Avaya Solution & Interoperability Test Lab

Application Notes for IPC Unigy V2.0.1 with Avaya Aura® Messaging 6.3 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 V2.0.1 to interoperate with Avaya Aura® Messaging 6.3 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.

1. Introduction

These Application Notes describe the configuration steps required for IPC Unigy V2.0.1 to interoperate with Avaya Aura® Messaging 6.3and 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 V2.0.1 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 6.3 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 Unigy V2.0.1 servers.

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, and call sender.

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 V2.0.1 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 Avaya Aura® Messaging pilot number as the Call Forwarding destination for the users.

- During the compliance test, shuffling was disabled, since issues were observed from the previous version, when shuffling was enabled.

- Issues were observed on transfer features from Avaya Aura® Messaging.

- An issue was observed on Multiple Call Forward without answer.

IPC does not expect their users to use these features, so the testing was passed. The issues listed here are for user awareness.

2.3. Support

Technical support on IPC Unigy V2.0.1 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 V2.0.1 consists of the Media Manager and Converged Communication Manager (HA system), and Turrets. SIP trunks are used from and the Virtual IP (VIP) of Converged Communication Manager 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 Unigy V2.0.1, 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.

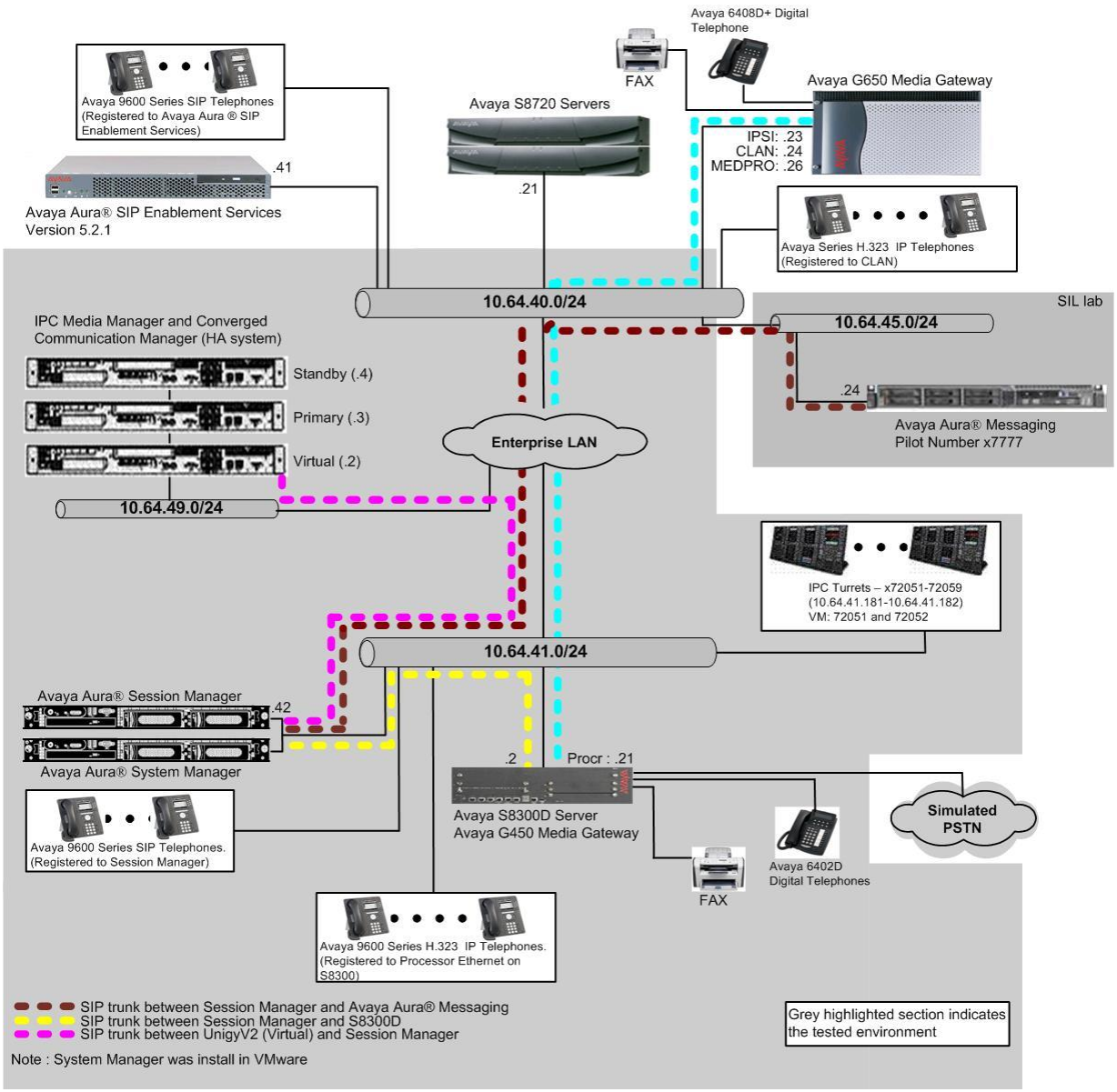


Figure 1: Test Configuration of IPC Unigy V2.0.1 with Avaya Aura® Messaging

4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Messaging	MSG-03.0.124.0-321_0103
Avaya Aura® Communication Manager on Avaya S8300D Server	6.3.7 (R016x.03.0.124-21754)
Avaya Aura® Session Manager	6.3.9.0.639011
Avaya Aura® System Manager	6.3.9.1.2482
Avaya 96xx IP Telephone (H.323)	3.1
Avaya 96x1 IP Telephone (H.323)	6.23
Avaya 96xx IP Telephone (SIP)	2.6.9.1
Avaya 96x1 IP Telephone (SIP)	6.3
IPC Unigy V2.0.1 • Media Manager • Converged Communication Manager • Turrets	 02.00.01.02.0045 02.00.01.02.0045 02.00.01.02.0045

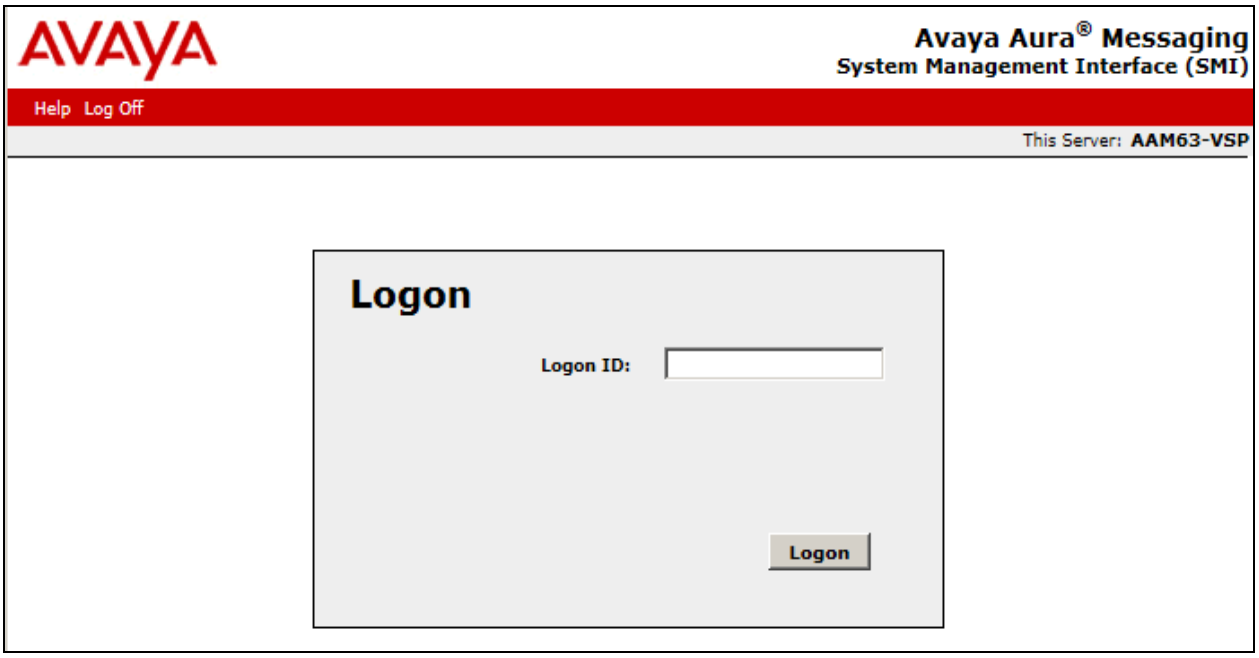
5. Configure Avaya Aura® Messaging

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

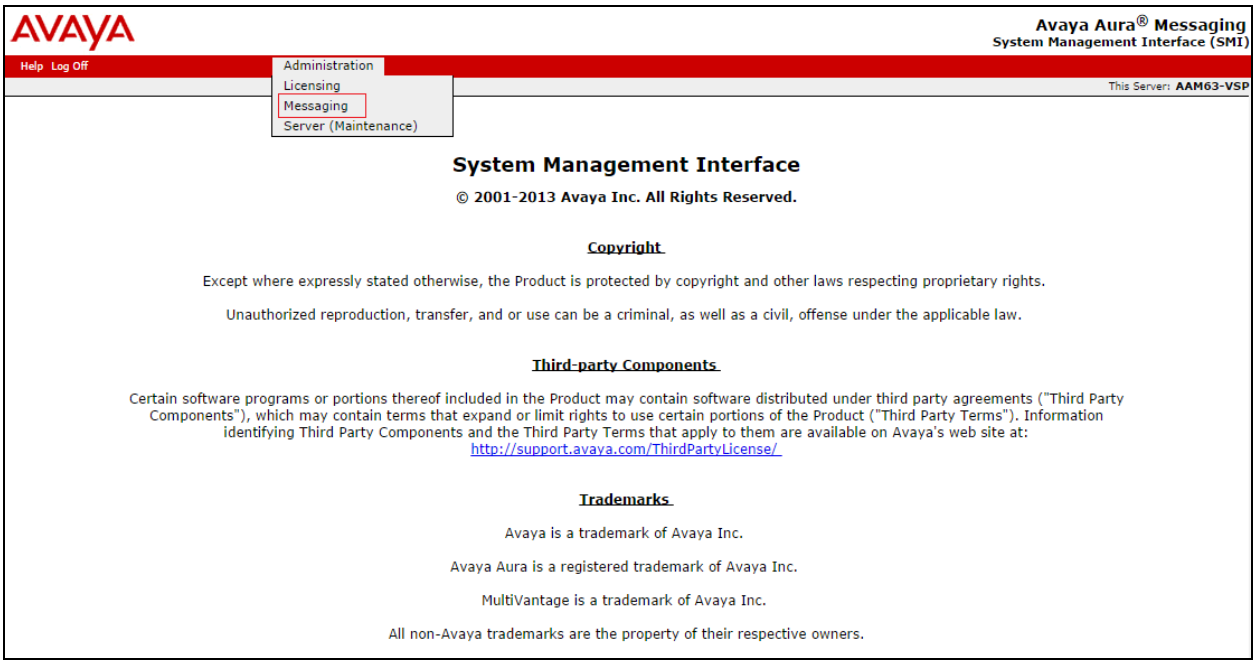
- Launch messaging administration
- Administer subscriber extension ranges
- Administer subscribers

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.

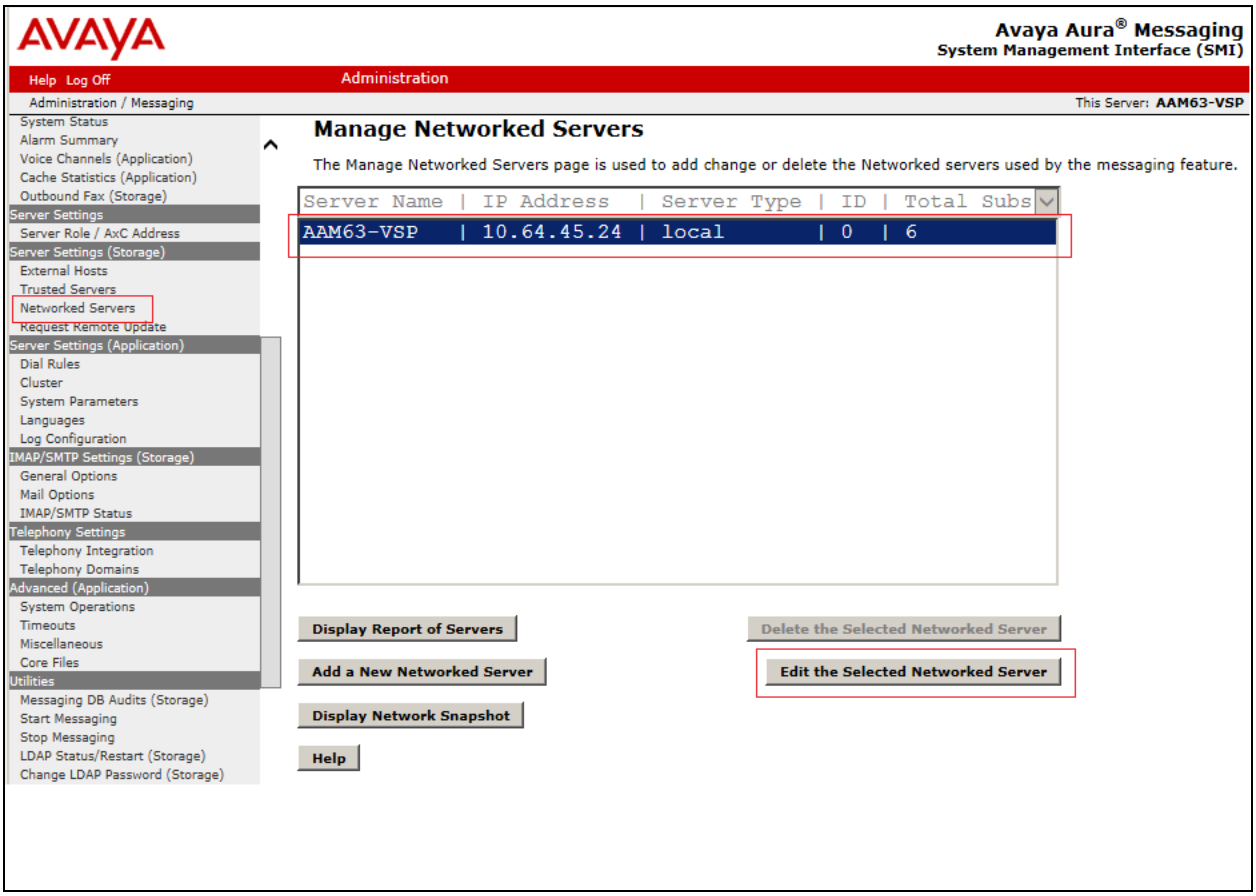


The **Messaging Administration** screen appears, as shown below. Navigate to **Administration → Messaging**.



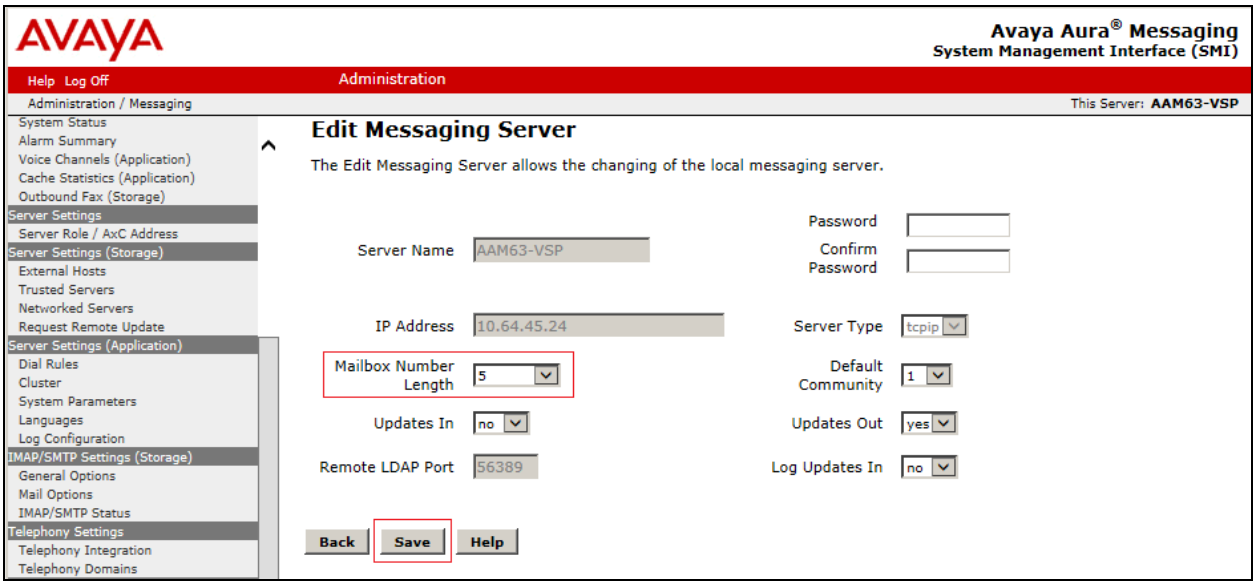
5.2. Administer Subscriber Extension Ranges

On the Messaging Administration page (not shown) 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.



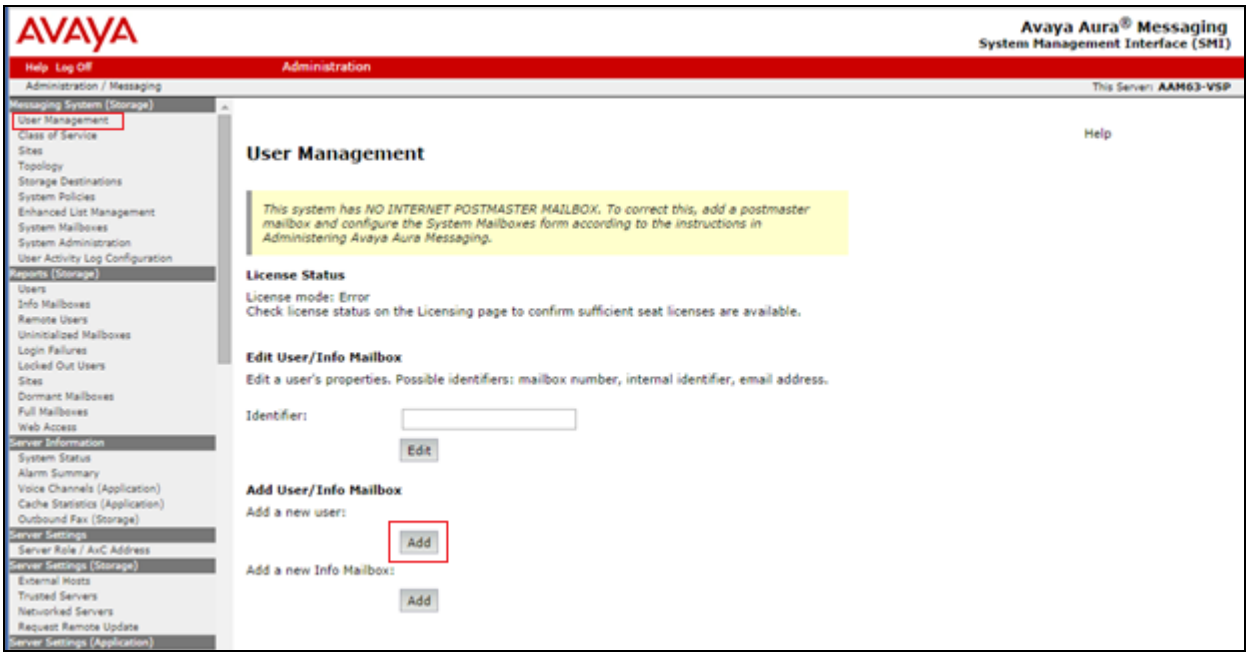
The **Edit Messaging Server** screen is displayed. Select **5** using drop-down menu on the Mailbox Number Length field. In the compliance test, the 5 digit extensions were used by Avaya Aura® Messaging.

Click on **Save** at the bottom of the screen.



5.3. Administer Subscribers

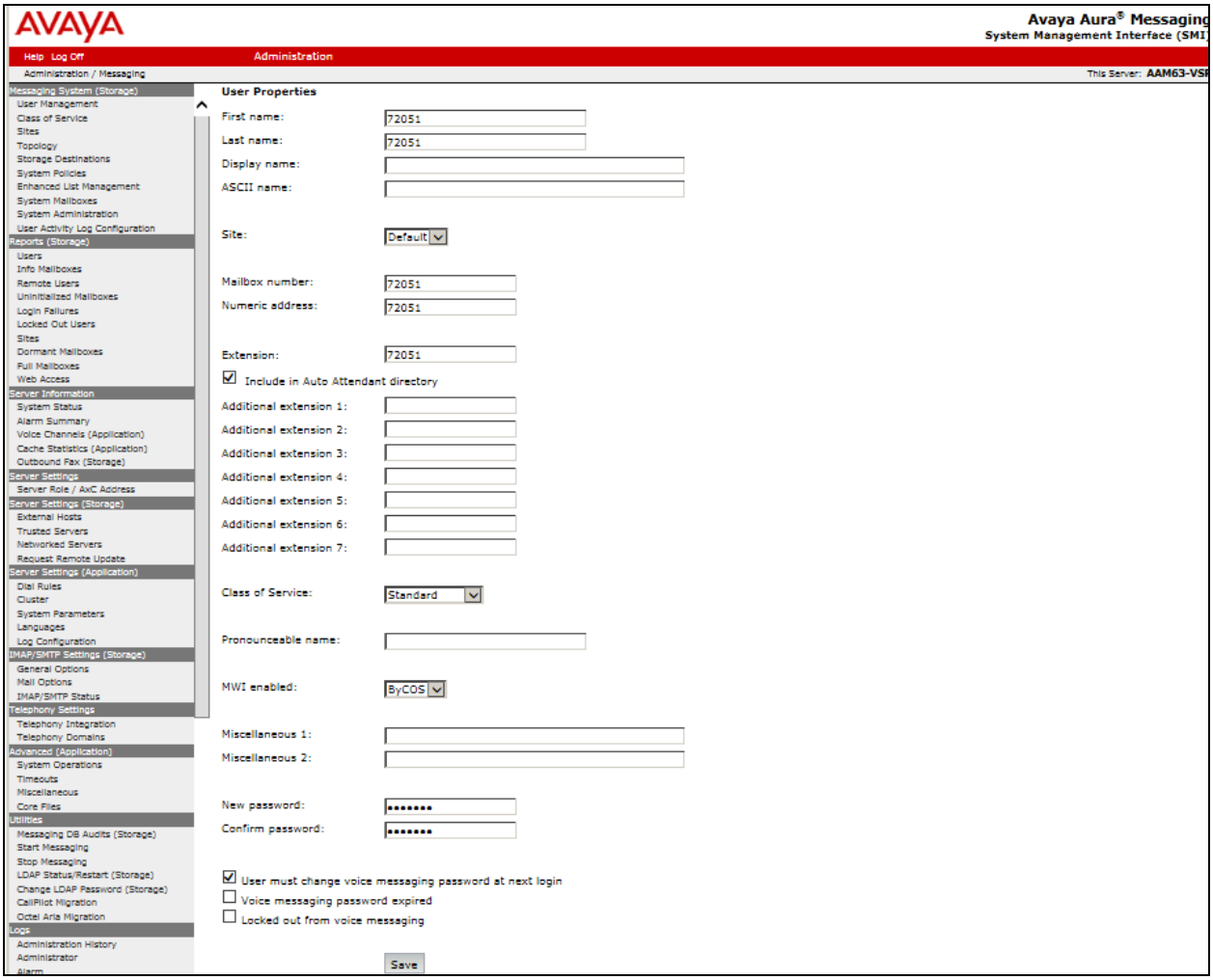
Select **Messaging System (Storage) → User Management** from the left pane, to display the **User Management** screen. Click **Add** under the **Add a new user** section.



The **User Management > Properties for New User** screen is displayed next. Enter the desired string into the **First Name**, **Last 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 **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, 72051 and 72052 were used.

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. Prior to the solution test, the following sections were already configured, and not discussed in these application Notes.

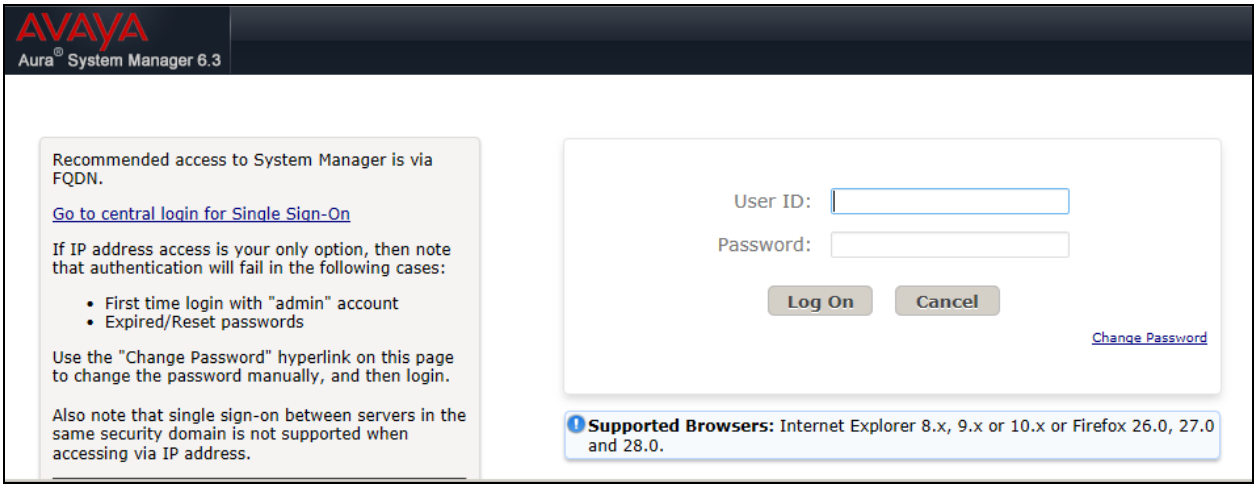
- Domain
- SIP Entities
- Entity Links
- Routing Policy

The discussed procedures include the following areas:

- Launch System Manager
- Administer dial patterns

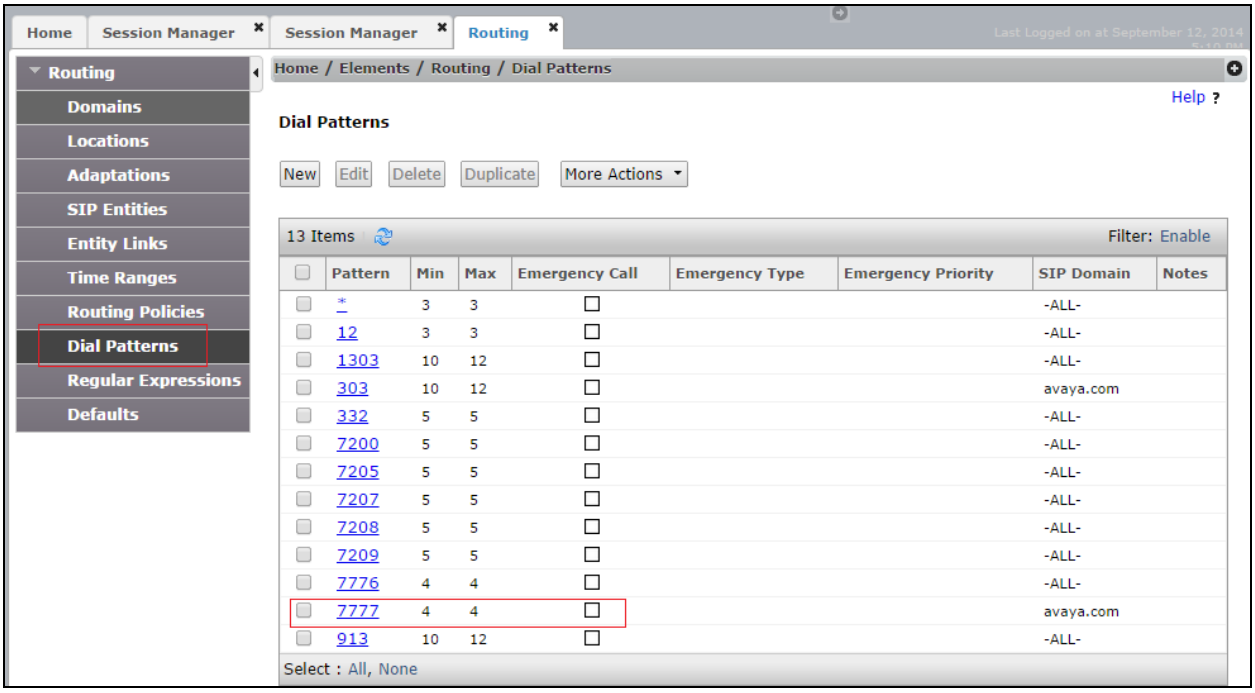
6.1. Launch System Manager

Access the System Manager web interface by using the URL http://<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.

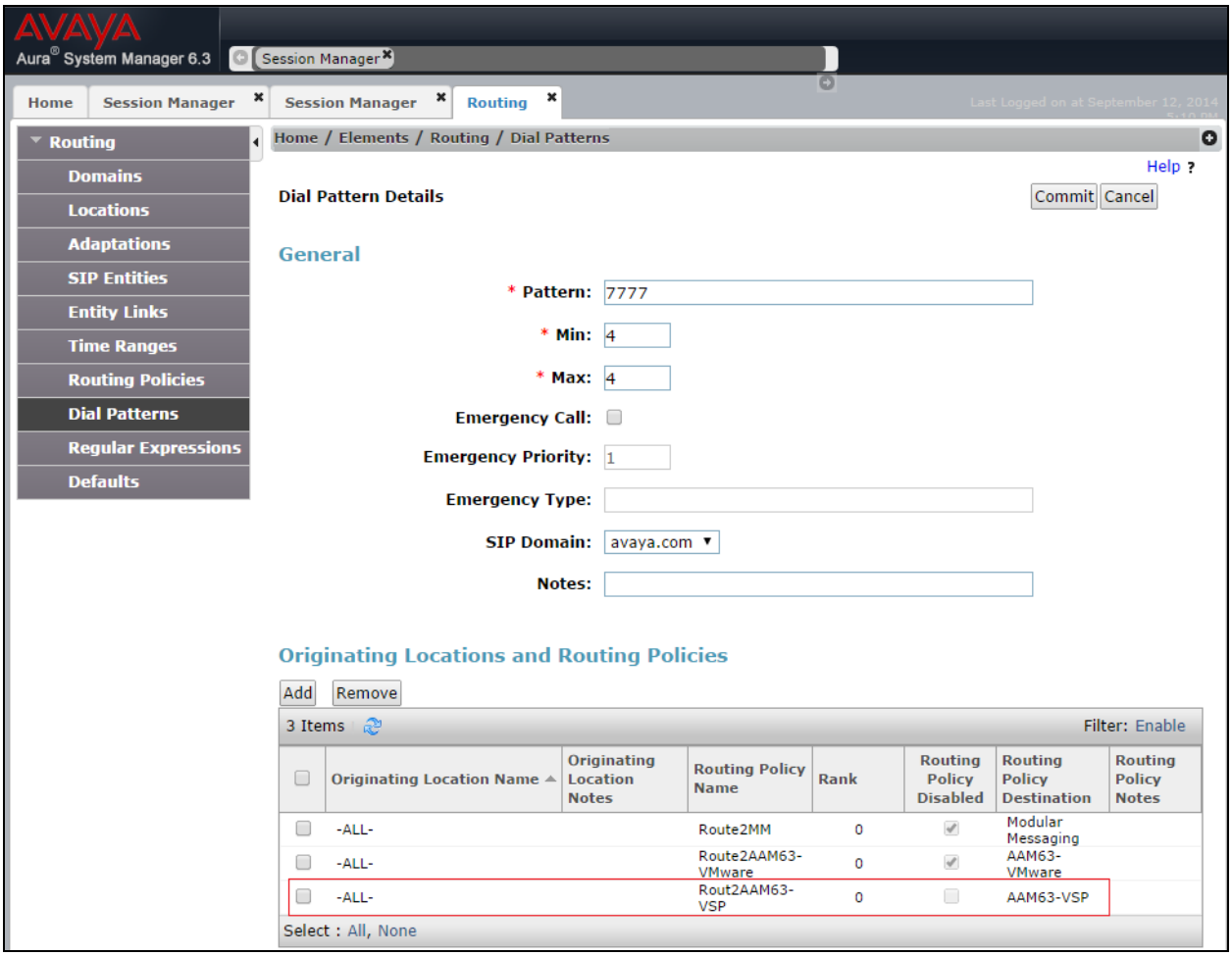


6.2. Administer Dial Patterns

In the subsequent screen (not shown), select **Home →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 Avaya Aura® Messaging pilot number, in this case "7777". The pilot number was configured prior to this solution test, and the following screen shows only for information purpose.

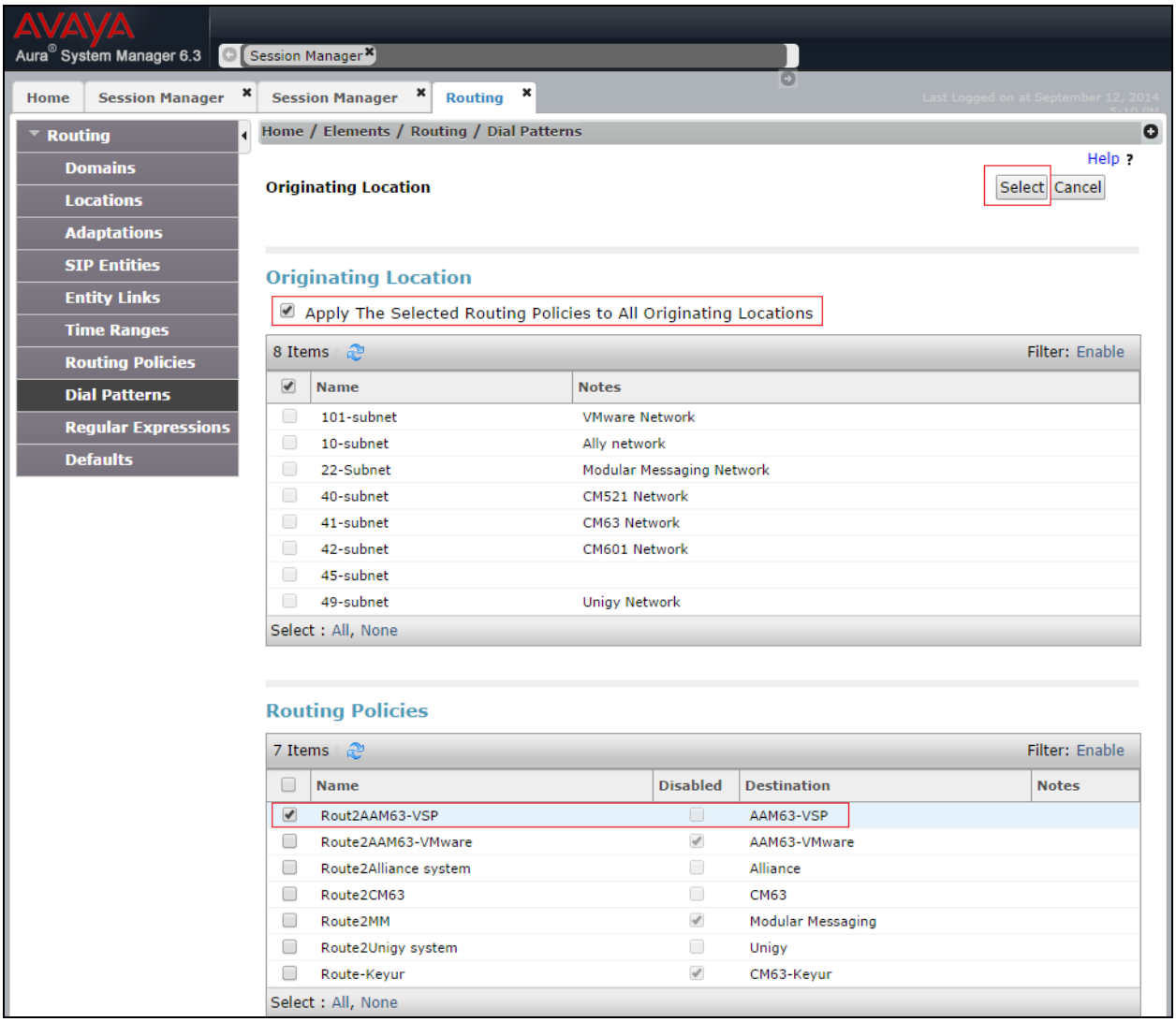


The **Dial Pattern Details** screen is displayed. In the **Originating Locations and Routing Policies** sub-section, add or modify the entry as desired to allow IPC turret users to reach Avaya Aura® Messaging. In the compliance testing, a new entry was created to allow for call origination from the existing IPC location, as shown below.



The following screen displays how to add **Originating Locations and Routing Policies**. During the compliance test, check the checkbox for **Apply The Selected Routing Policies to All Originating Locations**. For Routing Policy, check the checkbox for the **Rout2 AAM63-VSP**.

Click **Select**.



There should be dial patterns for three routing policies:

- Route 2 Unigy system
- Route2CM63
- Rout2AAM63-VSP (included in this section)

Configure other dial patterns for two routing policies using above procedures.

7. Configure IPC Unigy V2.0.1 Converged Communication Manager

This section provides the procedures for configuring IPC Unigy V2.0.1 Converged Communication Manager. The procedures include the following areas:

- Launch Unigy V2.0.1 Management System
- Administer SIP trunks
- Administer trunk groups
- Administer route lists
- Administer dial patterns
- Administer route plans

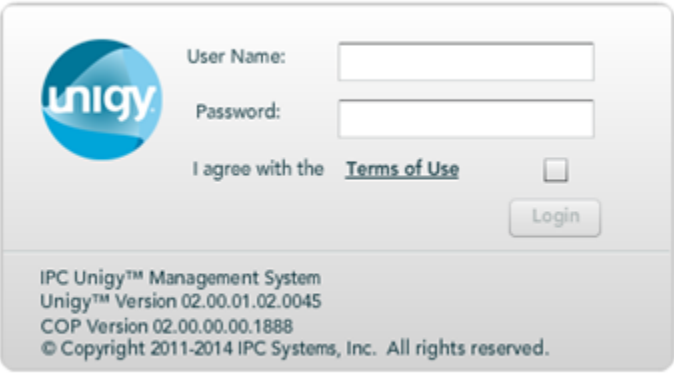
The configuration of Converged Communication Manager is typically performed by IPC installation technicians. The procedural steps are presented in these Application Notes for informational purposes.

7.1. Launch Unigy V2.0.1 Management System

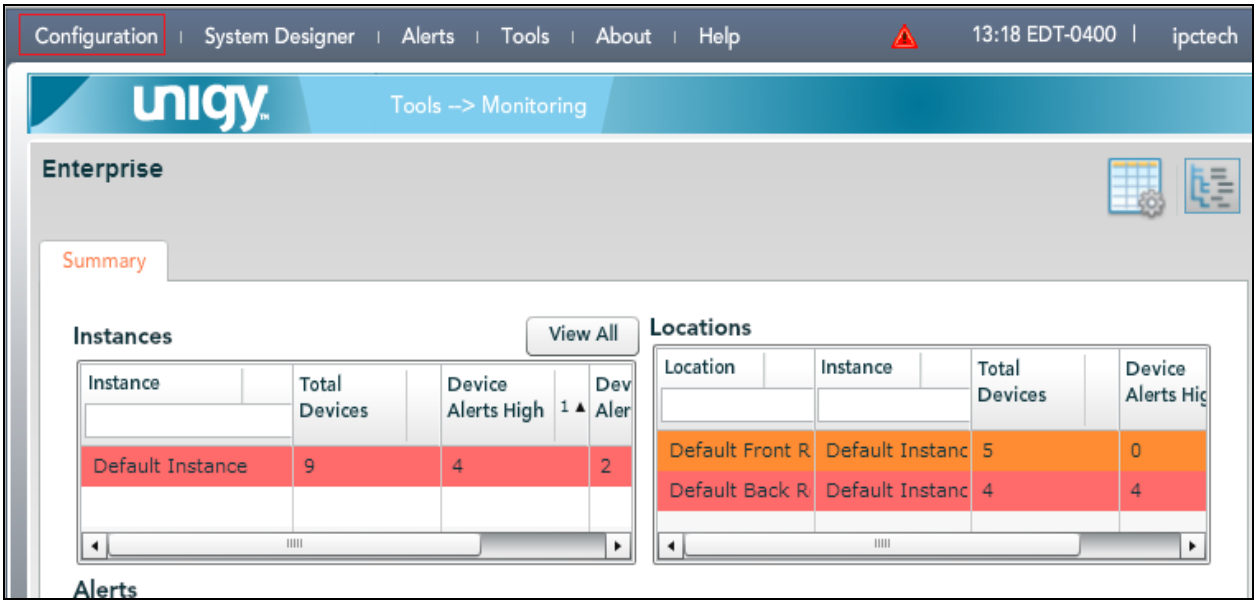
Access the UnigyV2.0.1 Management System web interface by using the URL "http://ip-address" in an Internet browser window, where "ip-address" is the IP address of VIP. Log in using the appropriate credentials.

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**.

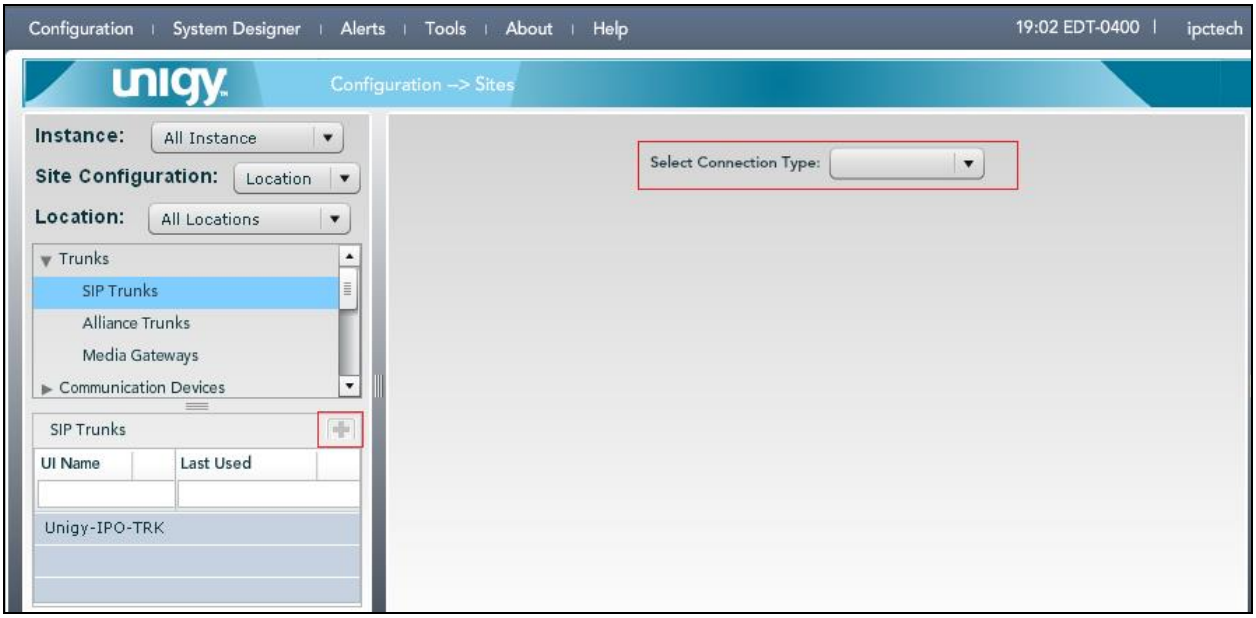


The following screen (Tools -> Monitoring) displays. Navigate to **Configuration → Site**.



7.2. Administer SIP Trunks

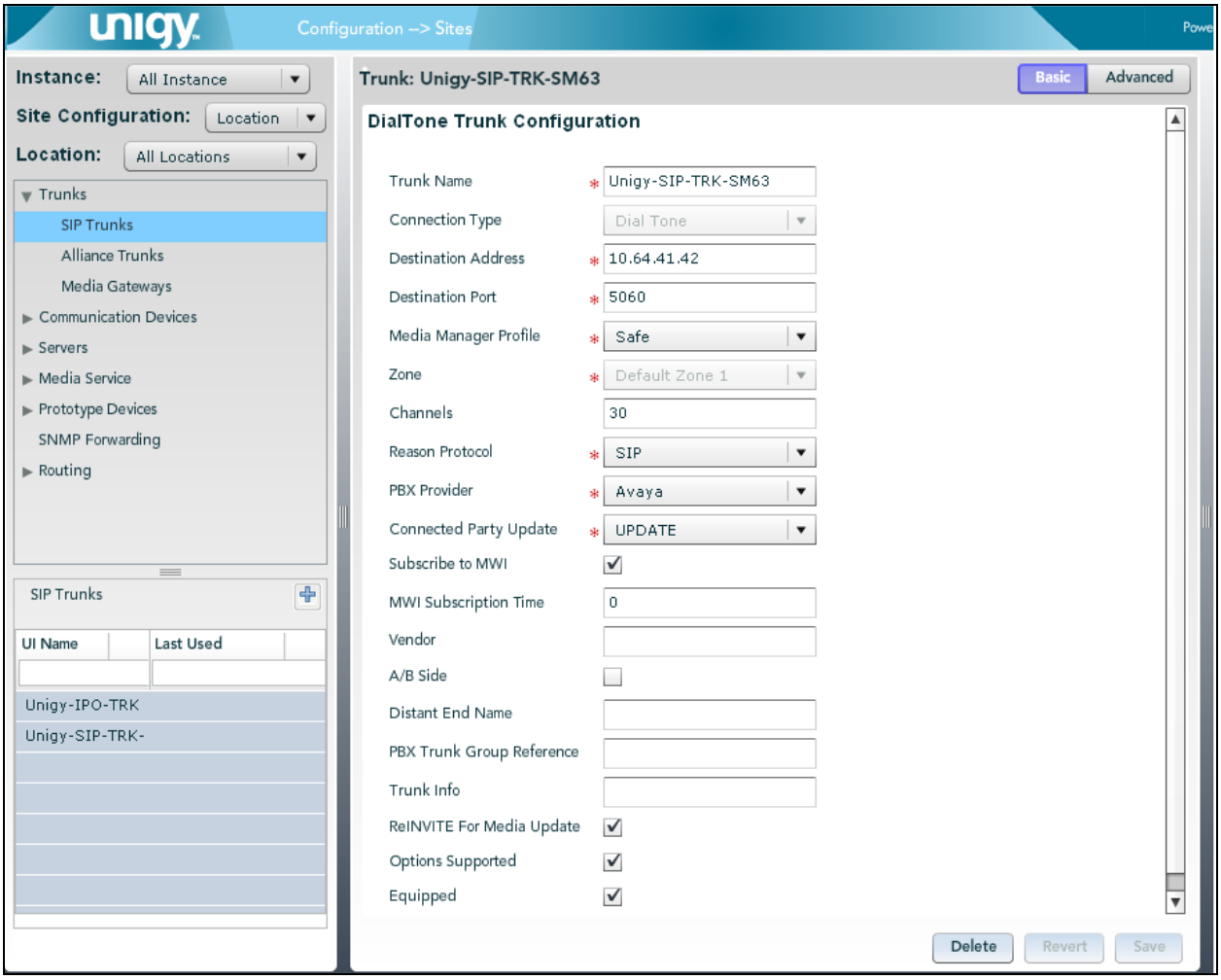
Select **Trunks → SIP Trunks** in the left pane, and click the **Add** icon ( ) in the lower left pane to add a new SIP trunk. Select "Dial Tone" from the **Select Connection Type** drop-down list.



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"

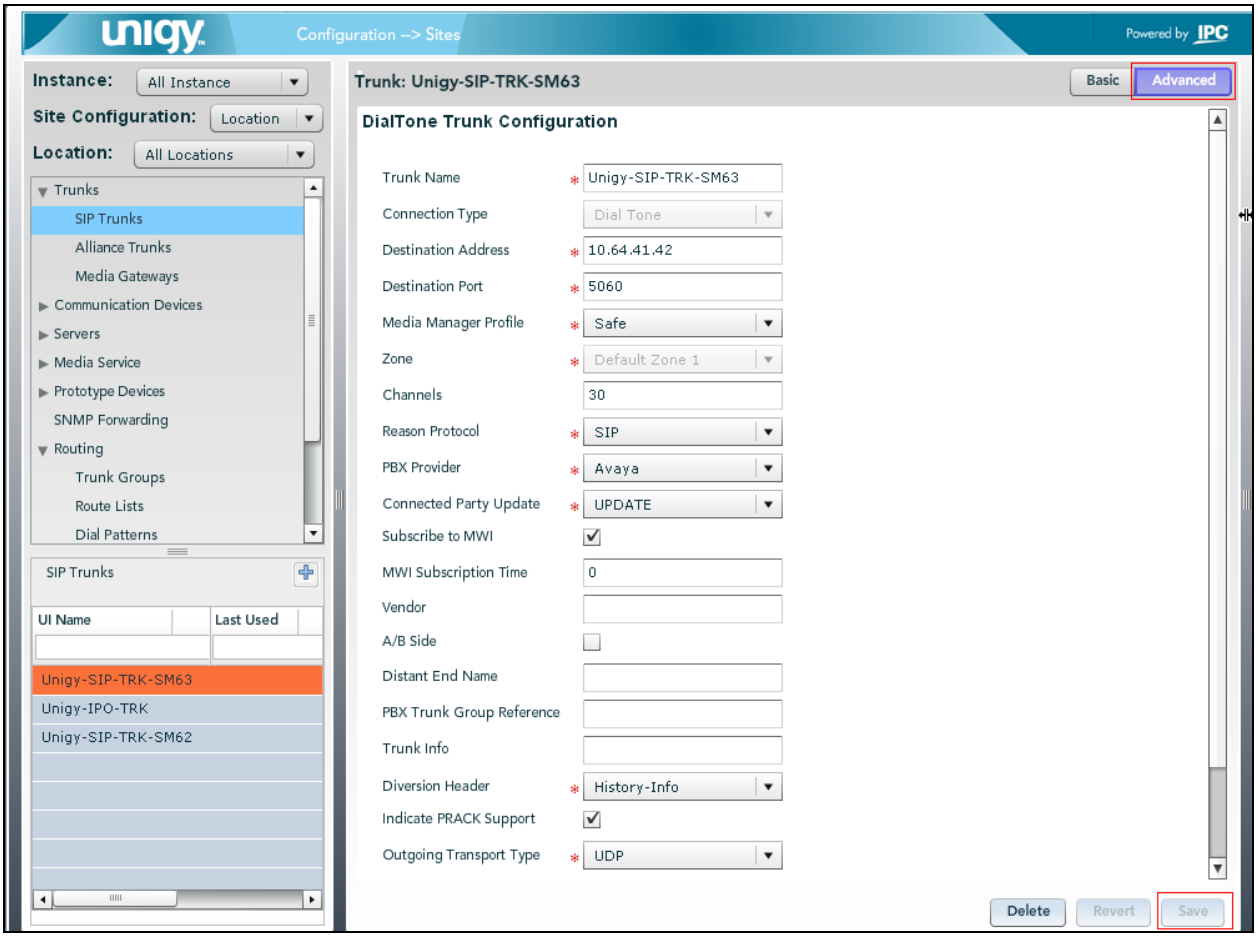
Retain the default values in the remaining fields.



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

- **Diversion Header:** Select “History-Info”.
- **Outgoing Transport Type:** Select “UDP”.

Click the **Save** button at the bottom of this page.



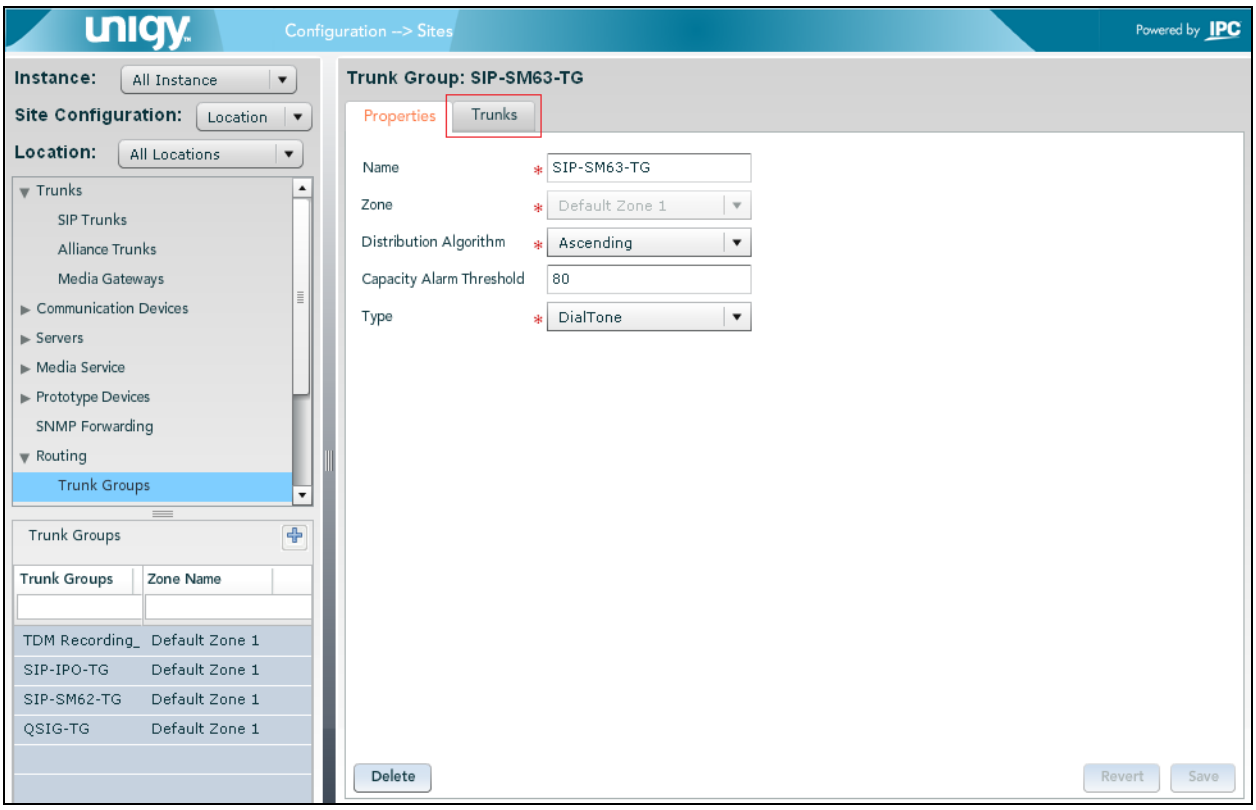
7.3. Administer Trunk Groups

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** (default) tab, enter a descriptive **Name**, select "Default Zone 1" for the **Zone** field, and select "Ascending" for the **Distribution Algorithm** field.

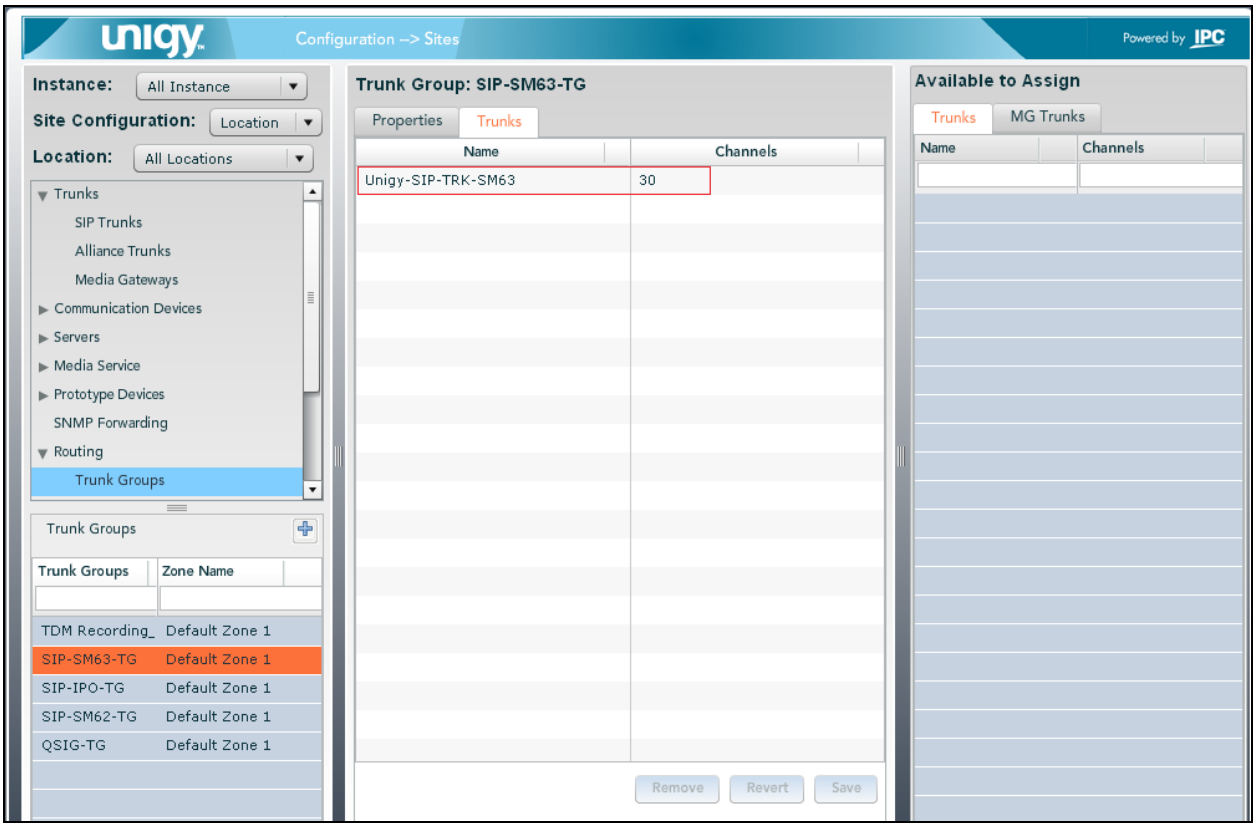
Click **Save**.

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 7.2** in the rightmost pane and drag to the middle pane as shown below.

Click **Save**.

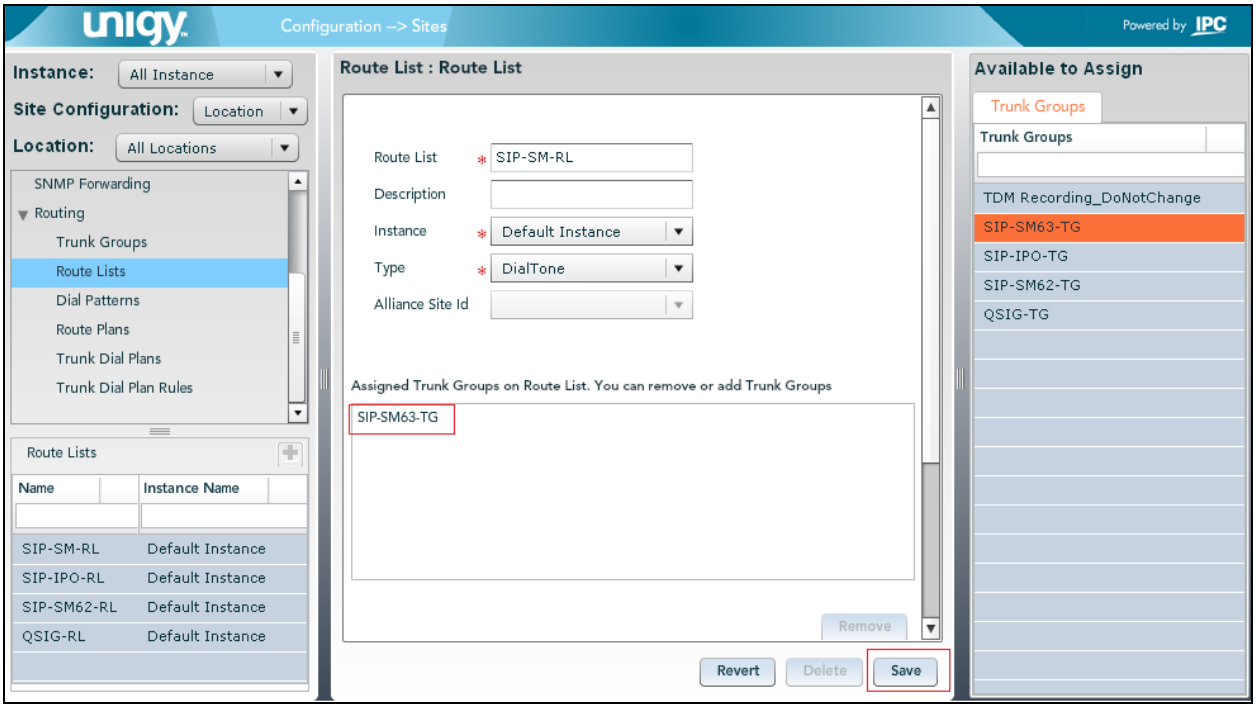


7.4. Administer Route Lists

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 7.3** and drag into the **Assigned Trunk Groups on Route List** sub-section in the middle pane, as shown below.

Click **Save**.



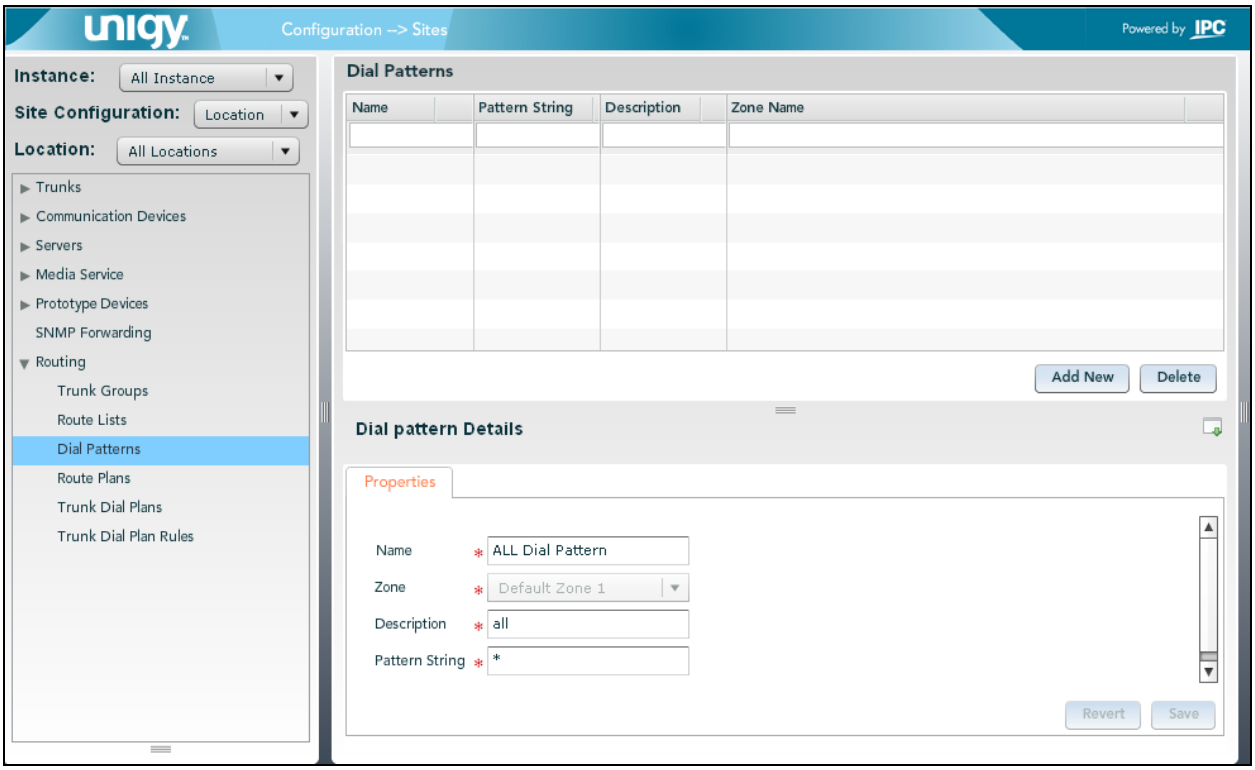
7.5. Administer Dial Patterns

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.



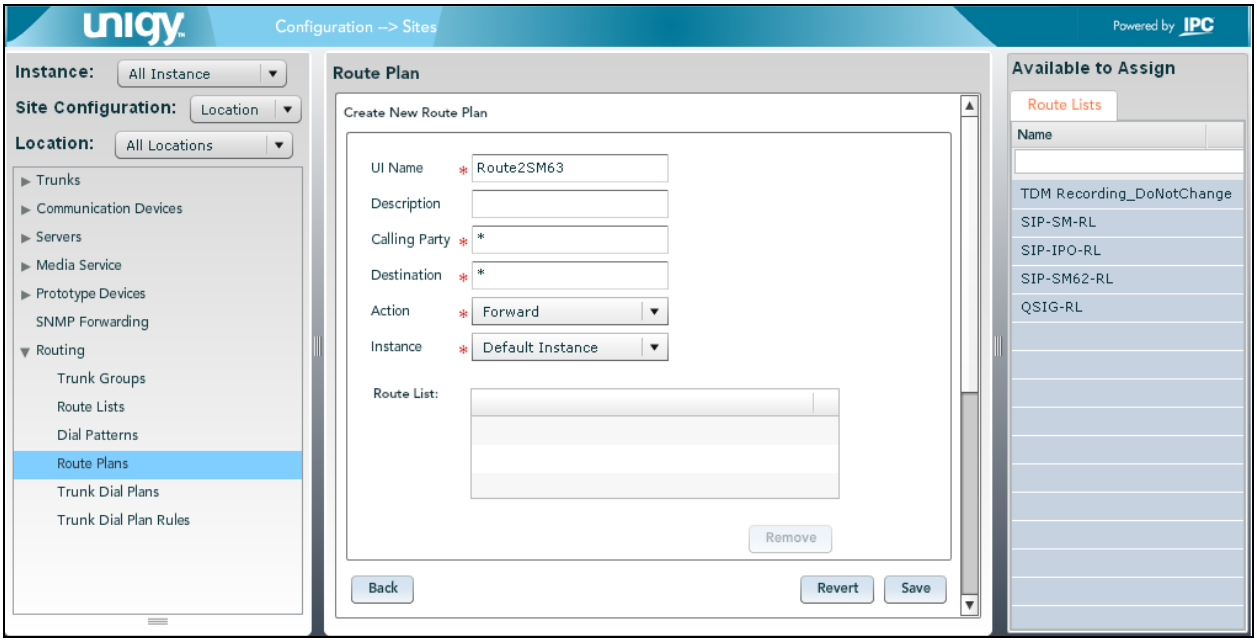
Repeat this section to add another dial pattern to reach the PSTN, and include any required prefix by Communication Manager.

7.6. Administer Route Plans

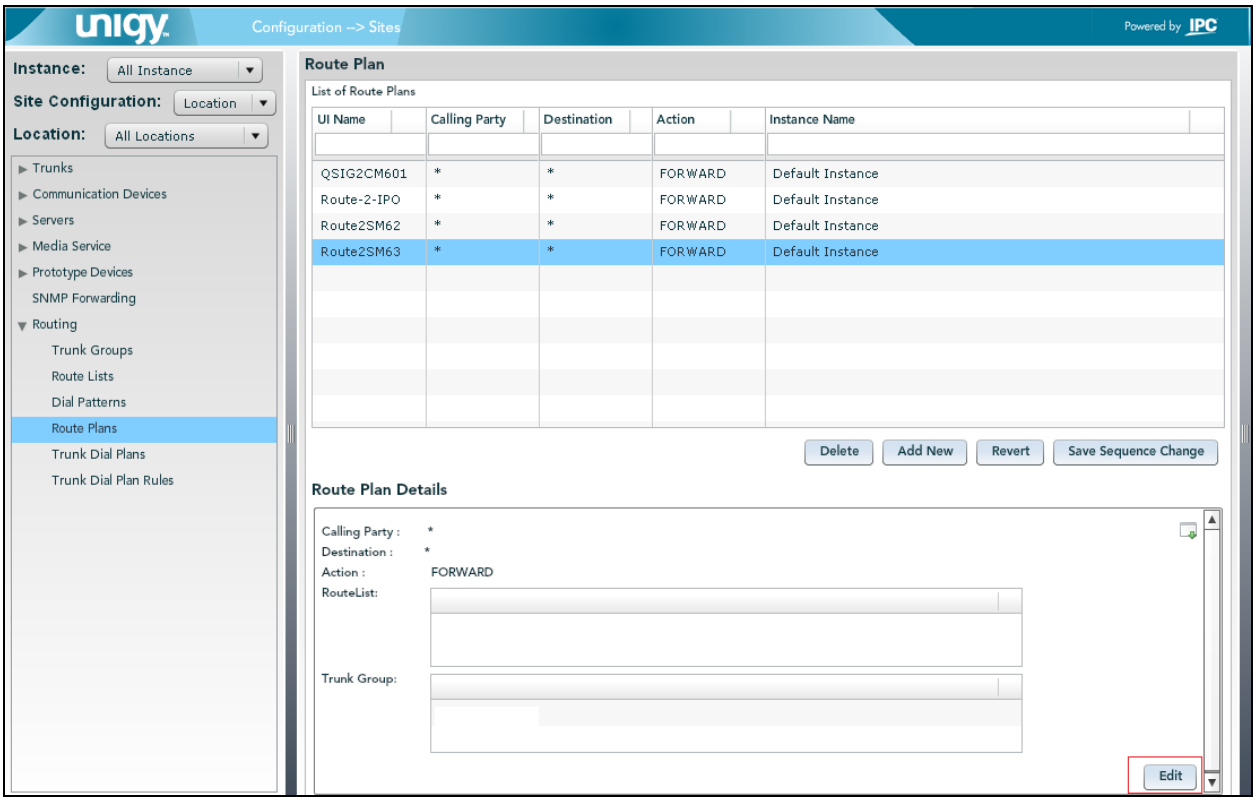
Select **Routing → Route Plans** in the left pane, and click **Add New** (not shown) in the right pane to create a new route plan.

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 UnigyV2.0.1. For **Called Party**, select the dial pattern for Avaya endpoints from **Section 7.5**. Select "Forward" for **Action**.

Click **Save**.

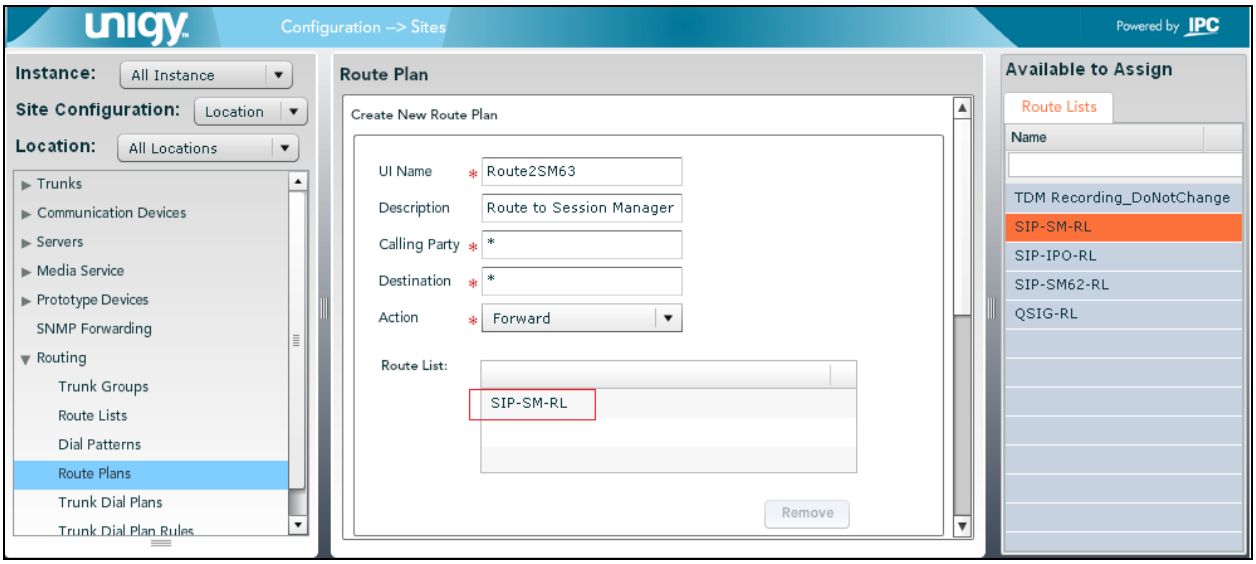


The screen is updated with the newly created route plan. Select the route plan, and click **Edit** toward the bottom of the screen.



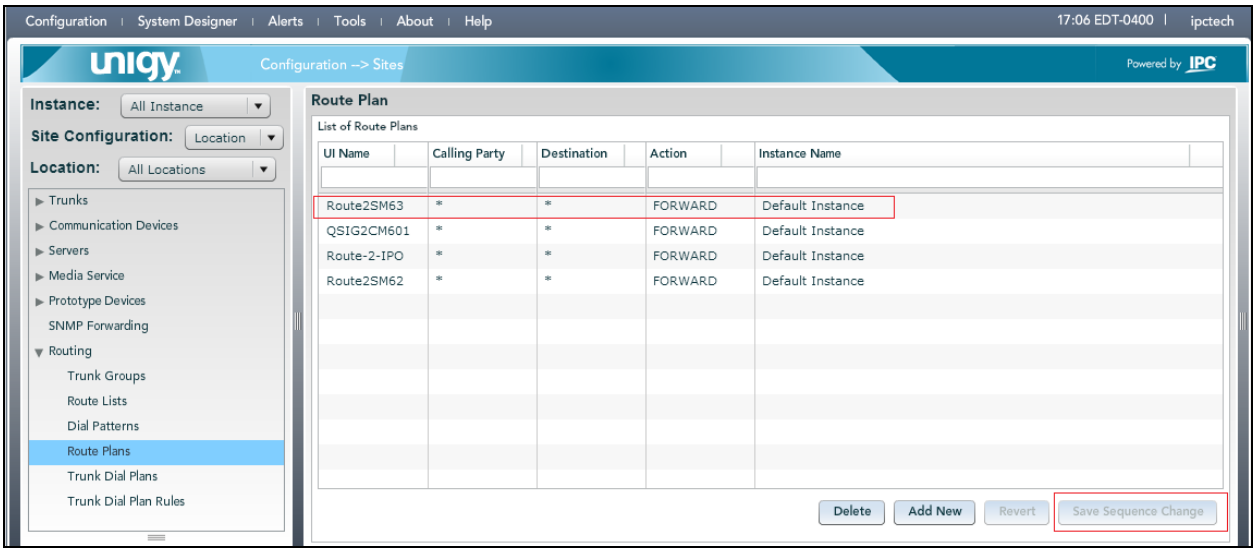
The screen is updated with three panes again, as shown below. In the right pane, select the route list from **Section 7.4** and drag into the **Route List** sub-section in the middle pane, as shown below.

Click **Save** (not shown).



Once the route plan configuration is completed, again select **Routing → Route Plans** in the left pane. List of route plans is displayed. Drag the latest route plan you've created, to the top.

Click the **Save Sequence Change** button to finish the Unigy V2.0.1 configuration.



8. Verification Steps

This section provides tests that may be performed to verify proper configuration of Communication Manager, Session Manager and IPC UnigyV2.0.1.

8.1. 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.

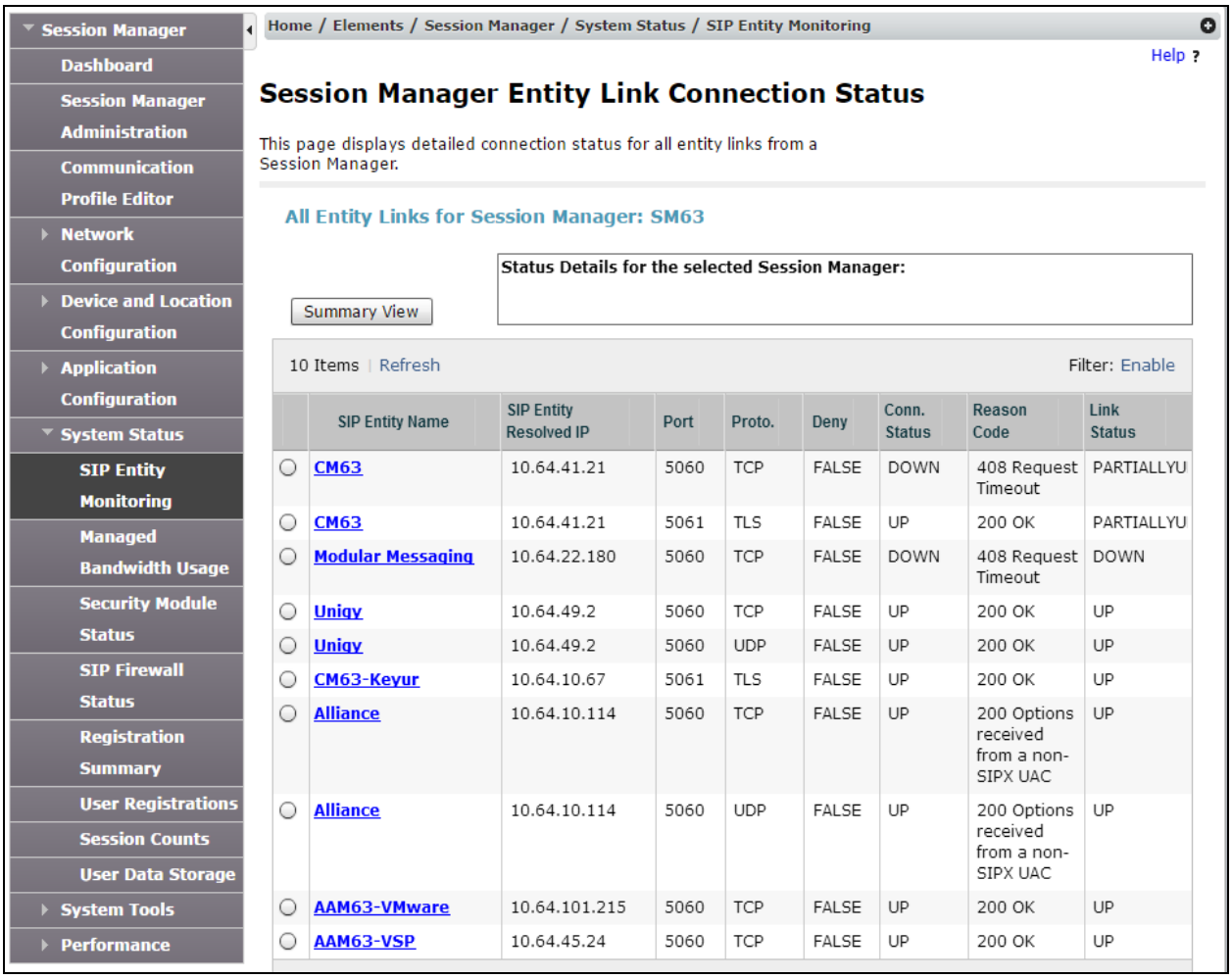
```
status signaling-group 92
                         STATUS SIGNALING GROUP

        Group ID: 92
      Group Type: sip

     Group State: in-service
```

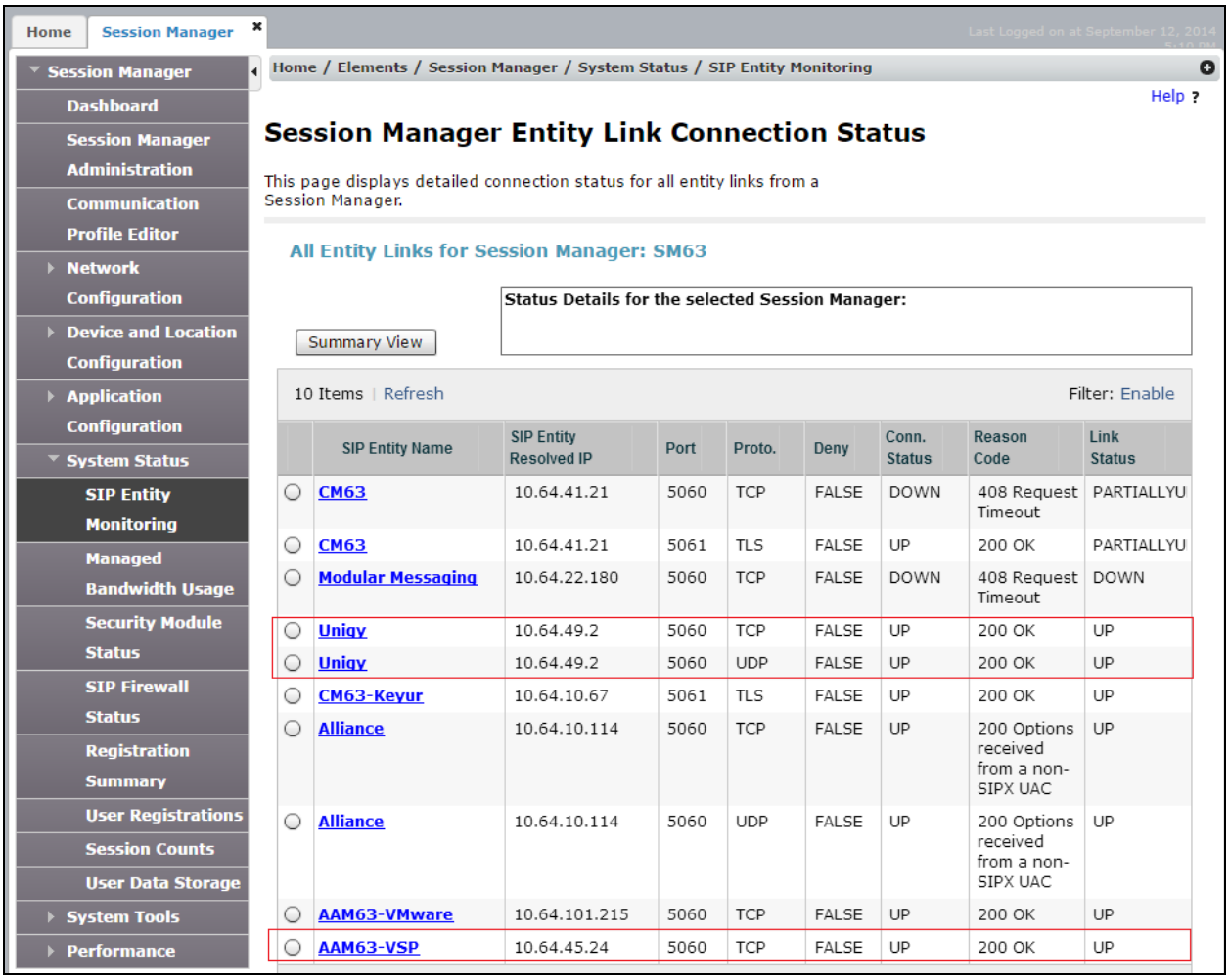
8.2. Verify Avaya Aura® Session Manager

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.



SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
CM63	10.64.41.21	5060	TCP	FALSE	DOWN	408 Request Timeout	PARTIALLYU
CM63	10.64.41.21	5061	TLS	FALSE	UP	200 OK	PARTIALLYU
Modular Messaging	10.64.22.180	5060	TCP	FALSE	DOWN	408 Request Timeout	DOWN
Uniqy	10.64.49.2	5060	TCP	FALSE	UP	200 OK	UP
Uniqy	10.64.49.2	5060	UDP	FALSE	UP	200 OK	UP
CM63-Keyur	10.64.10.67	5061	TLS	FALSE	UP	200 OK	UP
Alliance	10.64.10.114	5060	TCP	FALSE	UP	200 Options received from a non-SIPX UAC	UP
Alliance	10.64.10.114	5060	UDP	FALSE	UP	200 Options received from a non-SIPX UAC	UP
AAM63-VMware	10.64.101.215	5060	TCP	FALSE	UP	200 OK	UP
AAM63-VSP	10.64.45.24	5060	TCP	FALSE	UP	200 OK	UP

Click on the entity names, **Unigy** and **AAM63-VSP**, and verify that **Conn. Status** and **Link Status** are "UP", as shown below.



SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
CM63	10.64.41.21	5060	TCP	FALSE	DOWN	408 Request Timeout	PARTIALLYU
CM63	10.64.41.21	5061	TLS	FALSE	UP	200 OK	PARTIALLYU
Modular Messaging	10.64.22.180	5060	TCP	FALSE	DOWN	408 Request Timeout	DOWN
Unigy	10.64.49.2	5060	TCP	FALSE	UP	200 OK	UP
Unigy	10.64.49.2	5060	UDP	FALSE	UP	200 OK	UP
CM63-Keyur	10.64.10.67	5061	TLS	FALSE	UP	200 OK	UP
Alliance	10.64.10.114	5060	TCP	FALSE	UP	200 Options received from a non-SIPX UAC	UP
Alliance	10.64.10.114	5060	UDP	FALSE	UP	200 Options received from a non-SIPX UAC	UP
AAM63-VMware	10.64.101.215	5060	TCP	FALSE	UP	200 OK	UP
AAM63-VSP	10.64.45.24	5060	TCP	FALSE	UP	200 OK	UP

8.3. Verify IPC Unigy V2.0.1

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.

9. Conclusion

These Application Notes describe the configuration steps required for IPC Unigy V2.0.1 to successfully interoperate with Avaya Aura® Messaging 6.3 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, June 2014, Issue 10,Document Number 03-300509

[2] *Administering Avaya Aura® Session Manager*, Release 6.3, August 2014, Issue 6.

[3] *Administering Avaya Aura® System Manager*, Release 6.3.9, August 2014.

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.

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.