



Avaya Solution & Interoperability Test Lab

Application Notes for IPC Alliance 15.03 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 Alliance 15.03 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 Alliance is a trading communication solution. In the compliance testing, IPC Alliance 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.

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 15.03 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 Alliance is a trading communication solution. In the compliance testing, IPC Alliance 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 Enterprise SIP Server (ESS).

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 to recover from adverse conditions, such as disconnecting/reconnecting the LAN connection to the IPC ESS server.

2.2. Test Results

All test cases were executed. 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 Modular Messaging pilot number as the Call Forwarding destination for the users.
- The following Modular Messaging features are not supported in this solution, since they do not work as expected. It is recommended they are not enabled.
 - Receptionist /Personal Operator: 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.
 - Auto Attendant: Issues were encountered when using the Auto attendant function provided by Modular Messaging. The “extension does not answer” message was heard when turret is the set to Auto Attendant.
 - Find Me: In some cases (after the call goes to Find Me destination station), the Find Me destination station presses “#” to accept the call, and the “Connecting Caller” message was heard. However, the Find Me destination station goes disconnect. The calling party is still connected to VM.
 - Call Sender: In some cases, a calling party, or calling and called party, are disconnected after the call is transferred.
- In some instances, Direct IP-to-IP media (also known as “shuffling”) with SIP and H.323 telephones did not work. It is recommended that Direct IP-to-IP media be disabled on the IPC Turret endpoints.

These items were not deemed significant to fail the solution, and are listed here for user awareness. Testing of the sample configuration was completed with successful results for the IPC System Interconnect solution.

2.3. Support

Technical support on IPC Alliance 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 Alliance consists of the Enterprise SIP Server (ESS), Alliance MX, System Center, and Turrets. SIP trunks are used from IPC Alliance 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 among Communication Manager, Session Manager, and IPC Alliance, 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.

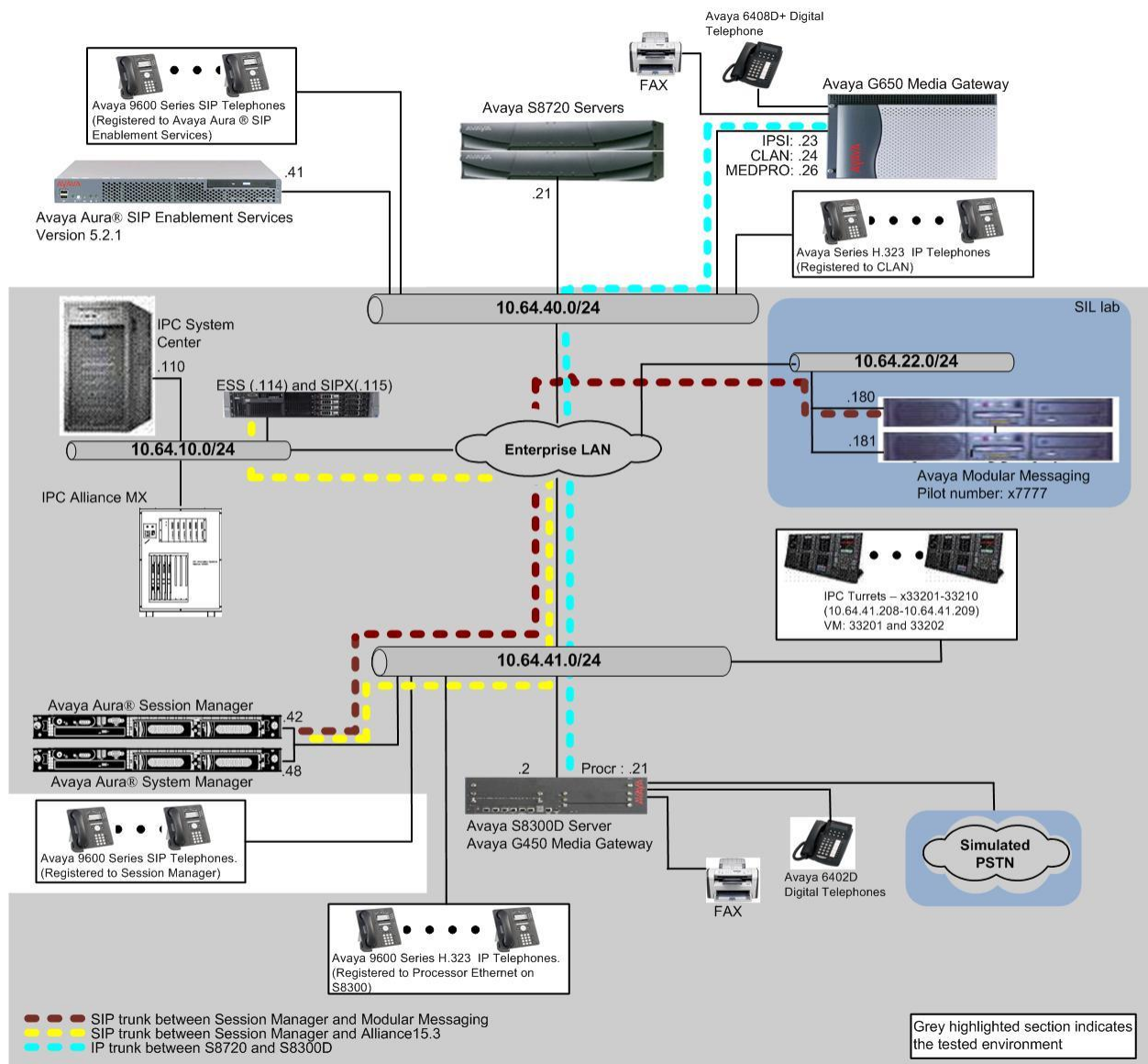


Figure 1: Test Configuration of IPC Alliance system with Avaya Modular Messaging

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 G650 Media Gateway <ul style="list-style-type: none">• TN799DP C-LAN Circuit Pack• TN2302AP IP Media Processor | HW01 FW038 HW20 FW122 |
| 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 Alliance <ul style="list-style-type: none">• Alliance MX• Enterprise SIP Server• System Center<ul style="list-style-type: none">○ SIPX Line Card• Turrets | SipProxy-2.01.00-03 15.03.00.23 15.03.00.23 15.03.00.23 15.03.00.22 15.03.01.04.0005 |


5. 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

5.1. 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 'Messaging Administration' web interface for 'Modular Messaging'. At the top, the title 'Messaging Administration' is in blue, with 'Modular Messaging' below it. A dark blue horizontal bar contains the word 'Help' in white. The main content area features a large blue box titled 'Logon' in white. Inside this box, the label 'Username' is followed by a white text input field. In the bottom right corner of the blue box is a 'Login' button with a blue border and white text. Below the blue box, a dark blue horizontal bar spans the width of the page. At the very bottom, a white footer bar contains the text '© 2009 Avaya Inc. All Rights Reserved.'

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'. Under 'Messaging Administration', there are links: Subscriber Management, Activity Log Configuration, Messaging Attributes, Classes-of-Service, Enhanced-Lists, Sending Restrictions, System Administration, Request Remote Update, Networked Machines, and Trusted Servers. 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.'

5.2. 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 top right corner displays 'This server: 10.64.22.181'. The left sidebar contains a menu with 'Messaging Administration' (highlighted) and 'Server Administration'. Under 'Messaging Administration', there are links: Subscriber Management, Activity Log Configuration, Messaging Attributes, Classes-of-Service, Enhanced-Lists, Sending Restrictions, System Administration, Request Remote Update, Networked Machines, and Trusted Servers. Under 'Server Administration', there are links: 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, and TCP/IP Service Settings. Under 'IMAP/SMTP Administration', there are links: SMTP Options, Mail Options, and IMAP/SMTP Status. Under 'Server Information', there are links: Server Status, Alarm Summary, Disk Information, Server Notes, CMOS Settings, RAID Status, Rebuild RAID Status, and Reboot Interval. The main content area is titled 'Manage Networked Machines' and contains 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 332xx 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](#)
[Enhancing-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"/> |

5.3. 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 “33201”. Click **Add or Edit**.

The screenshot displays the 'Modular Messaging Messaging Administration' web interface. The left sidebar contains a navigation menu with categories: 'Messaging Administration' (including Subscriber Management, Activity Log Configuration, etc.), 'Server Administration' (including Configure Using DCT, TCP/IP Network Configuration, etc.), 'IMAP/SMTP Administration' (including SMTP Options, Mail Options, etc.), and 'Server Information' (including Server Status, Alarm Summary, etc.). The main content area is titled 'Manage Subscribers'. At the top, there is a form for 'Local Subscriber Mailbox Number' with the value '33201' entered 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' for machine 'alpinemss1' with 34 mailboxes, 35 total subscribers, and 35 filtered subscribers; and 'Remote Subscribers' for machine 'internet' with 0 mailboxes, 0 total subscribers, and 0 filtered subscribers. Each row has a 'Filter' button and a 'Manage' button. At the bottom left of the main area is a 'Help' button, and at the bottom center is a 'Page Status' box.

| | <u>Machine Name</u> | <u>Local Subscriber Mailboxes</u> | <u>Total Subscribers</u> | | <u>Filtered Subscribers</u> | |
|----------------------|---------------------|-----------------------------------|--------------------------|--------|-----------------------------|--------|
| • Local Subscribers | alpinemss1 | 34 | 35 | Filter | 35 | Manage |
| • Remote Subscribers | internet | | 0 | Filter | 0 | Manage |

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.

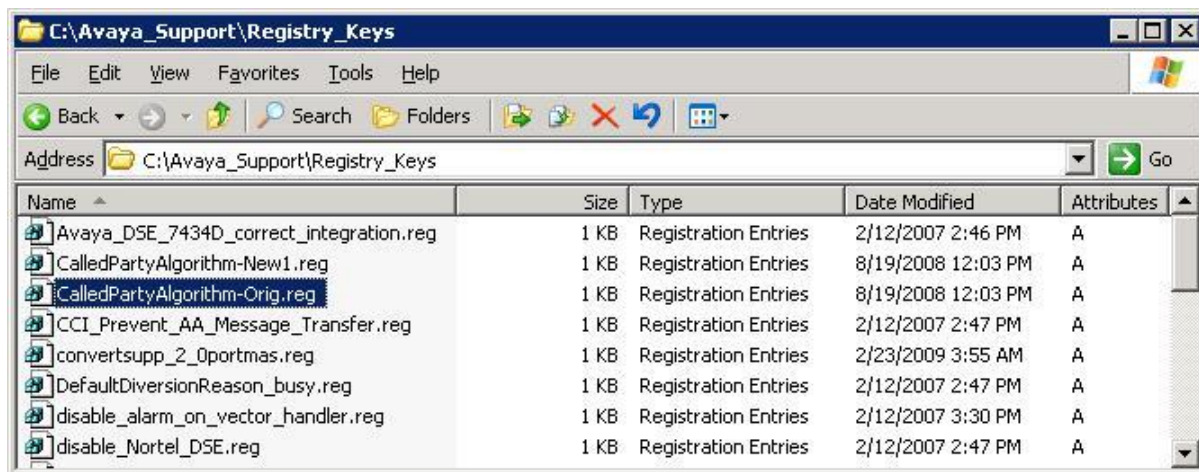
The screenshot displays the 'Add Local Subscriber' form within the 'Modular Messaging Administration' web interface. The interface includes a top navigation bar with 'Help' and 'Log Off' links, and a server status indicator 'This server: 10.64.22.181'. A left-hand menu lists various administration tasks under 'Messaging Administration' and 'Server Administration'. The main form area is titled 'Add Local Subscriber' and contains a 'BASIC INFORMATION' section with the following fields:

| BASIC INFORMATION * (Required Fields) | |
|--|-------------|
| *Last Name | 33201 |
| First Name | Ally15 |
| *Password | ***** |
| *Mailbox Number | 33201 |
| *Numeric Address | 33201 |
| PBX Extension | 33201 |
| *Class Of Service | 0 - class00 |
| *Community ID | 1 |

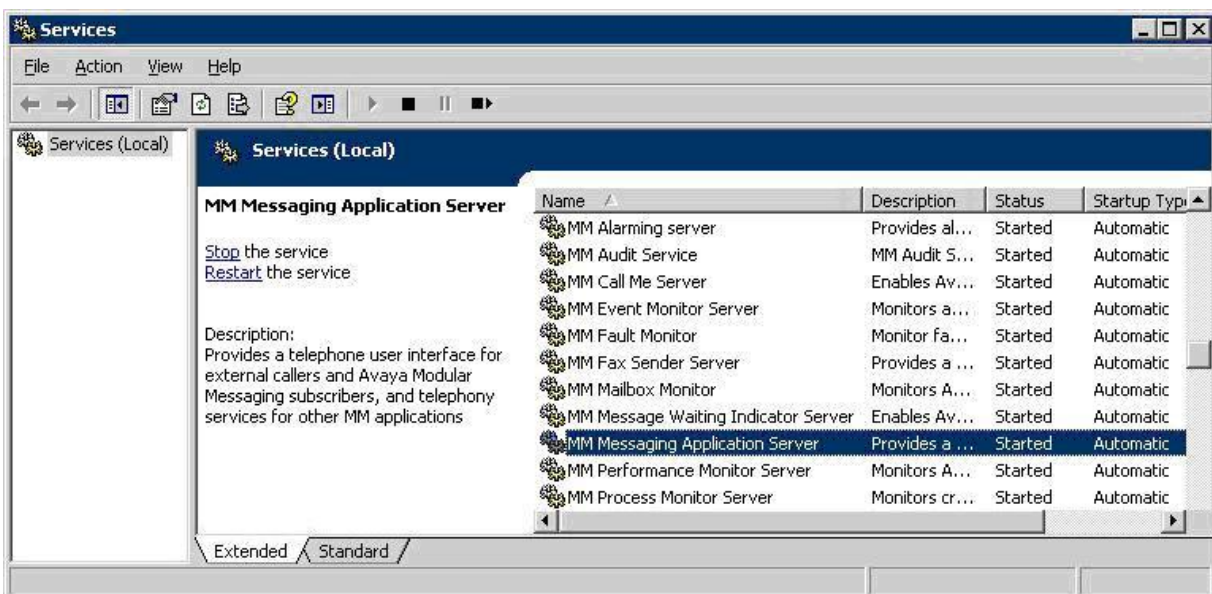
6. Configure Avaya Modular Messaging MAS

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**.



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.



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 “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.

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.

User ID:

Password:

[Change Password](#)

Supported Browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 19.0, 20.0 or 21.0.

7.2. 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 (not shown). 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](#)

8. Configure IPC Alliance

This section provides the procedures for configuring IPC Alliance. The procedures include the following areas:

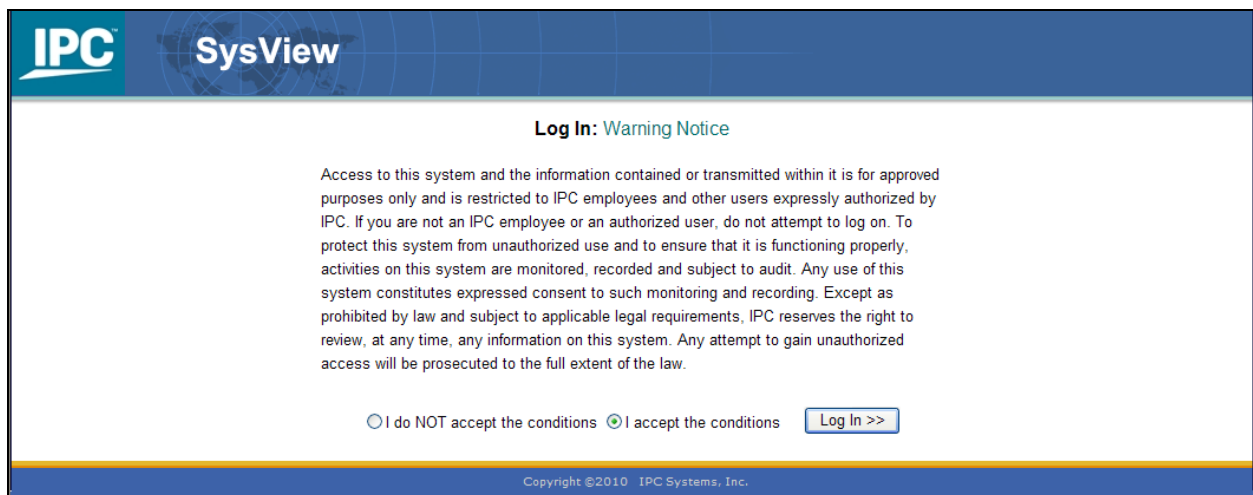
- Launch One Management System
- Administer voicemail buttons

The configuration of IPC Alliance is typically performed by IPC installation technicians. The procedural steps are presented in these Application Notes for informational purposes.

8.1. Launch One Management System

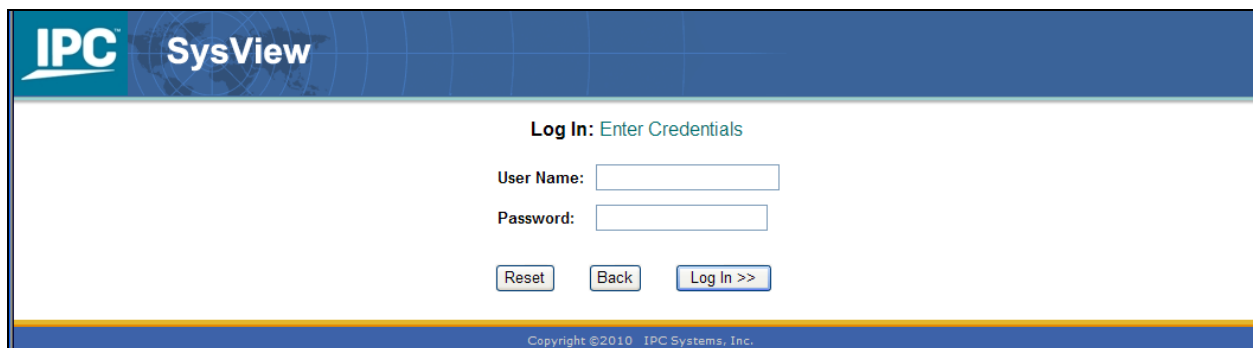
Access the System Center web interface by using the URL <http://<ip-address>/webadmin> in an Internet browser window, where <ip-address> is the IP address of IPC System Center. Log in using the appropriate credentials.

In the **Log In: Warning Notice** screen, check **I accept the conditions**, and click **Log In**.



The screenshot shows the 'Log In: Warning Notice' screen. At the top is the IPC SysView header. The main content area contains a warning message: 'Access to this system and the information contained or transmitted within it is for approved purposes only and is restricted to IPC employees and other users expressly authorized by IPC. If you are not an IPC employee or an authorized user, do not attempt to log on. To protect this system from unauthorized use and to ensure that it is functioning properly, activities on this system are monitored, recorded and subject to audit. Any use of this system constitutes expressed consent to such monitoring and recording. Except as prohibited by law and subject to applicable legal requirements, IPC reserves the right to review, at any time, any information on this system. Any attempt to gain unauthorized access will be prosecuted to the full extent of the law.' Below the text are two radio buttons: 'I do NOT accept the conditions' (unselected) and 'I accept the conditions' (selected). To the right is a 'Log In >>' button. The footer contains the copyright notice 'Copyright ©2010 IPC Systems, Inc.'

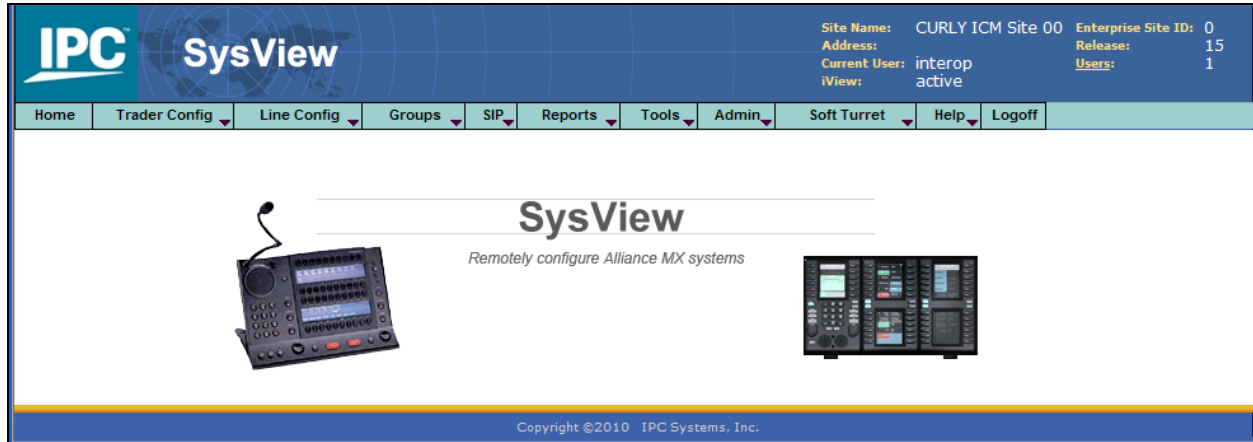
In the **Log In: Enter Credentials** screen, enter the appropriate credentials and click **Log In**. In the subsequent **Log In: Login Information** screen (not shown), click **Continue**.



The screenshot shows the 'Log In: Enter Credentials' screen. At the top is the IPC SysView header. The main content area contains the title 'Log In: Enter Credentials' and two input fields: 'User Name:' and 'Password:'. Below the input fields are three buttons: 'Reset', 'Back', and 'Log In >>'. The footer contains the copyright notice 'Copyright ©2010 IPC Systems, Inc.'

8.2. Administer Voicemail Buttons

The screen below is displayed next, with the **Main Menu** screen in the forefront. Select **Trader Config → Buttons → Add Buttons** (not shown).



The **Add Button: Enter Details** screen is displayed. Provide the following information:

- **TRID:** Enter the ID of the trader whose button sheet is being configured, in this case “123”. During the compliance test, two turrets were utilized (TRID: 122 and 123).
- **Button Number:** Enter a button numbers. Button number, 33 and 35 on TRID 123 turret, were configured for Voicemails
- **Class:** Select “MODULE BUTTON”
- **Type:** Select “VOICE MAIL”
- **Voice Mail System Access Number:** For the compliance test, entered “7776PP#33201”
- **Voice Mail Extension Number:** Enter the subscriber extension number, in this case “33201”

After entering above values, click **Add Buttons**.

| | | | | | | | | | | |
|--|---------------|-------------|--------|-----|---------|-------|-------|-------------|------|--------|
| Site Name: CURLY ICM Site 00 Enterprise Site ID: 0 | | | | | | | | | | |
| Address: Release: 15 | | | | | | | | | | |
| Current Users: interop Users: 1 | | | | | | | | | | |
| iView: active | | | | | | | | | | |
| Home | Trader Config | Line Config | Groups | SIP | Reports | Tools | Admin | Soft Turret | Help | Logoff |

Add Buttons: Enter Button Details

1. Select Station Type

☒ IQ/MAX ☐ BRI ☐ IQMX

2. Specify Traders

☒ TRID(s): ☐ Trader Group:

3. Enter Button Details

| | |
|----------------------------------|--|
| Button Number: | <input type="text" value="33"/> |
| Class: | <input type="text" value="MODULE BUTTON"/> |
| Type: | <input type="text" value="VOICE MAIL"/> |
| Site ID: | <input type="text" value="1"/> |
| Voice Mail System Access Number: | <input type="text" value="7776PP#33201#"/> |
| Voice Mail Extension Number: | <input type="text" value="33201"/> |
| Config. Notes: | <input type="text"/> |
| Extended Label: | <input type="text"/> |
| Surname: | <input type="text"/> |
| Given Name: | <input type="text"/> |
| Organization: | <input type="text"/> |
| Distinguished Name: | <input type="text"/> |

☐ Config. Lock

The **following** screen displays the updated button information. Repeat this for all trade users. In the compliance testing, two voicemail buttons for IPC subscriber extensions “33201” and “33202” were created on each of the two trade users.

| Home | Trader Config | Line Config | Groups | SIP | Reports | Tools | Admin | Soft Turret | Help | Logoff |
|--|---------------|----------------|---------|------------|--------------|-----------------|--------------|---|---------------|--------|
| Edit Buttons: Edit Selected Buttons | | | | | | | | | | |
| TRID | Num | Extended Label | Surname | Given Name | Organization | Class | Type | Speed Dial/Button Sequence /Voice Mail/Divert | | |
| 123 | 33 | VM 33201 | | | | MODULE BUTTON ▼ | VOICE MAIL ▼ | Voice Mail: 33201 7776PP# | | |
| | | | | | | | Back | Reset | Save Edits >> | |
| Copyright ©2010 IPC Systems, Inc. | | | | | | | | | | |

9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Modular Messaging, Avaya Aura® Session Manager, and IPC Alliance 15.03.

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 15.03 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**.

11. 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.