



Application Notes for IPC Unigy with Avaya Modular Messaging 5.2 and Avaya Aura® SIP Enablement Services 5.2.1 in a Centralized Messaging Environment using QSIG Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for IPC Unigy to interoperate with Avaya Modular Messaging 5.2 and Avaya Aura® SIP Enablement Services 5.2.1 in a centralized messaging environment using QSIG trunks to Avaya Aura® Communication Manager 5.2.1.

IPC Unigy is a trading communication solution. In the compliance testing, IPC Unigy 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 Unigy to Avaya Aura® Communication Manager, and SIP trunks were used from Avaya Aura® Communication Manager to Avaya Aura® SIP Enablement Services to reach Avaya Modular Messaging. The Avaya Modular Messaging system in the Central site supported local subscribers from Avaya Aura® Communication Manager at the Central site, and from IPC turret users at the Remote site.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required for IPC Unigy to interoperate with Avaya Modular Messaging 5.2 and Avaya Aura® SIP Enablement Services (SES) 5.2.1 in a centralized messaging environment using QSIG trunks to Avaya Aura® Communication Manager 5.2.1.

IPC Unigy is a trading communication solution. In the compliance testing, IPC Unigy 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® SES 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, Avaya Digital, PSTN users, and/or the Avaya Modular Messaging voicemail pilot to verify various call scenarios. The Avaya Modular Messaging Web Subscriber Options web-based interface was used to configure subscriber features such as Call Me.

The serviceability test cases were performed manually by disconnecting and reconnecting the E1 connection to IPC Unigy.

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 Unigy to recover from adverse conditions, such as disconnecting/reconnecting the E1 connection to IPC Unigy.

2.2. Test Results

All test cases were executed. The following were the observations on IPC Unigy 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.
- For all multiple call forward scenarios involving calls forwarded to the called party's forward-to extension and then covered subsequently to Modular Messaging based on the coverage setting at the forward-to extension, the greeting for the forward-to party will be played instead of the original called party due to the called number not being passed by IPC for diverted calls.
- Upon logging into a turret, DTMF digits cannot be sent for initial calls with Modular Messaging when using the speakerphone, and the digits will be outpulsed in subsequent calls with Avaya endpoints. The workaround is to use the handset.

2.3. Support

Technical support on IPC Unigy can be obtained through the following:

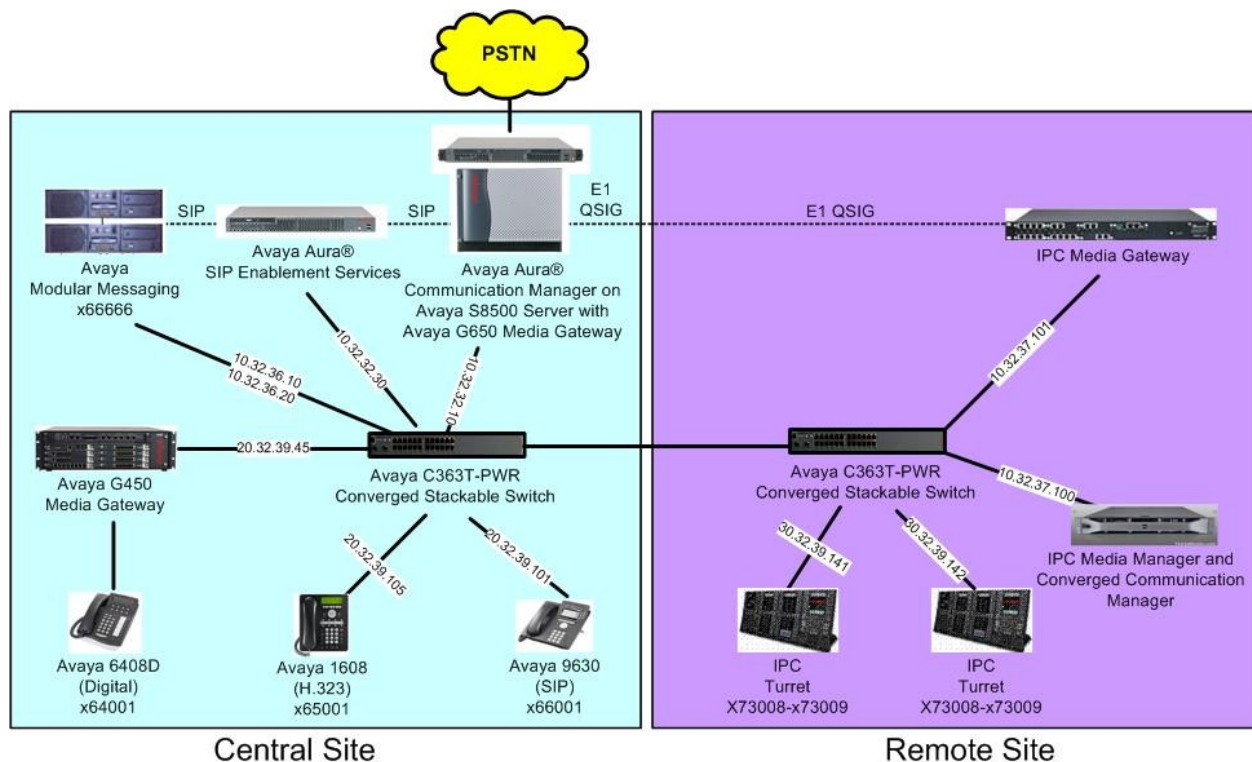
- **Phone:** (800) NEEDIPC, (203) 339-7800
- **Email:** systems.support@ipc.com

3. Reference Configuration

As shown in the test configuration below, IPC Unigy at the Remote Site consists of the Media Manager, Converged Communication Manager, and Turrets. E1 QSIG trunks were used from IPC Unigy to Avaya Aura® Communication Manager, and SIP trunks were used from Avaya Aura® Communication Manager to Avaya Aura® SES 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 detailed administration of basic connectivity among Avaya Aura® Communication Manager, Avaya Aura® SES, and Avaya Modular Messaging is not the focus of these Application Notes and will not be described. These Application Notes will focus on the additional configuration required to support IPC turret users as local subscribers on Avaya Modular Messaging.

The detailed administration of E1 QSIG trunks between Avaya Aura® Communication Manager and IPC Unigy, 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 [4]. 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 users at the Central site (64xxx-66xxx), and IPC turret users at the Remote site (73xxx). The Avaya Modular Messaging pilot number was 66666.



4. Equipment and Software Validated

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

Equipment	Software
Avaya Modular Messaging <ul style="list-style-type: none">Messaging Storage ServerMessaging Application Server	5.2 SP8 P4 5.2 SP8 P4
Avaya Aura® Communication Manager on Avaya S8500 Server	5.2.1 SP7.01 with special patch 19141 (R015x.02.1.016.4-19141)
Avaya G650 Media Gateway <ul style="list-style-type: none">TN799DP C-LAN Circuit PackTN2302AP IP Media ProcessorTN464HP DS1 Interface	HW01 FW038 HW20 FW122 HW02 FW024
Avaya G450 Media Gateway <ul style="list-style-type: none">MM712AP DCP	28.17 HW07 FW011
Avaya Aura® SIP Enablement Services	5.2.1 SP4 (SES-5.2.1.0-016.4-SP4C)
Avaya 1608 IP Telephone (H.323)	1.3
Avaya 9630 IP Telephone (SIP)	2.6.4
Avaya 6408D Digital Telephone	NA
IPC Unigy <ul style="list-style-type: none">Media ManagerConverged Communication ManageMedia GatewayTurrets	01.00.00.01.0003 01.00.00.01.0003 6.00AL.025.0002 01.00.00.01.0003

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Avaya Aura® Communication Manager.

Use the “change system-parameters coverage-forwarding” command. Enable **QSIG/SIP Diverted Calls Follow Diverted to Party’s Coverage Path**, as shown below.

```
change system-parameters coverage-forwarding          Page 1 of 2
                SYSTEM PARAMETERS CALL COVERAGE / CALL FORWARDING

CALL COVERAGE/FORWARDING PARAMETERS
    Local Cvg Subsequent Redirection/CFWD No Ans Interval (rings): 2
    Off-Net Cvg Subsequent Redirection/CFWD No Ans Interval (rings): 2
    Coverage - Caller Response Interval (seconds): 4
    Threshold for Blocking Off-Net Redirection of Incoming Trunk Calls: n
    Location for Covered and Forwarded Calls: called
    PGN/TN/COR for Covered and Forwarded Calls: caller
    COR/FRL check for Covered and Forwarded Calls? n
    QSIG/SIP Diverted Calls Follow Diverted to Party's Coverage Path? y
COVERAGE
```

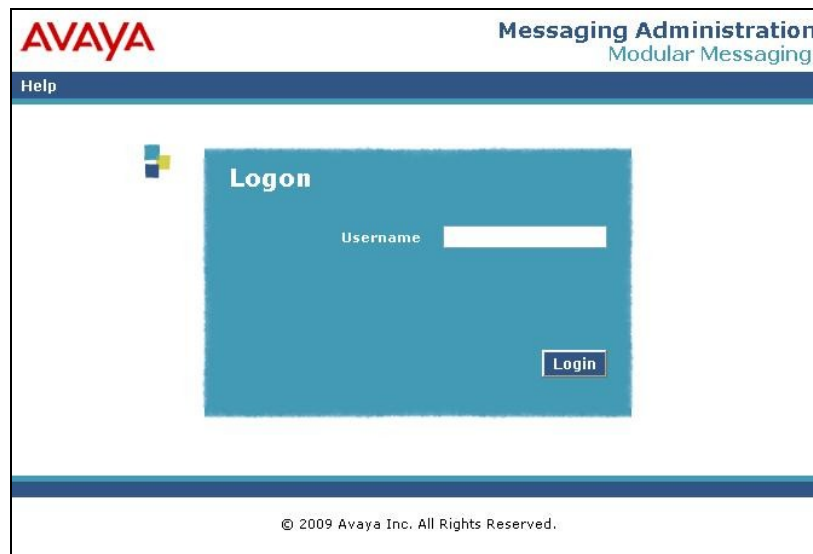
6. Configure Avaya Modular Messaging MSS

This section provides the procedures for configuring IPC turret users as local subscribers on Avaya Modular Messaging. The subscribers are 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 **Messaging Administration** screen appears, as shown below.



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 Avaya Modular Messaging Messaging Administration interface. The left pane lists navigation options under 'Messaging Administration' and 'Server Administration'. The main area is titled 'Manage Networked Machines' and contains a table with the following data:

Machine	IP Address	Machine Type	Total Subs
brmss1	10.32.36.10	local	11

Below the table 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 entry 70000-79999 was added for the IPC turret users.

The screenshot shows the 'Edit Networked Machine' screen. The left pane is the same as the previous screenshot. The main area contains a form with the following fields:

- Machine Name: brmss1
- Password: [empty]
- Confirm Password: [empty]
- IP Address: 10.32.36.10
- Machine Type: tcpip
- Mailbox Number Length: 5
- Default Community: 1
- Updates In: yes
- Updates Out: yes
- LDAP Port: 56389
- Log Updates In: no

Below the form is a section titled 'MAILBOX NUMBER RANGES' with a table:

Prefix	Starting Mailbox Number	Ending Mailbox Number
	60000	69999
	70000	79999

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 “73008”. Click **Add or Edit**.

	Machine Name	Local Subscriber Mailboxes	Total Subscribers	Filtered Subscribers
Local Subscribers	brmss1	22	23	23

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.

BASIC INFORMATION * (Required Fields)	
*Last Name	IPC
First Name	Trad 8
*Password
*Mailbox Number	73008
*Numeric Address	73008
PBX Extension	73008
*Class Of Service	0 - class00
*Community ID	1

SUBSCRIBER DIRECTORY	
Email Handle	@brmss1.br110.com
Telephone Number	

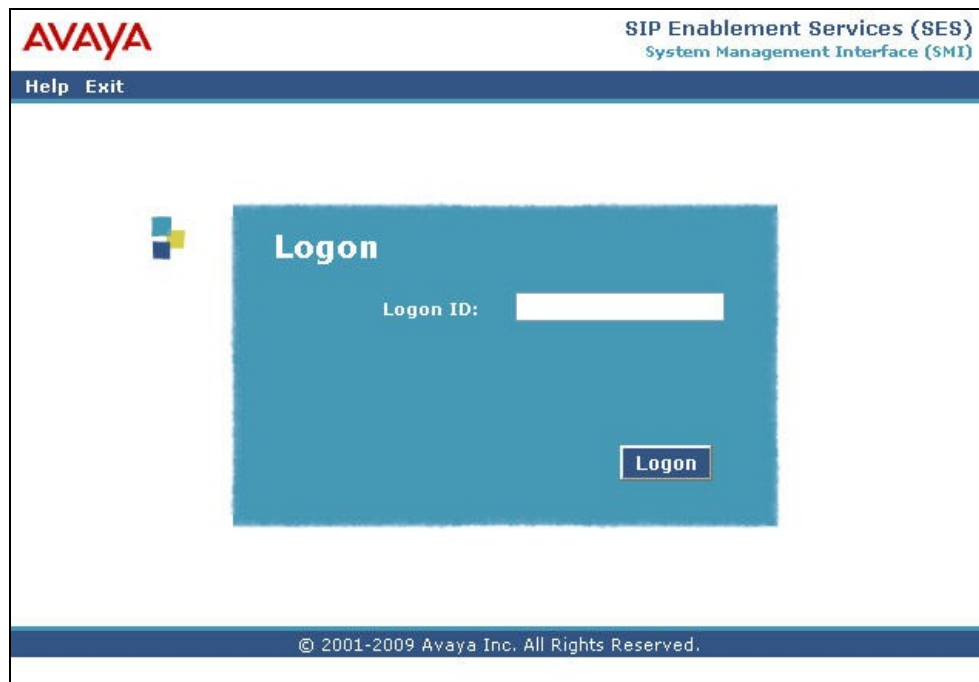
7. Configure Avaya Aura® SIP Enablement Services

The detailed configuration for adding Avaya Modular Messaging as an adjunct system on Avaya SES is assumed to be in place and will not be described. This section provides the procedures for adding a new address map for Modular Messaging to reach IPC turret users via Communication Manager, and for enabling unsolicited Notify messages, which is required for proper IPC integration. The configuration procedures include the following:

- Launch SES administration
- Administer Communication Manager servers address map
- Administer unsolicited Notify

7.1. Launch SES Administration

Access the SES web interface by using the URL “http://ip-address/admin” in an Internet browser window, where “ip-address” is the IP address of the SES server. Log in using the appropriate credentials.



The screenshot displays the Avaya SIP Enablement Services (SES) System Management Interface (SMI) login page. At the top left is the Avaya logo, and at the top right is the text "SIP Enablement Services (SES) System Management Interface (SMI)". Below this is a navigation bar with "Help" and "Exit" links. The main content area features a blue login box with the title "Logon". Inside the box, there is a "Logon ID:" label followed by a text input field. A "Logon" button is located at the bottom right of the box. To the left of the login box is a small Avaya logo icon. At the bottom of the page, a footer bar contains the copyright notice: "© 2001-2009 Avaya Inc. All Rights Reserved."

In the subsequent screen, select **Administration > SIP Enablement Services** from the top menu.

AVAYA SIP Enablement Services (SES)
System Management Interface (SMI)

Help Log Off Installation Administration Upgrade

This Server: [1] brses1

Legal Notice

**SIP Enablement Services
System Management Interface**

© 2001-2009 Avaya Inc. All Rights Reserved.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at:
<http://support.avaya.com/ThirdPartyLicense/>

The **Top** screen is displayed next.

AVAYA Integrated Management
SIP Server Management

Help Exit

This Server: [1] brses1

Top

Manage Users	Add and delete Users.
Manage Address Map Priorities	Adjust Address Map Priorities.
Manage Adjunct Systems	Add and delete Adjunct Systems.
Manage Event Aggregators	Add/Delete Event Aggregators.
Certificate Management	Manage Certificates.
Manage Conferencing	Add and delete Conference Extensions.
Manage Emergency Contacts	Add and delete Emergency Contacts.
Export Import to ProVision	Export and import data using ProVision on this host.
Manage Hosts	Add and delete Hosts.
IM logs	Download IM Logs.
Manage Communication Manager Servers	Add and delete Communication Manager Servers.
Manage Communication Manager Extensions	Add and delete Communication Manager Extensions.

7.2. Administer Communication Manager Servers Address Map

Select **Communication Manager Servers > List** from the left pane. The **List Communication Manager Servers** screen is displayed. Click on the **Map** link.

The screenshot shows the Avaya Integrated Management SIP Server Management interface. The left pane contains a navigation menu with the following items: Top, Users, Address Map Priorities, Adjunct Systems, Aggregator, Certificate Management, Conferences, Emergency Contacts, Export/Import to ProVision, Hosts, IM logs, Communication Manager Servers, Add, and List. The main pane displays the 'List Communication Manager Servers' screen. At the top right, it says 'Integrated Management SIP Server Management' and 'This Server: [1] brses1'. Below the title, there is a table with columns: Commands, Interface, and Host. The table contains one row with the following data: Edit, Extensions, Map (circled in red), Test-Link, Delete, CM-G650, and 10.32.32.30. Below the table, there is a link that says 'Add Another Communication Manager Server Interface'.

In the **List Communication Manager Server Address Map** screen below, click **Add Another Map** in the right pane.

The screenshot shows the Avaya Integrated Management SIP Server Management interface. The left pane contains a navigation menu with the following items: Top, Users, Address Map Priorities, Adjunct Systems, Aggregator, Certificate Management, Conferences, Emergency Contacts, Export/Import to ProVision, Hosts, IM logs, Communication Manager Servers, Add, and List. The main pane displays the 'List Communication Manager Server Address Map' screen. At the top right, it says 'Integrated Management SIP Server Management' and 'This Server: [1] brses1'. Below the title, there is a table with columns: Commands, Name, Commands, and Contact. The table contains two rows with the following data: Edit, Delete, CM-G650-6xxxx, and Edit, Delete, CM-G650-PSTN. Below the table, there is a link that says 'Add Another Map'. At the bottom, there is a link that says 'Add Map In New Group'.

The **Add Communication Manager Server Address Map** screen is displayed next. This screen is used to specify which calls are to be routed to Communication Manager. For **Name**, enter a descriptive name to denote the routing. For **Pattern**, enter an appropriate syntax for address mapping to IPC turret extensions. For the compliance testing, a pattern of “^sip:73[0-9]{3}” was used to match to IPC turret user extensions of 73xxx.



The screenshot displays the Avaya Integrated Management SIP Server Management interface. The top header features the Avaya logo on the left and the text 'Integrated Management SIP Server Management' on the right, with a status indicator 'This Server: [1] brses1'. Below the header is a navigation bar with 'Help' and 'Exit' links. A left-hand menu lists various system components: 'Top', 'Users', 'Address Map Priorities', 'Adjunct Systems', 'Aggregator', 'Certificate Management', 'Conferences', 'Emergency Contacts', and 'Export/Import to ProVision'. The main content area is titled 'Add Communication Manager Server Address Map'. It contains two required fields: 'Name*' with the value 'IPC-73xxx' and 'Pattern*' with the value '^sip:73[0-9]{3}'. A note states 'Fields marked * are required.' and an 'Add' button is positioned below the fields.

Add Communication Manager Server Address Map	
Name*	IPC-73xxx
Pattern*	^sip:73[0-9]{3}
Fields marked * are required.	
<input type="button" value="Add"/>	

7.3. Administer Unsolicited Notify

Log in to the Linux shell of the SES server with the appropriate credentials. Navigate to the `/usr/impress/sip-server/etc` directory, and open the `ccs.conf` file.

Navigate to the **Proxy** section, and set the **RouteUnsolicitedNotifyToPermanentContacts** parameters to “true”, as shown below. This will enable SES to support unsolicited Notify messages from Avaya Modular Messaging for IPC subscribers.

```
=====
[Proxy]
;
; EnableTlsClientAuthentication values are no longer true or false. Valid
; values are:
; none      - never use client certificates
; optional  - client certificates may or may not be present
; mandatory - client certificates must be present
=====
EnableAuthentication=true
;EnableSpoofingCheck=false
EnableTlsClientAuthentication=optional
EnableSubscribeRouting=false
EnableWCallFlow=true
PerContactWaitTime=180
MM_PerContactWaitTime=0
TimerB=2000
TimerC=180000
LocationSetTimer=180
EnableUnregisteredOptimContacts=true
InsertRecordRoute=false
CorrectReferToHeader=true
;EnableThirdPartyOriginatingProcessing=true
;SourcePaiHeaderFromFromHeader=true
ProxyType=TransactionStateful
EnableRecursion=true
EnableRecordRoute=true
;EnableOODReferRouting=false;
RouteUnsolicitedNotifyToPermanentContacts=true
```

From the Linux command line, restart the SipServer component using the commands shown below.

```
xxxxx@brses1> stop -s SipServer
Do you really want to continue? (y or n) y

xxxxx@brses1> start -s SipServer
xxxxx@brses1>
```

8. Configure IPC Media Manager

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

- Launch Unigy Management System
- Administer dial patterns
- Administer route plans
- Administer voicemail buttons

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

8.1. Launch Unigy Management System

Access the Unigy Management System web interface by using the URL “http://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Media Manager. Log in using the appropriate credentials.

The screen below is displayed. Enter the appropriate credentials. Check **I agree with the Terms of Use**, and click **Login**.

In the subsequent screen (not shown), click **Continue**.



The screenshot shows the login interface for the IPC Unigy Management System. On the left is the IPC logo. To its right are two input fields: 'User Name:' and 'Password:'. Below these fields is a checkbox labeled 'I agree with the' followed by a link 'Terms of Use'. A 'Login' button is positioned to the right of the checkbox. At the bottom of the form, the following text is displayed: 'IPC Unigy™ Management System', 'Unigy™ Version 01.00.00.01.0003', and '© Copyright 2011 IPC Systems, Inc.'

8.2. Administer Dial Patterns

In the subsequent screen, select **Configuration > Site Configuration** from the top menu. The **Site Configuration** information is displayed in the left pane.

Select **Routing > Dial Patterns** in the left pane, to display the **Dial Patterns** screen in the right pane. Click **Add New** in the upper right pane.

Add a new dial pattern for the Modular Messaging pilot number from **Section 3**, and another dial pattern for Modular Messaging that includes the routing prefix from Communication Manager. Note that when a call to an Avaya endpoint covers to Modular Messaging, the divert destination received from Communication Manager will include the routing prefix, which must be configured on Media Manager.

In the compliance testing, the existing dial pattern “6xxxx” included the Modular Messaging pilot number “66666”, and a new dial pattern was added below to include the existing AAR routing prefix “8” from Communication Manager.

In the **Dial pattern Details** sub-section in the lower right pane, enter the dial pattern to match in the **Pattern String** field, in this case “866666”. Enter desired **Name** and **Description**, and select “External” for **Call Classification**. Click **Save** (not shown).

The screenshot displays the UniGY configuration interface. The top navigation bar includes 'Configuration', 'System Designer', 'Alarms', 'Tools', 'About', and 'Help'. The main header shows 'Configuration -> Site Configuration' and 'Powered by'. The left sidebar, titled 'Site Configuration: Location', lists various configuration areas: Trunks, Communication Devices, Servers, Lines and Extensions, Hunt Group, Routing (selected), Trunk Groups, Route Lists, Dial Patterns (highlighted), Route Plans, Codecs, Voice Recording, License Manager, System, Directories, System Features, SNMP Profiles, SMTP, Prototype Devices, and AFM. The main content area is titled 'Dial Patterns' and contains a table with columns: Name, Pattern String, Outbound CLI, Call Classification, Prefix Digits, and Description. The table lists two existing patterns: '6xxxx' with pattern string '6\$\$\$\$' and 'Avaya Endpoints' description, and '91xxxxxxxxxx' with pattern string '91\$\$\$\$\$\$\$\$' and 'PSTN' description. Below the table are 'Add New' and 'Delete' buttons, with 'Add New' circled in red. The 'Dial pattern Details' section is visible below the table, showing fields for Name (866666), Description (MM Coverage), Pattern String (866666), Outbound CLI, and Call Classification (External).

Name	Pattern String	Outbound CLI	Call Classification	Prefix Digits	Description
6xxxx	6\$\$\$\$		External		Avaya Endpoints
91xxxxxxxxxx	91\$\$\$\$\$\$\$\$		External		PSTN

Dial pattern Details

Properties

Name * 866666

Description * MM Coverage

Pattern String * 866666

Outbound CLI

Call Classification * External

8.3. Administer Route Plans

Select **Routing > Route Plans** in the left pane, and click **Add New** (not shown) in the right pane to create a new route plan for each new dial pattern from **Section 8.2**.

The screen is updated with three panes, as shown below. In the **Route Plan** middle pane, enter a descriptive **UI Name** and optional **Description**. For **Calling Party**, enter “*” to denote any calling party from Unigy. For **Called Party**, select the dial pattern from **Section 8.2**. Select “Forward” for **Action**, and click **Save** (not shown).

The screenshot shows the Unigy configuration interface. The top navigation bar includes 'Configuration', 'System Designer', 'Alarms', 'Tools', 'About', and 'Help'. The right side of the top bar shows the time '10:21 EDT-0400' and the user 'mgr1'. The main header is 'Configuration -> Site Configuration'. The left pane, 'Site Configuration', has a 'Location' dropdown set to 'All Locations' and a tree view with 'Routing' selected. The middle pane, 'Route Plan', contains a 'Create New Route Plan' form with the following fields: 'UI Name' (IPC2MM), 'Description' (empty), 'Calling Party' (*), 'Called Party' (866666), and 'Action' (Forward). The right pane, 'Available to Assign', shows a 'Route Lists' section with a table containing one entry: 'Avaya QSIG Route'.

The screen is updated with the newly created route plan. Select the route plan, and click **Edit** toward the bottom of the screen (not shown).

The screenshot shows the Unigy configuration interface with the 'List of Route Plans' table. The top navigation bar and header are the same as the previous screenshot. The left pane is the same. The middle pane, 'Route Plan', now displays a table with the following data:

UI Name	Calling Party	Called Party	Action
IPC2Avaya	*	6xxxx	FORWARD
IPC2PSTN	*	91xxxxxxxxxx	FORWARD
IPC2MM	*	866666	FORWARD

The right pane, 'Available to Assign', remains the same.

The screen is updated with three panes again. In the right pane, select the applicable route list and drag into the **Route List** sub-section in the middle pane, as shown below. Click **Save**.

Repeat this section as necessary to add a new route plan for each new dial pattern from **Section 8.2**.

The screenshot displays the UniQy Configuration -> Site Configuration interface. The top navigation bar includes links for Configuration, System Designer, Alarms, Tools, About, and Help, along with the time 10:30 EDT-0400 and the user mgr1. The main interface is divided into three panes. The left pane, titled 'Site Configuration', shows a tree view with categories like Trunks, Communication Devices, Servers, Lines and Extensions, Hunt Group, Routing, Codecs, Voice Recording, License Manager, System, Directories, and System Features. The 'Routing' category is expanded, and 'Route Plans' is selected. The middle pane, titled 'Route Plan', contains a 'Create New Route Plan' form. The form fields are: UI Name (IPC2MM), Description (empty), Calling Party (*), Called Party (866666), and Action (Forward). Below these fields is a 'Route List' section with a table containing one entry: 'Avaya QSIG Route'. A 'Remove' button is located below the table. At the bottom of the form are 'Back', 'Revert', and 'Save' buttons. The right pane, titled 'Available to Assign', shows a 'Route Lists' section with a table containing one entry: 'Avaya QSIG Route'.

UI Name	Description	Calling Party	Called Party	Action
IPC2MM		*	866666	Forward

Route List
Avaya QSIG Route

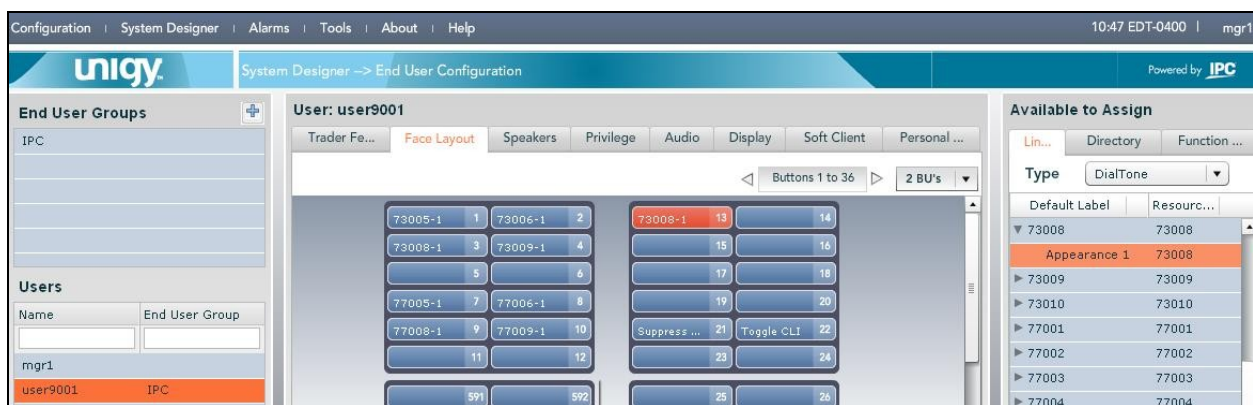
Route Lists
Avaya QSIG Route

8.4. Administer Voicemail Buttons

Select **System Designer > End User Configuration** from the top menu, to display the end user information in the left pane. Select the desired user from the left pane, in this case “user9001”.

In the middle pane, select the **Face Layout** tab.

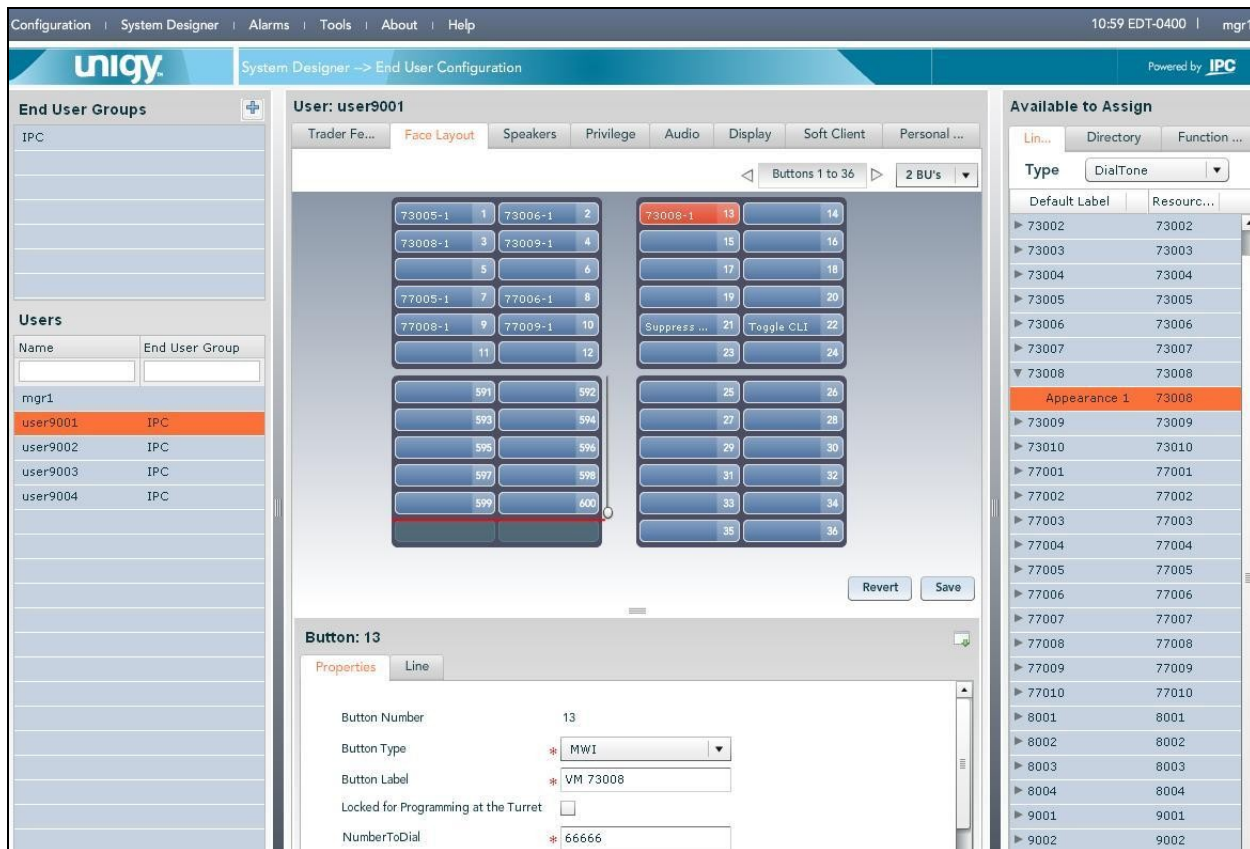
In the right pane, select the **Lines** tab. For **Type**, select “DialTone” from the drop-down list to display a list of available lines. Scroll the pane as necessary to locate and expand the desired turret extension, in this case “73008”. Select the corresponding appearance for the turret extension from the right pane, and drag into an available button in the middle pane, in this case button “13” as shown below.



Select the new button in the upper middle pane, in this case button “13”, to enable the button to be configured in the lower middle pane.

In the lower middle pane, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Button Type:** “MWI”
- **Button Label:** A descriptive name.
- **NumberToDial:** The Modular Messaging pilot number from **Section 3**.



Repeat this section for all desired users. In the compliance testing two voicemail buttons corresponding to turret subscriber extensions of “73008” and “73009” were created for the two turrets users.



9. Configure IPC Media Gateway

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

- Launch gateway web interface
- Obtain network interface name
- Administer media realm
- Administer proxy sets
- Administer IP group
- Administer trunk group settings
- Administer MWI notification

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

9.1. Launch Gateway Web Interface

Access the Media Gateway web interface by using the URL “http://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Media Gateway. Log in using the appropriate credentials.



The screenshot shows the login interface for the IPC Unigy Management System. It features a blue square logo with the letters 'IPC' in white. To the right of the logo are two input fields: 'User Name:' and 'Password:'. Below these fields is a checkbox labeled 'I agree with the' followed by a blue underlined link 'Terms of Use'. A 'Login' button is positioned to the right of the checkbox. At the bottom of the page, the text reads: 'IPC Unigy™ Management System', 'Unigy™ Version 01.00.00.01.0003', and '© Copyright 2011 IPC Systems, Inc.'

9.2. Obtain Network Interface Name

The screen below is displayed. Click the radio button for **Full** in the left pane, and select **VoIP > Network Settings > IP Settings** to display the **Multiple Interface Table** screen. Note the value of **Interface Name**, in this case “Voice”.

The screenshot shows the AudioCodes Mediant 1000 - MSBG web interface. The top navigation bar includes the AudioCodes logo, the device name 'Mediant 1000 - MSBG', and buttons for 'Submit', 'Burn', 'Device Actions', 'Home', 'Help', and 'Log off'. The left sidebar contains a tree view with 'Configuration' selected, and sub-tabs for 'Basic' and 'Full'. Under 'Full', the 'VoIP' section is expanded, showing 'Network Settings' > 'IP Settings' selected. The main content area is titled 'Multiple Interface Table' and includes a note: 'Note: Select row index to modify the relevant row.' Below the note is an 'Add Index' button and a 'Done' button. A table displays the interface configuration:

Index	Application Type	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	<input type="radio"/> QAMP + Media + Control	10.32.37.101	24	10.32.37.1	1	Voice

Below the table is a horizontal scrollbar.

9.3. Administer Media Realm

Select **VoIP > Protocol Configuration > Media Realm Configuration** from the left pane to display the **SIP Media Realm Table** screen. Enter “0” and click **Add Index**.

In the new index entry line, enter the values shown in the screenshot below. Note that the **Media Real Name** can be any descriptive name, and the **IPv4 Interface Name** is the interface name from **Section 9.2**.

AudioCodes Mediant 1000 - MSBG

Configuration Management Status & Diagnostics

Search

Basic

System

VoIP

Network Settings

Media Settings

PSTN Settings

Protocol Configuration

Media Realm Configuration

Applications Enabling

Trunk Group

Protocol Definition

Application Network Setting

Proxies, Registration, IP Groups

Coders And Profile Definitions

SIP Advanced Parameters

Manipulation Tables

Routing Tables

Alternative Routing

Routing General Parameters

Tel to IP Routing

IP to Trunk Group Routing

SIP Media Realm Table

Basic Parameter List

0 Add Index Delete Apply

Index	Media Realm Name	IPv4 Interface Name	Port Range Start	Number Of Media Session Legs	Port Range End
0	LanRealm	Voice	6000	120	7190

Default Media Realm Name

Submit

9.4. Administer Proxy Sets

Select **VoIP > Protocol Configuration > Proxies, Registration, IP Groups > Proxy Sets Table** from the left pane to display the **Proxy Sets Table** screen.

For **Proxy Set ID**, select “0”. Set the first **Proxy Address** to the IP address of IPC Media Manager, and set the corresponding **Transport Type** to “UDP”. Retain the default values in the remaining fields.

Repeat the above with **Proxy Set ID** of “1”. Note that the current release requires both proxy set IDs to be configured.

The screenshot shows the AudioCodes Mediant 1000 - MSBG configuration interface. The left pane displays a tree view with the following structure:

- System
 - VoIP
 - Network Settings
 - Media Settings
 - PSTN Settings
 - Protocol Configuration
 - Media Realm Configuration
 - Applications Enabling
 - Trunk Group
 - Protocol Definition
 - Application Network Setting
 - Proxies, Registration, IP Groups
 - IP Group Table
 - Account Table
 - Proxy & Registration
 - Proxy Sets Table**
 - Coders And Profile Definitions
 - SIP Advanced Parameters
 - Manipulation Tables
 - Routing Tables
 - Alternative Routing

The main pane displays the **Proxy Sets Table** configuration screen. At the top, there is a dropdown menu for **Proxy Set ID** set to 0. Below this is a table with 5 rows and 2 columns: **Proxy Address** and **Transport Type**.

	Proxy Address	Transport Type
1	10.32.37.100	UDP
2		
3		
4		
5		

Below the table is a section for additional settings:

Enable Proxy Keep Alive	Disable
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	No

A **Submit** button is located at the bottom right of the main pane.

9.5. Administer IP Group

Select **VoIP > Protocol Configuration > Proxies, Registration, IP Groups > IP Group Table** from the left pane to display the **IP Group Table** screen.

For **Proxy Set ID**, select “1”. For **Media Realm**, select the media realm name from **Section 9.3**. Retain the default values in the remaining fields.

The screenshot displays the AudioCodes Mediant 1000 - MSBG web interface. The left navigation pane shows the tree structure with 'IP Group Table' selected under 'Proxies, Registration, IP Groups'. The main content area is titled 'IP Group Table' and contains a 'Basic Parameter List' section. The 'Index' dropdown is set to '1'. The 'Common Parameters' section includes fields for 'Description', 'Proxy Set ID' (set to '1'), 'SIP Group Name', 'Contact User', 'IP Profile ID' (set to '0'), 'SRD' (set to '0'), and 'Media Realm' (set to 'LanRealm'). The 'Gateway Parameters' section includes fields for 'Always Use Route Table' (set to 'No'), 'Routing Mode' (set to 'Not Configured'), 'SIP Re-Routing Mode' (set to 'Standard'), 'Enable Survivability' (set to 'Disable'), and 'Service IP Group ID'. A 'Submit' button is located at the bottom right of the configuration area.

Basic Parameter List	
Index	1
Common Parameters	
Description	
Proxy Set ID	1
SIP Group Name	
Contact User	
IP Profile ID	0
SRD	0
Media Realm	LanRealm
Gateway Parameters	
Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard
Enable Survivability	Disable
Service IP Group ID	

9.6. Administer Trunk Group Settings

Select **VoIP > Protocol Configuration > Trunk Group > Trunk Group Settings** from the left pane to display the **Trunk Group Settings** screen.

Create a new trunk group entry with the following values for the specified fields.

- **Trunk Group ID:** “1”
- **Channel Select Mode:** “Cyclic Ascending”
- **Serving IP Group ID:** The IP group table index from **Section 9.5**.
- **MWI Interrogation Type:** “Use Result” to enable sending of SIP NOTIFY messages.

AudioCodes Mediant 1000 - MSGB

Configuration Management Status & Diagnostics

Search

Basic Full

System

VoIP

Network Settings

Media Settings

PSTN Settings

Protocol Configuration

Media Realm Configuration

Applications Enabling

Trunk Group

Trunk Group Settings

Protocol Definition

Application Network Setting

Proxies, Registration, IP Groups

Coders And Profile Definitions

SIP Advanced Parameters

Manipulation Tables

Routing Tables

Digital Gateway

IP Media

TDM Configuration

Advanced Applications

Data Settings

Trunk Group Settings

Basic Parameter List

Index 1-10

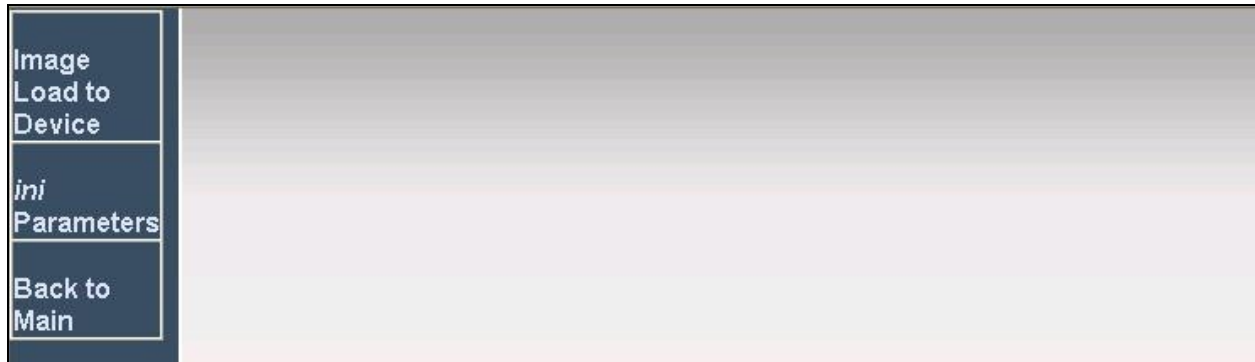
Trunk Group ID	Channel Select Mode	Registration Mode	Serving IP Group ID	Gateway Name	Contact User	MWI Interrogation Type
1	Cyclic Ascending		1			Use Result
2						Not Configured
3						Not Configured
4						Not Configured
5						Not Configured
6						Not Configured
7						Not Configured
8						Not Configured
9						Not Configured
10						Not Configured

Submit

9.7. Administer MWI Notification

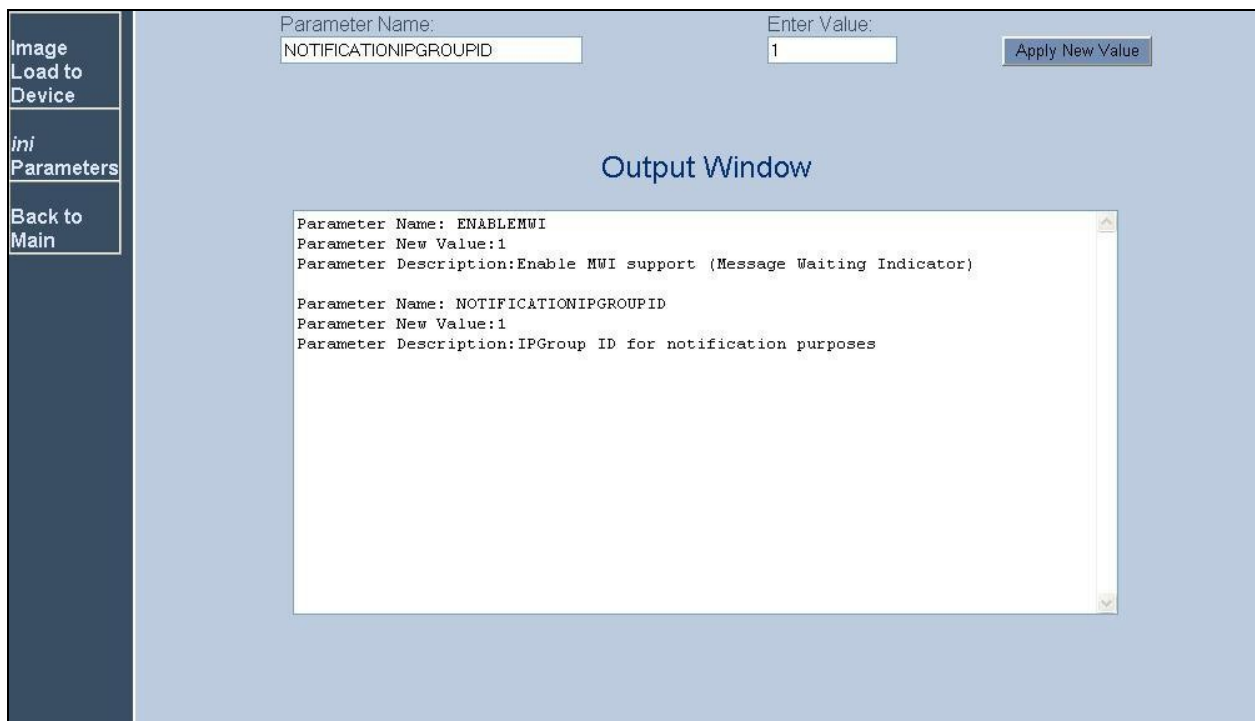
Access the Media Gateway administration page web interface by using the URL “http://ip-address/AdminPage” in an Internet browser window, where “ip-address” is the IP address of the Media Gateway.

The screen below is displayed. Select **ini Parameters**, and enter the appropriate credentials in the pop-up box (not shown).



The screen below is displayed next. Enter “ENABLEMWI” and “1”, and click **Apply New Value** to set the parameter.

Repeat with “NOTIFICATIONGROUPID” and “1” as shown below.



10. Verification Steps

This section provides tests that can be performed to verify proper configuration of Avaya Modular Messaging and IPC Unigy.

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.

11. Conclusion

These Application Notes describe the configuration steps required for IPC Unigy to successfully interoperate with Avaya Modular Messaging 5.2 and Avaya Aura® SIP Enablement Services 5.2.1 in a centralized messaging environment using QSIG trunks to Avaya Aura® Communication Manager 5.2.1. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

12. Additional References

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

1. *Administrator Guide for Avaya Aura™ Communication Manager*, Document 03-300509, Issue 8.0, Release 5.2, May 2009, available at <http://support.avaya.com>.
2. *Installing, Administering, Maintaining, and Troubleshooting Avaya Aura™ SIP Enablement Services*, Document ID 03-600768, Issue 8.0, November 2009, available at <http://support.avaya.com>.
3. *CN 88010 Avaya S8xx0 Session Initiation Protocol (SIP) Integration*, Version AH, August 2010, available at <http://support.avaya.com>.
4. *Avaya Modular Messaging for the Avaya Message Store Server (MSS) Configuration*, Release 5.0, February 2009, available at <http://support.avaya.com>.
5. *Application Notes for IPC Unigy with Avaya Aura® Communication Manager 5.2.1 using QSIG Trunks*, Issue 1.0, available at <http://support.avaya.com>.
6. *Unigy 1.1 System Configuration*, Part Number B02200187, Release 00, upon request to IPC Support.

©2011 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.