



Avaya Solution & Interoperability Test Lab

Application Notes for IPC Alliance MX 15.03 with Avaya Aura® Communication Manager 6.3 and 5.2.1, Avaya Aura® Session Manager 6.3 in a Centralized Messaging Environment using Avaya Modular Messaging 5.2 – 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 and 5.2.1, Avaya Aura® Session Manager 6.3 in a Centralized Messaging Environment using Avaya Modular Messaging 5.2.

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.

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 and 5.2.1, Avaya Aura® Session Manager 6.3 in a Centralized Messaging Environment using Avaya Modular Messaging 5.2.

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. 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. 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 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 basic call, basic display, G.711/G.729, hold/reconnect, DTMF, call forwarding unconditional/ring-no-answer/busy, blind/attended transfer, and conference.

For Avaya Modular Messaging, the solution test verified only up to login, greeting, voice message, and message waiting indicator. The main features of Avaya Modular Messaging (ie, personal operator, auto attendant, find me, call me, call sender, and transfer) were not part of the test and not included during the compliance test.

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 were the observations from the compliance testing.

- IPC does not offer the Coverage feature, therefore coverage to voicemail for the turret users was accomplished by setting the Modular Messaging pilot number as the Call Forwarding destination for the users.

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 **Figure 1**, 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 Communication Manager, and SIP trunks were used from Communication Manager to 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 Session Manager is performed via the web interface of System Manager. 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. 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 Communication Manager and IPC Alliance MX, 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 [3] in **Section 10**.

A five digit Uniform Dial Plan (UDP) was used to facilitate dialing between the Central and Remote sites. Unique extension ranges were associated with Communication Manager user(s) at the Central site (Communication Manager 6.3 – 72xxx), Remote site (Communication Manager 5.2.1 – 22xxx), and IPC turret users at the Remote site (33xxx). The Avaya Modular Messaging pilot number was 7777.

The call path from an IPC turret is following:

[Alliance 15.03] ← (QSIG trunk) → [Avaya **CM1** 6.3] ← (H.323 trunks) → [Avaya **CM2** 5.2.1] ← (SIP trunk) → [Session-Manager 6.3] ← (SIP trunk) → [Modular Messaging 5.2]

Note: In this call path, Session Manager was used solely for a routing purpose

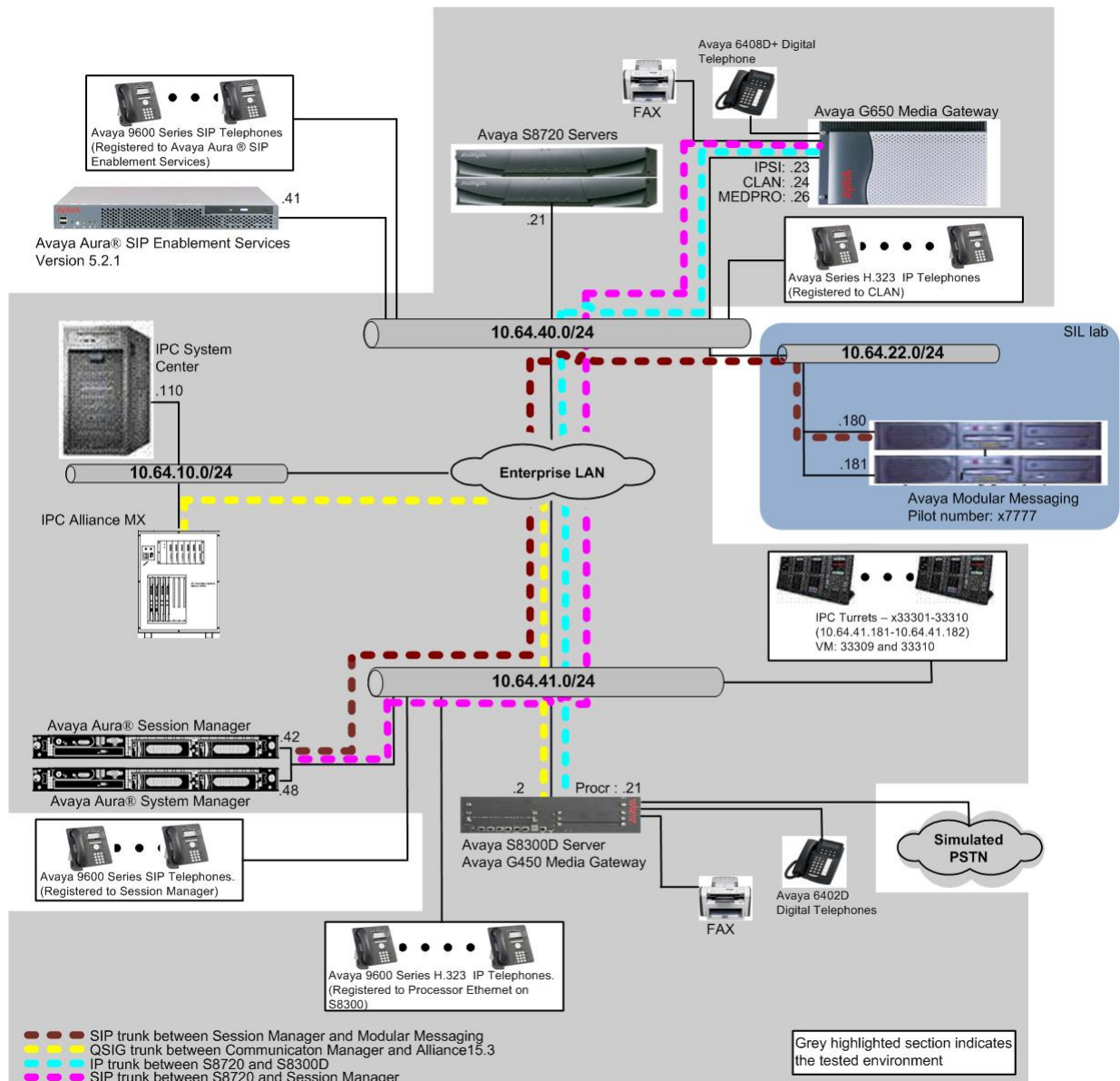


Figure 1: Test Configuration of IPC Alliance with Avaya Aura® Communication Managers, Avaya Aura® Session Manager, and Avaya Modular Messaging

4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager on Avaya S8300D Server	6.3 (R016x.03.0.124.0-20553)
Avaya G450 Media Gateway	33.13
Avaya Aura® Communication Manager on Avaya S8720 Server	5.2.1 (R015x.02.1.016.4-19880)
Avaya G650 Media Gateway	
Avaya Aura® Session Manager	6.3 SP2
Avaya Aura® System Manager	6.3 SP2
Avaya Modular Messaging <ul style="list-style-type: none">• Messaging Storage Server• Messaging Application Server	5.2 SP9 5.2 SP9
Avaya 96xx Series IP Telephones (H.323)	3.1
Avaya 96x1 Series IP Telephone (H.323)	6.22
Avaya DCP phone	-
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] in **Section 10**. Otherwise, there is no special configuration in Communication Manager.

This section describes the H.323 trunk configuration between Communication Manager 6.3 and Communication Manager 5.2.1. The following topics are discussed:

- Administer trunk group in Communication Manager 6.3.
- Administer hunt group in Communication Manager 6.3
- Administer hunt group in Communication Manager 5.2.1

Assumptions are made that routings (automatic alternate routing and route-pattern) in Communication Manager 6.3 and 5.2.1 are correctly set and working properly.

5.1. Administer a Trunk Group in Avaya Aura ® Communication Manager 6.3 (CM1)

Administer an ISDN trunk group to interface with Communication Manager. Use the “add trunk-group n” command, where “n” is an available trunk group number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “isdn”
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Direction:** “two-way”
- **Carrier Medium:** “H.323”
- **Service Type:** “tie”

change trunk-group 10		Page 1 of 21	
TRUNK GROUP			
Group Number: 10	Group Type: isdn	CDR Reports: y	
Group Name: S8720-IP trunk	COR: 1	TN: 1	TAC: 1010
Direction: two-way	Outgoing Display? y	Carrier Medium: H.323	
Dial Access? y	Busy Threshold: 255	Night Service:	
Queue Length: 0			
Service Type: tie	Auth Code? n		
	Member Assignment Method: auto		
	Signaling Group: 10		
	Number of Members: 10		

Navigate to **Page 2**. For **Supplementary Service Protocol**, enter “b”. For **Digit Handling (in/out)**, enter “enbloc/enbloc”. Retain the default values for the remaining fields.

change trunk-group 10		Page 2 of 21
Group Type: isdn		
TRUNK PARAMETERS		
Codeset to Send Display: 6	Codeset to Send National IEs: 6	
Charge Advice: none		
Supplementary Service Protocol: b	Digit Handling (in/out): enbloc/enbloc	
Incoming Calling Number - Delete: Insert:		Digital Loss Group: 18
		Format:
Disconnect Supervision - In? y Out? y		
Answer Supervision Timeout: 2		
XOIP Treatment: auto		CONNECT Reliable When Call Leaves ISDN? n
CPN to Send for Redirected Calls: calling		Delay Call Setup When Accessed Via IGAR? n

Navigate to **Page 3**. Enable **Send Name** and **Send Calling Number**. For **Format**, enter “private”.

change trunk-group 10		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: internal	
	Internal Alert? n	Maintenance Tests? y
	Data Restriction? n	NCA-TSC Trunk Member:
	Send Name: y	Send Calling Number: y
Used for DCS? n	Hop Dgt? n	Send EMU Visitor CPN? n
Suppress # Outpulsing? n	Format: private	
UI IE Treatment: shared		
Maximum Size of UI IE Contents: 128		
Replace Restricted Numbers? n		
Replace Unavailable Numbers? n		
Send Connected Number: y		
Hold/Unhold Notifications? y		
Send UI IE? y	Modify Tandem Calling Number: no	
Send UCID? y	BSR Reply-best DISC Cause Value: 31	
Send Codeset 6/7 LAI IE? y	Modify Reroute Number? y	
Show ANSWERED BY on Display? y		
DSN Term? n		

Note: Communication Manager 5.2.1 (CM2) should have the same information in the trunk group form.

5.2. Administer a hunt group in Avaya Aura® Communication Manager 6.3 (CM1)

To configure the hunt group, use the “add hunt-group n” command, where “n” is an available hunt-group number. On **Page 2** of the hunt group form, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Message Center:** “qsig-mwi”
- **Voice Mail Number:** Enter the pilot number.
- **Routing Digits:** Enter the aar access code from the feature access code form.

```
add hunt-group 94                                     Page 2 of 60
HUNT GROUP
LWC Reception: none                                AUDIX Name:
Message Center: qsig-mwi
Send Reroute Request: y
Voice Mail Number: 7777
Routing Digits (e.g. AAR/ARS Access Code): 8        Provide Ringback? n
TSC per MWI Interrogation? n
```

5.3. Administer a hunt group in Avaya Aura® Communication Manager 5.2.1 (CM2)

To configure the hunt group, use the “add hunt-group n” command, where “n” is an available hunt-group number. On **Page 2** of the hunt group form, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Message Center:** “sip-adjunct”
- **Voice Mail Handle:** Enter the pilot number.
- **Routing Digits:** Enter the aar access code from the feature access code form.

```
add hunt-group 72                                     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
```

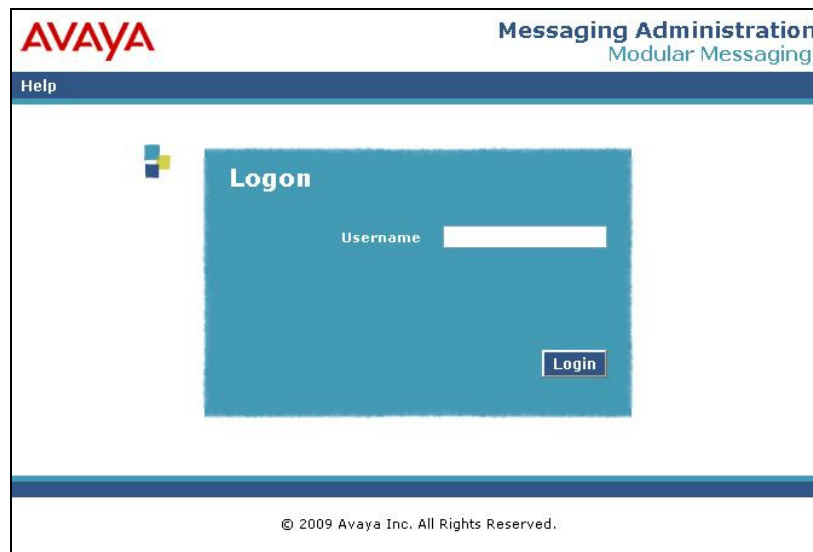
6. Configure Avaya Modular Messaging MSS

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. At the top right, it says "Messaging Administration" and "Modular Messaging". 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 is also visible to the left of the Logon box. At the bottom of the page, there is a copyright notice: "© 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 a status bar indicating 'This server: mss1'. A left-hand navigation menu lists various administrative tasks under 'Messaging Administration' and 'Server Administration'. The main content area is titled 'Messaging Administration' and contains a brief description: '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.'

AVAYA Modular Messaging
Messaging Administration

Help Log Off This server: mss1

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.

- ▼ 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

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-hand navigation menu is expanded to show 'Networked Machines' under the 'Messaging Administration' section. The main content area features a table with columns: 'Machine', 'IP Address', 'Machine Type', and 'Total Subs'. A single entry is listed: 'alpinemss1' with IP '10.64.22.181', type 'local', and 28 subscribers. Below the table are several action 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'.

AVAYA Modular Messaging
Messaging Administration

Help Log Off This server: mss1

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

- ▼ 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

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"/>	Machine Type	<input type="text" value="tcpip"/>
IP Address	<input type="text" value="10.64.22.181"/>	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"/>	Log Updates Out	<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

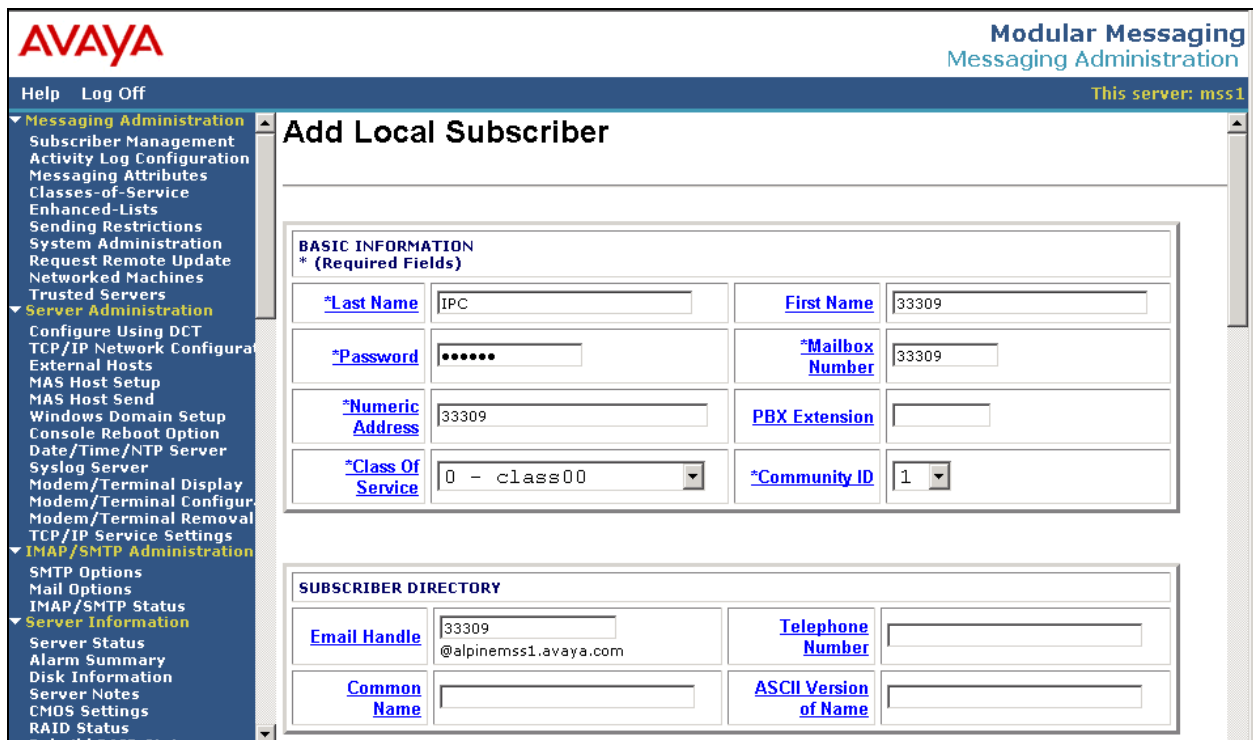
Select **Messaging Administration** → **Subscriber Management** from the left pane, to display the **Manage Subscribers** screen. For the **Local Subscriber Mailbox Number** field toward the top of the screen, enter the first IPC turret user extension to add as a local subscriber, in this case “33309”. 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 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] in **Section 10**.

8. Verification Steps

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

- Place a call from an IPC turret user, which is a subscriber in Modular Messaging, to the Modular Messaging pilot number. Verify that Modular Messaging recognizes the calling party as a local subscriber.
- Place calls from an IPC turret user to stations which are registered to Communication Manager 1. Verify there is two way audio.
- Place calls from an IPC turret user to stations which are registered to Communication Manager 2. Verify there is two way audio.

9. Conclusion

These Application Notes describe the configuration steps required for IPC Alliance MX 15.03 to successfully interoperate with Avaya Aura® Communication Manager 6.3, Avaya Aura® Communication Manager 5.2.1, Avaya Aura® Session Manager 6.3, and Avaya Modular Messaging 5.2 in a centralized messaging environment using QSIG trunks to Avaya Aura® Communication Manager 6.3. All feature and serviceability test cases were successfully completed with an observation noted in **Section 2.2**.

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, 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.