Avaya Solution & Interoperability Test Lab

Application Note for Configuring the Ascom wireless i75 VoWiFi Handset with Avaya Communication Manager, Avaya SIP Enablement Services, Avaya Modular Messaging and Avaya IA 770 INTUITY AUDIX in a Converged Voice over IP and Data Network - Issue 1.0

Abstract

These Application Notes describe a solution for supporting wireless interoperability between the Ascom wireless i75 VoWiFi Handsets with Avaya Communication Manager, Avaya SIP Enablement Services, Avaya Modular Messaging and Avaya IA 770 INTUITY AUDIX in a converged Voice over IP and Data Network in. Emphasis of the testing was placed on verifying good voice quality of calls with Ascom wireless SIP handsets registered to the Avaya telephony infrastructure.

Information in these Application Notes has been obtained through Developer*Connection* compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* 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, Avaya SIP Enablement Services, Avaya Modular Messaging, Avaya IA 770 INTUITY AUDIX and Ascom wireless i75 VoWiFi SIP Handsets in a Converged Voice over IP and Data Network. 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 appearance alerting, voicemail using Avaya Modular Messaging, MWI, hold and return from hold.

The Ascom wireless i75 VoWiFi Handset is a wireless 802.11 telephone available in two versions, the Protector model and the Medic model. Both versions are robust units designed to function in tough environments. The telephones 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 Ascom wireless 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 running on an Avaya S8300 Server with an Avaya G700 Media Gateway, and Avaya S8500 server running Avaya SIP Enablement Services, Avaya Modular Messaging Server, one Avaya 9630 IP Telephone (SIP), one Avaya 9620 IP Telephone (SIP), one Avaya 2420 Digital Telephone and two Ascom wireless i75 VoWiFi SIP Handsets.

The wireless network 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.

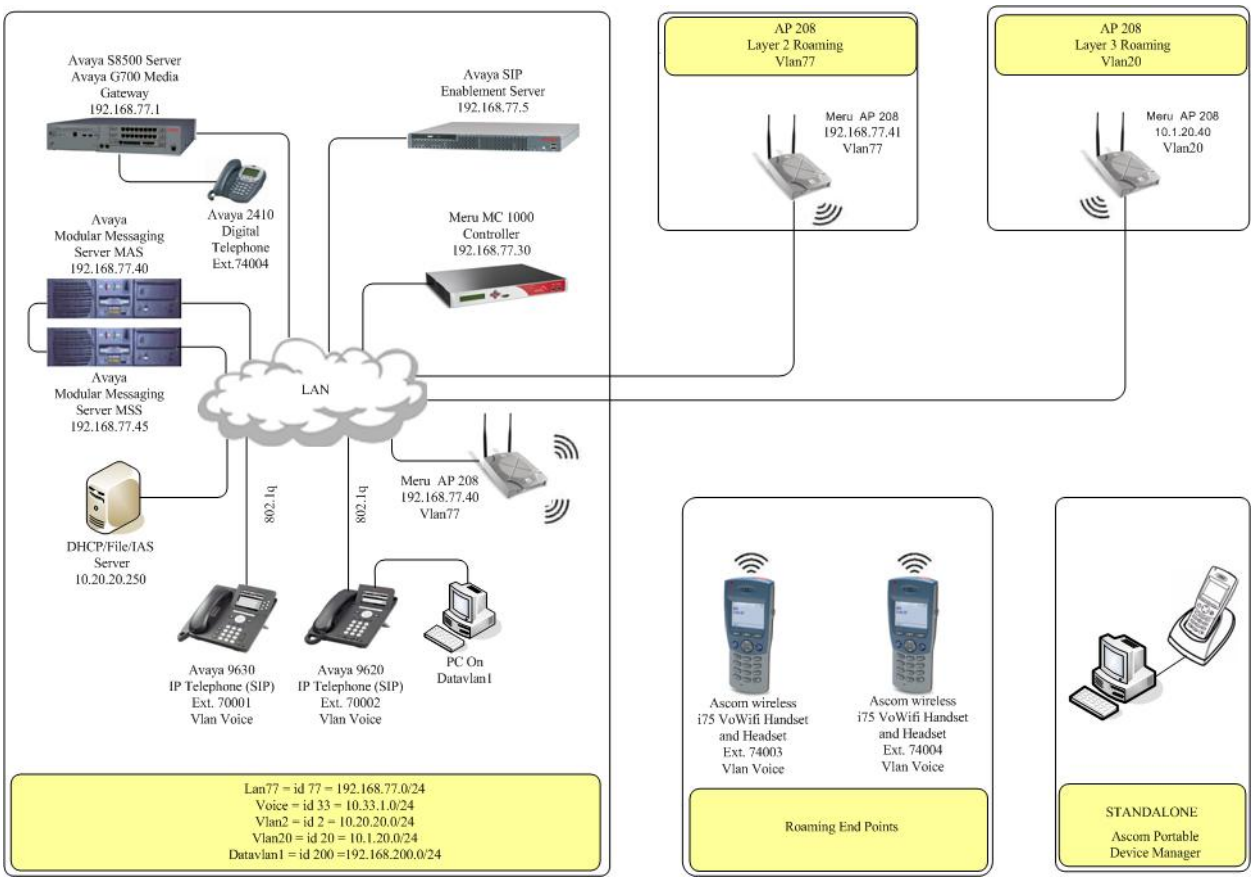


Figure 1: Sample Network Diagram for Ascom wireless i75 VoWiFi Handset with Avaya Communication Manager, Avaya SIP Enablement Services and Avaya Modular Messaging

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 5.0 - R015x.00.0.825.4
Avaya G700 Media Gateway (MM712 DCP Media Module 8)	26.31.0 HW05 / FW08
Avaya SIP Enablement Services	5.0 - SES-5.0.0.0-825.31
Avaya Modular Messaging - Messaging Application Server (MAS)	3.1
Avaya Modular Messaging - Message Storage Server (MSS)	3.1
Avaya 2420 Digital Telephone	5.0
Avaya 9600 Series IP Telephones	Avaya one-X Deskphone SIP 2.0.3 (SIP)
Avaya IA 770 INTUITY AUDIX	5.0
Ascom wireless i75 VoWiFi Handset	1.4.21 (SIP)
Ascom wireless Portable Device Manager	2.1.1
Meru Networks, MC500 Controller	3.4
Meru Networks AP208	3.4
Microsoft Windows 2003 Server DHCP Server	5.2
Microsoft Windows 2003 Server Internet Authentication Server	5.2.3790.0

3. Configure Avaya Communication Manager

Each Ascom wireless i75 VoWiFi SIP Handset configured in the sample network in **Figure 1** was administered as stations on Avaya Communication Manager with the Off-PBX stations option set. For information on how to administer these types of stations refer to **Section 10 [1]**, **[2]**, and **[3]**.

Step	Description
1.	To enable the features used for testing (Call Park, Call Park Answerback, Call Forwarding and Call Pickup) administer the configuration for Feature-Access-Codes (FAC) and Feature-Name-Extensions (FNE) on Avaya Communication Manager. 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.

```
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
```

2. From the SAT interface use the "**change off-pbx-telephone 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 recommended but 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
       61        2     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:** Configure Meru APs in the WLAN as depicted in **Figure 1**.
1.	To perform the initial configuration on the Meru Networks MC500 controller, setup a serial connection from a PC. Setup a terminal session with the following parameters: **Bits per second** **"115200"** **Data Bits** **"8"** **Parity** **"None"** **Stop bits** **"1"** **Flow control** **"None"** Log in to the Meru Networks MC500 Controller using default credentials, which can be obtained from the Meru Networks MC500 Controller documentation, and run **Setup**. Assign a hostname, IP address, DHCP Server and IP default gateway to the MC500 Controller. Default# Default# **Setup** Enter the following options when prompted: • **hostname = MC500** • **ip address = 192.168.77.30 255.255.255.0** • **ip default-gateway = 192.168.77.254** • **ip dhcp-server = 10.20.20.250**

4.1. Configure Vlans for Voice and Data

Step	**Description:** Configure Meru APs in the WLAN as depicted in Figure 1.
1.	The wireless IP endpoints that register with Avaya Communication Manager are assigned to vlan3 (Voice) and vlan200 (Data). Create two Vlans (**vlan3** and **vlan200**) with a tag of "3" and "200", respectively. Assign an IP address, default gateway, and DHCP server to the VLAN interface. This enables 802.1Q trunking on the MC500 Controller. MC500# **configure terminal** MC500(config)# MC500(config)# **vlan vlan33 tag 33** MC500(config-vlan)# **ip address 10.33.1.30 255.255.255.0** MC500(config-vlan)# **ip default-gateway 10.33.1.254** MC500(config-vlan)# **ip dhcp-server 10.20.20.250** MC500(config-vlan)# **exit** MC500# **configure terminal** MC500(config)# MC500(config)# **vlan vlan200 tag 200** MC500(config-vlan)# **ip address 192.168.200.20 255.255.255.0** MC500(config-vlan)# **ip default-gateway 192.168.200.254** MC500(config-vlan)# **ip dhcp-server 10.20.20.250** MC500(config-vlan)# **exit**

4.2. Configure Radius Server

Step	**Description:** Configure Radius Server
1.	The WPA2-CCMP-802.1X configuration in **Section 4, Step 4.5** requires a Radius Server object. MC500# MC500# **configure terminal** MC500(config)# MC500(config)# **radius-profile Radius1** MC500(config-radius)# **ip-address 10.20.20.250** MC500(config-radius)# **key meru1234** MC500(config-radius)# **port 1812** MC500(config-radius)# **mac-delimiter hyphen** MC500(config-radius)# **exit**

4.3. Configure Meru Networks AP-208 Access Points

Step	**Description:** Configure Meru APs in the WLAN as depicted in **Figure 1**.
1.	Configure Meru APs in the WLAN as depicted in **Figure 1.** **Note;** For compliance testing AP 3 was placed on Vlan20 for Layer 3 roaming. MC500# MC500# **configure terminal** MC500(config)# MC500(config)# **ap 1** MC500(config)# **description AP-1** MC500(config)# **mac-address XX:XX:XX:XX:XX:XX** MC500(config-ap)# **connectivity l3-preferred** MC500(config-ap-connectivity)#**ip address 192.168.77.40 255.255.255.0** MC500(config-ap-connectivity)# **ip default-gateway 192.168.77.1** MC500(config-ap-connectivity)# **controller ip 192.168.77.30** MC500(config-ap-connectivity)# **end** MC500# MC500# **configure terminal** MC500(config)# MC500(config)# **ap 2** MC500(config)# **description AP-2** MC500(config)# **mac-address XX:XX:XX:XX:XX:XX** MC500(config-ap)# **connectivity l3-preferred** MC500(config-ap-connectivity)#**ip address 192.168.77.41 255.255.255.0** MC500(config-ap-connectivity)# **ip default-gateway 192.168.77.1** MC500(config-ap-connectivity)# **controller ip 192.168.77.30** MC500(config-ap-connectivity)# **end** MC500# MC500# **configure terminal** MC500(config)# MC500(config)# **ap 3** MC500(config)# **description AP-3** MC500(config)# **mac-address XX:XX:XX:XX:XX:XX** MC500(config-ap)# **connectivity l3-preferred** MC500(config-ap-connectivity)#**ip address 10.1.20.40 255.255.255.0** MC500(config-ap-connectivity)# **ip default-gateway 10.1.20.1** MC500(config-ap-connectivity)# **controller ip 10.1.2.30** MC500(config-ap-connectivity)# **end**

4.4. Configure Security Profiles

Step	**Description:** Configure Security Profiles
1.	Configure the security profiles that will be assigned to the ESSID in **Section 4.5**. 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 **Section 4.5** *Clear Configuration* MC500(config)# **security-profile clear** MC500(config-security)# **allowed-l2-modes clear** MC500(config-security)# **exit** *WEP-128 Configuration* MC500(config)# **security-profile wep** MC500(config-security)# **allowed-l2-modes wep** MC500(config-security)# **encryption-modes wep128** MC500(config-security)# **start-wep key testtesttestt** MC500(config-security)# **exit** *WPA-PSK Configuration* MC500(config)# **security-profile wpa-psk** MC500(config-security)# **allowed-l2-modes wpa-psk** MC500(config-security)# **encryption-modes tkip** MC500(config-security)# **psk key testtesttest** MC500(config-security)# **exit** *WPA2-CCMP-AES-802.1X Configuration* MC500(config)# **security-profile wpa2-ccmp-8021x** MC500(config-security)# **allowed-l2-modes wpa2** MC500(config-security)# **encryption-modes ccmp** MC500(config-security)# **8021x-network-initiation** MC500(config-security)# **radius-server primary Radius1** MC500(config-security)# **exit**

4.5. Create and Configure ESSID's

Step	**Description:** Configure ESSID Profiles
1.	Create **ESSID's** and assign security profiles that were created in the previous in **Section 4.5**. *Clear Profile* MC500# **configure terminal** MC500(config)# **essid merusip** MC500(config-essid)# **security-profile clear** MC500(config-essid)# **tunnel-type configured-vlan-only** MC500(config-essid)# **ssid meru-clear** MC500(config-essid)# **vlan name vlan33** MC500(config-essid)# **ap-discovery join-virtual-ap** MC500(config-essid)# **exit** *WEP-128 profile* MC500# **configure terminal** MC500(config)# **essid meru-wep** MC500(config-essid)# **security-profile wep** MC500(config-essid)# **tunnel-type configured-vlan-only** MC500(config-essid)# **ssid meru-wep** MC500(config-essid)# **static-wep key 1234567890098** MC500(config-essid)# **vlan name vlan33** MC500(config-essid)# **ap-discovery join-virtual-ap** MC500(config-essid)# **exit** *WPA-PSK profile* MC500# **configure terminal** MC500(config)# **essid meru-wpa-psk** MC500(config-essid)# **security-profile wpa-psk** MC500(config-essid)# **tunnel-type configured-vlan-only** MC500(config-essid)# **ssid meru-wpa-psk** MC500(config-essid)# **psk key testtesttest** MC500(config-essid)# **vlan name vlan33** MC500(config-essid)# **ap-discovery join-virtual-ap** MC500(config-essid)# **exit** *WPA2-CCMP profile.* MC500# **configure terminal** MC500(config)# **essid meru-wpa2-E** MC500(config-essid)# **security-profile wpa2-ccmp-8021x** MC500(config-essid)# **tunnel-type radius-and-configured-vlan** MC500(config-essid)# **ssid meru-wpa2-E** MC500(config-essid)# **vlan name vlan33** MC500(config-essid)# **ap-discovery join-virtual-ap** MC500(config-essid)# **exit**

4.6. Configure QoS Polices

Step	**Description:** Delete QOSRULES 3 and 4
1.	The Ascom wireless 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 the Meru Networks MC500 controller need to be rebuilt (the Meru Networks MC500 does not allow the default rules to be modified). MC500(config)# **no qosrule 3** MC500(config)# **no qosrule 4** 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** 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**

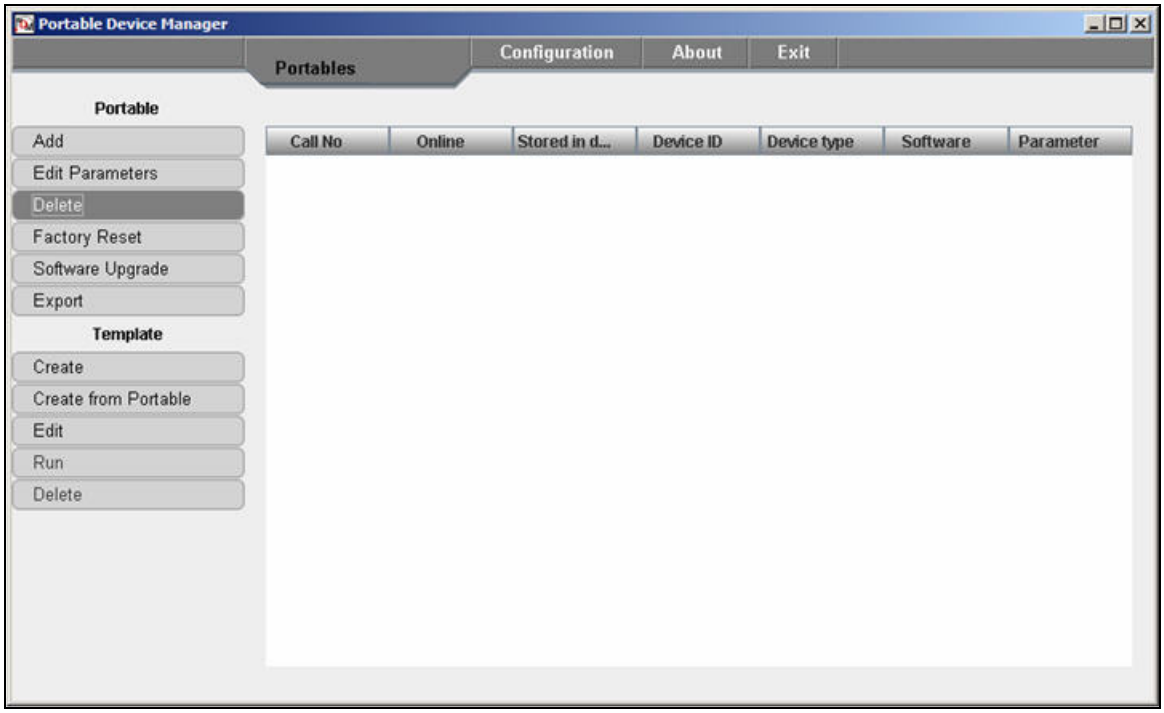
4.7. Save Configuration

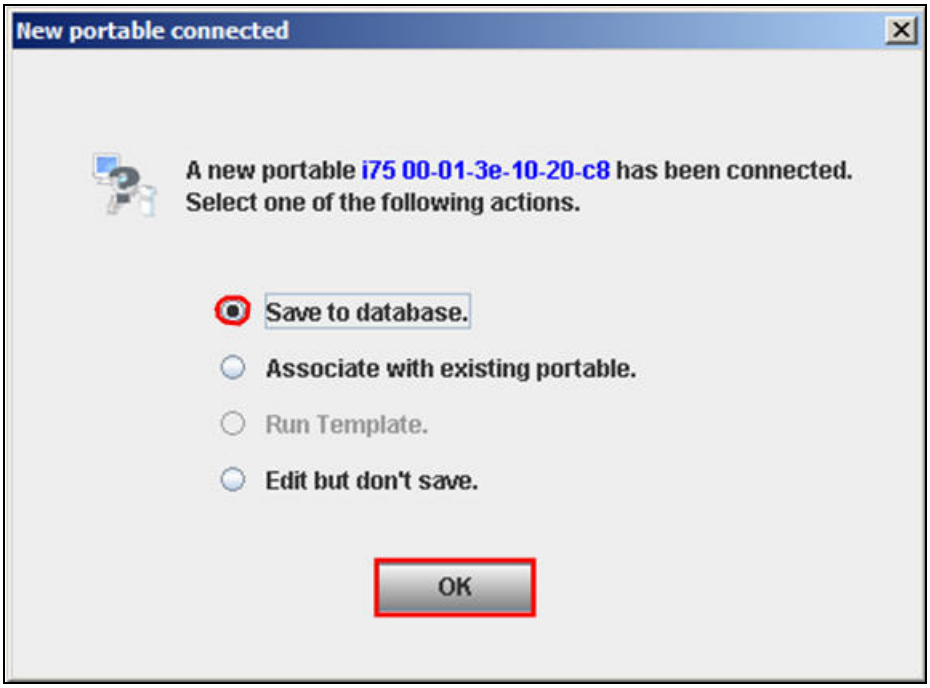
Step	**Description:** Save Configuration
1.	Save the newly configured information to the Meru Networks MC500 controller and reload it. MC500# **copy running-config startup-config** MC500# **reload all**

5. Configure the Ascom wireless i75 VoWiFi Handset

The following steps detail the configuration process for the Ascom wireless i75 VoWiFi Handset using the Ascom wireless Portable Device Manger (PDM) Windows-based application. For

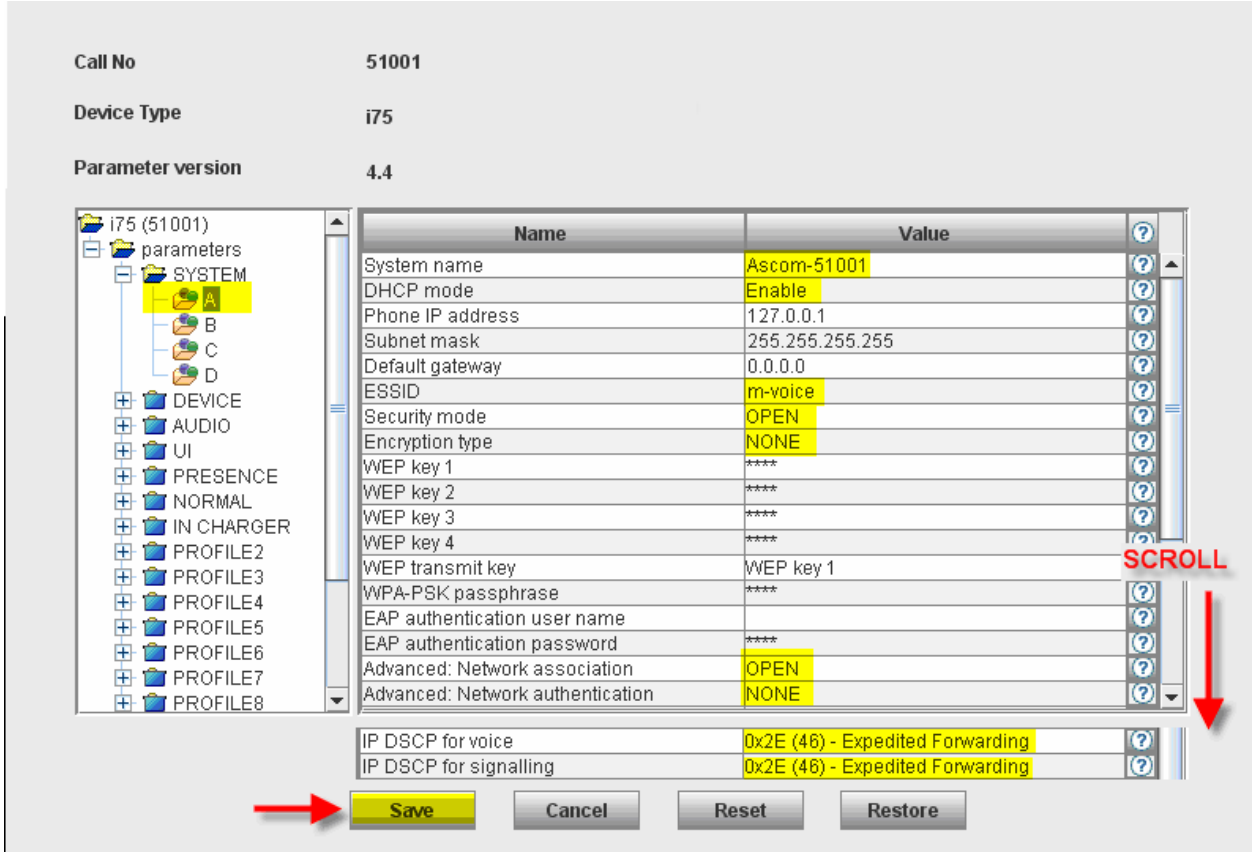
complete details on all the supported features on the Ascom wireless i75 VoWiFi Handset refer to **Section 10 [8]**.

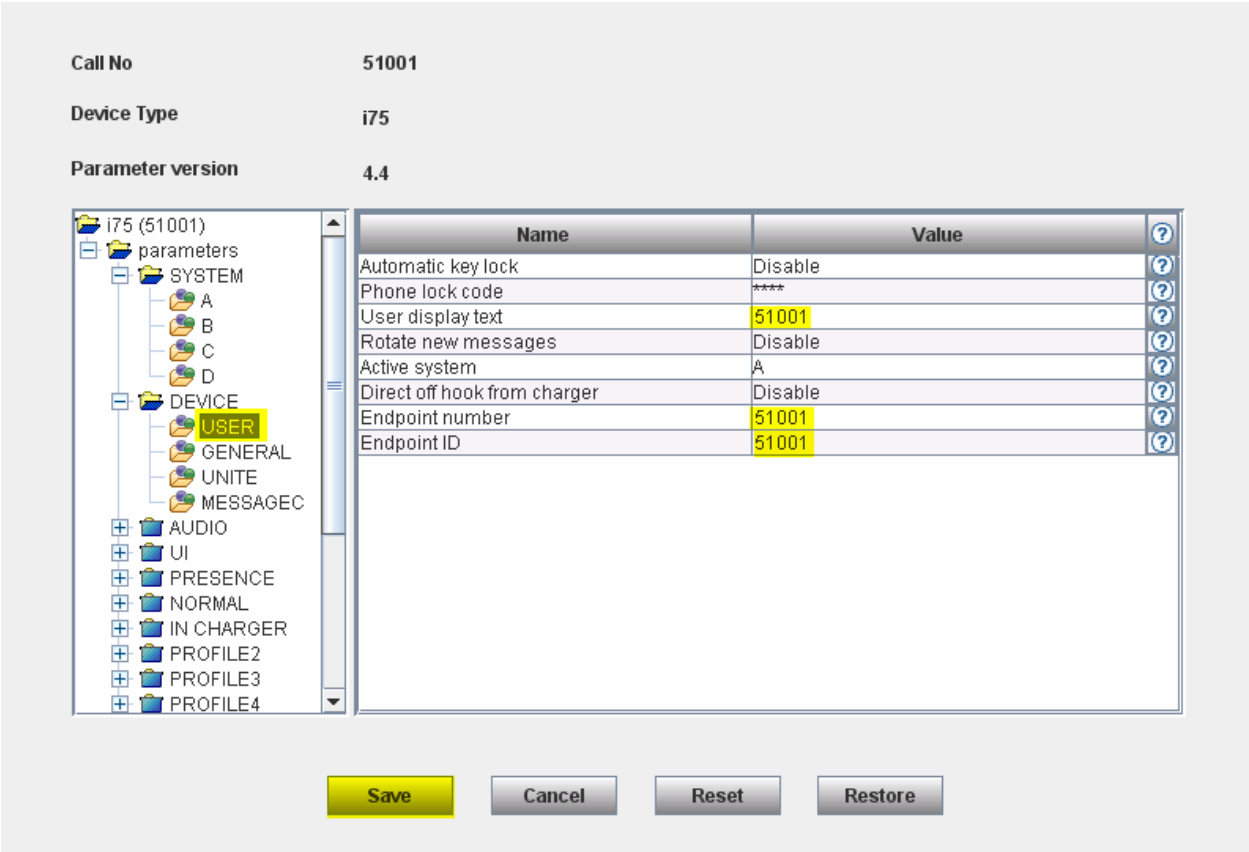
Step	Description
1.	Launch the PDM application from the computer that has the application installed and has the PDM physically attached via a USB cable. Before the user is presented with the following screen a login is required. See **Section [7]** for administration and configuration information on 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. 

Step	Description
2.	Once an Ascom wireless 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**". 

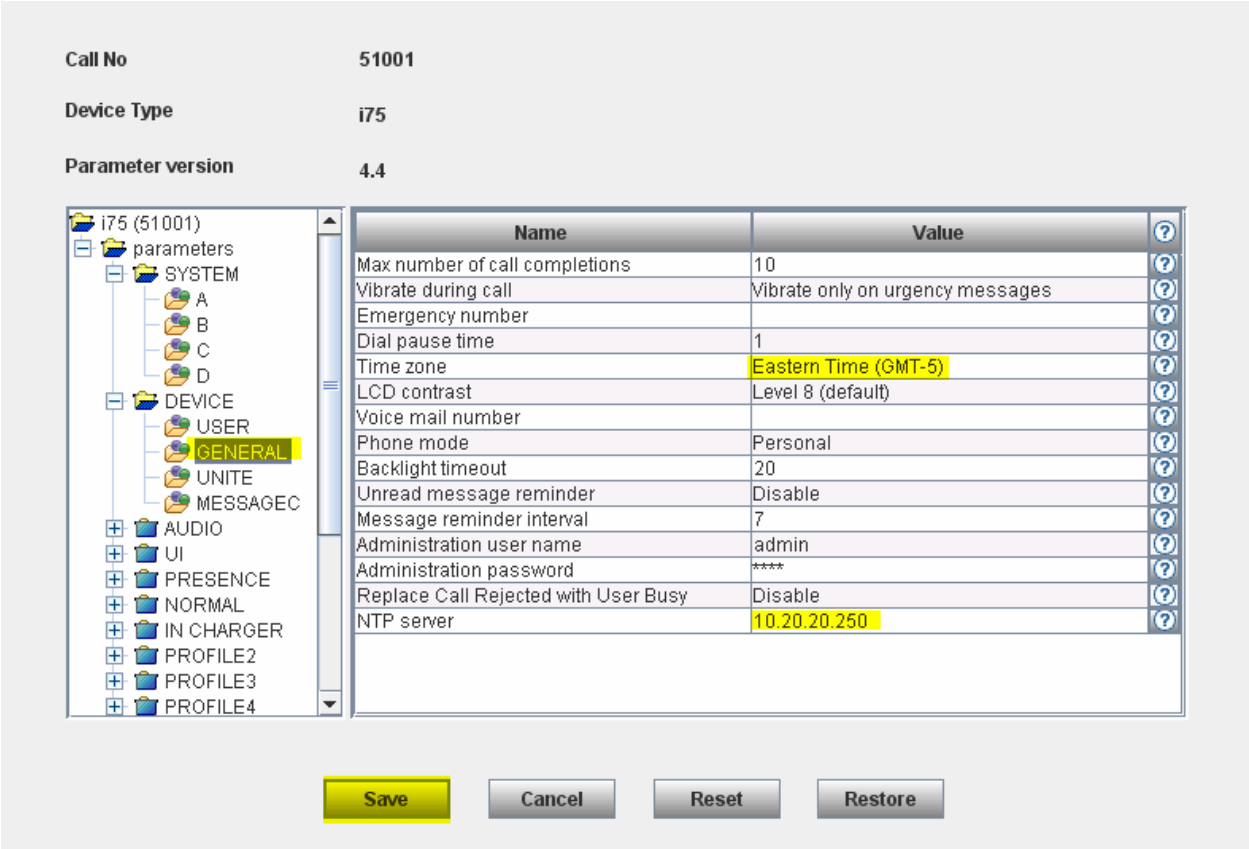
Step	Description
3.	Navigate to the "System A" configuration page by clicking **SYSTEM** and then **A**. From the "System A" configuration page configure the following parameters and then click "**Save**". These settings should be repeated for each Ascom wireless i75 VoWiFi Handset being provisioned. The **ESSID** field value must match the **ESSID** field value specified in **Section 4.5**. 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 [7]**.

System Name	**"Ascom-51001"**
DHCP mode	**"Enable"**
ESSID	**"m-voice"**
Security mode	**"Open"**
Encryption type	**"NONE"**
Advanced Network association	**"OPEN"**
Advanced Network authentication	**"NONE"**
IP DSCP for voice	**"0x2E (46) – Expedited Forwarding"**
IP DSCP for signalling	**"0x2E (46) – Expedited Forwarding"**

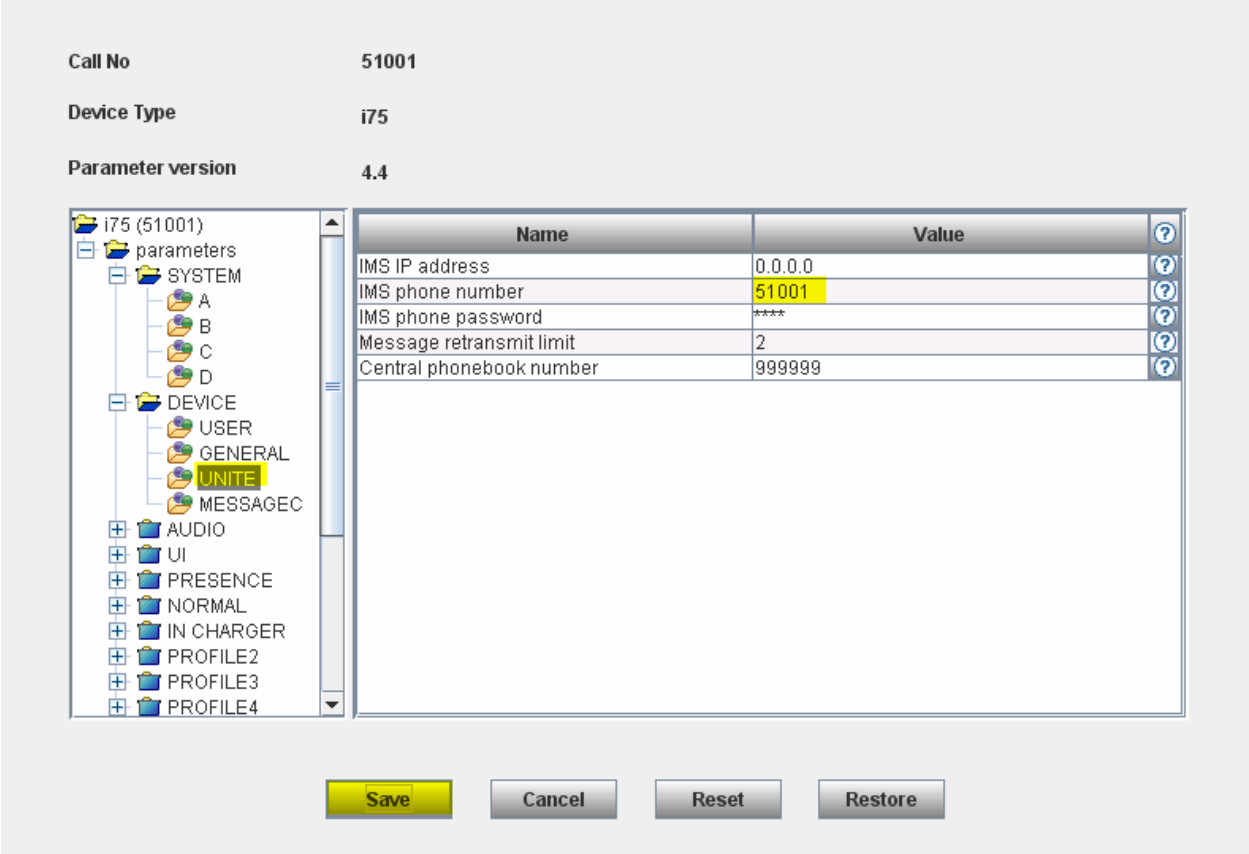


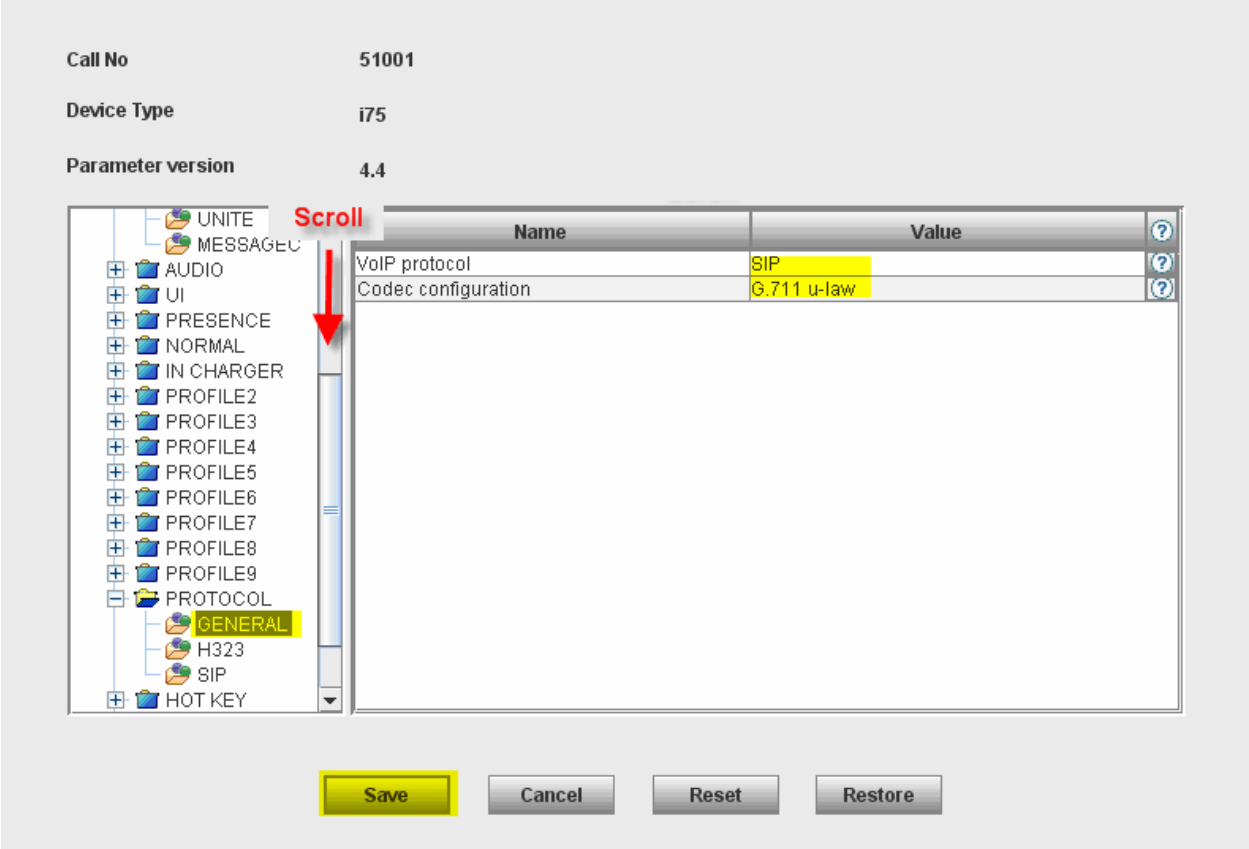
Step	Description
4.	Navigate to the **USER** configuration page by clicking **DEVICE** and then **USER**. Configure the following parameters and then click "**Save**". The **User display text** field does not need to be the extension assigned to the handset. This field can hold a 32 character alpha-numeric value which can display proper names. Repeat this process for each Ascom wireless i75 VoWiFi Handset being provisioned and modify the parameters to be unique per handset. **User display text** "51001" **Endpoint number** "51001" **Endpoint ID** "51001" 

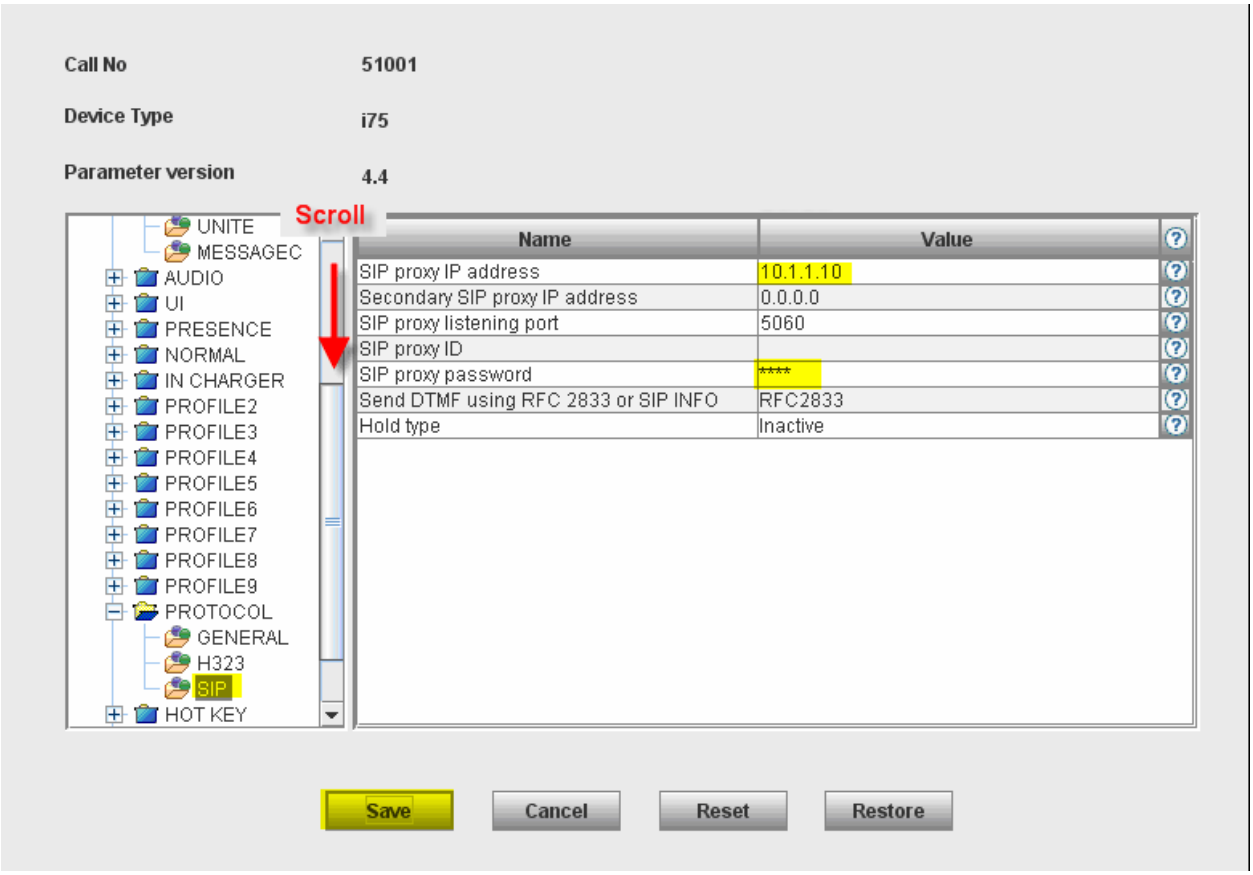
Step	Description
5.	Navigate to the **GENERAL** configuration page by clicking **DEVICE** and then **GENERAL**. Ensure that the **Time zone** and **NTP server** values are set. Click **Save** to continue.



Step	Description
6.	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 Ascom wireless i75 VoWiFi Handset being provisioned.



Step	Description
7.	Navigate to the "Protocol General" configuration page by clicking **PROTOCOL** and then **GENERAL**. Configure the following parameters and then click "**Save**". Ensure that the codec chosen matches whatever is used on Avaya Communication Manager. Click **Save** to continue. Note: G.729A codecs are set the same way. **VoIP protocol** "SIP" **Coder configuration** "G.711 u-law" 

Step	Description
8.	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 user password configured on Avaya SIP Enablement Services. Once the information has been configured, the PDM reports the information as ****. After clicking **Save**, pick up the telephone from the PDM in order to reboot the handset and activate the new configuration. Repeat **Steps 1 – 8** for each Ascom wireless i75 VoWiFi Handset being provisioned, but modify the appropriate extension fields to avoid duplication. **Note: It is recommended that the Avaya SES domain name be added to the SIP proxy ID field. This is required for systems that contain multiple SIP proxy servers.** **SIP proxy IP address** "10.1.1.10" **SIP proxy password** "123456" 

6. Interoperability Compliance Testing

The compliance testing focused on verifying interoperability of the Ascom wireless i75 VoWiFi Handset with Avaya Communication Manager, Avaya SIP Enablement Services and Avaya Modular Messaging. Additional testing verified proper operation between the Ascom wireless i75 VoWiFi Handset with the Avaya 9630 IP Telephone (SIP), Avaya 9620 IP Telephone (SIP), and the Avaya 2410 Digital Telephone. Voice mail and MWI using Avaya Modular Messaging and Avaya IA 770 INTUITY AUDIX 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 converged voice and data network configuration.

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 Ascom wireless 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, validating Quality of Service for voice traffic and verifying Avaya Modular Messaging/Avaya IA 770 INTUITY AUDIX voicemail and MWI.

6.2. Test Results

The Ascom wireless i75 VoWiFi Handset passed all test cases. Ascom wireless 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 Ascom wireless 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 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 appearance alerting, voicemail using Avaya Modular Messaging, MWI, hold and return from hold.

7. Verification Steps

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

- Ensure that the **ESSID** field value configured in **Section 4.5** on the Meru Networks MC500 matches the **ESSID** field value configured in **Section 5 Step 3** on the Ascom wireless i75 VoWiFi Handset.
- 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 Ascom wireless 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 Ascom wireless i75 VoWiFi Handset and verify two-way audio.
- Place a call to the Ascom wireless i75 VoWiFi Handset, allow the call to be directed to voicemail, leave a voicemail message and verify the MWI message is received.
- Using the Ascom wireless 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 Ascom wireless i75 VoWiFi Handset and exercise calling features such as transfer, conference and hold.

8. Support

Technical support for the Ascom wireless 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 illustrate the procedures necessary for configuring the Ascom wireless i75 VoWiFi Handset on Avaya Communication Manager, Avaya SIP Enablement Services and Avaya Modular Messaging, using a Meru Networks wireless network.

10. Additional References

Avaya documentation was obtained from http://support.avaya.com.

[1] *Administrator Guide for Avaya Communication Manager, February 2007, Issue 3.1, Document Number 03-300509*
[2] *SIP Support in Avaya Communication Manager Running on Avaya S83xx Servers, Issue 8, Doc ID 555-245-206, January, 2008*
[3] *Installing and Administering SIP Enablement Services, March 2007, Issue 2.1, Document Number 03-600768*
[4] *Avaya IA 770 INTUITY AUDIX Messaging Application Release 5.0Administering Communication Manager Servers to Work with IA 770 November 2007*
[5] *Messaging Application Server (MAS) Administration Guide Release 3.1 with the Avaya, February 2007*
[6] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide*

The Ascom wireless documentation was obtained from http://www.Ascom wireless.com.

[7] *Installation and Operation Manual – Portable Device Manager (PDM), Windows version,* December 2006, Version C, Document Number TD 92325GB
[8] *User Manual Ascom i75 VoWiFi Handset,* September 2006, Version B, Document Number TD 92319GB

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.