

# Mitel MiVoice Office

5624 WIFI PHONE CONFIGURATION GUIDE FOR MIVO 250

Release 6.2



## **NOTICE**

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

## **Trademarks**

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at [legal@mitel.com](mailto:legal@mitel.com) for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

## **5624 Wifi phone Configuration guide for MiVO 250**

Release 6.2

June 2016

®,™ Trademark of Mitel Networks Corporation  
© Copyright 2016, Mitel Networks Corporation  
All rights reserved

Introduction . . . . .	2
Abbreviations and Glossary . . . . .	3
Functionality matrix . . . . .	4
Pre-Installation. . . . .	6
VoWiFi System IP addresses . . . . .	6
Programming the WiFi Handset. . . . .	7
WinPDM . . . . .	7
WSM3 . . . . .	7
Over-the-Air . . . . .	8
Installation of WiFi Handsets . . . . .	9
Handset Installation in the WLAN System using Easy Deployment . . . . .	10
Installation with Central Device Management (WSM3) . . . . .	10
Create a Network Template in the Device Manager in the WSM3 . . . . .	11
Create a Common Template in the Device Manager in the WSM3 . . . . .	11
Create Numbers in the WSM3 . . . . .	12
Create a Network Template with Initial Configuration in the WinPDM . . . . .	12
Installation with WinPDM . . . . .	13
Installation using the Handset's Admin Menu . . . . .	15
Configure a Handset with a Template . . . . .	15
Create a template . . . . .	15
Apply a Template to a Handset with a Number . . . . .	16
Apply a Template to a Handset without a Number . . . . .	16
Save Handset Configuration as a Template . . . . .	16
Synchronizing a Handset with WinPDM . . . . .	17
Configure Handset without Saving It in WinPDM . . . . .	17
Maintenance . . . . .	18
Handset . . . . .	18
Configure Spare Handsets without a Number in Large Systems . . . . .	18
Upgrade Handset Software . . . . .	19
Upgrade Software OTA using TFTP . . . . .	19
Upgrade Software using WinPDM . . . . .	20
Upgrade Software Over the Air (OTA) through Centralized Device Management (WSM3) . . . . .	20
Recapture the Earlier Software . . . . .	20
Upgrade Handset Functionality using License . . . . .	21
Perform a Factory reset . . . . .	23
Replacement of Handsets . . . . .	24
Replacement Procedure Choice . . . . .	24
Replacement of Handset with WSM3 . . . . .	24
Replacement of the Handset with WinPDM and WSM3 . . . . .	26
Replacement of Handset with WinPDM Only . . . . .	27
Change Number of a Handset . . . . .	29
Update Parameters using WSM3 . . . . .	29

Perform a Security Upgrade using WSM3 .....	29
Upgrade the Template .....	30
Create a Configuration Backup .....	30
Handset Configuration .....	31
Select Network .....	31
Change Active Network .....	31
Change Name of Network .....	31
Enable Switch between Networks .....	31
IP Address Settings .....	32
Automatic IP Address Settings .....	32
Static IP Address (Manual) Settings .....	32
Network Settings .....	32
SSID .....	32
Voice Power Save Mode .....	33
World Mode Regulatory Domain .....	33
Radio and Channel Selection .....	33
Transmission Power .....	34
IP DSCP for Voice/Signaling .....	35
Security Settings .....	35
Open .....	35
WEP 64/128-bit Key .....	35
WPA-PSK & WPA2-PSK .....	36
802.1X with EAP-FAST .....	36
802.1X with PEAP-MSCHAPv2 .....	36
EAP-TLS .....	36
Handset Settings .....	37
Automatic key lock .....	38
Phone lock .....	38
Automatic lock time .....	38
Automatic key unlock .....	38
Audio adjustment .....	38
Headset Configuration .....	39
Actions when the Handset is Placed in the Charger .....	40
Hide Missed Call Window .....	41
Prevent Handset Switch off .....	41
Prevent Mute function .....	41
Prevent Calls from being saved in the Call list .....	42
Battery Warning .....	42
Shared Phone .....	42
Uploadable Language .....	42
Select Default Language .....	43
Shortcuts .....	43
Soft Key Functions During Call .....	44
In-call Menu .....	45

Call Services Menu .....	46
Import Contacts .....	46
Company Phonebook .....	47
Central Phonebook .....	47
Profiles .....	47
User Profiles .....	47
System Profiles .....	48
Telephony .....	52
Endpoint ID and Endpoint number .....	53
VoIP Protocol .....	53
Codec .....	55
Offer Secure RTP .....	55
Internal Call Number Length .....	55
Emergency Call Numbers .....	55
Voice Mail Number .....	56
Message Centre Number .....	56
Max number of Call Completions .....	56
Dial Pause Time .....	56
Direct off Hook from Charger .....	56
Replace Call Rejected with User Busy .....	57
Call waiting behavior .....	57
Connecting 5624 WiFi Phones to MiVoice Office 250 .....	57
Peripheral Devices for 5624 WiFi Phone .....	57
MiVoice Office 250 Database Programming .....	57
SIP Phone Creation .....	59
5624 WiFi Phone Configuration .....	64
MiVO 250 Feature Compatibility .....	69
Regional Settings .....	70
Set Time & Date .....	70
Select Default Language .....	71
Dialing Tone Pattern .....	72
Display .....	72
User Display Text .....	72
Rotate Display Text .....	72
Font style .....	72
Backlight Timeout .....	72
Brightness .....	72
Screen Saver .....	72
Menu Operation .....	73
Hide Menu Items .....	73
Services .....	73
Push-To-Talk (PTT) Group Call .....	74
Presence Management .....	74
Location .....	75
Configure Handset for Cisco/Ekahau RTLS Solution .....	75

Use Handset to Verify the VoWiFi System Deployment .....	76
Site Survey Tool .....	76
Scan the Channels .....	76
Scan all Channels .....	76
Scan a Specific Channel .....	77
Range Beep .....	77
Configurable RSSI Threshold .....	77
Range Beep on a Configurable RSSI Threshold .....	77
Location Survey .....	78
Handset Internal Web Administration Page.....	79
Access the Handset's Internal Web Administration page .....	79
General View .....	79
Troubleshoot View .....	80
Change Administration Password .....	80
Administration .....	81
Admin Menu Tree .....	81
Quick Access to the Handset's Device Information .....	82
LED indications .....	82
Troubleshooting.....	83
Fault Symptoms .....	83
Display Information .....	84
Troubleshooting from the handset Internal Web Administration Page .....	86
Related Documents .....	87
 <b>Appendix A:</b>	
<b>Working with Templates</b>	
Create a Template .....	90
Export a Template .....	90
Import a Parameter File .....	90
Import a Template .....	91
 <b>Appendix B:</b>	
<b>Programming Custom Sound</b>	
.....	96
 <b>Appendix C:</b>	
<b>Easy Deployment</b>	
Prerequisites .....	98
WLAN discovery .....	99
WSM3 server discovery .....	100
Server discovery using the DHCP Option 43 .....	100
Server discovery using the Ascom Service Discovery Protocol (ASDP) .....	100

Parameter download .....	101
Using Easy Deployment together with Client Certificate Distribution .....	101
The Ascom Service Discovery Protocol (ASDP) Explained .....	101
DHCP Vendor Options Explained .....	102
Configuration Example of a Linux Server using DHCP Option 43 .....	107
Configuration Example of an MS Windows 2003 Server using DHCP Option 43 .....	107
Configuration of Option 60 and 43 using the standard DHCP vendor class .....	108
Advanced Configuration of Option 60 and 43 using a new vendor class .....	109
Easy Deployment and VLAN .....	111
Easy Deployment and Certificates .....	112
Troubleshooting Easy Deployment in an MS 2003/2008 DHCP Server .....	113







---

## About this document

### *Cross-references in the document*

Throughout this document you will find cross-references in the text which indicate further details that can be found in other sections of this document. The cross-references are colored blue and linked to the relevant place in the document (example: see section on page 87). Positioning your cursor over the cross-reference text and clicking the left mouse button will take you to the relevant section.

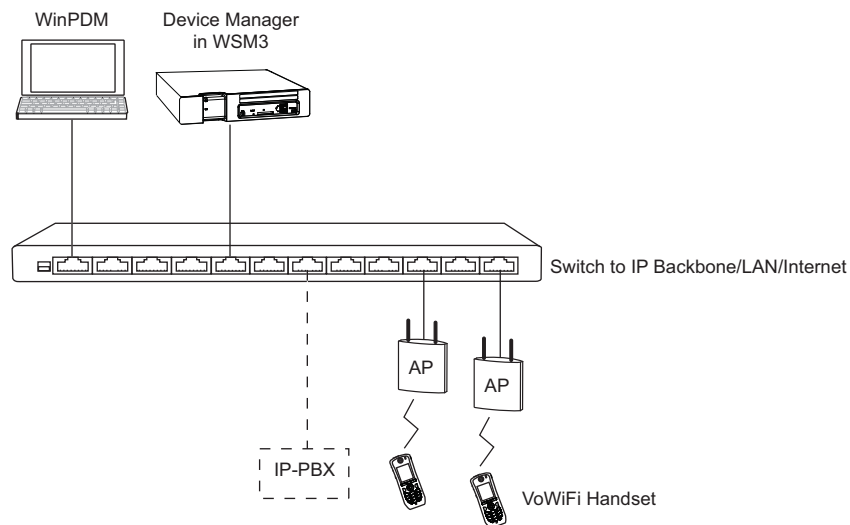
To return to the original page after viewing a cross-referred page in Adobe Acrobat or Adobe Reader, click on the “Previous View” arrow ( or ).

## Introduction

This document is a guide for installing, configuring, and maintaining the functionality of the Mitel WiFi 5624 Handsets.

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

Figure 1. VoWiFi System



This document provides guidelines to install the Mitel WiFi 5624 Handset in a VoWiFi system. The document describes the settings needed to make the handset function in a VoWiFi system, and is targeted at the following personnel:

- System Administrator
- Service Technician

The handset is first configured using Easy Deployment, or using the Portable Device Manager (WinPDM). In small systems where it is possible to collect all handsets to update settings, daily maintenance is also done by using the WinPDM. In larger installations, the Device Manager application in the Wireless Service Messaging gateway (WSM3) supports managing the handsets centrally using a web interface, without the need to collect the handsets.

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.

---

## 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.
802.1D	IEEE MAC Bridges standard (interworking for 802.11 among others).
802.1X	IEEE standard for port-based Network Access Control (authentication).
Ad-hoc WLAN	A WLAN between two wireless capable devices (normally PCs), where no Access Point (AP) is involved.
AES	Advanced Encryption Standard.
ALS	Acoustic Location Signal
AP	Access Point
BSS	Basic Service Set. A WLAN with at least one AP that is configured for it.
BSSID	Basic Service Set Identifier. Hard-coded 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
Device Manager	Application for managing devices, editing parameters, and updating devices with new software, without an administrator manually needing to collect the devices, as it is done by Centralized Management over the air (OTA). The Device Manager application runs on an WSM3 hardware.
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 using secure tunneling.
EAP-TLS	EAP-Transport Layer Security.
ELISE	Embedded Linux SErver: A hardware platform used for Unite modules
ESS	Extended Service Set. WLAN with multiple APs sharing the same SSID.
ESSID	Extended Service Set Identifier. The identifying name of a WLAN. It identifies an AP and distinguishes WLANS from one another. An ESSID is one type of SSID (BSSID is the other).
IM	Interactive Messaging makes it possible to access information from an application, and controlling the information, by selecting a choice received in a message.
License	An authorization to use a licensed function.
MAC	Medium Access Control.
MWI	Message Waiting Indication
NTP	Network Time Protocol
OTA	Over The Air
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.
PRI	Primary Rate Interfaces
RSSI	Received Signal Strength Indication.
RTLS	Real-Time Location System
RTS	Request-To-Send.
PTT	Push-To-Talk

Services	Services are predefined functions such as Phone Call, Send Data, Send Message etc. that are accessible from the Service menu.
SIP	Session Initiation 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 ESS wireless 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.
Unite	Name of Ascom IP based system for handling, events, messages, and alarms.
UP 6	User Presence (value between 0-7). Wireless QoS at the MAC Layer.
VoIP	Voice over IP.
VoWiFi	Wireless version of VoIP. Refers to an IEEE 802.11a, b, g, n network.
VoWLAN	Voice over WLAN.
WEP	Wired Equivalent Privacy.
Wi-Fi	Wireless Fidelity. The commonly understood name for wireless LAN networks. Originator is Wi-Fi Alliance.
WinPDM	Portable Device Manager (Windows version): Used for managing devices, editing parameters, and updating devices with new software.
WLAN	Wireless Local Area Network. Refers to an IEEE 802.11a, b, g, 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).
WSM3	Wireless Service Messaging gateway: Unite module that enables wireless services to and from the handsets in a WLAN system. It also includes the Device Manager.

## Functionality matrix

The following matrix shows the functionality that currently can be used by the different versions. These functions require configuration in the WinPDM.

	Mitel 5624	Mitel 5624 Services	Mitel 5624 Personal Alarm
Company Phonebook	Yes	Yes	Yes
Central Phonebook	Yes	Yes	Yes
Centralized Management	Yes	Yes	Yes
Customized GUI	Yes	Yes	Yes
System profiles	No	Yes	Yes
Interactive Messaging (IM)	No	Yes	Yes
Location	Yes	Yes	Yes
Push to Talk (PTT)	No	Yes	Yes
Multifunction button	Yes	Yes	No
Push Button Alarm	No	No	Yes
Man-down and No-movement alarm <sup>a</sup>	No	No	Yes
Acoustic Location Signal (ALS)	No	No	Yes
Services	No	No	Yes
Voice Mail	Yes	Yes	Yes
Upload Language	Yes	Yes	Yes
Clear lists in charger	Yes	Yes	Yes

a. These functions require a license.

---

The three versions Mitel 5624, Mitel 5624 Services, and Mitel 5624 Personal Alarm use the same hardware and software and features are enabled by licensing. The Mitel 5624 version is an unlicensed WiFi Handset with basic functionality, and the Mitel 5624 Services and Mitel 5624 Personal Alarm versions are licensed WiFi Handsets with additional functionalities such as messaging and alarm, respectively.

## Pre-Installation

Before installing handsets in a VoWiFi system, ensure that the following equipment is available:

- Set up chargers and charge the handset batteries before installation.
- Have a number plan available for the handsets.
- Check 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 that 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 WinPDM is used for administration and programming of the handsets. All settings and updates are in this case done using the Mitel 5624 Desktop Programmer cradle connected over USB.
- WSM3. The WSM3 handles all communication between the WLAN and its built-in Device Manager. Before installing the handset, make sure the WSM3 IP address is available.

For effective administration of a VoWiFi system with several handsets, it is required to have both a WinPDM and a Device Manager included in the WSM3. In this case, the WinPDM is only used to allow the handset to access the WLAN system. All other settings and updates are done with the Device Manager in the WSM3.

## VoWiFi System IP addresses

To configure the handsets, enter the IP addresses in the table below.

Table 1.

Device	IP address/Number/Port	Required
IP-PBX		If used
WSM3		If used
Subnet Mask <sup>a</sup>		If used
Number plan	N/A	Yes
NTP Server address <sup>b</sup>		
DNS Server address <sup>a</sup>		
VoIP settings <sup>c</sup>		Yes
Central Phonebook		If used
Syslog server		If used
TFTP server		If used
Ekahau RTLS <sup>d</sup>		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.

d. The IP address and port to the location server.

---

# Programming the WiFi Handset

This section describes how to configure handsets in the following three different ways:

- By inserting it into a Mitel 5624 Desktop Programmer cradle connected using USB to the WinPDM.
- Over-The-Air (OTA) using the Device Manager in the WSM3.

**Note:** This requires that the IP address to the WSM3 has been configured in the handset. The IP address is configured using WinPDM or using the handset's Admin menu.

- Using the Admin menu, it is possible to configure the basic network settings. See [Administration](#) on page 81 for more information about the settings that can be configured.

It is recommended to use the Device Manager application in the WSM3 to configure handsets in a large system. The Device Manager can install, upgrade, and configure a large amount of handsets simultaneously. Another benefit is that the collection of the handsets from users is not needed.

The WinPDM configures one handset at a time. The handset is inserted in the Mitel 5624 Desktop Programmer, connected to the administrator's computer using USB.

**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.

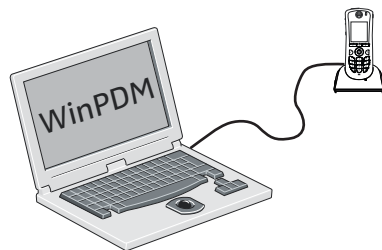
## WinPDM

The WinPDM runs on a PC and is used to configure the handset as follows:

- Connect a Mitel 5624 Desktop Programmer cradle through a USB port, to the computer running WinPDM.
- Start WinPDM.
- Place the handset in this cradle connected to WinPDM.

For instructions on how to install and use the WinPDM, see *Portable Device Manager, Windows version, Installation and Operation Guide*.

Figure 2. Configuration of handsets using WinPDM



## WSM3

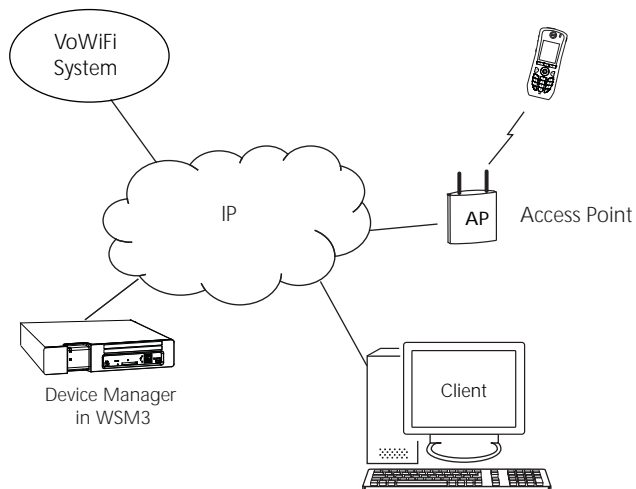
The WSM3 runs on an ELISE3 module.

For instructions on how to use the WSM3, see *Wireless Messaging Gateway (WSM3) Installation and Operation Guide*.

## Over-the-Air

There is no external equipment required, besides the Device Manager application in the WSM3 and the VoWiFi system. Proceed with [Installation of WiFi Handsets](#) on page 9.

Figure 3. Configuration of handsets using Over-the-Air (OTA)





---

# Installation of WiFi Handsets

This section describes the recommended procedure to install and configure handsets. There are several ways to install a handset but the procedures described here ensures minimal effort for the administrator.

There are two ways of configuring the handsets:

- Local management
- Centralized management (Over-the-air (OTA))

## *Local management of handsets*

**Note:** In larger installations local management is not recommended, since it requires physical access to all handsets.

Either the keypad on the handset, or the WinPDM is used to configure the handsets. It is only recommended to use the keypad, if a quick change of a parameter value is needed, for example, in a lab environment, or in a test installation. It is tedious to enter all parameters using the keypad. Access from the keypad is only available to a limited set of parameters, and to get access to all parameters, the WinPDM must be used.

The WinPDM is aimed for smaller sites where the handsets are near to hand. One handset at a time is configured, when inserted in a Mitel 5624 Desktop Programmer connected to the administrators computer over USB. See [Installation steps in small VoWiFi Systems using WinPDM](#) on page 10.

## Centralized management of handsets

**Note:** This is also referred to as Over-The-Air (OTA) management, where parameters changes are updated over the WLAN.

A WLAN connection and the Device Manager application (WSM3) is used to configure the handsets.

Prerequisites for Centralized management are as follows:

- The handset has a functional WLAN association.
- WLAN parameters are set correctly, to be able to connect to the Messaging system.
- The handset has the correct settings to access the Device Manager application as follows:
  - A configured number to be used as identity to login to the Messaging system.
  - The IP address of the Messaging system.

The WLAN and Messaging parameters are set manually, using the keypad or the WinPDM. Then the handset logs into the Messaging system, and downloads the intended handset profile, which contains all other needed parameters for a site.

See [Installation with Central Device Management \(WSM3\)](#) on page 10.

It is recommended to use the Easy Deployment process, where the needed WLAN parameters and the Messaging system information is distributed automatically to the handset, using a DHCP server (and optionally the Ascom Service Discovery Protocol).

See [on page 87](#).

**Note:** If the WLAN system uses a 802.1x security protocol that requires certificates for authentication/encryption to the WLAN, the certificates must be prepared and stored individually in the Device Manager for each number, before starting the Easy Deployment process, see [Installation with Central Device Management \(WSM3\)](#) on page 10.

See [Handset Installation in the WLAN System using Easy Deployment](#) on page 10

*Installation steps in large VoWiFi Systems using WSM3 and WinPDM*

**Note:** If the handset to be installed must use a certificate to access a WLAN, follow the instructions in section [Installation with WinPDM](#) on page 13.

These WLAN settings are common network settings for all handsets.

1. Create templates in the Device Manager in WSM3, one with network settings and another with common settings.
2. Create Numbers and apply the templates.
3. Use either the Easy Deployment procedure, or create a template with identical network settings in the WinPDM.

See [Handset Installation in the WLAN System using Easy Deployment](#) on page 10 or [Installation with Central Device Management \(WSM3\)](#) on page 10 for more information.

*Installation steps in small VoWiFi Systems using WinPDM*

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

See [Installation with WinPDM](#) on page 13 for more information.

## Handset Installation in the WLAN System using Easy Deployment

With the Easy Deployment procedure, handsets are installed without the need for the WinPDM.

Handsets are automatically installed if the following is fulfilled:

- The LAN and WLAN system is configured for Easy Deployment, see [on page 87](#).
- The handset is not associated to any network (SSID)
- The handset software is version 5.1.18 or higher
- The Call ID (endpoint number), that is, the phone number of the handset is decided.

For further details, see [on page 87](#).

## Installation with Central Device Management (WSM3)

Easy Deployment is the recommended procedure of using the Central Device Management (WSM3) for deployment, as the WLAN and Messaging parameters now are configured without the WinPDM.

Easy Deployment uses, in most parts, the same procedure, as the standard Central Device Management (WSM3) procedure. Special notes marked “(ED)” show where the procedure is unique for Easy Deployment.

**Note:** With Easy Deployment, it is very important that the building of the number plan and the parameters are correct, since the aim is to avoid using the WinPDM.

---

## Create a Network Template in the Device Manager in the WSM3

Create one template that contains the network parameters (also include the security settings). Besides the network parameters, additional parameters can also be set, for example VoIP settings and IP address to WSM3.

The template must be created, and applied, to prevent the WSM3 from restoring the parameters to default during the first synchronization.

**Note:** If using Easy Deployment, the IP-address to the Device manager in the template, can either be set, or left blank, in which case the server discovery process is used at every startup, see [A.3 WSM3 server discovery](#) on page 90.

**Note:** Only select the parameters that are modified, if all parameters are selected, the system performance decreases.

1. Open a web browser and enter the IP address or NetBIOS name to the WSM3.  
TIP: Be sure to configure all needed parameters for 802.1x security, but installing Server and/or Client Certificate can not be done using a template. This must be done individually on each Number, see [Client certificate](#) on page 102.
2. Click “Device Manager”. You might be prompted to log on the Device Manager.
3. Select the Templates tab and click “New”. The New template window is opened.
4. In the Device type and Parameter version drop-down lists, select the corresponding device type and parameter version to use, respectively.
5. In the Name field, enter a descriptive name for the template.
6. Click “OK”.
7. Set the following network parameters:
  - Network settings<sup>1</sup> (located under Network > Network A, B, C, or D)
  - VoIP settings<sup>2</sup> (located under VoIP)
  - Syslog settings<sup>3</sup> (if any) (located under Device > General)
  - Unite settings<sup>4</sup> (located under Device > Unite)
8. Click “OK” to save the template.  
TIP: See [Appendix](#) for tip on how to work with templates when using both WinPDM and WSM3.

## Create a Common Template in the Device Manager in the WSM3

Create another template with the common handset settings applicable to all handsets (exclude the parameters and security settings configured in the Network template). This template contains for example, hidden menu items in the display, certain level of ring signals and vibrators.

**Note:** Only select the parameters that are modified, if all parameters are selected, the system performance decreases.

1. Open a web browser and enter the IP address or NetBIOS name to the WSM3.
  2. Click “Device Manager”.
- 
1. All required system settings for the WLAN. For example SSID and Security mode. If using a security mode that requires certificates, also use an NTP server, to assure the correct time in the handset, as certificates only are valid within a certain time.
  2. For example 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”.
  4. IP address and password (if any) to the WSM3.

3. Select the Templates tab and click “New”.
4. In the Device Type and Parameter version drop-down lists, select the corresponding device type and parameter version to use, respectively.
5. In the Name field, enter a descriptive name for the template.
6. Set the specific parameters. See section [Configure a Handset with a Template](#) on page 15 for more information.

## Create Numbers in the WSM3

Create a range of Numbers and apply the templates previously created in the WSM3.

**IMPORTANT:** Do not add numbers for handsets that are already configured and functional, because these handsets already exist in the system, though they are not saved in the Device Manager application in WSM3. The Device Manager application overwrites the existing parameters in the handset.

**Note:** The parameter version of the template must be equal to or less than the selected parameter version.

1. Open a web browser and enter the address to the WSM3.
2. Click “Device Manager”.
3. Select the Numbers tab and click “New”. The New numbers window is opened.
4. In the Device Type and Parameter version drop-down lists, select the device type and the parameter version to use, respectively.
5. The device type and parameter version must match the handsets to be used to apply the template.
6. In the Prefix field, enter the numbers’ prefix (if needed).
7. Create a range of numbers by selecting the “Range” option. Enter the start call number and the end call number in the fields, respectively. Click “OK”.

**Note:** The maximum range that can be added at a time are 100 numbers.

8. Apply the network settings template to the selected handsets. See [Apply a Template to a Handset with a Number](#) on page 16.
9. Apply the common settings template to the selected handsets. See [Apply a Template to a Handset with a Number](#) on page 16.

**Note:** If the 802.1x security protocol with EAP-TLS or EAP-PEAP/MSCHAPv2 is used, also include the server certificate, select which Client certificate to use. The Client certificates must be installed first by editing each Number. Client certificates cannot be distributed using a template, as they are individual.

10. Close the WSM3.

## Create a Network Template with Initial Configuration in the WinPDM

In a factory delivered handset, the WLAN settings are not configured as required to access the WSM3. Using the WinPDM allows the handset to be primed with the WLAN parameters and allows the handset to log in to the Device Manager in WSM3 for future management over the air.

Create a template with the basic network settings and IP address to WSM3. This template is only used once for each handset because it must access the WLAN and then log on the Device Manager. After log in, the settings in the handset are changed according to the templates, that were applied to the Numbers, in the Device Manager application in WSM3.

---

**Note:** If using Easy Deployment, only perform step 6) below.

1. Open the WinPDM.
2. Do one of the following:
  - If a network template was created in the Device Manager in WSM3, export this template and import it to WinPDM. See [Appendix](#) for more information. (Recommended)
  - Create a template (see [Create a template](#) on page 15) with the following network parameters:
    - Network settings<sup>a</sup> (located under Network > Network A (B, C, or D)
    - Unite settings<sup>b</sup> (located under Device > Unite)

**Note:** NOTE: The parameters in this template should be identical to the parameters in the network template created in the WSM3.

  - a. All required system settings for the WLAN. For example SSID and Security mode.  
NOTE: If the production system is using 802.1x security, this method is not the best option, since the certificates must be manually installed in the handset before they login for the first time (before step 6). The Easy Deployment process overcomes this problem by using a staging WLAN, which does not use 802.1x.
  - b. IP address and password (if any) to WSM3.
3. Place the handset in the Mitel 5624 Desktop Programmer cradle.
4. Run the template. See [.Apply a Template to a Handset without a Number](#) on page 16.
5. Remove the handset when synchronization is finished.
6. Enter the Number and the password <sup>1</sup> (if any). Press “Login”.
7. Repeat step 3 – 6 for all handsets.

Settings that were stored for the handset in the Device Manager in WSM3 are now downloaded to the handset. This can, for example, be unique soft- or hot keys that have been prepared earlier. When the settings have been downloaded to the handset, the handset can restart, depending on the parameter changes.

The handset synchronizes with the WSM3 at startup, and also immediately after any handset parameter change. (The change is done either using the handset keypad, or when editing parameters in the Device Manager in the ). Depending on what is changed, and where the change is done, the parameters are synchronized to, or from, the handset.

Those changes are not stored in the WinPDM, as there is no connection between the WinPDM and the WSM3 Device Management database. The database in the WinPDM synchronizes with the handset, when the handset is placed in the Mitel 5624 Desktop Programmer cradle (online via USB).

**Note:** As there is no connection between the WinPDM and the WSM3 Device Management databases, except over the handset, the WLAN and WSM3 settings can differ in the WinPDM and the WSM3. Parameters can inadvertently be reverted with old values, when first, the WinPDM synchronization process runs, (when the handset is placed in the Mitel 5624 Desktop Programmer cradle), and after that, (when the handset is removed from the Mitel 5624 Desktop Programmer cradle), the handset goes online with the Messaging system, and the synchronization process with the WSM3 runs and vice versa. The solution for this, is to avoid storing handset numbers in the WinPDM.

## Installation with WinPDM

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

1. The password is only required if the “Password” parameter is set.

The synchronization is in this case not handled automatically by the system when a handset's parameters are changed in the WinPDM. When the parameters have been changed in WinPDM, each handset must be placed in the Mitel 5624 Desktop Programmer cradle connected to the administrator's computer in order to synchronize the parameters with the handset.

1. Open the WinPDM.
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 used, 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 [Create a template](#) on page 15) with the following network parameters:
  - Network settings<sup>1</sup> (located under Network > Network A, B, C, or D)
8. Create another template (see [Create a template](#) on page 15) with the common handset settings applicable to all handsets (exclude the network parameters and used security settings). Example of parameters settings:
  - VoIP settings<sup>2</sup> (located under VoIP)
  - Software TFTP IP address (if any) (located under Device > General)
  - Syslog settings<sup>3</sup> (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 [Apply a Template to a Handset with a Number](#) on page 16.
10. Apply the common settings template to the handset, see [Apply a Template to a Handset with a Number](#) on page 16.
11. Place the handset in the Mitel 5624 Desktop Programmer 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 WinPDM are now synchronized with the handset. In addition, the handset's Device ID is also synchronized with the number in the WinPDM.

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 "Manage certificates". A Manage certificate window opens.
  15. In the Root tab and Client tab, click "Browse" and select the certificates to import. Click "Close".
  16. In the Numbers tab, right-click the handset's number and select "Edit parameters".
1. All required system settings for the WLAN. For example SSID and Security mode, and if used, any certificates for 802.11x.
  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".

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 synchronization is finished.

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

## Installation using the Handset's Admin Menu

It is possible to install a handset using its Admin menu. This is useful when no WinPDM or WSM3 is available and the handset needs to be installed quickly.

**Note:** It is only possible to configure the basic settings through 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 settings<sup>1</sup> (located under Network setup)
  - VoIP settings<sup>2</sup> (located under VoIP)
  - Unite settings<sup>3</sup> (if any) (located under Unite)
  - Syslog settings<sup>4</sup> (if any) (located under Syslog)
  - Add license key (if any) (located under Enter license key)

## Configure a Handset with a Template

It is possible to select a handset in the WinPDM 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 control the changes applied to each handset.

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

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

### Create a template

1. Open the WinPDM or the Device Manager in the WSM3.
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 are left unchanged on the handset. The parameter version of an installed handset is visible under the Numbers tab or the Devices tab.

1. All required system settings for the WLAN. For example SSID and Security mode. Note that the certificates cannot be entered, nor referred to, using the keypad.
2. VoIP protocol, Gatekeeper IP address or SIP proxy IP address used to access the PBX.
3. IP address and password (if any) to the WSM3.
4. The parameter "Syslog" must be enabled in order to set the "Syslog IP address".



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

### Apply a Template to a Handset with a Number

1. Open the WinPDM or the Device Manager in the WSM3.
2. In the Numbers tab, select the handset(s) you want to apply the template to.

**Note:** If several handsets are selected, they must be of the same device type and have the same parameter version.

3. Right-click and select "Run template...".

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

The template is applied. The number of parameters in the template affects 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" shows the name of the most recently applied template.

### .Apply a Template to a Handset without a Number

This feature is only applicable for the WinPDM. It is possible to apply a template to a handset without a number in the WinPDM.

1. Place the handset in the Mitel 5624 Desktop Programmer 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 are shown.
4. Select the desired template and click "OK".

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

### 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 WinPDM or the Device Manager in the WSM3.
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 check box 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”.

## Synchronizing a Handset with WinPDM

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

- If a parameter has been changed in the handset, it is transferred to the WinPDM/WSM3.
- If a parameter has been changed in the WinPDM/WSM3 while the handset was disconnected, it is transferred to the handset.

If the same parameter has been changed in both the WinPDM/WSM3 and the handset, the value in WinPDM/WSM3 will be transferred to the handset.

## Configure Handset without Saving It in WinPDM

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

1. Place the handset in the Mitel 5624 Desktop Programmer cradle
2. Open WinPDM.
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 Mitel 5624 Desktop Programmer cradle. The handset is no longer visible in the WinPDM and the settings are only saved in the handset.

# Maintenance

## Handset

In an existing VoWiFi system, it is important to be able to replace handsets, install new handsets, and exchange faulty handsets. The recommended procedure is to use a template with basic network settings for log in, created in the WinPDM, and then import the rest of the settings that were created by the templates in Device Manager in WSM3.

It is also important to be able to upgrade system parameters and security settings in the handsets. These upgrades are preferably done in the WSM3, if available.

If you use WinPDM and WSM3, do one of the following:

- If you want to install new handset, see [Installation with Central Device Management \(WSM3\)](#) on page 10.
- If you want to create spare handsets to be used when broken handsets need to be replaced later on, see [Configure Spare Handsets without a Number in Large Systems](#).

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

- If you want to install new handset, see [Installation with WinPDM](#) on page 13.
- If you want to replace a broken handset, see [Replacement of Handset with WinPDM Only](#) on page 27.

### Configure Spare Handsets without a Number in Large Systems

In large systems where WSM3 is used, it is recommended to configure a few spare handsets without a number to quickly replace a broken handset later on.

#### *Create a Template*

1. Open WinPDM.
2. Select the Templates tab and click “New”. The New template window is opened.
3. In the Device type and Parameter version drop-down lists, select the matching device type and parameter version respectively, for the spare handset to use.
4. In the Name field, enter a descriptive name of the template.
5. Click “OK”.
6. Set the following network parameters:
  - Network settings<sup>1</sup> (located under Network > Network A, B, C, or D)
  - VoIP settings<sup>2</sup> (located under VoIP)
  - Syslog settings<sup>3</sup> (if any) (located under Device > General)
  - Unite settings<sup>4</sup> (if any) (located under Device > Unite)
7. Click “OK” to save the template.

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

2. For example 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”.

4. IP address and password (if any) to the WSM3.

---

### *Apply Template to a Handset without a Number*

1. Place the handset in the Mitel 5624 Desktop Programmer 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 are shown.
4. Select the desired template and click "OK".  
The template is applied. The number of parameters in the template affects the time it takes to apply the template to the selected handset.
5. Switch off the handset when User name and Password are displayed.  
TIP: If the handset replaces a broken handset, continue with [Replacement of Handset with WSM3](#) on page 24.

### *Upgrade Handset Software*

**Note:** Read the software Release Notes before changing the software.

The handset software can be upgraded over the air using Centralized Device Management (WSM3) or a TFTP server, or by cable using WinPDM.

#### *Upgrade Handset Parameter*

A parameter upgrade can restart the handset, for example, when upgrading the NTP server. The text "Remotely updated" is shown in the handset display when the handset restarts after an upgrade.

### *Upgrade Software OTA using TFTP*

If no WSM3 is available, it is recommended to use software upgrade OTA using TFTP, which 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.

To upgrade the software using TFTP, perform the following:

1. If needed, configure the handset in WinPDM 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 [Installation with WinPDM](#) on page 13.
2. If needed, upload a new software information file (packageinfo.inf) and a software (.bin) file to the TFTP server. These files are provided by your supplier. First rename the .pkg file to .zip and then unzip the files. Then the needed .inf and .bin files are available.  
See the manual for the TFTP server used, for more information on how to upload files.
3. Restart the handset. After the handset restarts, 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 downloads the software file (.bin) from the TFTP server. The handset restarts when the software upgrade is performed.

#### *Configure Access to the TFTP Server*

1. Place the handset in the Mitel 5624 Desktop Programmer cradle.
2. Open the WinPDM.

3. Open the Numbers tab and select the handset.
4. 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".

### Upgrade Software using WinPDM

Software upgrade using WinPDM is performed in small VoWiFi systems or when WSM3 is not available. The handsets need to be collected by the administrator because the software is upgraded using the Mitel 5624 Desktop Programmer connected to WinPDM.

1. Open the WinPDM.
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". The dialog window "Shutting down" followed by "Remotely updated" is shown in the handset display.

### Upgrade Software Over the Air (OTA) through Centralized Device Management (WSM3)

Software upgrade using WSM3 is performed in large VoWiFi systems. The benefit is that the handsets do not need to be collected by the administrator because the software upgrade is performed over the air (OTA).

1. Open the Device Manager in the WSM3.
2. Open the Devices tab and select the handsets to be upgraded.
3. Right-click and click "Upgrade software...".
4. In the Available software 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".
5. In the Upgrade section and Activate new software section, select when the software is upgraded and activated on the handset, respectively.
6. Click "OK".  
TIP: It is also possible to upgrade several handsets of the same device type simultaneously using the Baseline function in the WSM3. See *Wireless Messaging Gateway (WSM3) Installation and Operation Guide*.

### 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 is 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 keeps it, if the handset is not restarted.

---

## Upgrade Handset Functionality using License

Users can upgrade a handset by downloading a license. The following licenses are available:

- Mitel 5624 Services License
- Mitel 5624 Services to PAlarm Upgrade Lic
- Mitel 5624 WiFi Location License, see [Location](#) on page 75 for additional settings.
- Mitel 5624 Shared Phone License, see [Shared Phone](#) on page 42 for additional settings.
- Mitel 5624 PAlarm to MD/NM Alarm Upgrade Lic

There are three alternatives to upgrade a handset:

- Automatic upgrade, see [Automatic license upgrade](#).
- License upgrade using import/export, see [License upgrade using import/export](#).
- Manual upgrade, see [Manual license upgrade](#).

**Note:** A handset can be re-licensed up to 99 times.

### *Automatic license upgrade*

Use this option if the WinPDM has an internet connection to the License Server.

1. Open the WinPDM.
2. Place the handset in the Mitel 5624 Desktop Programmer cradle.  
The first time the handset logs on the WinPDM, the license key is automatically downloaded to the handset, go to step 4.
3. If the handset is logged on to the WinPDM after the first time, no automatic check for licenses is done. Synchronize the WinPDM and license server as follows:
  - Select the “Licences” tab.
  - Right-click the handset in the list.
  - Select “Refresh”.  
The license key is downloaded to the handset.
4. The handset restarts. See also [Upgrade Handset Functionality using License](#) on page 21 to view the handset’s license option(s).  
If the handset is updated to a new device type (to Mitel 5624 Services or Mitel 5624 Personal Alarm), both the new device and the old device is displayed in WinPDM. The old device has to be manually removed.

### *License upgrade using import/export*

Use this option if the WinPDM has no internet connection to the License Server. A product information file (.XML) must first be exported from the WinPDM, and then imported to the License Web.

1. Place the handset in the Mitel 5624 Desktop Programmer cradle.
2. Open the WinPDM.
  - Select the “Licences” tab.
  - Right-click the handset(s) in the list.
  - Select “Export”.

- Save the file on a computer with an internet connection to access the License Web later on.
3. In a web browser, enter the address to the License Web “https://www.xxxxxxxx”  
The License Web is used for;
    - Importing the product information file
    - Viewing/Purchasing the license(s) for the handset(s)
    - Downloading the license file containing the license key(s) for the handset(s)  
See the online help on the License Web for information on how to use the License Web.
  4. When the license file (.XML) containing the license key(s) is downloaded from the License Web, select File > Import > Licences in the WinPDM to import the file.
  5. When the file is imported, the license key(s) is downloaded to the handset(s), and the handset restarts. See also [Upgrade Handset Functionality using License](#) on page 21 to view the handset’s license option(s).  
If the handset is updated to a new device type (to Mitel 5624 Services or Mitel 5624 Personal Alarm), both the new device and the old device are displayed in WinPDM. The old device has to be manually removed.

### *Manual license upgrade*

Use this option if the serial numbers of the handset cannot be exported to a file because a WinPDM is not in use. The serial number(s) must be manually entered in the License Web to get the corresponding license key for the handset. The license key must also be manually entered in the handset. See the online help on the License Web for information on how to get a license key.

TIP: If several handsets are upgraded, it is recommended to use [License upgrade using import/export](#) on page 21.

The license key is added using the Admin menu in the handset, see [Admin Menu Tree](#) on page 81 for information on how to activate the Admin menu.

TIP: It is also possible to press \*#35# in idle mode for quick access to the “Enter license key” menu.

1. Press the soft key “Menu”.
2. Select “Calls”.
3. Select “Admin menu”.
4. Select “Enter license key”.
5. Enter license key without blanks.
6. Press “OK”.

If the license key is valid, a dialog window “License key accepted” is shown. The handset restarts.

If the handset has been updated to a new device type (to Mitel 5624 Services or Mitel 5624 Personal Alarm), both the new device and the old device are displayed in WinPDM. The old device has to be manually removed.

### *Move License*

It is possible to move a product license (Personal Alarm or Services ) to an unlicensed handset. Any optional licenses follow. For example, a Personal Alarm license can be moved from a

---

handset with a broken display to an unlicensed handset. The broken handset can then be sent for repairs.

Prerequisites: A WinPDM or Device Manager application (in WSM3) that supports the move license function, and a connection to the license server.

To move a license using the WinPDM:

1. Place the licensed handset in the desktop programmer.
2. On the Licenses tab, select the handset online.
3. On the License menu, click "Move license...".
4. In the Move license dialog, select the unlicensed handset and click "OK".  
The handset in the desktop programmer is restarted.
5. Place the unlicensed handset in the desktop programmer.
6. On the Licenses tab, select the handset online.
7. On the License menu, click "Refresh".  
The handset in the desktop programmer is restarted.

To move a license using the Device Manager application:

1. On the Licenses tab, select the licensed handset (must be online).
2. On the License menu, click "Move license...".
3. In the Move license dialog, select the unlicensed handset and click "OK".  
Both handsets are restarted.
4. If the unlicensed handset is currently shut down:
  - Switch on the handset.
  - On the Licenses tab, select the handset.
  - On the License menu, click "Refresh".
  - The handset is restarted.

## Perform a Factory reset

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

### *Factory Reset using WinPDM or Device Manager (WSM3)*

1. Open the WinPDM.
2. Place the handset in the Mitel 5624 Desktop Programmer In the Device tab, mark the handset to be factory reset. Note that the handset must be online.
3. In the Device menu, select "Factory reset". Alternatively, right-click the handset and select "Factory reset".
4. A Reset devices window appears, click "Yes". The handset is 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 is restarted.

## Replacement of Handsets

A handset can be replaced with a spare handset if it is broken. The handset registered in WinPDM or WSM3, is associated with its device type, device ID, and extension. During the replacement procedure, the broken handset's device type and extension are associated with the spare handset's device ID.

### Replacement Procedure Choice

- If you have WSM3 and already have applied the network template to the spare handset(s) to log on later, see [Replacement of Handset with WSM3](#) on page 24.
- If you have both WinPDM and WSM3, and need to apply the network template to the spare handset(s) to log on later, see [Replacement of the Handset with WinPDM and WSM3](#).
- If you only have WinPDM, see [Replacement of Handset with WinPDM 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
- Messages
- Company phonebook
- Downloaded language
- Certificates
- Licenses<sup>1</sup>

### Replacement of Handset with WSM3

There are two different replacement procedures as follows:

- If the broken handset and the spare handset have the same device type and functionality license, see [Replace without Move Licenses in WSM3](#).
- If the broken handset and the spare handset do not have the same device type and/or functionality license, the license must be moved to the spare handset, see [Replace and Move Licenses in WSM3](#) on page 25.

### *Replace without Move Licenses in WSM3*

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

1. A handset's license(s) can be moved to an unlicensed handset (Mitel 5624) if following the replacement instructions in [Replace and Move Licenses in WSM3](#) on page 25.



1. In both handsets, press \*#34# in idle mode and select "License" to check that they have same device type and licenses.  
If the login screen is displayed in the spare handset, press "Info", and select "License".
2. If the broken handset is online in the Device Manager, switch off the handset to make it offline.
3. Take a spare handset prepared with the network settings (including the IP-address to the WSM3).
4. Enter the number and leave the password blank. Press "Login".

The spare handset is automatically updated from the WSM3 and might be restarted depending on the changed settings. The last stored settings for the broken handset in the WSM3 are transferred to the spare handset.

### *Replace and Move Licenses in WSM3*

The broken handset and the spare handset do not have the same device type and/or have the same functionality license.

The spare handset must be an unlicensed Mitel 5624 to move the licenses to the spare handset. To check that the handset is unlicensed, press \*#34# in idle mode and select "License". Only Mitel 5624 must be displayed here.

1. Make sure that the broken handset is saved in the Device Manager (indicated by a ✓ in the Saved column. If not, in the Numbers tab, right-click the broken handset and select "Save".
2. Switch the broken handset off. The handset appears as offline in the Device Manager.
3. Take an unlicensed spare handset (Mitel 5624) prepared with the network settings (including the IP-address to the WSM3).
4. Enter the number and leave the password blank. Press "Login". The handset is now online in the Device Manager.
5. Make sure that the spare handset is saved in the Device Manager (indicated by a ✓ in the Saved column. If not, in the Numbers tab, right-click the spare handset and select "Save".
6. Switch the spare handset off. The handset appears as offline in the Device Manager.
7. Switch the broken handset on. The handset appears as online in the Device Manager.
8. In the Device Manager, select the "Licenses" tab.
9. Right-click the broken handset and select "Move license...".
10. In the Move license window, select the Mitel 5624 that should receive the license. Press "OK".
11. The broken handset restarts and has now become a Mitel 5624. Switch the broken handset off. The handset appears as offline in the Device Manager.
12. Switch the spare handset on. The handset appears as online in the Device Manager.
13. In the Device Manager, select the "Licenses" tab. Right-click the spare handset and select "Refresh".

The spare handset is automatically updated from the WSM3 and restarted. The last stored settings and licenses for the broken handset in the WSM3 are transferred to the spare handset.

## Replacement of the Handset with WinPDM and WSM3

If the spare handset to be used must be factory reset or no network template has been applied, a WinPDM is needed to apply the network template to the spare handset. When the network template is added, the handset can log on to the Device Manager.

There are two different replacement procedures as follows:

- If the broken handset and the spare handset have the same device type and functionality license, see [Replace without Move Licenses using WinPDM and WSM3](#).
- If the broken handset and the spare handset do not have the same device type and/or functionality license. The license must be moved to the spare handset, see [Replace and Move License using WinPDM and WSM3](#) on page 26.

### *Replace without Move Licenses using WinPDM and WSM3*

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

1. In the handset, press \*#34# in idle mode, and select “License” to check that both handsets have same device type and licenses.
2. Make sure that the broken handset is saved in the Device Manager (indicated by a ✓ in the Saved column. If not, in the Numbers tab, right-click the broken handset and select “Save”.
3. Switch the broken handset off. The handset appears as offline in the Device Manager. If the spare handset is not prepared with the basic network settings, also perform the steps 4 - 7.
4. Open the WinPDM.
5. Place the spare handset in the Mitel 5624 Desktop Programmer cradle.
6. Run the template with the basic network settings containing (see [Configure a Handset with a Template](#) on page 15):
  - Network settings<sup>1</sup> (located under Network > Network A, B, C, or D)
  - VoIP settings<sup>2</sup> (located under VoIP)
  - Unite settings<sup>3</sup> (located under Device > Unite)
7. Remove the handset from the Mitel 5624 Desktop Programmer cradle. The handset restarts, depending upon parameter changes.
8. Enter the number and the password<sup>4</sup> (if any). Press “Login”.

The spare handset is automatically updated from the WSM3 and restarts, depending upon parameter changes. The last stored settings for the broken handset in the WSM3 are transferred to the new handset.

### *Replace and Move License using WinPDM and WSM3*

The broken handset and the spare handset do not have the same device type and/or have the same functionality license.

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. IP address and password (if any) to the WSM3.
4. The password is only required if the “Password” parameter is set.

---

The spare handset must be an unlicensed Mitel 5624 to move the licenses to the spare handset. To check that the handset is unlicensed, press \*#34# in idle mode, and select "License". Only Mitel 5624 must be displayed here.

1. Make sure that the broken handset is saved in the Device Manager (indicated by a ✓ in the Saved column. If not, in the Numbers tab, right-click the broken handset and select "Save".
2. Switch the broken handset off to take the handset offline.
3. Open the WinPDM.
4. Place the unlicensed spare handset (Mitel 5624) in the Mitel 5624 Desktop Programmer cradle.
5. Run the template with the basic network settings containing (see [Configure a Handset with a Template](#) on page 15):
  - Network settings<sup>1</sup> (located under Network > Network A, B, C, or D)
  - VoIP settings<sup>2</sup> (located under VoIP)
  - Unite settings<sup>3</sup> (located under Device > Unite)
6. Remove the handset from the Mitel 5624 Desktop Programmer cradle. The handset restarts.
7. Enter the number and the password<sup>3</sup> (if any). Press "Login".
8. Make sure that the spare handset is saved in the Device Manager (indicated by a ✓ in the Saved column. If not, in the Numbers tab, right-click the spare handset and select "Save".
9. Switch the spare handset off to take the handset offline.
10. Switch the broken handset on to take the handset online.
11. In the Device Manager, select the "Licenses" tab.
12. Right-click the broken handset and select "Move license...".
13. In the Move license window, select the Mitel 5624 that should receive the license. Press "OK".
14. The broken handset restarts and has now become a Mitel 5624. Switch the broken handset off. The handset appears as offline in the Device Manager.
15. Switch the spare handset on. The handset appears as online in the Device Manager.
16. In the Device Manager, select the "Licenses" tab. Right-click the spare handset and select "Refresh".

The spare handset is automatically updated from the WSM3 and restarted. The last stored settings and licenses for the broken handset in the WSM3 are transferred to the spare handset.

## Replacement of Handset with WinPDM Only

Replacement through WinPDM is used in small VoWiFi systems or when WSM3 is not available.

- If the broken handset and the spare handset have the same device type and functionality license, see [Replace without Move Licenses using WinPDM](#).
- If the broken handset and the spare handset do not have the same device type and/or functionality license. The license must be moved to the spare handset, see [Replace and Move Licenses using WinPDM](#).

*Replace without Move Licenses using WinPDM*

Both the broken handset and the spare handset must be of the same device type and have same functionality license

1. In both handset, press \*#34# in idle mode and select “License” to check that they have same device type and licenses.  
Alternatively, if the spare handset has been factory reset, press “Info” and select “License”.
2. Place the broken handset in the Mitel 5624 Desktop Programmer cradle.
3. Open the WinPDM.
4. Make sure that the handset is saved in the WinPDM. In the Numbers tab, a saved handset has the symbol ✓ in the Saved column. If not, right-click the handset and select “Save” to transfer the settings to the spare handset later on.
5. If the spare handset has been previously used, perform a factory reset, see [Perform a Factory reset](#) on page 23.
6. Place the spare handset in the Mitel 5624 Desktop Programmer
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 is replaced and its settings are transferred to the spare handset.

*Replace and Move Licenses using WinPDM*

The broken handset and the spare handset do not have the same device type and/or have the same functionality license.

The spare handset must be an unlicensed Mitel 5624 to move the licenses to the spare handset. To check that the handset is unlicensed, press \*#34# in idle mode and select “License”. Only Mitel 5624 must be displayed here.

1. Place the broken handset in the Mitel 5624 Desktop Programmer cradle.
2. Open the WinPDM.
3. Make sure that the broken handset is saved in the WinPDM. 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.
4. Place an unlicensed spare handset (Mitel 5624) in the Mitel 5624 Desktop Programmer cradle.
5. Run the template with the basic network settings containing (see [Configure a Handset with a Template](#) on page 15):
  - Network settings<sup>1</sup> (located under Network > Network A, B, C, or D)
  - VoIP settings<sup>2</sup> (located under VoIP)
  - The handset can be restarted depending on parameter changes.
6. Place the broken handset in the Mitel 5624 Desktop Programmer cradle.
7. In the WinPDM, select the “Licenses” tab.
8. Right-click the broken handset and select “Move license...”.

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.

9. In the Move license window, select the Mitel 5624 that should receive the license. Select "Do Nothing". The broken handset restarts and has now become a Mitel 5624.
10. Place the spare handset in the Mitel 5624 Desktop Programmer cradle. The spare handset is restarted and the licenses for the broken handset in the WinPDM has been transferred to the spare handset.
11. A Found Device Wizard window appears. Select "Associate with Number" and click "Next >".
12. In the list, select the broken handset to be replaced with the spare handset. Click "OK". The spare handset can be restarted and the settings for the broken handset in the WinPDM are transferred to the spare handset.

## 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 WinPDM or the Device Manager in WSM3.
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 does not exist in another system. If several handsets have the same number, their settings overwrite each other when synchronizing with WSM3/ or WinPDM.

6. Click "OK".

The new number is synchronized with the handset when it is connected to WinPDM or WSM3.

## Update Parameters using WSM3

This section describes the general procedure to change/update parameters using the WSM3. The update starts when the handset is idle and does not interrupt an ongoing call.

**Note:** Only select the parameters that are changed, if all parameters are selected, the system performance decreases.

1. Open the WSM3.
2. Create a new template with only the parameters to be changed.
3. Select the numbers that should be updated and apply the template.  
The handsets are automatically updated from the WSM3 and can be restarted depending on which parameters are changed.

## Perform a Security Upgrade using WSM3

This section describes how to perform an update/change of the WLAN password/authentication using the WSM3.

**Note:** Change settings in the handset before change settings in the AP. Else, synchronization of new settings to the handset settings cannot be performed.

**Tip:** Leave one access point with the old configuration to allow switched off handsets to receive the updates when they are turned on. Bring the handset to that APs coverage area.

1. Open the WSM3.

2. Create a new template with the new security settings.
  - Security mode<sup>1</sup>
3. Apply the new template to the handsets.

The handsets are automatically updated from the WSM3 and restarted.

**Note:** At this time, the handsets have no access to the WLAN system.

4. Change the security settings for the APs.

The handsets are now able to access the WLAN.

## Upgrade the Template

The upgrade procedure of the templates definition version is described in the *Portable Device Manager, Windows version, Installation and Operation Guide*, and *Wireless Messaging Gateway (WSM3) Installation and Operation Guide*.

## 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 *Portable Device Manager, Windows version, Installation and Operation Guide* and *Wireless Messaging Gateway (WSM3) Installation and Operation Guide*.


1. All required settings for the WLAN. For example User name, Password, Regulatory domain etc.

---

# Handset Configuration

**Note:** This section describes settings in parameter definition files (.def). These files are regularly updated and settings can 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 WinPDM/WSM3. This section describes the available settings for the handset. The first part explains network settings and the second part explains the handset settings.

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

## 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 (using WinPDM or WSM3) and is visible in the handset, see [Change Name of Network](#).

A handset can be configured for up to four different WLANs but only for one WSM3 and one VoIP System.

The configured networks in WinPDM must have a SSID value 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".

### 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".

### 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.

### Enable Switch between Networks

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

1. Find parameter Network > General > Auto-switch network, and select "Enable".  
Parameter Auto-switch network time-out 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 time-out.
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).

## 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 [Automatic IP Address Settings](#).
- If no DHCP server is used, a unique IP address must be entered manually for each handset, see [Static IP Address \(Manual\) Settings](#).

### 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.

### 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 the DNS server that the handset uses. If the primary DNS server is available, it is always used. Otherwise, the secondary DNS server is used.

**Note:** The DNS parameters are only visible if the DHCP mode is set to “Disable (static mode)”, see [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 for 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 for the secondary DNS server.

## Network Settings

### SSID

The SSID is the name of the network that the handset associates with.

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



---

## 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 multiplies the talk time by more than 4 times compared to the NONE mode.

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

## World Mode Regulatory Domain

There is a set of regional rules for the world mode settings and the a-band that the handset complies with. 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

## 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 defines the 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 are to be set in the *Advanced: 802.11 channels* parameter, see [Advanced: 802.11 Channels](#) on page 34.

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 defines 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, 5.725 - 5.845 MHz	36,40,44,48 149,153,157,161, 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 the 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 APs, which decreases the WLAN performance. Select “Advanced” only if the channels are to 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).

### *Transmission Power*

This is the transmission power the handset uses 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)

---

## IP DSCP for Voice/Signaling

Differentiated Services Code Point (DSCP) defines the value to use for outgoing voice and signaling 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 results 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 signaling 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

## 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.

The most used encryption and authentication modes are directly available from the Security mode drop-down menu. The most required parameters per mode are shown.

**Tip:** To view all available security parameters, use the “Advanced” menu.

### 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”.

### WEP 64/128-bit Key

To use 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”.

## 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.

## 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.

## 802.1X with PEAP-MSCHAPv2

PEAP-MSCHAPv2 requires the use of root certificates for authentication of the WLAN. To select PEAP-MSCHAPv2 as the authentication method, do the following:

1. Ensure that the handset is online in WinPDM.
2. Import the root certificate by performing the following steps:
  - In the Numbers tab, right-click the handset's number and select "Manage certificates". A Manage certificate window opens.
  - In the Root tab, click "Browse" 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.
7. In the Validate server certificate field, select if validation of server certificate during authentication is to be disabled.

**WARNING:** BY DISABLING THE VALIDATION, THE SERVER IS NOT AUTHENTICATED AND MAY BE A ROGUE ONE.

## EAP-TLS

EAP-TLS requires the use of (server) root certificate to authenticate the WLAN, and client certificates to present to the WLAN for client authentication. To select EAP-TLS as the authentication method, do the following:

1. Ensure that the handset is online in WinPDM.
2. Import the certificates by performing the following steps:
  - In the Numbers tab, right-click the handset's number and select "Manage certificates". An Manage certificate window opens.
  - In the Root tab and Client tab, click "Browse" 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. In the Validate server certificate field, select if validation of server certificate during authentication is to be disabled.

**WARNING:** BY DISABLING THE VALIDATION, THE SERVER IS NOT AUTHENTICATED AND MAY BE A ROUGE ONE.

## 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 WinPDM/WSM3 to assist the user, or to set the initial value when the handset is commissioned.

General Settings	Keypad <sup>a</sup>	WinPDM
Automatic key lock on page 38	x	x
Phone lock on page 38	x	x
Headset type on page 39	x	x
Audio adjustment on page 38	x <sup>b</sup>	x
Shortcuts on page 43	x	x
Profiles on page 47	x	x
.Battery Warning on page 42	x	x
Actions when the Handset is Placed in the Charger on page 40	x <sup>b</sup>	x
Shared Phone on page 42		x
Uploadable Language on page 42		x
Telephony		
Message Centre Number on page 56		x
Max number of Call Completions on page 56		x
Dial Pause Time on page 56		x
Direct off Hook from Charger on page 56	x	x
Replace Call Rejected with User Busy on page 57		x
Emergency Call Numbers on page 55		x
Import Contacts on page 46		x
Company Phonebook on page 47		x
Central Phonebook on page 47		x
Voice Mail Number on page 56		x
Regional Settings		
Set Time & Date on page 70	x	x
Select Default Language on page 43	x	x
Dialing Tone Pattern on page 72		x
Customize Menu		
Uploadable Language on page 42		x
Call Services Menu on page 46		x
In-call Menu on page 45		x
Hide Menu Items on page 73		x
Services on page 73	x	x
Display		
User Display Text on page 72	x	x
Font style on page 72	x	x
Backlight Timeout on page 72		x
Brightness on page 72	x	x
Screen Saver on page 72	x	x
Alarm		
Telephony on page 52		x

- a. Refer to the User Guide for more information on how the user can change the settings using the handset’s keypad.
- b. Some parameters cannot be changed when using the keypad.

## Automatic key lock

Turn on the automatic key lock to avoid unintentional key presses.

**Note:** If configured, it is possible to dial any of up to five predefined emergency numbers when the keypad is locked, see [Emergency Call Numbers](#) on page 55.

1. Select Device > Settings.
2. In the Automatic key lock drop-down list, select one of the following:
  - On - activates the automatic key lock, also during an ongoing call.
  - Off - deactivates automatic key lock

## 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 any of up to five predefined emergency numbers when the handset is locked, see [Emergency Call Numbers](#) on page 55. It is not recommended to use Phone Lock when using the Shared Phone feature, see [Shared Phone](#) on page 42

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 and a password is required to open it again
  - On in charger - the handset is be locked when placed in charger.
  - Off - the phone lock is not activated.

## Automatic lock time

When either the key lock or the phone lock is set to On, the lock is activated after the specified time. It is possible to change the default time of 20 seconds.

1. Select Device > Settings.
2. In the Automatic lock time drop-down list, select desired time:
  - 5, 10, 20, 30 seconds, 1, or 3 minutes.

## Automatic key unlock

1. Select Device > Settings.
2. In the Automatic key unlock drop-down list, select one of the following:
  - On - the handset keypad is locked up automatically at incoming calls and messages.
  - Off - the handset is not locked up automatically to avoid unintentional key press

## Audio adjustment

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

1. Select Audio > Volume.
2. Select the appropriate volume type from 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 39.

**Note:** Changing this parameter can result in lower sound quality and high sound level. Evaluate carefully before applying.

## Headset Configuration

### *Headset type*

Select the headset model that is used.

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

**Note:** Do not select “Hearing protection” unless a Peltor headset is used.

- Hearing protection
- Mic on boom
- Mic on cable
- User model (If none of the headsets above are selected, 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 can result in lower sound quality and high sound level. Evaluate carefully before applying.

### *Corded headset button*

1. Select Headset > General.
2. In the Call with headset button list, select one of the following:
  - Not activated – it is only possible to answer/end a call.
  - Last called number – the last called number is dialled.
  - Predefined number – a predefined number is called (if selected, continue with step 3)

3. If needed, in the Predefined number field, enter the number to be dialled when the headset button is pressed.

## Actions when the Handset is Placed in the Charger

The behavior of the handset when it is placed in a charger can be configured.

### *In-charger call behavior*

1. Select Device > Call.
2. Choose a setting from the In charger call behavior list:
  - No action
  - End – the handset ends an ongoing call when placed in a charger.
  - Put on Loudspeaker – the handset turns on the loudspeaker when placed in a charger during a call.

### *In-charger action when not in call*

1. Select Device > Settings.
2. In the In charger action drop-down list, select one of the following:
  - No action - no action is performed when handset is placed in charger
  - Switch off - the handset is switched off when placed in charger
  - Sound off - the handset is silenced when placed in charger (except for messages with set “Break through” parameter, for example, “Prio 1” messages.)

NOTE: Messages with breakthrough (for example with high/alarm priority) are not muted. If you want to mute all messages (regardless of priority) also set the Device > Messaging > Show and indicate messages in charger > Off.

- Change profile - the handset changes profile when placed in charger.
    - In the Change profile in charger drop-down list, select the profile to be used.
    - If needed, configure the selected profile, see [Profiles](#).
3. In the In charger Message absent<sup>1</sup> drop-down list, select one of the following:
    - No - messages are saved in the handset’s messaging inbox while the handset is placed in a charger (default).
    - Yes - if a message is sent from a system it is notified that the handset is absent. Messages are not sent to the handset.

### *Clear lists in charger*

1. Select Device > General.
2. In the Clear lists in charger drop-down list, select one of the following:
  - Yes - message lists and call lists are deleted when the handset is placed in the charger.
  - No - no action is performed when the handset is placed in the charger.

### *Show and indicate messages in charger*

Defines how incoming messages are displayed/indicated when the handset is placed in the charger.

1. This function is applicable for Mitel 5624 Services and Mitel 5624 Personal Alarm only.



---

**Note:** All incoming messages are affected by this setting: that is PTT invitation received as a message, and all other messages regardless of priority (even messages with breakthrough such as high/alarm priority). If you only want to silence messages without breakthrough (low/normal priority), set the Sound off parameter instead (in Device Settings > In charger action > Sound off).

1. Select Device > Messaging.
2. In the Show and indicate messages in charger drop-down list, select one of the following:
  - On - Messages are shown and indicated (by beep) when the handset is placed in the charger (default)
  - Off - The message alert (if any) is muted and only the New message icon is displayed. The messages are stored as unread messages in the Message inbox.

### *Receive Messages in Charger<sup>1</sup>*

Defines if received messages are saved or discarded when the handset is placed in a charger.

1. Select Device > Messaging.
2. In the Receive messages in charger drop-down list, select one of the following:
  - On - Messages are saved while the handset is placed in a charger (default)
  - Off - Messages are discarded while the handset is placed in a charger.

### Hide Missed Call Window

By default, a Missed call window indicates a missed call. It is possible to hide this window, for example, if both a handset and a mobile is used. If the user answers the call using the mobile, the Missed call window is not displayed in the handset.

1. Select Device > Call.
2. In the Show missed calls popup drop-down list, select "No" to hide the Missed call window.

### Prevent Handset Switch off

It is possible to prevent the user from switching off the handset when the user holds down the End key for a long time. When the End key is pressed, no Switch off? dialog window appears in the handset.

1. Select Device > General.
2. In the Block switch off drop-down list, select one of the following:
  - No - The user can switch the handset off.
  - Yes - The user cannot switch the handset on.

### Prevent Mute function

It is possible to prevent that the handset is muted/set to silent by a user.

1. Select Audio > General.
2. In the Prevent silent drop-down list, select one of the following:
  - On - The user cannot set the handset to silent by using mute or decreasing the volume.
  - Off - The user can mute/reduce the volume to silent in the handset (default).

1. This function is applicable for Mitel 5624 Services and Mitel 5624 Personal Alarm only.

## Prevent Calls from being saved in the Call list

It is possible to prevent that the handset stores outgoing and incoming calls in the Call list. This can be useful to prevent that an unauthorized person views the call list.

1. Select Device > Call.
2. In the Enable call list drop-down list, select "Off" to prevent all calls being saved.

## .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

## Shared Phone

This setting defines if the handset is personal or shared. The default setting is "No" but if "Yes" is selected, the handset can be used by several users. Each user can still have their individual settings and access them using personal login and a password (the password can be a common password for all users or the call number). To use the Shared phone functionality, the following is required:

- The handset does not use certificate.
- WSM3
- Shared phone license (see [Upgrade Handset Functionality using License](#) on page 21)
- ESS (optional Ascom product)

A handset that is personal can also use a shared password (empty or specific) from the WSM3.

For personal password, a User Server (ESS) is required.

**Note:** If you accidentally enter a personal phone number in the shared handset, the handset becomes personal and cannot be used as a shared phone any longer. The handset must be configured to act as a shared phone again.

1. Select Device > General.
2. In the Shared phone license drop-down list, select one of the following:
  - No - The handset becomes a personal phone.
  - Yes - The handset becomes a shared phone.

**Note:** When the setting is changed, the handset is automatically restarted.

## Uploadable Language

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

TIP: It is also possible to upload a language on several handsets of the same device type simultaneously using the Baseline function in the WSM3. See *Wireless Messaging Gateway (WSM3) Installation and Operation Guide*.

---

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 is to be used in the handset, see [Select Default Language](#) for more information.

## 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.

## Shortcuts

One click access to predefined functions can be configured for the Soft keys, Hot keys, Navigation keys, and the Multifunction button<sup>1</sup>. For example a Soft key can be configured to make a call.

Shortcuts are configured using parameters in the "Shortcuts" folder, except Soft keys, which are configured in the "User Profiles" folder.

**Note:** A hot key configured to Services with the function "Data send" is also available during a call.

**Tip:** It is also possible to configure shortcuts using the handset menu. See the User Guide of the handset.

### *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. For example, the hot key function is used, to change the profile, send a message, or make a phone call to a specific number.

1. Select Shortcuts > Hot keys X (where X is 0, 2 - 9).
2. Continue with [Additional Shortcut Settings](#) on page 44.

### *Configure a Soft Key*

**Note:** When programming Soft keys, both name and function must be set.

1. Select User Profiles > Normal/Profile X > Soft keys > Soft key X (where X is Left, Middle, or Right)
2. In the Soft key name field, enter the name of the soft key shortcut to be displayed in the handset.
3. Continue with [Additional Shortcut Settings](#) on page 44.

1. The Multifunction button is applicable for Mitel 5624 and Mitel 5624 Services only.

### *Configure a Navigation Key*

1. Select Shortcuts > Navigation Key X (where X is Up, Down, Left, or Right)
2. Continue with [Additional Shortcut Settings](#) on page 44.

### *Configure the Multifunction Button<sup>1</sup>*

1. Select Shortcuts > Multifunction Button X (where X is Longpress or Multipress)
2. Continue with [Additional Shortcut Settings](#) on page 44.

### *Additional Shortcut Settings*

1. In the Function drop-down list, select the function to be used:
  - Phone call
  - Phone call "Loudspeaker mode"
  - Call List
  - Contact list
  - Central phonebook (system dependent feature)
  - Message inbox
  - Send Message
  - Change Profile Normal
  - Change Profile X (1- 4). (If selecting profile 1-4, the profile must first be configured, see [Profiles](#) on page 47.)
  - Open Menu (Main menu, Calls, Call Services, Connections, Contacts, Messaging, Services, Profiles, Settings.)
  - Executive Service X (1- 10) Services
  - Presence (system dependent feature)
  - Logout (applicable for the license dependent Shared Phone feature)
  - Call Diversions
  - RSSI Measure
  - Execute General Service X (1 - 16).
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 "Yes" if the Proceed? window is displayed after the key is pressed. This is used to prevent a function being accessed by mistake.
4. In the Read Only drop-down list, select "True" if the user is not able to change the shortcut.

### *Soft Key Functions During Call*

It is possible to configure the in-call functions for the left and right soft keys. The in-call functions are accessed by pressing the left or right soft key during a call.

1. Select Device > Call.
2. In the Left in call soft key name or Right in call soft key name field, enter the name of the soft key to be displayed during a call.
3. In the Left in call soft key action or Right in call soft key action drop-down list, select one of the following functions:

1. Applicable to Mitel 5624 and Mitel 5624 Services only.

- Conference
- Contacts
- Messaging (if applicable)
- Disabled
- End Call
- Hold
- Loudspeaker
- New call (put active on hold)
- Retrieve
- Switch
- Transfer (to held call)
- Transfer to new call (blind transfer)

4. Select OK.

## In-call Menu

The In Call menu is a configurable menu in the handset. The purpose of the In Call menu is to provide user friendly access to telephony functionality (PBX features) during a call, such as:

- Start a new call during a conversation
- Transfer a call
- Create a conference call
- Open Contacts (that is, Local phonebook and Company phonebook)
- Turning microphone on/off<sup>1</sup>

**Tip:** It is also possible to configure user-specific In-call functions, see [Configure Own In-call Functions](#) on page 45, or create a shortcut to a certain In call function, see [Create a Soft Key to an In-call Function](#) on page 46.

The menu is described in the *Mitel Wireless 5624 Handset User Guide*.

The programming of the menu is done with WinPDM. For instructions on how to work with WinPDM, see *Portable Device Manager, Windows version, Installation and Operation Guide*.

Using the WinPDM and the "Edit template" feature, the parameter can be found at Device > In call functionality.

Ask your supplier for example templates that configure the in-call menu for your PBX.

## Configure Own In-call Functions

Besides the default In-call functions (the left soft key configured as a loudspeaker key, and the right soft key configured as End-key), it is possible to define 10 extra system specific call services by codes. The codes can be programmed with any characters. Use \U to make the handset prompt for user input with numerical characters.

1. Select Device > In call functionality > General purpose <number>.
2. In the *Name* field, enter the name to be displayed in the In call menu.
3. In the *Data* field, enter the access code to be used for the function.

1. This option is always visible in the handset and cannot be disabled.

4. Click "OK" to save the settings.

**Tip:** Your supplier can have a template example that configures the In-call functions menu for the PBX.

#### *Create a Soft Key to an In-call Function*

It is possible to configure the left soft key or right soft key as a shortcut to a certain In call function, or hide the soft keys.

1. Select Device > Call > Left in call soft key name or Right in call soft key name. Enter a descriptive name for the soft key. This is not needed, if the functions *Loudspeaker* or *End call* are used.
2. In the drop-down list Device > Call > Left in call soft key action, or Right in call soft key action, select the function to be used:
  - Conference
  - Contacts
  - Messaging (if applicable)
  - Disabled
  - End call
  - Hold
  - Loudspeaker
  - New call (put active on hold)
  - Retrieve
  - Switch
  - Transfer (to held call)
  - Transfer to new call (blind transfer)
3. Click "OK" to save the settings.

#### *Hide a Soft Key to an In Call Function*

1. Select Device > Call > Left in call soft key action, or Right in call soft key action.
2. In the *Function* drop-down list, select "No action".
3. Click "OK" to save the settings. The soft key is not visible during a call, but is automatically replaced by the default soft key(s); left soft key Loudspeaker and right soft key End call.

### Call Services Menu

The Call services menu provides access to PBX dependent functionality when not in call, such as absence handling and call diversion. It is possible to use a Call service when the handset starts up, or when it shuts down.

The services are defined by parameters (Device > Call Services) in WinPDM.

The access codes are PBX dependent. Ask your supplier for an example template supporting your PBX.

### 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 WinPDM/WSM3 is used to import the phonebook file to the handset. See Import Contacts in

## Company Phonebook

It is possible to create a phonebook that is administered centrally and uploaded to the handset from WinPDM/WSM3. 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.

Perform the following steps:

1. Create a Company phonebook file, see [Create a Company Phonebook File](#).

Import the Company phonebook file to WinPDM/WSM3, see *Portable Device Manager, Windows version, Installation and Operation Guide* or *Wireless Messaging Gateway (WSM3) Installation and Operation Guide*.

Upload the company phonebook file to the handset(s), see *Portable Device Manager, Windows version, Installation and Operation Guide* or *Wireless Messaging Gateway (WSM3) Installation and Operation Guide*.

### *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 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).

## 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.

## Profiles

### User Profiles

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

1. Select User Profiles > User Profile X (where X represents the Normal profile (default) or Profile 1 - 4).
2. In the Name text field, enter the name of the profile.  
The name is visible in the handset and is also a selectable option in Profiles.
3. Select desired settings to edit:
  - Sound and Alerts
  - Presence and diversion
  - Answering
  - Alarm settings
  - Soft keys
  - Call service**Note:** The Call service is applicable to Profile X only (not profile "Normal")
4. If desired, select the profile to be active, by selecting User Profiles and change the default Active Profile "Normal" to desired profile.

**Tip:** It is also possible to configure profiles through the handset menu. See the User Guide of the handset.

## System Profiles

### Notes:

- This feature is applicable to Mitel 5624 Services and Mitel 5624 Personal Alarm only.
- A system profile overrides all profile "Normal" or Profile X settings, on all parameters in the group, for example, Soft Keys.

A system profile can be used when certain settings in a handset are required that the user is not allowed to change. The system profile is created in two steps:

1. Create the System Profile sub-group(s).

The following sub-groups are available:

- Presence groups, containing presence settings, and message absent.
- Answering groups, containing settings for how incoming calls are answered.
- Sound and alerts groups, containing sound and alert settings for calls and messages.
- Soft key groups, containing shortcut settings to predefined functions using key press.
- Alarm settings groups, containing settings for which alarm type is used and how.
- Idle display groups, containing settings to show the system profile name during idle mode.

2. Complete the System Profile by connecting it to the created sub-group(s), see [Create System Profile using Predefined Sub-groups](#) on page 51.

**Tip:** Once a System Profile is created, it can be used whenever desired and can be turned off and on again, see [Activate/Deactivate System Profile](#) on page 52.

### *Configure Presence groups (sub-group)*

1. Select System Profiles > System Profiles Sub Groups > Presence groups > Presence group X.
2. In the Name of group field, enter a descriptive name.
3. In the Message absent drop-down list, select one of the following:
  - On - When a handset receives a message, it indicates it is absent. The message can be redirected to another destination and is system dependent.
  - Off - The manual absence is disabled.



---

### *Configure Answering groups (sub-group)*

1. Select System Profiles > System Profiles Sub Groups > Answering groups > Answering group X.
2. In the Name of group field, enter a descriptive name.
3. In the Answer mode drop-down list, select one of the following:
  - Normal - The user must press the Call key to answer the call.
  - Automatically - The call is answered automatically after 1 second.
  - Loudspeaking - The user must press the Call key to answer the call, and the call is in loudspeaking mode.
  - Automatically loudspeaking - The call is automatically answered in loudspeaking mode after 1 second.
4. In the Answering key drop-down list, select one of the following:
  - Call key - Incoming calls are answered by pressing the Call key.
  - Any key - Incoming calls are answered by pressing any key

### *Configure Sounds and alerts groups (sub-group)*

1. Select System Profiles > System Profiles Sub Groups > Sound and alerts groups > Sound and alerts group X.
2. In the Name of group field, enter a descriptive name.
3. In the Ring volume mode drop-down list, select one of the following:
  - Silent - There is no ring signal.
  - Volume X (1 - 8) - Different ring signal volumes, from lowest (1) to highest (8) volume.
4. In the Vibrator drop-down list, select one of the following:
  - On - The vibrator function is active for incoming calls and messages (except when the handset is muted (Volume set to "Silent")).
  - On if silent - The vibrator function is active for incoming calls and messages, even if the handset is muted (Volume is set to "Silent").
  - Off - The vibrator function is off.
5. In the Internal ring signal drop-down list, select one of the following signals:  
There are three types:
  - Ring signal X (Sunrise etc.)- Defines one of 15 different predefined melodies.
  - Beep X (1 beep, 3 tone chime or alarm sweep etc.) X - Defines one of 7 beeps.
  - Custom sound X (Custom sound 8 - 10) - Defines one of 3 proprietary melodies made by coding with help of a specific code table in the On-Line Help.
6. In the External ring signal drop-down list, select one of the following signals:
  - The types are the same as for Internal ring signals.
7. In the Callback ring signal drop-down list, select one of the following signals:
  - The types are the same as for Internal ring signals.
8. In the Key sound drop-down list, select one of the following:
  - Click - A click is heard when a key is pressed on the handset.
  - Tone - A tone is heard when a key is pressed on the handset.
  - Silent - There is no sound when a key is pressed on the handset.

9. In the Message alert drop-down list, select one of the following:

The message sound for incoming messages can be either a melody or a single beep.

**Tip:** Any of the default handset beeps (Beeps and Enhanced beeps) are customizable, see [.Customize the default handset beeps](#) on page 95.

- Message X (1 - 7)- Defines the message sound for incoming messages as a certain melody.
- Beeps according to beep code - Defines the message sound for incoming messages according to the melody or beep coming from an application .
- High beeps according to beep code - The same type as “Beeps according to beep code”, but with a higher pitch.
- Enhanced beeps according to beep code - The same type as “Beeps according to beep code”, but in the form of a melody.
- Custom sounds according to beep code - Proprietary melody coming from an applicationIn the Message volume drop-down list, select one of the following:
- Silent - There is no message indication for incoming messages.
- Volume X (1 - 8) - Different message indication volumes, from lowest (1), to highest (8) volume.
- Follow ring volume - The message indication volume follows the ring volume.

#### *Configure Soft key groups (sub-group)*

1. Select System Profiles > System Profiles Sub Groups > Soft key groups > Soft key group X.
2. In the Name of group field, enter a descriptive name.
3. Select Soft key group X > Soft key X (left/middle/right), (in System Profiles > System Profiles Sub Groups > Soft key groups > Soft key group X) and edit required settings.
  - Soft key name - Defines the text that is shown in the handset display above the soft key.  
NOTE: A maximum number of 6 characters fits in the soft key name.
  - Function - Defines the function to be connected to the soft key.
  - Value - Defines a value (for example, a phone number) for a function.  
NOTE: The value is only needed for some functions.
  - Control Question - Defines if a Proceed? dialog window appears when pressing a soft key.

#### *Configure Alarm settings group (sub-group)*

1. Select System Profiles > System Profiles Sub Groups > Alarm settings groups > Alarm settings group X.
  2. In the Name of group field, enter a descriptive name.
  3. Select Alarm settings group X > Common (in System Profiles > System Profiles Sub Groups > Alarm settings groups) and edit required settings.
    - Stored alarm data - Predefined information that is sent with the alarm (for example a room number)
    - Indicate triggered alarm with LED<sup>1</sup>
    - Indicate triggered alarm with vibrator<sup>1</sup>
    - Indicate triggered alarm with beep signal<sup>1</sup>
1. If the parameter "Silent alarm" is set, no indication will be shown that an alarm has been sent or received, that is, there is no beep, vibrator, LED or pop-up window.

4. Select System Profiles > System Profiles Sub Groups > Alarm settings groups > Alarm settings X > Alarm on long press
  - Alarm type for long press - Defines the type of alarm that is sent by a long press (press and hold) on the alarm button. If Not used is selected, a predefined number can still be called automatically after an alarm, without sending an alarm.
  - ALS - Defines if a ramped up Acoustic Location Signal (ALS) sounds, after pressing the alarm button.  
NOTE: The ALS is not triggered if automatic call after alarm is active.
5. Select System Profiles > System Profiles Sub Groups > Alarm settings group > Alarm settings X > Alarm on multiple press
  - Alarm type for multiple press - Defines the type of alarm that is sent when pressing the alarm button twice or more. If Not used is selected, a predefined number can still be called automatically after an alarm without sending an alarm.
  - ALS - Defines if a ramped up Acoustic Location Signal (ALS) sounds after pressing the alarm button.  
NOTE: The ALS is not triggered if automatic call after alarm is active.

#### *Configure Idle display groups (sub-group)*

**Note:** By default, the name of a system profile is displayed in the handset. It is only needed to configure an idle display group, if the system profile name not shall be displayed in the handset.

1. Select System Profiles > System Profiles Sub Groups > Idle display groups > Idle display group X.
2. In the Name of group field, enter a descriptive name.
3. In the Show name of system profile drop-down list, select one of the following:
  - Yes - The system profile name is shown in the handset display in idle mode.
  - No - The system profile name is not shown in the handset display in idle mode.

#### *Create System Profile using Predefined Sub-groups*

In order to create a system profile, it must be connected to the desired predefined sub-groups.

**Note:** "Not Used" keeps "Normal" profile settings.

1. Select System Profiles > System Profile X.
  - Profile name - Enter a descriptive name to identify this system profile.
  - Presence groups - Defines which predefined presence group (sub-group) is used in this system profile.
  - Sound and alerts groups - Defines which predefined sound and alerts group (sub-group) is used in this system profile.
  - Soft keys groups - Defines which predefined soft key group (sub-group) is used in this system profile.
  - Answering groups - Defines which predefined answering group (sub-group) is used in this system profile.
  - Alarm settings groups - Defines which predefined alarm settings group (sub-group) is used in this system profile.  
NOTE: "Not Used" keeps the normal alarm settings defined under "Alarm".
  - Idle display groups - Defines which predefined idle display group (sub-group) is used in this system profile.  
NOTE: "Not Used" is not used.

### Activate/Deactivate System Profile

When a system profile is created, it can be activated on the handset using WinPDM/Device Manager or using an Unite application. For example, the application could be triggered by a positioning beacon. However, this section describes how to activate the system profile using WinPDM.

By default, when the system profile is activated, its name is displayed in the handset's idle screen.

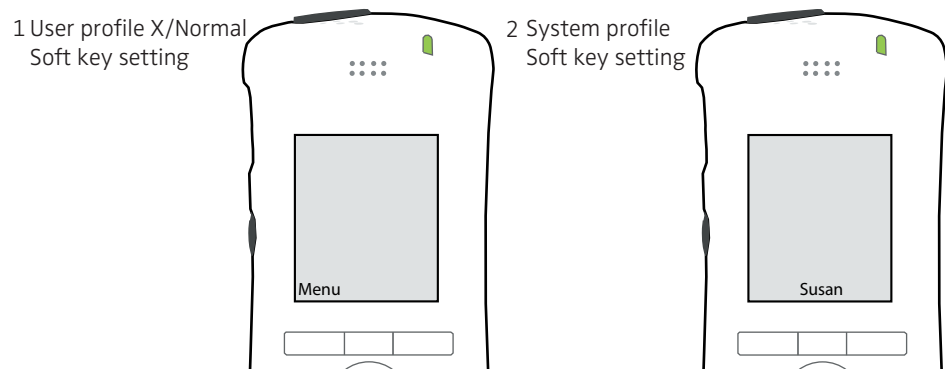
**Tip:** If a certain system profile always needs to be active on a handset, it is recommended to hide the settings/menus the user cannot change.

A System profile overrides all "User Profile X" and "Normal" (profile) settings on all parameters in the group, see the two examples below.

1. Select "System profiles".
2. In the Active system profile drop-down list, select one of the following:
  - Normal - no system profile is used.
  - [System profile]

Example 1:

Figure 4. A System profile affects a complete group of parameters, like all Soft keys.



On the left of the image above (1), the User Profile X (or the profile "Normal") is configured with a shortcut to open the menu on the left Soft key. Next, a System Profile shortcut to make a call to the administrator Susan, is configured for the free middle Soft key, see (2). When activating the System profile "Call to Susan", the left Soft key "Menu" disappears, because the System profile overrides the complete group of the Soft key parameters.

**Tip:** How parameters groups are arranged is seen under System Profiles > System Profiles Sub Groups.

Example 2:

If the user changes any settings that are specified in the System profile, the settings are not applied. In this case, the alarm settings have been configured in the system profile Alarm. Then the user cannot change any alarm settings using the handset, although the Alarm menu is visible. It is recommended to hide the Alarm menu to avoid misunderstanding.

## Telephony

The following parameters are required for the basic telephony settings.

---

## Endpoint ID and Endpoint number

The Endpoint ID and Endpoint number are automatically 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 the idle mode. To change the name displayed in the handset, see [User Display Text](#) on page 72.

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

## 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 section [H.323 Protocol](#) or section [SIP Protocol](#) 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 is required.

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

**Note:** To make the H.323 Gatekeeper registration work in Node environment, it is possible to only use the Endpoint ID for registration by selecting Voip > H.323 > Register with Endpoint ID only > Yes.

### *SIP Protocol*

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

- SIP Transport – defines the protocol (UDP, TCP or TLS) to use for SIP signaling. The TLS setting requires the PBX certificate to be uploaded as root certificate. It is also possible to turn off the validation of the server certificate, if set to "No".
- Outbound proxy mode – Set to "Yes" if the handsets are to connect with the SIP proxy through an outbound proxy. 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 either an IP address, a domain name, or an IP address together with a port number.

Examples of valid formats are:

192.168.1.1

proxy1.mydomain.com

192.168.1.1:5060

Domain names are resolved using DNS records, and refer either to a DNS A record (address record) or a DNS SRV record (service record). While an A record is a single IP address, a SRV record originates from multiple A records, of which the handset tries the two highest prioritized IP addresses it receives in the DNS response when it registers with the primary SIP proxy.

Only a plain IP address is shown in the handsets Admin menu (under VoIP > Protocol > SIP > SIP proxy IP address).

If the handset fails to register with the primary SIP proxy, it can register with the optional secondary SIP proxy.

NOTE: The parameter is only visible, if the parameter Outbound Proxy mode is set to "No".

- Secondary SIP proxy – defines the optional secondary SIP proxy, which is used if the handset fails to register with the primary SIP proxy. See definition examples in Primary SIP proxy above.  
When the handset has connected to the Secondary SIP proxy, it continuously tries to reconnect to the Primary SIP proxy.
- Outbound proxy – defines the primary outbound proxy by a domain name, an IP address, or an IP address together with a port number. The parameter is only visible, if the parameter Outbound Proxy mode is set to "Yes".
- 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 can 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 the path the DTMF signaling should take. If set to "RFC 2833", the DTMF signaling is sent in the RTP stream, that is, from handset to handset. If set to "SIP INFO", the DTMF signaling is sent using SIP signaling, that is, through the PBX.
- Hold type – defines type of hold to send when the handset puts a call on hold. The selection depends on what types of hold the PBX support. For more information about what types of hold the PBX support, see the applicable documentation for the PBX.
- Registration identity – defines if the endpoint uses its number or ID for the registration with the SIP proxy.
- Authentication identity – defines if the endpoint uses 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 the call forward locally functionality.

- 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.
- SIP Register Expiration - defines the number of seconds for register expiration to the PBX.

## 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.

## Offer Secure RTP

When enabled, voice is sent over Secure RTP, if the other party also supports Secure RTP.

### *SIP Protocol*

1. Set parameter VoIP > SIP > SIP Transport to “TLS”.
2. Set parameter VoIP > General > Offer Secure RTP to “Yes”.
3. Select the preferred SRTP encryption by assigning a value to parameter VoIP > General > Secure RTP Crypto, which appears when enabling Secure RTP.

### *H.323 Protocol*

1. Configure the gatekeeper to require password authentication.
2. Add the password to parameter VoIP > H.323 > Gatekeeper password.
3. Set parameter VoIP > General > Offer Secure RTP to “Yes”.
4. Select the preferred SRTP encryption by assigning a value to parameter VoIP > General > Secure RTP Crypto, which appears when enabling Secure RTP.

## 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.

## Emergency Call Numbers

Up to five different phone numbers can be reserved for emergency calls. These numbers can always be called even when the phone- or key locks are active.

**Note:** If emergency numbers of varying length are used, care must be taken to ensure that longer numbers do not begin with the same digits and ordering used by a shorter number. For example, if 124 and 1245 define two emergency numbers, the number 1245 cannot be used, because 124 is always evaluated and called before the longer number. However, 5421 and 1256 is, for example, allowed.

1. Select Device > Call.
2. In the Emergency call Numbers field, enter the desired emergency number(s).
3. Select Alarm<sup>1</sup> > Emergency call.
4. In the Emergency call alarm drop-down list, select one of the following:
  - On - An alarm is sent when the user calls the emergency number.
  - Off - No alarm is sent when the user calls the emergency number.
5. In the Alarm type text field, write the text to be shown in the handset display when an emergency call is made. If this field is empty, the default text "Emergency call alarm" is shown.

### 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.

### Message Centre Number

Specifies the number for the server responsible for Message Waiting Indication (MWI), if included in the system.

1. Select Device > Message centre.
2. In the Message Centre number field, enter the number for the server.

**Note:** The Voice mail call clears MWI drop-down list is not used.

### 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 the number of calls

### Dial Pause Time

By adding a "P" to a phone number, a pause is added and is activated when dialing. For how long time it is activated, is also defined here.

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

### Direct off Hook from Charger

The handset automatically answers 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".

1. This function is applicable for Mitel 5624 Personal Alarm only.



---

## 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”.

## Call waiting behavior

The default behavior is to indicate “call waiting” to the user. It is possible to change this behavior so that the next incoming call is rejected, and a busy indication is sent back to the SIP proxy.

1. Select Device > Call.
2. In the Call waiting behavior drop-down list, select one of the following:
  - Call waiting indication - The call is usually indicated by a short two-beep tone and an “Incoming call” dialog window in the handset display.
  - Reject call - The call is automatically rejected (No beep tone or dialog window occurs).
  - Reject call and show as missed - The call is automatically rejected and directed to the “Missed calls” list. (No beep tone or dialog window occurs).

## Connecting 5624 WiFi Phones to MiVoice Office 250

This chapter provides general guidelines for 5624 WiFi phone connection to MiVoice Office 250 R 6.2.

### Peripheral Devices for 5624 WiFi Phone

#### *Desktop Charger*

You use the desktop charger to charge the handset and the Mitel 5624 Desktop Programmer to download new software and synchronize parameters. The units look the same except that the Desktop Programmer has a USB connection. The handset is fully operational while placed in the charger.

#### *WinPDM software installed on your PC*

The Portable Device Manager (PDM) is an all-in-one portable handset management tool. The PDM software application, with a web browser-based environment and USB programming cradle, provides a simple administration process for portable handset subscription and configuration. Portable handset replacement and service is easily facilitated by the central storage of configuration information.

#### *WiFi Router*

For more information and installation steps please refer to Chapter 3 and Chapter 4 from the Mitel WiFi 5624 Handset Configuration Guide.

### MiVoice Office 250 Database Programming

#### *Network Requirements*

There must be adequate bandwidth to support the voice over IP (VOIP). As a guide, the Ethernet bandwidth is approximately 85 Kb/s per G.711 voice session and 29 Kb/s per G.729 voice session (assumes 20ms packetization). As an example, for 20 simultaneous SIP sessions, the Ethernet

bandwidth consumption will be approximately 1.7 Mb/s for G.711 and 0.6Mb/s. Almost all Enterprise LAN networks can support this level of traffic without any special engineering.

For high quality voice, the network connectivity must support a voice-quality grade of service (packet loss <1%, jitter < 30ms, one-way delay < 80ms).

Please refer to the MiVoice Office 250 Feature & Programming Guide in <http://edocs.mitel.com> for further information.

#### *Assumptions for the MiVoice Office Programming*

The SIP signaling connection uses UDP on Port 5060.

#### *Software License - SIP Licensing*

Ensure that MiVoice Office is equipped with enough Category 'F' Phones licenses for the connection of SIP end points. This can be verified within the Software License Feature section form.

File View Operations Tools Favorites Help	
Recent 5000 CP > Software License	
5000 CP	Software License Feature Value
Maintenance Accounts	System Type 5000 CP
Software License	ACD Hunt Group Yes
System	Additional T1/E1/PRI Ports 3
Users	Agent Help Yes
Voice Processor	Analog Voice Mail Hunt Group Yes
	Category 'A' Phones 100
	Category 'B' Phones 100
	Category 'C' Phones 100
	Category 'D' Phones 100
	Category 'E' Phones 32
	Category 'F' Phones 32
	Desktop Interface Yes
	Dynamic Extension Express Yes
	File-Based MOH Sources 100
	Hot Desking Yes
	IP Networking Unlimited
	Meet-Me Conferencing Yes
	Remote ACD Hunt Groups Yes
	SIP Trunks 100
	SIP Voice Mail Ports 100
	System Health Report Yes
	System OAI Events Yes
	System OAI Third Party Call Control Yes
	Voice Processor Messaging Networking Yes
	Unified Voice Messaging Ports 32
	Unified Voice Messaging Blackberry® Integration Yes
	Unified Voice Messaging E-mail Synchronization Yes
	User Web Portal Yes
Node 1	Online 5000 CP North America Dot51 192.168.101.51

Figure 5. Software License

## SIP Phone Creation

1. Add a SIP phone in MiVoice Office 250.

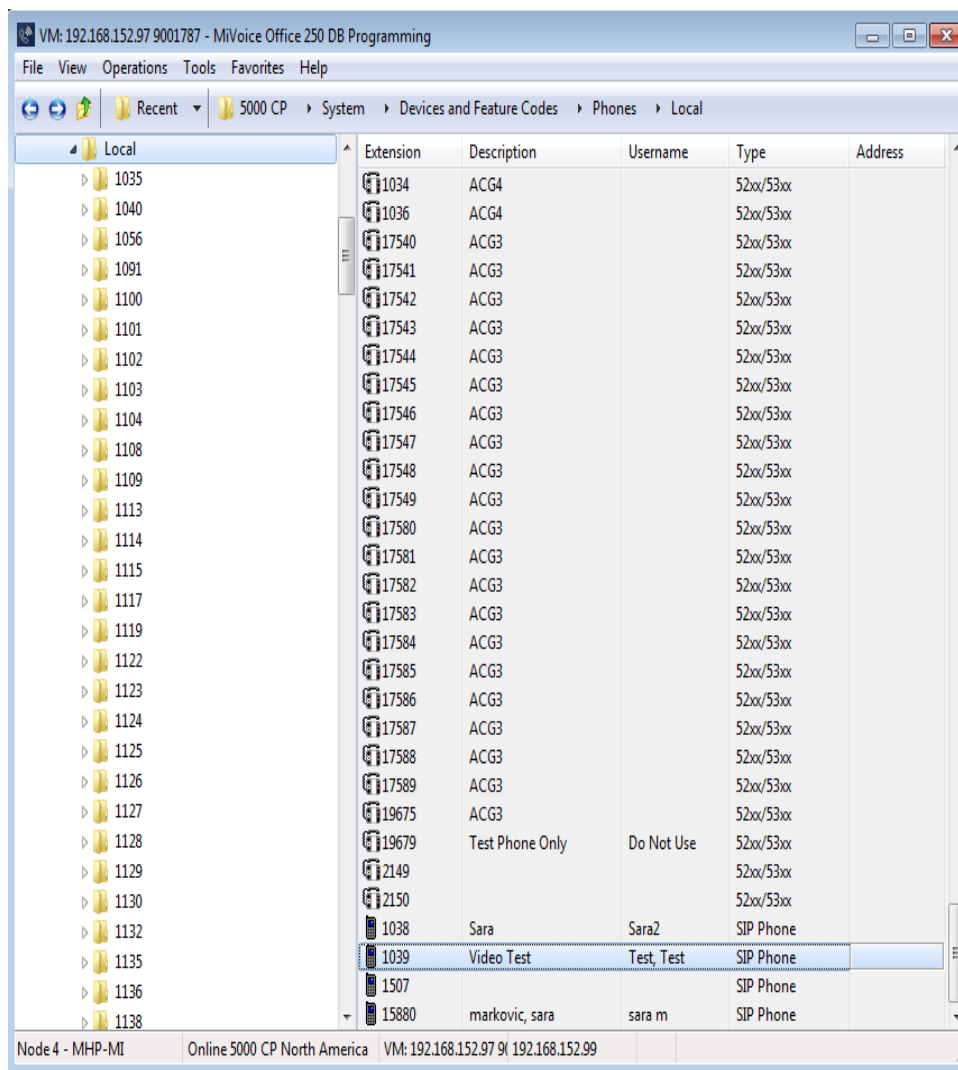


Figure 6. Adding a SIP phone in MiVoice Office 250

2. Change the password for security reasons. Remember the new password. The current password is the extension number.
3. Under **System > Devices and Feature Codes**, click **Phones**.
4. After creating the SIP phone, the MiVoice Office 250 Database Programming automatically creates a SIP Phone Group with a default configuration profile.  
Go to **System > Devices and Feature Codes > SIP Peers > SIP Phone Groups<the SIP Phone group> > Configuration**.  
The <SIP Phone group> in the following example is **P9004**.

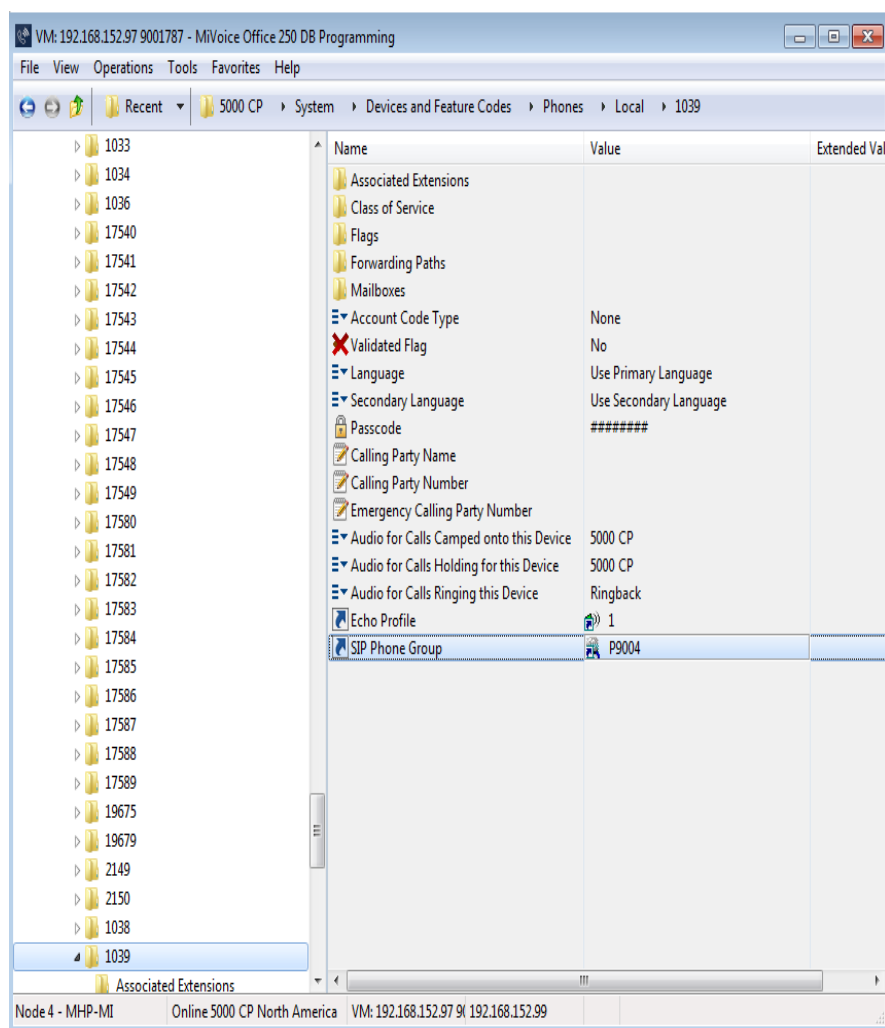


Figure 7. Configuring of SIP Phone Group on MiVoice Office 250

5. In the right-side pane, click **Maximum Number of Calls**, and select **4** from the adjacent drop-down list. No other changes are required under this profile.

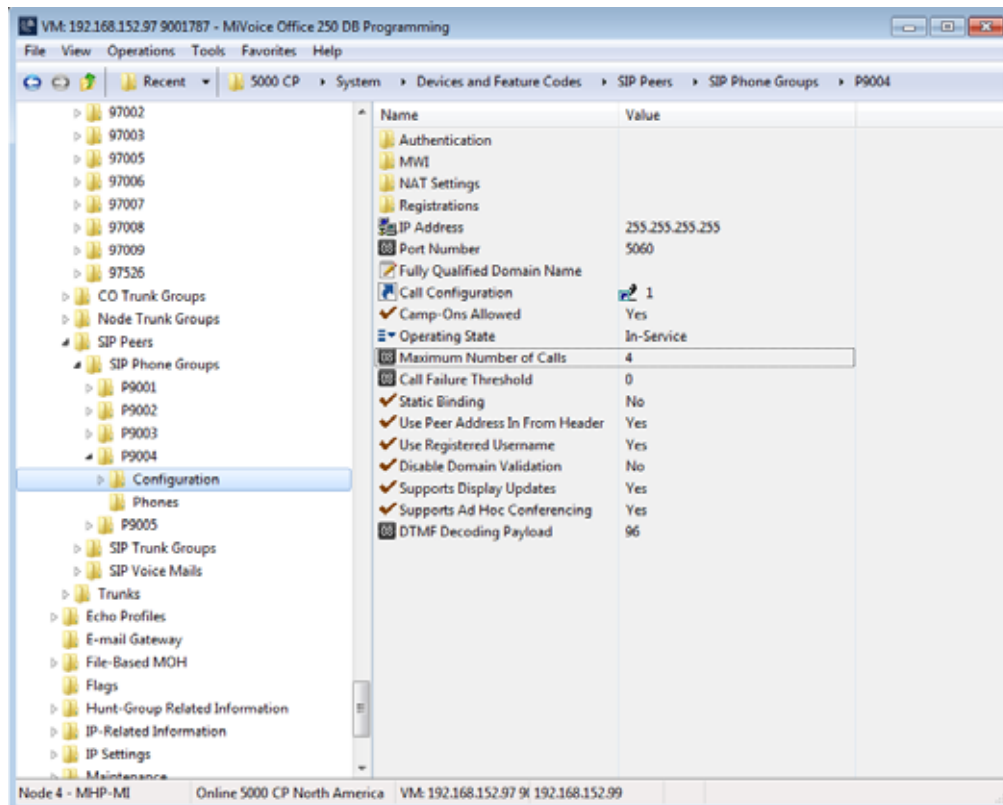


Figure 8. Configuring of SIP Phone Group on MiVoice Office 250

## 6. SIP Phone Authentication

To increase the security of SIP devices Mitel recommends enabling In-Bound Authentication where possible. Click **Authentication** and ensure that option **Enable In-bound Authentication** is set to **Yes** as shown in the following Figure 9.

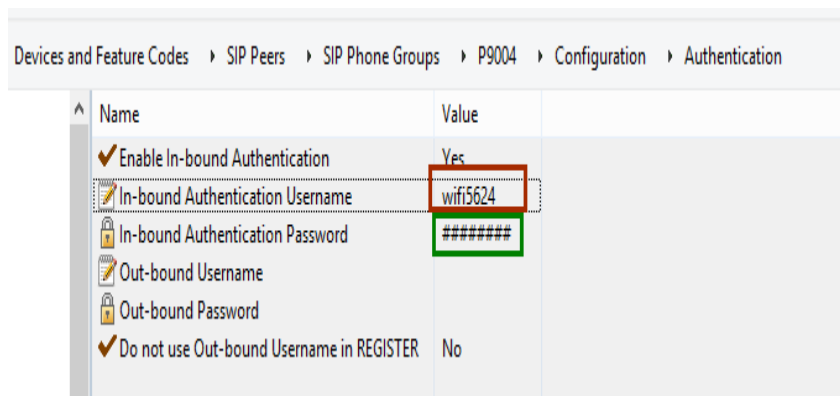


Figure 9. Enabling In-bound Authentication

Enter alphanumerical details in the In-Bound Authentication Username and Password fields.

Making these changes provides an increased level of security as the SIP device is challenged for log on, and its username and password checked against those you have configured.

In WinPDM:

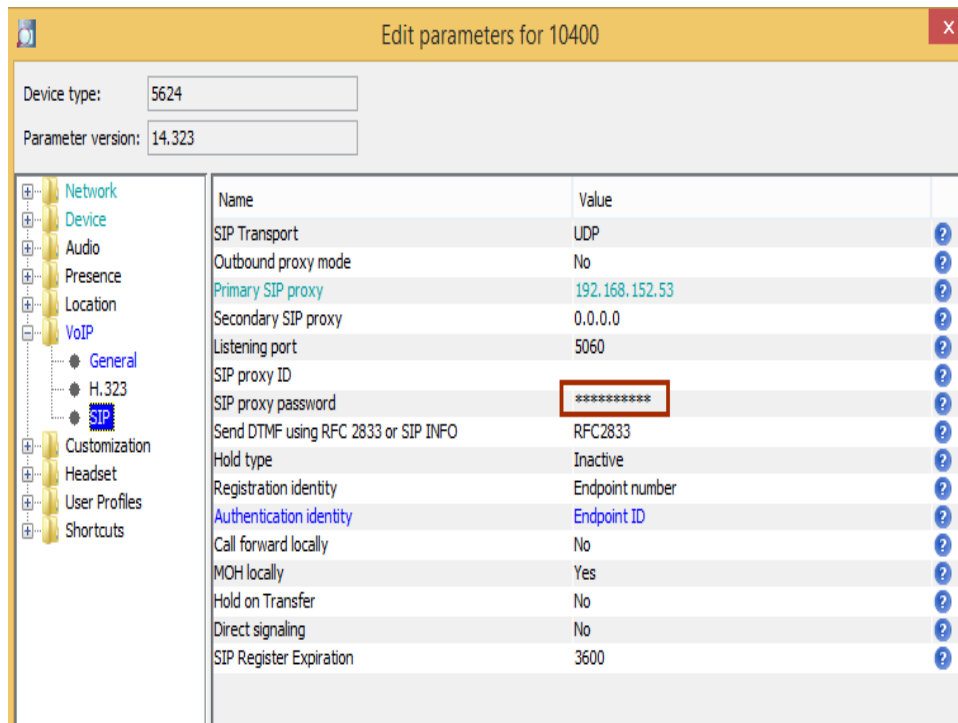
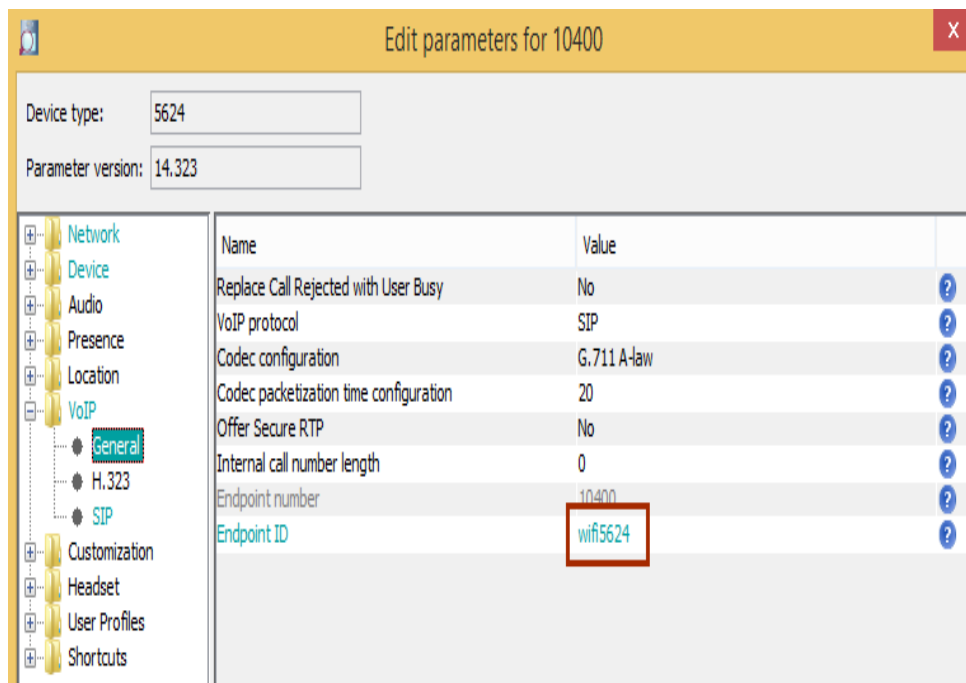


Figure 10. Edit Parameters for SIP Authentication

In left hand pane, click **VoIP** > **SIP**. Enter the IP address/FQDN of the Mitel MiVoice Office. Enter the password of the device as previously configured on the MiVoice Office in the **SIP proxy password** field.

Ensure that In-Bound Authentication password in DBP matches SIP proxy password set in the WinPDM.



In left hand pane, click **VoIP** > **General**. Enter the Endpoint number and Endpoint ID.

Ensure that In-bound Authentication Username in DBP matches with Endpoint ID set in WinPDM.

Please refer to the MiVoice Office 250 Feature and Programming Guidelines in <http://edocs.mitel.com> for further information.

## 5624 Wi-Fi Phone Configuration

### WinPDM

The WinPDM runs on a PC and is used to configure the handset as follows:

1. Connect a **Mitel 5624 Desktop Programmer** cradle through a USB port, to the computer running **WinPDM**.
2. Start **WinPDM**.

For instructions on how to install and use the WinPDM, see Portable Device Manager, Windows version, Installation and Operation Guide.

### Configuration Procedure

1. Open **WinPDM** and load the latest version of 5624 build:  
**File > File Management > Add** (add 5624.pkg file, for example see following image)



Mitel\_5624\_v5.1.30.pkg)

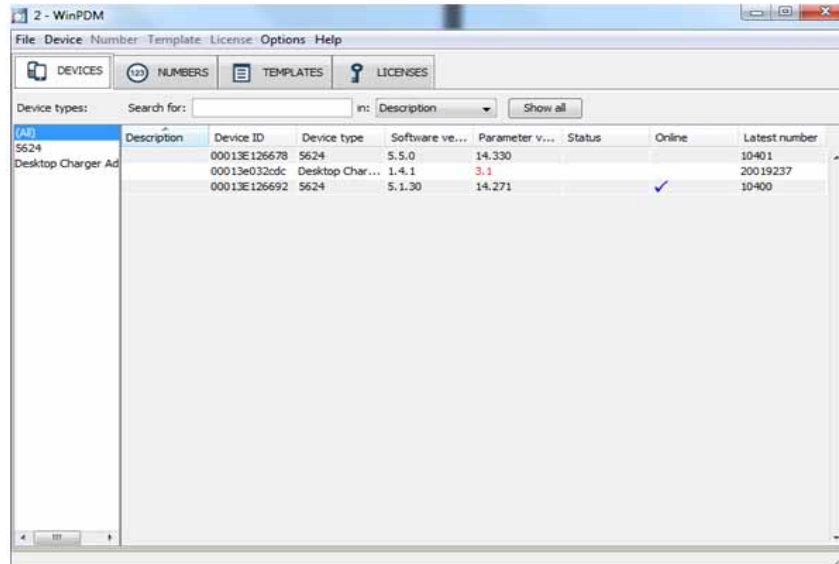


Figure 11. WinPDM main window

2. Place the **5624 WiFi** handset in this cradle connected to **WinPDM**. (5624 must appear in Devices with Online status).
3. Select 5624 phone and upgrade it (if needed).

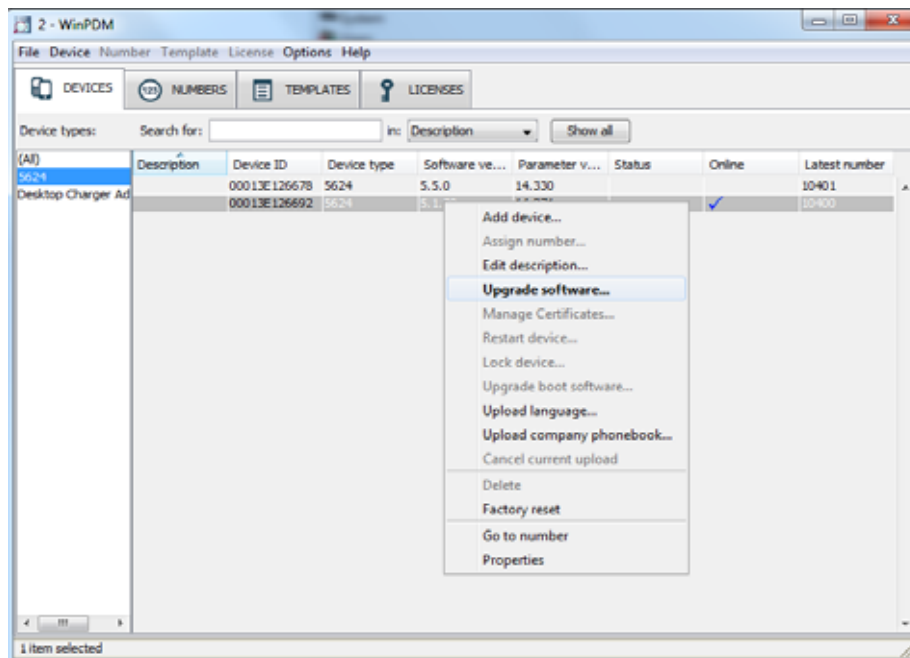
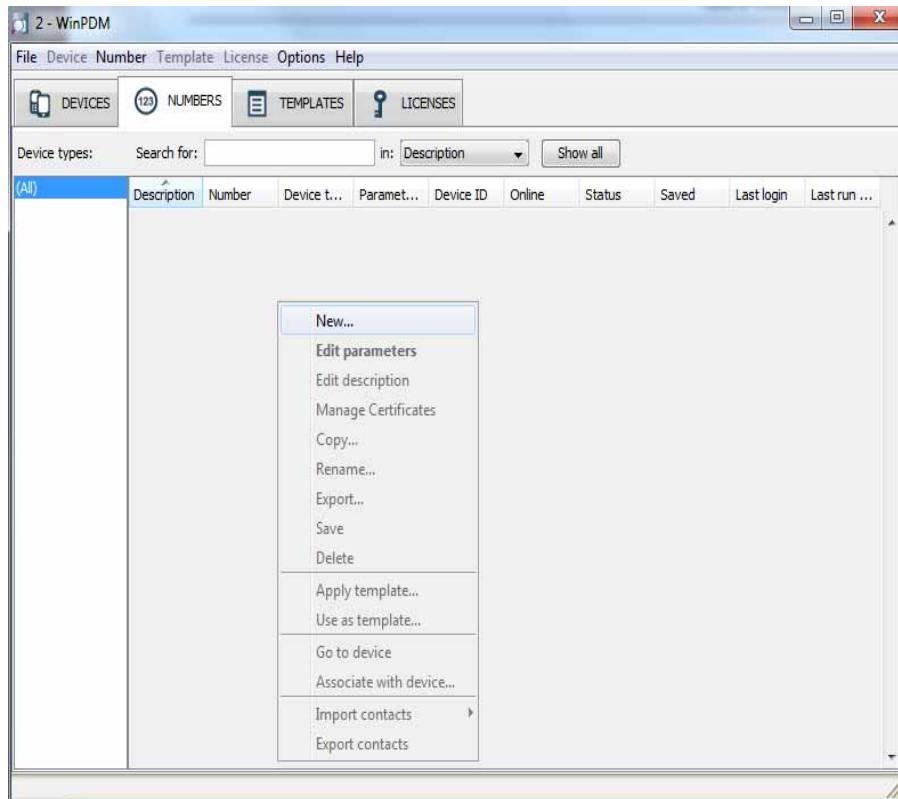


Figure 1: Upgrade Software

4. Import MiVO 250 template if required:
  1. Go to **File > Import > Templates** and import template for MiVO 250.

2. Go to **Numbers**.

(Please note that if the number does not appear after inserting 5624 into the Desktop Programmer you must create it manually).



5. In **Call Number** enter extension of SIP phone created on MiVoice Office 250.



Figure 12. New Number Creation

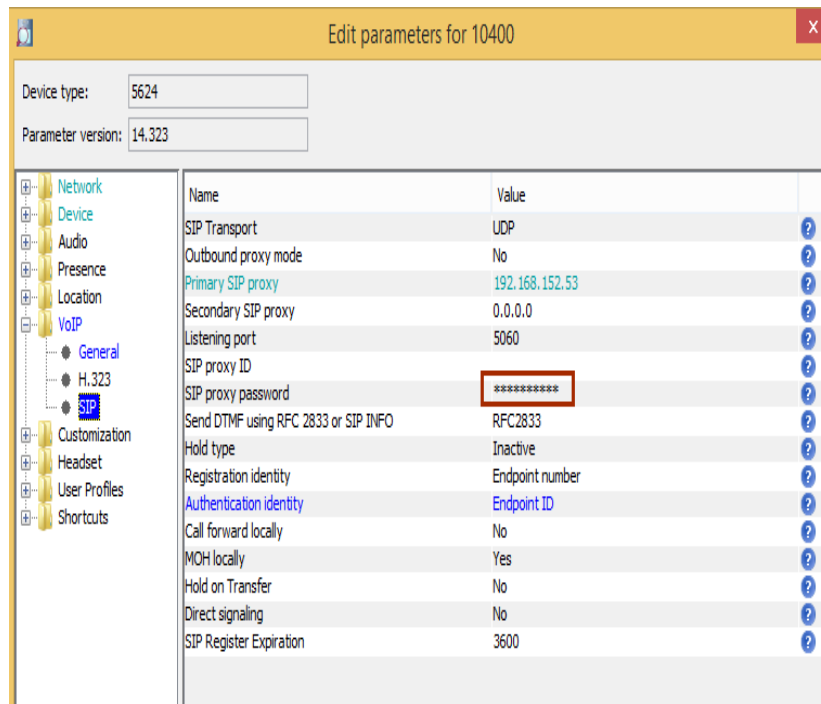


Figure 13. Edit Parameters for 5624 WiFi Phone

6. In **Edit Parameters** screen, collapse **System** node and select **Network A**. Configure the highlighted parameters.

**Note:** The setting for **SSID** must match exactly the one configured in your wireless access point (your router).



Figure 14. Network configuration

7. In **Edit Parameters** screen, expand **VoIP** node and click **General**. Select SIP as the VoIP protocol and ensure that the Codec configuration conforms to your Network deployment.
8. In **Settings**, enter User display text and User display number of your extension.

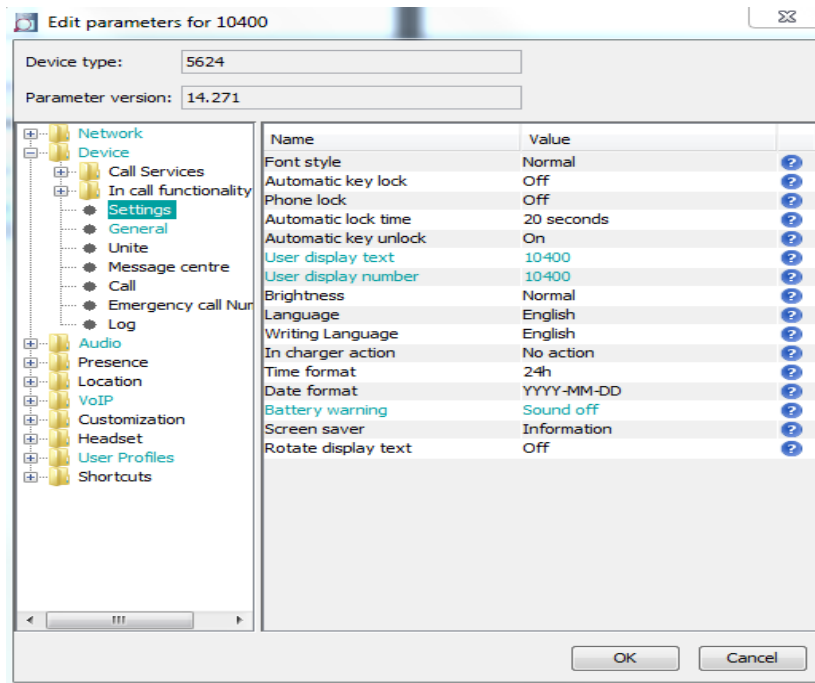


Figure 15. Add User display text and User display number

9. Enter Primary SIP proxy (your PBX system IP address) and press **OK**.

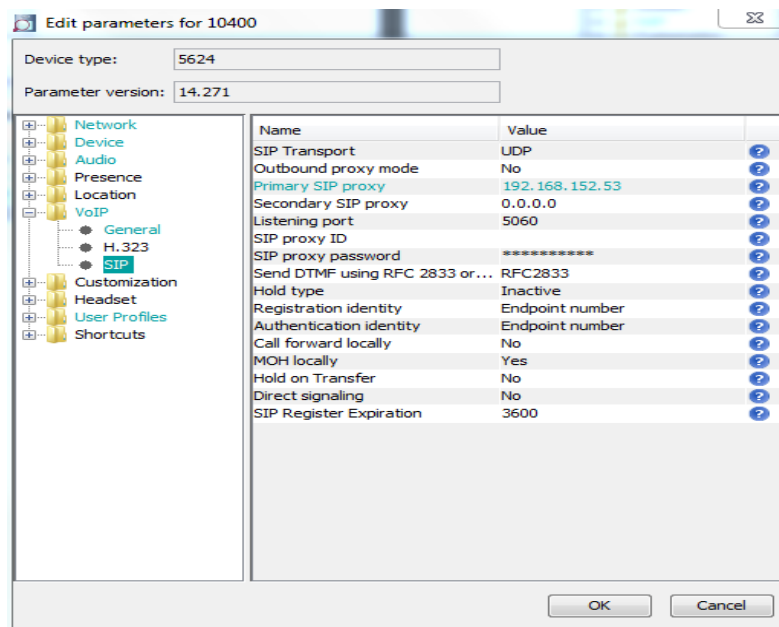


Figure 16. SIP Proxy Configuration

10. In the left pane, click **Device > Message Centre**.  
The "Message Centre number" is required for the handset to send SUBSCRIBE message to the MiVoice Office (needed for MWI). Enter the extension of the Voice Mail in both the "Message Centre number" and the "Voice mail number".
11. Verify 5624 phone is connected now to WiFi router.
12. There is no **No Access** warning on display.

---

## MiVO 250 Feature Compatibility

The table below provides the list of supported features:

**Table 2: MiVO 250 Supported Features List**

MiVO 250 Features	Supported
Basic Calls	YES
DTMF	YES
Transfer	YES
Hold	YES
Music on Hold	YES
Calls to Voicemail	YES
Switch Calls	YES
Trunk Calls	YES
Mute	YES
Forward	YES
DND	YES
Off-Node Device	YES
Peer-to-Peer Media	YES
Ring-In Destination	YES
SIP Peer Features	YES
User Web Portal	YES
Voice Mail	YES
Call Logging	YES
Call Screening	YES
Call Waiting (Camp-on)	YES
Conference Calls	YES
Configuration Assistant	YES
Dynamic Extension Express (DEE)	YES
Emergency Calls	YES
Handoff-Pull	YES
Hookflash	YES
Hunt Groups: UCD Hunt Group Number	YES
Hunt Groups: Recall Destination	YES
Intercom Calls	YES
Manual Forwarding	YES
Messages	YES
On-Hook Monitoring	YES
Outside calls	YES

Outgoing Access	YES
Outgoing Extension	YES
Record-A-Call	YES
Redial Calls	YES
Redirect Calls	YES
Speed Dials	YES
System Forwarding	YES

Following Table 2 provides the list of Unsupported features:

**Table 3: MiVO 250 Unsupported Features List**

Features	Supported
Directory	NO
Group Listen	NO
Handoff-Push	NO
Hold Recalls	NO
Hunt Groups: ACD Hunt Group Number	NO
Intelligent Directory Search	NO
Multilingual Capability	NO
Off-Hook Voice Announce	NO
Phone Feature Codes	NO
Queue	NO
Reminder Message	NO
Background Music	NO
Automatic Call Access	NO
Account Codes	NO

## Regional Settings

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

### Set Time & Date

1. Select **Device > General**.
2. In the Time zone drop-down list, select the applicable time zone.
3. If the time zone "Other" is selected, a string must be entered in the Time zone string field to define the time zone.  
For time zone format, see:  
[http://pubs.opengroup.org/onlinepubs/009695399/basedefs/xbd\\_chap08.html](http://pubs.opengroup.org/onlinepubs/009695399/basedefs/xbd_chap08.html)  
For time zones, see:  
<http://www.timeanddate.com>

**Note:** Only unquoted format is supported.

---

Enter the time zone string if automatically update for summer/winter is desired:

<String = StdOffset [Dst[Offset], Date/Time, Date/Time]>

- Std = Time zone (for example EST for Eastern Standard Time).
- Offset = time difference between the timezone and the UTC (Universal Time Coordinator).
- Dst = summertime zone (for example EDT for Eastern Daylight Time).
- Second Offset = time difference between the summer time and the UTC.
- Date/ Time, Date/ Time = beginning and end of summertime.
  - date format = Mm.n.d (d day of n week in the m month)
  - time format = hh:mm:ss in 24-hour format.  
Note that a week always starts on a Sunday and the number for Sunday is 0.

Example:

North Carolina is located in the Eastern Time Zone. Eastern Standard Time (EST) is 5 hours behind UTC (StdOffset = EST5), the Eastern Daylight Time (EDT) is 4 hours behind UTC (DstOffset = EDT4). Summertime for the year 2013 begins at two a clock, on a Sunday, the second week in March (M3.2.0/2). The summertime ends at two a clock, on a Sunday, the first week in November (M11.1.0/2).

<String = EST5EDT4,M3.2.0/2,M11.1.0/2>

4. In the NTP server field, enter the address to the time server. If not set, the IP PBX address is used.
5. Select Device > Settings.
6. In the Time format drop-down list, select the applicable time format:  
12h (for example 11:59 am/pm)  
24h (for example 23:59)
7. 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

## 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 [Uploadable Language](#) on page 42 for more information.

## Dialing Tone Pattern

Defines the tone pattern to use when dialing.

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

## Display

### User Display Text

Defines the 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 is displayed.

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

### Rotate Display Text

The handset can be configured to show the contents of the display (except the soft key bar) upside-down at incoming calls or messages.

1. Select Device > Settings > Display.
2. In the Rotate display text list, choose Normal or Inverted.

### 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.

### 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 off when handset is in idle mode.

### Brightness

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

### Screen Saver

1. Select Device > Settings.
2. In the Screen saver drop-down list, select one of the following:
  - Information - time and status (for example message indication) is shown on the screen saver.



- Black - no information is shown on the screen saver.
- Black also in call - the “Black” screen saver (with no information) is shown also during phone calls.

**Note:** It is recommended to only use the screen saver setting “Black also in call”, when extended battery life is needed. Use also other screen saver settings than “Black also in call” if the handset needs to be set to silent (muted).

## Menu Operation

### 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 is visible in the handset, but cannot be edited by the user. The following items can be hidden:
  - Connections (Network, Headset etc.)
  - Calls
  - Contacts
  - Shortcuts (Soft keys, Hot keys etc.)
  - Messaging
  - Services
  - Profiles
  - Settings (Sounds, Display, Language etc.)

### Services

**Note:** Applicable to Mitel 5624 Services and Mitel 5624 Personal Alarm only.

It is possible to configure up to ten services that can be accessed from the handset’s Services menu.

1. Select “Services”.
2. Select between 1 - 10.
3. In the Service name, enter the name of the service to be displayed in the handset’s Service menu.
4. Select the service to be used:
  - Phone Call
  - Send a message to predefined number (prompt for the message text)
  - Send data to message service centre (predefined data and/or prompt for the data)
  - Edit alarm data
  - PTT
5. In the Service user data field, enter the data to be sent/dialed when using the service.

**Note:** This field is not applicable for PTT.

6. In the Service prefix for user data field, enter the prefix for the service user data (if needed).

7. In the Service index field, enter the corresponding index used for PTT. For example, if PTT group 1 is configured (located under Push-To-Talk > 1), the service index must be set to 1.

**Note:** This field is only applicable for PTT.

If the PTT is not configured, continue, with [Push-To-Talk \(PTT\) Group Call](#).

**Tip:** It is also possible to configure soft keys to reach services quickly, see [Shortcuts](#) on page 43.

## Push-To-Talk (PTT) Group Call

To be able to configure a PTT session, the following must be known:

- The group number to the PTT group (defined in the WSM3)
- The phone number to the conference bridge

**Tip:** For more information about the PTT function, see also *Mitel VoWiFi Function Description* or *Mitel Wireless 5624 Handset User Guide*.

**Note:** If Music on Hold (MOH) is used in the system, it can affect an ongoing PTT group call. If someone in the group conference answers another incoming call, MOH is played for the whole group.

1. Select Push-To-Talk > X (where X represents 1-10).
2. In the *Session name* field, enter a name to identify the PTT session.
3. In the *Group number* field, enter the number for the PTT conference group.
4. In the Display text field, enter the text to be shown in the display during the PTT session.
5. In the PTT session signal drop-down list, select the indication of the PTT session.
6. In the Conference number field, enter the phone number to the conference bridge.
7. In the Answer mode drop-down list, select the answer mode for the PTT session.
8. In the Speaker mode drop-down list, select the speaker mode for the PTT session.
9. If it is desired to have the automatic key lock on during an ongoing call, select Device> Settings. In the Automatic key lock drop-down list, change the automatic key lock setting to "On", see [Automatic key lock](#) on page 38 and [Automatic lock time](#) on page 38.
10. A Service must be configured to access the PTT session from the handset. If not configured, continue with [Services](#).

## Presence Management

**Note:** This is a system dependent feature.

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

- The IP address of 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 *Mitel VoWiFi Function Description* or *Mitel Wireless 5624 Handset User Guide*.

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 of the presence management system.

5. In the *Listening port* field, enter the port number that the presence management system needs to 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 is visible under Call > Presence in the handset. It is also possible to configure a shortcut in order to access the Presence menu, see [Shortcuts](#) on page 43.

## Location

Two types of location are supported, either a basic location solution that gives an approximate location using Access Point (AP) location, or a personal security solution that gives a more accurate location using a third-party Real-Time Location System (RTLS) solution.

The following RTLS solutions are supported:

- Cisco RTLS Solution  
To use the Cisco RTLS solution, use a Cisco Mobility Services Engine and the handset must also be configured.
- Ekahau RTLS Solution  
To use the Ekahau RTLS solution, the handset must have the Ekahau license (see [Upgrade Handset Functionality using License](#) on page 21) and the handset must also be configured.

### Configure Handset for Cisco/Ekahau RTLS Solution

1. Select Location > Common.
2. In the *Location scanning drop-down list*, select “Enable”.
3. In the *Scanning interval*<sup>1</sup> field, set the time between the scanning periods.
4. In the *Scans per scanning period*<sup>1</sup> drop-down list, select how many scans that should be performed during each scanning period.  
If the Ekahau RTLS solution is used, also perform the steps 5 - 8.
5. Select Location > Ekahau.
6. In the EKAHAU license drop-down list, select “Yes”. Additional parameters are shown.
7. In the IP address field, enter the IP address for the Ekahau location appliance.
8. In the *Listening port* field, enter the port that the location appliance is listening to.

1. Note that close scanning periods, and frequently scans per period, will shorten the battery time.

# Use Handset to Verify the VoWiFi System Deployment

## 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 analyzers can be used to provide additional assistance during a site survey.

## Scan the Channels

To be able to use the site survey functions in the handset, configure the site survey functions 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 is limited to 1, 6, and 11.

The table is upgraded regularly, starting with scanning channel 1, then 6 and finally 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 can 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 scanning of channels 12 and 13 is also of interest use value "ETSI".

There are two ways of scanning channels:

- Scan all channels
- Scan a specific channel

### 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 menu:
  - 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.

---

## 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 menu:
  - 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.

## 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 AP. Sudden drops in field strength caused by the environment are delayed because the value of field strength is filtered. For example walking through a door into a room. Thus it is important to walk slowly through the site to cover all weak spots.

### 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 menu:
  - 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".

### 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 menu:
  - 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

## Location Survey

The location survey function makes it possible to use Site survey mode for Ekahau that causes location scanning to be performed at shorter intervals: 1s.

**Note:** This function requires the location license.

1. There are two options to access the Site Survey Tool menu:
  - 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 “Location survey”
3. Select one of the following:
  - On - Activates the location survey
  - Off - Deactivates the location survey

# Handset Internal Web Administration Page

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

- View general information about a handset
- Troubleshoot the VoWiFi System.
- View statistics

## 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).

### General View

In the "System" tab, the following information is displayed:

- Software version
- MAC address
- SNTP server
- Local time
- Uptime
- License information
- Network information
- VoIP information
- SIP proxy/H.323 gatekeeper IP address
- End User License Agreement (EULA).

Figure 17. Internal Web Administration Page

System	
Info	Version 3.4.6
EULA	MAC address 00:01:3e:11:03:ed
	SNTP server 172.20.9.219
	Local time 14:19 2012-06-13 (UTC+1)
	Uptime 124:56:51
-License info-	
	License i62 Protector
	Ekahau Location yes
	Shared Phone yes
	Man-down/No-movement no
-Network info-	
	DHCP enabled yes
	IP address 172.20.15.61
	Subnet mask 255.255.248.0
	Default gateway 172.20.8.1
	Primary DNS 172.20.8.145
	Secondary DNS 172.20.8.100
	Domain name ascom-ws.com
	Syslog enabled yes
	Syslog server 172.20.14.220
-VoIP info-	
	VoIP protocol SIP
	Endpoint number 6350
	SIP proxy IP address 172.20.9.219
	Secondary SIP proxy IP address -

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 WinPDM. See [1. Open the WinPDM](#) on page 80.

## 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 on "Troubleshoot".
3. If needed, enter administration user name and administration password to access further pages.

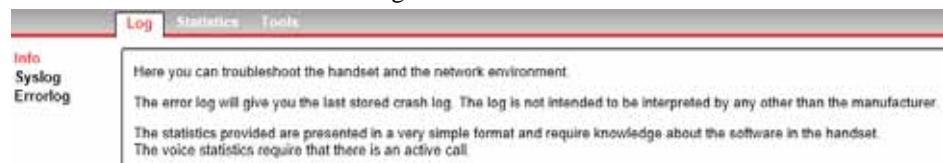
Default user name and password for an administrator:

- User name: admin
- Password: changeme

In the "Log", "Statistics" and "Tools" Tab, the following information is available (see [figure 18](#)):

- Syslog
- Errorlog
- Voice calls statistics
- WLAN connectivity statistics
- Network diagnostics tools (Ping and Traceroute)

Figure 18. Internal Web Administration Page - Troubleshoot View



## Change Administration Password

**Note:** The administration password can only be changed using the WinPDM.

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



# Administration

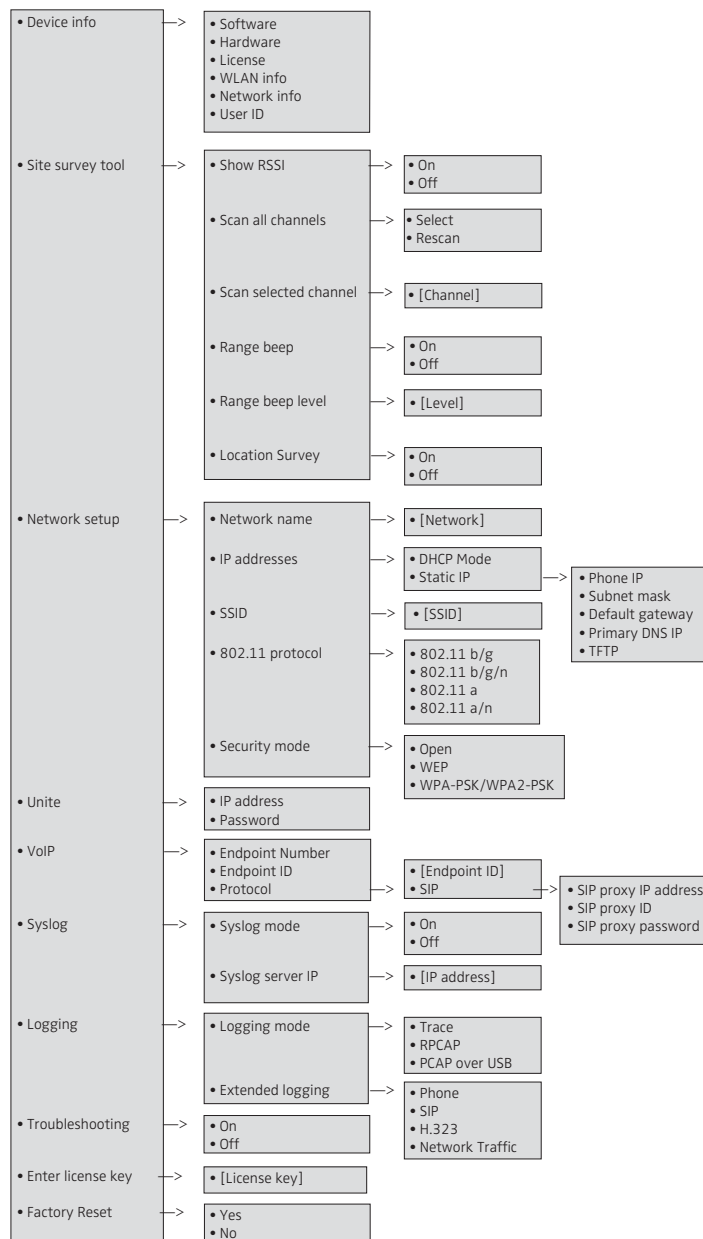
## Admin Menu Tree

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

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

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

Figure 19. Admin Menu in the Handset



Other menus are described in *Mitel Wireless 5624 Handset User Guide*.

## Quick Access to the Handset's Device Information

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

Information	Code
Software version	*#34# > Software
WLAN 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 license	*#34# > License
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 section [Handset Internal Web Administration Page](#) on page 79.

## 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.

---

# 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.

## 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	The handset is muted, 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.
Not possible to mute the handset by long press on the Sound off key/mute button	A handset restriction preventing the user to silence the handset.	Change the parameter Prevent silent (in Audio > General).
Not possible to set the ring volume to "Silent".		
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.
No entries in Call list	A handset restriction preventing calls from being saved in the call list.	Change the parameter Enable call list (in Device > Call > Enable call list > Yes
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 define 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 analyzer 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. Cisco/Ekahau location client settings need to be changed.	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 WinPDM. 7) If using Cisco/Ekahau location client, change the settings.

## 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 or the WSM3.	Switch off the handset and then switch it on again. If this does not work, contact the system administrator. 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. 4) Check the WSM3 address. Try to ping the WSM3 from another PC.
No network The handset beeps once a minute (for max 30 minutes) in a low tone, followed by a high tone (if enabled, the vibrator also follows the beeps).	The handset has lost connection and is in one of the following states: - No network (No connection to WLAN). - No access (Connection to WLAN but not to PBX nor IMS). - Voice only (Connection to WLAN, and PBX but not to the IMS (WSM3)). - Messaging only (Connection to WLAN, and IMS (WSM3) but not PBX).	Acknowledge the dialog window or press the mute button (the later keeps the dialog window visible). It is possible to configure the beep to Sound off or Sound once for each new state in the WinPDM (Device > General > No system warning). NOTE: When leaving a bad state for another bad state, the dialog window reopens, and the beep sounds again (if enabled).

Display shows	Probable cause	Action or comment
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.)	The handset is out of coverage, or faulty handset. The handset cannot find the wireless infrastructure with settings matching those configured in the handset.	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.
No channel available	The handset did not receive the expected answer from the PBX during call setup, or the user attempts to make a call when the handset is displaying "Messaging only".	Make another call (when the handset is not showing "Messaging only"). If the handset does not work after another try, contact the system administrator.
Voice only	The handset is configured to use both a gatekeeper and a WSM3, but has lost contact with the WSM3.	1) Check the WSM3 address. Try to ping the WSM3 from another PC. 2) Remove the handset from the Mitel 5624 Desktop Programmer. When connected to the WinPDM through USB on the Mitel 5624 Desktop Programmer, the handset cannot connect to the WSM3 and may then show "Voice only". 3) If messaging is not used in the system, verify that the WSM3 address is configured to 0.0.0.0.

**Display shows**

Messaging only

**Probable cause**

The handset is configured to use both a gatekeeper and an WSM3 but has lost contact with the gatekeeper.

**Action or comment**

1) Check the Gateway address. Try to ping the gateway from another wireless client.

2) Try to send a message. The idle connection check interval to the WSM3 is much longer than to the gateway. Sometimes when all network connection is lost the handset will show "Messaging only" for quite some time, because it discovers it has lost connection to the gateway much faster than it discovers loss of connection to the WSM3. In this case the handset will eventually change to "No access".

3) If the handset is supposed to use Gatekeeper discovery, verify that the configured Gatekeeper IP address is 0.0.0.0.

4) Check the Endpoint number and the Endpoint ID. If both are configured, they MUST match the Endpoint ID and Endpoint number registered in the IP PBX. Clear the Endpoint ID.

Select the reset option on the middle soft key. If this is not available or the problem persists send the handset for service.

SERVICE NEEDED

Parameters corrupt

NOTE: This display message is only shown in English.

Enter PIN code

Faulty handset.

Phone lock is activated.

Enter the required PIN code. If the PIN code has been lost, enter a new PIN code using the WinPDM/WSM3 or do a factory reset using the WinPDM/WSM3.

Battery low, charge now

The battery level is low.

Charge the handset, or replace or charge the battery.

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 using the admin menu or using the WinPDM/WSM3.

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 using the WinPDM/WSM3.

## 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 "Troubleshoot".  
Refer also to [Troubleshoot View](#) on page 80.

---

## Related Documents

Mitel Wireless 5624 Handset Data Sheet

Mitel Wireless 5624 Handset Quick Reference Guide

Mitel Wireless 5624 Handset User Guide

Mitel 5624 Desktop Programmer Data Sheet

Portable Device Manager, Windows version, Installation and Operation Guide

Wireless Messaging Gateway (WSM3) Installation and Operation Guide

IP-DECT System Global and Wireless System (EMEA) Wireless Handset Advanced Capability Licensing Guide

Mitel VoWiFi System Description

Mitel VoWiFi System Planning

Mitel VoWiFi Function Description





# Appendix A

## Working with Templates

This section describes how to manage templates when using both the WinPDM and the Device Manager in the WSM3.

When creating a template in the WinPDM and in the Device Manager, the templates must be identical to avoid that the template's parameters override each other when synchronizing the handset with WinPDM or Device Manager.

A template can be copied between WinPDM and Device Manager.

The following workflow describes how to create a template in the Device Manager and then copy it to the WinPDM. However, it is also possible to create a template in WinPDM and copy it to the Device Manager.

## Create a Template

1. Open the Device Manager in the WSM3.
2. Select the "Templates" tab and open the menu "Template > New...". The New Template window is opened.
3. Select the corresponding 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 and 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.

## Export a Template

1. Open the Device Manager in the WSM3.
2. Select the "Templates" tab.
3. Select the template to be exported.
4. Select "Template" > "Export". Alternatively, right-click the template and select "Export...". The Export templates window is opened.
5. Give the template (\*.tpl) a descriptive name and click "Save".  
See also A.3 Import a Parameter File.

## Import a Parameter File

The parameter version file (\*.def) the template is based on, must have been imported to the WinPDM to be able to import the template later on. If the parameter file is not imported, do as follows:

1. Open the WinPDM.
2. Select "File" > "File management".
3. Select the "Parameter definition" tab.
4. Click "Add". The Import files window is opened.
5. Locate the parameter file (\*.def), or the package file (\*.pkg) where the parameter file is included. Ask you supplier.

## Import a Template

1. Open the WinPDM.
2. Select “File” > “Import” > “Templates...”. The Import templates window is opened.
3. Locate the template to be imported.
4. Click “Open” to import the template.



# Appendix B

## Programming Custom Sound

**Note:** Applicable to Mitel 5624 Services and Mitel 5624 Alarm only.

Before starting programming custom sound, it is recommended to have basic knowledge about notes.

The melody in a custom sound is represented by a text string consisting of several elements.:

Element	Sub element	Values
Note	> Octave-prefix	*0 (A=55Hz)
		*1 (A=110Hz)
		*2
		*3
		*4 (default)
		*5
		*6
		*7
		*8 (A=14080 Hz)
		If no octave prefix is added, the prefix *4 will be used.
	Basic notes	c
		d
		e
		f
		g
		a
		b
	Ess notes (flat notes)	&d
		&e
		&g
		&a
		&b
	Iss notes (sharp notes)	#c
		#d
		#f
		#g
		#a
	Duration	0 (Full-note)
		1 (1/2-note)
		2 (1/4-note)
		3 (1/8-note)
		4 (1/16-note)
		5 (1/32-note)
Silence	> Rest Duration	r
		1 to 5 (1 = long pause, 5= short pause)

Element	Sub element	Values
	Duration specifier	. (Dotted note) : (Double dotted note) ; (2/3 length)
Vibration	N/A	Vibeon Vibeff
Repeat	N/A	@0 (repeat forever) @<number of repetitions>, for example: "@2" repeats the melody string 2 times.

Figure 20. Example of a melody/text string.

1 2 3 4 5 6 7 1 2 4 8 3 5  
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓  
**(\*6vibeonc3#c3vibeffr3@3)\*7vibeon#c3r1d3vibeff**

#### .Customize the default handset beeps

- 1 Octave-prefix
- 2 Vibration is turned on. The handset vibrates continuously.
- 3 Basic note with 1/8 duration
- 4 lss note with 1/8 duration
- 5 Vibration is turned off
- 6 Short pause
- 7 The melody within brackets is repeated 3 times before the handset plays the rest of the melody.
- 8 Long pause

If it is desired to create a custom sound out of any of the default handset beeps (Beep 1 - 7 and Enhanced beeps 1 - 7), the default definition of each beep can be used as a starting point for the further programming of the sound. The default definitions are as follows:

**Beeps:**

Beep 1:  
Beep 2:  
Beep 3:  
Beep 4:  
Beep 5:  
Beep 6:  
Beep 7:

**Definition (default):**

\*5b4r4  
(\*5b4r4@2)  
(\*5b4r4@3)  
(\*5b4r4@4)  
(\*5b4r4@5)  
(\*5b4r4@10)  
(\*6e4\*6a4\*6e4\*6a4r4@10)

**Enhanced beeps:**

Enhanced beep 1:  
Enhanced beep 2:  
Enhanced beep 3:  
Enhanced beep 4:  
Enhanced beep 5:  
Enhanced beep 6:  
Enhanced beep 7:

**Definition (default):**

\*6e2r2r1  
\*6e3r3e3r3r1  
\*6e4r4e4r4e4r4r1  
\*6c2r5:d2r5:e2r5r1  
\*6e4r4e4r4e4r3.e4r4e4r2e4r4e4r4e4r3.e4r4e4r4r1  
Beat 500, (\*5#f3g3#g3a3#a3b3\*6c3#c3d3#d3e3r3@9)  
\*6(c4e4@52)



# Appendix C

## Easy Deployment

With the Easy Deployment process, a handset is installed without the need for the WinPDM, by using a (staging) WLAN, with a predefined SSID and security profile.

**Note:** Easy Deployment can only be used in a 2.4 GHz staging WLAN. This is the default frequency band of the handset, when switched on. Thereafter the production WLAN is used with any configured channel and band.

### Prerequisites

- The WLAN network needs at least one AP on the 802.11b/g radio, that allows access to the WSM3 and uses the following default configuration, which cannot be changed:

SSID:	AWS-INIT
Security key:	WPA-PSK / WPA2-PSK
WPA-PSK passphrase:	AWS-INIT
- In the handset, all other network parameters must be at their default settings, which means for instance:

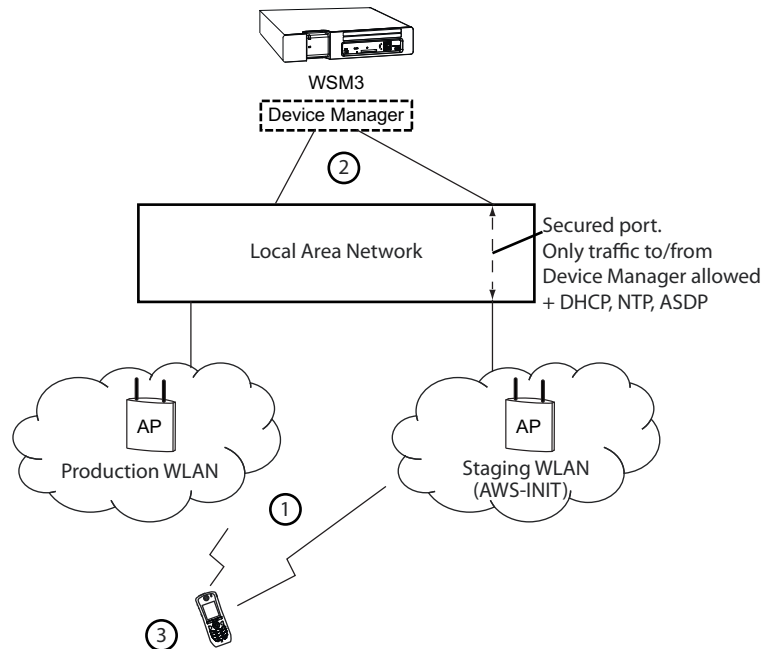
DHCP mode:	On
802.11 protocol:	802.11b/g/n
802.11b/g/n channels:	1,6,11
World mode regulatory domain:	World mode (802.11d)
- If it is used in the WSM3 server, the password to log in is needed.
- The WSM3 server port must be open and not blocked.
- No SSID for any of the networks A-D is configured in the handset.
- The DHCP offer for the AWS-INIT network must include an IP address of an NTP server, to provide the handset with the correct system time (needed for certificate validations).

**Note:** The intended number to be used by a handset, is entered from the handset's keypad, after a successful first access to the Messaging server(WSM3).

The Easy Deployment process, consists of three phases:

- WLAN discovery
- WSM3 server discovery
- Parameter download

Figure 21. Easy Deployment



## WLAN discovery

1. The WLAN discovery starts, when the new handset starts up. An already configured handset uses an entry stored in Network A, B, C, or D, and tries to associate with a WLAN, that uses the SSID, that once was configured in the Network A-D.

If there is no WLAN network (SSID) configured in the handset, the handset tries to associate with a predefined default WLAN with the SSID of AWS-INIT, on the 2.4 GHz frequency band on an AP running on channel 1, 6, or 11, see (1) in figure 21.

If the AWS-INIT is not connected to within ten seconds, the handset tries to connect to an open network. If this also fails, these two alternatives are tried for ten seconds each, until succeeded.

**Note:** It is not recommended to use an open network for staging, due to security reasons. The staging network (AWS-INIT) should be set up to only allow traffic to/from the WSM3, and services for Easy Deployment (like DHCP, NTP, ASDP). This is to block other, than dedicated clients, to use the network.

During this connection, a dialog window “No network” is displayed in the handset.

**Note:** The WLAN discovery process stops, if any SSID of Network A-D is manually filled in, either by using the handset’s Admin menu, or the WinPDM.

**Tip:** The SSID can be seen in the handset’s Admin menu; Press “Menu“, select “Settings” and enter 40022. In the Admin menu, select Device info > WLAN info. The SSID (channel): field shows the SSID (network name).

**Tip:** If the green wireless network connection bars (up in the left of the handset display) comes and goes alternately, the pre-shared key (PSK) on the AP is probably wrongly configured, and the handset cannot connect to the AP. After a time-out, “No network” is shown in the handset display.

## WSM3 server discovery

Once the handset has a WLAN connection, the second step is to automatically get the IP address to the WSM3, runs the Device Manager, see (2) in figure 21.

The two methods, on how to automatically get the IP address, are as follows:

- Using the vendor option functionality, Option 43 of a DHCP server
- Using the Ascom Service Discovery Protocol (ASDP) implemented in the handset

In both cases, the IP address received, is not saved, so this process is repeated on next startup, unless a WSM3 IP address is set.

### Server discovery using the DHCP Option 43

A DHCP server can be configured to return an WSM3 IP address, as a part of the DHCP response to the handset, together with other needed DHCP parameters. The WSM3 IP address is sent using Option 43 (Vendor Specific Data).

A DHCP request from a handset uses the Option 60 Vendor Class Identifier (VCI) to identify itself to the DHCP server. (The VCI string: Mitel\_WLAN\_Handset, is the Object Identifier (OID) for the handset). By this, a DHCP server can be configured to return an WSM3 IP address only to those clients that expect it. Option 60 also allows different clients to use different settings in the Option 43, if there are multiple clients in the network.

After the handset receives the (dynamic) IP address to the Messaging server(WSM3), it tries to login to the Device Manager. The DHCP Option 43 is ignored, once the WSM3 IP address is configured (static) in the WSM3 (the Device Manager, application). Setting up Option 43 on a DHCP server, is not that very well documented, and not very known by network administrators. There are many types of clients that can use this feature, for example, Cisco is using it for its LWAP APs to find a WLAN controller to attach to.

Examples on how to configure and troubleshoot Option 43 on a Linux and Microsoft Windows 2003/2008 server, is found at the end of this appendix.

### Server discovery using the Ascom Service Discovery Protocol (ASDP)

If the DHCP response does not contain a valid WSM3 IP address, the handset tries to find a WSM3 server using the Ascom Service Discovery Protocol (ASDP) instead. An ASDP discovery message is sent using UDP to the broadcast IP address, containing the MAC address of the handset.

An WSM3 server, configured to respond to ASDP discovery messages, responds with an ASDP offer as a unicast UDP message sent to the handset.

The protocol allows each WSM3 support different client services, and can separate different types of handsets WLAN to be serviced by different modules. If there are multiple WSM3 modules set up to support ASDP for WLAN, more than one response is received by the handset. A single response is randomly selected (normally the modules that responds fastest.)

If no response is received, a new ASDP request is retransmitted periodically, and the IP address remains unconfigured.

See the second section of The Ascom Service Discovery Protocol (ASDP) Explained on page 101, on how to configure an WSM3 to support the handset as an ASDP discovery client.

## Parameter download

1. After successfully receiving the WSM3 IP address, the handset tries to login to the Messaging system.

The handset has, at this stage, no number stored internally, and does not know its identity in the Messaging system. When the dialog window "Login:" is displayed in the handset, enter the intended endpoint number (that is, the phone number of the handset), that the handset uses to login to the Messaging system.

Once a valid endpoint number is stored in the handset, the handset tries to login.

After a successful login, the handset is synchronized with the parameters stored in the "Number record" in the Device Manager application (in the WSM3, see (1) in figure 21.

**Note:** It is vital, that especially the WLAN network settings, are configured correctly, as the handset receives a new set of parameters that contains the WLAN parameters for the production WLAN. It is also important that, if using any WLAN security protocol that uses certificates, the certificates (server/client) must be saved to each handset Number in the WSM3 (Device Manager application). If the WLAN parameters are wrong, the handset cannot associate with, neither the staging, nor the production WLAN, again.

**Tip:** If, by mistake, a wrong number is entered, when the dialog window "Login:" is displayed, make a factory reset, see [Perform a Factory reset](#) on page 23, and start over again.

**Note:** If there are no "Number records" already configured in the Device Manager before the handset logs in for the first time, perform as follows:

2. 1) In the Device Manager, be sure to check and save the automatically created "Numbers record" by right-clicking on the "Number's" entry. 2) Check in the created record, under Device > Unite > IP address, that the IP address for the Messaging system is correct. Then the handset can login to the same Device Manager again.

**Tip:** The Device Manager's IP address can also be checked by using the handset: In the handset's Admin menu, select "Device Info" > "Network info". Then scroll down to "Device manager:" to see the IP address.

## Using Easy Deployment together with Client Certificate Distribution

### The Ascom Service Discovery Protocol (ASDP) Explained

A handset can find the Messaging server (WSM3), using the Ascom Service Discovery Protocol (ASDP). The protocol is binary and uses Unite messaging.

For this purpose, a discovery message (BC) using the messaging protocol is sent, using UDP to the network's broadcast IP address. The discovery message contains the following data of the wanted service:

#### Client Description

Client class:	PP
Client family	WLAN
Client name:	< MAC Address of the handset >
etc.	

#### Service wanted

Service family:	""
Service name:	WGW
etc.	

A Messaging server (WSM3) that receives this message, responds with an offer (UC) as an unicast UDP message sent to the handset.

If more than one response is received by the handset, a single response is randomly selected. If no response is received, a new request is retransmitted periodically, while the IP address to WSM3 remains unconfigured.

#### *Configuring WSM3 to support WLAN service discovery clients*

For each module, the Ascom Service Discovery Protocol must be configured to support WLAN clients as follows:

1. Login in to the module and select Configuration > Other >Advanced configuration.
2. Select WLAN System and enable Service Discovery.

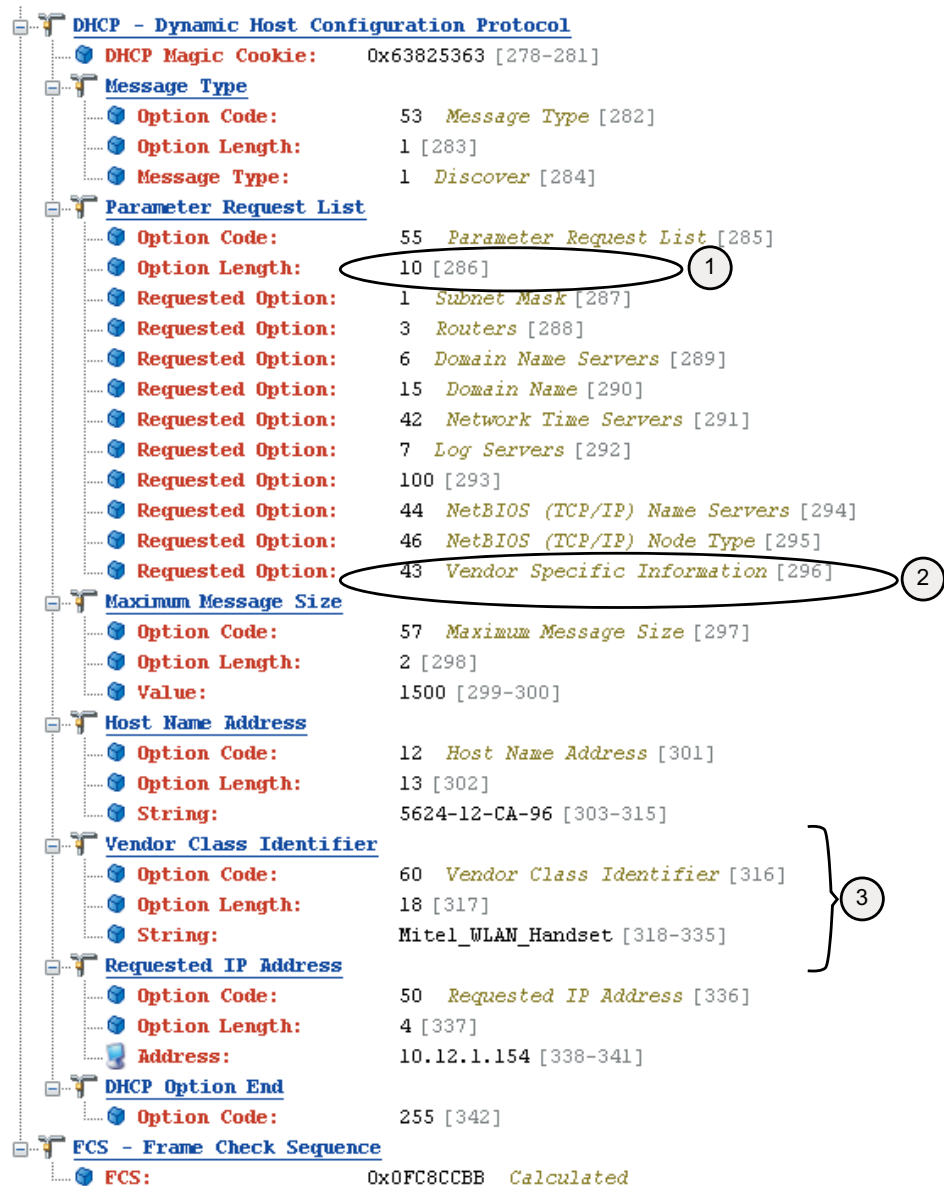
#### DHCP Vendor Options Explained

The Dynamic Host Configuration Protocol (DHCP) is described in the Request for Comment (RFC) No. 2131 and 2132. (The RFC is a publication of the Internet Engineering Task Force (IETF) and the Internet Society, which are the principal technical development and standards-setting bodies for the Internet.)

Although the RFC 2132 describes the BOOTP options and vendor options, the document lacks examples on how the vendor option 43 is used, configured, and troubleshooted, for a network administrator. An attempt to explain this, is made in the following sections of this [Appendix A](#).

The DHCP options described in the RFC 2132, can also, besides a DHCP server, also be used by a client. An example, on how a handset sends a DHCP Discover message to a DHCP server during the boot process, is shown in figure 22:

Figure 22. Example of a DHCP Discover message (Omnipeek trace).



In figure 22, the numbered points illustrate the following:

1. The amount of options requested
2. The handset asks for Vendor options

- The handset requests a specific set of Vendor options, by sending a Vendor Class Identifier (VCI)

Figure 23. Example of a DHCP Acknowledge (Omnipeek trace).



Figure 24. Example of a DHCP ACK in Hex (Omnipeek trace)



- In figure 23, the handset then sends a DHCP ACK, that confirms the settings the handset agreed upon to use, like the “43 Vendor Specific Information”. When comparing the, by the handset “Requested Options” in the trace in figure 22, it shows



that not all requests were agreed upon by the DHCP server. For example, the DHCP server does not acknowledge the options “42 Network Time Servers”, “7 Log servers”, and an, by Omnipieek unknown, option “100”. Some options are also added by the DHCP server (without being asked for by the handset), for example, option 58, 59, 51, and 54, which are compulsory.

### *The vendor 43 option field explained according to the RFC*

A DHCP server is configured with options prepared to supply clients with networking information that is requested, by the clients. Either the options are entered in the IP address scope, or for all scopes.

Less known, is that a selected set of options based on the client type, can be sent to clients. This allows a DHCP server to override the standard scope settings with other settings, which are unique for a specific client type, or transmit dedicated values, that are not part of the DHCP standard.

These are called “vendor options”, and they are sent to the client using option 43.

Adding vendor specific information to option 43, requires the use of tags (named fields), in the option 43 record. Such options are called “sub-options”, and they are included in the DHCP offer as type-length-value (TLV) blocks, embedded within Option 43. The definition of the sub-option codes and their related message format is left to the vendors.

The Option 43 is used in WLAN by several vendors. Handset vendors use Option 43 to send specific values to their family of handsets, and WLAN vendors use Option 43 to identify APs, and to find controllers (by distributing IP addresses using option 43). A dedicated tag for a specific client is only identified by a client which asks for it, and has a dedicated use for the tag. An example is the IP address to a WLAN controller, which probably only APs can use.

To avoid having to send all option 43 codes with useless tags to all clients, the use of option 60, makes a client identity itself as a specific client type. This type is then mapped to an entry in the DHCP server, which contains the vendor 43 options for that type.

Option 60 is normally coded as an ASCII string, but can also be binary. The Option 60 is called Vendor Class Identifier (VCI), and is defined by the manufacturer and programmed into the DHCP client of their devices.

The following table lists some examples of Option 60 string values:

Vendor	Device	String	Option 43 returned value
Ascom	i62 WLAN Handset	1.3.6.1.4.1.27614.2.2	Unite IP address
Aruba	Aruba AP	ArubaAP	Loopback address of Aruba master controller
Cisco	Cisco AP	Cisco AP c1250	IP address of WLAN controller
Siemens	WL3 WLAN Handset	OpenStageWL3	WSG IP address and hostname

### *Option 43 field definition*

The information in Option 43 is an opaque object of n octets, and the definition of this information is vendor specific.

**Option 43:**

Code	Length	Vendor specific information elements		
43 (2b)	n	i1	i2	i3 etc.

The code for the option is “43”, and its minimum length is 1. The number i1 ... etc refers to information bytes. The length value n refers to the amount information bytes in the field.

The value of the length octet does not include the two octets specifying the tag and length

*Option 43 with “Encapsulated vendor-specific information”:*

Normally a vendor needs to have multiple parameters to be used for configuration of the clients. Then the options are encoded using the “Encapsulated vendor-specific extensions”. This format uses the TLV syntax (type length value), and is described in RFC 2152. When “Encapsulated vendor-specific extensions” are used, the information bytes 1-n have the following format:

Code (tag)	Length	Data items			Code	Length	Data items			Code	Length
T1	n	D1	D2	...	T2	n	D1	D2	...	...	...

The different information bytes, sub-options, are in daily language called “tags”.

The tags codes are numbered options, created by the vendor like 01, 02, 83, 243 etc.

In the table above, the code for the option is “43”, as well as the total length, are omitted.

**Note:** Depending on the system that is used to configure the DHCP options, an administrator can enter each sub-option separately, or enter all values in a single concatenated string. Since each value contains a header, a length field, and the parameter itself, this can be difficult to enter correctly. Some servers require the entry of values in the hexadecimal format, while others use ASCII strings.

For the handset, the option 43 sub fields are defined according to the following table:

Code (tag)	Length	Data items	Code	Length	Data items	Code (optional)
01	5	Mitel	02	7-15	IP v4 address to WSM3 (Device Manager) (dot-decimal)	255

The code 255 is used as an optional marker of the end of the vendor field.

When entering this information in a DHCP server, the administrator must observe that the field length of the IP address can vary, depending on the amount of digits used. If, for example, using the address of 10.30.5.7, the length is 6 numbers, plus 3 dot-separators in all 9 bytes. If using an IP address like 192.168.100.101, the length is 15 bytes. Some server interfaces can assist in calculating the length.

Example:

To deploy a handset against an IMS3/Unite CM with IP address 10.30.4.120, the following data is be sent as option 43:

Hexadecimal:	<b>01:05:4D:69:74:65:6C:02:0B:31:30:2E:31:32:2E:31:2E:32</b>
Printable text:	\x01\x05Mitel\x02\x1210.30.4.120

**Note:** The first option in the OEM string (made bold in the table above), is used to verify that the data received in the client, is for the WLAN handset, this is called a “magic number”.

**Tip:** Search the internet for a tool that can assist in creating this string in Hexadecimal format.

**Vendor Class Identifier (VCI)****Vendor/OEM****Value**

Mitel

Mitel\_WLAN\_Handset

**Configuration Example of a Linux Server using DHCP Option 43**

The following example is from an Ubuntu Linux server, and the information is entered in the "/etc/ltsp/dhcpd.conf" file:

```
# Defining the option 43 with the proprietary sub-opcodes.
option space easy;
option easy.oem code 1 = string;
option easy.ims code 2 = string;

class "vendors" {
    match option vendor-class-identifier;
    vendor-option-space easy;
}

subclass "vendors" "1.3.6.1.4.1.27614.2.2" {
    option easy.oem "Ascom";
    option easy.ims "10.30.4.120";
}
```

There are two options, configured as code1 and code 2, and both are defined as strings.

The server maps the string "1.3.6.1.4.1.27614.2.2", that was received from the handset using option 60, as defined in the subclass paragraph.

Note that there is no need to describe the length of the fields.

**Configuration Example of an MS Windows 2003 Server using DHCP Option 43**

The DHCP server in a Microsoft Windows Server system, is by default already configured with the Vendor Classes seen in the table below, plus the DHCP standard options.

The standard options are used by all clients, while the Vendor class option adds/overrides options for specific clients.

Name	Options	Used by VCL clients with	Option 60 Vendor class mapping
Microsoft Windows 2000 options (Overrules the other two)	1, 3, 6, 15, 31, 33, 43, 44, 46, 47, 121 and 249	Windows 2000, and higher XP, Vista, Win7 and Win 8	"MSFT 5.0"
Microsoft Windows 98 options		Windows 98 and Window ME	"MSFT 98"

Name	Options	Used by VCL clients with	Option 60 Vendor class mapping
Microsoft options		Windows 98, Me and 2000 clients	"MSFT"

An administrator can add new Vendor classes as described below in the section Define new vendor class to support multiple types of clients on page 110. But it is not possible to delete the Microsoft built in classes and the standard class.

The DHCP server is pre-configured with a list of normally used DHCP options. Any missing DHCP option can be added as an administrator-defined option, either for each scope, or for the whole server.

### Configuration of Option 60 and 43 using the standard DHCP vendor class

Adding the option 60 and 43 to the standard set of DHCP, at least for a lab environment this is a simple, small and fast solution, but has the following drawback: There can only be one set of options configured per scope, so having different vendor's equipment in the system, requires different scopes. For example, lightweight APs and handsets may not use the same scope.

Option 43 should then contain a complete data set with all needed sub-options stored in a TLV format. This is, in some literature, described as using the RAW format of option 43. The TLV format is best entered using a data type of binary.

**Note:** By configuring option 43 direct on the standard scope, any DHCP client is offered this value, independent of the Vendor Class ID that is used by the client. Only clients who understand the received string benefit from this value. Trying to solve this problem, by manually setting option 60 to a specific Vendor Class ID on the standard scope, has no effect. On a Microsoft DHCP server, the Vendor class IDs are entered using a dedicated procedure, which allows the usage of Multiple Vendor Classes. This is why option 60 is not listed as an option in the default standard DHCP class. There is, therefore, no need to enter Option 60 values direct on a scope by creating a new option.

**Tip:** There are several documents on the internet that gets this process wrong.

#### *Configuration of Option 43*

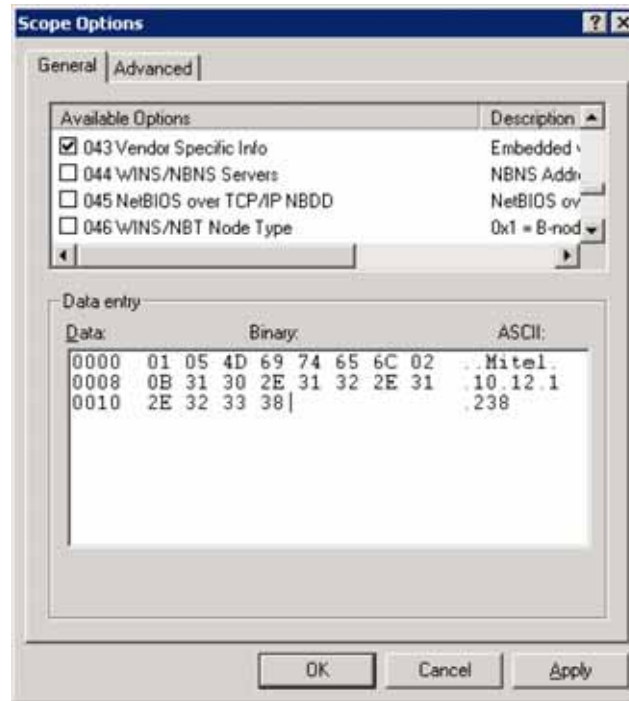
The following example illustrates how to set a vendor 43 option on the standard DHCP class, which is feasible if only vendor option 43 is needed:

**Note:** If set, this option 43 is also offered to client computers.

1. On the DHCP server, click the scope that the handsets should use, then right-click on Scope Options, and select Configure Options.
2. On the "General tab" (the default Standard DHCP class), scroll down, and select option 043 (which is the "Vendor Specific Info" option).
3. In the data entry field, there are two ways of entering the information. Click to the left in the box, to enter the string in binary, and to the right, to enter the string in ASCII. (It is possible to switch between them.)

Enter the values, as described in previous sections. Remember to get the length values in the TLV string correct.

Figure 25. Option 43 using a standard DHCP vendor class.



**Tip:** If the length value is unknown, enter the TLV value as follows, as everything inside the parenthesis is auto calculated using the “Auto-len” feature:

01 ("Mitel")02(192.168.5.1)

Then click OK and save the new option 43.

4. Check that the options are entered correctly. Note that the Vendor class is “Standard”, which means that no specific class is used, and that the User class is “None”, which means that it is the default user class. The handset does not send any request with a user class filled in.

**Note:** Do not enter the value 2b 14 (43 20), which is the option class and the total length. This is added by the DHCP server, when this option is presented to the client.

5. Test the configuration. If the Option 43 is not working as expected, verify the behavior with a packet capturing tool.

### Advanced Configuration of Option 60 and 43 using a new vendor class

The recommended way of setting up Vendor options, is to use Vendor classes, instead of the Global standard Default DHCP class. With this solution, option 60 is not configured as an option in a scope, instead a Vendor class is created.

Microsoft uses a method, that allows the administrator to set up the sub-options (that will be part of the vendor options, as a complete set of sub-options, which then are concatenated to the 43 option string by the server. Each sub-option (called “code”) is defined with the sub-option numbers, as described by the vendor. In the case of the VoWiFi handset, the sub-options are 01 and 02.

#### Notes:

- The DHCP server automatically calculates the length of each sub-option, and the total length of the whole string, and attaches the option ID of “43” at the beginning of the string.

- If option 43 is configured, using “code 43”, the “code 43” option is added to the concatenated string. Then double headers are added (one created by you, and one created by the system), and the string is not functioning as intended.

Instead, fill in the created sub-options with correct values. The sub-options are then automatically concatenated to the string, and creates an option 42 on the fly.

#### *Define new vendor class to support multiple types of clients*

To include the needed information for a handset, an administrator has to define a new vendor class as follows:

1. Right click on the DHCP server object, and select “Define Vendor Classes”. Then click “Add”.
2. In the New Class dialog box, enter a descriptive name for the Vendor class. For example enter, in the Display name: field: “Mitel5624 handset”, and in the Description: field: “Option 43 for Easy Deployment”. These fields are only used for displaying information for the administrator. In the ID: field, enter the VCI string seen in the table in Appendix (Mitel\_W-LAN\_Handset). Then click “OK”.

**Tip:** Click on the right side of the field to be able to write in ASCII.

**Note:** The VCI string has to exactly match with the vendor specification, since it is used in the mapping of the information sent from the handset in option 60 (case sensitive)

#### *Configure Sub-options for a vendor class in an MS Windows 2003 DHCP Server*

The current sub-options string for the handset contains two codes (which in some documentation from vendors, are referred to as “tags”). In order to build these two codes, they have to be defined as follows: one with the value of Mitel, and one with the IP-address of the WSM3Device Manager application).

1. Right click on the DHCP server and select “Set Predefined Options”.
2. Select the vendor class created earlier (in section [Define new vendor class to support multiple types of clients](#)) under “Option class” and click “Add”. The Option type window opens.
3. Enter a descriptive name for the first sub-option, for example enter, in the Name: field: “VoWiFi Vendor”, and in the Description: field: “Vendor Magic ID”
4. In the Data type: field, select “Binary”, to allow the entering of more than one byte.
5. In the Code: field, enter “001”. Then click “OK”.

**Note:** A predefined value (by selecting Edit Array) isn’t needed to be entered here. It can be preferred to be set per scope instead (explained below).

6. For the second sub-option, repeat the steps 1- 2 above.
7. Enter a descriptive name for the second sub-option, for example enter, in the Name: field: “WSM IP address”, and also copy it into the Description: field.
8. In the Data type: field, select “Binary”, to allow the entering of more than one byte.
9. In the Code: field, enter “002”. Then click “OK”.
10. Add the two sub-options to a scope and assign the values needed as follows:
  1. Right click on your scope, then select Scope Options > Configure Options.
11. Select the Advanced tab. In the Vendor class: field, select the new vendor class that was created in section [Define new vendor class to support multiple types of clients](#) (Mitel5624

handset). Checkmark the two sub-options that appear ("001 VoWiFi Vendor" and "002 WSM IP address").

**Note:** In the User class: field, leave the "Default User Class".

12. Select the first sub-option "001 VoWiFi Vendor" and enter the Vendor magic ID (Mitel or in Binary/Hex: 4D 69 74 65 6CE 73. Click to the left of the box for Binary code, and to the right for ASCII code.

**Notes:**

- Remove the 00 that is entered by default.
- A length value (in Data: field) isn't needed to be entered here (as normally done, when entering a TLV record). Then click "OK".

13. Select the second sub-option "002 WSM IP address" and enter the WSMIP address in Binary/Hex or ASCII. Then click "OK".

14. Test the configuration by factory reset a handset. If the configuration doesn't work, do a trace with a sniffer to see why.

**Tip:** Install Wireshark on the DHCP server and filter on the "bootp" protocol, to view the packet exchange when a handset is started up.

### *Configuration of DHCP options in a Cisco device running the Cisco IOS DHCP Server*

The Cisco IOS DHCP server only allows Option 43 definitions for one device type for each DHCP address pool, so only one device type can be supported for each DHCP address pool. Complete these steps in order to configure DHCP Option 43 for VoWiFi handsets:

1. Enter the configuration mode at the Cisco IOS command line interface (CLI).
2. Create the DHCP pool, which includes the necessary parameters, such as the default router and the server name. This is an example DHCP scope:

```
ip dhcp pool <pool name>
network <ip network> <netmask>
default-router <default-router IP address>
dns-server <dns server IP address>
```

3. Add the Option 60 line with the following syntax:  
option 60 ascii "VCI string of the handset"

**Note:** Avoid raw DHCP Option 43 without the specification of a VCI. Raw DHCP Option 43 limits the DHCP server to support a single device type for vendor specific information for each DHCP scope. Also, every DHCP client receives the Option 43 values in a DHCP Offer, regardless of whether the values are relevant to the device.

4. For the VCI string, use the value above. The quotation marks must be included. Add the Option 43 line with the following syntax:  
option 43 hex <hexadecimal string>  
This hexadecimal string is assembled as a sequence of the TLV values for the Option 43 sub-option: Type + Length + Value, as described above.

## Easy Deployment and VLAN

In a VoWiFi system, the WSM3 used for configuration must be positioned in the Voice VLAN, even if it is actually a data device (since the Voice and the Messaging services cannot be separated to two different SSIDs and thus not simply mapped to different VLAN in the AP/controller).



A mapping rule can, though, be created, that uses TCP/UDP port mapping, and connects the two services to different VLANs, instead of mapping SSIDs.

VLANs are not defined in the 802.11 standard. To achieve the same traffic separation for example between a Data and a Voice VLAN (and maybe including even a Deployment/Management VLAN), different SSIDs are used which are mapped to different VLAN IDs in the AP/Controller. The WLAN system must, therefore, be set up to support multiple SSIDs.

If using the AWS-INIT SSID on a single AP, be sure that the handset also can associate to the production SSID, after it has received its full configuration from the WSM3 (Device Manager application used for Easy Deployment.)

Remember that, when getting the production WLAN SSID, that it may be mapped to another VLAN, and that the IP address is changed, and also, that the DHCP server options are served by another scope, or eventually another DHCP server.

If using a deployment VLAN, you may be forced to have two Device Managers, or arranged for routing between VLANs.

You may try using a direct configuration of option 60 and option 43 on a scope by scope basis, if your system allows the separation of DHCP client devices to use independent scope ranges.

## Easy Deployment and Certificates

**Note:** If using a security model that requires certificates, also use an NTP server, to assure the correct time in the handset, as certificates only are valid within a certain time.

### *Client certificate*

If the production network is using individual client certificates, which for example are required for using EAP-TLS, first associate the certificates to the predefined number in the WSM3 (Device Manager) used for Easy Deployment, and after that select the required client certificate. Perform the steps, as described below in this section.

**Tip:** If there is no client certificate in the WSM3 (Device Manager) used for Easy Deployment, the handset is disconnected from the WLAN. To recover from this, first do a factory reset, and be sure that the client certificates are associated with the correct Number. You can also use the WinPDM to install the correct client certificate. Then try again.

### *Root certificate*

Upload at least one “Self-signed certificate” and up to three “Intermediate certificates”, which are used to establish the trust chain of the server certificate. The commonly understood name of these certificate types is “Root certificate”. Perform the steps of association of the root certificates as described below.

**Tip:** Information about certificates is described in the WSM3 Installation and Operation Guide (and also in the WinPDM Installation and Operation Guide), see . [Related Documents](#) on page 87.

### *Associate root/client certificates:*

1. In the Numbers tab, right-click the handset’s number and select “Manage certificates”. A Manage certificate window opens.
2. In the Root tab and Client tab, click “Browse” and select the certificates to import. Click “Close”.  
Select required client certificate:
3. In the Numbers tab, right-click the handset’s number and select “Edit parameters”.



4. Select "Network X" (X represents A, B, C, or D).
5. In the Security mode drop-down list, select "EAP-TLS".
6. In the EAP client certificate drop-down list, select the client certificate to be used. Click "OK".

## Troubleshooting Easy Deployment in an MS 2003/2008 DHCP Server

If you, by mistake, create a predefined DHCP option, and want to remove it, the server sometimes denies this operation (even if you have created the DHCP option). This is indicated by a grey Delete button. In such case, open a command prompt and use the "netsh" command as follows:  
`netsh dhcp server \\servername delete optiondef xx`  
where xx is the option number.



---

## Index

### A

Audio adjustment 38

### B

Baseline 42

### C

Central Phonebook 47

certificate 36

certificates 14

Company Phonebook 47

### E

Easy Deployment 9

### F

Factory reset 23

### H

Headset configuration 39

### I

Import Contacts 46

Installation 9

### L

LED indications 82

License upgrade 21

### O

over-the-air 8

### P

Profiles 47

### S

Services 73

Shared phone 42

Shortcuts 43

Site Survey Tool 43

### T

TFTP 19

### W

WinPDM 4



