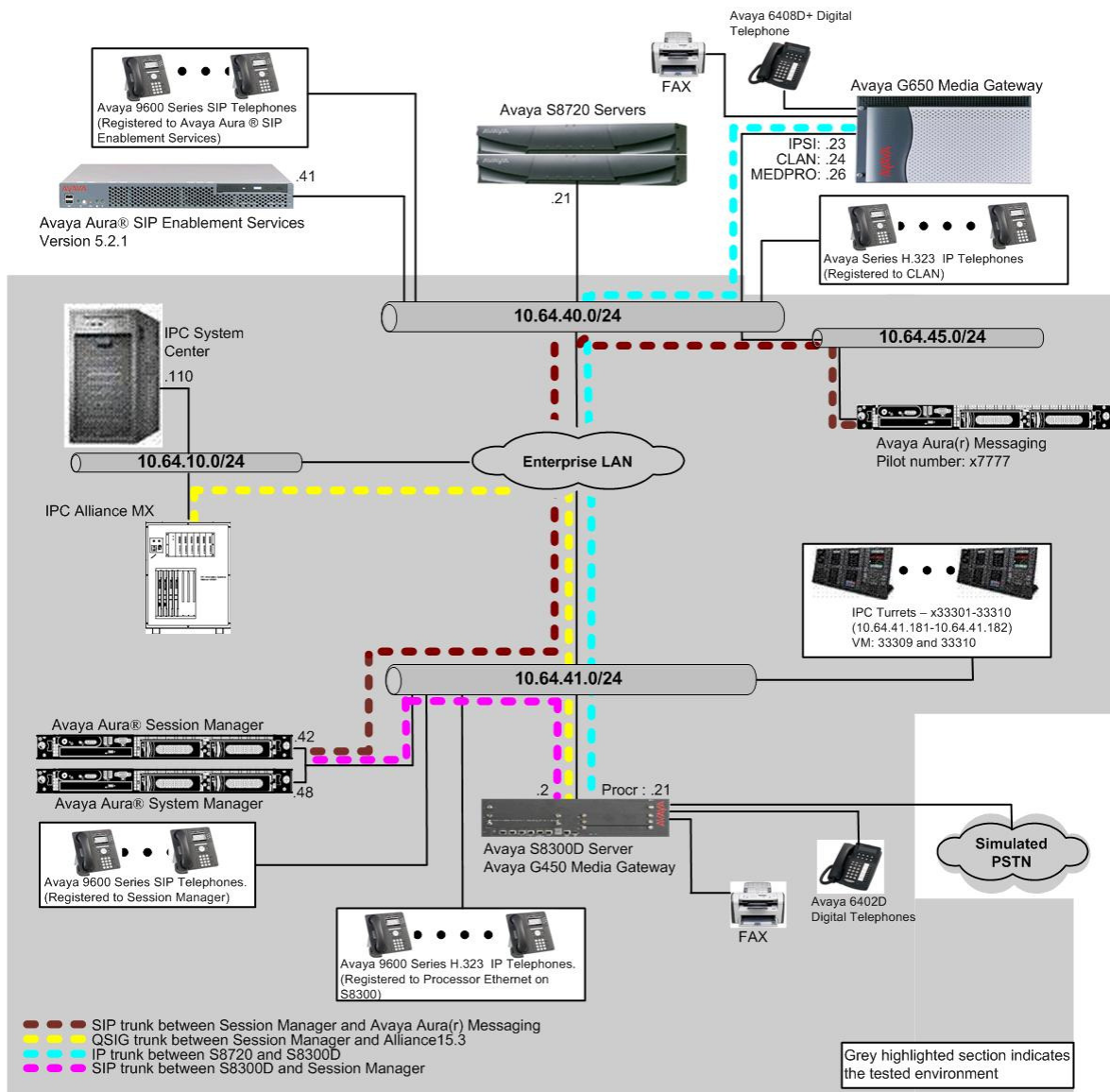


Figure 1: Test Configuration of IPC Alliance with Avaya Aura® Messaging

4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Messaging	6.2
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 Center• QSIG Line Card	15.03.00.18c 15.03.00.17a

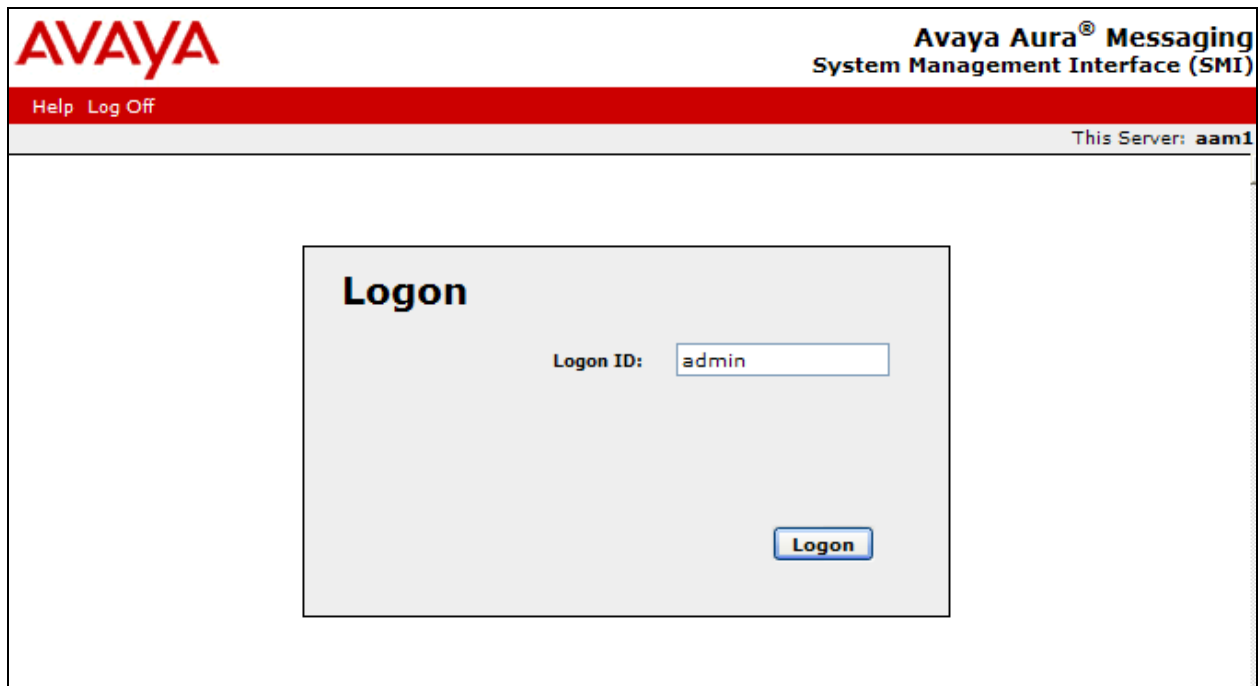
5. Configure Avaya Aura® Communication Manager

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 Aura® Messaging

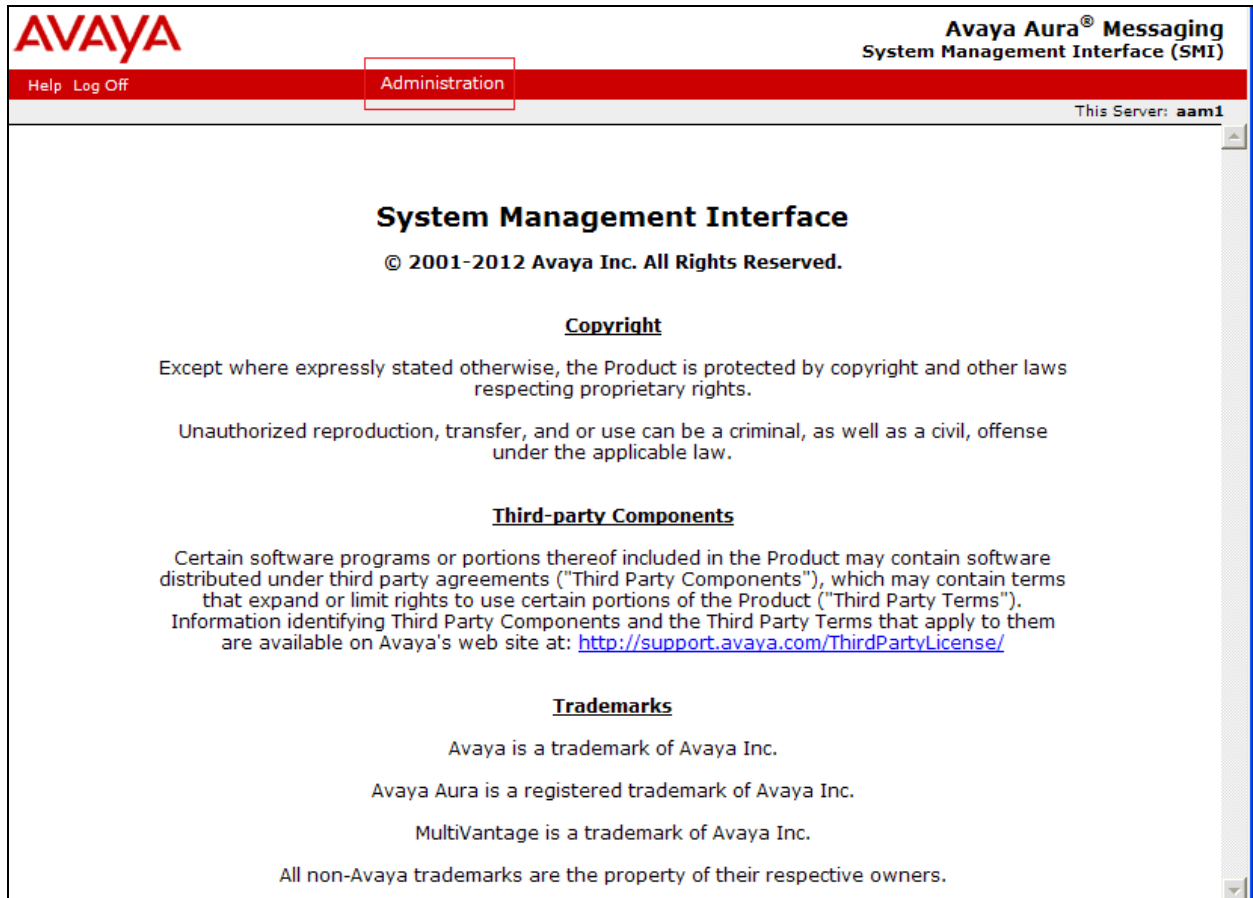
This section provides the procedures for configuring IPC turret users as local subscribers on Avaya Aura® Messaging. It is assumed that Avaya Aura® Messaging has been installed and basic configuration is completed. In this section, administrating subscriber is discussed.

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 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.

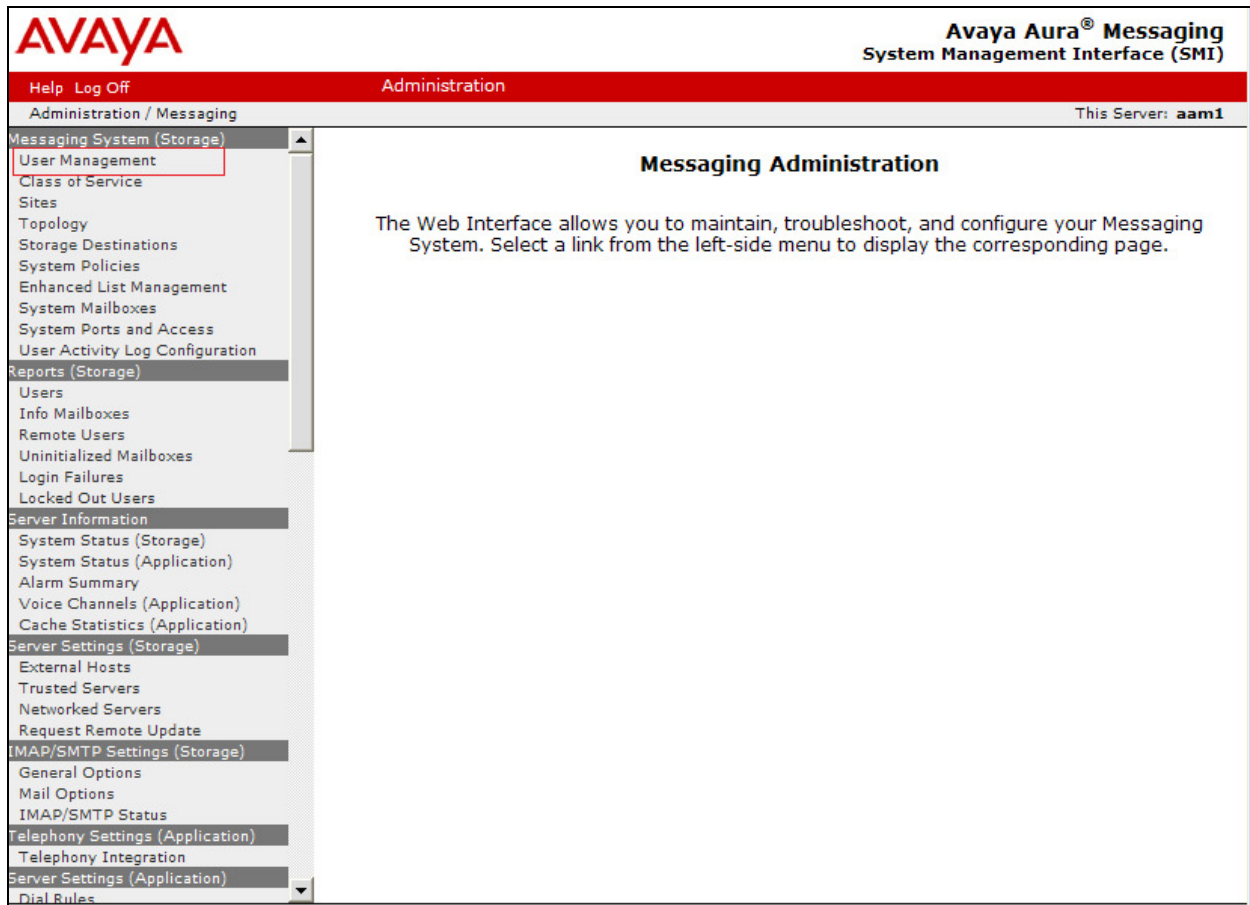


The screenshot shows the Avaya Aura® Messaging System Management Interface (SMI) web application. At the top left is the AVAYA logo. At the top right is the text "Avaya Aura® Messaging System Management Interface (SMI)". Below the logo is a red navigation bar with "Help" and "Log Off" links. On the right side of the page, it says "This Server: aam1". The main content area is a light gray box titled "Logon". Inside this box, there is a "Logon ID:" label followed by a text input field containing the text "admin". Below the input field is a blue "Logon" button.

The **System Management Interface** screen appears, as shown below. Select **Administration** → **Messaging** (not shown).



The **Messaging Administration** screen appears. From the left pane, select **User Management**.



From the **User Management** screen, select **Add** under the “Add a new user:” section.

AVAYA Avaya Aura® Messaging System Management Interface (SMI)

Help Log Off Administration

Administration / Messaging This Server: aam1

Messaging System (Storage)

- User Management
- Class of Service
- Sites
- Topology
- Storage Destinations
- System Policies
- Enhanced List Management
- System Mailboxes
- System Ports and Access
- User Activity Log Configuration

Reports (Storage)

- Users
- Info Mailboxes
- Remote Users
- Uninitialized Mailboxes
- Login Failures
- Locked Out Users

Server Information

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

Server Settings (Storage)

- External Hosts
- Trusted Servers
- Networked Servers
- Request Remote Update

User Management

License Status
License mode: Normal

Edit User/Info Mailbox
Edit a user's properties. Possible identifiers are: mailbox number.

Identifier:

Edit

Add User/Info Mailbox
Add a new user:

Add

Add a new Info Mailbox:

Add

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**, **Extension** fields. Select the appropriate **Class Of Service** and select **Yes** for the **WMI enabled** field. Retain the default values in the remaining fields. Repeat this section to add all IPC subscribers. Click **Save**.

During the compliance test, extensions, 33309 and 33310, were utilized.

AVAYA Avaya Aura® Messaging System Management Interface (SMI)

Help Log Off Administration This Server: aam1

Administration / Messaging

User Management > Properties for New User Help

User Properties

First name: 33309
Last name: 33309
Display name:
ASCII name:

Site: Default

Mailbox number: 33309

Extension: 33309

☒ Include in Auto Attendant directory

Additional extensions:

Class of Service: Standard

Pronounceable name:

MWI enabled: Yes

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

Save Delete

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 left is the AVAYA logo, and to its right is the text "Avaya Aura ® System Manager 6.3". Below this is a red navigation bar with the text "Home / Log On". Underneath the bar, the heading "Log On" is displayed. The main content area is divided into two sections. On the left, a box contains the following text: "Recommended access to System Manager is via FQDN." followed by a blue link "Go to central login for Single Sign-On". Below this, it 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". On the right side of the login area, there are two input fields: "User ID:" and "Password:". At the bottom right of the form, there are two buttons: "Log On" and "Cancel". Below the "Cancel" button is a blue link "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 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 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 333xx. 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. 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 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:**

* **Min:**

* **Max:**

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

[Add](#) [Remove](#)

1 Item [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-		Route2G450		<input type="checkbox"/>	S8300D-G450-63	

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

Avaya Aura® System Manager 6.3

Last Logged on at September 4, 2013 3:08 PM
[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 checked="" type="checkbox"/>	ModularMessaging	
<input type="checkbox"/>	-ALL-		Route2AAM		<input type="checkbox"/>	AAM	

Select : All, None

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 Aura® Messaging, Avaya Aura® Session Manager, and IPC Alliance MX.

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 MX 15.03 to successfully interoperate with Avaya Aura® Messaging 6.2 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. *Administering Avaya Aura® Messaging*, Release 6.2, Issue 2.2, May 2013, 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.