

Configuration Manual

WLAN Handset

Contents

1. Introduction	1
1.1 Abbreviations and Glossary	1
2. Pre-Installation.....	4
2.1 VoWiFi System IP addresses	4
3. Programming the WLAN Handset	5
3.1 PDM	5
4. Installation of WLAN Handsets.....	6
4.1 Installation without Central Device Management.....	6
4.2 Installation using the Handset's Admin Menu.....	7
4.3 Configure a Handset with a Template.....	7
4.3.1 Create a template	8
4.3.2 Apply a Template to a Handset with a Number	8
4.3.3 Apply a Template to Handset without a Number	8
4.3.4 Save Handset Configuration as a Template	9
4.3.5 Synchronizing a Handset with PDM	9
4.3.6 Configure Handset without Saving It in PDM	9
5. Maintenance	10
5.1 Handset	10
5.1.1 Upgrade Handset Software	10
5.1.2 Upgrade Software OTA via TFTP.....	10
5.1.3 Upgrade Software via PDM.....	11
5.1.4 Recapture the Earlier Software.....	11
5.1.5 Perform a Factory reset	11
5.2 Replacement of Handsets	12
5.2.1 Replacement Procedure Choice.....	12
5.2.2 Replacement of Handset with PDM Only.....	12
5.3 Change Number of a Handset	13
5.4 Upgrade the Template	13
5.5 Create a Configuration Backup.....	13
6. Handset Configuration.....	14
6.1 Select Network	14
6.1.1 Change Active Network	14
6.1.2 Change Name of Network.....	14
6.1.3 Enable Switch between Networks	14
6.2 IP Address Settings	15
6.2.1 Automatic IP Address Settings.....	15
6.2.2 Static IP Address (Manual) Settings.....	15

6.3	Network Settings	16
6.3.1	SSID	16
6.3.2	Voice Power Save Mode	16
6.3.3	World Mode Regulatory Domain	16
6.3.4	Radio and Channel Selection	16
6.3.5	Transmission Power	18
6.3.6	IP DSCP for Voice/Signalling	18
6.4	Security Settings	18
6.4.1	Open	18
6.4.2	WEP 64/128-bit Key	19
6.4.3	WPA-PSK & WPA2-PSK	19
6.4.4	802.1X with EAP-FAST	19
6.4.5	802.1X with PEAP-MSCHAPv2	19
6.4.6	EAP-TLS	20
6.5	Handset Settings	20
6.5.1	Automatic keylock	21
6.5.2	Phone lock	21
6.5.3	Audio adjustment	21
6.5.4	Headset Configuration	22
6.5.5	In Charger Behaviour	22
6.5.6	Configure Profiles	23
6.5.7	Battery Warning	23
6.5.8	Uploadable Language	24
6.5.9	Select Default Language	24
6.5.10	Short cuts	24
6.5.11	Soft Key Functions During Call	26
6.5.12	Import Contacts	26
6.5.13	Company Phonebook	26
6.5.14	Central Phonebook	27
6.6	Telephony	28
6.6.1	Endpoint ID and Endpoint number	28
6.6.2	VoIP Protocol	28
6.6.3	Codec	29
6.6.4	Internal Call Number Length	29
6.6.5	Emergency Number	30
6.6.6	Voice Mail Number	30
6.6.7	Max number of Call Completions	30
6.6.8	Dial Pause Time	30
6.6.9	Direct off Hook from Charger	30
6.6.10	Replace Call Rejected with User Busy	30
6.7	Regional Settings	31

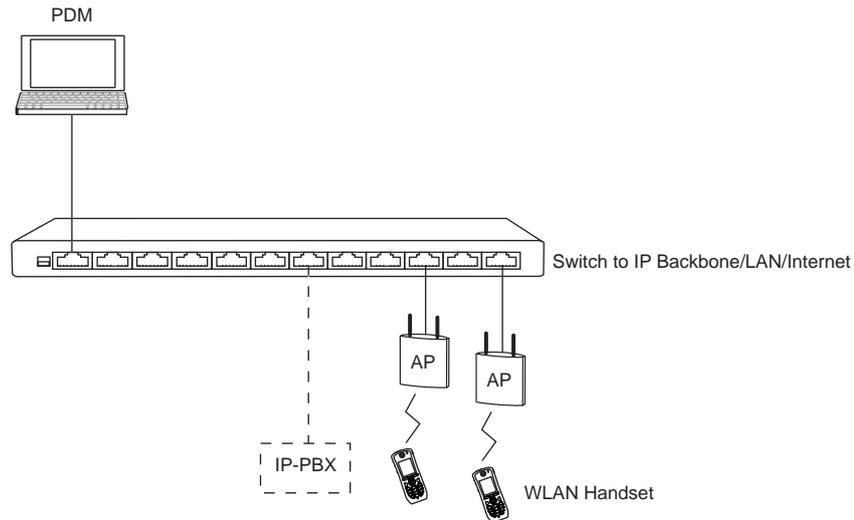
6.7.1	Set Time & Date	31
6.7.2	Select Default Language.....	31
6.7.3	Dialling Tone Pattern	31
6.8	Display	32
6.8.1	User Display Text	32
6.8.2	Font style	32
6.8.3	Backlight Timeout.....	32
6.8.4	Brightness.....	32
6.8.5	Screen Saver	32
6.9	Menu Operation.....	33
6.9.1	Hide Menu Items.....	33
6.10	Presence Management.....	33
7.	Use Handset to Verify the VoWiFi System Deployment	34
7.1	Site Survey Tool.....	34
7.2	Scan the Channels	34
7.2.1	Scan all Channels	34
7.2.2	Scan a Specific Channel.....	35
7.3	Range Beep.....	35
7.3.1	Configurable RSSI Threshold	35
7.3.2	Range Beep on a Configurable RSSI Threshold	35
8.	Handset Internal Web Administration Page	36
8.1	Access the Handset's Internal Web Administration page	36
8.1.1	System Setup View	36
8.1.2	Troubleshoot View	37
8.2	Change Administration Password	38
8.2.1	Change password via the handset's Internal Web Administration page	38
8.2.2	Change password via the PDM	38
9.	Administration	39
9.1	Admin Menu Tree	39
9.2	Quick Access to the Handset's Device Information.....	40
9.3	LED indications	40
10.	Troubleshooting	41
10.1	Fault Symptoms	41
10.2	Display Information.....	42
10.3	Troubleshooting from the handset Internal Web Administration Page.....	44
11.	Related Documents	45
12.	Document History	46
Index	47

1. Introduction

This document is a guide for installing, configuring and maintaining functionality of the WLAN Handset.

The Ascom Voice over Wireless Fidelity (VoWiFi) system provides wireless IP-telephony to enterprise LANs. Using third-party WLAN products as well as in-house developed hardware and software, the system enables data and voice transmission together with seamless roaming.

Figure 1.



Ascom VoWiFi System

This document is intended as a guide when installing the WLAN Handset in a VoWiFi system. The document describes the settings needed to make the handset function in a VoWiFi system and is relevant to the following personnel:

- System Administrator
- Service Technician

First configuration is done using the Portable Device Manager (PDM). In small systems where it is possible to collect all handsets to update settings, daily maintenance is also done by using the PDM. The handset behavior can be customized to suite each user profile.

It is recommended that the reader has basic knowledge of the VoWiFi system and basic knowledge of handset registration in the PBX.

1.1 Abbreviations and Glossary

802.11a	IEEE 802.11 standard for transmission rate of up to 54Mbps, operates in the 5GHz spectrum.
802.11b	IEEE 802.11 standard for transmission rate of up to 11Mbps, operates in the 2.4GHz spectrum.
802.11g	IEEE 802.11 standard for transmission rate of up to 54Mbps, operates in the 2.4GHz spectrum.
802.11d	IEEE 802.11 standard for regulatory domains.
802.11e	IEEE 802.11 standard that defines Quality of Service (QoS) for WLAN.
802.11i	Standard for security improvements for 802.11.

802.11n	IEEE 802.11 standard for transmission rate of up to 100 Mbps, operates in the 2.4GHz and 5GHz bands.
802.11D	IEEE MAC Bridges standard (interworking for 802.11 among others).
802.11X	IEEE standard for port-based Network Access Control (authentication).
Ad-hoc WLAN	A WLAN between two wireless capable devices (normally PCs), where no AP is involved.
AES	Advanced Encryption Standard.
AP	Access Point
BSS	Basic Service Set. A WLAN with at least one AP that is configured for it.
BSSID	Basic Service Set Identifier. Hardcoded name of an ad-hoc WLAN, usually the MAC address of the radio. One type of SSID (the other being ESSID).
CCX	Cisco Compatible eXtension
DHCP	Dynamic Host Configuration Protocol. Used to send config parameters to TCP/IP clients.
DNS	Domain Name System
DSCP	Differentiated Services Code Point. QoS on the Network Layer. Used both for WLANS and LANs.
DTIM	Delivery Traffic Indication Message
EAP	Extensible Authentication Protocol.
EAP-FAST	Flexible Authentication via secure tunneling.
EAP-TLS	EAP-Transport Layer Security.
ESS	Extended Service Set. WLAN with multiple APs sharing the same SSID.
ESSID	Extended Service Set Identifier. Identifying name of a WLAN - strictly it is the identifying name of an AP and distinguishes WLANS from another. ESSID is one type of SSID (the other being BSSID).
MAC	Medium Access Control.
PBX	Private Branch Exchange: Telephone system within an enterprise that switches calls between local lines and allows all users to share a certain number of external lines.
PEAP	Protected Extensible Authentication Protocol.
PDM	Portable Device Manager Used for management of portables, editing of parameters and updating the portables with new software.
PEAP	Protected Extensible Authentication Protocol.
SSID	Service Set Identifier. User friendly name of a WLAN. Identifier attached to packets sent over a WLAN that acts as a password. Daily used term for ESSID in an wireless ESS topology.
STA	Station. Client in a WiFi network.
QoS	Quality of Service: Defines to what extent transmission rates, error rates etc. are guaranteed in advance.
UP 6	User Presence (value between 0-7). Wireless QoS at the MAC Layer.
VoIP	Voice over IP.
VoWiFi	Wireless version of VoIP and refers to an IEEE 802.11a, b, g and n network.
VoWLAN	Voice over WLAN.

WEP	Wired Equivalent Privacy.
Wi-Fi	Wireless Fidelity. Has become a name for wireless LAN networks. Originator is Wi-Fi Alliance.
WLAN	Wireless Local Area Network. Refers to an IEEE 802.11a, b, g and n network.
WMM	Wi-Fi Multimedia. A Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. Provides basic QoS features to IEEE 802.11 networks.
WPA/WPA2	Wi-Fi Protected Access 2. Security method based on 802.11i standard for wireless networks (data protection and network access control).

2. Pre-Installation

Before installing handsets in a VoWiFi system, make sure that all equipment is available. It is recommended to set up chargers and charge the handset batteries before installation, and to have a number plan available for the handsets. Also be sure that the IP addressing plan is set up to support the amount of handsets to be deployed.

We assume that the VoWiFi system is installed including some or all of the following components (depending on system configuration):

- DHCP Server. A DHCP server allows devices to request and obtain an IP address from a server which has a list of addresses available for assignment. If the WLAN does not have access to a DHCP server, a list of static IP addresses is necessary.
- Portable Device Manager. The PDM is used for administration and programming of the handsets. All settings and updates are in this case done via the DP1 Desktop Programmer cradle connected over USB.

2.1 VoWiFi System IP addresses

Complete the table below with the IP addresses, as a help when configuring the handsets.

Table 1.

Device	IP address/Number/Port	Required
IP-PBX		If used
Subnet Mask ^a		If used
Number plan	N/A	Yes
NTP Server address ^b		
DNS Server address ^a		
VoIP settings ^c		Yes
Syslog server		If used
TFTP server		If used
DHCP range		

a. Only required if no DHCP is used, that is, static IP is used.

b. Depending on system configuration

c. Gatekeeper IP address or SIP proxy IP address used to access the PBX.

3. Programming the WLAN Handset

This chapter describes how to configure handsets in two different ways:

- It is possible to configure the handset by inserting it into a DP1 Desktop Programmer cradle connected via USB to the PDM.
- It is possible to configure the basic network settings of the handset via its Admin menu. See [9. Administration](#) on page 39 for more information about the settings that can be made.

The PDM enables configuration of one handset at the time inserted in the DP1 Desktop Programmer connected via USB to the administrator's computer.

Tip: It is recommended to use templates when configuring handsets. By using a template, the same configuration can easily be applied to many handsets simultaneously.

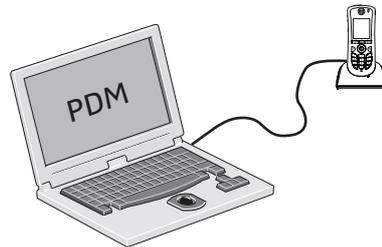
3.1 PDM

The PDM runs on a PC and is used for configuring the handset as follows:

- Connect a DP1 Desktop Programmer cradle via USB to the computer running PDM.
- Start PDM.
- Place the handset in this cradle connected to PDM.

For instructions on how to install and use the PDM, see *Installation and Operation Manual, Portable Device Manager, Windows version, TD 92881EN*.

Figure 2.



Configuration of handsets via PDM

4. Installation of WLAN Handsets

This section describes the recommended procedure for installing and configuring handsets. There are several ways to install a handset, but the procedures described here guarantees simple maintenance of the network.

The PDM enables administration of one handset at the time inserted in a Desktop Programmer (DP1) connected via USB to the administrator's computer. See [Installation steps in small VoWiFi Systems using PDM](#).

Installation steps in small VoWiFi Systems using PDM

- 1 Create Numbers.
- 2 Create one template for all settings in the PDM.

See [4.1 Installation without Central Device Management](#) for more information.

4.1 Installation without Central Device Management

In a small VoWiFi system, the administration can be handled using only the PDM.

The synchronization is in this case not handled automatically by the system when a handset's parameters are changed in the PDM. When the parameters have been changed in PDM, each handset must be placed in the DP1 cradle connected to the administrator's computer in order to synchronize the parameters with the handset.

- 1 Open the PDM.
- 2 In the *Numbers* tab, click "New". The *New numbers* window is opened.
- 3 In the *Device Type* and *Parameter version* drop-down lists, select the matching device type and the parameter version for the handset to be use, respectively.
- 4 In the *Prefix* field, enter the numbers' prefix (if needed).
- 5 Create a range of numbers by selecting the "Range" option. Enter the start call number and the end call number in the fields, respectively.
- 6 Click "OK".
- 7 Create a network settings template (see [4.3.1 Create a template](#) on page 8) with the following network parameters:
 - Network settings¹ (located under Network > Network A, B, C, or D)
- 8 Create another template (see [4.3.1 Create a template](#) on page 8) with the common handset settings applicable to all handsets (exclude the network parameters and used security settings). Example of parameters settings:
 - VoIP settings² (located under VoIP)
 - Software TFTP IP address (if any) (located under Device > General)
 - Syslog settings³ (if any) (located under Device > General)

In addition, settings for hiding menu items in the display, certain level of ring signal and vibrators etc can also be configured.
- 9 Apply the network settings template to the handset, see [4.3.2 Apply a Template to a Handset with a Number](#) on page 8.
- 10 Apply the common settings template to the handset, see [4.3.2 Apply a Template to a Handset with a Number](#) on page 8.

1. All required system settings for the WLAN. For example SSID and Security mode.

2. VoIP protocol, Gatekeeper IP address or SIP proxy IP address used to access the PBX.

3. The parameter "Syslog" must be enabled in order to set the "Syslog IP address".

- 11 Put the handset in the DP1 cradle.
- 12 In the *Device Wizard* window, select "Associate with number" and press "OK".
- 13 Select the handset to associate with. Press "OK".

The number and parameter settings saved in the PDM will now be synchronized with the handset. In addition, the handset's Device ID will also be synchronized with the number in the PDM.

If certificates must be used to access a VoWiFi system, also perform the steps 14 - 19.

- 14 In the *Numbers* tab, right-click the handset's number and select "Edit certificates". An *Edit certificate* window opens.
- 15 In the *Root* tab and *Client* tab, click "Edit" and select the certificates to import. Click "Close".
- 16 In the *Numbers* tab, right-click the handset's number and select "Edit parameters".
- 17 Select "Network X" (X represents A, B, C, or D).
- 18 In the *Security mode* drop-down list, select "EAP-TLS".
- 19 In the *EAP client certificate* drop-down list, select the client certificate to be used. Click "OK".
- 20 Remove the handset when synchronisation is finished.

Repeat the steps 11-13, 20 (if needed, perform the steps 14-19) for all handsets.

4.2 Installation using the Handset's Admin Menu

It is possible to install a handset using its Admin menu. This is useful when no PDM is available and the handset needs to be installed quickly.

NOTE: It is only possible to configure the basic settings via the Admin menu.

- 1 There are two options to access the Admin menu:
 - If the handset has been factory reset or not been configured; in idle mode, enter 40022.
 - If the handset has been configured; press "Menu", select "Settings" and enter 40022.
- 2 Set the following parameters:
 - Network settings¹ (located under Network setup)
 - VoIP settings² (located under VoIP)
 - Syslog settings³ (if any) (located under Syslog)

4.3 Configure a Handset with a Template

It is possible to select a handset in the PDM and directly change one or more configuration parameters. By using a template, the same configuration can easily be applied to many handsets simultaneously. Templates are also an efficient way to give good control over which changes that are applied to each handset.

Templates enables configuration of all aspects of a handset from sound volume to keypad short cuts.

1. All required system settings for the WLAN. For example SSID and Security mode
 2. VoIP protocol, Gatekeeper IP address or SIP proxy IP address used to access the PBX.
 3. The parameter "Syslog" must be enabled in order to set the "Syslog IP address".

Your supplier can provide example templates for different PBX:s. The handset will have full functionality towards the PBX even without such a template. By using such a template, though, the handset will be customized for that PBX with menu options for PBX specific functions.

4.3.1 Create a template

- 1 Open the PDM.
- 2 Select the *Templates* tab and open the menu "Template > New...". The *New Template* window is opened.
- 3 Select the device type and parameter version that matches the software version installed on the handset. Give the template a descriptive name.

The parameters that are not part of the template will be left unchanged on the handset. The parameter version of an installed handset is visible under the *Numbers* tab or the *Devices* tab.

- 4 Click "OK".
- 5 Select the checkbox of each parameter that you want to be part of this template and enter the proper value.
- 6 Click "OK" to save the template.

4.3.2 Apply a Template to a Handset with a Number

- 1 Open the PDM.
- 2 In the *Numbers* tab, select the handset(s) you want to apply the template to.

NOTE: If several handsets shall be selected, they must be of the same device type and have the same parameter version.

- 3 Make a right-click and select "Run template...".

Only templates with a parameters version matching the selected handsets will be shown. Select the template you want to apply and click "OK".

The template is applied. The number of parameters in the template will affect the time it takes to apply the template to the selected handsets.

When looking at a handset under the *Numbers* tab, the column "Last run template" will show the name of the most recently applied template.

4.3.3 Apply a Template to Handset without a Number

It is possible to apply a template to a handset without a number in the PDM.

- 1 Put the handset in the DP1 cradle.
- 2 In the *Found Device Wizard* window, select the "Run template" option.
- 3 Click "Next >".

Only templates with a parameter version matching the selected handset will be shown.

- 4 Select the template that shall be applied and click "OK".

The template is applied. The number of parameters in the template will affect the time it takes to apply the template to the selected handset.

4.3.4 Save Handset Configuration as a Template

It is possible to save all settings of a handset as template. Note that this does not include contacts, certificates and other personal data. The template will only contain configuration data.

This template can be used as a backup if you want to restore the configuration of the handset at a later stage or as a template that can be applied to a number of handsets.

- 1 Open PDM.
- 2 In the *Numbers* tab, select the handset you want to save as a template.
- 3 Make a right-click and select "Use as a template...". Enter a descriptive name for the template.
- 4 The *Edit template* window is opened. By default, all parameters are selected and are saved when clicking "OK".

If one or more parameters should be excluded, remove them by clearing the checkbox next to the parameter.

Some parameters are user specific. If it is decided to apply this type of template to several handsets, it is recommended to exclude the following parameters:

- User display text - A text string displayed in idle mode. The parameter is located directly under "Settings".
- Phone lock PIN code - The security code used to unlock the keypad. The parameter is located under Settings > Locks.
- Endpoint ID - The identity/name of the user registered in the PBX. The parameter is located under VoIP > General.

- 5 Click "OK".

4.3.5 Synchronizing a Handset with PDM

After installing and saving a handset, it will be synchronized each time it is connected to the PDM. The synchronization transfers parameter changes between the handset and the PDM and vice versa as follows:

- If a parameter has been changed in the handset, it will be transferred to the PDM.
- If a parameter has been changed in the PDM while the handset was disconnected, it will be transferred to the handset.

If the same parameter has been changed in both the PDM and the handset, the value in PDM will be transferred to the handset.

4.3.6 Configure Handset without Saving It in PDM

It is possible to configure a handset without saving it in the PDM. An unsaved handset do not have the symbol ✓ in the Saved column. The settings in the handset can be synchronized and saved in the PDM later on. However, it is recommended to save the handset in PDM if backup is needed. For example when a handset needs to be replaced.

- 1 Put the handset in the DP1 cradle.
- 2 Open PDM.
- 3 In the *Numbers* tab, select the unsaved handset you want to configure.
- 4 Select Number > Edit parameters.
- 5 The *Edit parameters* window is opened. Edit the parameters of the handset and click "OK".
- 6 Remove the handset from the DP1 cradle. The handset is no longer visible in the PDM and the settings are only saved in the handset.

5. Maintenance

5.1 Handset

In an existing VoWiFi system it is important to be able to replace handsets, install new handsets and exchange faulty handsets.

If only PDM is used, do one of the following:

- If you want to install new handset, see [4.1 Installation without Central Device Management](#) on page 6.
- If you want to replace a broken handset, see [5.2.2 Replacement of Handset with PDM Only](#) on page 12.

5.1.1 Upgrade Handset Software

NOTE: Pay attention to the software Release Notes before changing the software.

The handset software can be upgraded over the air using a TFTP server, or by cable using PDM.

5.1.2 Upgrade Software OTA via TFTP

Software upgrade OTA via TFTP is used in small VoWifi systems. The benefit is that the handsets do not need to be collected by the administrator since the software upgrade is performed over the air.

In order to upgrade the software via TFTP, the following must be done:

- 1 If needed, the handset must be configured in PDM to access a TFTP server, see [Configure Access to the TFTP Server](#).
Tip: It is recommended to configure the TFTP server's IP address when installing the handsets. See [4.1 Installation without Central Device Management](#) on page 6.
- 2 If needed, a new software information file (packageinfo.inf) and a software (.bin) file must be uploaded to the TFTP server. These files are provided by your supplier. See the manual for the TFTP server used for more information on how to upload files.
- 3 The handset must be restarted. When the handset has been restarted, it connects to the TFTP server and downloads the software information file (.inf) that contains information about the software version. If the software version differs from the handset's software version, the handset will download the software file (.bin) from the TFTP server. The handset will be restarted when the software upgrade is performed.

Configure Access to the TFTP Server

- 1 Put the handset in the DP1 cradle.
- 2 Open the PDM.
- 3 Open the Numbers tab and select the handset.
- 4 Make a right-click and click "Edit parameters".
- 5 Select Device > General.
- 6 In the *Software TFTP IP address* field, enter the IP address to the TFTP server.
- 7 Click "OK".

5.1.3 Upgrade Software via PDM

Software upgrade via PDM is used in small VoWiFi systems. The handsets need to be collected by the administrator due to the software upgrade is performed via the Desktop Programmer DP1 connected to PDM.

- 1 Open the PDM.
- 2 In the *Devices* tab, right-click the handset to be upgraded. Select "Upgrade software...".
- 3 In the *Available files* drop-down list, select the desired software file (.bin).
If needed, import the software file to be used by clicking "Import". Locate the software file (.bin or .pkg) and click "Open".
- 4 Click "OK".

5.1.4 Recapture the Earlier Software

The handset stores two software versions which makes it possible to force the handset to jump back to the earlier software. This feature shall be used if the current software does not work properly.

NOTE: The handset must be switched off to be able to load the earlier software.

Press and hold the keys "7" and "8" and press On/Off key at the same time. The handset loads the earlier software and will keep it as long it is not restarted.

5.1.5 Perform a Factory reset

When a factory reset is done on a handset, all configuration settings will be restored to default values; PBX subscriptions, contacts, downloaded language, certificate etc. will be removed. The software will be left intact.

Factory Reset using PDM

- 1 Open the PDM.
- 2 Put the handset in the DP1 cradle.
- 3 In the *Device* tab, mark the handset to be factory reset. Note that the handset must be online.
- 4 In the Device menu, select "Factory reset". Alternatively, right-click the handset and select "Factory reset".
- 5 A *Reset devices* window appears, click "Yes". The handset will be restarted.

Factory Reset using Handset

It is possible to factory reset a handset from its Admin menu.

- 1 To activate the Admin menu, select Menu > Settings and enter 40022.
- 2 Select "Factory Reset".
- 3 A *Reset portable?* window appears, press "Yes". The handset will be restarted.

5.2 Replacement of Handsets

A handset can be replaced with a spare handset if it is broken. The handset registered in PDM, is associated with its device type, device ID and extension. During the replacement procedure, the broken handset's device type and extension will be associated with the spare handset's device ID.

5.2.1 Replacement Procedure Choice

If you only have PDM, see [5.2.2 Replacement of Handset with PDM Only](#).

Data included in a replacement transfer

The following data is replaced during a replacement:

- User parameters
- Contacts (entered by the user)

Note that the following data is not replaced:

- Call list
- Company phonebook
- Downloaded language
- Certificates

5.2.2 Replacement of Handset with PDM Only

If the broken handset and the spare handset have the same device type, see [Replace using PDM](#).

Replace using PDM

Both the broken handset and the spare handset must be of the same device type.

- 1 Put the broken handset in the DP1 cradle.
- 2 Put the broken handset in the .
- 3 Open the PDM.
- 4 Make sure that the handset is saved in the PDM. In the *Numbers* tab, a saved handset has the symbol ✓ in the *Saved* column. If not, right-click the handset and select "Save" in order to transfer the settings to the spare handset later on.
- 5 If the spare handset has been previously used, perform a factory reset, see [5.1.5 Perform a Factory reset](#) on page 11.
- 6 Put the spare handset in the DP1 cradle.
- 7 A *Found Device Wizard* window appears. Select "Associate with Number" and click "Next >".
- 8 In the list, select the broken handset to be replaced with the spare handset. Click "OK".

The broken handset has been replaced and its settings have been transferred to the spare handset.

5.3 Change Number of a Handset

It is possible to change the number of a handset, but keep all other settings in the handset.

- 1 Open PDM.
- 2 Open the Numbers tab, and select the handset to be updated with a new number.
- 3 In the Number menu, select "Rename...". Alternatively, right-click the handset and select "Rename..." from the menu that appears.
- 4 In the New prefix field, enter the new prefix (if needed).
- 5 In the New number field, enter the new number.

NOTE: Make sure that the new number is not existing in another system. If several handsets have the same number, their settings will overwrite each other when synchronizing with PDM.

- 6 Click "OK".

The new number will be synchronized with the handset when it is connected to PDM.

5.4 Upgrade the Template

The upgrade procedure of the templates definition version is described in the *Installation and Operation Manual, Portable Device Manager, Windows version, TD 92881EN*.

5.5 Create a Configuration Backup

It is recommended to have a backup of the configuration in the handsets and the site.

The backup procedure is described in the *Installation and Operation Manual, Portable Device Manager, Windows version, TD 92881EN*.

6. Handset Configuration

NOTE: This chapter describes settings in parameter definition files (.def). These files are regularly updated and settings may change slightly. For example "On" to "Enable" or a parameter can be moved to another directory.

The handset requires some settings to function in the VoWiFi system. All settings are done in the PDM. This section describes the available settings for the handset. The first part explains network settings and the second handset settings.

For more information, see the PDM Online Help that is accessible for each parameter by clicking the icon  in the Edit parameters view, or the *Installation and Operation Manual, Portable Device Manager, Windows version, TD 92881EN*.

6.1 Select Network

The handset can switch between four different WLAN system configurations called Network A, Network B, Network C, and Network D. The name can be changed (via PDM) and is visible in the handset, see [6.1.2 Change Name of Network](#).

A handset can be configured for up to four different WLANs but only for one VoIP System.

The configured networks in PDM must have a SSID value in order to view them in the handset.

Network A is the default system and used throughout this manual.

- 1 Select Network > General.
- 2 In the *Active network* drop-down list, select "Network A".

6.1.1 Change Active Network

- 1 Select Network > General.
- 2 In the *Active network* drop-down list, select "Network A", "Network B", "Network C", or "Network D".

6.1.2 Change Name of Network

The name is shown when selecting network in the handset.

- 1 Select Network > Network A (or B, C, or D).
- 2 In the Network name field, enter the name of the network.

6.1.3 Enable Switch between Networks

The handset may be configured to switch between networks on the site.

- 1 Find parameter Network > General > Auto-switch network, and select "Enable".
Parameter Auto-switch network timeout appears. This parameter defines the time before the handset tries to connect with the next included network.
- 2 Enter a value in seconds for parameter Auto-switch network timeout.
- 3 For the networks that should be included in the auto-switch network:
Find parameter Network > Network A (B, C, D) > Include in auto-switch network, and select "Yes" to enable switch to Network A (B, C, D).

6.2 IP Address Settings

The IP address settings can be configured in two ways.

- The handset can be configured to receive an IP address automatically from a DHCP server, see [6.2.1 Automatic IP Address Settings](#).
- If no DHCP server is used, a unique IP address must be entered manually for each handset, see [6.2.2 Static IP Address \(Manual\) Settings](#).

6.2.1 Automatic IP Address Settings

- 1 Select Network > Network A (or B, C, D).
- 2 In the DHCP mode drop-down list, select "Enable".

The Phone IP address, Subnet mask and Default gateway are automatically set up.

6.2.2 Static IP Address (Manual) Settings

- 1 Select Network > Network A (or B, C, D).
- 2 In the DHCP mode drop-down list, select "Disable (static mode)". Additional parameters will be displayed.
- 3 In the Phone IP address field, enter the unique IP address for the handset.
- 4 In the Subnet mask field, enter the subnet mask.
- 5 In the Default gateway field, enter the IP address for the default gateway.

DNS Server Settings

It is possible to configure which DNS server the handset shall use. If the primary DNS server is available, it is always used. Otherwise, the secondary DNS server will be used.

NOTE: The DNS parameters are only visible if the DHCP mode is set to "Disable (static mode)", see [6.2.2 Static IP Address \(Manual\) Settings](#).

Primary DNS Server

- 1 Select Network > Network A (B, C, or D).
- 2 In the Primary DNS field, enter the IP address to the primary DNS server.

Secondary DNS Server

- 1 Select Network > Network A (B, C, or D).
- 2 In the Secondary DNS field, enter the IP address to the secondary DNS server.

6.3 Network Settings

6.3.1 SSID

The SSID is the name of the network the handset associates to.

- 1 Select Network > Network A (B, C, or D).
- 2 In the *SSID* field, enter system SSID.
Note that the SSID is case-sensitive.

6.3.2 Voice Power Save Mode

The voice power save mode is used during calls. NONE is recommended to obtain optimal voice quality. U-APSD uses less power but is more sensitive to network disturbances.

If supported by the infrastructure U-APSD is the preferred choice and multiple the talk time more than 4 times compared to NONE mode.

- 1 Select Network > Network A (B, C, or D).
- 2 In the *Voice power save mode* drop-down list, select one of following:
 - NONE
 - U-APSD

6.3.3 World Mode Regulatory Domain

There is a set of regional rules for the world mode settings and the a-band that the handset complies to. The preferred and the default setting is "World mode (802.11d)". The handset gets its regulatory settings from the AP. If this is not supported by the AP, then this has to be set in the handset as follows:

- 1 Select Network > Network A (B, C, or D).
- 2 In the *World mode regulatory domain* drop-down list, select one of the following:
 - World mode (802.11d) (default)
 - ETSI
 - Japan
 - USA

6.3.4 Radio and Channel Selection

The handset supports the 802.11a/n radio and 802.11b/g/n radio, but it cannot use the 802.11a/n radio and the 802.11b/g/n radio simultaneously. The radio determines which channels that can be used.

802.11 a/n Channels

Defines which 802.11a/n channels to use. It is recommended to use the value "UNII-1". Select "Advanced" only if the channels shall be set in the *Advanced: 802.11 channels* parameter, see [Advanced: 802.11 Channels](#) on page 17.

- 1 Select Network > Network A (B, C, or D).
- 2 In the *802.11 protocol* drop-down list, select "802.11a/n".
- 3 In the *802.11a/n channels* drop-down list, select one of the following:

NOTE: The selected World Mode Regulatory Domain determines which channels to be used. See [Bands and Channels used by WiFi a-radio](#).

- All
- Non DFS
- UNII-1
- UNII-3
- UNII-1, UNII-2
- UNII-1, UNII-2, UNII-3
- UNII-1, UNII-2, UNII-2 Extended
- Advanced

Bands and Channels used by WiFi a-radio

	Frequency band	Channels
Non DFS	5.150 - 5.250 MHz	36,40,44,48
	5.725 - 5.845 MHz	149,153,157,161, 165
UNII-1	5.150 - 5.250 MHz	36,40,44,48
UNII-2	5.250 - 5.350 MHz	52,56,60,64
UNII-2 Extended	5.470 - 5.725 MHz	100, 104, 108, 112,116, 120, 124, 128, 132, 126, 140
UNII-3	5.825 - 5.835 MHz	149,153,157,161

802.11 b/g/n Channels

Defines which 802.11b/g/n channels to use. It is recommended to use the default value "1,6,11". If set to "All", all channels are scanned for access points which decreases the WLAN performance. Select "Advanced" only if the channels shall be set in the parameter *Advanced: 802.11 channels*.

- 1 Select Network > Network A (B, C, or D).
- 2 In the *802.11 protocol* drop-down list, select "802.11b/g/n".
- 3 In the *802.11b/g/n channels* drop-down list, select one of the following:
 - All
 - 1,6,11
 - Advanced

Advanced: 802.11 Channels

Defines which 802.11 channels to use. Only used if the parameter in the *802.11b/g/n channels*, or *802.11a/n channels* is set to "Advanced".

NOTE: It is not possible to scan channels in 802.11b/g/n and 802.11a/n simultaneously.

- 1 Select Network > Network A (B, C, or D).
- 2 Enter channels to scan in a comma-separated list, for example 1,6,11 (the order has no impact; 11,6,1 will give the same result).

6.3.5 Transmission Power

This is the transmission power the handset will use when transmitting data to the WLAN system. If "Automatic" (default) is used, the transmission power is adapted according to 802.11h, CCX or maximum possible.

- 1 Select Network > Network A (B, C, or D).
- 2 In the Transmission power drop-down list, select one of the following:
 - Automatic
 - 0 dBm
 - 5 dBm
 - 11 dBm
 - 14 dBm
 - 20 dBm (max)

6.3.6 IP DSCP for Voice/Signalling

Differentiated Services Code Point (DSCP) defines which value to use for outgoing voice and signalling traffic. The DSCP value is used for QoS on the LAN. The settings in the handset must agree with the settings in the system, otherwise it will result in bad voice quality.

- 1 Select Network > Network A (B, C, or D).
- 2 In the IP DSCP for voice and/or IP DSCP for signalling drop-down list, select one of the following:
 - 0x38 (56) - Class selector 7
 - 0x30 (48) - Class selector 6
 - 0x2E (46) - Expedited Forwarding (default for voice)
 - 0x28 (40) - Class selector 5
 - 0x20 (32) - Class selector 4
 - 0x1A (26) - Assured forwarding 31 (default for signaling)
 - 0x18 (24) - Class selector 3
 - 0x10 (16) - Class selector 2
 - 0x08 (8) - Class selector 1
 - 0x00 (0) - Default

6.4 Security Settings

The WLAN system can be configured to use various encryption and/or authentication schemes. The use of extensive encryption/authentication schemes can cause incidents of dropped speech during handover due to the time to process the authentication.

6.4.1 Open

Select Open if no encryption/authentication is required. To select Open as the security mode, do the following:

- 1 Select Network > Network A (B, C, or D).
- 2 In the Security mode drop-down list, select "Open".

6.4.2 WEP 64/128-bit Key

To select WEP64/128-bit Key as the security mode. Do the following:

- 1 Select Network > Network A (B, C, or D).
- 2 In the *Security mode* drop-down list, select "WEP64/128-bit Key". Additional parameters can now be set. See below.
- 3 In the *WEP key 1* field, enter the WEP key to be used.
- 4 In the *WEP transmit key* drop-down list, select "WEP key 1".

6.4.3 WPA-PSK & WPA2-PSK

To select WPA-PSK & WPA2-PSK as the security mode. Do the following:

- 1 Select Network > Network A (B, C, or D).
- 2 In the *Security mode* drop-down list, select "WPA-PSK & WPA2-PSK".
- 3 In the *WPA-PSK passphrase* field, enter the passphrase for WPA-PSK/& WPA2-PSK.

6.4.4 802.1X with EAP-FAST

To select EAP-FAST as the authentication method. Do the following:

- 1 Select Network > Network A (B, C, or D).
- 2 In the *Security mode* drop-down list, select "EAP-FAST".
- 3 In the *EAP authentication user name* field, enter the user name for EAP authentication.
- 4 In the *EAP authentication password* field, enter the password for EAP authentication.

6.4.5 802.1X with PEAP-MSCHAPv2

Select PEAP-MSCHAPv2 if root certificate is to be used for authentication. To select PEAP-MSCHAPv2 as the authentication method. Do the following:

- 1 Ensure that the handset is online in PDM.
- 2 Import the root certificate by do the following:
 - In the *Numbers* tab, right-click the handset's number and select "Edit certificates". An *Edit certificate* window opens.
 - In the *Root* tab, click "Edit" and select the root certificates to import. Click "Close".
- 3 Select Network > Network A (B, C, or D)
- 4 In the *Security mode* drop-down list, select "PEAP-MSCHAPv2".
- 5 In the *EAP authentication user name* field, enter the user name for EAP authentication.
- 6 In the *EAP authentication password* field, enter the password for EAP authentication.

6.4.6 EAP-TLS

Select EAP-TLS if a client certificate is to be used for authentication. To select EAP-TLS as the authentication method, do the following:

- 1 Ensure that the handset is online in PDM.
- 2 Import the certificate by do the following:
 - In the *Numbers* tab, right-click the handset's number and select "Edit certificates". An *Edit certificate* window opens.
 - In the *Root* tab and *Client* tab, click "Edit" and select the certificates to import. Click "Close".
- 3 Select Network > Network A (B, C, or D).
- 4 In the *Security mode* drop-down list, select "EAP-TLS".
- 5 In the *EAP client certificate* drop-down list, select the client certificate to use.

6.5 Handset Settings

This section describes specific settings for the handset that can be changed using the keypad on the handset, and/or can be set in the PDM to assist the user or to set the initial value when the handset is commissioned.

General Settings	Keypad ^a	PDM
6.5.1 Automatic keylock on page 21	x	x
6.5.2 Phone lock on page 21	x	x
Headset type on page 22	x	x
6.5.3 Audio adjustment on page 21	x ^b	x
6.5.10 Short cuts on page 24	x	x
6.5.6 Configure Profiles on page 23	x	x
6.5.7 Battery Warning on page 23	x	x
6.5.5 In Charger Behaviour on page 22	x ^b	x
6.5.8 Uploadable Language on page 24		x
Telephony		
6.6.7 Max number of Call Completions on page 30		x
6.6.8 Dial Pause Time on page 30		x
6.6.9 Direct off Hook from Charger on page 30	x	x
6.6.10 Replace Call Rejected with User Busy on page 30		x
6.6.5 Emergency Number on page 30		x
6.5.12 Import Contacts on page 26		x
6.5.13 Company Phonebook on page 26		x
6.5.14 Central Phonebook on page 27		x
6.6.6 Voice Mail Number on page 30		x
Regional Settings		
6.7.1 Set Time & Date on page 31	x	x
6.5.9 Select Default Language on page 24	x	x
6.7.3 Dialling Tone Pattern on page 31		x

Customize Menu

6.5.8 Uploadable Language on page 24	x
6.9.1 Hide Menu Items on page 33	x

Display

6.8.1 User Display Text on page 32	x	x
6.8.2 Font style on page 32	x	x
6.8.3 Backlight Timeout on page 32		x
6.8.4 Brightness on page 32	x	x
6.8.5 Screen Saver on page 32	x	x

- a. Refer to the User Manual for more information on how the user can change the settings via the handset's keypad.
- b. Some parameters cannot be changed via the keypad.

6.5.1 Automatic keylock

NOTE: If configured, it is possible to dial a pre-defined emergency number when the keypad is locked, see [6.6.5 Emergency Number](#) on page 30.

- 1 Select Device > Settings.
- 2 In the *Automatic key lock* drop-down list, select one of the following:
 - Enable - activates automatic keylock.
 - Disable - deactivates automatic keylock

6.5.2 Phone lock

Activate the phone lock to prevent unauthorized usage of the handset. A password is required to unlock the handset in order to access its functions.

NOTE: If configured, it is possible to dial a pre-defined emergency number when the handset is locked, see [6.6.5 Emergency Number](#) on page 30.

- 1 Select Device > Settings.
- 2 In the *Phone lock* drop-down list, select one of the following:
 - On - the handset will be locked after a few seconds when it is not used.
 - On in charger - the handset will be locked when placed in charger.
 - Off - the phone lock is disabled.

6.5.3 Audio adjustment

Select the volumes for the different audio signals in the handset.

- 1 Select Audio > Volume.
- 2 Select the applicable volumes item in the drop-down lists:
 - Handsfree volume
 - Headset volume
 - Speaker volume
- 3 In the Persistent volume drop-down list, select "Enable" to automatically store volume changes in the handset for future calls.

The parameter affects the "Normal", "Headset", "Loudspeaking" mode.

For selection of headset, see [Headset type](#) on page 22.

NOTE: Changing this parameter may result in lower sound quality and high sound level.
Evaluate carefully before applying.

6.5.4 Headset Configuration

Headset type

Select the headset model that is used.

- 1 Select Headset > General.
- 2 Select the applicable item in the drop-down list:

IMPORTANT: Do not select "Hearing protection" unless a Peltor headset is used.

- Hearing protection
- Mic on boom
- Mic on cable
- User model (If not any headset is used above, this option can be used to configure an own headset profile. If selected, additional configuration is required, see [Headset user model](#))

Headset user model

These settings are required if *User model* is selected under Headset > General.

- 1 Select Headset > User model.
- 2 In the *Name of headset* field, enter a descriptive name. For example the headset model to be used.
- 3 In the following drop-down lists, select the applicable values for the headset:
 - Microphone gain
 - Speaker gain
 - Side tone

NOTE: Changing the parameters may result in lower sound quality and high sound level.
Evaluate carefully before applying.

6.5.5 In Charger Behaviour

The handset behaviour when placed in a charger can be configured.

In charger action

- 1 Select Device > Settings.
- 2 In the *In charger action* drop-down list, select one of the following:
 - No action - no action will be performed when handset is placed in charger
 - Switch off - the handset will be switched off when placed in charger
 - Sound off - the handset will be silenced when placed in charger

6.5.6 Configure Profiles

It is possible to set up an own profile for incoming calls, vibrating alerts, key sound etc. This can be useful when there are many users on the same handset, and they want different sound profiles. It can also be used for temporary settings, for example while in a meeting, incoming calls should be silent.

Profiles are configured via parameters in the "Profiles" folder.

- 1 Select "Profiles".
- 2 Select "Normal" or "Profile X" (where X represents 1- 4)
- 3 The following settings for the profile can be configured:
 - Profile name
 - Internal/External/Callback ring signal
 - Ring volume
 - Vibrator
 - Key sound
 - Answering settings
 - Diversion settings

Divisions

Calls can be diverted to other phone numbers, for example when busy.

- 1 In the applicable profile, select Divisions.
- 2 Activate a diversion by selecting "Enable" in the applicable diversion drop-down lists. The following diversions are possible:
 - Activate diversions for all calls
 - Activate diversions on user busy
 - Activate no answer diversions
- 3 Enter the diversion number in the applicable diversion number text field.
- 4 If the handset is configured to access the PBX via SIP protocol, the handset can be configured to manage the diversion locally instead of using the PBX. Requires that the handset is within the coverage area and is switched on.
Select VoIP > SIP. In the *Call forward locally* drop-down list, select "Enable".

6.5.7 Battery Warning

- 1 Select Device > Settings
- 2 In the *Battery warning* drop-down list, select one of the following:
 - Sound repeatedly
 - Sound once
 - Sound off

6.5.8 Uploadable Language

It is possible to upload one additional language to the handset. The language file is generated via an Excel file. The Excel file used to generate language files is delivered from your supplier.

NOTE: If another language file is uploaded, the first additional language is overwritten.

Certain special characters are allowed when generating the language file, see information in the Excel file.

To upload an additional language, do as follows:

- 1 In the Devices tab, select the device(s) to be uploaded with additional language.
- 2 In the Device menu, select "Upload language...".
- 3 If the uploaded language shall be used in the handset, see [6.5.9 Select Default Language](#) for more information.

6.5.9 Select Default Language

Defines the default operating language for the handset. This setting can later be changed by the user.

- 1 Select Device > Settings.
- 2 In the *Language* drop-down list, select the language to be used.
- 3 If the downloaded language is selected, it might be needed to select matching characters as text input language, and the sort order in the phonebook
In the *Input Language* drop-down list, select the text input language to be used.

NOTE: This parameter is only applicable for the downloaded language and cannot be changed by the user.

6.5.10 Short cuts

One click access to predefined functions can be configured for the Soft keys, Hot keys, Navigation keys, and the Multifunction button¹. It is for example possible to define the soft key to make a call.

1. The Multifunction button is applicable for and only.

Configure a Hot Key

A hot key is activated by pressing a preprogrammed button "0", "2" - "9" for more than 1 second in idle mode. The function is used, for example, to change profile or make a phone call to a specific number.

- 1 Select Shotcuts > Hot key X (where X is 0, 2 - 9).
- 2 Continue with [Additional Shortcut Settings](#).

Configure Soft Key

- 1 Select Shotcuts > Soft Key X (where X is Left, Middle, or Right)
- 2 In the Name field, enter the name of the soft key to be displayed in the handset.
- 3 Continue with [Additional Shortcut Settings](#).

Configure Navigation Key

- 1 Select Shotcuts > Navigation Key X (where X is Up, Down, Left, or Right)
- 2 Continue with [Additional Shortcut Settings](#).

Configure Multifunction Button

- 1 Select Short cuts > Multifunction Button X (where X is Longpress or Multipress)
- 2 Continue with [Additional Shortcut Settings](#).

Additional Shortcut Settings

- 1 In the Function drop-down list, select the function to be used:
 - Phone call
 - Call List
 - Contact list
 - Central phonebook (system dependent feature)
 - Change profile (if selecting profile 1-4, the profile must first be configured, see [6.5.6 Configure Profiles](#) on page 23.)
 - Open a menu
 - Presence
 - Call diversions
 - RSSI measurement
- 2 In the *Value* field, enter the applicable value. This is mandatory when using Phone call function.
- 3 In the Control Question drop-down list, select "Enable" if the *Proceed?* window shall be displayed after the key is pressed. This is used to avoid that a function is accessed by mistake.
- 4 In the *Read Only* drop-down list, select "True" if the user shall not be able to change the shortcut.

6.5.11 Soft Key Functions During Call

It is possible to access a predefined function by pressing the right soft key during a call.

- 1 Select Device > Call.
- 2 In the *Right in call soft key name* field, enter the name of the soft key to be displayed during a call.
- 3 In the *Right in call soft key action* drop-down list, select one of the following functions:
 - Conference
 - Contacts
 - Disabled
 - End Call
 - Hold
 - Loudspeaker
 - New call (put active on hold)
 - Retrieve
 - Switch
 - Transfer (to held call)
 - Transfer to new call (blind transfer)

6.5.12 Import Contacts

It is possible to import a phonebook file (that is, local phonebook) to a handset. The phonebook file is a tab-separated .txt file, and contains two items per row; number and name. The PDM is used to import the phonebook file to the handset. See Import Contacts in *Installation and Operation Manual, Portable Device Manager, Windows version, TD 92881EN*.

6.5.13 Company Phonebook

It is possible to create a phonebook that is administered centrally and uploaded to the handset from PDM. If this feature is used, entries from Contacts and Company Phonebook are merged. The Company Phonebook entries are locked and cannot be edited in the handset.

The following steps must be performed:

- 1 Create a Company phonebook file, see [Create a Company Phonebook File](#).
- 2 Import the Company phonebook file to PDM, see *Installation and Operation Manual, Portable Device Manager, Windows version, TD 92881EN*.
- 3 Upload the company phonebook file to the handset(s), see *Installation and Operation Manual, Portable Device Manager, Windows version, TD 92881EN*.

Create a Company Phonebook File

The company phonebook file (.cpb) is normally created from an Excel file using a script to extract the information and create to the phonebook file (.cpb). The Excel file, "Company Phonebook.xls" is delivered from your supplier.

The format of the rows in the phonebook file is:

<Name><tab><phone number><carriage return>

followed by additional rows for each entry.

The handset supports a maximum length of 24 characters in each field, additional characters are truncated when the phonebook file is created. The following characters are accepted in the handset number field in the phonebook file, but are ignored when the phonebook file is created: "(, ", "-", and " "(space).

6.5.14 Central Phonebook

NOTE: This is a system dependent feature.

If the network is equipped with a messaging server with a phonebook service, the Central Phonebook on that server can be accessed from the handset.

- 1 Select Device > Message centre.
- 2 In the *Central phonebook* field, enter the number to the Central phonebook
The number to be used is set to default 999999. If the system is not equipped with a Central Phonebook, this menu option can be removed from the handset by entering an empty value.

6.6 Telephony

The following parameters are required for the basic telephony settings.

6.6.1 Endpoint ID and Endpoint number

The Endpoint ID and Endpoint number will automatically be received when registering the handset in the VoWiFi system. The Endpoint ID is normally the user's name registered in the PBX and is displayed in the handset in idle mode. To change the name displayed in the handset, see [6.8.1 User Display Text](#) on page 32.

NOTE: If the Endpoint ID needs to be changed, this must be also done in the PBX.

6.6.2 VoIP Protocol

A protocol is a set of standard rules for data traffic required to send information over a communication channel. Communication protocol is basically following certain rules so that the system works properly. The following VoIP protocols are supported: H.323 and SIP.

- 1 Select VOIP > General.
- 2 In the *VoIP protocol* drop-down list, select "H.323" or "SIP".
- 3 Continue with chapter [H.323 Protocol](#) on page 28 or chapter [SIP Protocol](#) on page 28 depending on the selected protocol.

H.323 Protocol

If the H.323 protocol is used the Gatekeeper IP Address is usually automatically distributed. No configuration necessary.

- 1 Select VoIP > H.323.
- 2 The following settings are applicable for the H.323 protocol.
 - Gatekeeper IP address
 - Secondary Gatekeeper address
 - Gatekeeper listening port
 - Gatekeeper ID (name)
 - Gatekeeper password

SIP Protocol

The following SIP protocol parameters are located under VoIP > SIP:

- SIP Transport – defines the protocol to use for SIP signaling, either UDP, TCP or TLS. The setting TLS requires the PBX certificate to be uploaded as root certificate.
- Outbound proxy – Set to "Yes" if the handsets are to connect with the SIP proxy through an outbound proxy (there may be two). Set to "No" if the handsets are to connect directly with the SIP proxy (there may be two).
- Primary SIP proxy – defines the primary SIP proxy by a domain name, an IP address or an IP address together with a port number.
- Secondary SIP proxy – defines the secondary SIP proxy by a domain name, an IP address or an IP address together with a port number.
- Primary outbound proxy – defines the primary outbound proxy by a domain name, an IP address or an IP address together with a port number.
- Secondary outbound proxy – defines the secondary outbound proxy by a domain name, an IP address or an IP address together with a port number.

- Listening port – the port that the handset listens to for incoming SIP traffic.
- SIP proxy ID – defines the SIP proxy by a domain name.
NOTE: This parameter is only needed when an outbound proxy is defined. It may also be used to specify a domain name when parameters Primary SIP proxy and Secondary SIP proxy have been assigned IP-addresses.
- SIP proxy password
- Send DTMF using RFC 2833 or SIP INFO – this parameter defines which path the DTMF signalling should take. If set to "RFC 2833", the DTMF signalling will be sent in the RTP stream, i.e. from handset to handset. If set to "SIP INFO", the DTMF signalling will be sent using SIP signalling, i.e. via the PBX.
- Hold type – defines type of hold to send when the handset puts a call on hold. The selection depends on what type of hold the PBX support. For more information about what type of hold the PBX support, see the applicable documentation for the PBX.
- Registration identity – defines if the endpoint shall use its number or ID for the registration with the SIP proxy.
- Authentication identity – defines if the endpoint shall use its number or ID for the authentication with the SIP proxy.
- Call forward locally – when enabled the call forwarding is handled locally by the handset instead of updating the PBX.
NOTE: The handset must be switched on and within coverage to handle this.
- MOH locally – Music on hold is played by the handset i.e. if the PBX does not supply MOH the handset plays a tone when the call is on hold.
- Hold on transfer – puts a second call on hold before transfer, which is required by some SIP proxy servers.
- Direct signaling – defines whether calls originating from other sources than the configured SIP Proxy should be accepted or redirected using "USE PROXY" message.

6.6.3 Codec

A codec encodes a stream or signal for transmission. Codecs are often used in streaming media applications. This setting defines how to packetize and compress the sound in a voice call.

- 1 Select VoIP > General.
- 2 In the *Codec configuration* drop-down list, select the applicable codec. The following are possible:
 - G.711 A-law (EU)
 - G.711 u-law (US)
 - G.729
 - G.729A
 - G.722
- 3 In the *Codec packetization time configuration* drop-down list, select packetization time to use for speech (value between 10 and 60 ms). Default value is 20 ms.

6.6.4 Internal Call Number Length

Defines the maximum number of digits to be interpreted as an internal call. "0" means the same number of digits as in the endpoint number.

- 1 Select VoIP > General.
- 2 In the *Internal call number length* field, enter the number of digits.

6.6.5 Emergency Number

This is a phone number for emergency calls. It is always possible to call this number, regardless of whether phone-lock or key-lock are active or not.

- 1 Select Device > Call.
- 2 In the Emergency number field, enter the emergency number.

6.6.6 Voice Mail Number

In some systems it is needed to assign the handset number of the Voice Mail service.

- 1 Select Device > Message centre.
- 2 In the *Voice mail number* field, enter the number to the handset's voice mail inbox.

6.6.7 Max number of Call Completions

Specifies the maximum number of call back requests the handset can handle.

- 1 Select Device > Call.
- 2 In the *Max number of call completions* drop-down list, enter number of calls

6.6.8 Dial Pause Time

By adding a "P" to a phone number, a pause is added and will be activated when dialling. For how long is defined here.

- 1 Select Device > Call.
- 2 In the *Dial pause time* field, enter a pause time between 1 - 3 seconds.

6.6.9 Direct off Hook from Charger

The handset will automatically answer a call (that is quick answer) when removed from the charger.

- 1 Select Device > General.
- 2 In the *Direct off hook from charger* drop-down list, select "Enable".

6.6.10 Replace Call Rejected with User Busy

Is used if the system does not support call rejected.

- 1 Select Device > General.
- 2 In the *Replace Call Rejected with User Busy* drop-down list, select "Enable".

6.7 Regional Settings

This section include settings suitable for a specific region or country.

6.7.1 Set Time & Date

- 1 Select Device > General.
- 2 In the *Time zone* drop-down list, select the applicable time zone.
- 3 In the *NTP server* field, enter the address to the time server. If not set, the IP PBX address is used.
- 4 Select Device > Settings.
- 5 In the *Time format* drop-down list, select the applicable time format:
12h (for example 11:59 am/pm)
24h (for example 23:59)
- 6 In the *Date format* drop-down list, select the applicable date format:
DD/MM/YYYY, for example, 31/01/2010 (also called Europe)
MM/DD/YYYY, for example, 01/31/2010 (also called US)
YYYY-MM-DD, for example, 2010-01-31 (ISO 8601)
MMM DD YYYY, for example, Jan 31 2010
DD MMM YY, for example, 31 Jan 10
DD.MM.YYYY, for example, 31.01.2010
DD-MM-YYYY, for example, 31-01-2010

6.7.2 Select Default Language

Defines the default operating language for the handset. This setting can later be changed by the user.

- 1 Select Device > Settings.
- 2 In the *Language* drop-down list, select the language to be used.
- 3 If the downloaded language is selected, it might be needed to select matching characters as text input language, and the sort order in the phonebook
In the *Input Language* drop-down list, select the text input language to be used.

NOTE: This parameter is only applicable for the downloaded language and cannot be changed by the user. See [6.5.8 Uploadable Language](#) on page 24 for more information.

6.7.3 Dialling Tone Pattern

Defines which tone pattern to use when dialling.

- 1 Select Audio > General.
- 2 In the Dialling tone pattern drop-down list, select the applicable region.

6.8 Display

6.8.1 User Display Text

Defines a text to be shown in the display in idle mode instead of the endpoint ID. If nothing is entered in this text field, the endpoint ID will be shown.

- 1 Select Device > Settings.
- 2 In the *User display* text field, enter the text to be displayed.

6.8.2 Font style

The display font style can be changed to bold for increased readability.

- 1 Select Device > Settings.
- 2 In the *Font style* list, choose Normal or Bold.

6.8.3 Backlight Timeout

Numbers of seconds before the backlight is turned off.

- 1 Select Device > General.
- 2 In the *Backlight timeout* field, enter number of seconds before the backlight is turned of when handset is idle.

6.8.4 Brightness

- 1 Select Device > Settings.
- 2 In the *Brightness* drop-down list, select one of the following:
 - Normal - maximum backlight will be used.
 - Power save - reduced backlight will be used.

6.8.5 Screen Saver

- 1 Select Device > Settings.
- 2 In the *Screen saver* drop-down list, select one of the following:
 - Information - time and status will be displayed when the screen saver is activated.
 - Black - no information will be displayed when the screen saver is activated.

6.9 Menu Operation

6.9.1 Hide Menu Items

It is possible to hide menu items for the users. To hide or show a menu item, do the following:

- 1 Select Customization > Visibility.
- 2 Select "Hide", "Show", or "Read only" for the applicable menu item in the drop-down list. If "Read only" is selected, the menu item will be visible in the handset, but cannot be edited by the user. The following items can be hidden:
 - Connections (Network, Headset etc.)
 - Calls
 - Contacts
 - Short cuts (Soft keys, Hot keys etc.)
 - Profiles
 - Settings (Sounds, Display, Language etc)

6.10 Presence Management

NOTE: This is a system dependent feature.

To be able to configure presence management, the following must be known:

- The IP address to the Presence Management system.
- The user name and password used in the Presence Management system for each handset.

For more information about presence management, see *User Manual, WLAN Handset, TD 92922EN*.

- 1 Select Presence > Common.
- 2 In the *Presence Management* system drop-down list, select presence management system.
- 3 Select "Presence" and the presence management system selected in previous step.
- 4 In the *IP address* field, enter the IP address to the presence management system.
- 5 In the *Listening port* field, enter the port number the presence management system shall listen to.
- 6 In the *user name* field, enter the user name.
- 7 In the *password* field, enter the password.

If the Presence function is configured, it will be visible under Call > Presence in the handset. It is also possible to configure a shortcut in order to access the Presence menu, see [6.5.10 Short cuts](#) on page 24.

7. Use Handset to Verify the VoWiFi System Deployment

7.1 Site Survey Tool

It is recommended to do site surveys with the built-in tools in the handset.

This provides a true measurement of the RF environment based upon the radio of the handset. Wireless analysers may be used to provide additional assistance during a site survey.

7.2 Scan the Channels

To be able to use the site survey functions in the handset, it must be configured correctly.

Default configuration for the handset is to use channels 1, 6 and 11. If the handset is intended for site survey use, scanning all channels will be limited to 1, 6 and 11.

The table is upgraded regularly, starting with scanning channel 1, then 6 and last 11. In between, the handset is in sleeping mode. The handset consults this table when making roaming decisions.

It is possible to scan all 802.11b/g/n channels, or scan all 802.11a/n channels by setting the parameter *802.11b/g/n channels* or *802.11a/n channels* to "All", respectively.

For 802.11b/g/n channels, it is strongly recommended to set back the handset to "1,6,11" before normal use. For 802.11a/n channels, it is strongly recommended to set back the handset to "UNII-1" before normal use.

The World mode regulatory domain will also affect which channels that may be used. To scan channels 1-11 it is recommended that the handset is configured so the "World mode regulatory domain" parameter is set to "USA". If also scanning of channels 12 and 13 is of interest use value "ETSI".

There are three ways of scanning channels:

- Scan all channels
- Scan a specific channel

7.2.1 Scan all Channels

This gives a filtered list of the channels in the SSID found during the scan.

- 1 There are two options to access the Site Survey Tool meny:
 - If the handset has been factory reset or not configured; in idle mode, enter "40022", select "Site survey tool".
 - If the handset has been configured; in idle mode, enter "*#77#".
- 2 Select "Scan all channels".
- 3 Select the SSID to display the associated AP.
- 4 Select an AP to display information such as SSID, Channel, MAC address, Beacon period, QoS, and Privacy.

7.2.2 Scan a Specific Channel

This gives a list of all the APs found on that channel in the specified SSID.

- 1 There are two options to access the Site Survey Tool meny:
 - If the handset has been factory reset or not configured; in idle mode, enter "40022", select "Site survey tool".
 - If the handset has been configured; in idle mode, enter "*#77#".
- 2 Select "Scan selected channel".
- 3 Enter the channel to be scanned.
- 4 Select an AP to display information such as SSID, Channel, MAC address, Beacon period, QoS, and Privacy.

7.3 Range Beep

The range beep function enables a beep to be played whenever the handset experiences a filtered field strength of below the configured value (default -70 dBm) from the currently associated access point. Since the value is filtered, sudden drops in field strength caused by the environment, for example walking through a door into a room, will be delayed, thus it is important to walk slowly through the site to cover all weak spots.

7.3.1 Configurable RSSI Threshold

The RSSI threshold of the handset is set to -70 dBm (default). In the site survey menu there is the possibility to change the RSSI threshold. This is useful if a specific area is designed to have another coverage level than -70 dBm.

- 1 There are two options to access the Site Survey Tool meny:
 - If the handset has been factory reset or not configured; in idle mode, enter "40022", select "Site survey tool".
 - If the handset has been configured; in idle mode, enter "*#77#".
- 2 Select "Range beep level".
- 3 Enter the new RSSI threshold and press "OK".

7.3.2 Range Beep on a Configurable RSSI Threshold

A beep is played when the signal goes below the selected threshold.

- 1 There are two options to access the Site Survey Tool meny:
 - If the handset has been factory reset or not configured; in idle mode, enter "40022", select "Site survey tool".
 - If the handset has been configured; in idle mode, enter "*#77#".
- 2 Select "Range beep".
- 3 Select one of the following:
 - On - Activates the range beeps
 - Off - Deactivates the range beeps

8. Handset Internal Web Administration Page

The internal web administration page for the handset makes it possible to:

- Troubleshoot the VoWiFi System.
- View statistics

8.1 Access the Handset's Internal Web Administration page

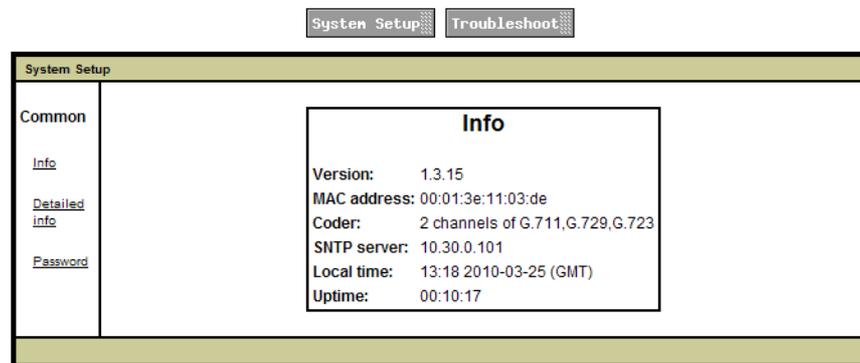
In a web browser, enter the handset's IP address to access the internal web administration page for the handset. The IP address can be found in the handset's menu (Settings >Device info >Network info).

8.1.1 System Setup View

In the System Setup view, the following are shown:

- Software version
- MAC address
- Coder
- SNTP server
- Local time
- Uptime

Figure 3.



The information view

Enter administration user name and administration password to access further pages.

Default user name and password for an administrator:

- User name: admin
- Password: changeme

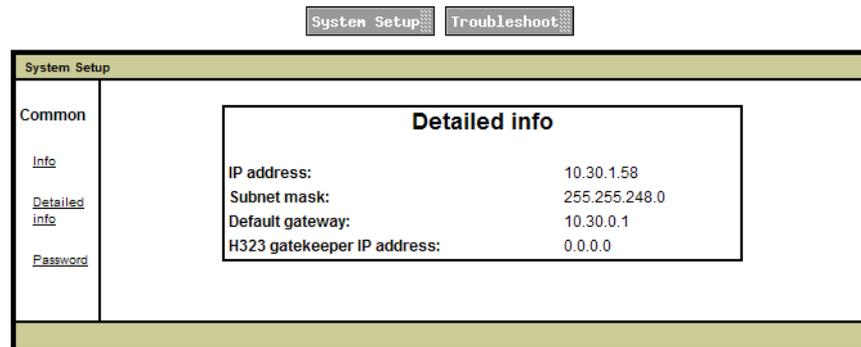
NOTE: If the user name or password is forgotten, it can be changed in the PDM. See [8.2.2 Change password via the PDM](#) on page 38.

Show Detailed Information

Click the *Detailed info* link. The following information are shown (see [figure 4](#)):

- IP address
- Subnet mask
- Default gateway

Figure 4.



Internal Web Administration Page - Detailed Information

8.1.2 Troubleshoot View

- 1 In a web browser, enter the handset's IP address to access the internal web administration page for the handset. The IP address can be found in the handset's menu (Settings >Device info >Network info).
- 2 Click the "Troubleshoot" button.
- 3 If needed, enter administration user name and administration password to access further pages.

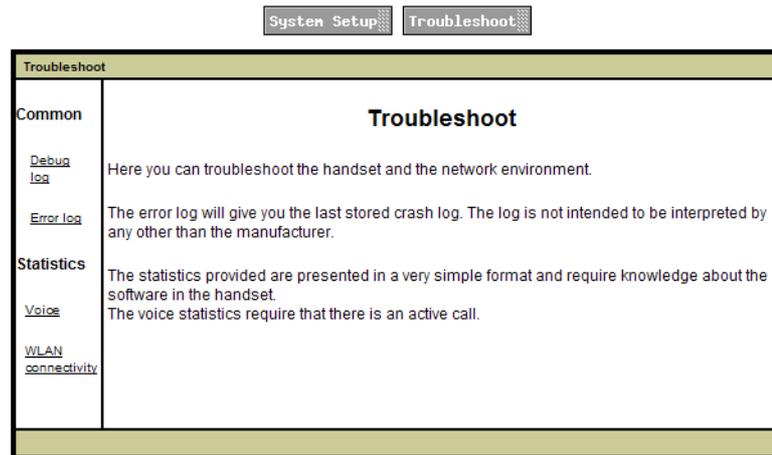
Default user name and password for an administrator:

- User name: admin
- Password: changeme

In the *Troubleshoot* view, the following can be shown (see [figure 5](#)):

- Debug log
- Error log
- Voice calls statistics
- WLAN connectivity statistics

Figure 5.



Internal Web Administration Page - Troubleshoot view

8.2 Change Administration Password

The administration password can be changed either via the internal Web Administration page or via the PDM.

8.2.1 Change password via the handset's Internal Web Administration page

- 1 In a web browser, enter the handset's IP address to access the internal web administration page for the handset. The IP address can be found in the handset's menu (Settings >Device info >Network info).
- 2 Click the "Password" link.s
- 3 In the *User* field, enter the new user name .
- 4 In the *Password* field, enter the new password.
- 5 Confirm the new password and click the "Change" button.

8.2.2 Change password via the PDM

- 1 Open the PDM.
- 2 Select Device > General.
- 3 In the *Administration user name* field, enter user name.
- 4 In the *Administration password* field, enter password.

9. Administration

9.1 Admin Menu Tree

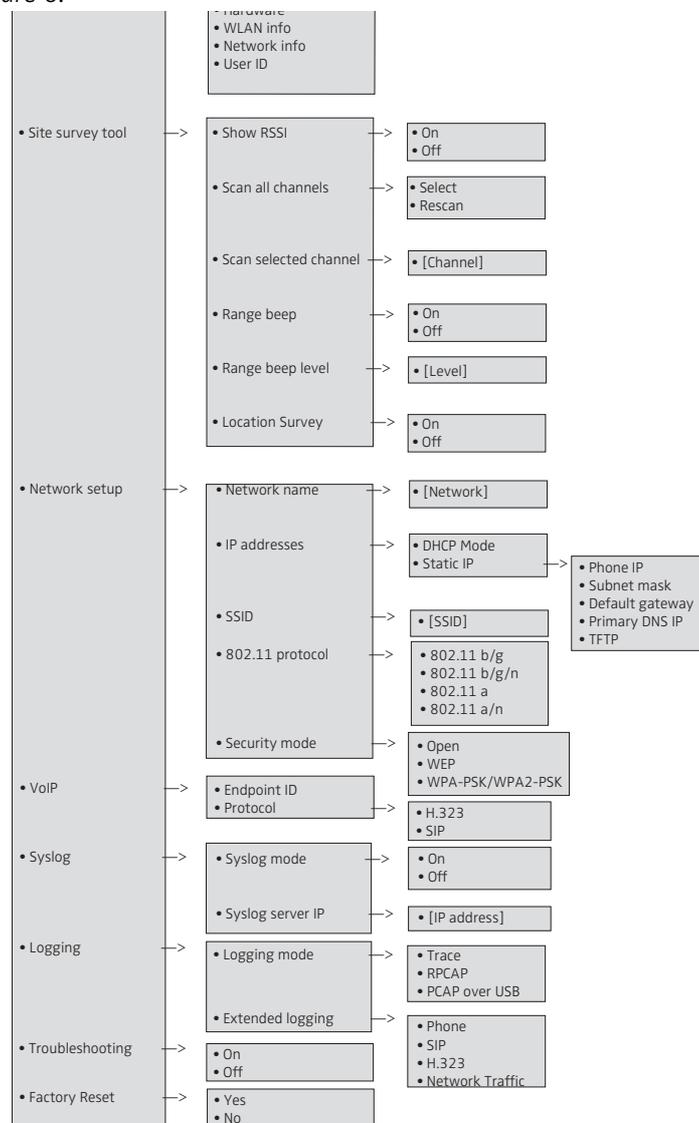
The handset has a hidden menu for system administrators. The Admin menu contains:

- Software and hardware information
- WLAN, network, system information
- Site survey tool
- Network setup menus
- Factory reset option

To activate the Admin Menu, select Menu > Settings and press 40022.

The following figure shows the menu tree for the Admin menu in the handset.

Figure 6.



Admin Menu in the Handset. Other menus are described in User Manual, WLAN Handset, TD 92922EN.

9.2 Quick Access to the Handset's Device Information

For quick access to device information, short codes can be used from the idle menu. To display this information, enter the following codes in the handset.

Information	Code
Software version	*#34# > Software
Hardware version	*#34# > Hardware
IP address	*#34# > Network info
Subnet mask	*#34# > Network info
Default gateway	*#34# > Network info
MAC address	*#34# > Hardware
Current BSSID	*#76#
Current ESSID	*#76# or *#34#
Current RSSI	*#76#
Current channel	*#76#
Site survey functions	*#77#

NOTE: Other settings and information can be found on the internal web administration page, refer to chapter 8. [Handset Internal Web Administration Page](#) on page 36.

9.3 LED indications

The following table shows the LED indications that are used for the handset.

LED indication	Description
None	Switched off.
Green, fixed	Handset fully charged and in charger.
Green, flashing, slow	Switched on, but not in charger.
Orange, fixed	Charging
Orange, flashing	Low battery
Red, fixed	Software error. Service needed.
Red, flashing	Very low battery
Red, flashing, slow:	No network connection.

10. Troubleshooting

This section contains information on how to solve common operational problems, and information on warnings you may receive.

Go through the following lists if you encounter any problems. If this checklist does not solve the problem, contact the system administrator.

If other users have similar problems, there may be a system error.

10.1 Fault Symptoms

If any of the following Fault Symptoms occur, follow the instructions below.

Fault	Probable cause	Action or comment
The display stays dark	Low battery level or faulty handset.	Charge the battery. If the handset does not work after charging, contact the system administrator.
There is no ring signal	"Ringer off" icon is on, or ringer volume is set to silent, or faulty handset.	Press and hold the Mute key, or increase volume (in the handset, select Settings > Sound & Alerts > Volume) or contact the system administrator.
Connected call but no sound or one way sound	IP addressing fault, or muted or bad speaker/ microphone	1) Note the IP address of the handset. Turn the handset off and ping the IP address. If something is found, the problem is an IP address conflict. 2) Check if the handsets are muted. 3) Use a headset to eliminate bad speakers/microphone.
Voice quality is bad	Increased traffic load or interference.	1) Check if QoS is working in both directions. Voice traffic should be prioritized on both the LAN and the WLAN. 2) Connect to other phones (wired, analogue or external) to determine if it is the other end that may cause bad quality. 3) Do a site survey and check for areas with under/over coverage and other interfering 802.11 systems. 4) Do a network performance test to ensure the wired LAN/backbone has adequate capacity. 5) Use a spectrum analyser and look for non 802.11 interference.

Fault	Probable cause	Action or comment
Battery life is bad	DTIM might not be set correctly. U-APSD is not used.	<ol style="list-style-type: none"> 1) Check "Beacon interval" and "DTIM" settings in the AP. 2) Verify the coverage, since low signal strength will make the handset to constantly search for other APs and thereby consuming more power. 3) Use a sniffer and check the amount of broadcast traffic that is transmitted on the WLAN. 4) Check if correct models of the chargers are used. 5) Verify with another battery. 6) If the system is supposed to use U-APSD for voice calls check the voice power save mode parameter in the PDM.

10.2 Display Information

The following error messages can be shown in the handset display:

Display shows	Probable cause	Action or comment
No access	The handset is in range, but has no access rights. Handset has found and associated to the WLAN (a wireless network with the configured SSID and correct security settings). But it cannot connect to the gatekeeper.	<p>Switch off the handset and then switch it on again. If this does not work, contact the system administrator.</p> <ol style="list-style-type: none"> 1) Check if the handset has an IP address by entering the "Network info" screen. If not check the WEP key if used or WPA/WPA2 passphrase. 2) If using WEP, double-check the key if the handset has no IP address. If you have a wireless sniffer, configure it to the correct key and try to decode packets both from and to the handset. 3) Check the Gateway address. Try to ping the gateway from another PC.

Display shows	Probable cause	Action or comment
<p>No network. (The handset beeps once a minute with a low tone followed by a high tone (during max 30 minutes). If the vibrator is enabled, it vibrates after the last beep.)</p>	<p>The handset is out of coverage, or faulty handset. The handset cannot find the wireless infrastructure with settings matching those configured in the handset.</p>	<p>The beeps can be stopped with the mute button. Then go into range. Note: When re-entering the coverage area it can take a couple of minutes before the handset automatically has registered into the system. If this does not work, contact the system administrator. 1) Check the SSID. The SSID configured in the handset must be identical to the SSID configured in the system infrastructure. 2) Check the security settings. The security settings, that is, authentication and encryption must match the settings in the system infrastructure. 3) Check for 802.11d multi regulatory domain settings. The handset (software version 2.x.x) must be able to detect in which country it is located to use the correct channel and transmit power settings. Later versions have a parameter specifying if 802.11d should be used or not. This is provided by the infrastructure according to the 802.11d standard. 4) Check which channels are used. The handset uses by default channel 1, 6 and 11. If the infrastructure is configured to use any other channel, change it to use only 1, 6 and 11 as this is the recommended setting. 5) Check that the correct Network (A, B, C or D) setting is selected.</p>
<p>SERVICE NEEDED Parameters corrupt Note: This display message is only shown in English.</p>	<p>Faulty handset.</p>	<p>Select the reset option on the middle soft key. If this is not available or the problem persists send the handset for service.</p>
<p>Enter PIN code</p>	<p>Phone lock is activated.</p>	<p>Enter the required PIN code. If the PIN code has been lost, enter a new PIN code via the PDM or do a factory reset via the PDM.</p>
<p>Battery low, charge now</p>	<p>The battery level is low.</p>	<p>Charge the handset, or replace or charge the battery.</p>

Display shows	Probable cause	Action or comment
Phonebook is not available at the moment.	The phonebook is not activated or does not respond.	Try again later or if the fault persists do a factory reset via the admin menu or via the PDM. Note that it may take several minutes for the phonebook to be available if there are many entries in Contacts and/or company phonebook.
Voice mail number not defined	There is no Voice mail number defined in the handset.	Define a Voice mail number via the PDM.

10.3 Troubleshooting from the handset Internal Web Administration Page

It is possible to view statistics for Voice and WLAN connectivity and to create debug and error logs from the internal web administration page. The logs and the statistics can then be interpreted by your supplier.

- 1 In a web browser, enter the handset's IP address to access the internal web administration page for the handset. The IP address can be found in the handset's menu (Settings >Device info >Network info).
- 2 Click the "Troubleshoot" button.
- 3 If needed, enter administration user name and administration password to access further pages.

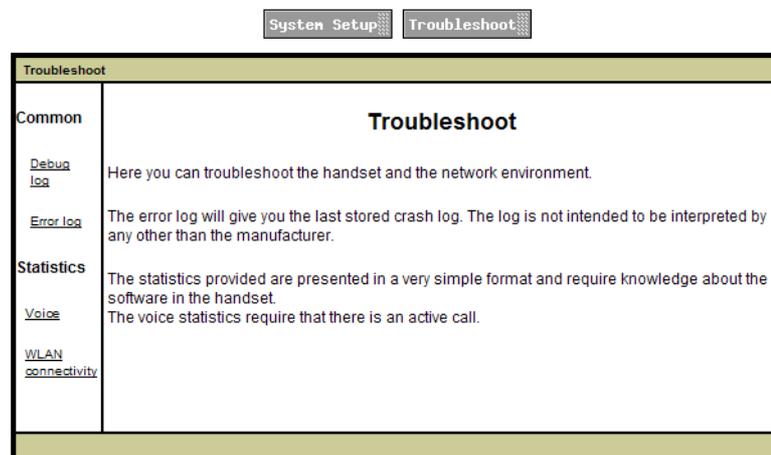
Default user name and password for an administrator:

- User name: admin
- Password: changeme

In the *Troubleshoot* view, the following can be shown (see [figure 7](#)):

- Debug log
- Error log
- Voice calls statistics
- WLAN connectivity statistics

Figure 7.



Troubleshoot page

11. Related Documents

Data Sheet, WLAN Handset	TD 92920EN
Quick Reference Guide, WLAN Handset	TD 92921EN
User Manual, WLAN Handset	TD 92922EN
Data Sheet, DP1 Desktop Programmer for WLAN Handset	TD 92925EN
Data Sheet, Portable Device Manager (PDM), Windows version	TD 92895EN
Installation and Operation Manual, Portable Device Manager, Windows version	TD 92881EN

12. Document History

For details in the latest version, see change bars in the document.

Version	Date	Description
A	31 May 2012	First version

Index

A

Audio adjustment 21

C

Central Phonebook 27

certificate 20

certificates 7

Company Phonebook 26

F

Factory reset 11

H

Headset configuration 22

I

Import Contacts 26

Installation 6

L

LED indications 40

P

PDM 2

Profiles 23

S

Shortcuts 24

Site Survey Tool 24

T

TFTP 10