



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the Varaha Systems uMobility Fixed-Mobile Convergence Solution with an Avaya Aura™ Telephony Infrastructure - Issue 1.0

Abstract

These Application Notes describe a compliance-tested configuration comprised of the Varaha Systems uMobility Fixed-Mobile Convergence (FMC) Solution connected to an Avaya telephony infrastructure using Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services. The Varaha Systems uMobility Solution integrates mobile devices with existing Private Branch Exchanges (PBXs) so that the PBX sees the mobile device as another desk phone and allows roaming seamlessly to and from WiFi to mobile networks.

Information in these Application Notes has been obtained through 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 a compliance-tested configuration comprised of the Varaha Systems uMobility FMC Solution connected to an Avaya telephony infrastructure using Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services. The Varaha Systems uMobility Solution fuses WLAN, Cellular and IP Private Branch Exchanges (PBXs) technology in order to extend enterprise PBX functionality to mobile devices. This allows end users to be accessible when out of the office as well as to leverage WLAN networks to improve wireless coverage and reduce costs. The Varaha uMobility Solution integrates mobile devices with existing Private Branch Exchanges (PBXs) so that the PBX sees the mobile device as another desk phone. This allows the existing PBX feature set to be applied consistently across both devices. Mobile specific functionality is then layered on top.

The Varaha Systems uMobility Solution transparently handles all mobile call originations from a user's mobile device and redirects them through the enterprise leveraging the WLAN network when available or routing over cellular when outside of WLAN coverage areas. This allows calls made from a mobile device to receive the same originating services (e.g., Abbreviated Dialing, Class of Service, Accounting, etc.) as a desk phone.

1.1. Interoperability Compliance Testing

Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab. Compliance testing verified the integration between Varaha Systems uMobility Solution and an Avaya telephony infrastructure and the ability for an enterprise user to be accessible via one business number whether the user is in the office or mobile.

The telephony features verified to operate correctly included Single Number Reach (SNR), Enterprise Dialing (ED), Handoff (HO), transfer (WiFi), conference call participation, conference call add/drop, multiple call appearances, caller ID operation, call forwarding unconditional, call forwarding on busy, call park (WiFi), call pick-up (WiFi), bridged call appearances (WiFi), voicemail using Avaya Modular Messaging and Avaya IA770 INTUITY AUDIX, Message Waiting Indicator (MWI) (WiFi), and hold and return from hold.

Serviceability testing was conducted to verify the ability of the Avaya/Varaha solution to recover from adverse conditions, such as power cycling network devices and disconnecting cables between the LAN interfaces. In all cases, the ability to recover after the network normalized from failures was verified.

1.2. Support

For technical support on Varaha products, consult the support pages at:

<http://www.varaha.com/support.php>

2. Reference Configuration

The configuration in **Figure 1** shows a single site converged VoIP and data network with multiple closets and labs configured with link aggregation, rapid spanning tree, load balancing and OSPF.

For compliance testing, a centralized corporate DHCP server was used. To better manage the different traffic types, the voice and data traffic were separated onto different VLANs.

2.1. Test Environment

The test environment consisted of an Avaya Aura™ Communication Manager running on an Avaya S8300 Server with an Avaya G450 Media Gateway, one Avaya Aura™ SIP Enablement Services server, one Avaya Modular Messaging Application Server, one Avaya Modular Messaging Storage Server, one Avaya 2400 Series Digital Telephone, one Avaya 9630 IP Telephone running Avaya one-X™ Deskphone SIP, one Varaha Systems uMobility Controller, two dual mode cell phones running Varaha Systems uMobility Client, one WiFi controller and access point and one DHCP/File Server.

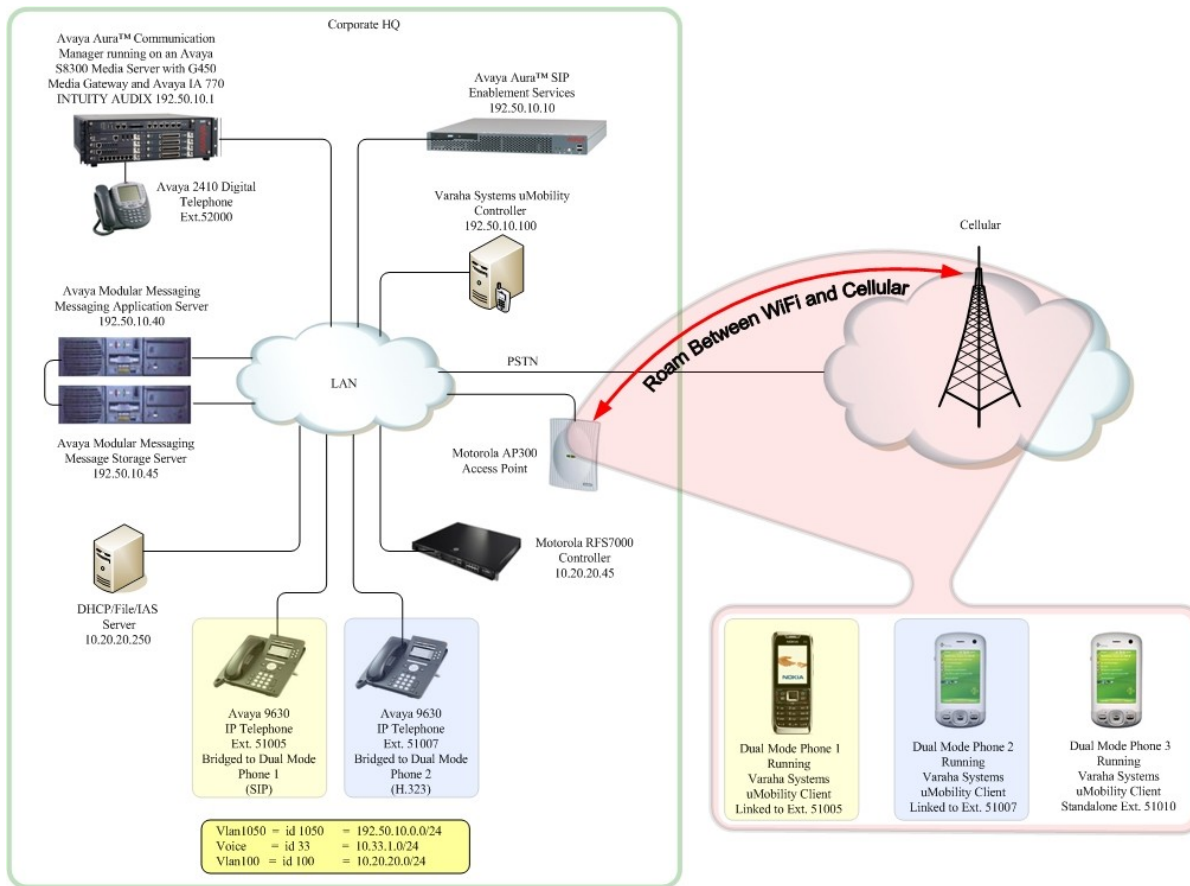


Figure 1: Network Diagram

3. Equipment and Software Validated

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

Equipment	Software/Firmware
<i>Avaya PBX Products</i>	
Avaya S8300 Server running Avaya Aura™ Communication Manager	Avaya Aura™ Communication Manager 5.2
Avaya G450 Media Gateway (Corporate Site) MGP MM712 DCP Media Module Avaya IA 770 INTUITY AUDIX	28.22.0 HW9 5.2
<i>Avaya SIP Enablement Services (SES)</i>	
Avaya Aura™ SIP Enabled Services (SES) Server	5.2 SP2
<i>Avaya Messaging (Voice Mail) Products</i>	
Avaya Modular Messaging - Messaging Application Server (MAS)	5.0
Avaya Modular Messaging - Message Storage Server (MSS)	5.0
Avaya IA 770 INTUITY AUDIX	5.1
<i>Avaya Telephony Sets</i>	
Avaya 9600 Series IP Telephones	Avaya one-X Deskphone Edition 3.0.1
Avaya 9600 Series IP Telephones	Avaya one-X Deskphone SIP 2.4
Avaya 2410 Digital Telephone	5.0
<i>Varaha Systems Products</i>	
Varaha Systems uMobility Controller	3.2.21
Varaha Systems uMobility Client (WM)	3.2
Varaha Systems uMobility Client (Symbian)	3.1
<i>MS Products</i>	
Microsoft Windows 2003 Server	File/DHCP Service
<i>Dual mode CELL/WiFi phones</i>	
Nokia E51	S60 3 rd edition1 FP1
HTC-P3600 (ROM - 3.00.707.18)	Windows Mobile 6 (CE OS 5.2.1437)

4. Configure Avaya Aura™ Communication Manager

This section describes the steps required for Communication Manager to support the configuration shown in **Figure 1**. The assumption is that the appropriate license and authentication files have been installed on the servers and that login and password credentials are available. It is assumed the Communication Manager and SES are configured; please consult references 1 thru 4 in Section 10.

4.1. Configure Station and Off-PBX Telephone Information

There are differences in the way Avaya SIP and H.323 endpoints are configured for the Varaha Systems uMobility FMC Solution. Every uMobility user must have a SIP user on SES as well as be defined as an off-PBX station in order to enable simultaneous ringing.

4.2. Configure Station Information for H.323 Desktop

There are no special settings for H.323 endpoint to be used, so no configuration will be shown. Reference Section 10 [1] thru [4] for more information on station configuration.

4.3. Configure Station Information for SIP Desktop

This step is required if the Avaya IP Telephone is a SIP station. Because SES will only allow one SIP endpoint to register at a time, another station ID needs to be created. To keep the button appearance consistent on both the uMobility handset and the Avaya SIP desktop, the uMobility endpoint will login into SES as the primary phone number and the Avaya IP telephone (SIP) will login using the secondary phone number. For this example, station 51005 is the primary number and 53005 is the secondary number. There are no special settings for station 51005 so the configuration will not be shown. Reference Section 10 [1] thru [4] for more information on station configuration.

Step	Description
1.	<p>Enter change station 53005, Enter the following information:</p> <ul style="list-style-type: none"> • Station Extension = 53005 • Type = 9630 • Name = User Name • Message Lamp Ext: = 51005 <p>Go to page 4 to continue:</p> <pre> change station 53005 Page 1 of 6 STATION Extension: 53005 Lock Messages? n BCC: 0 Type: 9620 Security Code: 123456 TN: 1 Port: S00014 Coverage Path 1: 99 COR: 1 Name: User Name Coverage Path 2: COS: 1 Hunt-to Station: STATION OPTIONS Time of Day Lock Table: Personalized Ringing Pattern: 1 Message Lamp Ext: 51005 Mute Button Enabled? y Expansion Module? n Speakerphone: 2-way Display Language: english Survivable GK Node Name: </pre>

2.	<p>Change the BUTTON ASSIGNMENTS to use the primary station number, 51005.</p> <pre> change station 53005 Page 4 of 6 STATION SITE DATA Room: Headset? n Jack: Speaker? n Cable: Mounting: d Floor: Cord Length: 0 Building: Set Color: ABBREVIATED DIALING List1: List2: List3: BUTTON ASSIGNMENTS 1: brdg-appr B:1 E:51005 4: 2: brdg-appr B:2 E:51005 5: 3: brdg-appr B:3 E:51005 6: </pre>
----	--

4.4. Configure off-pbx-telephone Information for the H.323 Desktop as shown in Figure 1

Step	Description												
1.	<div>Enter change off-pbx-telephone station-mapping n, where n is the number of the phone extension where a mobile extension shall be configured. Enter the following information:</div> <div><ul style="list-style-type: none">• Station Extension = Station Extension• Application = OPS• Phone Number = Phone Number of the new Extension• Trunk Selection = Trunk used to SES• Configuration Set = 1</div> <div>Go to page 2</div> <div><div>change off-pbx-telephone station-mapping 51007</div><div>STATIONS WITH OFF-PBX TELEPHONE INTEGRATION</div><div>Page1 of 2</div><table><tr><td>Station Extension</td><td>Application</td><td>Dial Prefix</td><td>Phone Number</td><td>Trunk Selection</td><td>Configuration Set</td></tr><tr><td>51007</td><td>OPS</td><td>-</td><td>51007</td><td>1</td><td>1</td></tr></table></div>	Station Extension	Application	Dial Prefix	Phone Number	Trunk Selection	Configuration Set	51007	OPS	-	51007	1	1
Station Extension	Application	Dial Prefix	Phone Number	Trunk Selection	Configuration Set								
51007	OPS	-	51007	1	1								
2.	<div>Change the following:</div> <div><ul style="list-style-type: none">• Call Limit = 4• Mapping Mode = both• Bridged Calls = both</div> <div><div>change off-pbx-telephone station-mapping 51000</div><div>STATIONS WITH OFF-PBX TELEPHONE INTEGRATION</div><div>Page2 of 2</div><table><tr><td>Station Extension</td><td>Call Limit</td><td>Mapping Mode</td><td>Calls Allowed</td><td>Bridged Calls</td><td>Location</td></tr><tr><td>51007</td><td>4</td><td>both</td><td>all</td><td>both</td><td></td></tr></table></div>	Station Extension	Call Limit	Mapping Mode	Calls Allowed	Bridged Calls	Location	51007	4	both	all	both	
Station Extension	Call Limit	Mapping Mode	Calls Allowed	Bridged Calls	Location								
51007	4	both	all	both									

4.5. Configure off-pbx-telephone Information for SIP Desktop.

Step	Description																		
1.	<div><p>Enter change off-pbx-telephone station-mapping n, where n is the number of the phone extension where a mobile extension shall be configured. Enter the following information:</p><p>Note: link the second SIP extension (53005) to the first extension (51005) so both stations will ring when 51005 is called.</p><ul style="list-style-type: none">• Station Extension = Station Extension• Application = OPS• Phone Number = Phone Number of the new Extension• Trunk Selection = Trunk used to SES• Configuration Set = 1<p>Go to page 2 to continue:</p></div> <div><div>change off-pbx-telephone station-mapping 51005</div><div>STATIONS WITH OFF-PBX TELEPHONE INTEGRATION</div><div>Page1 of2</div><table><tr><th>Station Extension</th><th>Application</th><th>Dial Prefix</th><th>Phone Number</th><th>Trunk Selection</th><th>Configuration Set</th></tr><tr><td>51005</td><td>OPS</td><td>-</td><td>51005</td><td>1</td><td>1</td></tr><tr><td>51005</td><td>OPS</td><td>-</td><td>53005</td><td>1</td><td>1</td></tr></table></div>	Station Extension	Application	Dial Prefix	Phone Number	Trunk Selection	Configuration Set	51005	OPS	-	51005	1	1	51005	OPS	-	53005	1	1
Station Extension	Application	Dial Prefix	Phone Number	Trunk Selection	Configuration Set														
51005	OPS	-	51005	1	1														
51005	OPS	-	53005	1	1														
2.	<div><p>Change the following:</p><ul style="list-style-type: none">• Mapping Mode = both• Bridged Calls = both• Call Limit = 4</div> <div><div>change off-pbx-telephone station-mapping 51005</div><div>STATIONS WITH OFF-PBX TELEPHONE INTEGRATION</div><div>Page2 of2</div><table><tr><th>Station Extension</th><th>Call Limit</th><th>Mapping Mode</th><th>Calls Allowed</th><th>Bridged Calls</th><th>Location</th></tr><tr><td>51005</td><td>4</td><td>both</td><td>all</td><td>both</td><td></td></tr><tr><td>51005</td><td>4</td><td>both</td><td>all</td><td>both</td><td></td></tr></table></div>	Station Extension	Call Limit	Mapping Mode	Calls Allowed	Bridged Calls	Location	51005	4	both	all	both		51005	4	both	all	both	
Station Extension	Call Limit	Mapping Mode	Calls Allowed	Bridged Calls	Location														
51005	4	both	all	both															
51005	4	both	all	both															

4.6. Dial Plan

This section describes the steps for setting the route pattern in Communication Manager for proper routing of calls from Communication Manager to SES. These calls are ultimately destined for the uMobility Controller.

Note: Route handling varies from location to location. The following example was used for compliance testing. Refer to Section 10 [1] for further options.

From the SAT, enter the following commands and information:

Step	Description
1.	<p>To handle the incoming calls to the uMobility Controller the dial string needs to be altered. This is done with the change inc-call-handling-trmt trunk-group j command, where “j” is the trunk group for inbound call from the PSTN. For the compliance testing, the uMobility Controller was expecting the dial string without the 1 so the 1 was deleted. In addition, Automatic Alternate Routing (AAR) was used to route to uMobility Controller so the AAR feature access code of 3 was inserted.</p> <pre> change inc-call-handling-trmt trunk-group 56 INCOMING CALL HANDLING TREATMENT Service/ Called Called Del Insert Per Call Night Feature Len Number tie 11 1732555 6 tie 11 17328522963 1 3 </pre>
2.	<p>Use the change aar analysis command to add an AAR entry for the uMobility Controller.</p> <pre> change aar analysis 0 AAR DIGIT ANALYSIS TABLE Location: all Percent Full: 0 Dialed Total Route Call Node ANI String Min Max Pattern Type Num Req'd 732582963 10 10 24 aar n </pre>
3.	<p>Use the change route-pattern command to associate a route pattern to the SIP trunk which is used to access the uMobility Controller.</p> <pre> change route-pattern 24 Pattern Number: 24 Pattern Name: SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC No Mrk Lmt List Del Digits QSIG Intw 1: 1 0 n user 2: n user </pre>

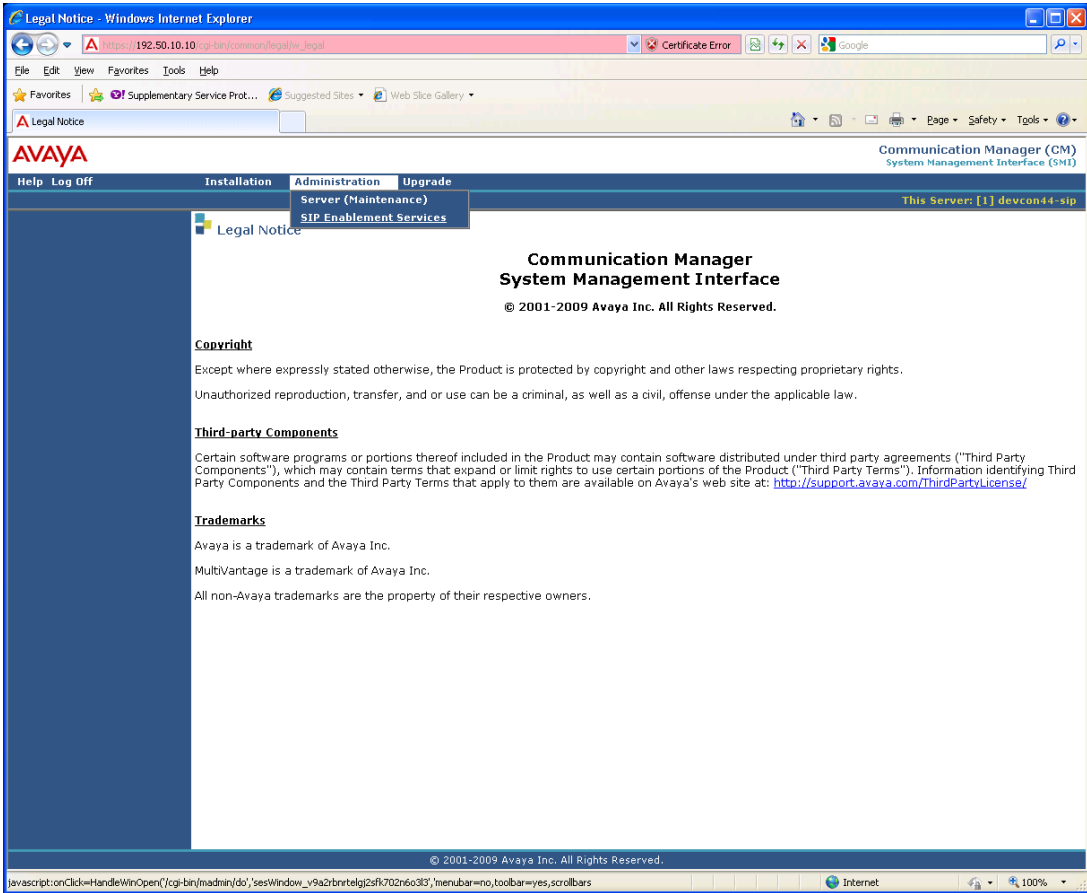
5. Configure Avaya Aura™ SIP Enablement Services

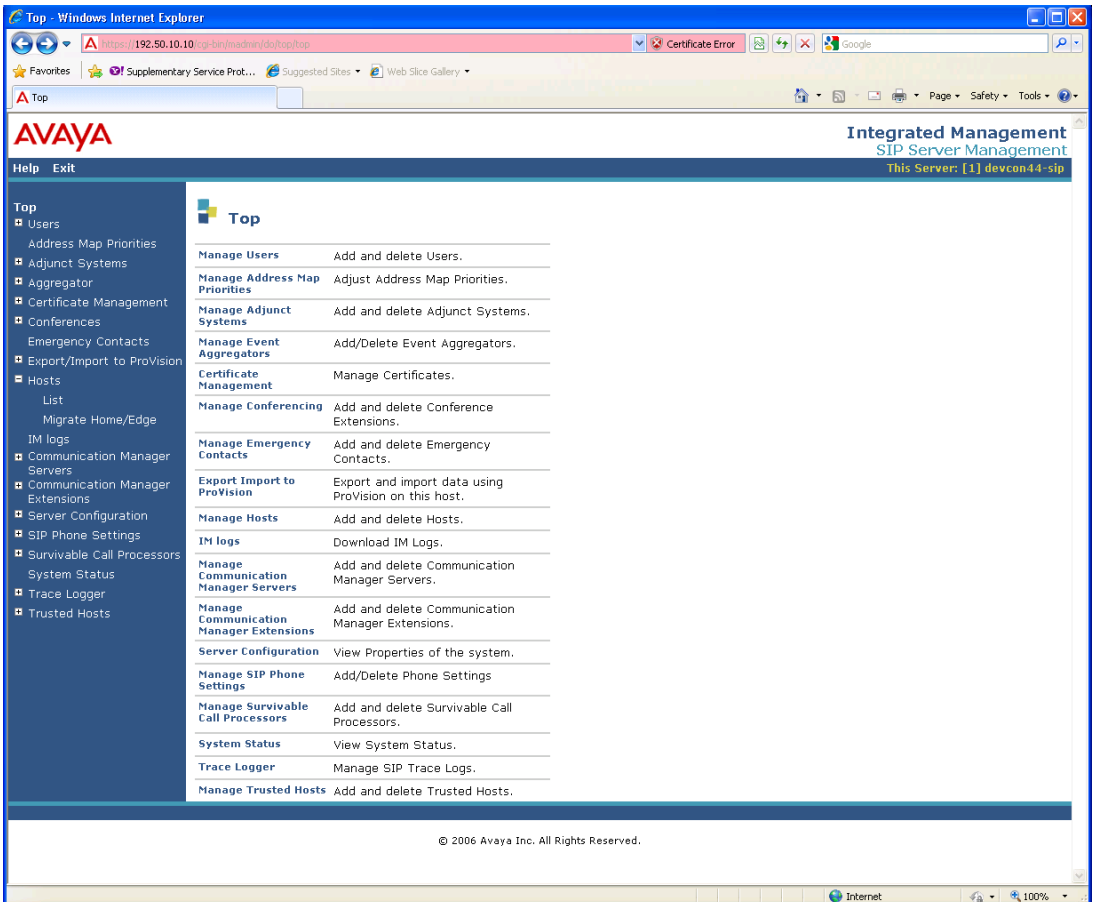
This section describes the steps required for Avaya Aura™ SIP Enablement Services to support the configuration in **Figure 1**. The following pages provide step-by-step instructions on how to create the media server entry, define the host address map entry along with contact information for the Varaha Systems uMobility Fixed-Mobile Convergence Solution.

Note: It is assumed that the appropriate license and authentication files have been installed on the servers and that login and password credentials are available. It is assumed that the reader has a basic understanding of the administration of Avaya Aura™ SIP Enablement Services and has access to SES Administrator web interface.

5.1. SES Configuration

On SES, the uMobility Controller needs to be configured as a station and a trusted host. The SIP trunk interface(s) are used by the uMobility Controller to terminate a call to the wireless operator's network. A SIP trunk is also used by Communication Manager to route mobile calls through SES to the uMobility Controller using the Direct Inward Dialing (DID) number assigned to the uMobility Controller. The trunk creation will not be covered in this document, Reference Section 10 [1] thru [4] for more information on SES installation.

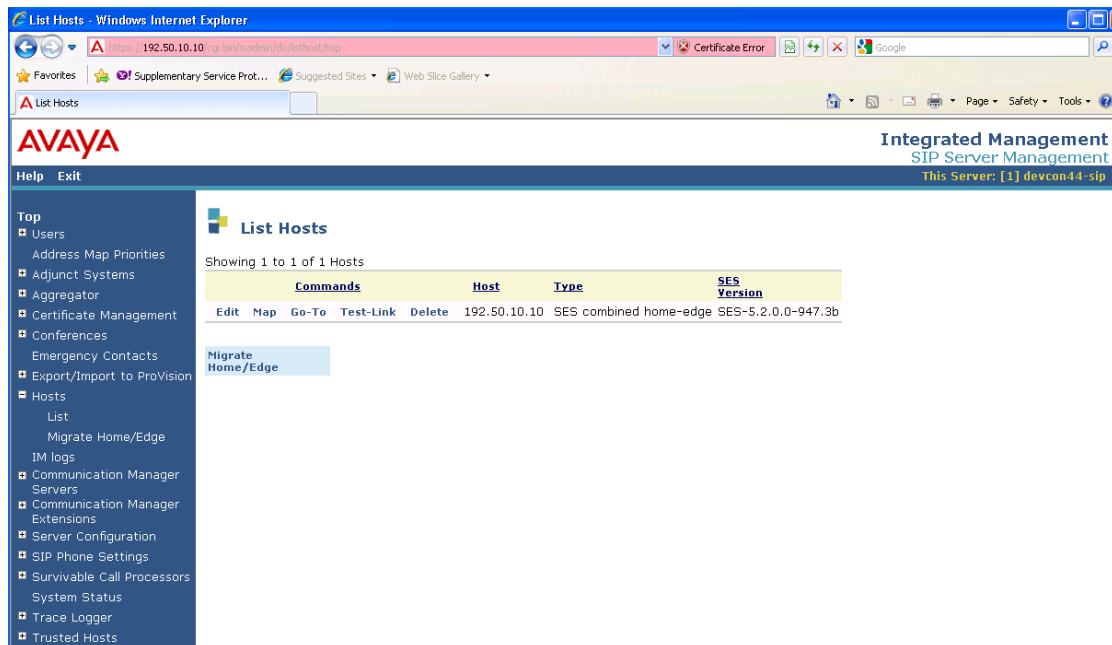
Step	Description
1.	<p>Access SES administration web interface by using the URL HTTP://ip-address/ADMIN in an Internet browser window, where ip-address is the IP address of SES server. Log in with the appropriate credentials. The first screen of the interface is displayed. Select Administration → SIP Enablement Services.</p>  <p>The screenshot shows a web browser window titled 'Legal Notice - Windows Internet Explorer'. The address bar displays 'https://192.50.10.10/cgi-bin/common/legalw_legal'. The page content includes the Avaya logo, a navigation bar with 'Help', 'Log Off', 'Installation', 'Administration', and 'Upgrade'. The 'Administration' menu is expanded, showing 'Server (Maintenance)' and 'SIP Enablement Services'. The main content area is titled 'Communication Manager System Management Interface' and contains copyright information for Avaya Inc. (© 2001-2009) and a legal notice regarding the use of the product.</p>

Step	Description																																						
2.	<p>The following screen is displayed. From the left pane, select Hosts → List.</p>  <table border="1"> <thead> <tr> <th colspan="2">Top</th> </tr> </thead> <tbody> <tr> <td>Manage Users</td> <td>Add and delete Users.</td> </tr> <tr> <td>Manage Address Map Priorities</td> <td>Adjust Address Map Priorities.</td> </tr> <tr> <td>Manage Adjunct Systems</td> <td>Add and delete Adjunct Systems.</td> </tr> <tr> <td>Manage Event Aggregators</td> <td>Add/Delete Event Aggregators.</td> </tr> <tr> <td>Certificate Management</td> <td>Manage Certificates.</td> </tr> <tr> <td>Manage Conferencing</td> <td>Add and delete Conference Extensions.</td> </tr> <tr> <td>Manage Emergency Contacts</td> <td>Add and delete Emergency Contacts.</td> </tr> <tr> <td>Export Import to ProVision</td> <td>Export and import data using ProVision on this host.</td> </tr> <tr> <td>Manage Hosts</td> <td>Add and delete Hosts.</td> </tr> <tr> <td>IM logs</td> <td>Download IM Logs.</td> </tr> <tr> <td>Manage Communication Manager Servers</td> <td>Add and delete Communication Manager Servers.</td> </tr> <tr> <td>Manage Communication Manager Extensions</td> <td>Add and delete Communication Manager Extensions.</td> </tr> <tr> <td>Server Configuration</td> <td>View Properties of the system.</td> </tr> <tr> <td>Manage SIP Phone Settings</td> <td>Add/Delete Phone Settings</td> </tr> <tr> <td>Manage Survivable Call Processors</td> <td>Add and delete Survivable Call Processors.</td> </tr> <tr> <td>System Status</td> <td>View System Status.</td> </tr> <tr> <td>Trace Logger</td> <td>Manage SIP Trace Logs.</td> </tr> <tr> <td>Manage Trusted Hosts</td> <td>Add and delete Trusted Hosts.</td> </tr> </tbody> </table> <p>© 2006 Avaya Inc. All Rights Reserved.</p>	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.	Server Configuration	View Properties of the system.	Manage SIP Phone Settings	Add/Delete Phone Settings	Manage Survivable Call Processors	Add and delete Survivable Call Processors.	System Status	View System Status.	Trace Logger	Manage SIP Trace Logs.	Manage Trusted Hosts	Add and delete Trusted Hosts.
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.																																						
Server Configuration	View Properties of the system.																																						
Manage SIP Phone Settings	Add/Delete Phone Settings																																						
Manage Survivable Call Processors	Add and delete Survivable Call Processors.																																						
System Status	View System Status.																																						
Trace Logger	Manage SIP Trace Logs.																																						
Manage Trusted Hosts	Add and delete Trusted Hosts.																																						

Outbound calls are first routed by Communication Manager to the SIP trunk group. These calls are then subject to further routing decisions determined by Host Address Maps in SES.

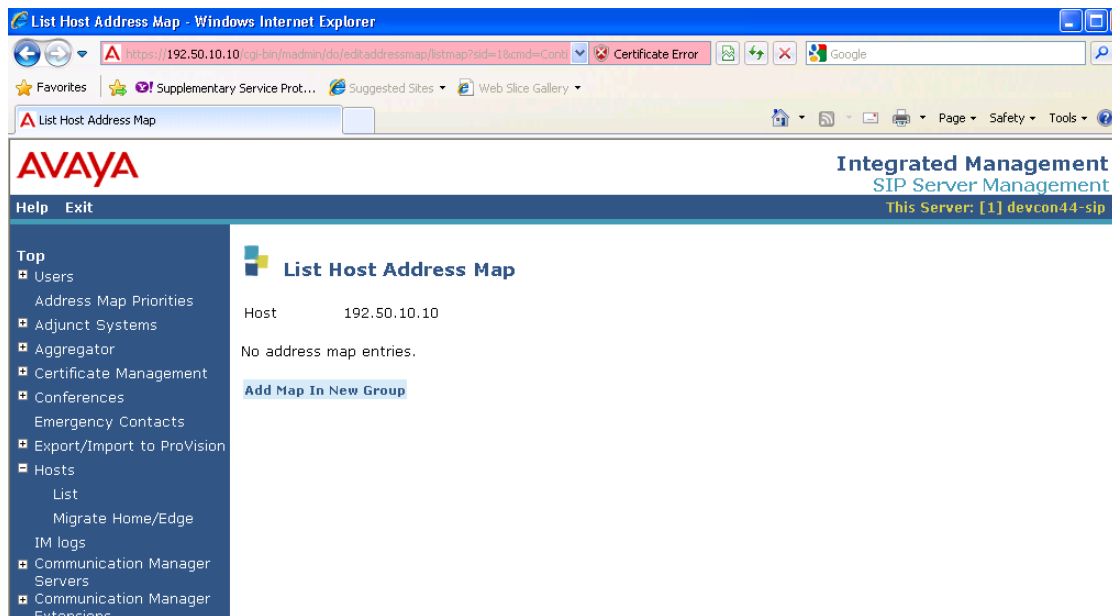
3.

The **List Hosts** screen is displayed; click on **Map** in the right pane.



4.

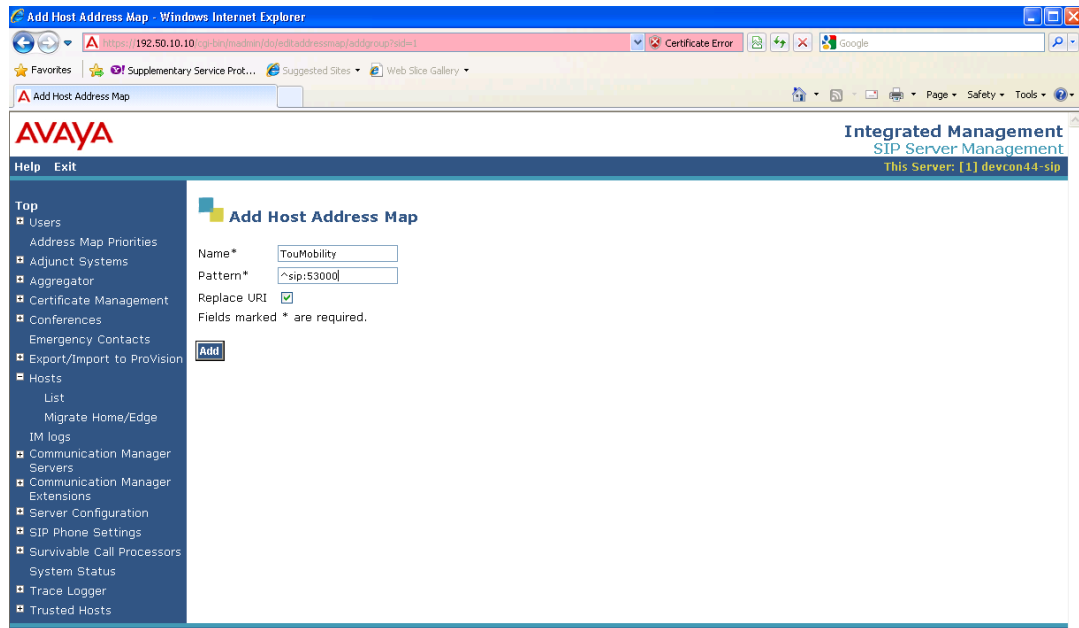
The **List Host Address Map** screen is displayed. Select **Add Map In New Group**.



5.

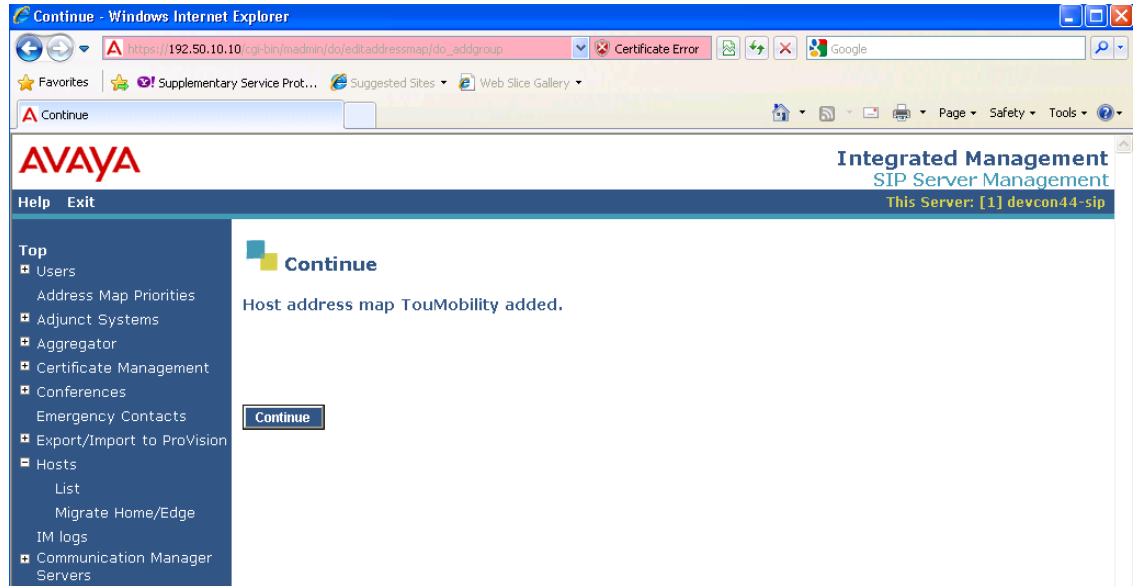
The **Add Host Address Map** screen is displayed. Enter the following:

- For the **Name** field, enter a descriptive name to denote the routing pattern.
- For the **Pattern** field, define an appropriate syntax for address mapping that matches the format of the DID number used to route mobile calls into the uMobility Controller. Extension 53000 (Pilot Number) was used for Compliance testing; this will be configured in Section 6.3.
- Retain the check in **Replace URI**, and click **Add**.



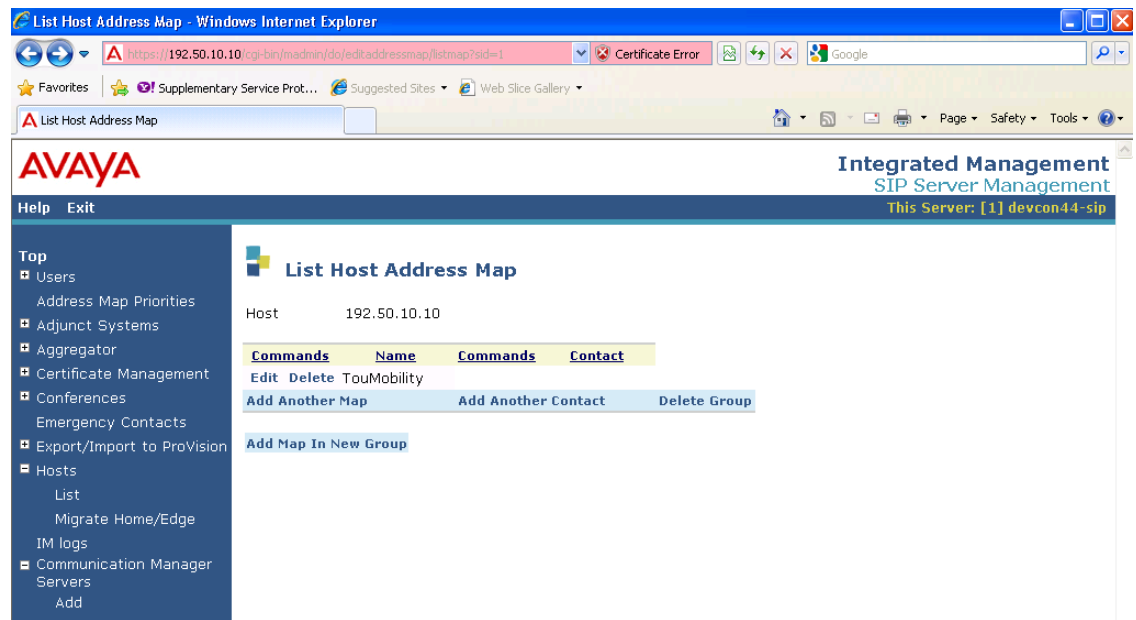
6.

At the next screen, click **Continue**.



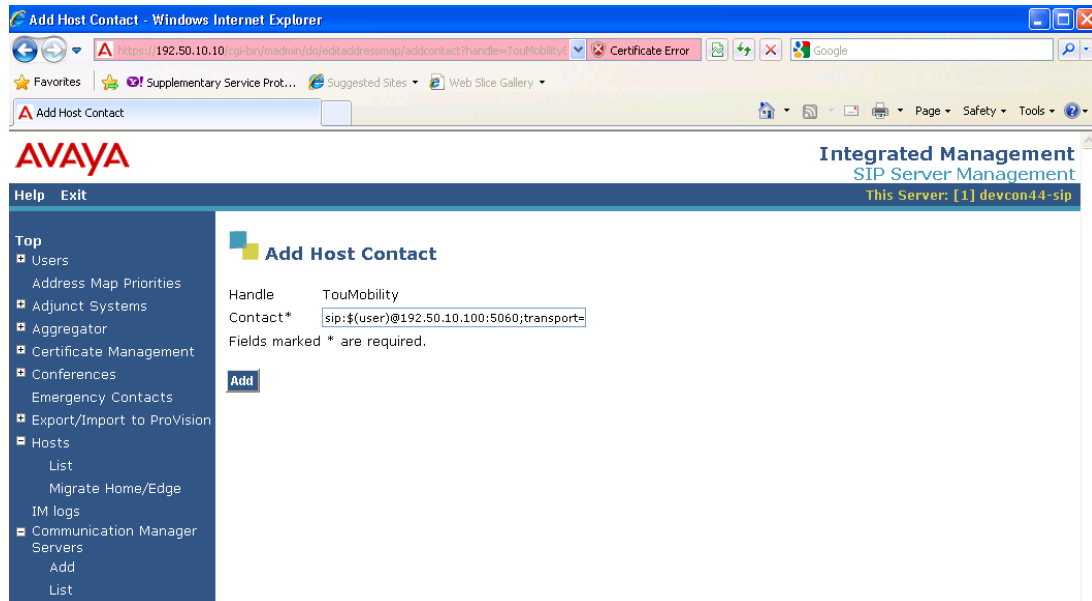
7.

The **List Host Address Map** screen is redisplayed, showing the newly added item. On the **List Host Address Map** screen, define the contact address for the uMobility Controller by clicking on **Add Another Contact** on the line below TouMobility.



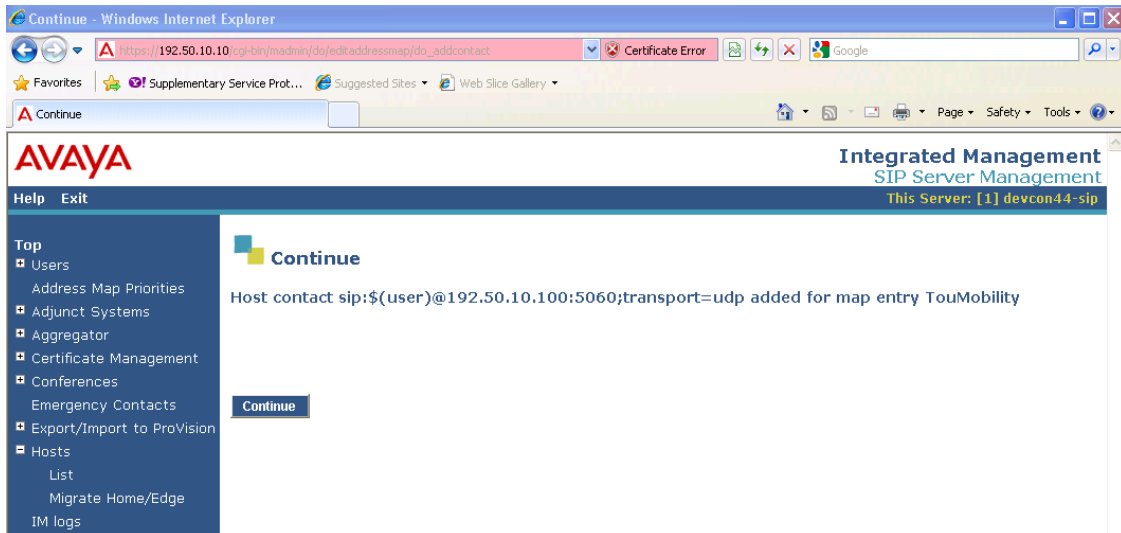
8.

The **Add Host Contact** screen is displayed. The Contact field specifies the destination for the call. Populate the **Contact** field with the service IP address of the uMobility Controller that SES should substitute into the required URI before sending a message to the uMobility Controller. SES replaces **\$(user)** with the user portion of the request URI before sending the message. Click the **Add** button.



9.

At the next screen click **Continue**.



10.

Administer the uMobility Controller as a trusted host so that SES will not challenge SIP messages from the uMobility Controller. From the left pane, select **Trusted Hosts** → **Add Trusted Host (not shown)**. Enter the IP address of the uMobility Controller; check the **Perform Origination Processing** box. Click **Add** to continue.

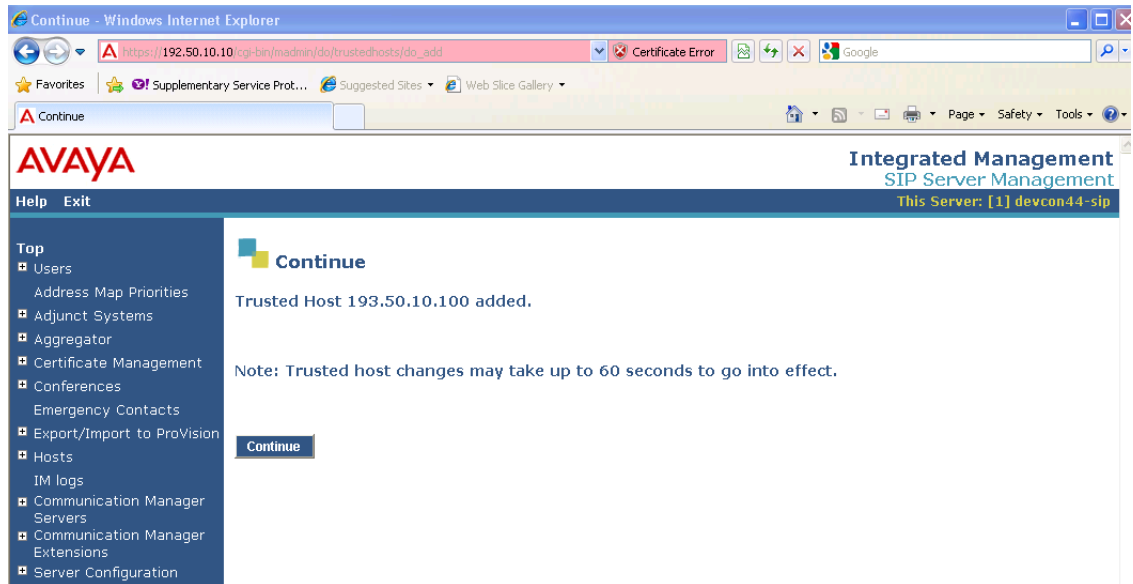
The screenshot shows a web browser window titled "Add Trusted Host - Windows Internet Explorer". The address bar displays "https://192.50.10.10/cg-bin/madmm/do/trustedhosts/add". The page features the Avaya logo and the title "Integrated Management SIP Server Management". A sidebar on the left lists various management options, with "Trusted Hosts" selected. The main content area is titled "Add Trusted Host" and contains the following form fields:

- IP Address*: 193.50.10.100
- Host*: 192.50.10.10
- Comment: uMobility Controller
- Perform Origination Processing: ☒

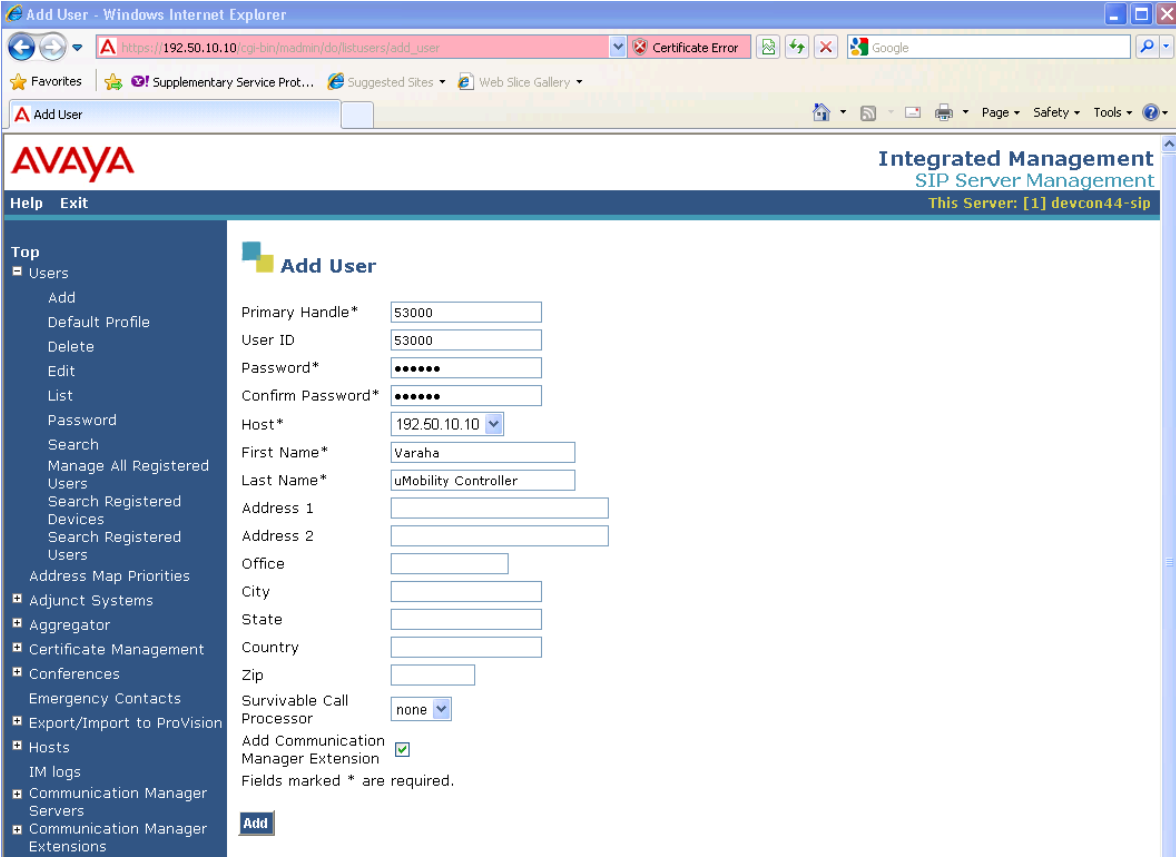
Below the form fields, a note states: "Fields marked * are required." An "Add" button is located at the bottom left of the form area.

11.

At the next screen click **Continue**.



5.2. Create Varaha uMobility Controller User on SES (Pilot Number)

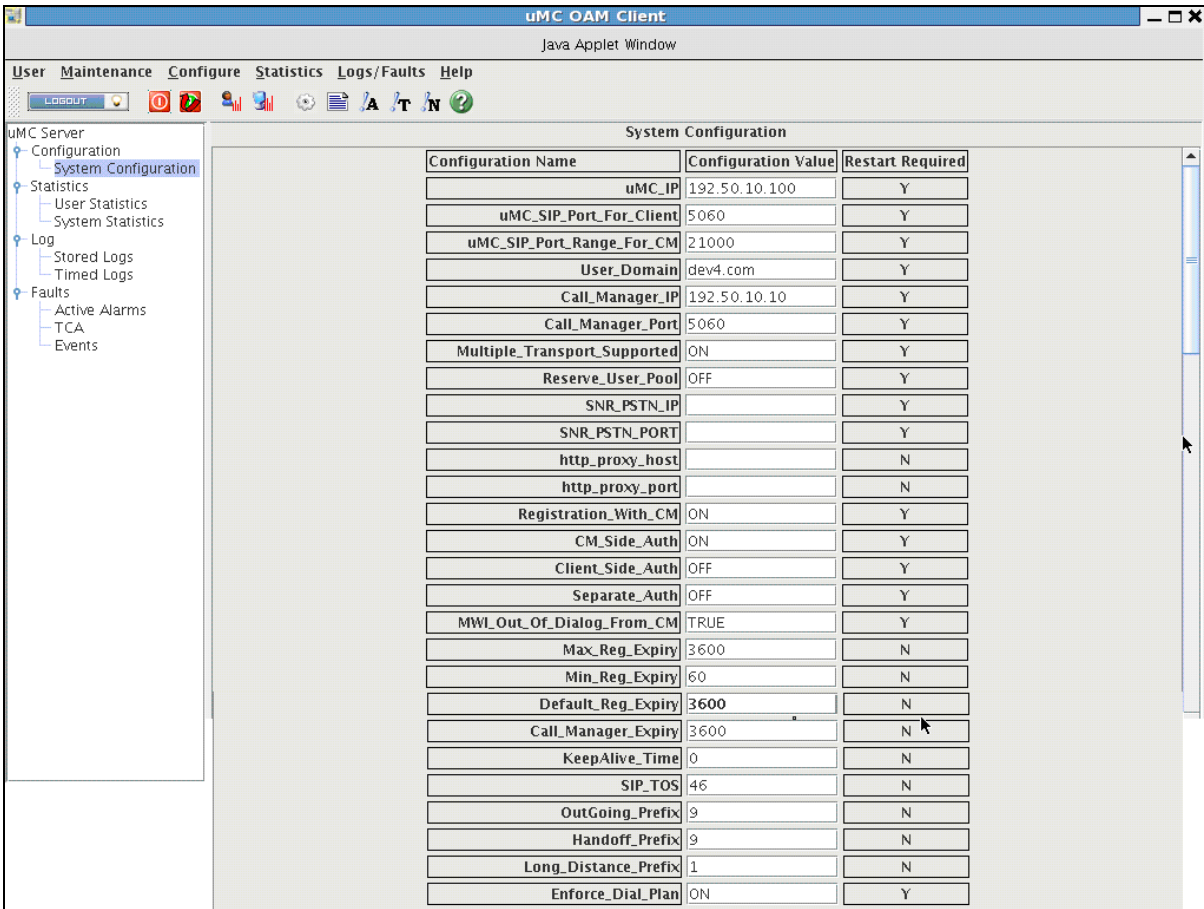
Step	Description
1.	<p>Select Users → Add. Fill in the screens as follows.</p> <ul style="list-style-type: none"> • Primary handle to 53000 • User ID to 53000 • Password to (create User password) • Confirm Password • Host to 192.50.10.10 • First Name to Varaha • Last Name to uMobility Controller • Click the Add Communication Manage Extension check box. • Select Add • A dialogue box appears, Click Continue to continue. 

Step	Description
2.	<p>The Add Communication Manager Extension page appears, enter the Extension. Click Add to continue (not shown).</p> 

6. Configure the Varaha Systems uMobility Controller

6.1. Configure Trunk to SES

The following configuration steps outline the required settings to enable the Varaha Systems uMobility Controller to interoperate with the Avaya telephony infrastructure.

Step	Description
1.	<p>Open a web browser, type <code>http://<IP address of the uMobility controller>:8080/oam</code> to access the uMC OAM client page. Click on System Configuration on the left panel and then click on the button Show Advance Config Parameter. Configure the parameters as shown below, and then click update. For detailed information about these parameters, please refer to uMobility System Administrator's Guide in Section 10 [8].</p> 

continued

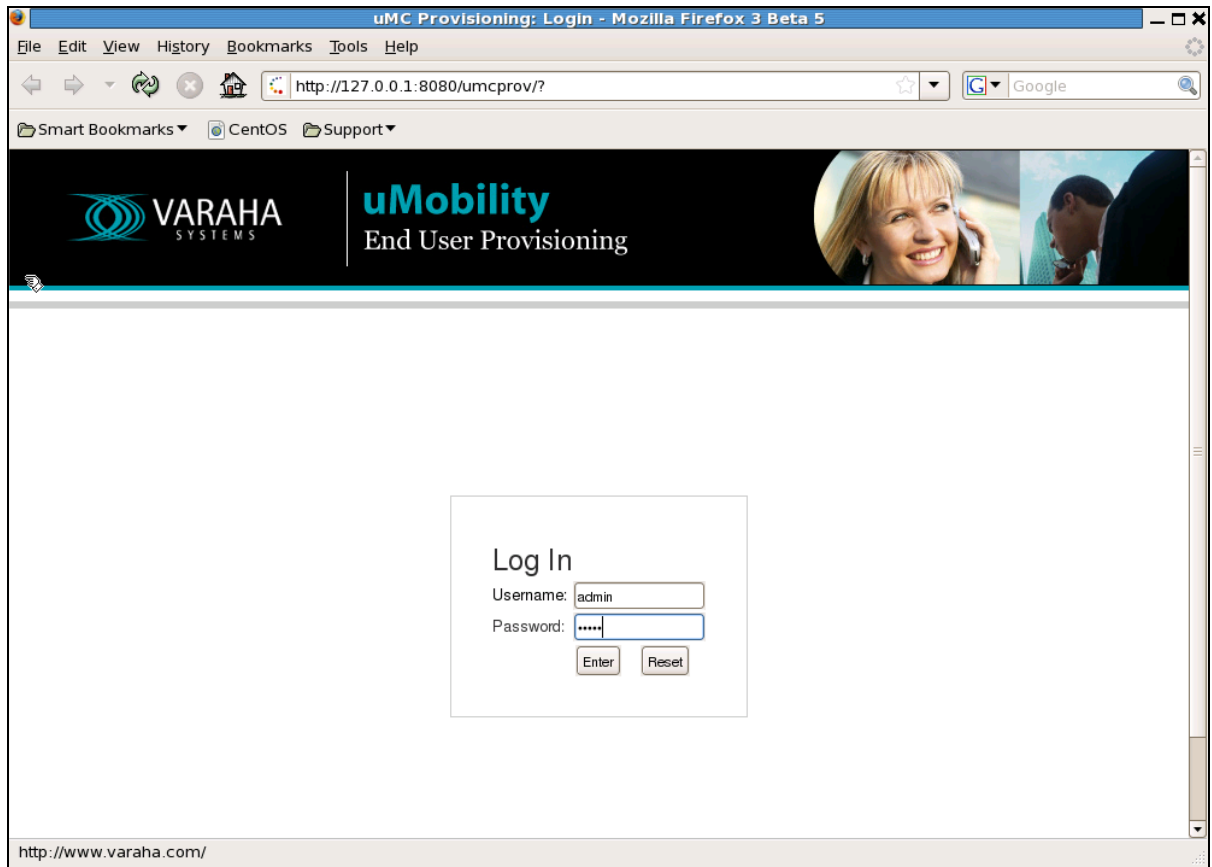
Max_Enterprise_Digits	5	Y
Long_Distance_Digits	10	N
SNR_CLID_Access_Code		Y
File_Level_Log	4	N
Sip_Stack_Level_Log	5	N
uMC_MT_Level_Log	4	Y
uMC_MT_Stack_Level_Log	5	Y
Packet_Trace_Level	1	N
HO_Cell_AutoAnswer_CLID		N
Sip_Trigger	-62	N
Cell_Trigger	-71	N
Answer_Packet_DTMF	***#	Y
HO_Delayed_Hangup_Timer	25	N
Cell_Timeout	15	N
Cell_Call_Pulse_Rate	60	Y
Minimum_Duration_Per_Pulse	50	Y
ED_Huntgroup	OFF	Y
uMC_DID_Prefix		N
Ring_Back_ED_Type	4	Y
DTMF_Dialing_Option	1	N
Ed_Error_Response	567	N
ENT_DIALBACK_PAUSE_TIME	2	Y
ED_Dtmf_Receive_Timeout	25	Y
SNR_StaleCall_Time	4	N
Client_Cell_Answer_Ack_Timeout	5	Y
Dtmf_Info_Support	TRUE	N
Cell_Vm_Direct_Answer_Timeout	2	N
Cell_Vm_Busy_Noanswer_Timeout	20	N
DM_Command	77	N
Mid_Call_Signaling_Prefix	**	N
DM_Request_Timeout	20	N
DM_InterDigitTimeout	5	N
OTA_Auth	OFF	N
CM_Side_DTMF	rfc2833	Y

Update ☒ Show Advance Config Parameter

6.2. Log on to the uMobility End User Provisioning Window

1.

User opens a browser, type in **http://<IP address of the uMobility controller>:8080/umcprov** to access the End User Provisioning window. Type in the **Username** and **Password**, and select **Enter** to continue.



6.3. Configure Pilot Number

1. From the **uMobility End User Provisioning** Window, click **List uMobility Users**. Select **umc_pilot** to continue.

The screenshot shows a web browser window titled "uMC Provisioning: User Listing - Mozilla Firefox 3 Beta 5". The address bar shows the URL "http://127.0.0.1:8080/umcprov/servlet/prov?action=list". The page header includes the VARAHA SYSTEMS logo and the text "uMobility End User Provisioning". On the right side of the header, there are links for "Logout", "Upgrade License", and "Change Password". Below the header is a navigation menu with buttons for "System Information", "Add Proxy Profile", "List Proxy Profiles", "ADD User", "List uMobility Users" (which is highlighted), "List Reserve Users", "Add VPNClient Profile", "List VPNClient Profile", "Device/Product", "Upload Product", "OTA Configuration", and "Backup". Below the navigation menu is a search section with a "Search User By:" dropdown set to "Sip Number", a text input field, and "Search" and "Clear" buttons. To the right of the search section is a "User Per Page:" dropdown and a "Set" button. Below the search section is a "User Listing" table. The table has a checkbox in the first column and the following headers: "Sip Number", "User Name", "Cell Number", "DID Number", "Send Mail", "Device", and "Proxy Profile". There is a "Show Comment" checkbox to the right of the table. The table contains one row with the following data: an empty checkbox, an empty "Sip Number" field, "umc_pilot" in the "User Name" column, empty "Cell Number", "DID Number", and "Send Mail" fields, an empty "Device" field, and "Default Proxy" in the "Proxy Profile" column. Below the table is a "Delete Selected" button. At the bottom of the page, there is a footer with the text "uMC Provision version : 03_02_21-26Jun09" and "Copyright © 2005-2008 Varaha Systems Inc., All rights reserved."

	Sip Number	User Name	Cell Number	DID Number	Send Mail	Device	Proxy Profile
<input type="checkbox"/>		umc_pilot					Default Proxy

2. The **Update the User Account** dialogue window appears, Set the following options:

- **SIP Number = 53000 (Pilot Number used for Compliance testing)**
- **Authorization User Name = 53000**
- **Password & Re-Enter New Password**
- **User Name = umc_pilot**
- **DID Number = 7328522963**

Select **Updatenow** to continue.

uMC Provisioning: Update the User Account - Mozilla Firefox 3 Beta 5

File Edit View History Bookmarks Tools Help

http://127.0.0.1:8080/umcprov/servlet/prov?action=modifydmm

Smart Bookmarks CentOS Support

VARAHA SYSTEMS | **uMobility** End User Provisioning

Logout
Upgrade License
Change Password

System Information	Add Proxy Profile	List Proxy Profiles	ADD User	List uMobility Users	List Reserve Users	Add VPNClient Profile	List VPNClient Profile	Device/Product	Upload Product	OTA Configuration	Backup
--------------------	-------------------	---------------------	----------	----------------------	--------------------	-----------------------	------------------------	----------------	----------------	-------------------	--------

Update the User Account

Sip Number: 53000 *

Authorization User Name: 53000 *

Password:

Re-Enter New Password:

User Name: umc_pilot

Proxy Profile: Default Proxy

DID Number: 7328522963

Updatenow Reset

Fields marked with an asterisk (*) are mandatory.

uMC Provision version : 03_02_21-26Jun09
Copyright © 2005-2008 Varaha Systems Inc., All rights reserved.

6.4. Create users

1. From the **uMobility End User Provisioning** Window, click **ADD User**. The **Create New User** dialogue window appears, Set the following options:

- **SIP Number = 51010 (Number used for Compliance testing)**
- **Authorization User Name = 51010**
- **Password & Re-Enter New Password**
- **User Name = 51010User**
- **Cell Number = 9723220449**
- **DID Number = 7328522963**

Select **Create** to continue.

The screenshot shows a web browser window titled "uMC Provisioning: Add New DMM User - Mozilla Firefox 3 Beta 5". The address bar shows the URL "http://127.0.0.1:8080/umcprov/adddmm.jsp". The page header includes the VARAHA SYSTEMS logo and the text "uMobility End User Provisioning". A navigation bar contains several tabs: System Information, Add Proxy Profile, List Proxy Profiles, **ADD User**, List uMobility Users, List Reserve Users, Add VPNClient Profile, List VPNClient Profile, Device/Product, Upload Product, OTA Configuration, and Backup. The "Create New User" form is displayed with the following fields and values:

Field	Value
Sip Number	51010 *
Authorization User Name	51010 *
Password	*****
Re-Enter Password	*****
Device IMEI	
User Name	51010User
User Type	uMobility User
Proxy Profile	Default Proxy
Cell Number	9723220449
DID Number	7328522962
Email-ID	
Device Type	Select Device
Product	
VPN Profile	Select One
Comment	

Fields marked with an asterisk (*) are mandatory.

Buttons: Create, Reset

Character count: (512 Characters Left)

2. Repeat Step 1 to create the other extensions used for compliance testing, 51005 and 51007.

3. List Users and select the **List uMobility Users** tab.

uMC Provisioning: User Listing - Mozilla Firefox 3 Beta 5

File Edit View History Bookmarks Tools Help

http://127.0.0.1:8080/umcprov/servlet/prov?action=list

Smart Bookmarks CentOS Support

VARAHA SYSTEMS | **uMobility** End User Provisioning

Logout Upgrade License Change Password

System Information Add Proxy Profile List Proxy Profiles ADD User **List uMobility Users** List Reserve Users Add VPNClient Profile List VPNClient Profile Device/Product Upload Product OTA Configuration Backup

Search User By: Sip Number User Per Page: Set

Search Clear

User Listing

☐ Show Comment

<input type="checkbox"/>	Sip Number	User Name	Cell Number	DID Number	Send Mail	Device	Proxy Profile
<input type="checkbox"/>	51007	51007User	14692889428	7328522961			Default Proxy
<input type="checkbox"/>	51010	51010User	19723220449	7328522962			Default Proxy
<input type="checkbox"/>	51005	51005User	14692889422	7328522965			Default Proxy
<input type="checkbox"/>	53000	umc_pilot		7328522963			Default Proxy

Delete Selected

uMC Provision version : 03_02_21-26Jun09
Copyright © 2005-2009 Varaha Systems Inc., All rights reserved.

7. General Test Approach and Test Results

Testing was conducted via the *DevConnect* Program at the Avaya Solution and Interoperability Test Lab. Compliance testing verified the integration between an Avaya telephony infrastructure and Varaha Systems uMobility FMC Solution and the ability for an enterprise user to be accessible via one business number whether the user is in the office or mobile.

7.1. Test Approach

The general test approach was to make mobile originating and mobile terminating calls route through the Avaya telephony infrastructure. All feature functionality test cases were performed manually. In addition, testing entailed verifying different types of Avaya telephones and system features interacting with the Varaha Systems uMobility FMC Solution. Tests were performed focusing on the following calling patterns:

- Mobile originated calls routed through the Avaya telephony infrastructure terminating to a [desk phone, mobile device or PSTN], both in WiFi and Cellular domain.
- Mobile terminated calls routed through the Avaya telephony infrastructure, both in WiFi and Cellular domain.
- Seamlessly move calls from the WiFi network to the mobile network and vice-versa.
- Desktop originated calls routed to mobile devices
- DTMF digit support for voicemail
- Abbreviated Dialing
- Call Forward All
- Call Hold/Unhold
- Shared Line Appearance
- Transfer
- Transfer To Desk

7.2. Test Results

The test objectives of section 7.1 were verified. The Varaha Systems uMobility FMC Solution successfully completed all test cases for the features identified in section 7.1. The Varaha Systems uMobility FMC Solution is able to route inbound/outbound calls to/from Avaya telephony infrastructure with all services tested.

7.3. Observations

While calling the mobile user on the cell network using the uMobility extension number, if the user rejects the call it goes to the cell voicemail, not the enterprise voicemail.

If the uMobility controller is restarted, the SIP extensions are orphaned on SES. When the uMobility controller re-registers it adds another occurrence for the SIP registered user. If this happens more than 6 times in a short period, the phones are not able to register with SES. To resolve the problem the user has to be removed and restored on SES.

Calls out to the cell phones from the enterprise (single number reach (SNR)) use the caller ID of the uMobility controller pilot number. Caller ID of original caller can be enabled if the network doesn't use H323 endpoints.

If the WiFi infrastructure is not configured correctly it could cause a 1 to 3 second delays in WiFi to Cell roaming.

MWI was not validated when the mobile phone was in the cell network due the test environment and time constraints.

8. Verification Steps

This section provides the steps for verifying Varaha Systems uMobility FMC Solution. In general, the verification steps include:

- Verify Mobile originated calls routed through the Avaya telephony infrastructure terminating to a [desk phone, mobile device or PSTN] correctly completed.
- Seamlessly move calls from the WiFi network to the mobile network and vice-versa.
- Place internal and external calls between all the telephones in the test environment.

9. Conclusion

These Application Notes describe the configuration steps required for integrating the Varaha Systems uMobility FMC Solution into an Avaya telephony infrastructure. For the configuration described in these Application Notes, the Varaha Systems uMobility FMC Solution was responsible for bridging landline connectivity to Avaya telephony infrastructure with the wireless connectivity to the CELL network and allowed roaming seamlessly between WiFi and mobile networks. The functionality of the Avaya/Varaha Systems uMobility FMC Solution was validated via the DevConnect Program at the Avaya Solution and Interoperability Test Lab. All feature functionality test cases passed.

10. Additional References

The following Avaya product documentation can be found at <http://support.avaya.com>.

- [1] *Administering Avaya Aura™ Communication Manager*, May 2009, Issue 5.0, Document Number 03-300509.
- [2] *Administering Avaya Aura™ SIP Enablement Services*, May 2009, Issue 2.1, Document 03-602508.
- [3] *Avaya Aura™ SIP Enablement Services (SES) Implementation Guide*, May 2009, Issue 6, Document 16-300140.
- [4] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 3.0*, Document Number 16-300698.
- [5] *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Administrator Guide, Release 2.0*, Document Number 16-601944.
- [6] *Modular Messaging, Release 5.0 with the Avaya MSS Messaging Application Server (MAS) Administration Guide*, January 2009.
- [7] *Avaya IA 770 INTUITY AUDIX Messaging Application Release 5.1 Administering. Communication Manager Servers to Work with IA 770*, June 2008.

Varaha Systems product documentation can be found at:
<http://www.varaha.com/channelpartners.php>

- [8] *uMobility System Administrator's Guide Generic Master 3.2.21*, July 2009.

11. Change History

Issue	Date	Reason
1.0	11/10/09	Initial issue
2.0	11/17/09	Second issue

©2009 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.