



**Avaya Solution & Interoperability Test Lab**

---

**Application Notes for Configuring Avaya Distributed Office  
with the Ascom i75 VoWiFi SIP Handset using the Aruba  
Networks Wireless Network - Issue 1.0**

**Abstract**

These Application Notes detail the steps for configuring interoperability between Avaya Distributed Office and Ascom i75 VoWiFi SIP Handsets. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

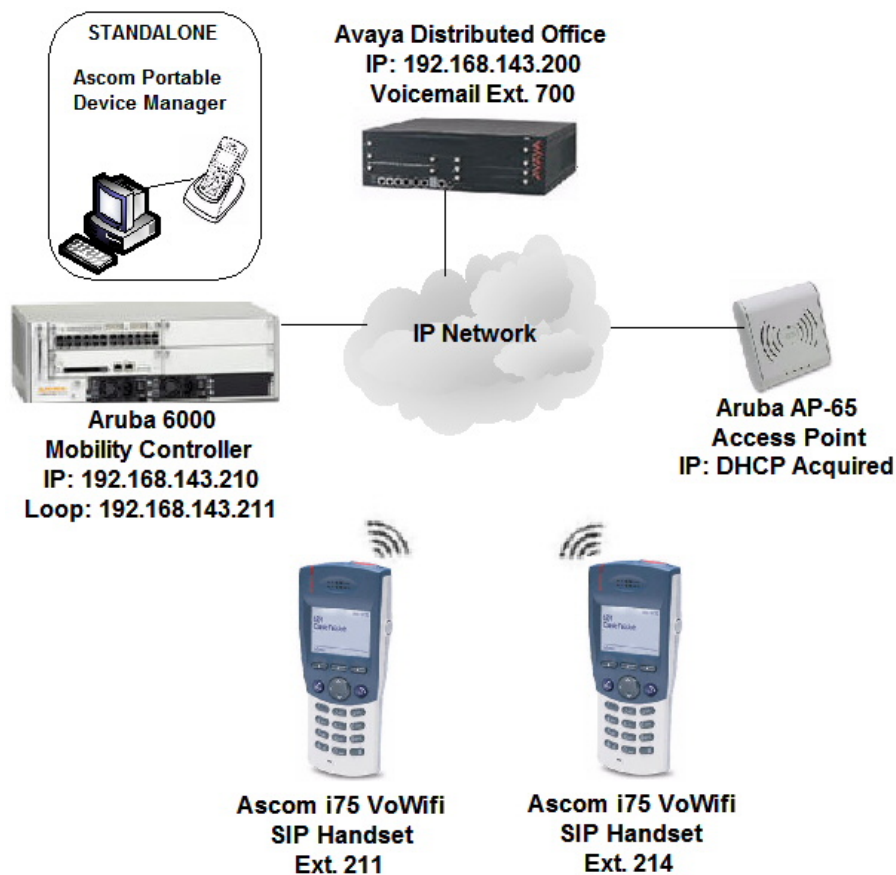
# 1. Introduction

As new products are delivered to industry, proving interoperability between both existing and new platforms is important to customers who plan on deploying new platforms. Avaya Distributed Office extends telephony features to the Ascom i75 VoWiFi SIP Handset.

These Application Notes demonstrate the configuration process that enables interoperability between the Ascom i75 VoWiFi SIP Handset with Avaya Distributed Office. The Ascom i75 VoWiFi SIP Handset is an 802.11b/g wireless SIP handset capable of registering with Avaya Distributed Office.

## 1.1. Network Diagram

The network diagram shown in **Figure 1** illustrates the testing environment used for compliance testing. The network is comprised of an Avaya Distributed Office, an Aruba 6000 Mobility Controller, an Aruba AP-65 wireless access point and two Ascom i75 VoWiFi SIP Handsets. In the sample network the Avaya Distributed Office was providing DHCP services. The standalone environment depicted illustrates that a computer running the Ascom Portable Device Manager was used to provision the Ascom i75 VoWiFi SIP Handset.



**Figure 1: Sample Network Diagram**

## 2. Equipment and Software Validated

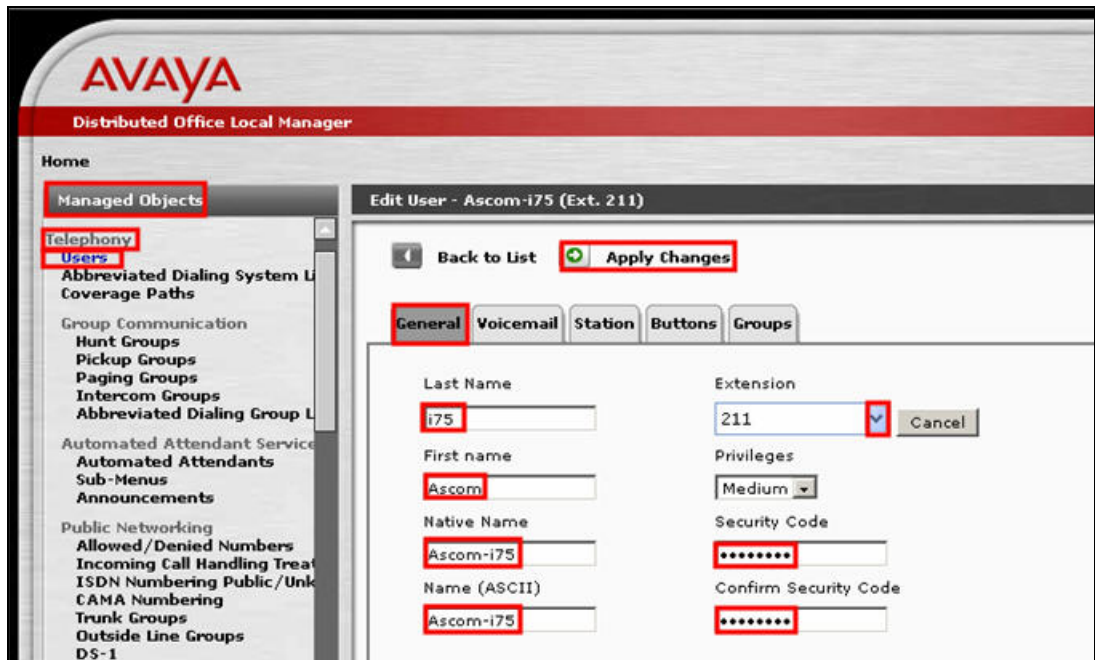
The following equipment and software were used for the sample configuration provided:

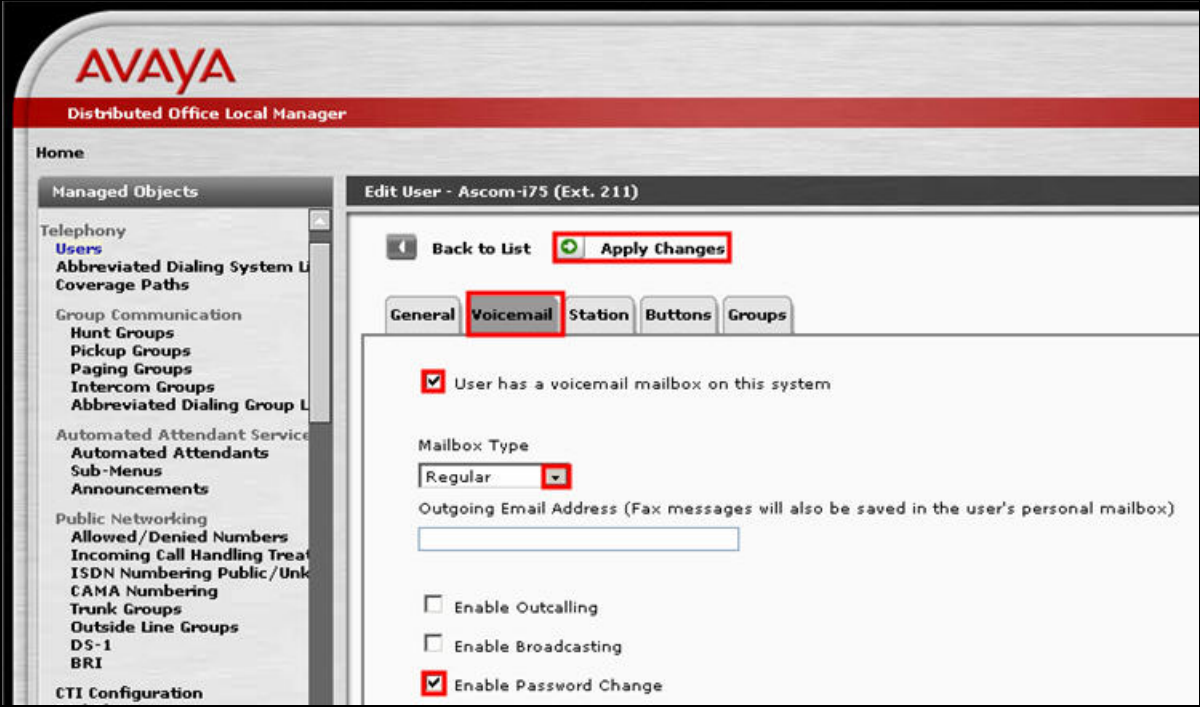
<b>Equipment</b>	<b>Software</b>
Avaya Distributed Office i120	1.1.0 (33.02) Service Pack 3.0.0
Ascom i75 VoWiFi SIP Handsets	1.4.2
Aruba 6000 Mobility Controller	3.1.0.7
Aruba AP-65 Access Point	3.1.0.7

### 3. Avaya Distributed Office Configuration

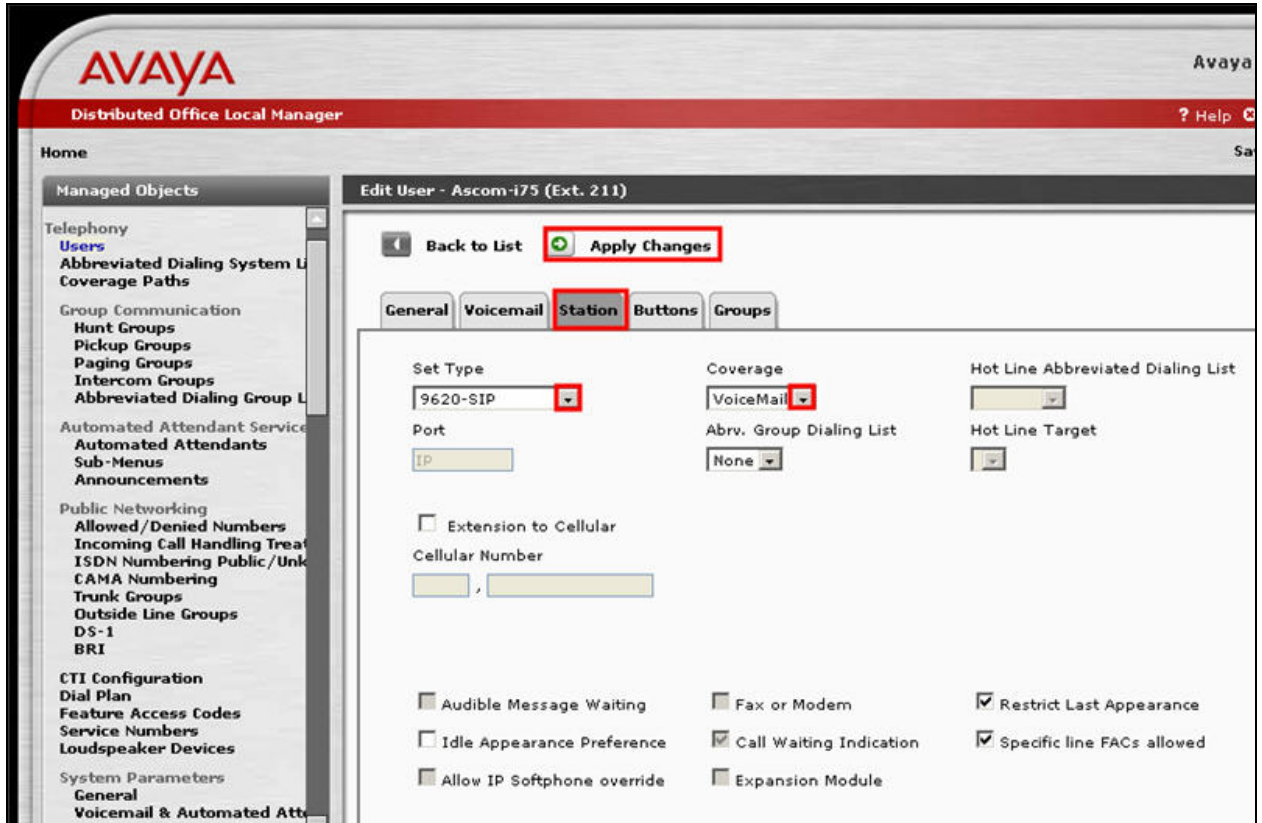
Avaya Distributed Office is administered via a web interface. In the sample network, the Avaya Distributed Office was assigned the IP address 192.168.143.200 and the URL <http://192.168.143.200> was used to access the administration interface. For information on how to access and setup a factory default system, refer to **Reference [1]**.

Step	Description
1.	<p>Navigate to the <b>Edit User</b> frame by clicking <b>Managed Object</b>→<b>Telephony</b>→<b>Users</b>. Enter the values displayed below and then click <b>Apply Changes</b>. <b>Last Name</b>, <b>First name</b> and <b>Native Name</b> can be any descriptive text that identifies this user. <b>Name (ASCII)</b> may be populated with the same information that is entered in <b>Native Name</b>. <b>Security Code</b> and <b>Confirm Security Code</b> are numeric codes that must match. Use the drop-down list for <b>Extension</b> and select any available extension. The remaining parameters were left to default values.</p>

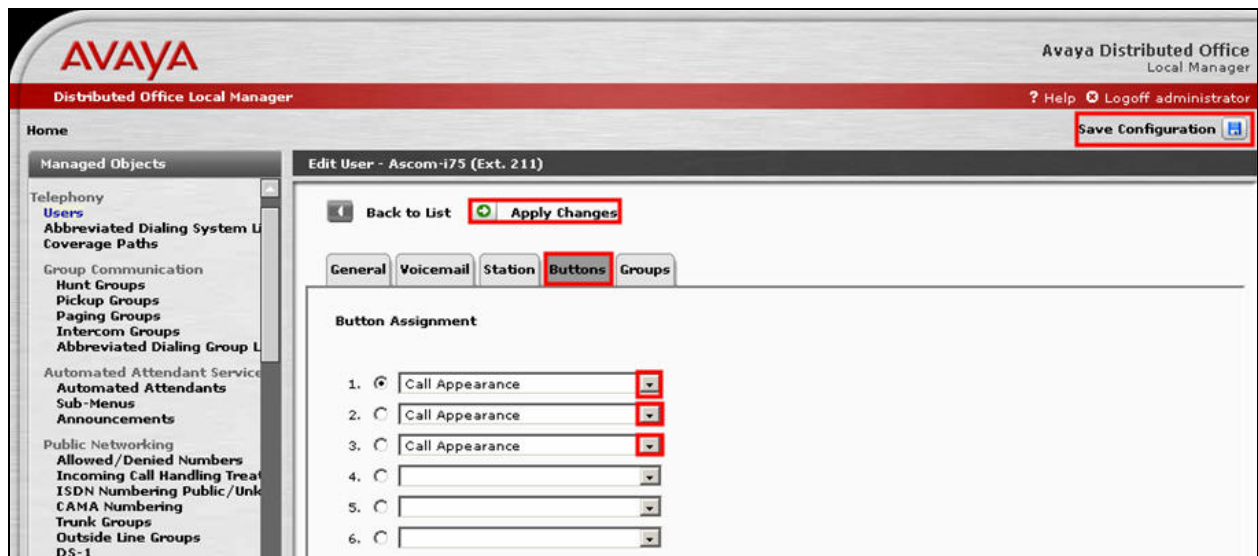


Step	Description
2.	<p>Navigate to the <b>Voicemail</b> tab by clicking <b>Voicemail</b>. Check the <b>User has a voice mailbox on this system</b> and <b>Enable Password Change</b> check boxes. Use the drop-down list for <b>Mailbox Type</b> to select “Regular”. Click <b>Apply Changes</b>.</p>  <p>The screenshot shows the Avaya Distributed Office Local Manager interface. The main content area is titled 'Edit User - Ascom-i75 (Ext. 211)'. There are two buttons at the top: 'Back to List' and 'Apply Changes'. Below these are tabs for 'General', 'Voicemail', 'Station', 'Buttons', and 'Groups'. The 'Voicemail' tab is active. In this tab, there is a checked checkbox for 'User has a voicemail mailbox on this system'. Below that is a 'Mailbox Type' dropdown menu currently set to 'Regular'. Underneath is an 'Outgoing Email Address' field. At the bottom of the tab, there are three checkboxes: 'Enable Outcalling' (unchecked), 'Enable Broadcasting' (unchecked), and 'Enable Password Change' (checked). The 'Apply Changes' button is highlighted with a red box.</p>

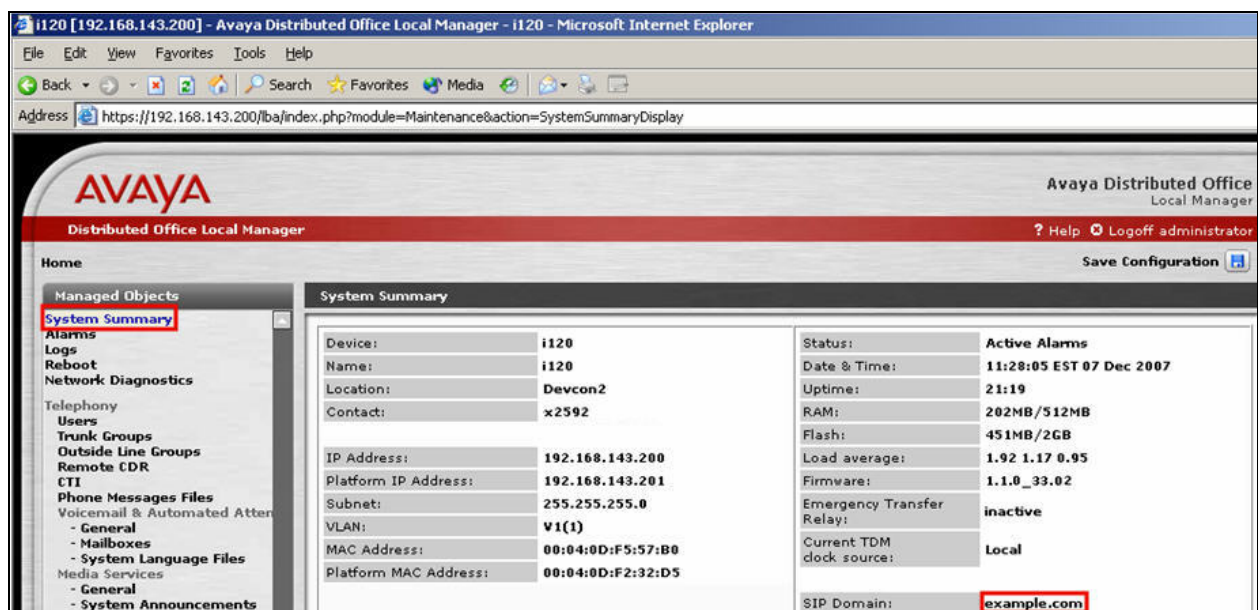
Step	Description
3.	<p>Navigate to the <b>Station</b> tab by clicking <b>Station</b>. Use the drop-down list for <b>Set Type</b> to select “9620-SIP”. This release of Avaya Distributed Office does not have a specific <b>Set Type</b> for third-party SIP telephones, therefore, the “9620-SIP” <b>Set Type</b> was used. Use the drop-down list for <b>Coverage</b> to select “VoiceMail”. The remaining parameters were left to default values. Click <b>Apply Changes</b>.</p>



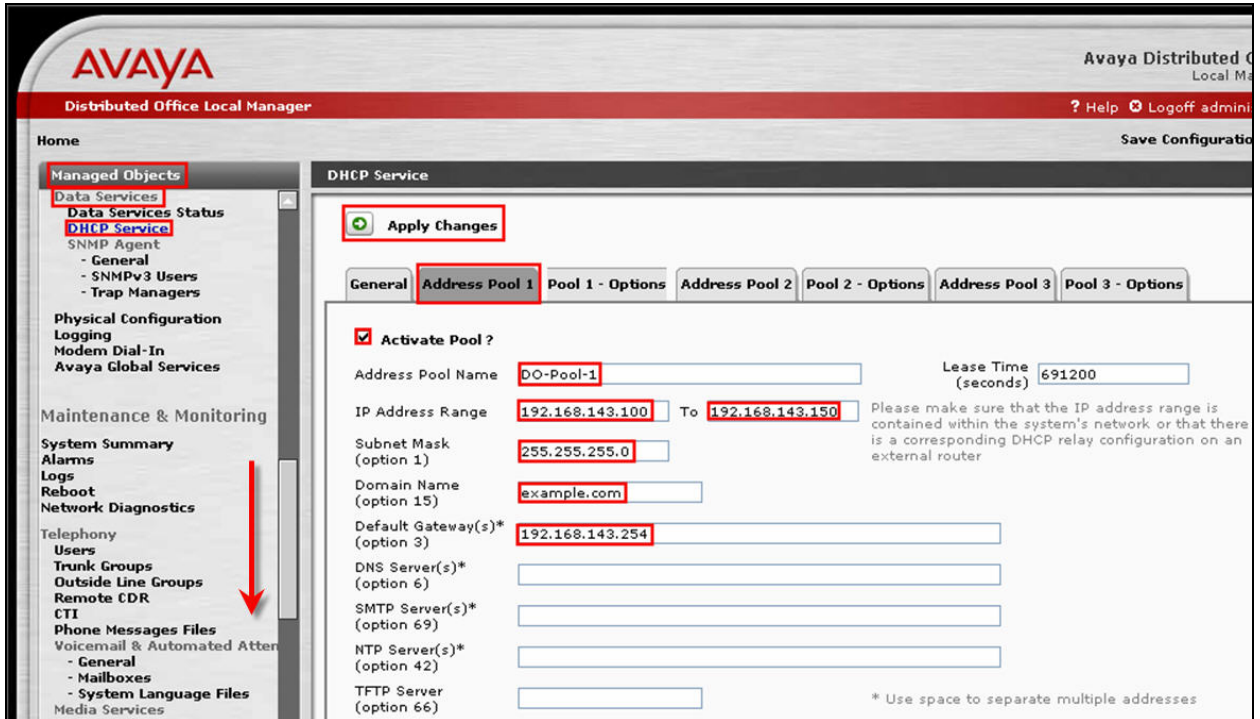
Step	Description
4.	Navigate to the <b>Buttons</b> tab by clicking <b>Buttons</b> . Use the drop list for <b>Button Assignment 1 – 3</b> and select “Call Appearance”. The remaining parameters were left to default values. Click <b>Apply Changes</b> and then click <b>Save Configuration</b> . Note the user may receive a message indicating the system is busy if <b>Save Configuration</b> is clicked immediately after <b>Apply Changes</b> . If that occurs, simply click <b>Save Configuration</b> after one or two minutes. Repeat <b>Steps 1 - 4</b> for each Ascom i75 VoWiFi SIP Handset.



5.	Navigate to the <b>System Summary</b> web page by clicking <b>System Summary</b> . There are no configurations to be made on this page. <b>SIP Domain</b> must match <b>SIP Proxy ID</b> configured in <b>Section 5, Step 6</b> . The <b>SIP Domain</b> was configured as part of the initial installation.
----	---

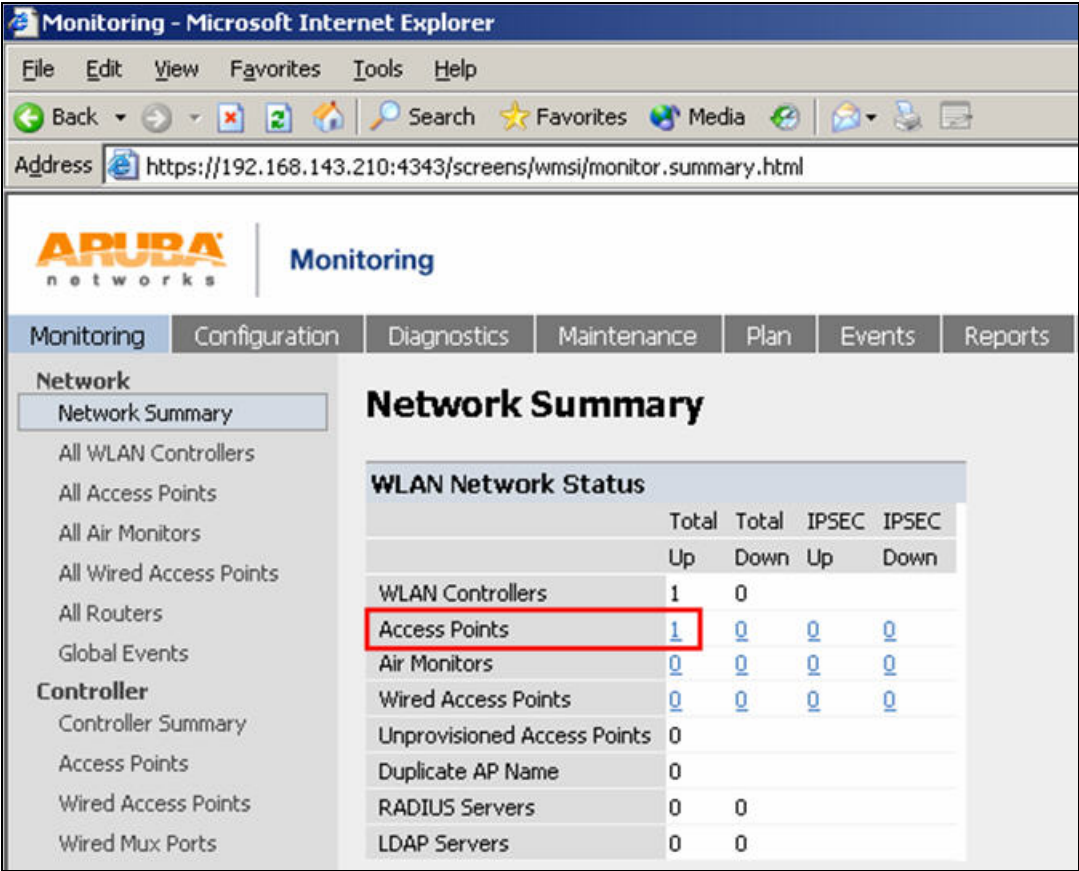


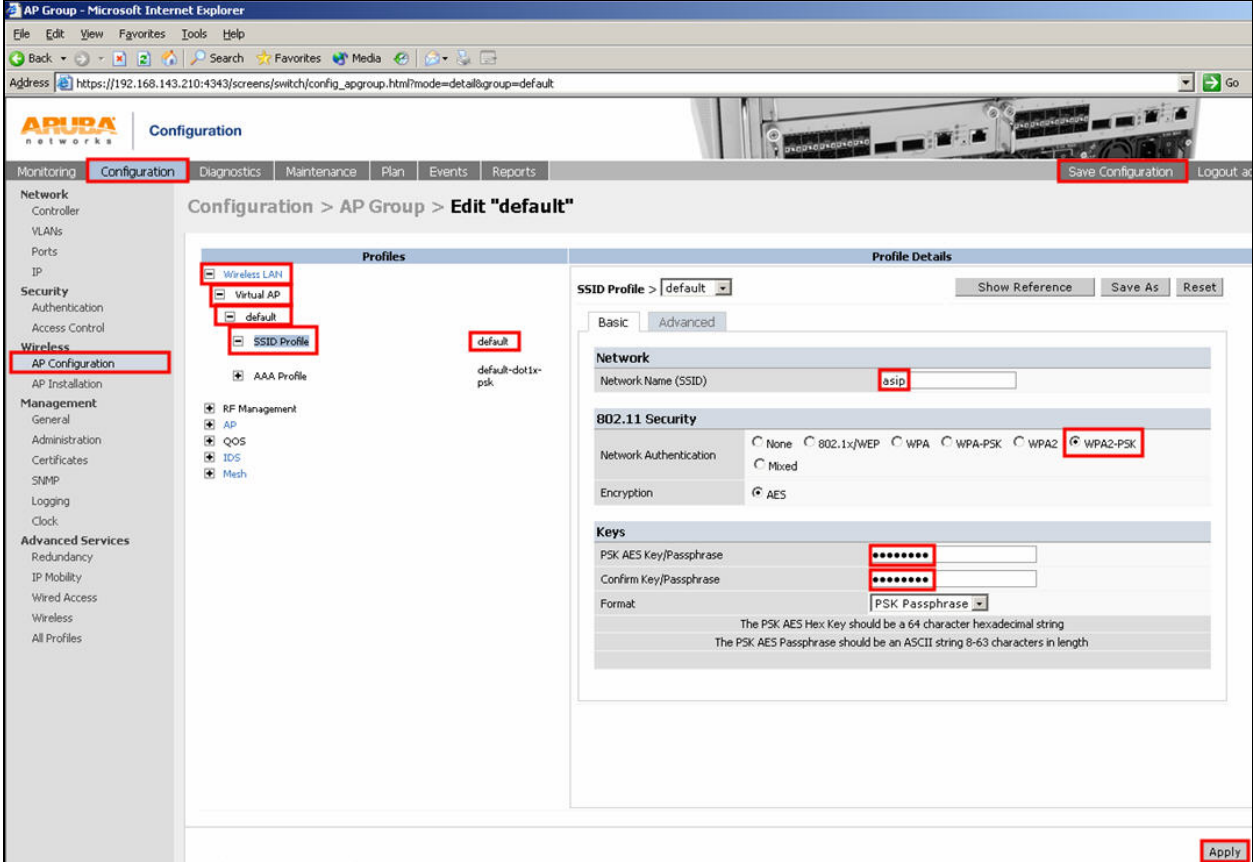
Step	Description
6.	<p>Navigate to the <b>DHCP Service</b> frame by clicking <b>Managed Objects</b>→<b>Data Services</b>→ <b>DHCP Service</b>. The user will need to use the scroll bar to navigate to this option. Then click the <b>Address Pool 1</b> tab. Enter the information displayed below and then click <b>Apply Changes</b>. Check the <b>Activate Pool?</b> check box. <b>Address Pool Name</b> can be any descriptive text. <b>IP Address Range</b> and <b>To</b> were configured to support a DHCP range from “192.168.143.100” through “192.168.143.150”. <b>Domain Name</b> was configured to “example.com”. <b>Default Gateways(s)*</b> was set to “192.168.143.254”. Note the values used here are only applicable to the sample configuration.</p>



## 4. Aruba 6000 Mobility Controller Configuration

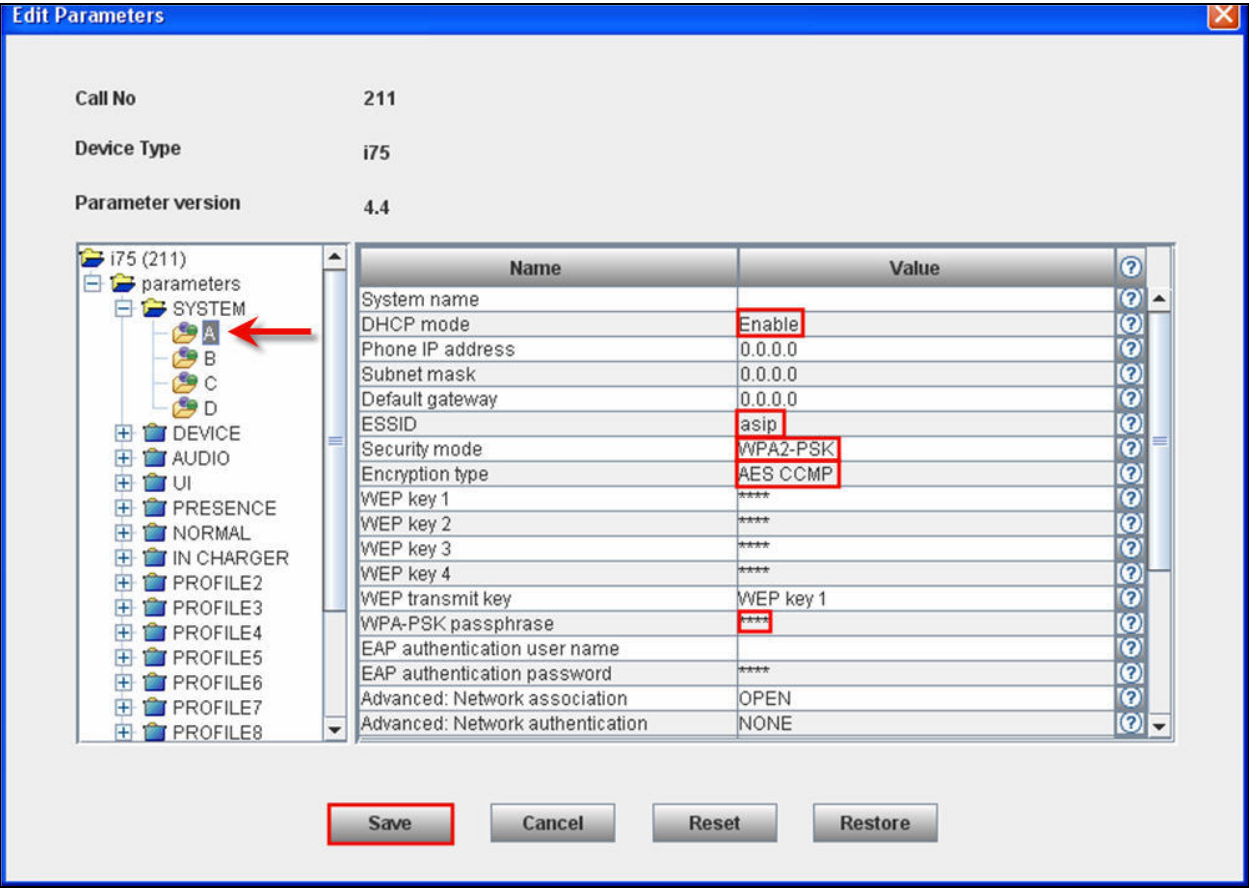
Step	Description
1.	<p>To perform the initial configuration on the Aruba 6000 Mobility Controller, setup a serial connection from a PC or laptop. Setup a terminal session with the following parameters:</p> <ul style="list-style-type: none"> <li>• 9600 baud</li> <li>• 8 bits</li> <li>• no parity</li> <li>• 1 stop bit</li> <li>• No flow control</li> </ul> <p>Log into the Aruba 6000 Mobility Controller using default credentials which can be obtained from the Aruba Networks documentation, see <b>Reference [3]</b>. Provision <b>System name, VLAN 1 interface IP address, VLAN 1 interface subnet mask, IP Default gateway, Switch Role</b> and confirm the US country code on the Aruba 6000 Mobility Controller. Once all the information has been configured, the system confirms the acceptance of these changes and requires a reboot.</p> <pre> Enter System name [Aruba6000]:Aruba6000 Enter VLAN 1 interface IP address [172.16.0.254]: 192.168.143.210 Enter VLAN 1 interface subnet mask [255.255.255.0]: 255.255.255.0 Enter IP Default gateway [none]: 192.168.143.254 Enter Switch Role, (master local) [master]: master This controller is restricted to Country code US for United States, please confirm (yes no)?: yes  Do you wish to shutdown all the ports (yes no)? [no]: no  If you accept the changes the switch will restart! Type &lt;ctrl-P&gt; to go back and change answer for any question Do you wish to accept the changes (yes no) yes  System will now restart! </pre>
2.	<p>After the Aruba 6000 Mobility Controller has rebooted, the switch port and loopback can be configured as shown below.</p> <pre> (Aruba6000) #configure t Enter Configuration commands, one per line. End with CNTL/Z  (Aruba6000) (config) #interface loopback (Aruba6000) (config-loop)#ip address 192.168.143.211 Switch IP Address is Modified. Switch should be rebooted now  (Aruba6000) (config) #interface fastethernet 3/0 (Aruba6000) (config-if)#switchport mode access (Aruba6000) (config-if)#switchport access vlan 1 (Aruba6000) (config-if)#end  (Aruba6000) #write mem Saving Configuration...  Configuration Saved.  (Aruba6000) #reload Do you really want to reset the system(y/n): y System will now restart! </pre>

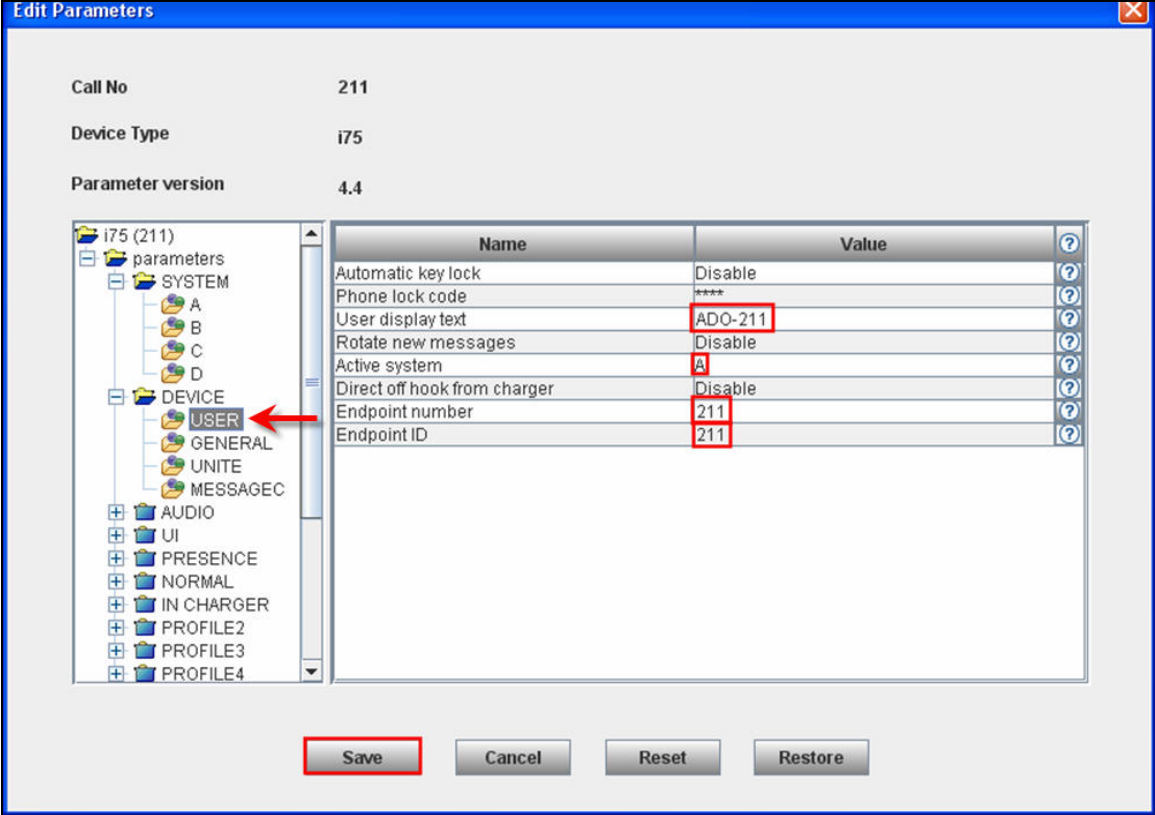
Step	Description																																																	
3.	<p>Once the Aruba 6000 Mobility Controller has rebooted, open a web browser connection to any IP of the IP addresses assigned to the Aruba 6000 Mobility Controller. In the sample network, <a href="http://192.168.143.210">http://192.168.143.210</a> was used to access the Aruba 6000 Mobility Controller web interface. Appropriate login credentials are required in order to access the web interface, refer to <b>Reference [3]</b>. Once logged on, the user is presented with the <b>Monitoring</b> web page. This page can be used to quickly ascertain the state of Aruba access points.</p>  <p>The screenshot shows the Aruba Monitoring web interface in Microsoft Internet Explorer. The address bar displays <a href="https://192.168.143.210:4343/screens/wmsj/monitor.summary.html">https://192.168.143.210:4343/screens/wmsj/monitor.summary.html</a>. The page title is "Monitoring - Microsoft Internet Explorer". The navigation menu includes "Monitoring", "Configuration", "Diagnostics", "Maintenance", "Plan", "Events", and "Reports". The "Monitoring" section is expanded, showing "Network Summary" as the selected option. The "Network Summary" page displays the "WLAN Network Status" table, which is summarized below:</p> <table border="1" data-bbox="727 947 1323 1346"> <thead> <tr> <th rowspan="2"></th> <th colspan="2">Total</th> <th colspan="2">IPSEC</th> </tr> <tr> <th>Up</th> <th>Down</th> <th>Up</th> <th>Down</th> </tr> </thead> <tbody> <tr> <td>WLAN Controllers</td> <td>1</td> <td>0</td> <td></td> <td></td> </tr> <tr> <td><b>Access Points</b></td> <td><b>1</b></td> <td><b>0</b></td> <td><b>0</b></td> <td><b>0</b></td> </tr> <tr> <td>Air Monitors</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Wired Access Points</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Unprovisioned Access Points</td> <td>0</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Duplicate AP Name</td> <td>0</td> <td></td> <td></td> <td></td> </tr> <tr> <td>RADIUS Servers</td> <td>0</td> <td>0</td> <td></td> <td></td> </tr> <tr> <td>LDAP Servers</td> <td>0</td> <td>0</td> <td></td> <td></td> </tr> </tbody> </table>		Total		IPSEC		Up	Down	Up	Down	WLAN Controllers	1	0			<b>Access Points</b>	<b>1</b>	<b>0</b>	<b>0</b>	<b>0</b>	Air Monitors	0	0	0	0	Wired Access Points	0	0	0	0	Unprovisioned Access Points	0				Duplicate AP Name	0				RADIUS Servers	0	0			LDAP Servers	0	0		
	Total		IPSEC																																															
	Up	Down	Up	Down																																														
WLAN Controllers	1	0																																																
<b>Access Points</b>	<b>1</b>	<b>0</b>	<b>0</b>	<b>0</b>																																														
Air Monitors	0	0	0	0																																														
Wired Access Points	0	0	0	0																																														
Unprovisioned Access Points	0																																																	
Duplicate AP Name	0																																																	
RADIUS Servers	0	0																																																
LDAP Servers	0	0																																																

Step	Description
4.	<p>Navigate to the <b>AP Group</b> web page by clicking <b>Configuration→AP Configuration→Wireless LAN→Virtual AP→default→SSID Profile→default</b>. Enter the information displayed below, click <b>Apply</b>, and then click <b>Save Configuration</b>. <b>Network Name (SSID)</b> can be any alphanumeric string, in the sample network “asip” was used. Click the “WPA2-PSK” button, which automatically selects “AES” as the <b>Encryption</b>. <b>PSK AES Key/Passphrase</b> and <b>Confirm Key/Passphrase</b> can be any alpha numeric string and must match. The values configured here for the wireless network will need to match those configured in <b>Section 5, Step 1</b>. For complete information on all of the encryption schemas supported by the Aruba 6000 Mobility Controller and their configurations refer to <b>Reference [3]</b>.</p> 

## 5. Ascom i75 VoWiFi SIP Handset Configuration

The Ascom i75 VoWiFi SIP Handset was configured using the Ascom Portable Device Manager (PDM). The Ascom PDM is a Windows-based application that uses a USB connection to configure the Ascom i75 VoWiFi SIP Handsets. For complete information on how to administer the Ascom i75 VoWiFi SIP Handset, refer to **Reference [2]**.

Step	Description															
1.	<p>Navigate to the “System A” configuration page by clicking <b>parameters</b>→<b>SYSTEM</b>→<b>A</b>. The Ascom i75 VoWiFi SIP Handset supports four configuration profiles labeled “A, B, C, D”. “System A” is the first configuration profile. Enter the information displayed below and then click <b>Save</b>. The values configured here must match the values configured in <b>Section 4, Step 4</b>.</p> <table> <tr> <td><b>DHCP mode</b></td> <td>“Enable”</td> <td></td> </tr> <tr> <td><b>ESSID</b></td> <td>“asip”</td> <td><b>Network Name (SSID), Section 4, Step 4</b></td> </tr> <tr> <td><b>Security mode</b></td> <td>“WPA2-PSK”</td> <td><b>Network Authentication, Section 4, Step 4</b></td> </tr> <tr> <td><b>Encryption type</b></td> <td>“AES CCMP”</td> <td><b>Encryption, Section 4, Step 4</b></td> </tr> <tr> <td><b>WPA-PSK passphrase</b></td> <td>“XXXX”</td> <td><b>PSK AES Key/Passphrase, Section 4, Step 4</b></td> </tr> </table> 	<b>DHCP mode</b>	“Enable”		<b>ESSID</b>	“asip”	<b>Network Name (SSID), Section 4, Step 4</b>	<b>Security mode</b>	“WPA2-PSK”	<b>Network Authentication, Section 4, Step 4</b>	<b>Encryption type</b>	“AES CCMP”	<b>Encryption, Section 4, Step 4</b>	<b>WPA-PSK passphrase</b>	“XXXX”	<b>PSK AES Key/Passphrase, Section 4, Step 4</b>
<b>DHCP mode</b>	“Enable”															
<b>ESSID</b>	“asip”	<b>Network Name (SSID), Section 4, Step 4</b>														
<b>Security mode</b>	“WPA2-PSK”	<b>Network Authentication, Section 4, Step 4</b>														
<b>Encryption type</b>	“AES CCMP”	<b>Encryption, Section 4, Step 4</b>														
<b>WPA-PSK passphrase</b>	“XXXX”	<b>PSK AES Key/Passphrase, Section 4, Step 4</b>														

Step	Description
2.	<p>Navigate to the <b>USER</b> configuration page by clicking <b>DEVICE</b>→<b>USER</b>. Enter the information displayed below and click <b>Save</b>. <b>User display text</b> can be any descriptive text that will be displayed on the LCD of the Ascom i75 VoWiFi SIP Handset. <b>Active System</b> indicates which configuration profile will be used, A was chosen in <b>Step 1</b>. <b>Endpoint number</b> and <b>Endpoint ID</b> are the extension assigned to the Ascom i75 VoWiFi SIP Handset, see <b>Section 3, Step 1</b>.</p> <p><b>User display text</b>            “ADO-211”  <b>Active system</b>                “A”  <b>Endpoint number</b>            “211”  <b>Endpoint ID</b>                 “211”</p> 

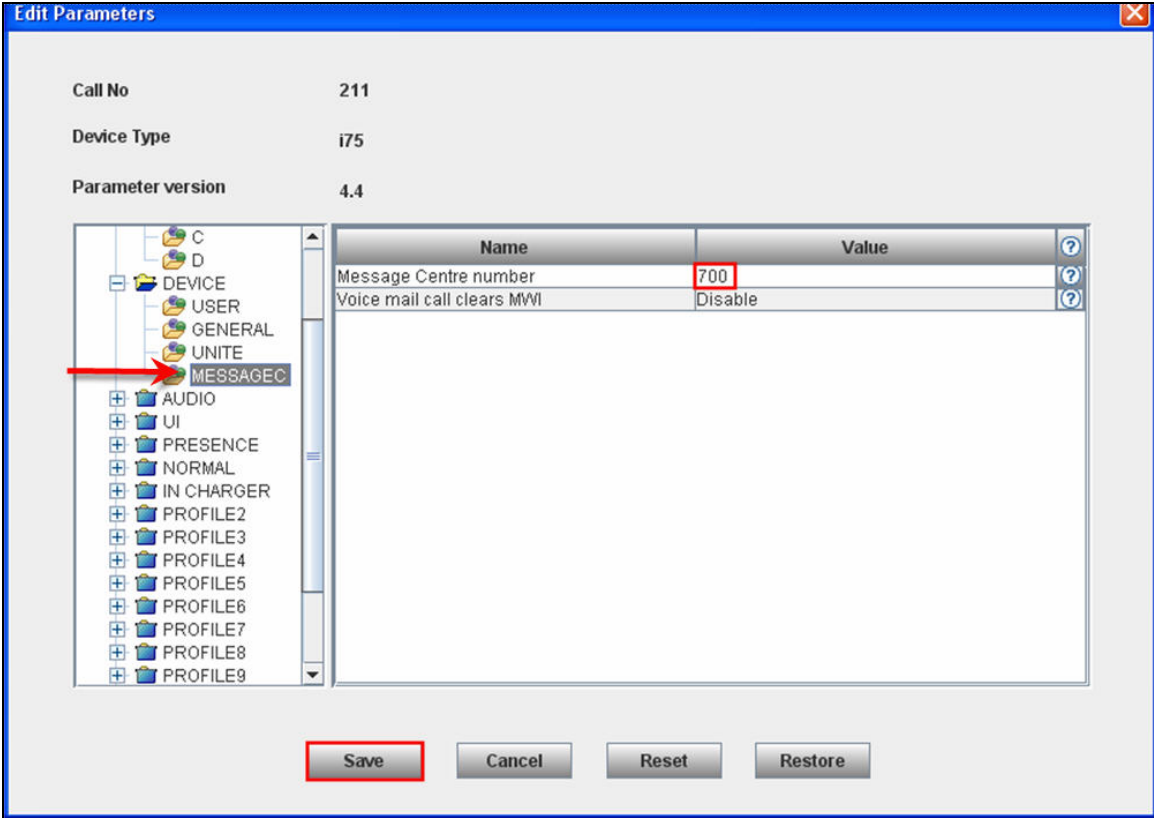
Step	Description
3.	<p>Navigate to the <b>GENERAL</b> configuration page by clicking <b>GENERAL</b>. Enter the information displayed below and then click <b>Save</b>. The <b>Replace Call Rejected with User Busy</b> field needs to be enabled in order for certain calling features to operate correctly.</p>

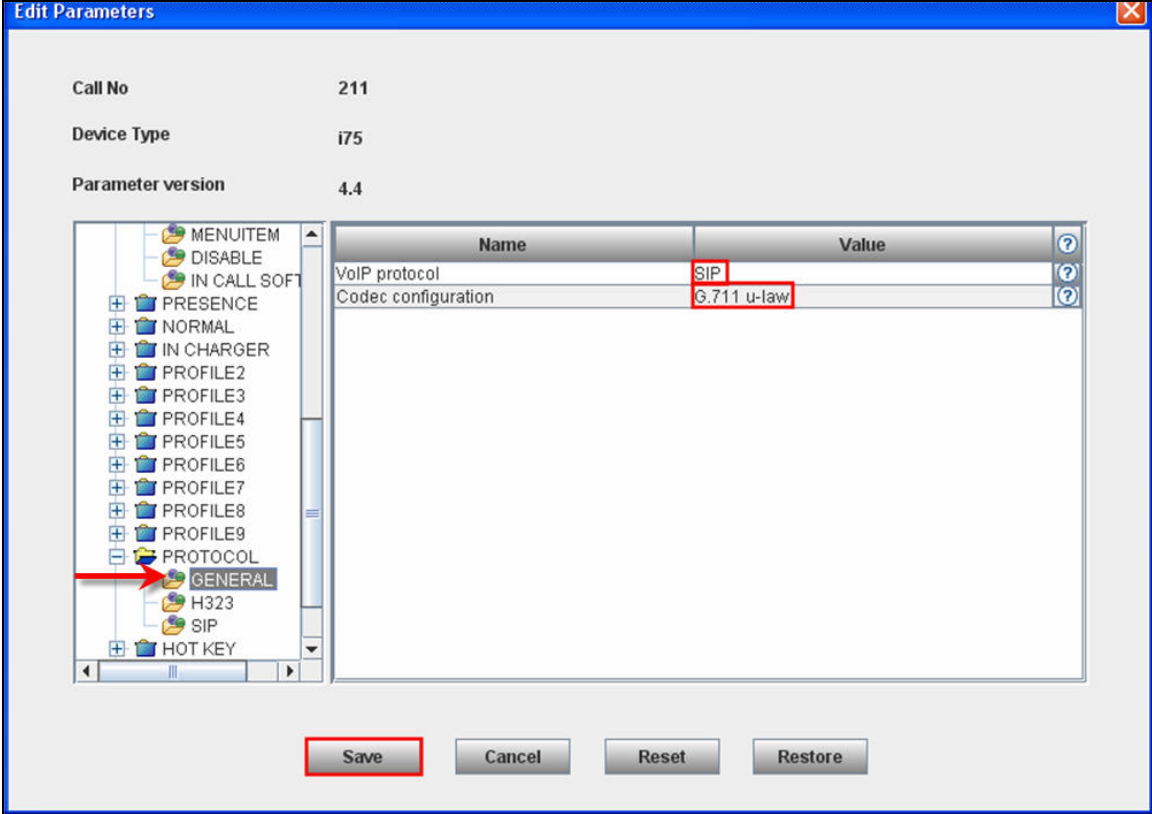
**Edit Parameters**

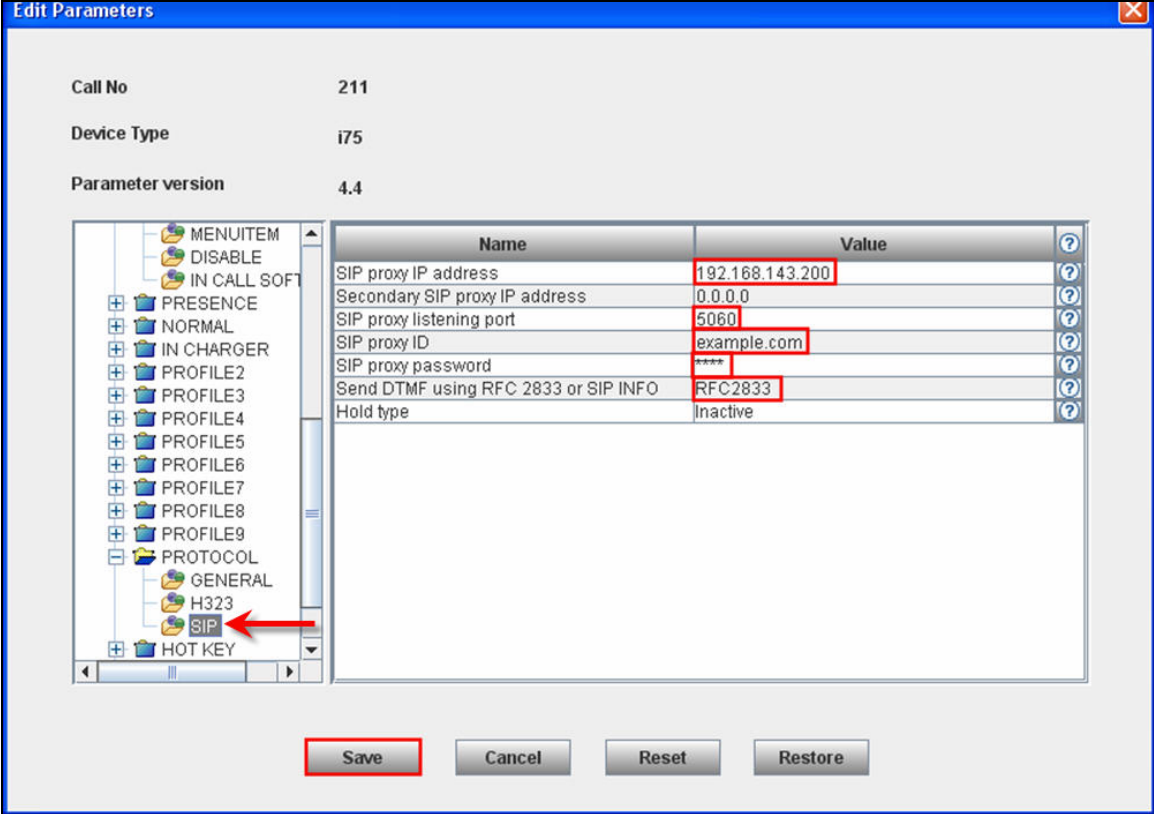
Call No: 211  
Device Type: i75  
Parameter version: 4.4

Name	Value
Max number of call completions	2
Vibrate during call	Vibrate only on urgency messages
Emergency number	
Dial pause time	1
Time zone	Western European Time (GMT)
LCD contrast	Level 8 (default)
Voice mail number	
Phone mode	Personal
Backlight timeout	20
Unread message reminder	Disable
Message reminder interval	7
Administration user name	admin
Administration password	****
Replace Call Rejected with User Busy	Enable
NTP server	0.0.0.0

Buttons: Save, Cancel, Reset, Restore

Step	Description
4.	<p>Navigate to the <b>MESSAGEC</b> configuration page by clicking <b>MESSAGEC</b>. Enter the information displayed below and then click <b>Save</b>. <b>Message Centre number</b> is the extension associated with voicemail on the Avaya Distributed Office. In the sample configuration, the Avaya Distributed Office uses extension 700 for voicemail.</p> 

Step	Description
5.	<p>Navigate to the <b>PROTOCOL GENERAL</b> configuration page by clicking <b>PROTOCOL→GENERAL</b>. Enter the information displayed below and then click <b>Save</b>.</p> <p><b>VoIP protocol</b> "SIP"  <b>Codec configuration</b> "G.711 u-law"</p> 

Step	Description
6.	<p>Navigate to the <b>SIP</b> configuration page by clicking <b>SIP</b>. Enter the information displayed below and then click <b>Save</b>. <b>SIP proxy password</b> must match the <b>Security Code</b> configured on Avaya Distributed Office in <b>Section 3, Step 1</b>. <b>SIP Proxy ID</b> must match the <b>SIP Domain</b> from <b>Section 3, Step 5</b>.</p> <p><b>SIP proxy IP address</b> "192.168.143.200"  <b>SIP proxy listening port</b> "5060"  <b>SIP proxy ID</b> "example.com"  <b>Send DTMF using RFC 2833 or SIP INFO</b> "RFC2833"</p> 

## 6. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying the capability of the Ascom i75 VoWiFi SIP Handset to interoperate with Avaya Distributed Office when configured as a “9620-SIP” set type.

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 i75 VoWiFi SIP Handset with Avaya Distributed Office. Calls were made between telephones and basic calling features were tested and verified to operate properly.

### 6.2. Test Results

The Ascom i75 VoWiFi SIP Handset passed all test cases. The Ascom i75 VoWiFi SIP Handset was verified to successfully register with Avaya Distributed Office as a “9620-SIP” set type. The Ascom i75 VoWiFi SIP Handset was verified to be capable of placing/receiving calls with proper caller ID information. Basic calling features such as hold/return from hold, transfer (attended/unattended), conference, call forwarding (on busy/unconditional/clear), multiple call appearances, voicemail and MWI were verified to operate correctly. Calls were maintained for durations lasting longer than one minute.

## 7. Verification Steps

The following steps can be used to ascertain the functional state of the Ascom i75 VoWiFi SIP Handset.

- Place calls to other telephones within the network and verify two-way audio between endpoints.
- Dial into the Avaya Distributed Office Auto Attendant or voicemail and verify audio is heard, digits are properly interpreted and the Ascom i75 VoWiFi SIP Handset can navigate the menus using the keypad present on the telephone.
- Exercise and verify proper operation of calling features such as hold/return from hold, transfer and call forwarding.

## 8. Support

Technical support for the Avaya Distributed Office can be obtained from the following:

- **Phone:** 1-866-GO-AVAYA
- **Email:** [support@avaya.com](mailto:support@avaya.com)

Technical support for the Ascom i75 VoWiFi SIP Handset can be obtained from the following:

- **Phone:** 1-877-71ASCOM or 1-877-712-7266
- **Email:** [techsupport@ascomwireless.com](mailto:techsupport@ascomwireless.com)

## 9. Conclusion

These Application Notes detail the configuration process that enables interoperability between the Ascom i75 VoWiFi SIP Handset and Avaya Distributed Office. These Application Notes also demonstrate the configuration that enables multiple call appearances and a voicemail box for the extension associated with the Ascom i75 VoWiFi SIP Handset.

## 10. Additional References

- [1] *Avaya Distributed Office i20 Installation Quick Start*, May 2007 Issue 1, Document Number 03-602289
- [2] *Ascom i75 VoWiFi SIP Handset Administrator Guide*, March 2007 Issue 2, Document Number 16-602203
- [3] *ArubaOS 3.2 User Guide*, September 2007, Document Number 0510339

---

**©2007 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](mailto:devconnect@avaya.com).