AVAYA

Avaya Solution & Interoperability Test Lab

Application Notes for IPC Unigy V2 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 Unigy V2 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.

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.

CRK; Reviewed:
SPOC 7/10/2014
Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.
1 of 34
UniV2-SM63MM-SS

1. Introduction

These Application Notes describe the configuration steps required for IPC Unigy V2 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 Unigy is a trading communication solution. In the compliance testing, IPC Unigy 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 Unigy V2 server.

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 consists of feature and serviceability testing.

The feature testing included subscriber login, greeting, voice message (leaving/retrieving), 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 V2 to recover from adverse conditions, such as disconnecting/reconnecting the LAN connection to the IPC Unigy V2 server.

2.2. Test Results

All test cases were executed. The following were the observations from the compliance testing.

- With shuffling on, the greeting stops in the middle of greeting, during retrieving messages. Recommends shuffling to be OFF.

- 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.

- Receptionist/Personal Operator/Auto Attendant/Transfer – 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.

- Find Me – When a turret is a Find Me station, the following symptoms were observed;
    - After the call goes to FindMe, the FindMe station can't acknowledge the call. The DTMF digit ("#") did not work.
    - During the Find Me message, the message cuts off and disconnects the call. Calling party was still connected to MM and directly goes to the called party VoiceMail.

- Call Me – When a Turret is a Call Me station, the following symptoms were observed;
    - During the message at the CallMe station, the message cuts off and disconnects the call.
    - When Called is Turret, Call Me feature did not work.

- Transfer – When a turret is a Transfer-to station, the same symptom were observed as Receptionist/Personal Operator/Auto Attendant test cases.

IPC does not expect their users to use these features, so the testing was passed. The issues are listed here for user awareness, and the above mentioned features are not supported with this solution.

2.3. Support

Technical support on IPC Unigy V2 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 Unigy V2 consists of the Media Manager and Converged Communication Manager (HA system), and Turrets. SIP trunks are used from IPC Media Manager and Converged Communication Manager (virtual) 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 between Session Manager, and IPC Unigy V2, 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.
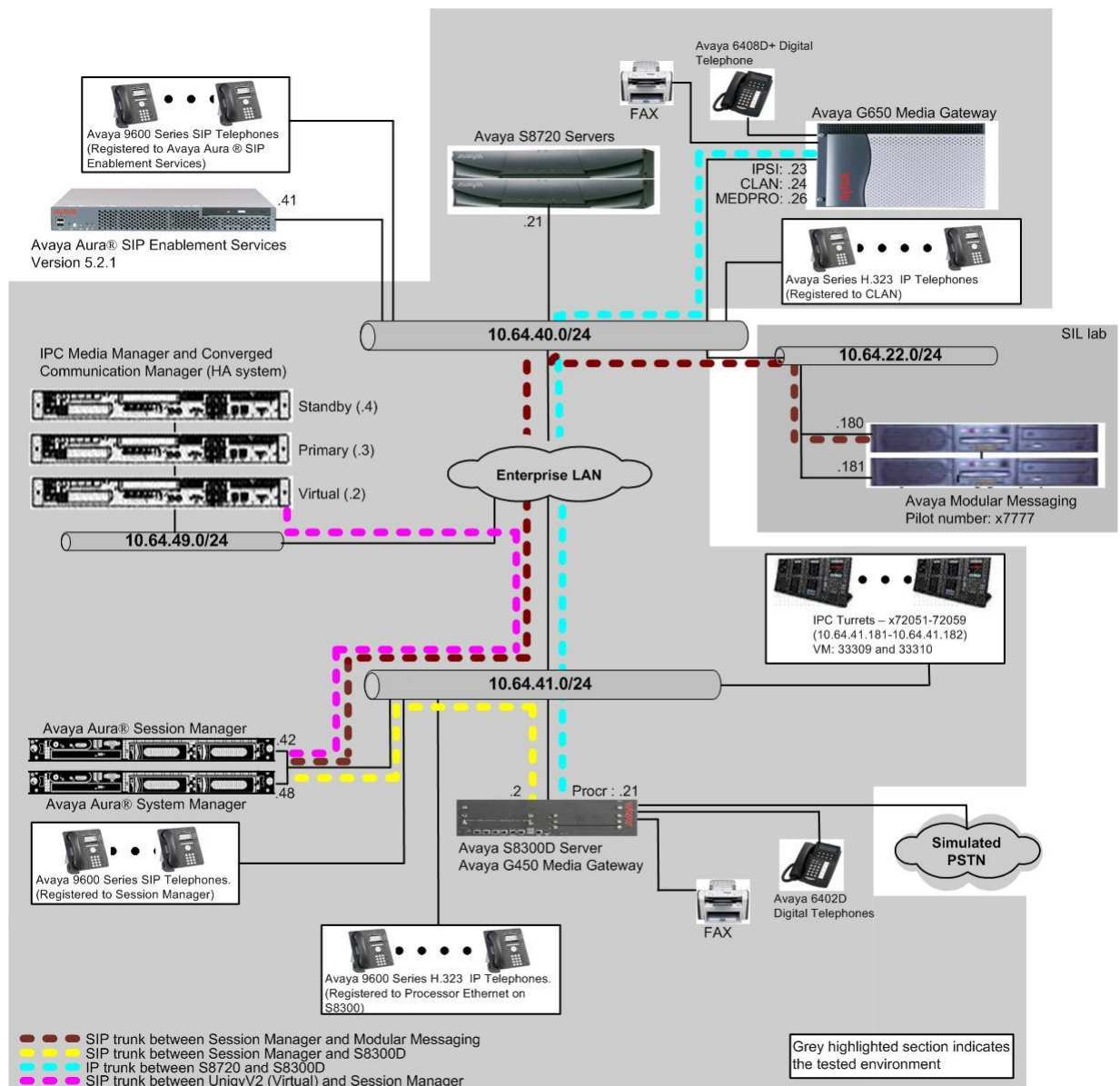
Figure 1: Test Configuration of IPC Unigy system with Avaya Modular Messaging

4. Equipment and Software Validated

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

Equipment	Software
Avaya Modular Messaging • 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 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 Unigy V2 • Media Manager • Converged Communication Manager • Turrets	02.00.00.07.0025 02.00.00.07.0025 02.00.00.07.0025

5. Configure Avaya Aura® Communication Manager

The configuration of Communication Manager is not a part of these Application Notes, since the test involves Avaya Modular Messaging. However, during the test, abnormal behavior was observed. During retrieving messages from IPC turrets, messages cut-off in the middle of greeting. To remedy the issue, the following topics are discussed:

- Configure hunt group
- Configure signaling group

5.1. Configure Hunt Group

This section describes the steps for administering a hunt group in Communication Manager, as a work-around solution. The following describes the call path that failed and a work-around.

Failed scenario:

- Turret →Session Manager →Avaya Modular Messaging (x7777)

Work-around solution:

- Turret → Session Manager → Communication Manager Hunt Group (x7776) →Session Manager → Avaya Modular Messaging (x7777)

Enter the **add hunt-group <h>** command; where **h** is an allocated hunt group number. The following fields were configured for the compliance test.

- Group Name – Enter a descriptive name
- Group Extension – Enter a group extension. This is the extension that IPC turrets will be used to retrieve calls.

```
add hunt-group 98                                              Page   1 of  60
                              HUNT GROUP

            Group Number: 98                              ACD? n
              Group Name: ToMMviaSM                     Queue? n
         Group Extension: 7776                          Vector? n
              Group Type: ucd-mia             Coverage Path:
                      TN: 1         Night Service Destination:
                     COR: 1                     MM Early Answer? n
           Security Code:             Local Agent Preference? n
 ISDN/SIP Caller Display: mbr-name
```

On **Page 2**, provide the following information:

- Message Center – Enter **sip-adjunct**, indicating the type of messaging adjunct used for this hunt group.
- Voice Mail Number – Enter the Voice Mail Pilot Number, which is x7777.
- Voice Mail Handle –Enter the Voice Mail Handle which is the pilot number, x7777.
- Routing Digit (e.g. AAR/ARS Access Code) – Enter the AAR Access Code as defined in the Feature Access Code form.

```
display hunt-group 98                                      Page   2 of  60
                              HUNT GROUP




                        Message Center: sip-adjunct

     Voice Mail Number         Voice Mail Handle          Routing Digits
                                                    (e.g., AAR/ARS Access Code)
       7777                      7777                          8
```

5.2. Configure Signaling Group

This section describes a step for disable shuffling (also known as IP-to-IP direct).
An assumption is made that the signaling group is already configured, and here, only shows the field that disables shuffling. Set to **n** on the **Direct IP-IP Audio Connections** field.

```
display signaling-group 92                                 Page   1 of   2
                            SIGNALING GROUP

 Group Number: 92            Group Type: sip
  IMS Enabled? n        Transport Method: tls
       Q-SIP? n
    IP Video? y          Priority Video? y       Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

   Near-end Node Name: procr               Far-end Node Name: SM-1
 Near-end Listen Port: 5061              Far-end Listen Port: 5061
                                        Far-end Network Region: 1


Far-end Domain:
                                        Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate            RFC 3389 Comfort Noise? y
       DTMF over IP: rtp-payload         Direct IP-IP Audio Connections? n
Session Establishment Timer(min): 3                 IP Audio Hairpinning? n
       Enable Layer 3 Test? y
                                        Alternate Route Timer(sec): 6
```

6. Configure Avaya Modular Messaging MSS

This section provides the procedures for configuring IPC turret users as local subscribers on Avaya Modular Messaging. The subscriber management is configured on the Messaging Storage Server (MSS) component. The configuration procedures include the following areas:

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

6.1. Launch Messaging Administration

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

The **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.

Solution & Interoperability Test Lab Application Notes
©2014 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 7205x extensions used by the IPC turret users.

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 "72051". Click **Add or Edit**.

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.

7. 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**. Confirm to add information in the file to the registry on the Registry Editor window (not shown).
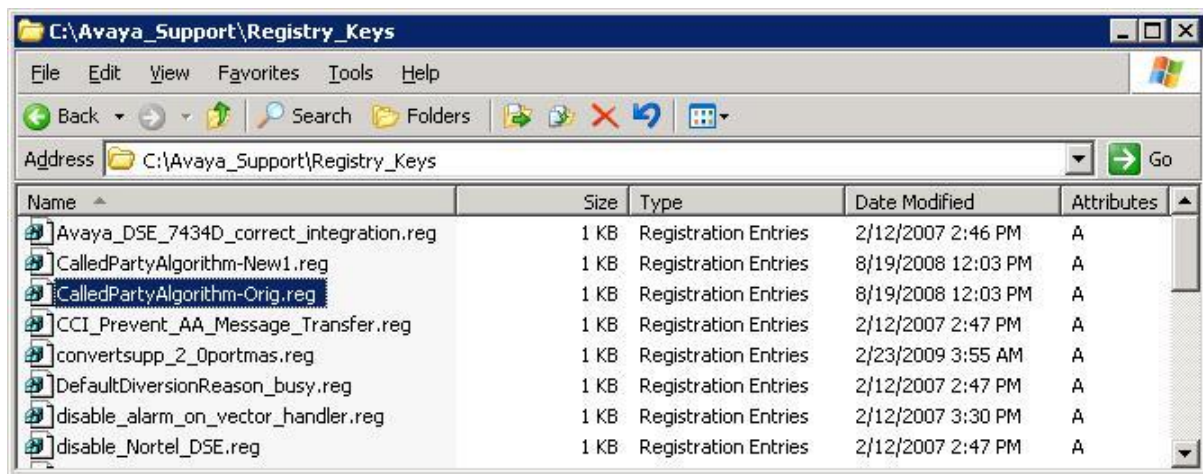
Select **Start → Settings → Control Panel → Administrative Tools → Services**, to display the **Services** screen. Navigate to the **MM Messaging Application Server** entry, right-click on the entry and select **Restart**. Repeat these procedures on all MAS servers.

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.
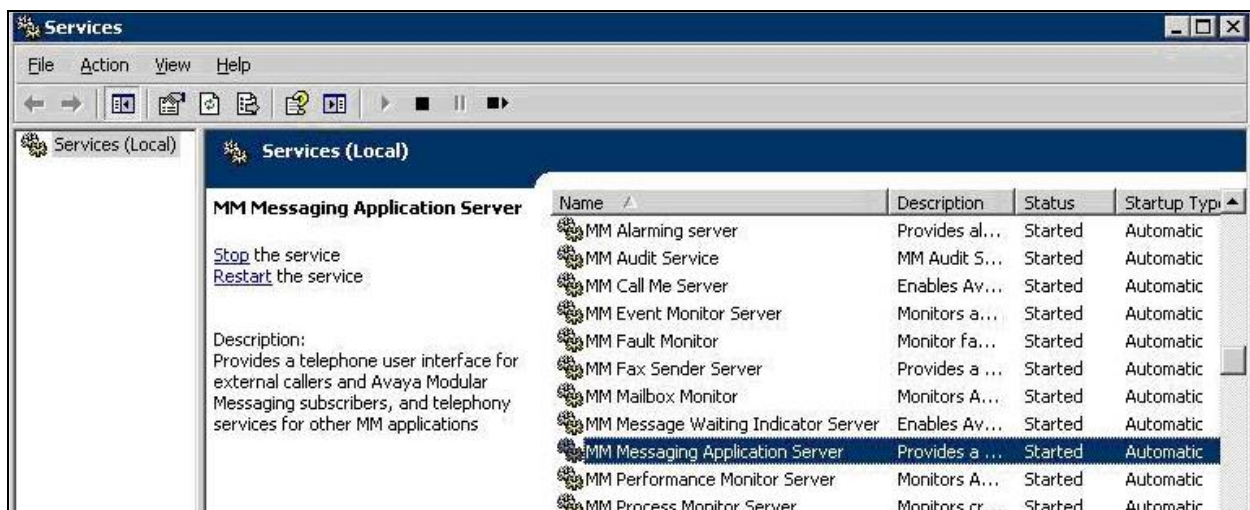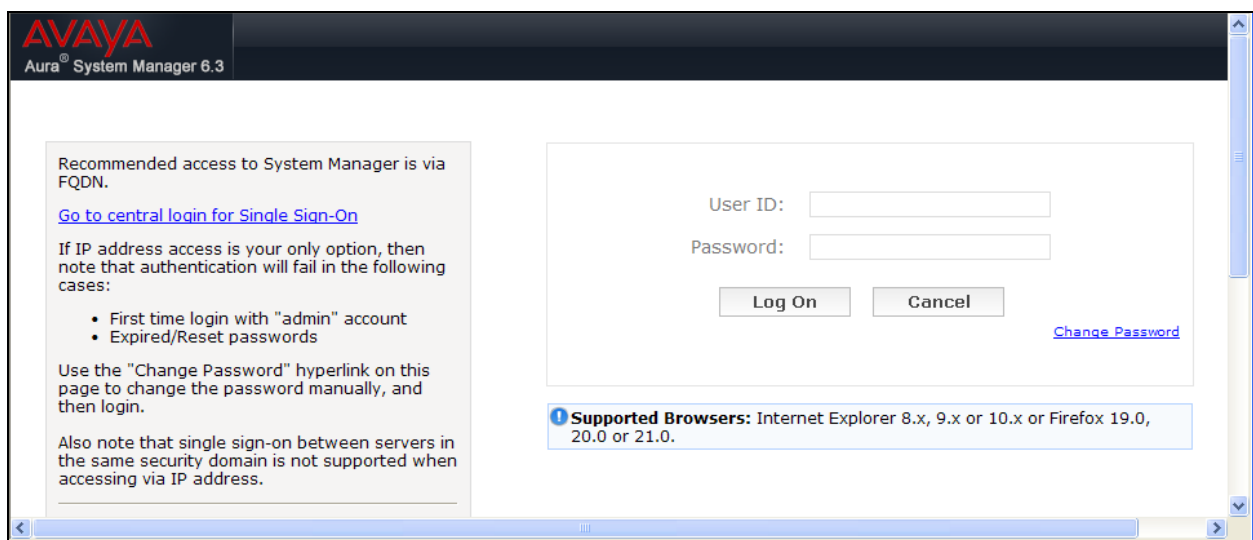
8. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer dial patterns

8.1. 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.

8.2. 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. Locate and click on the dial pattern that corresponds to the Modular Messaging pilot number, in this case "7777".

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.

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

9. Configure IPC Unigy V2 Converged Communication Manager

This section provides the procedures for configuring IPC Unigy V2 Converged Communication Manager. The procedures include the following areas:

- Launch Unigy V2 Management System
- Administer SIP trunks
- Administer trunk groups
- Administer route lists
- Administer dial patterns
- Administer route plans

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

9.1.   Launch Unigy V2 Management System

Access the UnigyV2 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 following screen (Tools -> Monitoring) displays. Navigate to **Configuration** ➔ **Site**.

1.1. Administer SIP Trunks

Select **Trunks → SIP Trunks** in the left pane, and click the **Add** icon ( ) in the lower left pane to add a new SIP trunk. Select "Dial Tone" from the **Select Connection Type** drop-down list.
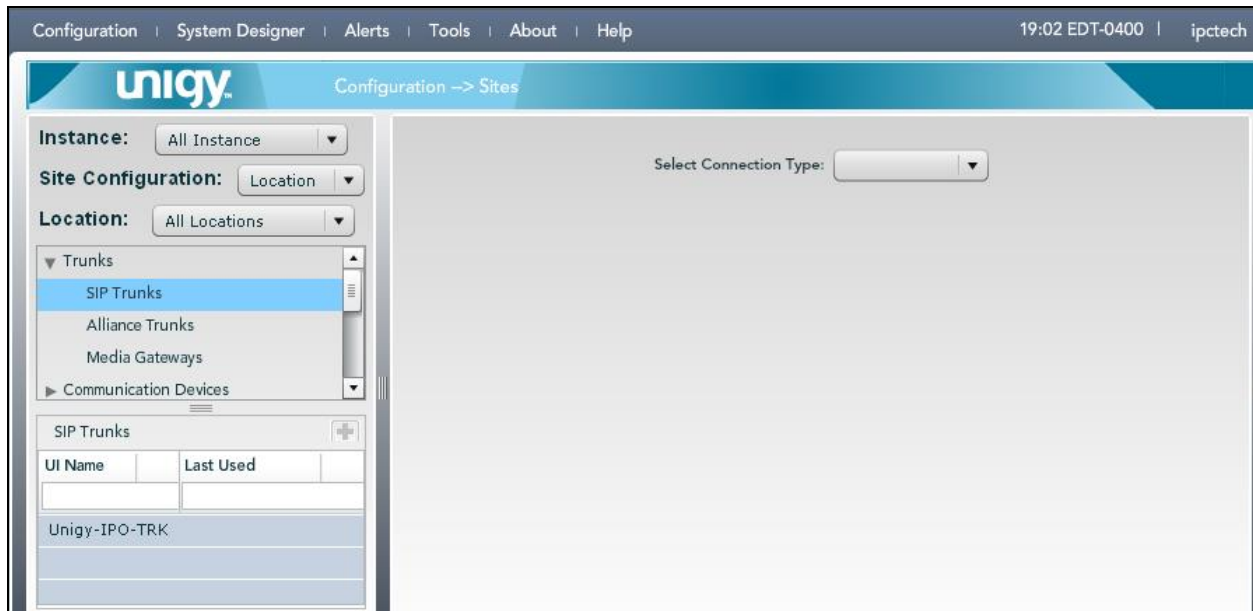
The screen below is displayed next. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Trunk Name:** A descriptive name.
- **Destination Address:** Enter the IP address of the Session Manager signaling interface.
- **Destination Port:** Enter the port number.
- **Zone:** An available zone, in this case "Default Zone 1".
- **Channels:** Enter the number of SIP trunk group members.
- **Reason Protocol** "SIP"
- **PBX Provider:** "Avaya"
- **Connected Party Update:** "UPDATE"

Retain the default values in the remaining fields.

CRK; Reviewed:
SPOC 7/10/2014

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

21 of 34
UniV2-SM63MM-SS

Select the Advance tab in the upper right. .Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Diversion Header:**   "History-Info.
- **Outgoing Transport Type:**   **"**UDP".
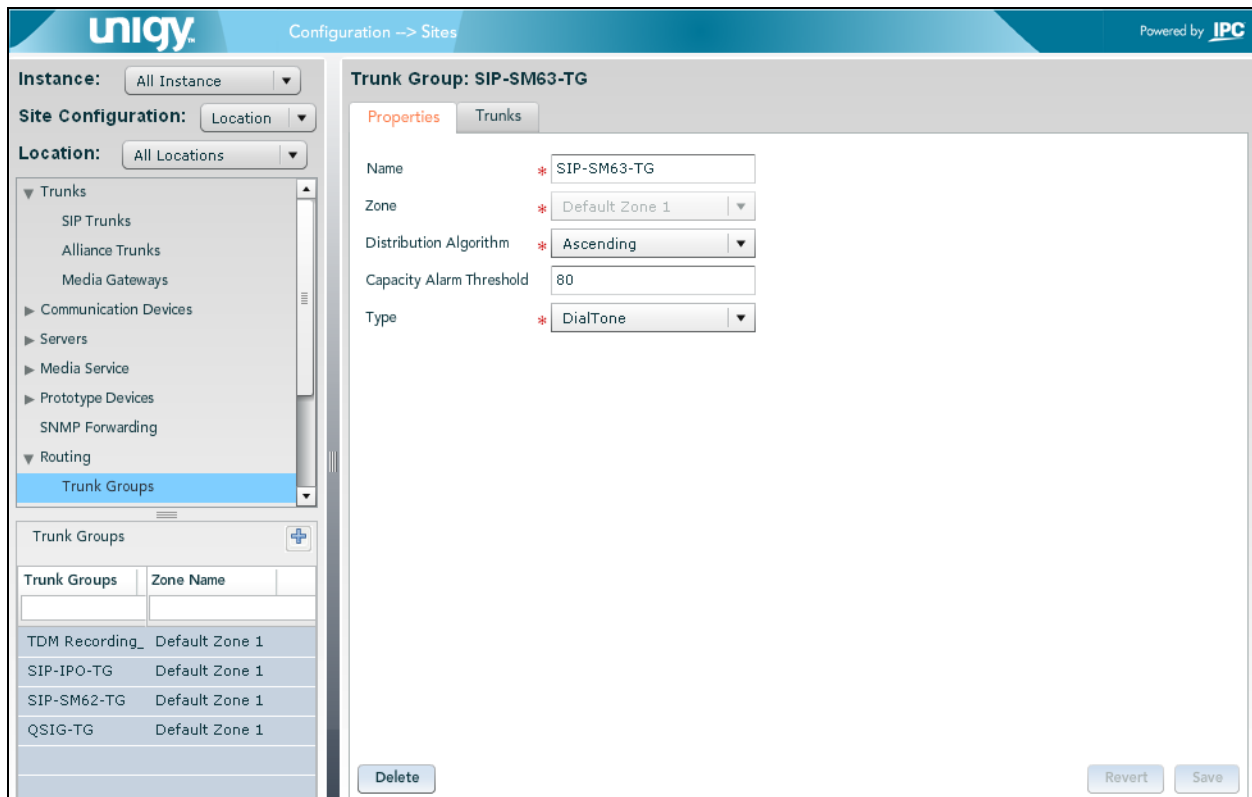
Click **Save** at the bottom

1.2. Administer Trunk Groups

Select **Routing → Trunk Groups** in the left pane, and click the **Add** icon ( ) in the lower left pane to add a new trunk group.

The **Trunk Group** screen is displayed in the right pane. In the **Properties** tab, enter a descriptive **Name**, select "Default Zone 1" for the **Zone** field, select "Ascending" for the **Distribution Algorithm** field, and click **Save**.

Select the **Trunks** tab in the right pane.

The screen is updated with three panes. In the rightmost pane, select the Trunks tab to display a list of trunks. Select the SIP trunk from **Section 1.1** in the rightmost pane and drag to the middle pane as shown below. Click **Save**.

1.3. Administer Route Lists

Select **Routing** ➔ **Route Lists** in the left pane, and click the **Add** icon ( ) in the lower left pane to add a new route list.

The **Route List** screen is displayed in the middle pane. For **Route List**, enter a descriptive name. In the right pane, select the trunk group from **Section 1.2** and drag into the **Assigned Trunk Groups on Route List** sub-section in the middle pane, as shown below. Click **Save**.

CRK; Reviewed:
SPOC 7/10/2014
Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.
25 of 34
UniV2-SM63MM-SS

1.4. Administer Dial Patterns

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

In the **Dial pattern Details** sub-section in the lower right pane, enter the desired **Name** and **Description**. For **Pattern String**, enter the dial pattern to match for Avaya endpoints, in this case "*" meaning any digits will be sent to Session Manager. Click **Save**. Once the **Save** button is clicked, the newly created Dial pattern should be displayed under the Dial Patterns section.

Repeat this section to add another dial pattern to reach the PSTN, and include any required prefix by Avaya Aura® Communication Manager.

CRK; Reviewed:
SPOC 7/10/2014

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

26 of 34
UniV2-SM63MM-SS

1.5. 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.

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 UnigyV2. For **Called Party**, select the dial pattern for Avaya endpoints from **Section 1.4**. Select "Forward" for **Action**, and click **Save**.

The screen is updated with the newly created route plan. Select the route plan, and click **Edit** toward the bottom of the screen.

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

The screen is updated with three panes again, as shown below. In the right pane, select the route list from **Section 1.3** and drag into the **Route List** sub-section in the middle pane, as shown below. Click **Save** (not shown).

10. Verification Steps

This section provides tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and IPC UnigyV2.

10.1. Verify Avaya Aura® Communication Manager

From the SAT interface, verify the status of the SIP trunk groups by using the "status trunk n" command, where "n" is the trunk group number administered in Communication Manager. Verify that all trunks are in the "in-service/idle" state as shown below.

```
status trunk 92


                        TRUNK GROUP STATUS

Member   Port      Service State      Mtce Connected Ports
                                      Busy

0092/001 T00135    in-service/idle    no
0092/002 T00136    in-service/idle    no
0092/003 T00137    in-service/idle    no
0092/004 T00138    in-service/idle    no
0092/005 T00139    in-service/idle    no
0092/006 T00140    in-service/idle    no
0092/007 T00141    in-service/idle    no
0092/008 T00142    in-service/idle    no
0092/009 T00143    in-service/idle    no
0092/010 T00144    in-service/idle    no
```

Verify the status of the SIP signaling groups by using the "status signaling-group n" command, where "n" is the signaling group number administered in Communication Manager. Verify that the signaling group is "in-service" as indicated in the **Group State** field, shown below.

```
status signaling-group 92
                    STATUS SIGNALING GROUP

     Group ID: 92
   Group Type: sip

   Group State: in-service
```

10.2. Verify Avaya Aura® Session Manager

From the System Manager home page (not shown), select **Elements** → **Session Manager** to display the **Session Manager Dashboard** screen (not shown). Select **Session Manager** → **System Status** → **SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. Click on the IPC entity name.

The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that **Conn. Status** and **Link Status** are "UP", as shown below.

10.3. Verify IPC UnigyV2

Make a call from/to an IPC turret user to an Avaya endpoint. Verify that the call can be connected with two-way talk paths.

CRK; Reviewed:
SPOC 7/10/2014

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

32 of 34
UniV2-SM63MM-SS

11. Conclusion

These Application Notes describe the configuration steps required for IPC Unigy V2 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**.

12. 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 Number03-603324

[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.