



Avaya Solution & Interoperability Test Lab

Application Notes for IPC Alliance 15.03 with Avaya Aura® Messaging 6.2 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 Aura® Messaging 6.2 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 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 15.03 to interoperate with Avaya Aura® Messaging 6.2 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 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 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 attendant/assistant, operator/live attendant, and call sender.

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 Aura® Messaging pilot number as the Call Forwarding destination for the users.
- The following Avaya Aura® Messaging features are not supported in this solution, since they do not work as expected. It is recommended they are not enabled.
 - Multiple Call Forward: Issues were observed when tested the multiple call forward function provided by Avaya Aura® Messaging. The call goes to the forward-to station greeting, instead of called station greeting.
 - Call Sender: In some instances, reply to calling party did not work. Ringing to the calling party was observed, but no RTP.

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 Aura® Messaging for voice messaging services.

The detailed administration of basic connectivity among Communication Manager, Session Manager, and Avaya Aura® 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 between 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 Aura® Messaging.

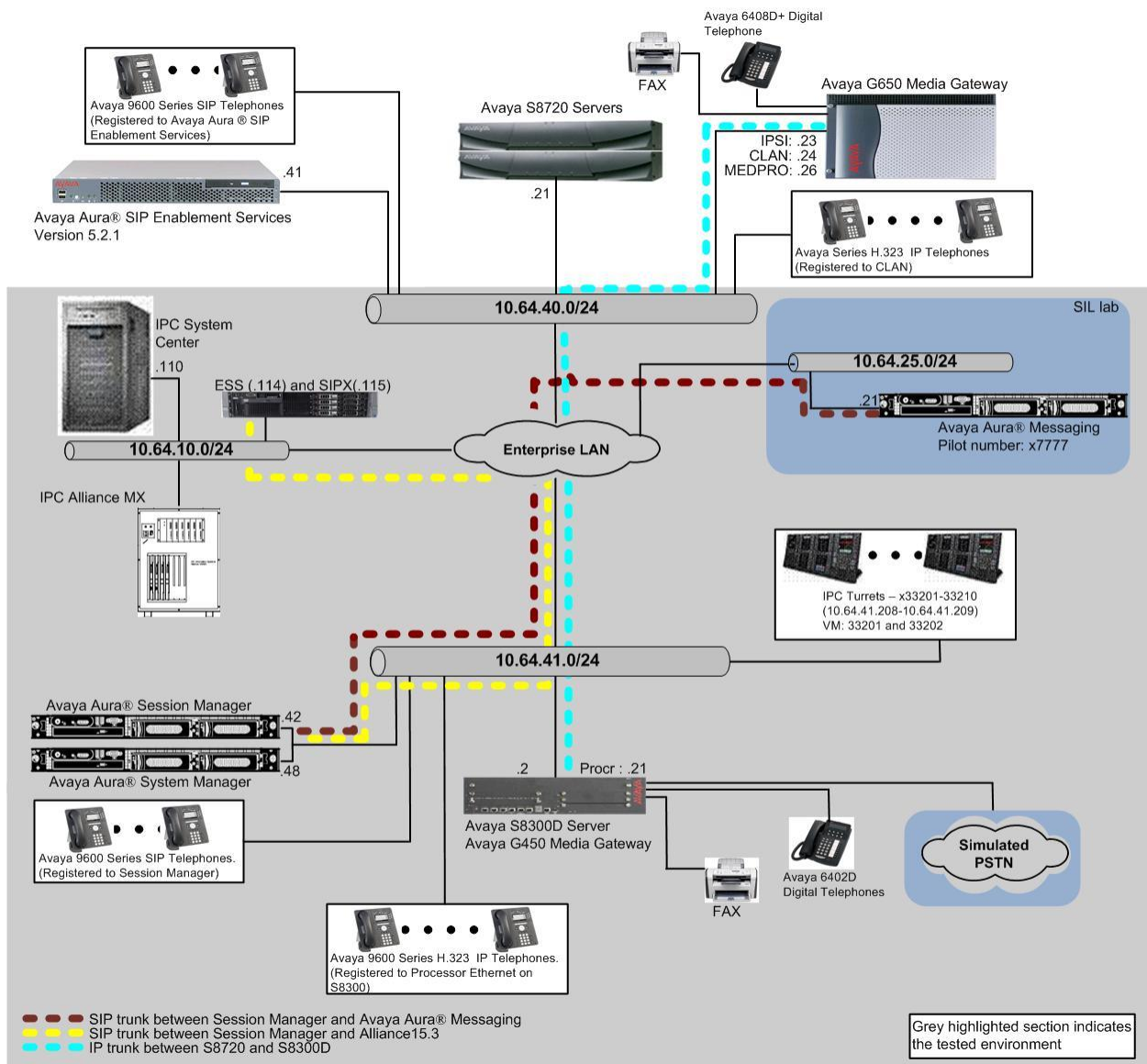


Figure 1: Test Configuration of IPC Alliance system with Avaya Aura® Messaging

4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Messaging	MSG-02.0.823.0-109_0304
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 PackTN2302AP 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 MXEnterprise SIP ServerSystem Center<ul style="list-style-type: none">SIPX Line CardTurrets	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 Aura® Messaging

This section provides the procedures for configuring IPC turret users as local subscribers on Avaya Aura® Messaging. The configuration procedures include the following areas:

- Launch messaging administration
- Administer subscriber extension ranges
- Administer subscribers

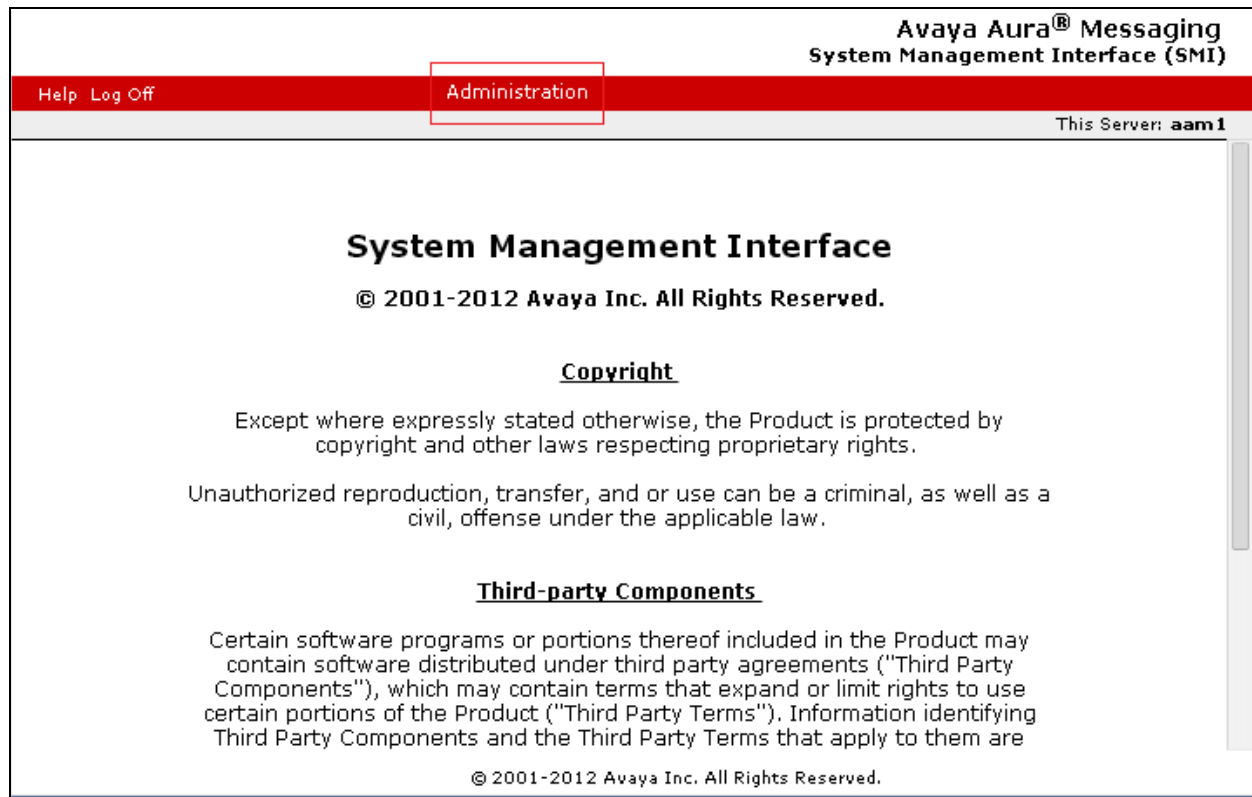
5.1. Launch Messaging Administration

Access the Avaya Aura® Messaging web interface by using the URL “http://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Avaya Aura® Messaging server. The **Logon** screen is displayed. Log in using a valid user name and password. The **Password** field will appear after a value is entered into the **Username** field.



The screenshot displays the Avaya Aura® Messaging System Management Interface (SMI) web application. At the top right, the title "Avaya Aura® Messaging System Management Interface (SMI)" is visible. Below the title bar, there is a red navigation bar with "Help" and "Log Off" links. On the right side of this bar, it says "This Server: aam1". The main content area features a "Logon" box with a "Logon ID:" label and a text input field. A "Logon" button is positioned below the input field. At the bottom of the page, the copyright notice "© 2001-2012 Avaya Inc. All Rights Reserved." is displayed.

The **System Management Interface** screen appears, as shown below. Navigate to **Administration → Messaging**.



5.2. Administer Subscriber Extension Ranges

Select **Server Settings (Storage) → Networked Servers** from the left pane, to display the **Manage Networked Servers** screen. Select the Avaya Aura® Messaging server from the table listing, and click **Edit the Selected Networked Server** toward the bottom right of the screen.

Avaya Aura® Messaging
System Management Interface (SMI)

Help Log Off Administration

Administration / Messaging This Server: aam1

Manage Networked Servers

The Manage Networked Servers page is used to add change or delete the Networked servers used by the messaging feature.

Server Name	IP Address	Server Type	ID	Total Subs
aam1	10.64.45.21	local	0	16

Display Report of Servers

Add a New Networked Server

Display Network Snapshot

Help

Delete the Selected Networked Server

Edit the Selected Networked Server

Display Report of Server Ranges

© 2001-2012 Avaya Inc. All Rights Reserved.

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.

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

IMAP/SMTP Settings (Storage)

General Options

Mail Options

IMAP/SMTP Status

Telephony Settings (Application)

Telephony Integration

Server Settings (Application)

Dial Rules

Cluster

System Parameters

Languages

Log Configuration

Advanced (Application)

System Operations

Timeouts

AxC Address

Edit Networked Machine

The Edit Networked Server allows the changing or deletion of a networked server record.

Machine Name	<input type="text" value="aam1"/>	Password	<input type="password"/>
		Confirm Password	<input type="password"/>
IP Address	<input type="text" value="10.64.45.21"/>	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"/>
Remote 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="99999"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>

5.3. Administer Subscribers

Select **Messaging System (Storage) → User Management** from the left pane, to display the **User Management** screen. Click **Add** under the **Add a new user** section.

The screenshot displays the Avaya Aura® Messaging System Management Interface (SMI) for server **aam1**. The interface is divided into a left navigation pane and a main content area. The navigation pane lists various system components, with **Messaging System (Storage)** selected. Under this category, **User Management** is highlighted. The main content area is titled **User Management** and contains the following sections:

- License Status**: License mode: Normal
- Edit User/Info Mailbox**: Edit a user's properties. Possible identifiers are: mailbox number. Below this is an **Identifier:** text box and an **Edit** button.
- Add User/Info Mailbox**: Add a new user: Below this is an **Add** button, which is highlighted with a red rectangle.
- Add a new Info Mailbox:** Below this is an **Add** button.

The **User Management > Properties for New User** 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** and **Extension** fields. Select the appropriate **Class Of Service**, and retain the default values in the remaining fields.

Scroll down to the bottom of the screen and click **Save**.

Repeat this section to add all IPC subscribers. During the compliance test, 33201 and 33202 were used.

Avaya Aura® Messaging
System Management Interface (SMI)

Help Log Off Administration This Server: aam1

Administration / Messaging

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

IMAP/SMTP Settings (Storage)

- General Options
- Mail Options
- IMAP/SMTP Status

Telephony Settings (Application)

- Telephony Integration

Server Settings (Application)

- Dial Rules
- Cluster
- System Parameters
- Languages
- Log Configuration

Advanced (Application)

- System Operations
- Timeouts
- AXC Address
- Miscellaneous
- Core Files

Utilities

- Messaging DB Audits (Storage)
- Start Messaging
- Stop Messaging
- LDAP Status/Restart (Storage)
- Change LDAP Password (Storage)

Logs

- Administration History
- Administrator
- Alarm
- Software Management

User Management > Properties for New User

User Properties

First name: 33201

Last name: 33201

Display name: 33201

ASCII name: 33201

Site: Default

Mailbox number: 33201

Extension: 33201

☒ 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

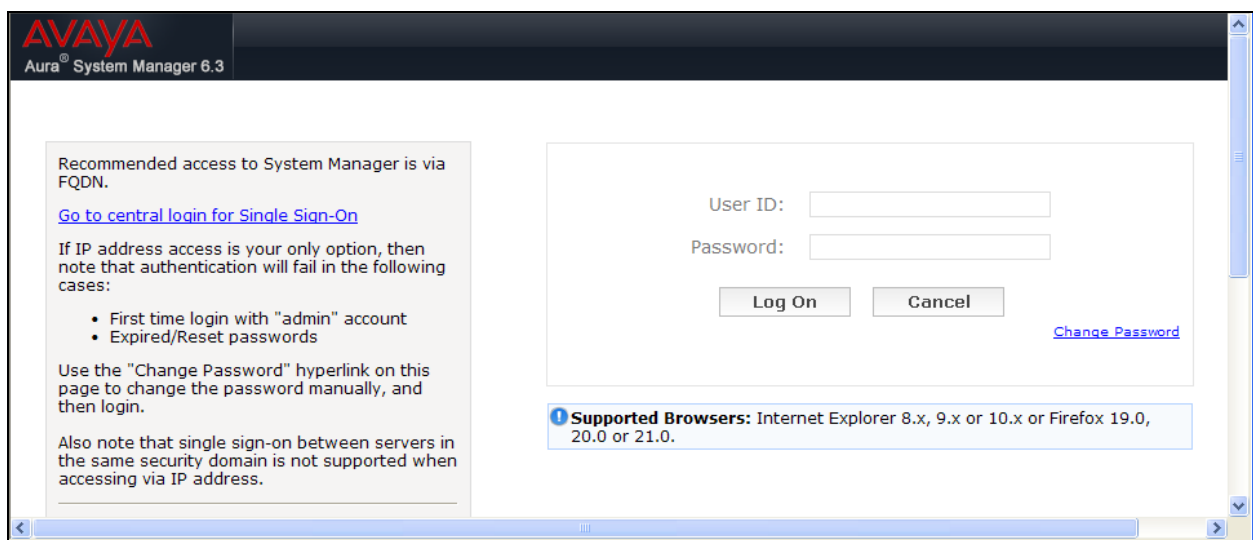
6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Avaya Aura® Session Manager. The procedures include the following areas:

- Launch System Manager
- Administer dial patterns

6.1. 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.



The screenshot shows the Avaya Aura System Manager 6.3 login interface. The header features the Avaya logo and the text "Aura® System Manager 6.3". The main content area is divided into two sections. The left section contains instructions: "Recommended access to System Manager is via FQDN." followed by a link "Go to central login for Single Sign-On". It then 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". Below this, it says: "Use the 'Change Password' hyperlink on this page to change the password manually, and then login." and "Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address." The right section contains the login form with fields for "User ID:" and "Password:", "Log On" and "Cancel" buttons, and a "Change Password" link. At the bottom, a blue box lists "Supported Browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 19.0, 20.0 or 21.0." The interface is displayed in a browser window with standard navigation buttons.

6.2. 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 Aura® 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 Aura® 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](#)

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

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

7. Configure IPC Alliance

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

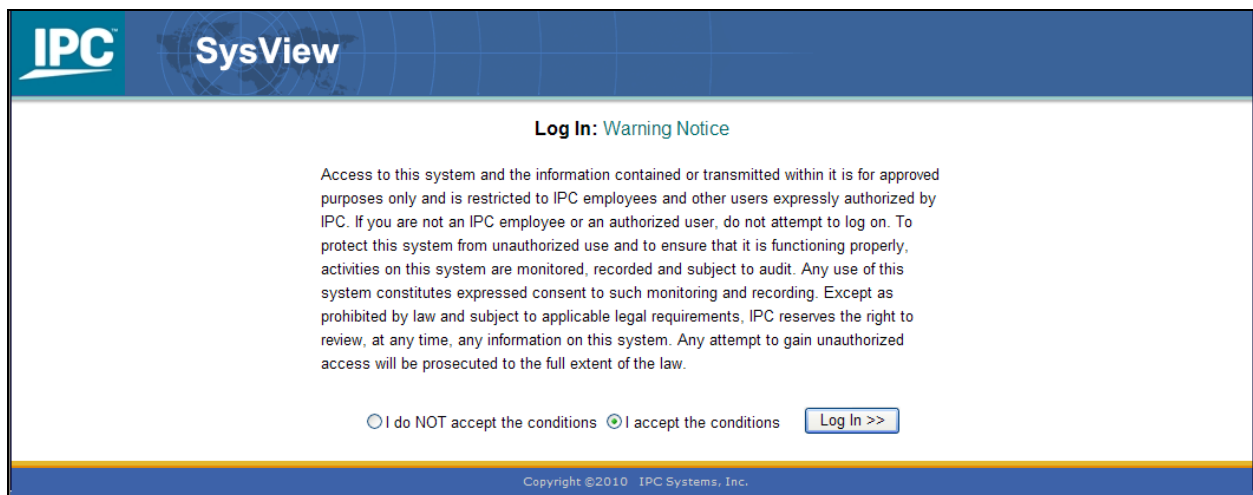
- Launch One Management System
- Administer voicemail buttons

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

7.1. Launch One Management System

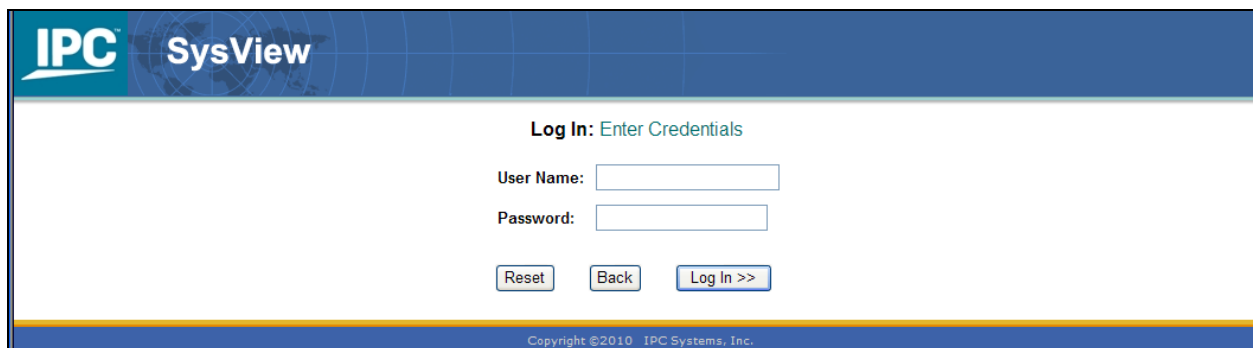
Access the System Center web interface by using the URL <http://<ip-address>/webadmin> in an Internet browser window, where <ip-address> is the IP address of IPC System Center. Log in using the appropriate credentials.

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, there is a blue header with the 'IPC' logo and 'SysView' text. Below the header, the title 'Log In: Warning Notice' is displayed. A paragraph of text explains the system's security and usage policies. At the bottom, there are two radio buttons: 'I do NOT accept the conditions' (unselected) and 'I accept the conditions' (selected). To the right of the radio buttons is a 'Log In >>' button. The footer contains the copyright notice 'Copyright ©2010 IPC Systems, Inc.'

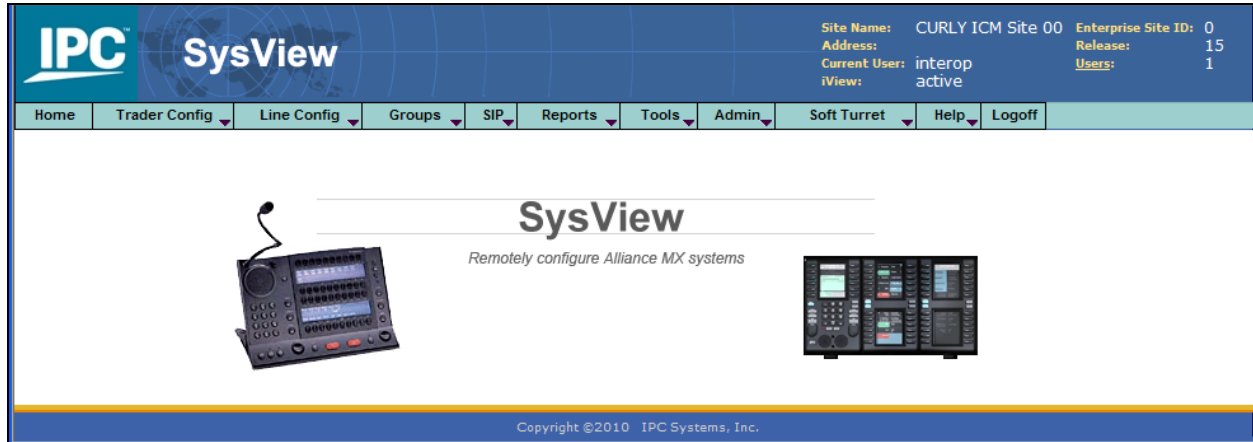
In the **Log In: Enter Credentials** screen, enter the appropriate credentials and click **Log In**. In the subsequent **Log In: Login Information** screen (not shown), click **Continue**.



The screenshot shows the 'Log In: Enter Credentials' screen. At the top, there is a blue header with the 'IPC' logo and 'SysView' text. Below the header, the title 'Log In: Enter Credentials' is displayed. There are 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.'

7.2. 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**.

<div>Site Name: CURLY ICM Site 00 Enterprise Site ID: 0 Address: Release: 15 Current Users: interop Users: 1 iView: active</div>										
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: ☐

Back

Reset

Add Buttons >>

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.										

8. Verification Steps

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

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.

9. Conclusion

These Application Notes describe the configuration steps required for IPC Alliance 15.03 to successfully interoperate with Avaya Aura® Messaging 6.2 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**.

10. 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 Patch11 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.