



Avaya Solution & Interoperability Test Lab

Application Note for Configuring the Ascomwireless i75 VoWiFi Handset with Avaya Communication Manager and Avaya SIP Enablement Services - Issue 1.2

Abstract

These Application Notes detail the configuration process for interoperability between Ascomwireless i75 VoWiFi Handsets with Avaya Communication Manager and Avaya SIP Enablement Services. Information in these Application Notes has been obtained through DeveloperConnection compliance testing and additional technical discussions. Testing was conducted via the DeveloperConnection Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

Implementing wireless telephony requires interoperability between the wireless telephony products and the telephony infrastructure. As IP telephony evolves, potential implementers of this technology look for flexibility and choice when deciding on which particular technology to implement. Regardless of the technology chosen the telephony infrastructure needs to be flexible enough to support solutions using all available technologies.

These Application Notes describe the configuration process necessary to provide interoperability between Avaya Communication Manager with Avaya SIP Enablement Services and Ascomwireless i75 VoWiFi SIP Handsets. Specific calling features tested and verified to operate correctly include attended/unattended transfer, conference call participation, conference call add/drop, conference call creation, multiple call appearances, caller ID operation, call forwarding unconditional, call forwarding on busy, call forwarding clear, pick groups, call pickup, bridged appearances, voicemail using IA770, MWI, hold and return from hold.

The Ascomwireless i75 VoWiFi Handset is a wireless 802.11 telephone available in two versions, the Protector and the Medic model. The only differences between the Protector and Medic model are the Medic model is made with a tougher exterior and treated to be more resistant to temperature. Both versions are robust units designed to function in tough environments. The case is made of durable PC/ABS plastic, which makes it drop proof from 1.5 meters onto concrete. For added protection the antenna is integrated inside the handset.

The Ascomwireless i75 VoWiFi Handset has both an illuminated display and keypad. The display is a 128 x 64 pixels LCD screen which is covered by anti-reflex treated plastic glass for maximum readability.

The handset memory contains all personal settings such as phonebook, identity, alert signal and user defined functions of the soft and programmable hot keys. In addition, the memory holds up to two versions of firmware.

1.1. Network Diagram

The network diagram shown in **Figure 1** illustrates the testing environment used for compliance testing. The network consists of an Avaya Communication Manager, an Avaya SIP Enablement Services (SES), three different models of wired IP telephones, one wireless IP telephone, two software based IP telephones, one digital telephone, and the wireless network infrastructure described below. Three computers are also present in the network providing network services such as DHCP, TFTP and RADIUS. The RADIUS service was provided by Microsoft Internet Authentication Server (IAS). One of the computers runs the Ascomwireless Portable Device Manager application. The computer used for provisioning the telephones was not attached to the network.

The wired IP telephones include the Avaya 9630, the Avaya 4620SW and the Avaya 4625SW IP Telephones. The wireless IP telephones are the Ascomwireless i75 VoWiFi Handset. The Ascomwireless i75 VoWiFi Handsets also have the Ascomwireless i75 Headset attached. Present in the network is an Avaya 2420 Digital Telephone, which is directly connected to Avaya Communication Manager. Two wireless laptops, one running Avaya one-X Desktop Edition and the other running Avaya IP Softphone, are connected to the network.

The wireless network is provided by Meru Networks and consists of one Meru Networks MC500 controller and three Meru Networks AP-208 access points. Two access points are on the same VLAN and the third access point is on a separate VLAN. The MC500 controller is on a different subnet than the access points.

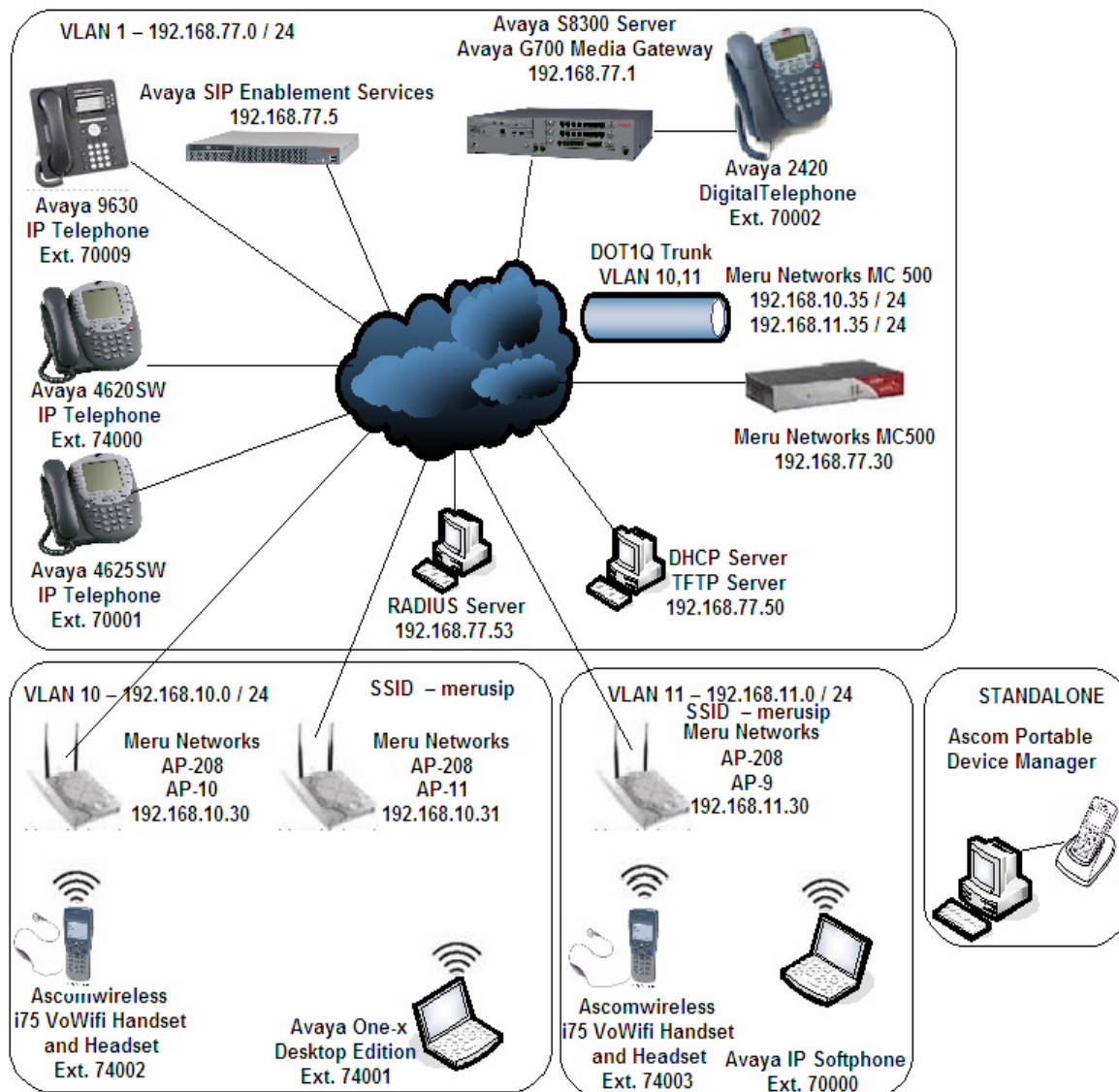


Figure 1: Sample network diagram for Ascomwireless i75 VoWiFi Handset with Avaya Communication Manager and Avaya SIP Enablement Services

2. Equipment and Software Validated

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

Equipment	Software
Avaya S8300 Server	Avaya Communication Manager 4.0.5 (R014x.00.0.730.5)
Avaya G700 Media Gateway <ul style="list-style-type: none">• MM711 Analog Media Module• MM712 DCP Media Module	26.31.0 HW04 / FW87 HW05 / FW08
Avaya SIP Enablement Services	3.1.2 (SES-3.1.2.0-309.0)
Avaya 2420 Digital Telephone	N/A
Avaya 4620SW IP Telephone (SIP)	2.2.2
Avaya 4625SW IP Telephone (H.323)	2.8
Avaya 9630 IP Telephone (H.323)	1.2.1
Avaya IP Softphone	6.0.0.25
Avaya one-X Desktop Edition Softphone	R2.1 SP1
Ascomwireless i75 VoWiFi Handset	1.4.9
Ascomwireless i75 Headset	N/A
Ascomwireless Portable Device Manager	2.1.1
Meru Networks, MC500 Controller	3.4
Meru Networks AP208	3.4
Microsoft 2003 Server DHCP Server	5.2
Microsoft 2003 Server Internet Authentication Server	5.2.3790.0

3. Configure Avaya Communication Manager and Avaya SIP Enablement Services

All of the telephones configured in the sample network in **Figure 1** were administered as H.323 or SIP stations in Avaya Communication Manager and Avaya SIP Enablement Services (SES). SIP stations were administered as Off-PBX stations in Avaya Communication Manager. For complete references on how to administer these types of stations please refer to **Section 10 [1]** and **[2]**. Certain specific Avaya Communication Manager features were tested with the Ascomwireless i75 VoWiFi Handset. The configuration related to the specific features tested is included.

3.1. Avaya Communication Manager Feature Configuration

Step	Description
1.	<p>To enable the features used for testing (Call Park, Call Answer, Call Forwarding and Call Pickup) administer the configuration for Feature-Access-Codes (FAC) and Feature-Name-Extensions (FNE) on Avaya Communication Manager. The features implemented for SIP stations need to be paired with the features implemented for H.323 stations, therefore, these parameters need to be specified even when using only SIP stations. From the SAT (System Administration Terminal) interface on Avaya Communication Manager use the “change feature-access-codes” command to configure the following parameters on page 1 and Submit the changes.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <pre> change feature-access-codes Page 1 of 7 FEATURE ACCESS CODE (FAC) Abbreviated Dialing List1 Access Code: Abbreviated Dialing List2 Access Code: Abbreviated Dialing List3 Access Code: Abbreviated Dial - Prgm Group List Access Code: Announcement Access Code: Attendant Access Code: Answer Back Access Code: #11 Auto Alternate Routing (AAR) Access Code: 60 Auto Route Selection (ARS) - Access Code 1: 61 Call Forwarding Activation Busy/DA: #15 All: #16 Deactivation: #17 Automatic Callback Activation: Deactivation: Call Forwarding Enhanced Status: Act: Deactivation: Call Park Access Code: #10 Call Pickup Access Code: #12 CAS Remote Hold/Answer Hold-Unhold Access Code: CDR Account Code Access Code: Change COR Access Code: Change Coverage Access Code: Contact Closure Open Code: Close Code: ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help </pre> </div>

2. From the SAT interface use the “**change off-pbx-stations feature-name extensions**” command to configure the following parameters on page 1 and Submit the changes. Note that the extensions used for FNEs match those used for FACs by pre-pending the FAC code with “710”. Having this uniformity between FACs and FNEs is not required.

```

change off-pbx-telephone feature-name-extensions                               Page 1 of 2

EXTENSIONS TO CALL WHICH ACTIVATE FEATURES BY NAME

Active Appearance Select:
  Automatic Call Back:
Automatic Call-Back Cancel:
  Call Forward All: 71016
Call Forward Busy/No Answer: 71015
  Call Forward Cancel: 71017
  Call Park: 71010
  Call Park Answer Back: 71011
  Call Pick-Up: 71012
Calling Number Block:
Calling Number Unblock:
Conference on Answer:
Directed Call Pick-Up:
Drop Last Added Party:
Exclusion (Toggle On/Off):
Extended Group Call Pickup:
Held Appearance Select:

ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help

```

3. In order for the FACs and FNEs to be routed through the system properly the digits used for Auto Route Selection (ARS), Auto Alternate Routing (AAR) and FACs need to be administered in the dial plan. From the SAT interface on Avaya Communication Manager use the “**change dialplan analysis**” command to configure the following parameters on page 1 and Submit the change. The values specified for the “Dialed String” field value must match the ones configured in **Step 1** for AAR and ARS.

```

change dialplan analysis                                                       Page 1 of 12

DIAL PLAN ANALYSIS TABLE
Percent Full: 3

Dialed   Total   Call   Dialed   Total   Call   Dialed   Total   Call
String   Length Type   String   Length Type   String   Length Type
  60      2     fac    60      2     fac
  61      2     fac    61      2     fac
  #       3     fac    #       3     fac

ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help

```

4. Configure the Meru Networks MC500 Controller

The following steps detail the initial configuration for the Meru Networks wireless network used for the compliance testing. The configuration on the Meru Networks MC500 was administered via the command line interface over a console connection.

Step	Description
1.	<p>To perform the initial configuration on the Meru Networks MC500 controller, setup a serial connection from a PC or laptop. Setup a terminal session with the following parameters:</p> <p>Bits per second "115200" Data Bits "8" Parity "None" Stop bits "1" Flow control "None"</p>
2.	<p>From the console connection to the Meru Networks MC500 log in to the controller using default credentials which can be obtained from the Meru Networks MC500 Controller documentation. Assign a hostname, IP address, and IP default gateway to the MC500 Controller. In addition, specify the IP address of the DHCP server. This enables DHCP relay on the MC500 Controller to allow dynamic IP addressing for the wireless IP endpoints.</p> <pre>MC500# configure terminal MC500(config)# hostname MC500 MC500(config)# ip address 192.168.77.30 255.255.255.0 MC500(config)# ip default-gateway 192.168.77.254 MC500(config)# ip dhcp-server 192.168.77.50</pre>

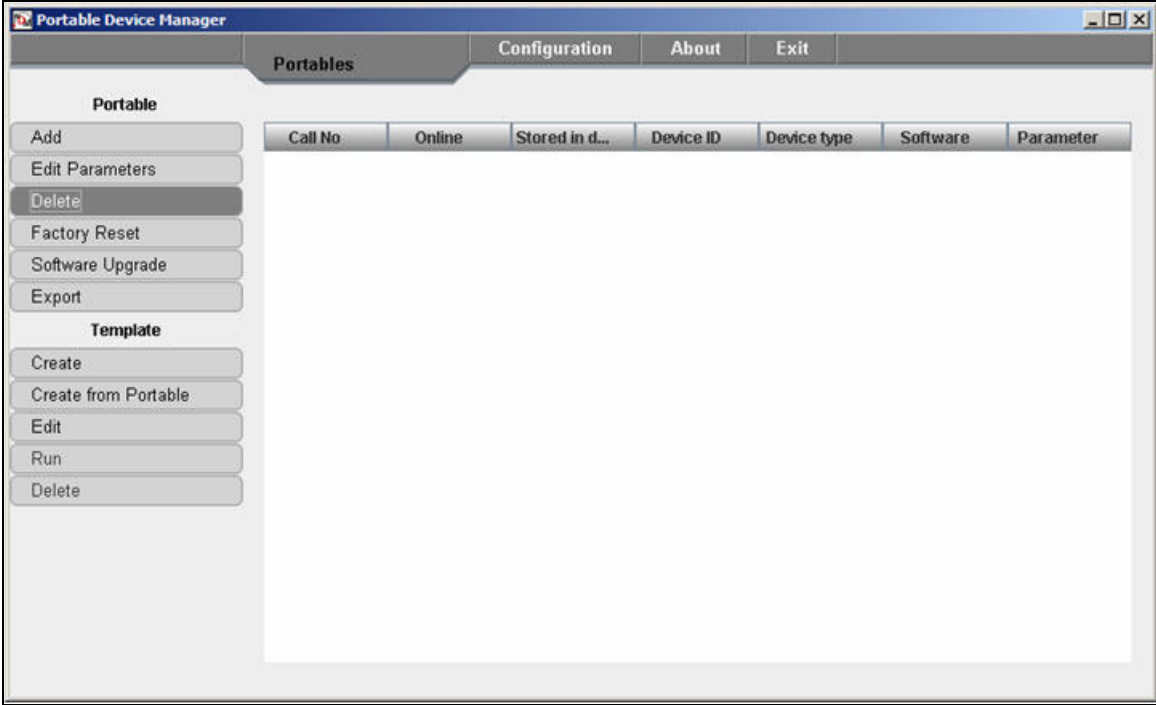
Step	Description
3.	<p>Configure the three Access Points (APs) in the WLAN configuration depicted in Figure 1. AP-9, AP-10 and AP-11 are in different subnets than the MC500 Controller. Therefore these APs are configured for “Layer 3 connectivity”, which requires the MC500 Controller IP address to be specified.</p> <pre> MC500(config)# ap 10 MC500(config)# description AP-10 MC500(config)# mac-address 00:0c:e6:00:40:58 MC500(config-ap)# connectivity l3-preferred MC500(config-ap-connectivity)#ip address 192.168.10.30 255.255.255.0 MC500(config-ap-connectivity)# ip default-gateway 192.168.10.254 MC500(config-ap-connectivity)# controller ip 192.168.77.30 MC500(config-ap-connectivity)# end MC500(config)# ap 11 MC500(config)# description AP-11 MC500(config)# mac-address 00:0c:e6:00:40:6c MC500(config-ap)# connectivity l3-preferred MC500(config-ap-connectivity)# ip address 192.168.10.31 255.255.255.0 MC500(config-ap-connectivity)# ip default-gateway 192.168.10.254 MC500(config-ap-connectivity)# controller ip 192.168.77.30 MC500(config-ap-connectivity)# end MC500(config)# ap 9 MC500(config)# description AP-9 MC500(config)# mac-address 00:0c:e6:00:3e:e1 MC500(config-ap)# connectivity l3-preferred MC500(config-ap-connectivity)#ip address 192.168.11.30 255.255.255.0 MC500(config-ap-connectivity)# ip default-gateway 192.168.11.254 MC500(config-ap-connectivity)# controller ip 192.168.77.30 MC500(config-ap-connectivity)# end </pre>
4.	<p>The wireless IP endpoints that register with Avaya SIP Enablement Services Server are assigned to vlan10 and vlan11. Create two VLANs (vlan10 and vlan11) with a tag of “10” and “11”, respectively. Assign an IP address, default gateway, and DHCP server to the VLAN interface. This enables 802.1Q trunking on the MC500 Controller.</p> <pre> MC500(config)# vlan vlan10 tag 10 MC500(config-vlan)# ip address 192.168.10.35 255.255.255.0 MC500(config-vlan)# ip default-gateway 192.168.10.254 MC500(config-vlan)# ip dhcp-server 192.168.77.50 MC500(config-vlan)# exit MC500(config)# vlan vlan11 tag 11 MC500(config-vlan)# ip address 192.168.11.35 255.255.255.0 MC500(config-vlan)# ip default-gateway 192.168.11.254 MC500(config-vlan)# ip dhcp-server 192.168.77.50 MC500(config-vlan)# exit </pre>

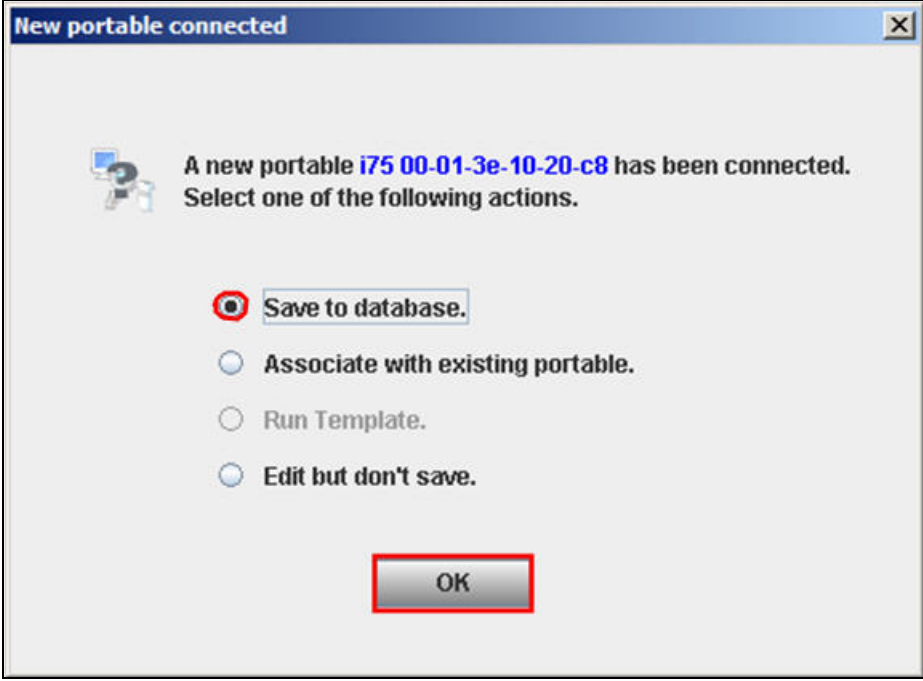
Step	Description
5.	<p>Configure the security profiles that will be assigned to the ESSID in Step 6. Four different security schemas were tested Clear, WEP-128, WPA-PSK TKIP and WPA2-CCMP-802.1X using radius. All four security profiles were configured but tested independently by modifying the “security-profile” command under the ESSID configuration in Step 6.</p> <p>Clear Configuration</p> <pre>MC500(config)# security-profile clear MC500(config-security)# allowed-12-modes clear MC500(config-security)# exit</pre> <p>WEP128 Configuration</p> <pre>MC500(config)# security-profile wep MC500(config-security)# allowed-12-modes wep MC500(config-security)# encryption-modes wep128 MC500(config-security)# static-wep key 0123456789012 MC500(config-security)# static-wep key-index 1 MC500(config-security)# exit</pre> <p>WPA-PSK Configuration</p> <pre>MC500(config)# security-profile wpa MC500(config-security)# allowed-12-modes wpa-psk MC500(config-security)# encryption-modes tkip MC500(config-security)# psk key 123456789 MC500(config-security)# exit</pre> <p>WPA2-CCMP-802.1X Configuration</p> <pre>MC500(config)# security-profile wpa2-ccmp-8021x MC500(config-security)# allowed-12-modes wpa2 MC500(config-security)# encryption-modes ccmp MC500(config-security)# 8021x-network-initiation MC500(config-security)# radius-server primary Dev7-Radius MC500(config-security)# exit</pre> <p>The WPA2-CCMP-802.1X configuration also requires the additional configuration of a Radius Server object.</p> <pre>MC500(config)# radius-profile Dev7-Radius MC500(config-radius)# ip-address 192.168.77.53 MC500(config-radius)# key meru1234 MC500(config-radius)# port 1812 MC500(config-radius)# mac-delimiter hyphen MC500(config-radius)# exit</pre>

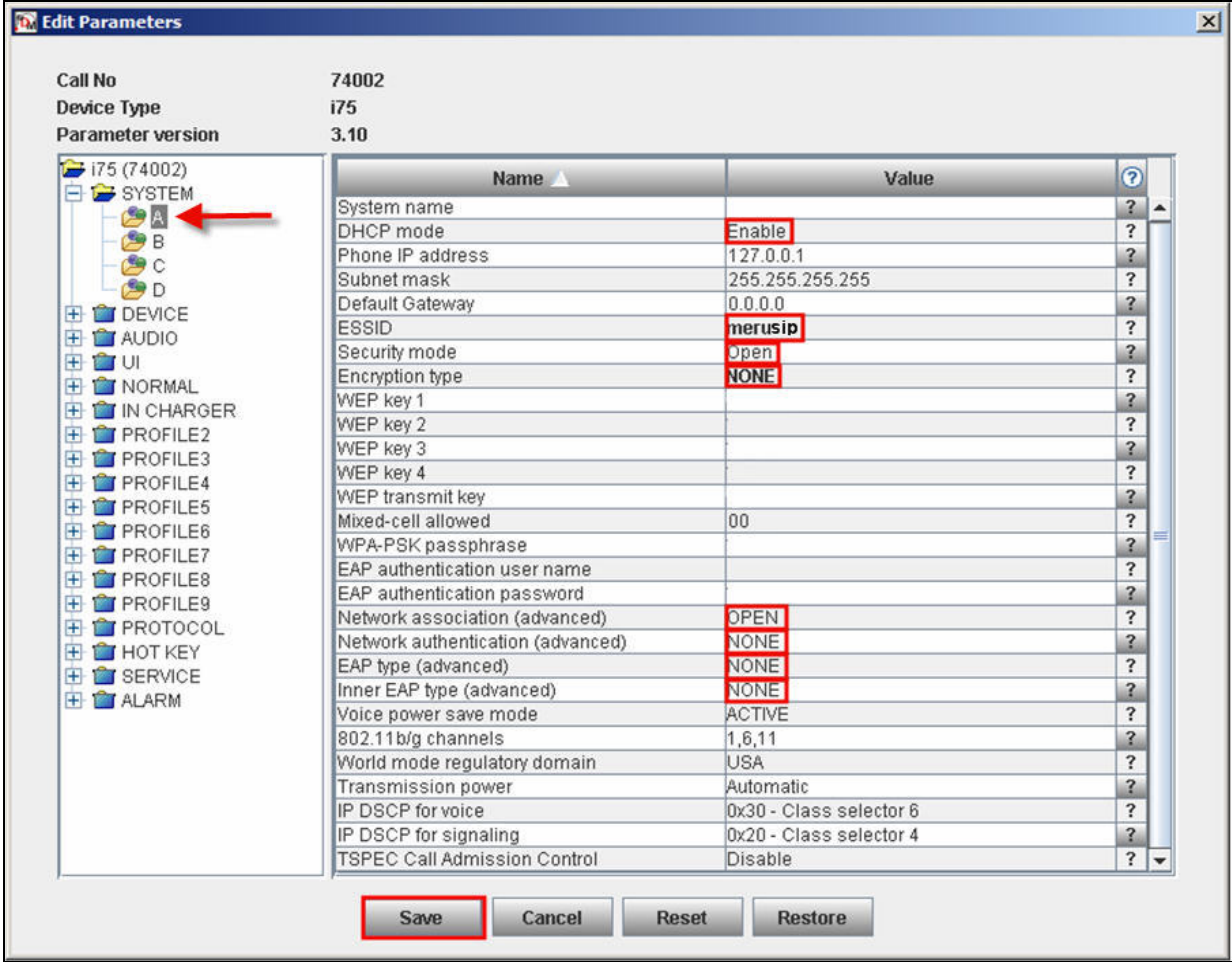
Step	Description
6.	<p>Create ESSID merusip and assign security profile clear that was created in the previous step. In order to support the other encryption modes replace the keyword clear, with the name of another security profile.</p> <pre> MC500(config)# ssid merusip MC500(config-ssid)# security-profile clear MC500(config-ssid)# vlan support configured-vlan-only MC500(config-ssid)# ssid merusip MC500(config-ssid)# ap-discovery join-virtual-ap MC500(config-ssid)# exit </pre> <p>In order to support the Radius server the additional commands need to be added under the ESSID. This is only needed for the WPA2-CCMP-802.1X configuration.</p> <pre> MC500(config)# ssid merusip MC500(config-ssid)# vlan support radius-and-configured-vlan MC500(config-ssid)# exit </pre>
7.	<p>The Ascomwireless i75 VoWiFi Handset requires the Meru Networks MC500 controller to rewrite the IP TOS (Type of Service or DSCP Differential Services Code Point) bits. Therefore, the default QoS rules for SIP on Meru Networks MC500 controller need to be rebuilt (since the Meru Networks MC500 does not allow the default rules to be modified).</p> <pre> MC500(config)# no qosrule 3 MC500(config)# no qosrule 4 </pre> <pre> MC500(config-qosrule)# qosrule 3 netprotocol 17 qosprotocol sip MC500(config-qosrule)# dstport 5060 MC500(config-qosrule)# dscp ef MC500(config-qosrule)# action capture MC500(config-qosrule)# exit </pre> <pre> MC500(config-qosrule)# qosrule 4 netprotocol 17 qosprotocol sip MC500(config-qosrule)# srcport 5060 MC500(config-qosrule)# dscp ef MC500(config-qosrule)# action capture MC500(config-qosrule)# exit </pre>
8.	<p>Save the newly configured information to the Meru Networks MC500 controller and reload it.</p> <pre> MC500# copy running-config startup-config MC500# reload all </pre>

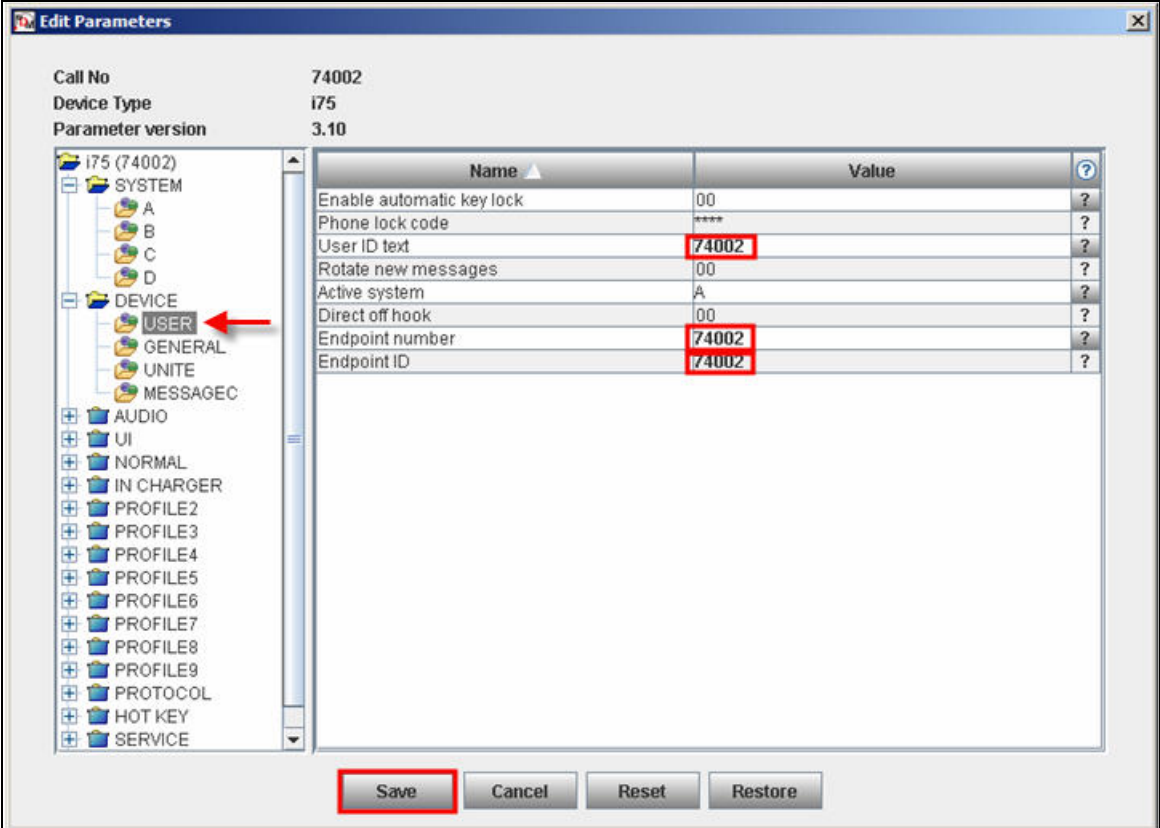
5. Configure the Ascomwireless i75 VoWiFi Handset

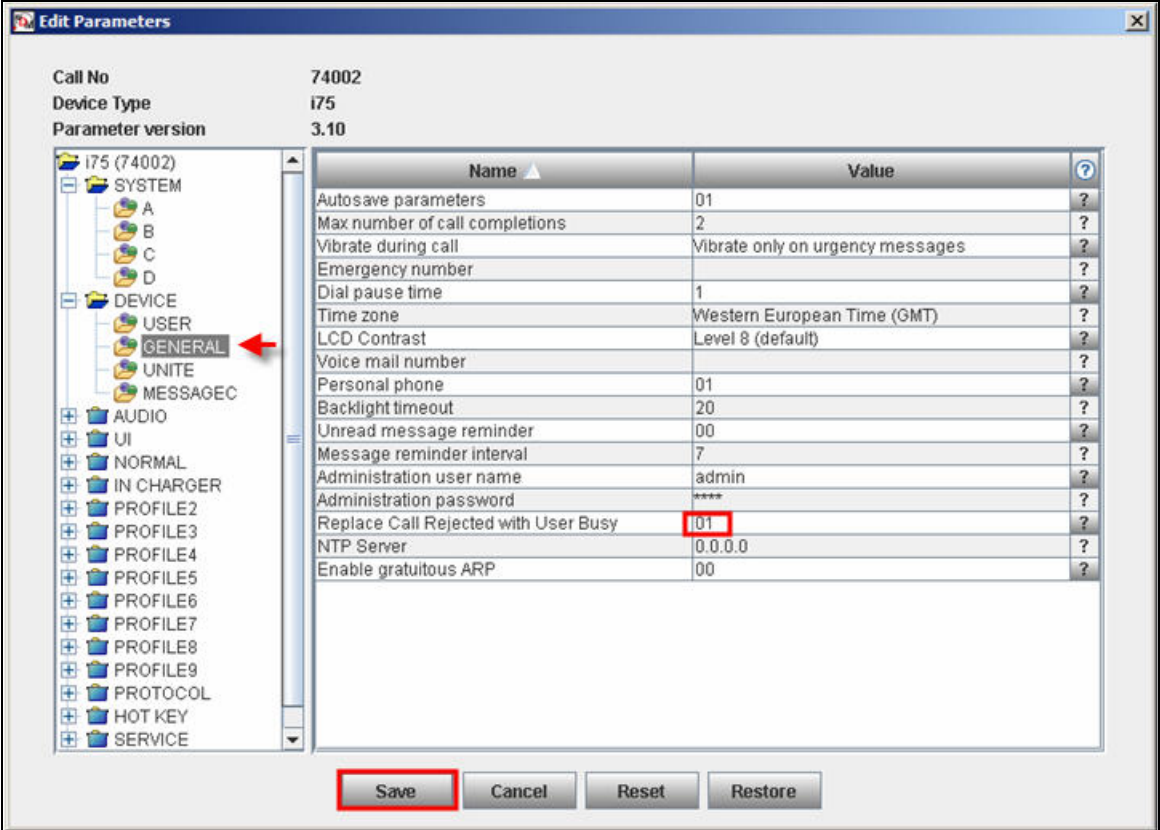
The following steps detail the configuration process for the Ascomwireless i75 VoWiFi Handset using the Ascomwireless Portable Device Manger (PDM) Windows-based application. For complete details on all the supported features on the Ascomwireless i75 VoWiFi Handset refer to **Section 10 [4]**.

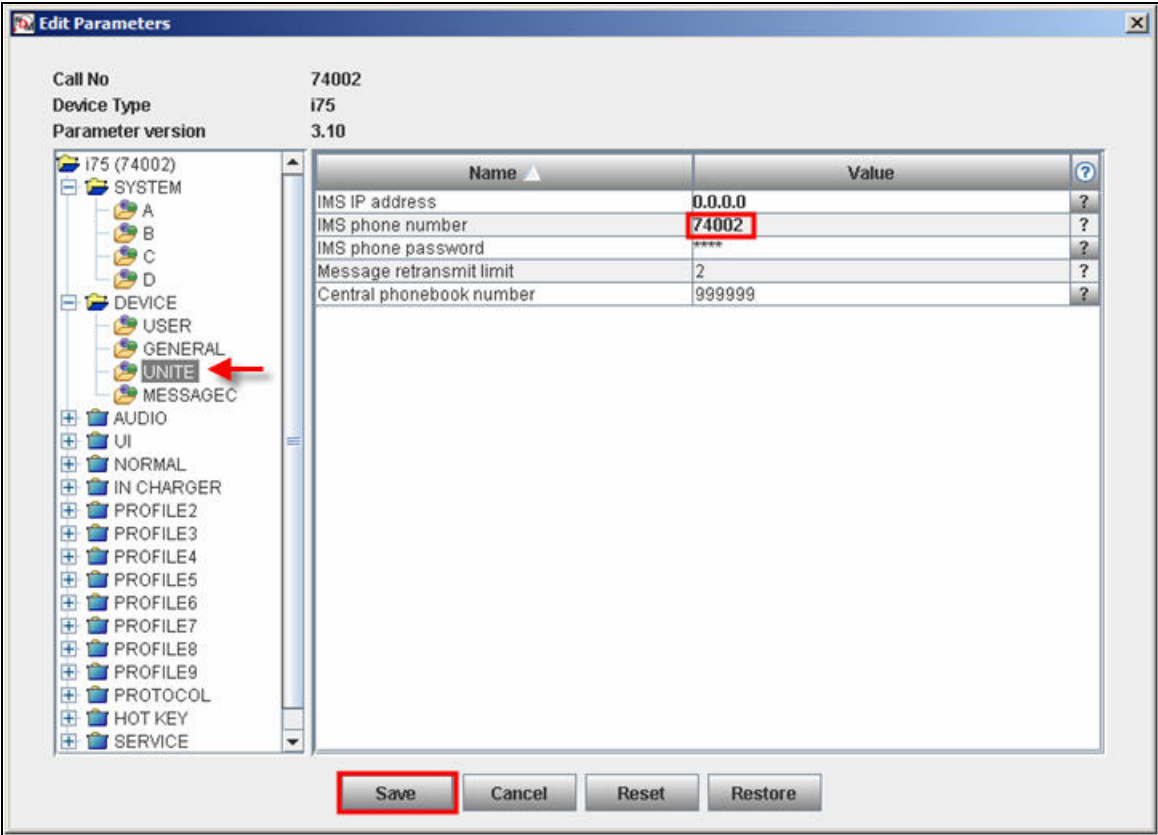
Step	Description
1.	<p>Launch the PDM application from the computer that has the application installed and has the PDM physically attached via a USB cable. Before the user is presented with the following screen a login is required. See Section 10 [3] for administration and configuration information on the PDM. After the user has logged on to the PDM the following screen is displayed which shows the devices found in the database. Since no devices have been plugged into the PDM, none are shown at this time.</p> 

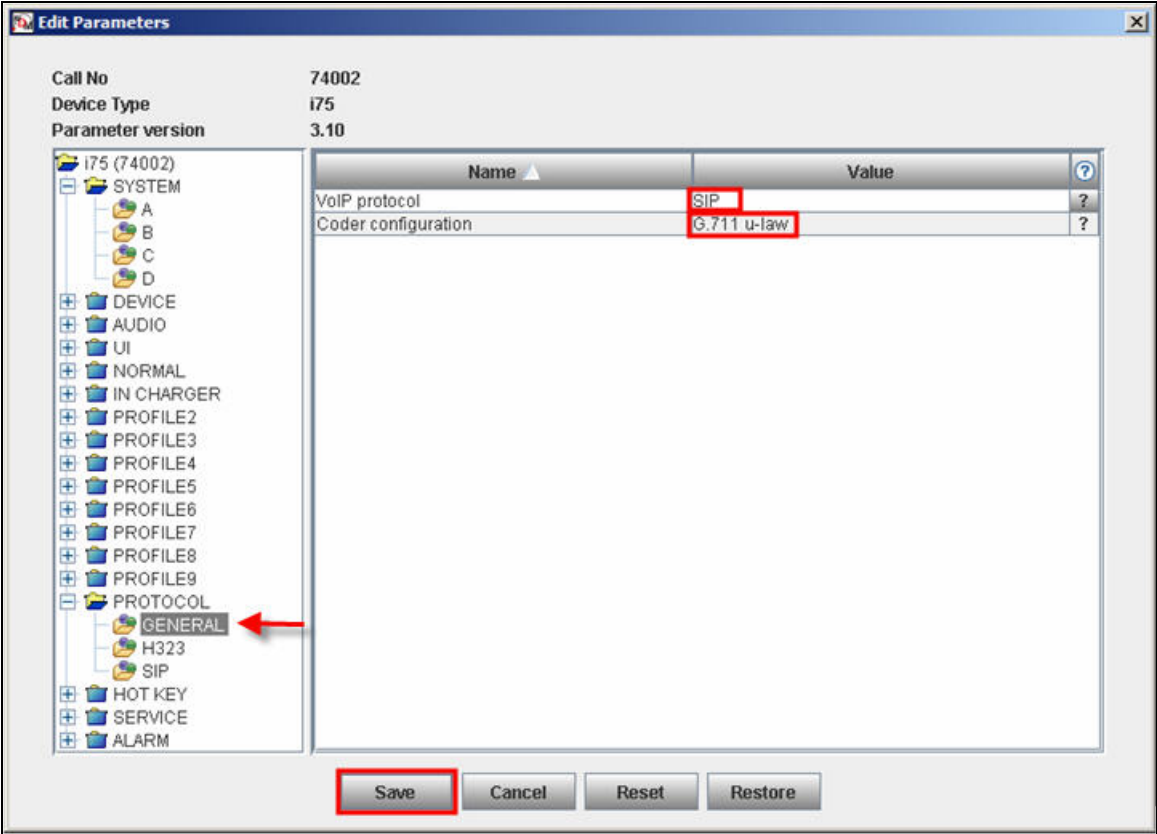
Step	Description
2.	<p>Once an Ascomwireless i75 Portable Handset is placed into the cradle the PDM recognizes the telephone and cross references the database of telephones. If the telephone is not found in the database the PDM prompts the user to save the new telephone to the database. Click the radio button labeled “Save to database” and then click “OK”.</p> 

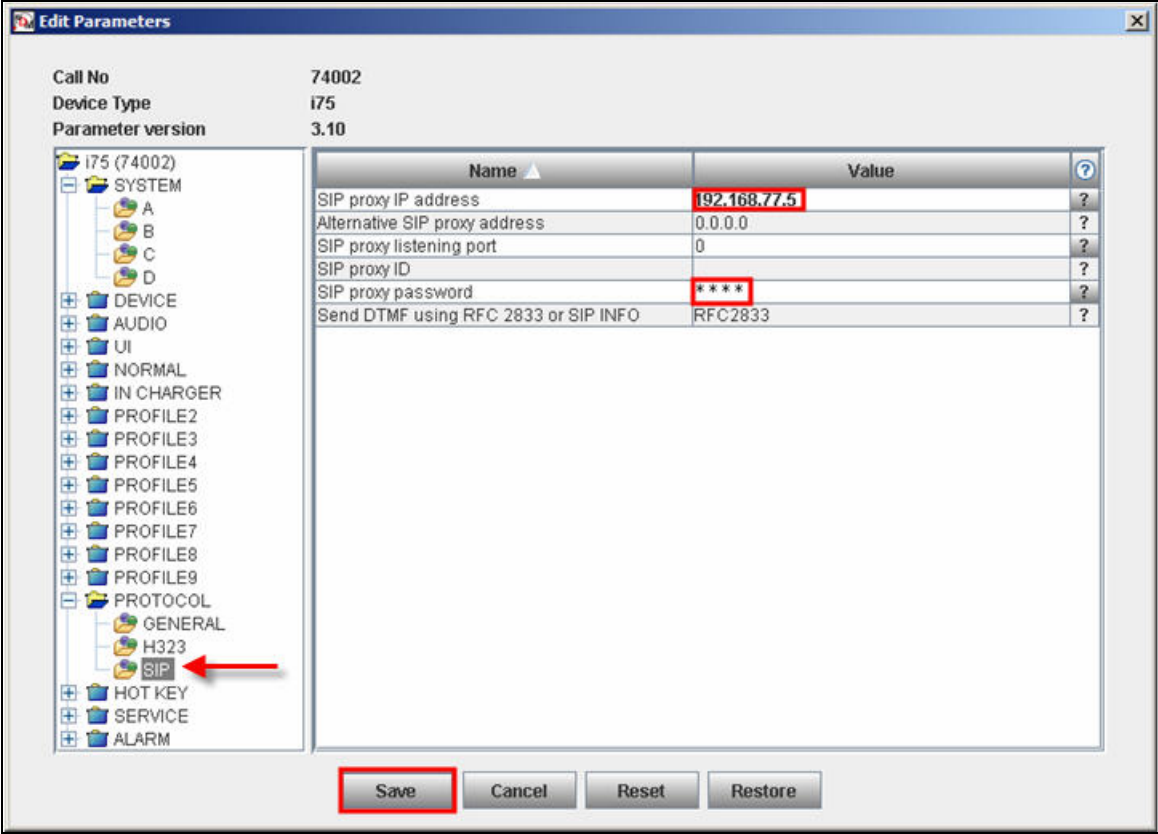
Step	Description																
3.	<p data-bbox="277 239 1479 489">Navigate to the “System A” configuration page by clicking SYSTEM and then A. From the “System A” configuration page configure the following parameters and then click “Save”. These settings should be repeated for each Ascomwireless i75 VoWiFi Handset being provisioned. The ESSID field value must match the ESSID field value specified in Section 4, Step 6. Four different security schemas were tested: None/Open, WEP-128, WPA-PSK TKIP and WPA2- CCMP-8021X. For complete details on how to configure these parameters using the PDM refer to Section 10 [3].</p> <table data-bbox="321 527 954 821"> <tr> <td>DHCP mode</td> <td>“Enable”</td> </tr> <tr> <td>ESSID</td> <td>“merusip”</td> </tr> <tr> <td>Security mode</td> <td>“Open”</td> </tr> <tr> <td>Encryption type</td> <td>“NONE”</td> </tr> <tr> <td>Network association (advanced)</td> <td>“OPEN”</td> </tr> <tr> <td>Network authentication (advanced)</td> <td>“NONE”</td> </tr> <tr> <td>EAP type (advanced)</td> <td>“NONE”</td> </tr> <tr> <td>Inner EAP type (advanced)</td> <td>“NONE”</td> </tr> </table> 	DHCP mode	“Enable”	ESSID	“merusip”	Security mode	“Open”	Encryption type	“NONE”	Network association (advanced)	“OPEN”	Network authentication (advanced)	“NONE”	EAP type (advanced)	“NONE”	Inner EAP type (advanced)	“NONE”
DHCP mode	“Enable”																
ESSID	“merusip”																
Security mode	“Open”																
Encryption type	“NONE”																
Network association (advanced)	“OPEN”																
Network authentication (advanced)	“NONE”																
EAP type (advanced)	“NONE”																
Inner EAP type (advanced)	“NONE”																

Step	Description
4.	<p>Navigate to the USER configuration page by clicking DEVICE and then USER. Configure the following parameters and then click Save. The “User ID text” field does not need to be the extension assigned to the handset. This field can hold a 32 character alpha-numeric value which can display proper names. Repeat this process for each Ascomwireless i75 VoWiFi Handset being provisioned and modify the parameters to be unique per handset.</p> <p>User ID text “74002” Endpoint number “74002” Endpoint ID “74002”</p> 

Step	Description
5.	<p>Navigate to the GENERAL configuration page by clicking DEVICE and then GENERAL. Ensure that the Replace Call Rejected with User Busy field value is set to “01” and then click “Save”. If this value is not set correctly certain calling features, such as transfer, will not operate properly. This setting should be repeated for each Ascomwireless i75 VoWiFi Handset being provisioned.</p> 

Step	Description												
6.	<p>Navigate to the UNITE configuration page by clicking DEVICE and then UNITE. Configure the following parameters and then click “Save”. The IMS phone number should be the extension associated with the Ascomwireless i75 VoWiFi Handset being provisioned. This setting should be repeated for each Ascomwireless i75 VoWiFi Handset being provisioned.</p>  <p>The screenshot shows the 'Edit Parameters' window for device i75 (74002). The 'UNITE' parameter is selected in the left tree. The 'IMS phone number' is set to 74002. The 'Save' button is highlighted.</p> <table border="1" data-bbox="625 562 1409 1163"> <thead> <tr> <th>Name</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>IMS IP address</td> <td>0.0.0.0</td> </tr> <tr> <td>IMS phone number</td> <td>74002</td> </tr> <tr> <td>IMS phone password</td> <td>*****</td> </tr> <tr> <td>Message retransmit limit</td> <td>2</td> </tr> <tr> <td>Central phonebook number</td> <td>999999</td> </tr> </tbody> </table>	Name	Value	IMS IP address	0.0.0.0	IMS phone number	74002	IMS phone password	*****	Message retransmit limit	2	Central phonebook number	999999
Name	Value												
IMS IP address	0.0.0.0												
IMS phone number	74002												
IMS phone password	*****												
Message retransmit limit	2												
Central phonebook number	999999												

Step	Description
7.	<p>Navigate to the “Protocol General” configuration page by clicking PROTOCOL and then GENERAL. Configure the following parameters and then click “Save”. These settings should be repeated for each Ascomwireless i75 VoWiFi Handset being provisioned.</p> <p>VoIP protocol “SIP” Coder configuration “G.711 u-law”</p> 

Step	Description
8.	<p>Navigate to the SIP configuration page by clicking PROTOCOL and then SIP. Configure the following information and then click “Save”. The SIP proxy password field must match the Media Server Extension password configured on Avaya SIP Enablement Services. Once the information has been configured, the PDM reports the information as ****. After clicking save, pickup the telephone from the PDM in order to reboot the handset and activate the new configuration. Repeat Steps 1 – 8 for each Ascomwireless i75 Portable Handset being provisioned, but modify the appropriate extension fields to avoid duplication.</p> <p>SIP proxy IP address “192.168.77.5” SIP proxy password “123456”</p> 

6. Interoperability Compliance Testing

The compliance testing focused on verifying interoperability of the Ascomwireless i75 VoWiFi Handset with Avaya Communication Manager, Avaya SIP Enablement Services, Avaya one-X Desktop Edition and Avaya IP Softphone. Additional testing verified proper operation between the Ascomwireless i75 VoWiFi Handset with the Avaya 4620SW, the Avaya 4625SW, the Avaya 9630 IP Telephones and the Avaya 2420 Digital Telephone. Voice mail using IA770 and voice mail MWI was tested and verified to operate correctly. Network level tests included verifying seamless roaming from access point to access point and validating Quality of Service for voice calls in a congested network.

Avaya's formal testing and Declaration of Conformity is provided only on the headsets/handsets that carry the Avaya brand or logo. Avaya may conduct testing of non-Avaya headset/handset to determine interoperability with Avaya phones. However, Avaya does not conduct the testing of non-Avaya headsets/handsets for: Acoustic Pressure, Safety, Hearing Aid Compliance, EMC regulations, or any other tests to ensure conformity with safety, audio quality, long-term reliability or any regulation requirements. As a result, Avaya makes no representations whether a particular non-Avaya headset will work with Avaya's telephones or with a different generation of the same Avaya telephone.

Since there is no industry standard for handset interfaces, different manufacturers utilize different handset/headset interfaces with their telephones. Therefore, any claim made by a headset vendor that its product is compatible with Avaya telephones does not equate to a guarantee that the headset will provide adequate safety protection or audio quality.

6.1. General Test Approach

The general test approach was to register the Ascomwireless i75 VoWiFi Handset with Avaya Communication Manager and Avaya SIP Enablement Services through the Meru Networks wireless network. Calls were made between both wired and wireless telephones and specific calling features were exercised. To validate Quality of Service, low priority background traffic was injected into the network and the Meru Networks wireless network was verified to maintain voice calls while dropping the low priority traffic. Network level tests included verifying roaming from one access point to another and validating Quality of Service for voice traffic.

6.2. Test Results

The Ascomwireless i75 VoWiFi Handset passed all test cases. Ascomwireless i75 VoWiFi Handsets were verified to successfully register with Avaya Communication Manager and Avaya SIP Enablement Services. The compliance testing also focused on verifying Quality of Service for voice traffic while low priority background traffic was competing for bandwidth. The Ascomwireless i75 VoWiFi Handset was verified to roam successfully between access points on the same network (Layer 2 roaming) and between access points on a different network (Layer 3 roaming) while maintaining voice calls. Four different security schemas were tested: Clear, WEP-128, WPA-PSK TKIP and WPA2-CCMP-802.1X. Two codecs were used for testing: G7.11MU and G.729AB. Telephone calls were verified to operate correctly with the media path direct between the telephones (shuffling enabled) and with the media path centralized through Avaya Communication Manager (shuffling disabled). Calls were maintained for durations over

one minute without degradation to voice quality. The proprietary headset for the Ascomwireless i75 VoWiFi Handset was verified to provide two-way audio. The telephony features verified to operate correctly included attended/unattended transfer, conference call participation, conference call add/drop, multiple call appearances, caller ID operation, call forwarding unconditional, call forwarding on busy, call forwarding clear, pick groups, call pickup, bridged appearances, voicemail using IA770, MWI, hold and return from hold.

7. Verification Steps

The following steps can be used to verify proper operation of the Ascomwireless i75 VoWiFi Handset.

- Ensure that the **ESSID** field value configured in **Section 4, Step 6** on the Meru Networks MC500 matches the **ESSID** field value configured in **Section 5, Step 3** on the Ascomwireless i75 VoWiFi Handset.
- Ensure that the **Replace Call Rejected with User Busy** field value specified in **Section 5, Step 5** is set to “01”. If this value is set incorrectly certain calling features such as transfer or on-hold may not operate properly.
- Ensure that the **VoIP Protocol** and **Coder configuration** field values are set correctly, see **Section 5, Step 7**.
- Ensure that the **SIP proxy IP address** and **SIP proxy password** field values are set correctly, see **Section 5, Step 8**.
- Ensure that the Ascomwireless i75 VoWiFi Handset was removed from the Portable Device Manager after completing the configuration to apply the changes and reboot the handset.
- Place calls from the Ascomwireless i75 VoWiFi Handset and verify two-way audio.
- Place a call to the Ascomwireless i75 VoWiFi Handset, allow the call to be directed to voicemail, leave a voicemail message and verify the MWI message is received.
- Using the Ascomwireless i75 VoWiFi Handset that received the voicemail, connect to the voicemail system to retrieve the voicemail and verify the MWI message clears.
- Place calls to the Ascomwireless i75 VoWiFi Handset and exercise calling features such as transfer, conference and hold.

8. Support

Technical support for the Ascomwireless i75 VoWiFi handset can be obtained through the following:

- **Phone:** 1-877-71ASCOM or 1-877-712-7266
- **Email:** techsupport@ascomwireless.com

9. Conclusion

These Application Notes demonstrate how to build a sample VoIP-enabled wireless network using the Meru Networks wireless network with the Ascomwireless i75 VoWiFi Handset. These Application Notes also demonstrate how to provide interoperability between Avaya Communication and Avaya SIP Enablement Services with the Ascomwireless i75 VoWiFi Handset.

10. Additional References

The documents referenced below were used for additional support and configuration information. The Avaya documentation was obtained from <http://support.avaya.com>. The Ascomwireless documentation was obtained from <http://www.ascomwireless.com> (access to Ascomwireless documentation may require a support account).

- [1] *Administrator Guide for Avaya Communication Manager*, May 2006, Issue 2.1, Document Number 03-300509
- [2] *Installing and Administering SIP Enablement Services R3.1.1*, August 2006, Issue 2.0, Document Number 03-600768
- [3] *Installation and Operation Manual – Portable Device Manager (PDM), Windows version*, December 2006, Version C, Document Number TD 92325GB
- [4] *User Manual Ascom i75 VoWiFi Handset*, September 2006, Version B, Document Number TD 92319GB

©2008 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 Developer*Connection* Program at devconnect@avaya.com.